Notas de versão para Rolling Patches

Esta seção contém as notas de versão para os patches contínuos recentes do XenMobile® Server. Clique em um link abaixo para ver os problemas corrigidos e conhecidos, as alterações de recursos e as ações necessárias.

O Rolling Patch mais recente contém todas as correções dos Rolling Patches anteriores para a mesma versão.

NOTAS DE VERSÃO PARA PATCHES DA VERSÃO ATUAL	DATA DE PUBLICAÇÃO	ARTIGO DE SUPORTE
10.16 Rolling Patch 9	Sep 17, 2026	Notas de Versão
10.16 Rolling Patch 8	Jan 27, 2026	Notas de Versão
10.16 Rolling Patch 7	Nov 13, 2025	Notas de Versão
10.16 Rolling Patch 6	Sep 26, 2025	Notas de Versão
10.16 Rolling Patch 5	Apr 22, 2025	CTX692919
10.16 Rolling Patch 4	Dec 18, 2024	CTX692370
10.16 Rolling Patch 3	Aug 28, 2024	CTX691503
10.16 Rolling Patch 2	Jul 02, 2024	CTX678043
10.16 Patch Contínuo 1	Jun 17, 2024	CTX677872

NOTAS DE VERSÃO PARA PATCHES DE VERSÕES ANTERIORES	DATA DE PUBLICAÇÃO	ARTIGO DE SUPORTE
10.15 Patch Contínuo 14	Jul 02, 2026	Notas de Versão
10.15 Patch Contínuo 13	Nov 20, 2025	Notas de Versão

XENMOBILE® SERVER

NOTAS DE VERSÃO PARA PATCHES DE VERSÕES ANTERIORES	DATA DE PUBLICAÇÃO	ARTIGO DE SUPORTE
10.15 Patch Contínuo 12	Oct 23, 2025	Notas de Versão
10.15 Pacote Cumulativo 11	May 13, 2025	CTX693257
10.15 Pacote Cumulativo 10	Jan 27, 2025	CTX692560
10.15 Pacote Cumulativo 9	Dec 04, 2024	CTX692268
10.15 Pacote Cumulativo 8	Jul 11, 2024	CTX691107
10.15 Pacote Cumulativo 7	Jun 06, 2024	CTX677079
10.15 Patch Contínuo 6	Mar 06, 2024	CTX625010
10.15 Patch Contínuo 5	Nov 13, 2023	CTX583748
10.15 Patch Contínuo 4	Sep 18, 2023	CTX579528
10.15 Patch Contínuo 3	Jul 19, 2023	CTX565649
10.15 Patch Contínuo 2	Apr 26, 2023	CTX546782
10.15 Patch Contínuo 1	Feb 23, 2023	CTX478719
10.14 Patch Contínuo 13	Mar 08, 2024	CTX628921
10.14 Patch Contínuo 12	Oct 19, 2023	CTX582535
10.14 Patch Contínuo 11	May 31, 2023	CTX558678
10.14 Patch Contínuo 10	Mar 23, 2023	CTX491036
10.14 Rolling Patch 9	Dec 20, 2022	CTX477055
10.14 Rolling Patch 8	Sep 22, 2022	CTX464099
10.14 Rolling Patch 7	Aug 18, 2022	CTX463691
10.14 Rolling Patch 6	May 23, 2022	CTX459871

NOTAS DE VERSÃO PARA PATCHES DE VERSÕES ANTERIORES	DATA DE PUBLICAÇÃO	ARTIGO DE SUPORTE
10.14 Rolling Patch 5	Mar 30, 2022	CTX399411
10.14 Patch Contínuo 4	Jan 26, 2022	CTX339069
10.14 Patch Contínuo 3	Dec 22, 2021	CTX335897
10.14 Patch Contínuo 2	Dec 15, 2021	CTX335763
10.14 Patch Contínuo 1	Nov 19, 2021	CTX335342

Notas de Versão para XenMobile Server 10.16 Rolling Patch 9 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 9. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 9 em Fazer login para baixar.

O que há de novo

- **Suporte para Habilitar informações do sistema na política de dispositivo de Configuração do Launcher:**

  Uma nova configuração, **Habilitar informações do sistema**, é adicionada à política de dispositivo de Configuração do Launcher para dispositivos Android Enterprise. Essa configuração permite que o Citrix Launcher exiba as informações do sistema na barra de status. O padrão é **Desativado** e requer o Secure Hub 26.8 ou posterior. Para obter mais informações, consulte Política de Configuração do Launcher.

- **Suporte para aplicativo de inicialização automática na política de dispositivo de Configuração do Launcher:**

  Uma nova configuração, **Aplicativo de inicialização automática**, é adicionada à política de dispositivo de Configuração do Launcher para dispositivos Android Enterprise. Essa configuração permite que os administradores selecionem um dos **Aplicativos permitidos** para iniciar automaticamente quando o Citrix Launcher for iniciado. O padrão é **Nenhum (não iniciar automaticamente)** e requer o Citrix Launcher 26.8 ou posterior. Para obter mais informações, consulte Política de Configuração do Launcher.

O XenMobile Server possui uma nova propriedade, `afw.launcher.auto_launch`, que permite aos administradores configurar o aplicativo de inicialização automática para dispositivos Android Enterprise configurados com políticas de Configuração do Launcher. O valor padrão é **False**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para a opção Pesquisar aplicativos para aplicativos de dispositivo:**

  No console do XenMobile Server, a página **Dispositivos > Detalhes do dispositivo > Aplicativos** agora inclui uma nova opção **Pesquisar aplicativos**.

- **Suporte para a política de dispositivo de Configurações de Aplicativo:**

  Uma nova política de dispositivo, **Configurações de Aplicativo**, é adicionada em **Configurações (Declarativas)**. Essa política permite configurar listas de permissão e negação de aplicativos usando o Gerenciamento Declarativo de Dispositivos da Apple. Esta política suporta apenas dispositivos iOS 27 e posteriores supervisionados. Para obter mais informações, consulte Política de dispositivo de Configurações de Aplicativo.

  O XenMobile Server possui uma nova propriedade, `ios.mdm.ios27.ddm.support`, que habilita a política de dispositivo de Configurações de Aplicativo. O valor padrão é **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para Número de Série em regras de implantação para iOS e macOS:**

  O XenMobile Server agora suporta uma nova regra de implantação, **Número de Série**, para iOS e macOS. Você adiciona esta regra em **Regras de Implantação > Avançado**.

- **Suporte para Android 17:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora oferecem suporte a dispositivos Android Enterprise executando o Android 17. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.

- **Suporte para iOS 27:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 27.

- **Renovação do certificado APNs do Secure Hub:**

  O certificado do serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.16 expira em November 9, 2026. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até September 18, 2027.

Problemas corrigidos

- As atualizações de aplicativos iOS por meio da /api/v1/application/store/{id}/platform/iphone REST API falham com o erro 1493.
- Após migrar de uma licença de Avaliação para uma licença do Serviço de Ativação de Licenças (LAS), o tipo de licença não é definido corretamente e a opção iOS está ausente no perfil de registro.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**
>
> Antes de instalar esta atualização, certifique-se de ter atualizado para o XenMobile Server versão 10.16.0.48. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.
>
> Para sistemas configurados no modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

   A página Release Management mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Release Management, clique em **Update**. A caixa de diálogo Update é exibida.
4. Clique em **Browse** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Update** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar até **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 9 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 9. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 9 em Fazer login para baixar.

O que há de novo

- **Suporte para Habilitar informações do sistema na política de dispositivo de Configuração do Launcher:**

  Uma nova configuração, **Habilitar informações do sistema**, é adicionada à política de dispositivo de Configuração do Launcher para dispositivos Android Enterprise. Essa configuração permite que o Citrix Launcher exiba as informações do sistema na barra de status. O padrão é **Desativado** e requer o Secure Hub 26.8 ou posterior. Para obter mais informações, consulte Política de Configuração do Launcher.

- **Suporte para aplicativo de inicialização automática na política de dispositivo de Configuração do Launcher:**

  Uma nova configuração, **Aplicativo de inicialização automática**, é adicionada à política de dispositivo de Configuração do Launcher para dispositivos Android Enterprise. Essa configuração permite que os administradores selecionem um dos **Aplicativos permitidos** para iniciar automaticamente quando o Citrix Launcher for iniciado. O padrão é **Nenhum (não iniciar automaticamente)** e requer o Citrix Launcher 26.8 ou posterior. Para obter mais informações, consulte Política de Configuração do Launcher.

  O XenMobile Server possui uma nova propriedade, `afw.launcher.auto_launch`, que permite aos administradores configurar o aplicativo de inicialização automática para dispositivos Android Enterprise configurados com políticas de Configuração do Launcher. O valor padrão é **False**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para a opção Pesquisar aplicativos para aplicativos de dispositivo:**

  No console do XenMobile Server, a página **Dispositivos > Detalhes do dispositivo > Aplicativos** agora inclui uma nova opção **Pesquisar aplicativos**.

- **Suporte para a política de dispositivo de Configurações de Aplicativo:**

Uma nova política de dispositivo, **Configurações de Aplicativo**, é adicionada em **Configurações (Declarativas)**. Essa política permite configurar listas de permissão e negação de aplicativos usando o Gerenciamento Declarativo de Dispositivos da Apple. Esta política suporta apenas dispositivos iOS 27 e posteriores supervisionados. Para obter mais informações, consulte Política de dispositivo de Configurações de Aplicativo.

O XenMobile Server possui uma nova propriedade, `ios.mdm.ios27.ddm.support`, que habilita a política de dispositivo de Configurações de Aplicativo. O valor padrão é **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para Número de Série em regras de implantação para iOS e macOS:**

  O XenMobile Server agora suporta uma nova regra de implantação, **Número de Série**, para iOS e macOS. Você adiciona esta regra em **Regras de Implantação > Avançado**.

- **Suporte para Android 17:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora oferecem suporte a dispositivos Android Enterprise executando o Android 17. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.

- **Suporte para iOS 27:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 27.

- **Renovação do certificado APNs do Secure Hub:**

  O certificado do serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.16 expira em November 9, 2026. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até September 18, 2027.

Problemas corrigidos

- As atualizações de aplicativos iOS por meio da /api/v1/application/store/{id}/platform/iphone REST API falham com o erro 1493.
- Após migrar de uma licença de Avaliação para uma licença do Serviço de Ativação de Licenças (LAS), o tipo de licença não é definido corretamente e a opção iOS está ausente no perfil de registro.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**

> Antes de instalar esta atualização, certifique-se de ter atualizado para o XenMobile Server versão 10.16.0.48. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.

> Para sistemas configurados no modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

   A página Release Management mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Release Management, clique em **Update**. A caixa de diálogo Update é exibida.
4. Clique em **Browse** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Update** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar até **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 8 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 8. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 8 em Fazer login para baixar.

O que há de novo

- **Suporte para Gerenciamento Declarativo de Dispositivos (DDM):**

O XenMobile Server adiciona suporte ao Gerenciamento Declarativo de Dispositivos (DDM) da Apple no iOS 15 e posterior. Esse recurso melhora o desempenho e a escalabilidade usando um modelo de dados declarativo, reduzindo a dependência de comandos serializados e sondagem de dispositivos. Para obter mais informações, consulte Aproveitando o modelo de dados de gerenciamento declarativo para escalar dispositivos.

O XenMobile Server possui as duas novas propriedades a seguir:

`ios.mdm.declarative.management`: habilita o Gerenciamento Declarativo de Dispositivos (DDM) do iOS.

`ios.mdm.software.update.settings`: habilita a política de dispositivo de Imposição de Atualização de Software.

O valor padrão de ambas as propriedades é **False**. Para obter mais informações, consulte Propriedades do servidor.

As seguintes políticas de dispositivo declarativas são suportadas quando você habilita o recurso DDM:

- Conta do Google
- Código de Acesso
- Imposição de Atualização de Software
- Configurações de Atualização de Software
- Assinaturas de Status
- Identidade do Usuário

- **Suporte para recuperação de informações de dispositivo relacionadas à rede da operadora para dispositivos iOS:**

  O XenMobile Server agora oferece suporte à recuperação de informações adicionais do dispositivo relacionadas à rede da operadora para cada SIM em dispositivos iOS. Você pode visualizar esses detalhes em **Detalhes do dispositivo > Propriedades > Informações do SIM do Slot x**. Os campos recém-suportados incluem:

  - Slot x — versão das configurações da operadora
  - Slot x — rede da operadora atual
  - Slot x — código de país móvel atual (anteriormente listado em Informações de rede)
  - Slot x — código de rede móvel atual (anteriormente listado em Informações de rede)

- Slot x — dados preferenciais
- Slot x — em roaming
- Slot x — voz preferencial
- Slot x — ID do rótulo

- **Suporte à autenticação OAuth para Microsoft Exchange Online:**

  A Microsoft anuncia que o Exchange Online removerá permanentemente o suporte para autenticação Básica com Envio de Cliente (SMTP AUTH) em março de 2026 e atingindo 100% de rejeições em April 30, 2026. Para obter mais informações, consulte Exchange Online to retire Basic auth for Client Submission (SMTP AUTH).

  O XenMobile Server oferece suporte à autenticação OAuth para o servidor SMTP. Habilite essa capacidade selecionando **Microsoft Exchange Online OAuth 2.0** e fornecendo o **ID do Locatário**, **ID do Cliente** e **Segredo do Cliente** necessários. A Citrix recomenda mudar para a autenticação OAuth se você usa o Microsoft Exchange Online. Para detalhes de configuração, consulte Notificações.

- **Suporte para impedir que dispositivos iOS façam a configuração por proximidade:**

  O XenMobile Server adiciona uma nova opção **Na próxima reinicialização, a Configuração por Proximidade não é permitida e o painel no Assistente de Configuração será ignorado** para limpeza completa do dispositivo. Esta opção impede que dispositivos iOS façam a configuração por proximidade durante a configuração do dispositivo. O recurso está disponível para iOS 11.3 e posterior. Para obter mais informações, consulte Ações de segurança.

- **Aprimorar o Inventário de Aplicativos para oferecer suporte à recuperação do tamanho de aplicativos iOS 26.x:**

  O XenMobile Server oferece suporte à recuperação de informações de tamanho de aplicativos para dispositivos que executam iOS 26.x. Você pode encontrar as informações em **Detalhes do dispositivo > Aplicativos**.

Problemas corrigidos

- Operações como o gerenciamento de dispositivos, aplicativos e grupos de entrega no console do XenMobile Server tornam-se visivelmente mais lentas e, às vezes, falham após a atualização para o 10.16 Rolling Patch 5.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**

> Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.16.0.48 do XenMobile Server. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.

> Para sistemas configurados no modo cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Configurações > Gerenciamento de Versões**.

   A página Gerenciamento de Versões mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Gerenciamento de Versões, clique em **Atualizar**. A caixa de diálogo Atualizar é exibida.
4. Clique em **Procurar** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Atualizar** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 7 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 7. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 7 em Fazer login para baixar.

O que há de novo

- **Suporte aprimorado para dual SIM e eSIM em dispositivos Android Enterprise:**

O XenMobile Server agora oferece suporte abrangente a dual SIM para dispositivos Android Enterprise para garantir a paridade de recursos com o iOS. Este aprimoramento permite que os administradores visualizem todos os cartões SIM e eSIMs instalados nas propriedades do dispositivo, incluindo configurações com dois cartões SIM físicos, um cartão SIM mais um eSIM, ou dois eSIMs. Esta atualização aborda a crescente adoção de dispositivos Android Enterprise com dual SIM e oferece aos clientes visibilidade completa sobre suas opções de conectividade de dispositivos móveis, correspondendo às capacidades de eSIM entregues anteriormente para dispositivos iOS. Este recurso é suportado apenas em:

- Secure Hub versão 25.7.0 ou posterior, e
- Android 13 ou posterior

O XenMobile Server possui uma nova propriedade `ae.esim.support`, que permite ao XenMobile Server obter as informações de eSIM dos dispositivos Android Enterprise e exibir as propriedades do dispositivo relacionadas ao eSIM na interface do usuário. O valor padrão desta propriedade é **True**. Para mais informações, consulte Propriedades do servidor.

- **Serviço de Ativação de Licenças:**

O XenMobile Server agora oferece suporte ao mecanismo de licenciamento do Serviço de Ativação de Licenças (LAS). O LAS é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa moderna ao licenciamento tradicional baseado em arquivo em todo o conjunto de produtos Citrix. Registre seu Citrix License Server com o Citrix Cloud para usar as licenças e direitos que seu Serviço de Ativação de Licenças possui. Para mais informações, consulte Serviço de Ativação de Licenças.

Importante:

Estamos em transição para uma arquitetura de licenciamento baseada em nuvem e padrão da indústria para a plataforma Citrix. Essa mudança automatiza o direito e a ativação, trazendo benefícios essenciais para o cliente:

- **Sem gerenciamento de arquivos de licença:** Elimina a necessidade de baixar, alocar ou gerenciar arquivos de licença, simplificando suas tarefas administrativas.
- **Atualizações automáticas de direitos:** Os direitos são atualizados automaticamente em segundo plano na renovação do contrato, garantindo um serviço ininterrupto.

- **Resiliência aprimorada:** O License Server não é mais um único ponto de falha para sessões de usuário, aumentando a estabilidade do seu ambiente.

Nós o encorajamos a usar o tempo que antecede a mudança para planejar e executar sua transição para adotar o novo modelo de licenciamento até April 15, 2026, e estamos comprometidos em apoiá-lo em cada etapa do processo. Para mais informações, consulte Anúncio de Licenciamento Moderno da Citrix.

- **Renovação do certificado APNs do Secure Hub:**

  O certificado do serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.16 expira em January 4, 2026. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até November 9, 2026.

- **Suporte a novas restrições do iOS para a versão 18.x do iOS:**

  Na política de Restrição para iOS, as seguintes novas configurações foram adicionadas para bloquear o acesso ao Apple Intelligence (IA) ou restringir alguns dos novos recursos. Essas configurações são aplicáveis para as versões 18 e posteriores do iOS. O padrão é **Ativado**. Para mais informações, consulte Política de Restrições.

  - Permitir integrações de inteligência externa
  - Permitir login em integrações de inteligência externa
  - Permitir Respostas Inteligentes no Mail
  - Permitir Transcrição de Notas
  - Permitir Resumo do Safari
  - Permitir resumo de inteligência visual
  - Permitir Resumo da Transcrição de Notas
  - Permitir Relatório de Inteligência da Apple
  - Permitir Modificação do Aplicativo de Chamada Padrão
  - Permitir Modificação do Aplicativo de Mensagens Padrão
  - Permitir IDs de Workspace de Inteligência Externa
  - Modificação do Navegador Padrão
  - Permitir Controle Remoto do FaceTime

Problemas corrigidos

- O registro do dispositivo falha devido ao alto uso de CPU e memória no servidor XenMobile.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**
>
> Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.16.0.48 do XenMobile Server. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.

> Para sistemas configurados no modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

   A página Release Management mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Release Management, clique em **Update**. A caixa de diálogo Update é exibida.
4. Clique em **Browse** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Atualizar** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Configurações > Gerenciamento de Versões > Atualizações**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 6

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 6. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 6 em Fazer login para baixar.

O que há de novo

- **Suporte para Android 16**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora suportam dispositivos Android Enterprise executando Android 16. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.

- **Suporte para iOS 26**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com iOS 26.

- **Suporte para notificações de atualização de política MDX legadas**

  O XenMobile Server agora exibe alertas de atualização quando os aplicativos MDX Secure Mail e Secure Web existentes que usam políticas legadas são atualizados para a versão 25.9.0.

- **Suporte a novos mapeamentos de certificado fortes para autenticação baseada em certificado**

  Um novo método de mapeamento é introduzido para permitir maior flexibilidade na emissão de certificados que atendam aos requisitos de mapeamento forte. O XenMobile Server agora anexa `URL=tag:microsoft.com` , `2022-09-14:sid:<user's SID>` ao Subject Alternative Name (SAN) dos certificados.

  - Para habilitar esse recurso para usuários existentes, os administradores de clientes devem adicionar a Propriedade de Cliente `MICROSOFT_CERTIFICATE_STRONG_MAPPING`. Para obter detalhes, consulte Propriedades do Cliente.
  - O mapeamento de certificado forte é suportado apenas no **Windows Server 2019 e posterior**. Para obter mais informações, consulte Mapeamento Forte da Microsoft.

- **Suporte a novas restrições do iOS para a versão 17.x do iOS**

  Na política de Restrição para iOS, a seguinte nova configuração foi adicionada para as versões 17.2 e posteriores do iOS. O padrão é **Ativado**. Para obter mais informações, consulte Política de Restrições.

- Permitir Correio de Voz ao Vivo

- **Caixa de texto da política de Gerenciamento de Configuração**

  Quando o cliente usa o **Knox Service Plugin** juntamente com a **política de Configuração Gerenciada**, o comprimento máximo de caracteres para todas as caixas de texto nas **Políticas de Aplicativos Separados** aumenta para 8.192 caracteres.

- **Suporte a novas opções do Assistente de Configuração do iOS na página Programas de Implantação da Apple**

  A Apple adiciona algumas novas telas de Opções do Assistente de Configuração do iOS para o registro no Apple Business Management. As seguintes novas opções são adicionadas na página **Configurações > Programas de Implantação da Apple > Opções do Assistente de Configuração do iOS**. Você pode configurar o XenMobile Server para ignorar essas telas. Para obter mais informações, consulte Opções do Assistente de Configuração do iOS.

  - Botão de Ação
  - Modo de Bloqueio
  - Inteligência
  - Botão da Câmera

- **Sincronizar com o Apple Business Manager para gerenciar atribuições de dispositivos**

  O XenMobile® Server (XMS) agora garante a atribuição precisa de dispositivos sincronizando com o Apple Business Manager (ABM). Esta atualização verifica se apenas os dispositivos corretamente atribuídos aparecem no XMS, impedindo registros de dispositivos que foram removidos do XMS e atribuídos a outra solução de gerenciamento de fornecedores. Por exemplo, se os dispositivos forem movidos para outra solução, eles não aparecerão mais no XMS após a sincronização.

  O XMS agora inclui uma nova propriedade `remove.unassigned.abm.devices`, que permite ao XMS remover dispositivos que não estão mais atribuídos a este servidor. Por padrão, esta propriedade é definida como **False**. Para obter mais informações, consulte Propriedades do servidor.

Problemas corrigidos

- O alerta Legacy MDX continua a ser exibido no console do XMS mesmo quando nenhum aplicativo Legacy MDX foi carregado.

- O botão de login fica esmaecido no portal do XenMobile quando a senha é inserida usando o botão direito do mouse e colar.
- Quando o recurso **Mostrar Nova Visualização** está ativado, a contagem de dispositivos é exibida incorretamente mesmo quando filtros são aplicados à lista de dispositivos.
- Usuários de iOS não conseguem iniciar os aplicativos Secure Mail/Secure Web e recebem o erro "Não é possível abrir" ao redirecionar do Secure Mail/Secure Web para o Secure Hub.
- Dispositivos do Programa de Registro de Dispositivos (DEP) continuam a realizar o registro **MDM+MAM** mesmo quando o Perfil de Registro está configurado como **somente MDM**.
- Quando um dispositivo iOS tem uma política de Bloqueio de Aplicativo para um aplicativo desinstalado, o dispositivo bloqueia com o erro "O aplicativo Acesso Guiado está indisponível. Entre em contato com o administrador" e a tela sensível ao toque para de responder, mesmo após uma reinicialização forçada.
- Ao registrar clientes Windows com a solução XenMobile MDM, a implantação do grupo de entrega falha. Como resultado, são necessárias operações de sincronização manual para aplicar as políticas enviadas. Como solução alternativa, é necessária a implantação manual em um único dispositivo.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**
>
> Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.16.0.48 do XenMobile Server. Também tire um instantâneo das configurações atuais e crie um backup do banco de dados.
>
> Para sistemas configurados no modo cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Configurações > Gerenciamento de Versões**.

A página Gerenciamento de Versões mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.

3. Em Gerenciamento de Versões, clique em **Atualizar**. A caixa de diálogo Atualizar é exibida.
4. Clique em **Procurar** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Atualizar** e então, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador, então navegar para **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 5 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 5. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 5 em Fazer login para baixar.

O que há de novo

- **Suporte a feedback de configurações gerenciadas (Technical Preview)**

  Este recurso permite que os administradores obtenham feedback sobre os estados dos aplicativos de dispositivos Android configurados com políticas de configuração gerenciadas. Para obter mais informações, consulte Suporte a feedback de configurações gerenciadas (Technical Preview).

  O XenMobile Server agora inclui uma nova propriedade `afw.app_managed_configurations.feedback`, que habilita o recurso que permite aos administradores obter feedback sobre os estados dos aplicativos de dispositivos Android configurados com políticas de configuração gerenciadas. Por padrão, esta propriedade é definida como **False**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para filtros persistentes na página Dispositivo**

  Na nova página de dispositivo, os filtros agora são suportados para todas as opções **filtráveis**. Esses filtros são salvos entre as sessões para o usuário logado, eliminando a necessidade de o administrador reaplicar os mesmos filtros cada vez que visita a página de dispositivo. Os filtros são removidos automaticamente se a coluna correspondente for desmarcada.

- **Suporte para preservar o plano de dados para iPhone e iPad**

  Uma nova opção, Preservar Plano de Dados Celulares na Limpeza, está disponível ao realizar uma limpeza completa do dispositivo. Esta opção permite preservar o plano de dados celulares (por exemplo, eSIM) no dispositivo durante o processo de limpeza. Este recurso está disponível para versões do iOS 11 e posteriores. Para obter mais informações, consulte Ações de Segurança.

- **Suporte a novas configurações do iOS 18 para iOS**

  Na política de Restrição para iOS, as seguintes novas configurações foram adicionadas para bloquear o acesso à Apple Intelligence (IA) ou restringir alguns dos novos recursos. Essas configurações são aplicáveis para versões do iOS 18 e posteriores. O padrão é **Ativado**. Para obter mais informações, consulte Política de Restrições.

  - Gravação de Chamadas
  - Aplicativos a Serem Ocultados
  - Aplicativos a Serem Bloqueados
  - Resumo de E-mail
  - Mensagens RCS
  - Modificação do Navegador Padrão

- **Suporte a novas configurações do macOS 15 para macOS**

  Na política de Restrição para macOS, as seguintes novas configurações foram adicionadas para bloquear o acesso à Apple Intelligence (IA) ou restringir alguns dos novos recursos. Essas configurações são aplicáveis para versões do macOS 15 e posteriores. Para mais informações, consulte Política de Restrições.

  - Permitir Modificação de Compartilhamento de Mídia
  - Forçar Ignorar Alerta de Captura de Tela
  - Resumo de E-mail

Problemas corrigidos

- O administrador de Controle de Acesso Baseado em Função (RBAC) é desconectado inesperadamente ao alternar 'Mostrar Nova Visualização (Prévia Técnica)' na página Dispositivo se não tiver a permissão 'Propriedades do Servidor'.
- O ícone do aplicativo do Programa de Compra por Volume (VPP) não é atualizado quando o aplicativo é atualizado para uma nova versão.

- Quando a renovação do certificado MDM falha, o certificado antigo é marcado como revogado pelo XenMobile® Server, impedindo que o Secure Hub (SH) se reconecte ao servidor. Como resultado, o SH não consegue se comunicar com o servidor usando o certificado antigo, mesmo que ele ainda não tenha expirado.
- Quando o recurso **Prévia Técnica da Nova Visualização** está ativado, os administradores de Controle de Acesso Baseado em Função (RBAC) veem inesperadamente a caixa de entrada de pesquisa.
- Numerosos certificados de payload são gerados para dispositivos AE.
- Algumas políticas não são implantadas em dispositivos AE durante o novo registro quando a **condição de Implantação** está definida como "Somente quando a implantação anterior falhou" no **Agendamento de Implantação**.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 4

Estas notas de versão descrevem melhorias e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 4. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 4 em Sign-in to Download.

Novidades

- **Renovação do certificado APNs do Secure Hub**

  O certificado do serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.16 expira em February 9, 2025. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até January 4, 2026.

- **Suporte para macOS 15**

  O XenMobile® Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o macOS 15, mas atualmente não oferecem suporte a todos os novos recursos do macOS 15.

- **Suporte para iOS 18**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 18, mas atualmente não oferecem suporte a todos os novos recursos do iOS 18.

- **Suporte para Android 15**

O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora suportam atualizações de dispositivos Android Enterprise para Android 15. Para obter mais informações sobre os benefícios de segurança e privacidade, consulte a Android developer documentation.

- **Atualizar o documento da API REST Pública para incluir a API de Modo Perdido do dispositivo**

  Adicionada a API de Modo Perdido no Public Rest API document.

- **Modificar chamada de API para usar corpo da requisição em vez de URL**

  Atualizada a chamada de API para incluir os dados no corpo da requisição em vez de na URL no Public Rest API document.

- **Suporte para bloquear ou restringir o Apple Intelligence para iOS**

  Na política de Restrição para iOS, as seguintes novas configurações são adicionadas para bloquear o acesso ao Apple Intelligence (IA) ou restringir alguns dos novos recursos. Essas configurações são aplicáveis para versões do iOS 18 e posteriores. O padrão é **Ativado**. Para mais informações, consulte Política de Restrições.

  - Genmoji
  - Image Playground
  - Image Wand
  - iPhone Mirroring
  - Personalized Handwriting Results
  - Writing Tools

- **Suporte para bloquear ou restringir o Apple Intelligence para macOS**

  Na política de Restrição para macOS, as seguintes novas configurações foram adicionadas para bloquear o acesso ao Apple Intelligence (IA) ou restringir alguns dos novos recursos. Essas configurações são aplicáveis para versões do macOS 15 e posteriores. O padrão é **Ativado**. Para mais informações, consulte Política de Restrições.

  - Image Playground
  - iPhone Mirroring
  - Writing Tools

- **Suporte para instalar atualizações do SO imediatamente em dispositivos iOS**

Na política de dispositivo Controlar Atualização do SO, um novo botão de opção chamado **Instalar o mais rápido possível** é adicionado nas opções de atualização do SO para iOS. Este recurso permite que você instale as atualizações do SO previamente baixadas imediatamente em dispositivos iOS. Para mais informações, consulte Política de dispositivo Controlar Atualização do SO para iOS.

- **Suporte para preservar o eSIM quando o sistema apaga o dispositivo**

  Uma nova configuração, **Preservar eSIM ao Apagar**, é adicionada à Política de Restrição. Essa configuração garante que o eSIM seja preservado quando o sistema apaga o dispositivo devido a várias tentativas de senha falhas ou quando a opção **Apagar Todo o Conteúdo e Ajustes** é selecionada em **Ajustes** > **Geral** > **Redefinir**. Este recurso está disponível para versões iOS 17.2 e posteriores, com a configuração padrão definida como **Desativado**. Para obter mais informações, consulte Política de Restrições.

- **Suporte para bloqueio de aplicativos de terceiros distribuídos pela web**

  Na política de Restrição, uma nova configuração de aplicativos **Distribuição Web** é adicionada para bloquear aplicativos de terceiros distribuídos pela web em dispositivos iOS. Essa configuração é aplicável para versões iOS 17.5 e posteriores. Para obter mais informações, consulte Política de Restrições.

- **Suporte para gerenciar a funcionalidade de copiar e colar**

  Na política de Restrição, uma nova configuração **Exigir área de transferência gerenciada** é adicionada para permitir que a funcionalidade de copiar e colar siga as mesmas restrições que você aplica a **Documentos de aplicativos gerenciados em aplicativos não gerenciados** e **Documentos de aplicativos não gerenciados em aplicativos gerenciados**. O padrão é **Desativado**. Para obter mais informações, consulte Política de Restrições.

- **Suporte para Samsung Enhanced Attestation v3**

  O Samsung Enhanced Attestation v3 melhora a funcionalidade de segurança do XMS em dispositivos Samsung Knox. Para obter mais informações, consulte Samsung Knox Enhanced Attestation. O XenMobile Server agora inclui uma nova propriedade `afw.knox.attestation.v3`, que habilita o recurso que pode melhorar a funcionalidade de segurança do XMS em dispositivos Samsung Knox. Por padrão, esta propriedade é definida como **True**. Para obter mais informações, consulte Propriedades do servidor.

Problemas corrigidos

- O XenMobile Server não consegue registrar novos dispositivos Android Enterprise com sucesso devido a problemas de desempenho que surgem quando o SQL Server aciona mensagens de alerta.
- Embora o cliente tenha habilitado a configuração FIPS para **true**, os logs continuam a mostrá-la como desabilitada. Além disso, quando o cliente tenta modificar as configurações do banco de dados através da CLI, o XenMobile Server falha ao estabelecer uma conexão com o banco de dados, impedindo que a atualização seja aplicada.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.16 Rolling Patch 3 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 3. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 3 em Fazer login para baixar.

O que há de novo

- **Suporte para Retorno ao Serviço para iPhone e iPad**

  Com o recurso Retorno ao Serviço, o servidor MDM pode enviar um comando de apagamento que inclui detalhes de Wi-Fi e um perfil de registro MDM padrão para o dispositivo do usuário. O dispositivo então apaga automaticamente todos os dados do usuário, conecta-se à rede Wi-Fi especificada e se registra novamente no servidor MDM usando o perfil de registro fornecido. Para obter mais informações, consulte Ações de Segurança.

  O XenMobile Server agora inclui uma nova propriedade, `ios.mdm.return.to.service`, que habilita o recurso Retorno ao Serviço para iPhones e iPads executando iOS 17 ou posterior. Por padrão, esta propriedade é definida como **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Impor uma versão mínima do SO para concluir a configuração no Registro Automatizado**

  Com o iOS 17, os MDMs agora podem impor uma versão mínima do sistema operacional necessária para registrar dispositivos por meio do Registro Automatizado de Dispositivos. Para obter mais informações, consulte Implantar dispositivos por meio do Programa de Implantação da Apple.

O XenMobile Server agora inclui uma nova propriedade, `ios.mdm.minimum_os_version.enrollment`, que permite impor um requisito de versão mínima do SO para concluir a configuração durante o Registro Automatizado no iOS 17 ou posterior. Por padrão, esta propriedade é definida como **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte para acessar e usar o aplicativo de e-mail do perfil de trabalho a partir do perfil pessoal**

  Na política de dispositivo de Restrições, uma nova configuração **Acessar aplicativo de e-mail de perfis de trabalho e pessoal** é adicionada nas configurações do Android Enterprise. Esta configuração permite que você acesse e use o aplicativo de e-mail do perfil de trabalho a partir do seu perfil pessoal. Para obter mais informações, consulte Política de dispositivo de Restrições - Configurações do Android Enterprise.

  O XenMobile Server agora inclui uma nova propriedade, `afw.mailapp.crossworkprofile`, que habilita o recurso que pode acessar e usar o aplicativo de e-mail do perfil de trabalho a partir do perfil pessoal nas configurações do Android Enterprise. Por padrão, esta propriedade é definida como **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Suporte a novas restrições do iOS para as versões iOS 11.x, 12.x e 13.x**

  Novas configurações adicionadas na política de Restrições para iOS:

  - Permitir sessão temporária de iPad compartilhado
  - Permitir modificação de eSIM
  - Permitir conexões de unidade de rede
  - Permitir conexões de dispositivo USB
  - Permitir Buscar Meu Dispositivo
  - Permitir Buscar Meus Amigos
  - Permitir Teclado QuickPath
  - Forçar Wi-Fi ativado
  - Forçar autenticação antes do preenchimento automático
  - Modificar configurações de Hotspot pessoal

  Para obter mais informações, consulte Política de dispositivo de restrições - configurações do iOS.

- **Aprimoramento para a política de Configurações Gerenciadas do Android Enterprise**

O comprimento máximo de caracteres para todas as caixas de texto na página **Políticas de gerenciamento de aplicativos** na política de **Configurações Gerenciadas** foi aumentado para 4096 caracteres.

Problemas corrigidos

- A opção Atualizar não está disponível na loja do Secure Hub para aplicativos habilitados para MAM SDK com nova versão.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para o Lançamento do Pacote Cumulativo 2 do XenMobile Server 10.16

Estas notas de versão descrevem aprimoramentos, problemas corrigidos e problemas conhecidos para o XenMobile Server 10.16 Pacote Cumulativo 2. Você pode baixar os binários do software XenMobile Server 10.16 Pacote Cumulativo 2 em Entrar para Baixar.

Problemas corrigidos

- Após a atualização para a versão 10.16 do XenMobile Server, o XenMobile Server parou de enviar logs para o Servidor Syslog.
- O Firebase Cloud Messaging usando a API HTTP v1 não funciona corretamente quando um proxy está configurado.

Para obter informações sobre pacotes cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para Pacotes Cumulativos.

Notas de Versão para o Lançamento do XenMobile Server 10.16 Rolling Patch 1

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.16 Rolling Patch 1. Você pode baixar os binários do software XenMobile Server 10.16 Rolling Patch 1 em Fazer login para baixar.

O que há de novo

- **Suporte para bloquear aplicativos de terceiros para iOS 17.4 e posterior:** Na política de Restrição, uma nova configuração **Alternative App Marketplace** foi adicionada para impedir a instalação de aplicativos de mercados alternativos da web e impedir que quaisquer aplicativos

de mercados alternativos instalados instalem outros aplicativos. Para obter mais informações, consulte Política de dispositivo de restrições.

- **Exibir um alerta no console do XMS se houver aplicativos MDX com modo MDX herdado publicados:** Um alerta é exibido no console do XenMobile Server se você tiver aplicativos MDX com modo MDX herdado publicados. Para obter mais informações, consulte **Alerta de Descontinuação do MDX Legado** em Propriedades do Servidor.
- **Suporte para Firebase Cloud Messaging migrado para usar a nova API http v1:** As APIs legadas do FCM para HTTP serão descontinuadas pelo Google em June 21, 2024. Para fazer o FCM funcionar bem com a nova API, um novo campo **Arquivo de Chave da Conta de Serviço** foi adicionado à página Firebase Cloud Messaging para você carregar o arquivo JSON da chave da conta de serviço. Para obter mais informações, consulte Firebase Cloud Messaging.

  O XenMobile Server tem uma nova propriedade `afw.fcm.httpv1.migration`, que permite usar o Firebase Cloud Messaging com a nova API HTTP v1. O valor padrão desta propriedade é **False**. Para obter mais informações, consulte Propriedades do servidor.

  Para habilitar a API FCM V1 para XenMobile Server 10.16 Rolling Patch 1 e posterior, consulte o artigo da Central de Conhecimento CTX677031.

Problemas corrigidos

- Após a atualização para a versão 10.16 do XenMobile Server, os links da web opcionais são reinstalados continuamente.
- Após a atualização do XenMobile Server para a versão 10.16, os logs do Secure Hub não podem ser enviados para o suporte de TI quando você seleciona **Enviar logs do dispositivo para o suporte de TI** como **diretamente** nas configurações de **Suporte ao Cliente**.
- No console do XenMobile® Server > **Restrições** > **Android Enterprise**, a descrição da dica de ferramenta para a configuração da política **Configurar redes móveis** está incorreta em alemão.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.16.0, consulte Notas de versão para patches cumulativos.

Notas de Versão para o XenMobile Server 10.15 Rolling Patch 14

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 14. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 14 em Fazer login para baixar.

O que há de novo

- **Suporte para Android 17:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora oferecem suporte a dispositivos Android Enterprise que executam o Android 17. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.

- **Suporte à autenticação OAuth para Microsoft Exchange Online:**

  A Microsoft anuncia que o Exchange Online removerá permanentemente o suporte à autenticação Básica com Envio de Cliente (SMTP AUTH) em March 2026 e atingirá 100% de rejeições em April 30, 2026. Para obter mais informações, consulte Exchange Online descontinuará a autenticação Básica para Envio de Cliente (SMTP AUTH).

  O XenMobile Server oferece suporte à autenticação OAuth para o servidor SMTP. Habilite essa capacidade selecionando **Microsoft Exchange Online OAuth 2.0** e fornecendo o **ID do Locatário**, **ID do Cliente** e **Segredo do Cliente** necessários. A Citrix recomenda mudar para a autenticação OAuth se você usar o Microsoft Exchange Online. Para obter detalhes de configuração, consulte Notificações.

- **Aprimorar o Inventário de Aplicativos para oferecer suporte à recuperação do tamanho de aplicativos iOS 26.x:**

  O XenMobile Server oferece suporte à recuperação de informações de tamanho de aplicativos para dispositivos que executam iOS 26.x. Você pode encontrar as informações em **Detalhes do dispositivo > Aplicativos**.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**

> - Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.15.0.23 do XenMobile Server. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.

- Se você estiver atualizando do 10.15 RP2 ou de qualquer versão anterior, incluindo 10.15 RTM, siga as etapas em Para atualizar implantações XenMobile em cluster para atualizar todos os nós do cluster.

Para sistemas configurados em modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização do XenMobile Server (.bin) para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

   A página Release Management mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Release Management, clique em **Update**. A caixa de diálogo Update é exibida.
4. Clique em **Browse** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Update** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para o XenMobile Server 10.15 Rolling Patch 14

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 14. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 14 em Fazer login para baixar.

O que há de novo

- **Suporte para Android 17:**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora oferecem suporte a dispositivos Android Enterprise que executam o Android 17. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.
- **Suporte à autenticação OAuth para Microsoft Exchange Online:**

A Microsoft anuncia que o Exchange Online removerá permanentemente o suporte à autenticação Básica com Envio de Cliente (SMTP AUTH) em March 2026 e atingirá 100% de rejeições em April 30, 2026. Para obter mais informações, consulte Exchange Online descontinuará a autenticação Básica para Envio de Cliente (SMTP AUTH).

O XenMobile Server oferece suporte à autenticação OAuth para o servidor SMTP. Habilite essa capacidade selecionando **Microsoft Exchange Online OAuth 2.0** e fornecendo o **ID do Locatário**, **ID do Cliente** e **Segredo do Cliente** necessários. A Citrix recomenda mudar para a autenticação OAuth se você usar o Microsoft Exchange Online. Para obter detalhes de configuração, consulte Notificações.

- **Aprimorar o Inventário de Aplicativos para oferecer suporte à recuperação do tamanho de aplicativos iOS 26.x:**

  O XenMobile Server oferece suporte à recuperação de informações de tamanho de aplicativos para dispositivos que executam iOS 26.x. Você pode encontrar as informações em **Detalhes do dispositivo > Aplicativos**.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**
>
> - Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.15.0.23 do XenMobile Server. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.
> - Se você estiver atualizando do 10.15 RP2 ou de qualquer versão anterior, incluindo 10.15 RTM, siga as etapas em Para atualizar implantações XenMobile em cluster para atualizar todos os nós do cluster.

> Para sistemas configurados em modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização do XenMobile Server (.bin) para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

A página Release Management mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.

3. Em Release Management, clique em **Update**. A caixa de diálogo Update é exibida.
4. Clique em **Browse** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Update** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Settings > Release Management > Updates**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 13 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 13. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 13 em Fazer login para baixar.

O que há de novo

- **Serviço de Ativação de Licença:**

  O XenMobile Server agora oferece suporte ao mecanismo de licenciamento do Serviço de Ativação de Licença (LAS). O LAS é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa moderna ao licenciamento tradicional baseado em arquivo em todo o conjunto de produtos Citrix. Registre seu Citrix License Server no Citrix Cloud para usar as licenças e direitos que seu Serviço de Ativação de Licença possui. Para obter mais informações, consulte Serviço de Ativação de Licença.

  > **Importante:**
  >
  > Estamos fazendo a transição para uma arquitetura de licenciamento baseada em nuvem e padrão da indústria para a plataforma Citrix. Essa mudança automatiza o direito e a ativação, trazendo os principais benefícios para o cliente:

- **Sem gerenciamento de arquivos de licença:** Elimina a necessidade de baixar, alocar ou gerenciar arquivos de licença, simplificando suas tarefas administrativas.
- **Atualizações automáticas de direitos:** Os direitos são atualizados automaticamente em segundo plano após a renovação do contrato, garantindo um serviço ininterrupto.
- **Maior resiliência:** O License Server não é mais um único ponto de falha para sessões de usuário, aumentando a estabilidade do seu ambiente. Nós o encorajamos a usar o tempo que antecede a mudança para planejar e executar sua transição para adotar o novo modelo de licenciamento até April 15, 2026, e estamos comprometidos em apoiá-lo em cada etapa do processo. Para obter mais informações, consulte Anúncio de Licenciamento Moderno da Citrix.

Se o Serviço de Ativação de Licença estiver ativado no 10.15 Rolling Patch 13 ou Rolling Patches posteriores, a atualização direta para 10.16.0.48 redefine a configuração do Serviço de Ativação de Licença. Continue a aplicar os rolling patches 10.16 da versão 10.16 Rolling Patch 7 ou posterior, onde o Serviço de Ativação de Licença pode ser reconfigurado. Os dispositivos existentes permanecem inalterados.

Problemas corrigidos

- O registro do dispositivo falha devido ao alto uso de CPU e memória no servidor XenMobile.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Instalar atualizações do XenMobile Server

Importante:

- Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.15.0.23 do XenMobile Server. Também tire um instantâneo das configurações atuais e crie um backup do banco de dados.
- Se você estiver atualizando da versão 10.15 RP2 ou de qualquer versão anterior, incluindo 10.15 RTM, siga as etapas em Para atualizar implantações XenMobile em cluster para atualizar todos os nós do cluster.

> Para sistemas configurados no modo de cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login na sua conta no site da Citrix® e baixe o arquivo de atualização do XenMobile Server (.bin) para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Configurações > Gerenciamento de Lançamentos**.

   A página Gerenciamento de Lançamentos mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Gerenciamento de Lançamentos, clique em **Atualizar**. A caixa de diálogo Atualizar é exibida.
4. Clique em **Procurar** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Atualizar** e, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Configurações > Gerenciamento de Lançamentos > Atualizações**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 12 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 12. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 12 em Fazer login para baixar.

O que há de novo

- **Suporte a novos mapeamentos de certificado fortes para autenticação baseada em certificado**

  Um novo método de mapeamento é introduzido para permitir maior flexibilidade na emissão de certificados que atendam aos requisitos de mapeamento forte. O XenMobile Server agora anexa `URL=tag:microsoft.com` , `2022-09-14:sid:<user's SID>` ao Subject Alternative Name (SAN) dos certificados.

  - Para habilitar este recurso para usuários existentes, os administradores de clientes devem adicionar a Propriedade de Cliente `MICROSOFT_CERTIFICATE_STRONG_MAPPING`. Para obter detalhes, consulte Propriedades do Cliente.
  - O mapeamento forte de certificados é suportado apenas no **Windows Server 2019 e posterior**. Para obter mais informações, consulte Mapeamento Forte da Microsoft.

- **Suporte para iOS 26**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 26.

- **Suporte para Android 16**

  O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora suportam dispositivos Android Enterprise executando Android 16. Para obter detalhes sobre segurança e privacidade, consulte a documentação do desenvolvedor Android.

- **Caixa de texto da política de Configuração Gerenciada**

  Quando o cliente usa o **Knox Service Plugin** juntamente com a **política de Configuração Gerenciada**, o comprimento máximo de caracteres para todas as caixas de texto nas **Políticas de Aplicativos Separados** aumenta para 8.192 caracteres.

- **Renovação do certificado APNs do Secure Hub**

  O certificado do serviço Apple Push Notification (APNs) do Secure Hub para o XenMobile Server 10.15 expira em January 4, 2026. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até November 9, 2026.

Problemas corrigidos

- O botão Entrar fica esmaecido no portal do XenMobile quando a senha é inserida usando o botão direito do mouse e colar.
- Os usuários do iOS não conseguem iniciar os aplicativos Secure Mail/Secure Web e recebem o erro "Não é possível abrir" ao redirecionar do Secure Mail/Secure Web para o Secure Hub.
- Os dispositivos do Programa de Registro de Dispositivos (DEP) continuam a realizar o registro **MDM+MAM** mesmo quando o Perfil de Registro está configurado como **somente MDM**.
- Ao registrar clientes Windows com a solução XenMobile MDM, a implantação do grupo de entrega falha. Como resultado, são necessárias operações de sincronização manual para aplicar as políticas enviadas. Como solução alternativa, é necessária a implantação manual em um único dispositivo.

- Quando um dispositivo iOS tem uma política de Bloqueio de Aplicativo para um aplicativo desinstalado, o dispositivo bloqueia com o erro "Aplicativo Acesso Guiado Indisponível. Entre em contato com o administrador" e a tela sensível ao toque fica sem resposta, mesmo após a reinicialização forçada.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Instalar atualizações do XenMobile Server

> **Importante:**
>
> - Antes de instalar esta atualização, certifique-se de ter atualizado para a versão 10.15.0.23 do XenMobile Server. Além disso, tire um instantâneo das configurações atuais e crie um backup do banco de dados.
> - Se você estiver atualizando da 10.15 RP2 ou de qualquer versão anterior, incluindo a 10.15 RTM, siga as etapas em Para atualizar implantações XenMobile em cluster para atualizar todos os nós do cluster.

> Para sistemas configurados no modo cluster, siga estas etapas para atualizar cada nó, um após o outro:

1. Faça login em sua conta no site da Citrix® e baixe o arquivo de atualização (.bin) do XenMobile Server para um local apropriado.
2. No console do XenMobile Server de um nó, clique em **Settings > Release Management**.

   A página Gerenciamento de Versões mostra a versão do software atualmente instalada e uma lista de quaisquer atualizações, patches e upgrades que você carregou.
3. Em Gerenciamento de Versões, clique em **Atualizar**. A caixa de diálogo Atualizar é exibida.
4. Clique em **Procurar** para carregar o arquivo de atualização (.bin) que você baixou da página de downloads da Citrix.
5. Clique em **Atualizar** e, em seguida, se solicitado, reinicie o nó do XenMobile Server usando a linha de comando.

Para verificar a implantação do patch

Após instalar este patch, faça login no console do XenMobile Server como administrador e, em seguida, navegar para **Configurações > Gerenciamento de Versões > Atualizações**. Esta página mostra detalhes sobre o patch instalado mais recentemente.

Notas de Versão do XenMobile Server 10.15 Rolling Patch 11

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 11. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 11 em Fazer login para baixar.

Problemas Corrigidos

- Algumas políticas não são implantadas em dispositivos AE durante o recadastramento quando a condição de Implantação está definida como "Somente quando a implantação anterior falhou" no Agendamento de Implantação.
- Vários certificados de payload são gerados para dispositivos AE.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 10 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 10. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 10 em Fazer login para baixar.

Novidades

Renovação do certificado APNs do Secure Hub: O certificado do serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.15 expira em February 9, 2025. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado, válido até January 4, 2026.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 9 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 9. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 9 em Fazer login para baixar.

Novidades

- **Suporte para Android 15**: O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora suportam atualizações de dispositivos Android Enterprise para Android 15. Para obter mais informações sobre os benefícios de segurança e privacidade, consulte a documentação do desenvolvedor Android.
- **Suporte para iOS 18**: O XenMobile® Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 18, mas atualmente não suportam todos os novos recursos do iOS 18.
- **Suporte para macOS 15**: O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o macOS 15, mas atualmente não suportam todos os novos recursos do macOS 15.
- **Atualizar o documento da API Rest Pública para incluir a API de Modo Perdido do dispositivo**: Adicionada a API de Modo Perdido no documento da API Rest Pública.
- **Modificar chamada de API para ser corpo de postagem em vez de URL**: A chamada de API foi atualizada para incluir os dados no corpo da solicitação em vez de na URL no documento da API Rest Pública.
- **Caixa de texto da política de Configuração Gerenciada**: O comprimento máximo de caracteres para todas as caixas de texto na página **Políticas de gerenciamento de aplicativos** na política de Configurações Gerenciadas foi aumentado para 4.096 caracteres.

Problemas corrigidos

- A opção **Atualizar** não está disponível na loja Secure Hub para aplicativos habilitados para MAM SDK com nova versão.
- O XenMobile Server não consegue registrar novos dispositivos Android Enterprise com sucesso devido a problemas de desempenho que surgem quando o SQL Server aciona mensagens de alerta.
- Embora o cliente tenha habilitado a configuração FIPS para **true**, os logs continuam a mostrá-la como desabilitada. Além disso, quando o cliente tenta modificar as configurações do banco de dados através da CLI, o servidor XenMobile falha ao estabelecer uma conexão com o banco de dados, impedindo que a atualização seja aplicada.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para o XenMobile Server 10.15 Rolling Patch 8 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 8. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 8 em Fazer login para baixar.

Problemas corrigidos

- O Firebase Cloud Messaging usando a API HTTP v1 não funciona corretamente quando um proxy é configurado.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para patches cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 7 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 7. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 7 em Fazer login para baixar.

O que há de novo

- **Suporte para bloquear aplicativos de terceiros para iOS 17.4 e posterior:** Na política de Restrição, uma nova configuração **Alternative App Marketplace** foi adicionada para impedir a instalação de aplicativos de mercados alternativos da web e impedir que quaisquer aplicativos de mercados alternativos instalados instalem outros aplicativos. Para obter mais informações, consulte Política de dispositivo de restrições.
- **Exibir um alerta no console do XMS se houver aplicativos MDX com modo MDX herdado publicados:** Um alerta é exibido no console do XenMobile Server se você tiver aplicativos MDX com modo MDX herdado publicados. Para obter mais informações, consulte **Alerta de Descontinuação do MDX Herdado** em Propriedades do Servidor.
- **Suporte para Firebase Cloud Messaging migrado para usar a nova API http v1:** As APIs legadas do FCM para HTTP serão descontinuadas pelo Google em June 21, 2024. Para fazer o FCM funcionar bem com a nova API, um novo campo **Arquivo de Chave da Conta de Serviço** foi adicionado à página Firebase Cloud Messaging para você carregar o arquivo JSON da chave da conta de serviço. Para obter mais informações, consulte Firebase Cloud Messaging.

  O XenMobile Server possui uma nova propriedade `afw.fcm.httpv1.migration`, que permite usar o Firebase Cloud Messaging com a nova API HTTP v1. O valor padrão desta propriedade é **False**. Para obter mais informações, consulte Propriedades do servidor.

Para habilitar a API FCM V1 para XenMobile Server 10.15 Rolling Patch 7 e posterior, consulte o artigo da Central de Conhecimento CTX677031.

Problemas corrigidos

- Para o iPad Compartilhado do Apple Business Manager (ABM), o XenMobile® Server exibe os usuários logados como "anônimos" se eles não estiverem presentes no banco de dados do servidor antes do registro.
- Quando o aplicativo VPP público que suporta as plataformas MacOS e iOS é sincronizado com o XenMobile, apenas a plataforma iOS é exibida e a plataforma MacOS está ausente.
- Alguns aplicativos públicos do iOS no XenMobile Server não podem ser localizados na Apple Store.
- Após a atualização para o XenMobile Server 10.15 RP6, a configuração DEP "Aguardar a conclusão da configuração" não tem mais efeito, fazendo com que a página de assistência de configuração DEP apareça rapidamente em vez de aguardar o recebimento das políticas.
- Uma mensagem de erro “**java.util.ConcurrentModificationException**” é exibida na guia Gerenciar ao fazer login no console do XenMobile Server após a atualização.
- Após a atualização para o XenMobile Server 10.15 RP6, os links da web opcionais são reinstalados continuamente.
- No console do XenMobile Server > **Restrições** > **Android Enterprise**, a descrição da dica de ferramenta para a configuração de política **Configurar redes móveis** está incorreta em alemão.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 6 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 6. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 6 em Fazer login para baixar.

O que há de novo

- **Renovação do certificado APNs do Secure Hub**

  O certificado do Serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.15 expira em March 12, 2024. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado que expirará em February 9, 2025.

- **Adicionado novo campo Escopo do perfil em Configurações de política de Webclip para iOS**

  Para dispositivos iOS, um novo campo chamado **Escopo do perfil** é adicionado em **Configurações de política** na política de dispositivo Webclip. Este recurso permite que você selecione se a política se aplica a um usuário ou a um sistema. Para obter mais informações, consulte Política de dispositivo Webclip - configurações do iOS.

- **Atualizar regra de implantação para o aplicativo da loja pública usando a API REST**

  Um novo campo chamado **regras** é adicionado às APIs REST **Adicionar Novo Aplicativo da Loja Pública** e **Atualizar Aplicativo da Loja Pública**. Este recurso permite que você atualize as regras de implantação para o aplicativo da loja pública. Para obter mais informações, consulte a documentação da API REST Pública.

- **A política de dispositivo de atributos de aplicativo oferece suporte a novos atributos de aplicativo iOS**

  Agora você pode especificar os seguintes atributos para aplicativos instalados em dispositivos iOS:

  - **Aplicativo removível:** Especifique se o aplicativo pode ser removido pelos usuários quando é um aplicativo gerenciado.
  - **Habilitar download direto de domínio associado:** Especifique se o aplicativo pode fazer a verificação de associação de site reivindicada diretamente nos domínios.
  - **Domínios associados:** Especifique os domínios associados a serem adicionados a um aplicativo.

  Para obter mais informações, consulte Política de dispositivo de atributos de aplicativo.

- **Adicionada nova política de dispositivo Knox Platform for Enterprise Key**

  Uma nova política de dispositivo chamada **Knox Platform for Enterprise Key** foi adicionada. Esta política permite que você forneça as informações de licença necessárias do Samsung Knox Platform for Enterprise (KPE) e use as licenças KPE para aprimorar a segurança do seu dispositivo Samsung. Para obter mais informações, consulte a política de dispositivo Knox Platform for Enterprise Key.

- **Suporte para Apple Business Manager para iPads compartilhados**

  A partir do XenMobile Server 10.15 RP6, os iPads compartilhados suportam o Apple Business Manager (ABM) com o XenMobile Server. Este recurso permite que você faça login nos iPads

compartilhados usando as contas ABM e os utilize. Para obter mais informações, consulte Configurando iPads compartilhados.

> **Nota:**
>
> Atualmente, existe uma limitação neste recurso em que o usuário logado pode ser exibido como "Anônimo" no console do XenMobile® Server. Consequentemente, certas ações seguras, como "Excluir Todos os Usuários", podem falhar ao serem executadas em dispositivos, particularmente aqueles utilizados como iPads compartilhados. Para contornar esse problema, é recomendável adicionar manualmente usuários DEP (Apple IDs gerenciados) ao console do XenMobile Server, especialmente se você estiver usando iPads compartilhados do ABM. Uma solução permanente será incluída em futuras versões.

- **Adicionada nova ação de segurança chamada Excluir Todos os Usuários para iPads compartilhados**

  A partir do XenMobile Server 10.15 RP6, uma nova ação de segurança chamada **Excluir Todos os usuários** é adicionada para iPads compartilhados no XenMobile Server. Este recurso permite que você exclua todos os usuários do dispositivo. Para obter mais informações, consulte Ações de segurança para iPads compartilhados.

- **Clonar um grupo de entrega para usar como base para um novo grupo de entrega**

  Este recurso permite copiar um grupo de entrega complexo que inclui várias políticas, aplicativos e ações. Você pode então editar a cópia, como adicionar perfis de registro ou um novo conjunto de usuários do Active Directory. Para obter mais informações, consulte Clonar um grupo de entrega.

- **Suporte para atualização automática de aplicativos opcionais no iOS**

  A partir do XenMobile Server 10.15 RP6, uma nova propriedade de servidor chamada `apple.ios.optional_app_update` é adicionada. Esta propriedade permite que você atualize automaticamente os aplicativos opcionais no iOS. O valor padrão de `apple.ios.optional_app_update` é definido como `False`. Para obter mais informações, consulte Propriedades do Servidor.

  Para obter mais informações sobre a atualização automática de aplicativos opcionais comprados em volume, consulte Verificar atualizações de aplicativos.

- **Otimizar mecanismo de atualização de banco de dados**

  O processo de atualização do banco de dados é otimizado para garantir que cada cluster seja atualizado apenas uma vez. Isso permite minimizar o tempo de inatividade durante as atualizações do Rolling Patch no cluster HA.

Problemas corrigidos

- Não é possível implantar a política de dispositivo Webclip em dispositivos iOS compartilhados ao usar configurações ABM ou ASM.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 5 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 5. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 5 em Fazer login para baixar.

O que há de novo

- **Adicionado um novo campo obrigatório “Domínio” nas configurações 802.1x para Android Enterprise**

  Um novo campo **Domínio** é adicionado na página de configurações da política de rede da plataforma Android Enterprise para o tipo de autenticação **802.1x EAP**. Para obter mais informações, consulte Configurações 802.1x para Android Enterprise.

  O XenMobile Server tem uma nova propriedade `afw.network.domain.support`, que adiciona o campo *Domínio* nas **configurações 802.1x para Android Enterprise**. O valor padrão desta propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

- **Adicionada nova opção "Versão das atualizações do SO" na política Controlar Atualização do SO para iOS**

  Na política **Controlar Atualização do SO** para a plataforma **iOS**, uma nova opção **Versão das atualizações do SO** é adicionada após o campo **Frequência de atualização do SO**. Esta opção permite especificar a versão do SO a ser usada para atualizar os dispositivos iOS supervisionados. Para obter mais informações, consulte Configurações do iOS.

- **Adicionadas novas configurações na política de Restrições e na política do Exchange para iOS**
  - Adicionadas novas configurações **Permitir Mail Drop** na política do Exchange para iOS. Para obter mais informações, consulte Política de dispositivo do Exchange - configurações do iOS.
  - Adicionadas as seguintes novas configurações na política de Restrições para iOS:
    - Permitir inicialização para recuperação por um dispositivo não emparelhado
    - Instalar resposta de segurança rápida
    - Remover resposta de segurança rápida
    - Permitir proteção de privacidade de e-mail
    - NFC
    - Permitir App Clips
    - Permitir publicidade personalizada da Apple
    - Desbloqueio automático

    Para obter mais informações, consulte Política de dispositivo de restrições - configurações do iOS.
- **Atualizações do SO**
  - **Suporte para Android 14:** O XenMobile Server e os aplicativos de produtividade móvel da Citrix agora suportam atualizações de dispositivos Android Enterprise para Android 14. Para obter mais informações sobre os benefícios de segurança e privacidade, consulte a documentação do Android.
  - **Suporte para iOS 17:** O XenMobile® Server e os aplicativos de produtividade móvel da Citrix agora são compatíveis com o iOS 17, mas atualmente não suportam nenhum novo recurso do iOS 17.
  - **Suporte para macOS 14:** O XenMobile Server e os aplicativos de produtividade móvel da Citrix agora são compatíveis com o macOS 14, mas atualmente não suportam nenhum novo recurso do macOS 14.

Problemas corrigidos

- Após a atualização para o XenMobile Server 10.15 RP3 ou 10.15 RP4, o botão **Organizar Aplicativos** não está disponível na página **Configurar** > **Aplicativos** para **Android Enterprise** > **Aplicativos da Google Play Store Gerenciada**.

- Após a atualização para o XenMobile Server 10.15 RP3 ou 10.15 RP4, não é possível ver nenhum valor no menu suspenso **Certificado CA** ao configurar a política de Wi-Fi para a plataforma **Android Enterprise**. Apenas a opção **Selecionar certificado** é exibida.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para Patches Cumulativos.

Notas de versão para XenMobile Server 10.15 Rolling Patch 4

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 4. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 4 em Fazer login para baixar.

Novidades

- **Acesso a relatórios de Dispositivos e Aplicativos**

  Anteriormente, a página de relatórios de **Dispositivos e Aplicativos** exibia as informações sobre todos os dispositivos e aplicativos para todos os usuários, independentemente do grupo de usuários, mesmo que o controle de acesso baseado em função (RBAC) fosse aplicado.

  A partir da versão XenMobile Server 10.15 Rolling Patch 4, a página de relatórios de **Dispositivos e Aplicativos** exibe os dispositivos e aplicativos específicos dos grupos de usuários definidos na configuração **Para grupos de usuários específicos** que a função RBAC tem permissão para gerenciar. Para obter mais informações sobre como configurar funções com RBAC, consulte Configurar funções com RBAC.

- **Suporte para redefinir a política de dispositivo de Controle de Atualizações do SO para o padrão do sistema**

  A partir da versão XenMobile Server 10.15 Rolling Patch 4, um novo valor **Padrão** é adicionado à lista suspensa **Política de atualização do sistema** na página **Controle de Atualizações do SO** para Android Enterprise. Este recurso permite redefinir a Política de atualização do sistema para o padrão do sistema. Para obter mais informações, consulte Política de dispositivo de Controle de Atualizações do SO.

- **Adicionados novos campos URL de login OAuth e URL de solicitação de token OAuth nas configurações da política de dispositivo do Exchange para iOS**

  A partir da versão XenMobile Server 10.15 Rolling Patch 4, os campos **URL de login OAuth** e **URL de solicitação de token OAuth** são adicionados sob o botão de opção **Política do Exchange** > **iOS** > **Usar OAuth**. Para obter mais informações, consulte Política de dispositivo do Exchange.

- **Suporte para sincronizar ou substituir Serviços do Exchange Sincronizados para iOS**

  A partir da versão XenMobile Server 10.15 Rolling Patch 4, você pode escolher se deseja sincronizar ou substituir os seguintes Serviços do Exchange sincronizados para iOS ativando as configurações relevantes.

  - Calendários
  - Contatos
  - E-mail
  - Notas
  - Lembretes

  Para obter mais informações, consulte Política de dispositivo do Exchange.

- **Suporte para eSIM em dispositivos iOS**

  O XenMobile Server tem uma nova propriedade `ios.esim.support`, que permite ao XenMobile Server obter as informações do eSIM dos dispositivos iOS e exibir as propriedades do dispositivo relacionadas ao eSIM na interface do usuário. O valor padrão desta propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.15.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 3 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 3. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 3 em Fazer login para baixar.

Novidades

- **Suporte para tipos de licença mistos com o XenMobile Server.** Este recurso permite que os clientes ativem uma mistura de tipos e edições de licença do XenMobile usando o XenMobile Server ou o Citrix Licensing Server. Para obter mais informações, consulte Para ativar uma licença diferente.
- **Suporte para aplicativos Enterprise em dispositivos macOS.** O XenMobile Server tem uma nova propriedade `mac.app.push`, que permite o suporte a aplicativos Enterprise em dispositivos que executam macOS. O valor padrão desta propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

Problemas Corrigidos

- Você não consegue baixar aplicativos de **Contas Gerenciadas do Google Play**.
- No console do XenMobile® Server, você não consegue ver a versão do Rapid Security Response (RSR).
- Em dispositivos Android, quando os usuários mudam do MDX Toolkit legado para o MAM SDK, o aplicativo Secure Mail é removido da Secure Hub Store.
- Após a atualização para o XenMobile Server 10.15 RP2, as políticas de dispositivo de Restrições do iOS existentes que usam "**Uso de aplicativo restrito**" falham ao serem implantadas nos dispositivos iOS.

Notas de Versão para XenMobile Server 10.15 Rolling Patch 2 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 2. Você pode baixar os binários do software XenMobile Server 10.15 Rolling Patch 2 em Fazer login para baixar.

Novidades

Descontinuação da Ferramenta XenMobile Analyzer. Devido à nossa cadência de lançamento frequente e estável, a Ferramenta XenMobile Analyzer não é mais necessária. A Citrix descontinuou este serviço a partir de March 31, 2023. Recomendamos que você use as verificações de conectividade disponíveis no console do Citrix XenMobile ou no Citrix NetScaler Gateway. Para obter mais informações, consulte Verificações de conectividade.

Problemas Corrigidos

- Não é possível configurar aplicativos Enterprise na plataforma Android, usando o algoritmo APK Signature Scheme v2 e posterior.
- Não é possível acessar o MAM em dispositivos Android e iOS quando as políticas de autenticação nFactor são usadas no NetScaler.
- Ao exportar os scripts de configuração da Autenticação do Citrix Gateway em versões do XenMobile Server 10.14 ou posteriores, os scripts são truncados e não funcionam.
- No XenMobile Server, não é possível reeditar aplicativos VPP sincronizados cuja descrição contém **\b**.
- Nas versões 10.15 e posteriores do XenMobile Server, o Online Certificate Status Protocol (OCSP) não está respondendo às solicitações.
- No XenMobile® Server, não é possível registrar dispositivos que executam o Windows 11.

Notas de Versão do XenMobile Server 10.15 Rolling Patch 1

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.15 Rolling Patch 1. Você pode baixar os binários de software do XenMobile Server 10.15 Rolling Patch 1 em Entrar para Baixar.

Novidades

- **Controle de Acesso à Rede.** Use sua solução de Controle de Acesso à Rede (NAC) para estender a avaliação de segurança de dispositivos XenMobile para dispositivos Android e Apple. Sua solução NAC usa a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação. Depois de configurar seu appliance NAC, as políticas de dispositivo e os filtros NAC que você configura no XenMobile são aplicados. Para obter mais informações, consulte Controle de Acesso à Rede.
- **Renovação do certificado APNs do Secure Hub.** O certificado do Serviço de Notificação Push da Apple (APNs) do Secure Hub para XenMobile Server 10.15 expira em April 8, 2023. Esta atualização renova o certificado APNs do Secure Hub, que expirará em March 12, 2024.

Problemas Corrigidos

- Você recebe um erro ao editar ou implantar a política de configuração gerenciada em dispositivos Android Enterprise.
- Em dispositivos iOS registrados no modo somente MAM, você não consegue instalar aplicativos empresariais ou MDX da loja Secure Hub.
- Após configurar o ID de rastreamento de um aplicativo, você não consegue visualizar a versão de visualização esperada do aplicativo no console do XenMobile® Server. Em vez disso, você vê a versão de produção do aplicativo.
- No XenMobile Server, você não consegue instalar aplicativos empacotados em MDX da loja Secure Hub quando a política de dispositivo de perfil de provisionamento está em status pendente.
- Após a renovação do perfil MDM, os iPads compartilhados ABM entram em status não gerenciado.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 13 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 13.

Novidades

Renovação do certificado APNs do Secure Hub:

O certificado do Serviço de Notificação por Push da Apple (APNs) do Secure Hub para XenMobile Server 10.14 expira em March 12, 2024. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado que expirará em February 9, 2025.

Para obter informações sobre patches cumulativos anteriores para XenMobile Server 10.14.0, consulte Notas de versão para Rolling Patches.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 13 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 13.

Novidades

Renovação do certificado APNs do Secure Hub:

O certificado do Serviço de Notificação por Push da Apple (APNs) do Secure Hub para XenMobile Server 10.14 expira em March 12, 2024. Esta atualização renova automaticamente o certificado APNs do Secure Hub para um novo certificado que expirará em February 9, 2025.

Para obter informações sobre patches cumulativos anteriores para XenMobile Server 10.14.0, consulte Notas de versão para Rolling Patches.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 12 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 12.

Problemas Corrigidos

- Não é possível baixar aplicativos de **Contas Gerenciadas do Google Play**.
- Após a atualização para o XenMobile Server 10.14 RP11, a política de Restrição do iOS existente falha ao ser implantada no dispositivo.
- Ao registrar um dispositivo móvel no Secure Hub, os aplicativos não são exibidos na loja do Secure Hub e na loja gerenciada do Google Play.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 11 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 11.

Problemas Corrigidos

- Não é possível configurar aplicativos Enterprise na plataforma Android, usando o algoritmo APK Signature Scheme v2 e posterior.
- No XenMobile Server, não é possível reeditar aplicativos VPP sincronizados cuja descrição contém *b*.
- Nas versões 10.14 RP9 e posteriores do XenMobile Server, o Online Certificate Status Protocol (OCSP) não está respondendo às solicitações.
- No XenMobile® Server, não é possível registrar dispositivos que executam o Windows 11.
- No console do XenMobile Server, não é possível ver a versão do Rapid Security Response (RSR).

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para o XenMobile Server 10.14 Rolling Patch 10

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 10.

Novidades

- **Renovação do certificado APNs do Secure Hub.** O certificado do Apple Push Notification Service (APNs) do Secure Hub para o XenMobile Server 10.14 expira em April 8, 2023. Esta atualização renova o certificado APNs do Secure Hub, que expirará em March 12, 2024.
- **Descontinuação da Ferramenta XenMobile Analyzer.** Devido à nossa cadência de lançamento frequente e estável, a Ferramenta XenMobile Analyzer não é mais necessária. A Citrix decidiu descontinuar este serviço a partir de March 31, 2023. Recomendamos que você use as verificações de conectividade disponíveis no console do Citrix XenMobile ou no Citrix NetScaler Gateway. Para obter mais informações, consulte Verificações de conectividade.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problemas Corrigidos

- Após a renovação do perfil MDM, os iPads compartilhados do ABM ficam com status não gerenciado.
- Em dispositivos iOS registrados no modo somente MAM, não é possível instalar aplicativos empresariais ou MDX da loja Secure Hub.
- Não é possível acessar o MAM em dispositivos Android e iOS quando as políticas de autenticação nFactor são usadas no NetScaler.
- Ao exportar os scripts de configuração da Autenticação do Citrix Gateway em versões do XenMobile Server 10.14 ou posteriores, os scripts são truncados e não funcionam.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 9 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 9.

Novidades

Controle de Acesso à Rede. Use sua solução de Controle de Acesso à Rede (NAC) para estender a avaliação de segurança de dispositivos XenMobile para dispositivos Android e Apple. Sua solução NAC usa a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação. Depois de configurar seu dispositivo NAC, as políticas de dispositivo e os filtros NAC que você configura no XenMobile são aplicados. Para obter mais informações, consulte Controle de Acesso à Rede.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problemas Corrigidos

- Na versão 10.14 do XenMobile Server, você recebe um aviso de expiração de licença, mesmo que a data de expiração da licença esteja fora da janela de notificação.
- Em alguns aplicativos, você vê o status **Atualizações Pendentes** na loja de aplicativos do Secure Hub, mesmo que a versão instalada seja a mais recente.
- No XenMobile® Server, você não consegue criar ou editar a política de dispositivo Restrições no local alemão.
- Na versão 10.14 do XenMobile Server, a guia **Propriedade de** aparece em branco para dispositivos iOS que não são DEP.

- A política de dispositivo SCEP falha quando o **Tipo de nomes alternativos do assunto** não é *Nenhum*.
- Você recebe um erro ao editar ou implantar a política de configuração gerenciada em dispositivos Android Enterprise.
- Em dispositivos iOS registrados no modo somente MAM, você não consegue instalar aplicativos empresariais ou MDX da loja de aplicativos do Secure Hub.
- Após configurar o ID de rastreamento de um aplicativo, você não consegue visualizar a versão de visualização esperada do aplicativo no console do XenMobile Server. Em vez disso, você vê a versão de produção do aplicativo.
- No XenMobile Server, você não consegue instalar aplicativos empacotados em MDX da loja Secure Hub quando a política de dispositivo de perfil de provisionamento está em status pendente.

Notas de Versão para o Lançamento do Rolling Patch 8 do XenMobile Server 10.14

Estas notas de versão descrevem melhorias e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 8.

Novidades

Suporte obsoleto para a política de Proteção de Informações do Windows. De acordo com o anúncio do Windows, o XenMobile Server tornou obsoleto o suporte para a Proteção de Informações do Windows (WIP). O suporte para WIP foi descontinuado adicionando uma propriedade de servidor chamada **windows.wip.deprecation**, cujo valor é definido como **True** por padrão. Para obter mais informações, consulte Propriedades do servidor.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problemas Corrigidos

- No XenMobile® Server, não é possível criar ou editar a política **Atualizar aplicativos gerenciados automaticamente** no local alemão.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 7

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 7.

Novidades

- **Atualizações do SO**
  - **Suporte para iOS 16.** O XenMobile® Server e os aplicativos de produtividade Citrix Mobile são compatíveis com o iOS 16, mas atualmente não oferecem suporte a nenhum novo recurso do iOS 16.
  - **Suporte para Android 13**. O XenMobile Server agora oferece suporte a atualizações de dispositivos Android Enterprise para Android 13. Para um resumo dos benefícios de segurança e privacidade, consulte a documentação do Android.
- **Recursos preteridos.** O suporte para os seguintes recursos foi removido:
  - Função RBAC - registrador de dispositivos compartilhados e COSU
  - Android - Sony e HTC
  - Modo de registro de alta segurança
  - Credenciais derivadas
  - SEAMS
  - Dispositivos Windows Phone ,
  - Entidades PKI genéricas, gerenciadas pela DigiCert e adaptadores Entrust.

  Para obter mais informações, consulte Preterição.
- **Suporte obsoleto para a interface do Provedor de Serviços Móveis (MSP).** O suporte para MSP foi descontinuado com a adição de uma nova propriedade de servidor chamada `deprecate.mobile.service.provider` que remove a interface MSP do console, que é definida como **True** por padrão. Para obter mais informações, consulte Propriedades do servidor.
- **O suporte para a política de restrição *Permitir conexão automática a hotspots do WiFi Sense* para dispositivos Windows 10 foi removido.** Para obter mais informações, consulte Configurações de desktop/tablet do Windows.
- **Suporte obsoleto para o gateway SMS Nexmo.** O suporte para SMS Nexmo foi descontinuado com a adição de uma propriedade de servidor chamada `deprecate.carrier.sms.gateway`, que é definida como **True** por padrão. O SMS Nexmo também foi descontinuado no Portal de Autoatendimento. Para obter detalhes, consulte Notificações.

- **Descontinuação de APIs pelo Google.** O Google está descontinuando várias APIs usadas para categorias de aplicativos e licenças no XenMobile Server. As seguintes alterações estão em vigor:
  - Agora você seleciona aplicativos para adicionar em vez de aprovar. Consulte Aplicativos da loja de aplicativos gerenciados.
  - Agora você organiza os aplicativos em coleções em vez de categorias. Consulte Organizar aplicativos.
  - Você não pode mais desassociar licenças de aplicativos de usuários. Consulte Adicionar aplicativos.
- **Configure uma prioridade para atualizar automaticamente aplicativos gerenciados do Android Enterprise.** Especifique se os aplicativos gerenciados do Android Enterprise são atualizados automaticamente com baixa ou alta prioridade. Você também pode adiar as atualizações automáticas. Para obter mais informações, consulte Política de dispositivo de atualização automática de aplicativos gerenciados.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para patches cumulativos.

Problemas Corrigidos

- Em alguns dispositivos Android, você não consegue acessar o Secure Hub quando alguns aplicativos públicos não estão disponíveis no Google Play.
- Em certos dispositivos macOS, perfis e certificados instalados são removidos automaticamente após a renovação dos certificados SSL.
- No console do XenMobile Server, você não consegue editar as políticas de dispositivo de Restrições cujo nome contém o símbolo ***/***.
- Dispositivos DEP liberados ainda aparecem no console do XenMobile Server.
- Você não consegue acessar a Secure Hub Store. Você recebe o seguinte erro: **Seu logon expirou. Faça logon novamente para continuar.**

Notas de Versão para XenMobile Server 10.14 Rolling Patch 6 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 6.

Novidades

Adicionada nova Política de Restrições. Adicionadas **Permitir copiar e colar do perfil de trabalho** e **Permitir compartilhamento de dados do perfil pessoal** à política de Restrições. Defina essas políticas como **DESATIVADO** para restringir a cópia, colagem e importação de um perfil pessoal para um perfil de trabalho. Para mais detalhes, consulte Política de dispositivo de Restrições.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problemas Corrigidos

- No XenMobile® Server, a versão correta de alguns aplicativos VPP não é atualizada automaticamente.
- Na versão 10.14 do XenMobile Server, não é possível excluir determinados usuários do Active Directory.
- No novo registro de dispositivos executando iOS 15, a implantação da Política de VPN falha quando o tipo de conexão é definido como **AlwaysOn IKEv2 Dual Configuration**.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 5 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 5.

Novidades

- **Habilitar o Google Analytics**. Para habilitar o Google Analytics no XenMobile Server, defina o valor da propriedade do servidor **xms.ga.enabled** como **True**. O valor padrão é **True**.
- **Renovação do certificado APNs do Secure Hub.** O certificado do Serviço de Notificação Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.14 expira em May 7, 2022. Esta atualização renova o certificado APNs do Secure Hub, que expirará em April 8, 2023.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problemas Corrigidos

- No XenMobile® Server, a CA Emissora de Certificados de Dispositivo não é atualizada após a renovação da CA nos dispositivos.

- Em alguns dispositivos, há duas entradas de certificado no banco de dados SQL, o que leva a um erro.
- Na versão 10.14 do XenMobile Server, não é possível editar a política de dispositivo do perfil de Provisionamento.
- No XenMobile Server, a GUI não é atualizada no grupo de entrega ao mudar de ShareFile Enterprise para Conectores.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 4 Lançamento

Estas notas de versão descrevem melhorias e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 4.

Novidades

Habilitar serviço WSDL. Para habilitar o serviço WSDL no XenMobile Server, defina o valor da propriedade do servidor `wsdl.service.enabled` como **True**. É necessário ao usar o conector de gateway ActiveSync. O valor padrão é **False**.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para patches cumulativos.

Problemas Corrigidos

- Em alguns dispositivos Android Enterprise, grupos de entrega e políticas ou aplicativos atribuídos não são aplicados intermitentemente.
- Na versão 10.13 do XenMobile Server, não é possível conectar e configurar o controlador de zonas de armazenamento apenas com conectores de zona de armazenamento.
- Em dispositivos iOS registrados no modo somente MDM, não é possível adicionar aplicativos por meio de navegadores abertos pelo Secure Hub da App Store. Você recebe o seguinte erro: **Seu logon expirou. Faça logon novamente para continuar.**
- Nas versões 10.13 RP1 e posteriores do XenMobile Server, a armadilha de conectividade inter-nó do XenMobile do monitoramento SNMP não funciona.
- No XenMobile® Server, a hora errada é exibida no fuso horário W-SU.

Notas de Versão para o XenMobile Server 10.14 Rolling Patch 3 Lançamento

Estas notas de versão descrevem melhorias e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 3.

Esta versão inclui correções de bugs.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 2 Release

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 2.

Para obter informações sobre patches cumulativos anteriores para o XenMobile Server 10.14.0, consulte Notas de versão para Patches Cumulativos.

Problema Corrigido

No XenMobile® Server, você observa alta utilização da CPU nos nós do servidor em horários de pico.

Notas de Versão para XenMobile Server 10.14 Rolling Patch 1

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos para o XenMobile Server 10.14 Rolling Patch 1.

Novidades

- **Suporte para dispositivos Windows 11.** Agora você pode usar o XenMobile para gerenciar dispositivos Windows 11. Para obter mais informações, consulte a lista de suporte do sistema operacional.
- **Configurar o modo de conexão e a prioridade da rede para macOS.** Na política de dispositivo Wi-Fi, ative a configuração **Modo de conexão** para dispositivos macOS para escolher como os usuários se conectam à rede. O dispositivo pode usar as credenciais do sistema ou as credenciais inseridas na janela de login para autenticar o usuário. Se você tiver várias redes, digite um número no campo **Prioridade** para definir a prioridade da conexão de rede. O dispositivo escolhe a rede com o número mais baixo. Para obter mais informações, consulte as configurações do macOS em política de dispositivo Wi-Fi.
- O XenMobile Server não poderá sincronizar licenças de grupo com o Google, devido à descontinuação do suporte para licenças de grupo em dispositivos Android Enterprise pelo Google. Para obter mais informações, consulte este artigo.

Problemas Conhecidos

Dispositivos registrados atualizados do macOS 11 ou anterior para o macOS 12, ou dispositivos recém-registrados no macOS 12, podem ser exibidos como "Não Verificado" em **Preferências do**

Sistema > Perfis no dispositivo. Para obter mais informações e uma solução alternativa, consulte este artigo de Suporte.

Problemas Corrigidos

- Após registrar um dispositivo iOS 15 ou macOS 12, o perfil de configuração MDM é exibido como **Não Verificado**.
- No console do XenMobile® Server, ao modificar as configurações de um aplicativo para limpar todas as plataformas e salvar, o aplicativo não é listado em **Configurar > Aplicativos**.
- Você não consegue sair do iniciador Citrix® na plataforma Android Enterprise. Você recebe o seguinte erro: **Senha incorreta**.
- Na versão 10.14 do XenMobile Server, você não consegue editar a política **Importar perfil iOS e macOS**.

Novidades no XenMobile Server 10.16

Suporte contínuo para as políticas Clássicas descontinuadas do Citrix ADC

A Citrix anunciou recentemente a descontinuação de alguns recursos baseados em políticas Clássicas a partir do Citrix ADC 12.0 build 56.20. Os avisos de descontinuação do Citrix ADC não têm impacto nas integrações existentes do XenMobile Server com o Citrix Gateway. O XenMobile Server continua a oferecer suporte às políticas Clássicas e nenhuma ação é necessária.

Anúncios de descontinuação

Para aviso prévio dos recursos do Citrix XenMobile que estão sendo descontinuados, consulte Descontinuação.

Antes de atualizar endpoints para iOS 14.5

Antes de atualizar qualquer endpoint para iOS 14.5, a Citrix recomenda que você execute as seguintes ações para mitigar falhas de aplicativo:

- Atualize o Citrix Secure Mail e o Secure Web para 21.2.X ou superior. Consulte Atualizar aplicativos MDX ou corporativos.
- Se você usa o MDX Toolkit, encapsule todos os aplicativos iOS de terceiros com o MDX Toolkit 21.3.X ou superior. Verifique a página de download do MDX Toolkit para a versão mais recente.

Antes de atualizar um Citrix ADC local

A atualização de um Citrix ADC local para determinadas versões pode resultar em um erro de logon único. O logon único no Citrix Files ou na URL de domínio do ShareFile em um navegador com a opção **Logon de Funcionário da Empresa** resulta em um erro. O usuário não consegue fazer logon.

Para contornar esse problema: Se você ainda não executou o seguinte comando da CLI do ADC no Citrix Gateway, execute-o para habilitar o SSO global:

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

Para obter mais informações, consulte:

- Versão do Citrix ADC (Fase de Recurso) 13.1 Build 33.52
- Configurações de SSO afetadas

Após concluir a solução alternativa, os usuários podem autenticar no Citrix Files ou na URL do domínio ShareFile usando SSO em um navegador com a opção de login de funcionário da empresa.

Antes de fazer upgrade para o XenMobile 10.16 (no local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos de sistema e compatibilidade e Compatibilidade do XenMobile.

1. Se a máquina virtual que executa o XenMobile® Server a ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.
2. Atualize seu Citrix License Server para 11.17.2.0 Build 47000 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.16.

   A versão mais recente do XenMobile requer o Citrix License Server 11.17 (versão mínima).

   > **Nota:**
   >
   > A data dos Serviços de Sucesso do Cliente (anteriormente, data do Subscription Advantage) no XenMobile 10.16 é November 15, 2022. A data dos Serviços de Sucesso do Cliente em sua licença Citrix deve ser posterior a esta data.
   >
   > Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.

> Para renovar a data em sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Consulte Serviços de Sucesso do Cliente.

Serviço de Ativação de Licença (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. Se o Serviço de Ativação de Licença estiver habilitado no 10.15 Rolling Patch 13 ou Rolling Patches posteriores, a atualização direta para 10.16.0.48 redefine a configuração do Serviço de Ativação de Licença. Continue a aplicar os rolling patches 10.16 da versão 10.16 Rolling Patch 7 ou posterior, onde o Serviço de Ativação de Licença pode ser reconfigurado. Os dispositivos existentes permanecem inalterados.

3. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm os seguintes requisitos:

   - Se o Citrix Gateway estiver configurado para persistência SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.

4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante uma atualização, backups completos permitem que você se recupere.

Para fazer upgrade

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de atualizar para 10.14 ou posterior, antes de instalar ou atualizar o ESXi 7.0.

Você pode atualizar diretamente para o XenMobile 10.16 a partir do XenMobile 10.15.x ou 10.14.x. Para fazer a atualização, baixe o binário mais recente disponível: Vá para a página de downloads da Citrix. navegar para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para seu hipervisor, clique em **Download File**.

Para carregar a atualização, use a página **Release Management** no console do XenMobile. Consulte Para atualizar usando a página Release Management.

Após a atualização

Se a funcionalidade envolvendo conexões de saída parar de funcionar e você não tiver alterado a configuração de suas conexões, verifique o log do XenMobile Server em busca de erros como o

seguinte: "Não é possível conectar ao Servidor VPP: O nome do host '192.0.2.0' não corresponde ao assunto do certificado fornecido pelo par".

- O erro de validação do certificado significa que você deve desabilitar a verificação do nome do host no XenMobile Server.
- Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor Microsoft PKI.
- Se a verificação do nome do host quebrar sua implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão desta propriedade é `false`.

Atualizações da plataforma

- **Suporte para Android 14:** O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora oferecem suporte a atualizações de dispositivos Android Enterprise para Android 14. Para obter mais informações sobre os benefícios de segurança e privacidade, consulte a documentação do Android.
- **Suporte para iOS 17:** O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o iOS 17, mas atualmente não oferecem suporte a nenhum novo recurso do iOS 17.
- **Suporte para macOS 14:** O XenMobile Server e os aplicativos de produtividade Citrix Mobile agora são compatíveis com o macOS 14, mas atualmente não oferecem suporte a nenhum novo recurso do macOS 14.

Acesso aos relatórios de Dispositivos e Aplicativos

Anteriormente, a página de relatórios **Dispositivos e Aplicativos** exibia as informações sobre todos os dispositivos e aplicativos para todos os usuários, independentemente de seu grupo de usuários, mesmo que o controle de acesso baseado em função (RBAC) fosse aplicado.

A partir da versão 10.16 do XenMobile Server, a página de relatórios **Dispositivos e Aplicativos** exibe os dispositivos e aplicativos específicos para os grupos de usuários definidos em **To specific user groups** que a função RBAC tem permissão para gerenciar. Para obter mais informações sobre como configurar funções com RBAC, consulte Configurar funções com RBAC.

Adicionado um novo campo obrigatório “Domínio” nas configurações 802.1x para Android Enterprise

Um novo campo **Domínio** é adicionado na página de configurações da política de rede da plataforma Android Enterprise para o tipo de autenticação **802.1x EAP**. Para obter mais informações, consulte Configurações 802.1x para Android Enterprise.

Novas configurações adicionadas na política de dispositivo de Restrições e na política de dispositivo do Exchange para iOS

- Adicionada uma nova configuração **Permitir Mail Drop**" na política de dispositivo do Exchange para iOS. Para obter mais informações, consulte Política de dispositivo do Exchange - configurações do iOS.
- Adicionadas as seguintes novas configurações na política de dispositivo de Restrições para iOS:
  - Permitir inicialização para recuperação por um dispositivo não emparelhado
  - Instalar resposta de segurança rápida
  - Remover resposta de segurança rápida
  - Permitir proteção de privacidade de e-mail
  - NFC
  - Permitir App clips
  - Permitir publicidade personalizada da Apple
  - Desbloqueio automático

Para obter mais informações, consulte Política de dispositivo de Restrições - configurações do iOS.

Adicionados novos campos URL de login OAuth e URL de solicitação de token OAuth nas configurações da política de dispositivo do Exchange para iOS

A partir da versão 10.16 do XenMobile Server, os campos **URL de login OAuth** e **URL de solicitação de token OAuth** são adicionados em **Política do Exchange** > **iOS** > botão de opção **Usar OAuth**. Para obter mais informações, consulte Política de dispositivo do Exchange.

Adicionada nova política de dispositivo Chave da Plataforma Knox para Empresas

Uma nova política de dispositivo chamada **Chave da Plataforma Knox para Empresas** foi adicionada. Esta política permite que você forneça as informações de licença necessárias da Plataforma Knox para Empresas (KPE) da Samsung e use as licenças KPE para aprimorar a segurança do seu dispositivo Samsung. Para obter mais informações, consulte Política de dispositivo Chave da Plataforma Knox para Empresas.

Clonar um grupo de entrega para usar como base para um novo grupo de entrega

Este recurso permite copiar um grupo de entrega complexo que inclui várias políticas, aplicativos e ações. Você pode então editar a cópia, como adicionar perfis de registro ou um novo conjunto de usuários do Active Directory. Para obter detalhes, consulte Clonar um grupo de entrega.

Suporte para Apple Business Manager para iPads compartilhados

A partir da versão 10.16 do XenMobile Server, os iPads compartilhados suportam o Apple Business Manager (ABM) com o XenMobile Server. Isso permite que você faça login nos iPads compartilhados usando as contas ABM e os utilize. Para obter mais informações, consulte Configurando iPads compartilhados.

Adicionada nova ação de segurança chamada Excluir Todos os Usuários para iPads compartilhados

A partir da versão 10.16 do XenMobile Server, uma nova ação de segurança chamada **Excluir todos os usuários** é adicionada para iPads compartilhados no XenMobile Server. Isso permite que você exclua todos os usuários do dispositivo. Para obter mais informações, consulte Ações de segurança para iPads compartilhados.

A política de dispositivo de atributos de aplicativo suporta novos atributos de aplicativo iOS

Agora você pode especificar os seguintes atributos para aplicativos instalados em dispositivos iOS:

- **Aplicativo removível:** Especifique se o aplicativo pode ser removido pelos usuários quando é um aplicativo gerenciado.
- **Habilitar download direto de domínio associado:** Especifique se o aplicativo pode realizar a verificação de associação de site reivindicada diretamente nos domínios.
- **Domínios Associados:** Especifique os domínios associados a serem adicionados a um aplicativo.

Para obter mais informações, consulte Política de dispositivo de atributos de aplicativo.

Suporte para sincronizar ou substituir Serviços de Exchange Sincronizados para iOS

A partir da versão 10.16 do XenMobile Server, você pode escolher se deseja sincronizar ou substituir os seguintes Serviços de Exchange sincronizados para iOS, ativando as configurações relevantes.

- Calendários
- Contatos
- E-mail
- Notas
- Lembretes

Para obter mais informações, consulte política de dispositivo do Exchange.

Suporte para redefinir a política de dispositivo de Controle de Atualizações do SO para o padrão do sistema

A partir da versão 10.16 do XenMobile Server, um novo valor **Padrão** é adicionado na lista suspensa **Política de atualização do sistema** em **Controle de Atualizações do SO** para Android Enterprise. Esse recurso permite redefinir a política de atualização do sistema para o padrão do sistema. Para obter mais informações, consulte política de dispositivo de Controle de Atualizações do SO.

Adicionada nova opção "Versão das atualizações do SO" na política de Atualização do SO para iOS

Na **política de Atualização do SO** para a plataforma **iOS**, uma nova opção **Versão das atualizações do SO** é adicionada após o campo **Frequência de atualização do SO**. Essa opção permite especificar a versão do SO a ser usada para atualizar os dispositivos iOS supervisionados. Para obter mais informações, consulte configurações do iOS.

Controle de Acesso à Rede

Use a solução de Controle de Acesso à Rede (NAC) para estender a avaliação de segurança de dispositivos XenMobile para dispositivos Android e Apple. A solução NAC usa a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação. Depois de configurar o dispositivo NAC, as políticas de dispositivo e os filtros NAC que você configura no XenMobile são aplicados. Para obter mais informações, consulte Controle de Acesso à Rede.

Suporte para tipos de licença mistos com o XenMobile Server

Este recurso permite ativar uma mistura de tipos e edições de licença do XenMobile usando o XenMobile Server ou o Citrix Licensing Server. Para obter mais informações, consulte Para ativar uma licença diferente.

Suporte para eSIM em dispositivos iOS

O XenMobile Server tem uma nova propriedade `ios.esim.support`, que permite ao XenMobile Server obter as informações do eSIM dos dispositivos iOS e exibir as propriedades do dispositivo relacionadas ao eSIM na interface do usuário. O valor padrão dessa propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

Política de dispositivo VPN para a plataforma Android Enterprise

Anteriormente, você podia habilitar o serviço VPN para dispositivos executando o Android Enterprise ativando a opção **Enable Always-On VPN** na **política de dispositivo Opções do XenMobile**.

A partir do XenMobile Server 10.16, você pode habilitar o serviço VPN sempre ativo para dispositivos executando o Android Enterprise ativando a opção **Enable Always-On VPN** na **política de dispositivo VPN**. Se você já habilitou a opção **Enable Always-On VPN** na **política de**

dispositivo Opções do XenMobile em uma versão anterior, certifique-se de habilitar a mesma na **política de dispositivo VPN** novamente para os dispositivos recém-registrados. Nenhuma alteração é necessária para os dispositivos já registrados. Para obter mais informações, consulte Política de dispositivo VPN para a plataforma Android Enterprise.

Adicionado novo campo Escopo do perfil em Configurações de política de Webclip para iOS

Para dispositivos iOS, um novo campo chamado **Escopo do perfil** é adicionado em **Configurações de política** na política de dispositivo Webclip. Isso permite que você selecione se a política se aplica a um usuário ou a um sistema. Para obter mais informações, consulte Política de dispositivo Webclip - configurações do iOS.

Renovação do certificado APNs do Secure Hub

Esta atualização renova automaticamente o certificado do Serviço de Notificação por Push da Apple (APNs) do Secure Hub para o XenMobile Server 10.16 para um novo certificado que expirará em February 9, 2025.

Atualizar regra de implantação para o aplicativo da loja pública usando a API REST

Um novo campo chamado **rules** é adicionado às APIs REST **Add New Public Store App** e **Update Public Store App**. Isso permite que você atualize as regras de implantação para o aplicativo da loja pública. Para obter mais informações, consulte Documentação da API REST pública.

Suporte para atualização automática de aplicativos opcionais no iOS

A partir do XenMobile Server 10.16, uma nova propriedade de servidor chamada `apple.ios.optional_app_update` é adicionada. Esta propriedade permite que você atualize automaticamente os aplicativos opcionais no iOS. O valor padrão de `apple.ios.optional_app_update` é definido como **False**. Para obter mais informações, consulte Propriedades do servidor.

Para obter mais informações sobre a atualização automática de aplicativos opcionais comprados em volume, consulte Verificar atualizações de aplicativos.

Suporte para aplicativos corporativos em dispositivos macOS

O XenMobile Server tem uma nova propriedade `mac.app.push` que permite o suporte a aplicativos corporativos em dispositivos que executam macOS. O valor padrão desta propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

Aprimoramento do relatório de dispositivos para Tentativas Totais de Implantação de Aplicativos e 100 Principais Aplicativos Instalados

No Console do XenMobile Server, em Analisar -> Relatórios, duas novas colunas, **Versão do sistema operacional** e **Modelo do dispositivo**, são adicionadas em Tentativas Totais de Implantação de Aplicativos, e o novo relatório de dispositivos **100 Principais Aplicativos Instalados** é adicionado para mostrar os 100 principais aplicativos instalados para cada plataforma. Para obter mais informações, consulte Relatórios.

O XenMobile Server tem uma nova propriedade `device.report.enhancement.enabled`, que permite o aprimoramento do novo relatório de dispositivos acima. O valor padrão desta propriedade é **True**. Para obter mais informações, consulte Propriedades do servidor.

Modernizando a classificação e filtragem no registro de dispositivos

As exibições de lista no XenMobile Server são atualmente difíceis de navegar e menos amigáveis ao usuário. Ao mover as opções de filtragem e classificação para os cabeçalhos das colunas, os usuários podem combinar essas funções, tornando muito mais simples e intuitivo encontrar os dados necessários.

Descontinuações e remoções

Descontinuação da Ferramenta XenMobile Analyzer: De acordo com nosso ritmo de lançamento frequente e estável, a Ferramenta XenMobile Analyzer não é mais necessária. A Citrix descontinuou este serviço a partir de March 31, 2023. A Citrix recomenda que você use as verificações de conectividade disponíveis no console do Citrix XenMobile ou no Citrix Gateway. Para obter mais informações, consulte Verificações de conectividade.

O que há de novo no XenMobile Server 10.15

XenMobile Server 10.15 (Download em PDF)

Suporte contínuo para as políticas Clássicas descontinuadas do Citrix ADC

A Citrix anunciou recentemente a descontinuação de alguns recursos baseados em políticas Clássicas a partir do Citrix ADC 12.0 build 56.20. Os avisos de descontinuação do Citrix ADC não têm impacto nas integrações existentes do XenMobile Server com o Citrix Gateway. O XenMobile Server continua a oferecer suporte às políticas Clássicas e nenhuma ação é necessária.

Anúncios de descontinuação

Para aviso antecipado dos recursos do Citrix XenMobile que estão sendo desativados, consulte Descontinuação.

Antes de atualizar endpoints para iOS 14.5

Antes de atualizar qualquer endpoint para iOS 14.5, a Citrix recomenda que você execute as seguintes ações para mitigar falhas de aplicativos:

- Atualize o Citrix Secure Mail e o Secure Web para 21.2.X ou superior. Consulte Atualizar aplicativos MDX ou corporativos.
- Se você usa o MDX Toolkit, encapsule todos os aplicativos iOS de terceiros com o MDX Toolkit 21.3.X ou superior. Verifique a página de download do MDX Toolkit para a versão mais recente.

Antes de atualizar um Citrix ADC local

A atualização de um Citrix ADC local para certas versões pode resultar em um erro de logon único. O logon único no Citrix Files ou na URL de domínio do ShareFile em um navegador com a opção **Entrar como funcionário da empresa** resulta em um erro. O usuário não consegue fazer login.

Para contornar esse problema: Se você ainda não executou o seguinte comando da CLI do ADC no Citrix Gateway, execute-o para habilitar o SSO global:

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

Para obter mais informações, consulte:

- Citrix ADC Release (Feature Phase) 13.1 Build 33.52
- Configurações de SSO impactadas

Depois de concluir a solução alternativa, os usuários podem autenticar no Citrix Files ou no URL do domínio ShareFile usando SSO em um navegador com a opção de login do funcionário da empresa.

Antes de fazer upgrade para o XenMobile 10.15 (no local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos de sistema e compatibilidade e Compatibilidade do XenMobile.

1. Se a máquina virtual que executa o XenMobile® Server a ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.
2. Atualize seu Citrix License Server para a versão 11.17 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.15.

   A versão mais recente do XenMobile requer o Citrix License Server 11.17 (versão mínima).

   > **Nota:**
   >
   > A data dos Serviços de Sucesso do Cliente (anteriormente, data do Subscription Advantage) no XenMobile 10.15 é November 15, 2022. A data dos Serviços de Sucesso do Cliente em sua licença Citrix deve ser posterior a esta data.
   >
   > Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.
   >
   > Para renovar a data em sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Consulte Serviços de Sucesso do Cliente.
3. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm o seguinte requisito. Se o Citrix Gateway estiver configurado para persistência SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante um upgrade, backups completos permitirão que você se recupere.

Para fazer upgrade

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de fazer upgrade para 10.14 ou posterior, antes de instalar ou fazer upgrade do ESXi 7.0.

Você pode fazer o upgrade diretamente para o XenMobile 10.15 a partir do XenMobile 10.14.x ou 10.13.x. Para realizar o upgrade, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para seu hypervisor, clique em **Download File**.

Para carregar o upgrade, use a página **Release Management** no console do XenMobile. Consulte Para fazer upgrade usando a página Release Management.

Após o upgrade

Se a funcionalidade que envolve conexões de saída parar de funcionar e você não tiver alterado a configuração das suas conexões, verifique o log do XenMobile Server em busca de erros como o seguinte: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

- O erro de validação do certificado significa que você deve desabilitar a verificação do nome do host no XenMobile Server.
- Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor Microsoft PKI.
- Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão dessa propriedade é `false`.

Atualizações da plataforma

Suporte para iOS 16. O XenMobile Server e os aplicativos de produtividade Citrix Mobile são compatíveis com o iOS 16, mas atualmente não oferecem suporte a nenhum novo recurso do iOS 16.

Suporte para Android 13. O XenMobile Server oferece suporte a atualizações de dispositivos Android Enterprise para Android 13. Para um resumo dos benefícios de segurança e privacidade, consulte a documentação do Android.

Suporte para dispositivos Windows 11. Agora você pode usar o XenMobile para gerenciar dispositivos Windows 11. Para obter mais informações, consulte Lista de suporte do sistema operacional.

Configurar o modo de conexão e a prioridade da rede para macOS

Na política de dispositivo Wi-Fi, habilite a configuração **Modo de conexão** para dispositivos macOS para escolher como os usuários se conectam à rede. O dispositivo pode usar as credenciais do sistema ou as credenciais inseridas na janela de login para autenticar o usuário. Se você tiver várias redes, digite um número no campo *Prioridade* para definir a prioridade da conexão de rede. O dispositivo escolhe a rede com o número mais baixo. Para obter mais informações, consulte as configurações do macOS em Política de dispositivo Wi-Fi.

Configurar uma prioridade para atualizar automaticamente aplicativos gerenciados do Android Enterprise

Especifique se os aplicativos gerenciados do Android Enterprise são atualizados automaticamente com baixa ou alta prioridade. Você também pode adiar as atualizações automáticas. Para obter mais informações, consulte Política de dispositivo de atualização automática de aplicativos gerenciados.

Usar imagens de modo virtualizado por hardware (HVM) em versões 8.2 CU1 e posteriores do Citrix Hypervisor

As versões 8.2 CU1 e posteriores do Citrix Hypervisor não oferecem mais suporte a VMs paravirtualizadas (PV). Para obter mais informações, consulte Atualização Cumulativa 1 para obter detalhes.

A partir das versões 10.15 do XenMobile Server, o modo virtualizado por hardware (HVM) é suportado. Para novas instalações do XenMobile Server, baixe a imagem HVM xva em citrix.com. Para ambientes XenMobile Server existentes, siga as etapas para migrar de PV para convidado HVM. A imagem de convidado HVM está disponível em citrix.com na versão 10.15 e posteriores do XenMobile Server.

Pré-requisitos

- Certifique-se de que os clusters estejam habilitados e que o banco de dados seja remoto.
- Como backup, mantenha o nó PV antigo ou salve um instantâneo. Se o nó PV estiver nas versões 10.14 ou 10.13 do XenMobile Server, faça backup do banco de dados também.

- Antes da migração, baixe o pacote de suporte do nó PV antigo que não será transferido para o novo nó HVM.

Etapas para migrar

1. Baixe a imagem HVM xva do XenMobile Server 10.15.
2. Desligue o nó convidado PV antigo.
3. Inicialize o novo nó HVM no Citrix Hypervisor.
4. Configure o nó do XenMobile Server 10.15 com as mesmas configurações de banco de dados do nó antigo, juntamente com a senha do armazenamento de chaves PKI do servidor do cluster existente.
5. Atualize as configurações do Citrix Gateway, se necessário.

> **Nota:**
>
> Se houver uma falha durante a migração, inicialize o nó PV antigo com a mesma versão do banco de dados.

> **Importante:**
>
> Não execute o comando `/opt/xensource/bin/pv2hvm` para seus convidados XenMobile PV. Isso causa falha na inicialização da VM.

Habilitar Google Analytics

Para habilitar o Google Analytics no XenMobile Server, defina o valor da propriedade do servidor *xms.ga.enabled* como **True**. O padrão é **True**.

Adicionada nova política de Restrições

Adicionadas *Permitir copiar e colar do perfil de trabalho* e *Permitir compartilhamento de dados do perfil pessoal* à política de Restrições. Defina essas políticas como **OFF** para restringir a cópia, colagem e importação de um perfil pessoal para um perfil de trabalho. Para mais detalhes, consulte Política de dispositivo de restrições.

Renovação do certificado APNs do Secure Hub

O certificado do Serviço de Notificação Push da Apple (APNs) do Secure Hub para XenMobile Server expirou em May 7, 2022. Esta atualização renova o certificado APNs do Secure Hub, que expirará em April 8, 2023.

Descontinuações e remoções

- **Descontinuação de APIs pelo Google.** O Google está descontinuando várias APIs usadas para categorias de aplicativos e licenças no XenMobile Server. As seguintes alterações estão em vigor:
  - Agora você seleciona aplicativos para adicionar em vez de aprovar. Consulte Aplicativos da loja de aplicativos gerenciados.
  - Agora você organiza aplicativos em coleções em vez de categorias. Consulte Organizar aplicativos.
  - Você não pode mais desassociar licenças de aplicativos de usuários. Consulte Adicionar aplicativos.
- **Suporte descontinuado para a política de Proteção de Informações do Windows.** De acordo com o anúncio do Windows, o XenMobile Server descontinuou o suporte para a Proteção de Informações do Windows (WIP). O suporte para WIP foi descontinuado adicionando uma propriedade de servidor chamada *windows.wip.deprecation*, cujo valor é definido como *True* por padrão. Para mais informações, consulte Propriedades do servidor.
- **Suporte descontinuado para a interface do Provedor de Serviços Móveis (MSP).** O suporte para MSP foi descontinuado adicionando uma nova propriedade de servidor chamada *deprecate.mobile.service.provider* que remove a interface MSP do console, que é definida como *True* por padrão. Para mais informações, consulte Propriedades do servidor.
- **Suporte obsoleto para gateway SMS Nexmo.** O suporte para SMS Nexmo foi descontinuado com a adição de uma nova propriedade de servidor chamada *deprecate.carrier.sms.gateway*, que é definida como *True* por padrão. O SMS Nexmo também foi descontinuado no Portal de Autoatendimento. Consulte Notificações para obter detalhes.
- **Suporte obsoleto para a política de restrição *Permitir conexão automática a hotspots do WiFi Sense* para dispositivos Windows 10.** Para obter mais informações, consulte Configurações de Desktop/Tablet Windows.
- **Configuração de convite de registro.** Suporte obsoleto para usar IMEI, número de série e UDID de um dispositivo para criar um convite de registro. Ao criar um convite de registro,

configure as configurações disponíveis em **Gerenciar > Convites de Registro** no console do XenMobile Server.

- **O suporte para os seguintes recursos foi removido:**
  - Android - Amazon
  - Android - Sony e HTC
  - XML personalizado em dispositivos Zebra
  - Credenciais derivadas
  - Entidades PKI genéricas, gerenciadas pela DigiCert e de adaptador Entrust.
  - Modo de registro de alta segurança
  - Função RBAC - registrador de dispositivos compartilhados e COSU
  - Samsung SAFE e Knox
  - SEAMS
  - Dispositivos Windows Phone

  Para obter mais informações, consulte Descontinuação.

O que há de novo no XenMobile Server 10.14

XenMobile Server 10.14 (Download em PDF)

Suporte contínuo para as políticas Clássicas descontinuadas do Citrix ADC

A Citrix anunciou recentemente a descontinuação de alguns recursos baseados em políticas Clássicas a partir do Citrix ADC 12.0 build 56.20. Os avisos de descontinuação do Citrix ADC não têm impacto nas integrações existentes do XenMobile Server com o Citrix Gateway. O XenMobile Server continua a oferecer suporte às políticas Clássicas e nenhuma ação é necessária.

Anúncios de descontinuação

Para aviso prévio dos recursos do Citrix XenMobile que estão sendo descontinuados, consulte Descontinuação.

Antes de atualizar os endpoints para iOS 14.5

Antes de atualizar qualquer endpoint para iOS 14.5, a Citrix recomenda que você execute as seguintes ações para mitigar falhas de aplicativos:

- Atualize o Citrix Secure Mail e o Secure Web para 21.2.X ou superior. Consulte Atualizar aplicativos MDX ou empresariais.
- Se você usa o MDX Toolkit, encapsule todos os aplicativos iOS de terceiros com o MDX Toolkit 21.3.X ou superior. Verifique a página de download do MDX Toolkit para a versão mais recente.

Antes de atualizar um Citrix ADC local

A atualização de um Citrix ADC local para determinadas versões pode resultar em um erro de logon único. O logon único no Citrix Files ou na URL do domínio ShareFile em um navegador com a opção **Entrar como funcionário da empresa** resulta em um erro. O usuário não consegue fazer login.

Para contornar esse problema: Se você ainda não executou o seguinte comando da CLI do ADC no Citrix Gateway, execute-o para habilitar o SSO global:

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

Para obter mais informações, consulte:

- Citrix ADC Release (Feature Phase) 13.0 Build 67.39/67.43
- Configurações de SSO impactadas(/pt-br/citrix-adc/current-release/aaa-tm/single-sign-on-types/enable-sso-for-auth-pol.html#impacted-sso-configurations)

Depois de concluir a solução alternativa, os usuários podem autenticar no Citrix Files ou na URL de domínio do ShareFile usando SSO em um navegador com a opção de login de funcionário da empresa.

Antes de fazer upgrade para o XenMobile 10.14 (no local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos de sistema e compatibilidade e Compatibilidade do XenMobile.

1. Se a máquina virtual que executa o XenMobile® Server a ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.
2. Atualize seu Citrix License Server para 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.14.

A versão mais recente do XenMobile requer o Citrix License Server 11.16 (versão mínima).

> **Nota:**
>
> A data dos Serviços de Sucesso do Cliente (anteriormente, data do Subscription Advantage) no XenMobile 10.14 é September 15, 2021. A data dos Serviços de Sucesso do Cliente em sua licença Citrix deve ser posterior a esta data.
>
> Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.
>
> Para renovar a data da sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Consulte Serviços de Sucesso do Cliente.

3. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos com iOS 11 e posterior têm os seguintes requisitos. Se o Citrix Gateway estiver configurado para persistência SSL, você deverá abrir a porta 80 em todos os nós do XenMobile Server.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do banco de dados de configuração do seu sistema. Se você tiver problemas durante um upgrade, os backups completos permitirão que você se recupere.

Para fazer upgrade

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de fazer upgrade para 10.14 antes de instalar ou fazer upgrade do ESXi 7.0.

Você pode atualizar diretamente para o XenMobile 10.14 a partir do XenMobile 10.13.x ou 10.12.x. Para fazer a atualização, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para o seu hipervisor, clique em **Download File**.

Para carregar a atualização, use a página **Release Management** no console do XenMobile. Consulte Para atualizar usando a página Release Management.

Após a atualização

Se a funcionalidade envolvendo conexões de saída parar de funcionar e você não tiver alterado sua configuração de conexão, verifique o **log do XenMobile Server** para erros como o seguinte: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

- O erro de validação do certificado significa que você deve desabilitar a verificação do nome do host no XenMobile Server.
- Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor Microsoft PKI.
- Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão desta propriedade é `false`.

Atualizações de suporte à plataforma

- **iOS 15:** O XenMobile Server e os aplicativos de produtividade Citrix Mobile são compatíveis com o iOS 15, mas atualmente não oferecem suporte a nenhum novo recurso do iOS 15.
- **Android 12:** O XenMobile Server oferece suporte ao Android 12. Para obter informações sobre como a descontinuação das APIs de Administração de Dispositivos do Google afeta os dispositivos que executam o Android 10+, consulte Migrar da administração de dispositivos para o Android Enterprise. Consulte também este blog da Citrix.

Políticas de dispositivo

- Adicionamos duas configurações a todos os modos de registro do Android Enterprise para se alinhar mais de perto com as configurações do Google e simplificar a configuração.
  - **Permitir compartilhamento Bluetooth:** Se não selecionado, os usuários não podem estabelecer compartilhamento Bluetooth de saída em seu dispositivo.
  - **Permitir desinstalação de aplicativo:** Permite que os usuários desinstalem aplicativos da Managed Google Play Store.

  Além disso, movemos a configuração **Permitir atualização over-the-air** da política de Restrições para a política de atualização do SO.

  Para obter mais informações sobre essas alterações, consulte política de dispositivo Restrições e política de dispositivo Atualização do SO.

- As configurações de restrição para Android Enterprise foram reorganizadas para maior clareza. Às vezes, pequenas alterações nos nomes das configurações foram feitas. Para obter mais informações sobre a reorganização, consulte configurações do Android Enterprise.
- Agora você pode atualizar automaticamente aplicativos gerenciados em dispositivos Android Enterprise. Para obter mais informações, consulte política de dispositivo Atualizar aplicativos gerenciados automaticamente.
- Você pode configurar uma lista de tipos de arquivo que podem ser carregados usando a política de dispositivo Arquivos. Os seguintes tipos de arquivo não podem ser carregados mesmo se você os adicionar a esta lista de permissões:
  - o .cab
  - o .appx
  - ponto ipa
  - ponto apk
  - arquivo .xap
  - arquivo .mdx
  - .executável

  Para obter mais informações, consulte Propriedades do servidor

Registro de dispositivo

- Agora você pode criar diferentes perfis de registro para dispositivos iOS e Android. O XenMobile Server oferece suporte a vários perfis de registro com diferentes tipos de registro. Para obter mais informações, consulte Perfis de registro.
- Dispositivos Android 11+ totalmente gerenciados são registrados no modo de perfil de trabalho em dispositivos de propriedade corporativa. O novo modo separa ainda mais os perfis pessoal e de trabalho em um dispositivo. Essa alteração oferece à organização maior controle sobre o perfil gerenciado e oferece aos usuários mais privacidade em seu perfil pessoal. Para obter mais informações, consulte Android Enterprise e Propriedades do servidor.
- Agora você pode especificar mais telas de configuração para pular quando os usuários configurarem dispositivos iOS ou macOS.
  - iOS
    - **Restauração concluída:** Impede que os usuários vejam se uma restauração é concluída durante a configuração. Para iOS 14.0 e posterior.

- **Atualização concluída:** Impede que os usuários vejam se uma atualização de software é concluída durante a configuração. Para iOS 14.0 e posterior.

- macOS
  - **Acessibilidade:** Impede que o usuário ouça o Voice Over automaticamente. Disponível apenas se o dispositivo estiver conectado à Ethernet. Para macOS 11 e posterior.
  - **Biometria:** Impede que o usuário configure o Touch ID e o Face ID. Para macOS 10.12.4 e posterior.
  - **True Tone:** Impede que os usuários configurem sensores de quatro canais para ajustar dinamicamente o balanço de branco da tela. Para macOS 10.13.6 e posterior.
  - **Apple Pay:** Impede que os usuários configurem o Apple Pay. Se esta configuração for desmarcada, os usuários devem configurar o Touch ID e o Apple ID. Certifique-se de que as configurações de **Apple ID** e **Biometria** estejam desmarcadas. Para macOS 10.12.4 e posterior.
  - **Tempo de Uso:** Impede que os usuários ativem o Tempo de Uso. Para macOS 10.15 e posterior.

Para obter mais informações sobre como configurar as opções de configuração, consulte Implantar dispositivos por meio do Programa de Implantação da Apple

Exibir arquivos de log de atualização

Uma nova opção chamada **Exibir arquivo de log de atualização** está disponível na interface de linha de comando **Logs** do **Menu de Solução de Problemas**. Esta opção permite que você veja uma lista do conteúdo do log de atualização e aumenta a eficiência da solução de problemas. Para obter mais informações sobre as ferramentas da interface de linha de comando, consulte Opções da interface de linha de comando.

Arquivo de log de erros

Ao visualizar logs em **Solução de Problemas e Suporte > Logs**, agora você pode visualizar um log que exibe erros filtrados do log de depuração. Para obter mais informações, consulte Visualizar arquivos de log no XenMobile.

Propriedades do servidor

- Você pode decidir se os aplicativos Android legados são entregues a aplicativos Android Enterprise configurando a propriedade do servidor `afw.allow.legacy.apps`. Para obter mais informações, consulte Propriedades do servidor.

- O XenMobile Server agora oferece suporte ao uso da porta 2197 como alternativa à porta 443. Você usa a porta 2197 para enviar e receber notificações APNs de `api.push.apple.com`. A porta usa a API do provedor APNs baseada em HTTP/2. O valor padrão da propriedade do servidor `apns.http2.alternate.port.enabled` é `false`. Para usar a porta 2197, atualize a propriedade do servidor e reinicie o servidor.
- A validação de senha impede usuários com senhas fracas. Quando a propriedade `enable.password.strength.validation` é definida como `true`, você não pode criar usuários locais com senhas fracas.

Aprimoramento da lista de servidores virtuais VPN

Se o nome do servidor VPN não incluir `_XM_XenMobileGetway`, o XenMobile Server selecionará o primeiro servidor virtual VPN disponível na lista.

Suporte para Citrix Launcher

O XenMobile Server oferece suporte ao Citrix Launcher em dispositivos Android Enterprise. Para obter mais informações, consulte Política de dispositivo de configuração do Launcher.

Renovação de cores para o XenMobile Server

O XenMobile Server está em conformidade com as atualizações de cores da marca Citrix.

O que há de novo no XenMobile Server 10.13

XenMobile Server 10.13 (Download em PDF)

Suporte contínuo para as políticas Clássicas descontinuadas do Citrix ADC

A Citrix anunciou recentemente a descontinuação de alguns recursos baseados em políticas Clássicas a partir do Citrix ADC 12.0 build 56.20. Os avisos de descontinuação do Citrix ADC não têm impacto nas integrações existentes do XenMobile Server com o Citrix Gateway. O XenMobile Server continua a oferecer suporte às políticas Clássicas e nenhuma ação é necessária.

Anúncios de descontinuação

Para aviso prévio dos recursos do Citrix XenMobile que estão sendo descontinuados, consulte Descontinuação.

Antes de atualizar os endpoints para iOS 14.5

A Citrix recomenda que, antes de atualizar qualquer endpoint para iOS 14.5, você execute as seguintes ações para mitigar falhas de aplicativos:

- Atualize o Citrix Secure Mail e o Secure Web para 21.2.X ou superior. Consulte Atualizar aplicativos MDX ou corporativos.
- Se você usa o MDX Toolkit, empacote todos os aplicativos iOS de terceiros com o MDX Toolkit 21.3.X ou superior. Verifique a página de download do MDX Toolkit para a versão mais recente.

Antes de atualizar um Citrix ADC local

A atualização de um Citrix ADC local para certas versões pode resultar em um erro de logon único. O logon único no Citrix Files ou na URL do domínio ShareFile em um navegador com a opção **Entrar como funcionário da empresa** resulta em um erro. O usuário não consegue fazer login.

Para contornar esse problema: Se você ainda não executou o seguinte comando da CLI do ADC no Citrix Gateway, execute-o para habilitar o SSO global:

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

Para obter mais informações, consulte:

- Citrix ADC Release (Feature Phase) 13.0 Build 67.39/67.43
- Configurações de SSO impactadas

Depois de concluir a solução alternativa, os usuários podem autenticar no Citrix Files ou na URL de domínio do ShareFile usando SSO em um navegador com a opção de login de Funcionário da Empresa.

Antes de fazer upgrade para o XenMobile 10.13 (no local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos do sistema e compatibilidade e Compatibilidade do XenMobile.

1. Se a máquina virtual que executa o XenMobile® Server a ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.

2. Atualize seu Citrix License Server para a versão 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.13.

   A versão mais recente do XenMobile requer o Citrix License Server 11.16 (versão mínima).

   > **Nota:**
   >
   > A data dos Serviços de Sucesso do Cliente (anteriormente, data do Subscription Advantage) no XenMobile 10.13 é September 29, 2020. A data dos Serviços de Sucesso do Cliente em sua licença Citrix deve ser posterior a esta data.
   >
   > Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.
   >
   > Para renovar a data em sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Consulte Serviços de Sucesso do Cliente.

3. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm os seguintes requisitos. Se o Citrix Gateway estiver configurado para persistência SSL, você deverá abrir a porta 80 em todos os nós do XenMobile Server.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante um upgrade, backups completos permitirão que você se recupere.

Para fazer upgrade

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de fazer upgrade para 10.13 antes de instalar ou fazer upgrade do ESXi 7.0.

Você pode fazer upgrade diretamente para o XenMobile 10.13 a partir do XenMobile 10.12.x ou 10.11.x. Para fazer o upgrade, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (XenMobile) >**

XenMobile Server > Product Software > XenMobile Server 10. No bloco do software XenMobile Server para seu hipervisor, clique em **Download File**.

Para carregar o upgrade, use a página **Release Management** no console do XenMobile. Consulte Para fazer upgrade usando a página Release Management.

Após o upgrade

Se a funcionalidade que envolve conexões de saída parar de funcionar e você não tiver alterado sua configuração de conexão, verifique o **log do XenMobile Server** em busca de erros como o seguinte: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer".

- O erro de validação do certificado significa que você deve desabilitar a verificação do nome do host no XenMobile Server.
- Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor Microsoft PKI.
- Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão dessa propriedade é `false`.

Atualizações de suporte à plataforma

- **iOS 14:** O XenMobile Server e os aplicativos de produtividade Citrix Mobile são compatíveis com o iOS 14, mas atualmente não oferecem suporte a nenhum novo recurso do iOS 14. Use o MDX Toolkit 20.8.5 ou posterior ou prepare os aplicativos usando o MAM SDK.
- **Android 11:** O XenMobile Server oferece suporte ao Android 11. Para obter informações sobre como a descontinuação das APIs de Administração de Dispositivos do Google afeta os dispositivos que executam o Android 10+, consulte Migrar da administração de dispositivos para o Android Enterprise. Consulte também este blog da Citrix.

Configurar vários modos de gerenciamento de dispositivos e aplicativos em um único ambiente

Agora você pode configurar um único site XenMobile para oferecer suporte a várias configurações de registro. A função dos perfis de registro foi expandida para incluir configurações de registro para gerenciamento de dispositivos e aplicativos.

Os perfis de registro suportam vários casos de uso e caminhos de migração de dispositivos em um único console XenMobile. Os casos de uso incluem:

- Gerenciamento de Dispositivos Móveis (somente MDM)
- MDM+Gerenciamento de Aplicativos Móveis (MAM)
- Somente MAM
- Registros de propriedade corporativa
- Registro BYOD (a capacidade de optar por não participar do registro MDM)
- Migração de registros de administrador de dispositivo Android para registros do Android Enterprise (totalmente gerenciado, perfil de trabalho, dispositivo dedicado)

Os perfis de registro substituem a propriedade de servidor agora obsoleta, `xms.server.mode`. Essa alteração não afeta seus grupos de entrega existentes e dispositivos registrados.

Se você não precisar registrar dispositivos dedicados, poderá desativar esse recurso definindo a propriedade do servidor `enable.multimode.xms` como `false`. Consulte Propriedades do servidor.

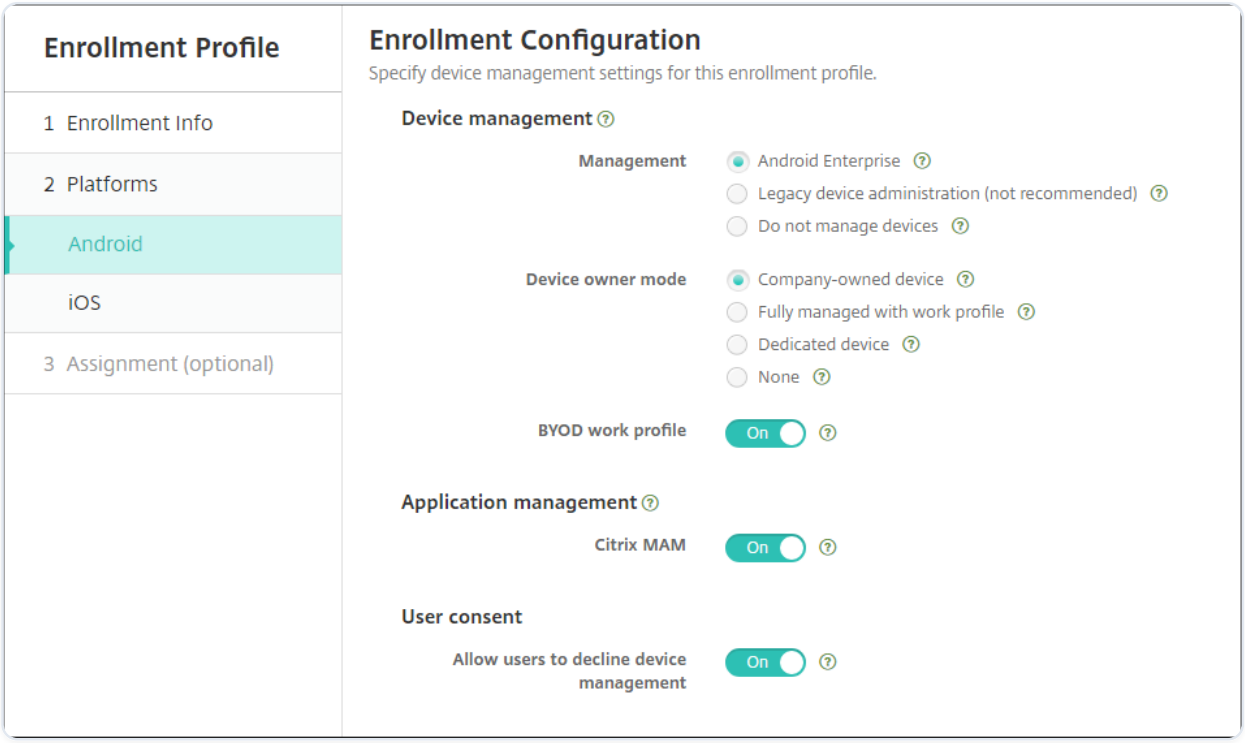
A tabela a seguir mostra o caminho de migração automatizado do modo de propriedade de servidor existente para o novo recurso de perfil de registro:

PROPRIEDADE DE SERVIDOR EXISTENTE	NOVO MODO DE GERENCIAMENTO
Modo ENT (iOS)	Registro de dispositivo Apple com Citrix MAM
Modo ENT (Android)	Administrador de dispositivo legado com Citrix MAM
Modo ENT (Android Enterprise)	Perfil de trabalho em totalmente gerenciado (anteriormente COPE), com Citrix MAM
Modo MAM (iOS e Android)	Citrix MAM
Modo MDM (iOS)	Registro de dispositivo Apple
Modo MDM (Android)	Administrador de dispositivo herdado
Modo MDM (Android Enterprise)	Perfil de trabalho em totalmente gerenciado

Ao criar um grupo de entrega, você pode anexar um perfil de registro ao grupo. Se você não anexar um perfil de registro, o XenMobile anexará o perfil de registro Global.

Os perfis de registro fornecem os seguintes recursos de gerenciamento de dispositivo:

- **Migração mais fácil do modo de administrador de dispositivo Android (DA) para Android Enterprise.** Para dispositivos Android Enterprise, as configurações incluem um modo de proprietário de dispositivo, como: Totalmente gerenciado, perfil de trabalho em totalmente gerenciado ou dedicado. Consulte Android Enterprise.



Para esta atualização, sua configuração atual do XenMobile para o modo de servidor e **Configurações > Android Enterprise** são mapeadas para as novas configurações de perfil de registro da seguinte forma.

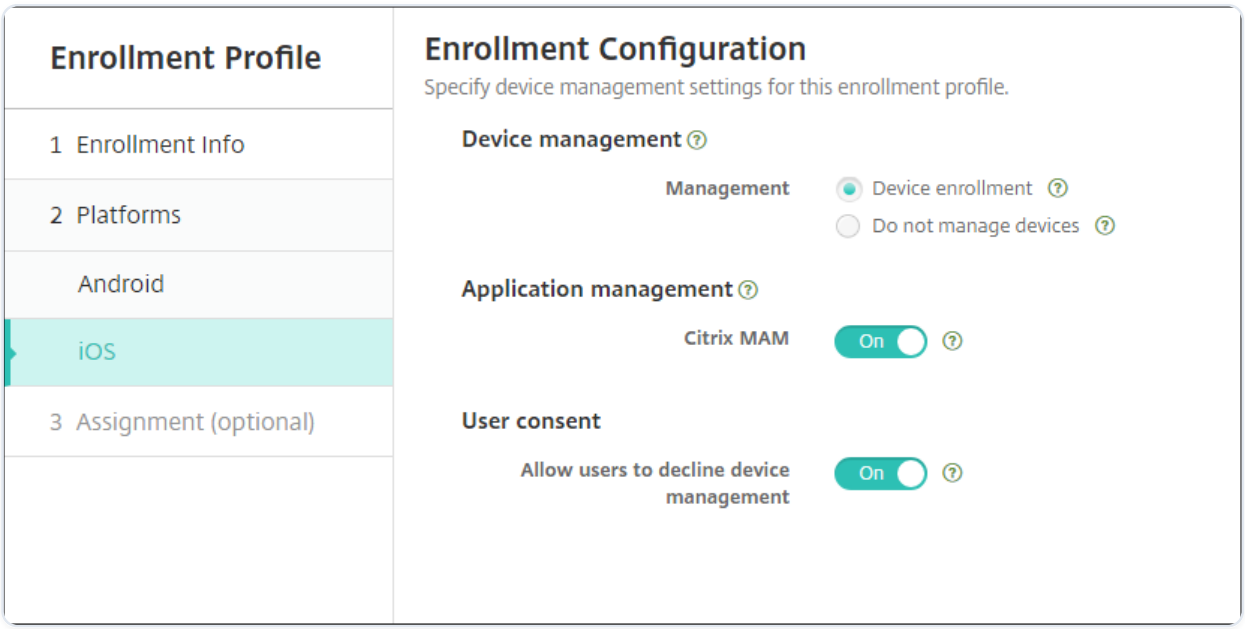
CONFIGURAÇÃO ATUAL	CONFIGURAÇÃO DE GERENCIAMENTO	CONFIGURAÇÃO DO MODO DE PROPRIETÁRIO DO DISPOSITIVO	CONFIGURAÇÃO DO CITRIX MAM
MDM. Google Play Gerenciado (Android Enterprise)	Android Enterprise	Perfil de trabalho em totalmente gerenciado	Desativado
MDM; G Suite (DA herdado)	DA Herdado	não aplicável	Desativado
MAM	Não gerenciar dispositivos	não aplicável	Ativado

CONFIGURAÇÃO ATUAL	CONFIGURAÇÃO DE GERENCIAMENTO	CONFIGURAÇÃO DO MODO DE PROPRIETÁRIO DO DISPOSITIVO	CONFIGURAÇÃO DO CITRIX MAM
MDM+MAM. Google Play Gerenciado (Android Enterprise)	Android Enterprise*	Perfil de trabalho em totalmente gerenciado	Ativado
MDM+MAM; G Suite (DA herdado)	DA Herdado*	não aplicável	Ativado

* Se o registro for obrigatório, **Permitir que os usuários recusem o gerenciamento de dispositivos** estará **Desativado**.

Após a atualização, seus perfis de registro atuais refletem esses mapeamentos. Considere se você deseja criar outros perfis de registro para manipular quaisquer novos casos de uso à medida que você faz a transição do DA herdado.

- **Gerenciamento de iOS mais fácil.** Para dispositivos iOS, as configurações incluem uma escolha entre registrar dispositivos como gerenciados ou não gerenciados.



Para esta atualização, suas configurações anteriores são mapeadas para as novas configurações de perfil de registro da seguinte forma.

MODO DE SERVIDOR	CONFIGURAÇÃO DE GERENCIAMENTO	CONFIGURAÇÃO DO CITRIX MAM
MDM	Registro de dispositivo	Desativado
MAM	Não gerenciar dispositivos	Ativado
MDM+MAM	Registro de dispositivo	Ativado

Se o registro for obrigatório, **Permitir que os usuários recusem o gerenciamento de dispositivos** estará **Desativado**.

As seguintes limitações existem para perfis de registro aprimorados:

- O recurso de perfil de registro aprimorado não está disponível para convites de registro de PIN único ou autenticação de dois fatores.

Consulte Perfis de registro.

Suporte para a API de provedor APNs baseada em HTTP/2 mais recente

O suporte da Apple para o protocolo binário legado do serviço Apple Push Notification termina a partir de March 31, 2021. A Apple recomenda que você use a API de provedor APNs baseada em HTTP/2. O XenMobile Server agora oferece suporte à API baseada em HTTP/2. Para obter mais informações, consulte a atualização de notícias, "Apple Push Notification Service Update" em `<https://developer.apple.com/>`. Para obter ajuda com a verificação de conectividade com APNs, consulte Verificações de conectividade.

As seguintes versões do XenMobile Server habilitam o suporte para a API baseada em HTTP/2 por padrão:

- XenMobile Server 10.13
- XenMobile Server 10.12 Rolling Patch 5 e superior

Se você usa as seguintes versões do XenMobile Server, você deve adicionar a propriedade de servidor **apple.apns.http2** para habilitar o suporte:

- XenMobile Server 10.12 Rolling Patches 2–4 e superior
- XenMobile Server 10.11 Rolling Patch 5 e superior

Não oferecemos mais suporte ao XenMobile Server 10.11 e recomendamos que você atualize para a versão mais recente.

Use uma VPN IPsec baseada em certificado de dispositivo com muitos dispositivos iOS

Em vez de configurar uma política de dispositivo VPN e uma política de dispositivo de Credenciais para cada dispositivo iOS que requer uma VPN IPsec baseada em certificado de dispositivo, automatize o processo.

1. Configure uma política de dispositivo VPN iOS com o tipo de conexão **Always on IKEv2**.
2. Selecione **Certificado de dispositivo baseado na identidade do dispositivo** como o método de autenticação do dispositivo.
3. Selecione o **Tipo de identidade do dispositivo** a ser usado.
4. Importe em massa seus certificados de dispositivo usando a API REST.

Para obter mais informações sobre como configurar a política de dispositivo VPN, consulte Política de dispositivo VPN. Para obter informações sobre como importar certificados em massa, consulte Carregar certificados em massa usando a API REST.

Atualizações automáticas para aplicativos de Compra por Volume da Apple

Ao adicionar uma conta de Compra por Volume (**Configurações > Configurações do iOS**), agora você pode habilitar atualizações automáticas para todos os aplicativos iOS. Consulte a configuração **Atualização Automática de Aplicativos** em Compra por Volume da Apple.

Requisitos de senha para uma conta de usuário local

Ao adicionar ou editar uma conta de usuário local no console do XenMobile, certifique-se de seguir os requisitos de senha mais recentes.

Para obter mais informações, consulte Para adicionar uma conta de usuário local.

- **Requisitos de senha:** Ao adicionar ou editar uma conta de usuário local no console do XenMobile Server, siga os requisitos de senha mais recentes. Consulte Para adicionar uma conta de usuário local.
- **Bloqueio de conta de usuário local:** Se um usuário atingir o número máximo de tentativas de login inválidas consecutivas, a conta de usuário local será bloqueada por 30 minutos. O sistema negará todas as tentativas de autenticação futuras até que o período de bloqueio expire. Para desbloquear a conta no console do XenMobile Server, vá para **Gerenciar > Usuários**, selecione a conta de usuário e clique em **Desbloquear Usuário Local**. Consulte Para desbloquear uma conta de usuário local.

Políticas de dispositivo

Novas políticas de dispositivo e configurações de política de dispositivo foram adicionadas para dispositivos Android Enterprise.

Ocultar o ícone da barra de bandeja em dispositivos Android Enterprise

Agora você pode selecionar se o ícone da barra de bandeja está oculto ou visível para dispositivos Android Enterprise. Consulte Política de dispositivo de opções do XenMobile.

Mais recursos de gerenciamento de certificados para dispositivos Android Enterprise no modo de perfil de trabalho ou modo totalmente gerenciado

Além de instalar autoridades de certificação no keystore gerenciado, agora você pode gerenciar os seguintes recursos:

- **Configurar os certificados usados por aplicativos gerenciados específicos.** A política de dispositivo Credenciais para Android Enterprise agora inclui a configuração **Aplicativos para usar os certificados**. Você pode especificar os aplicativos para usar os certificados de usuário emitidos pelo provedor de credenciais selecionado nesta política. Os aplicativos recebem acesso silencioso aos certificados durante o tempo de execução. Para usar os certificados para todos os aplicativos, deixe a lista de aplicativos em branco. Consulte Política de dispositivo Credenciais.
- **Remover silenciosamente certificados do keystore gerenciado ou desinstalar todos os certificados CA não-sistema.** Consulte Política de dispositivo Credenciais.
- **Impedir que os usuários modifiquem credenciais armazenadas no keystore gerenciado.** A política de dispositivo Restrições para Android Enterprise agora inclui a configuração **Permitir que o usuário configure credenciais de usuário**. Por padrão, essa configuração está **Ativada**. Consulte Política de dispositivo Restrições.

Uso mais fácil do alias do certificado em configurações gerenciadas

Use a nova configuração **Alias do certificado** na política de dispositivo **Credenciais** com a política de dispositivo **Configuração gerenciada**. Isso permite que os aplicativos autenticar na VPN sem a ação do usuário. Em vez de encontrar o alias da credencial nos logs do aplicativo, você cria o alias da credencial. Crie o alias digitando-o no campo **Alias do certificado** da política de dispositivo **Configurações gerenciadas**. Em seguida, digite o mesmo alias do certificado na configuração **Alias do certificado** na política de dispositivo **Credenciais**. Consulte Política de configurações gerenciadas e Política de dispositivo de credenciais.

Controle a configuração "Usar um bloqueio" em dispositivos Android Enterprise

A nova configuração **Habilitar senha unificada** na política de dispositivo **Senha** permite controlar se um dispositivo exige uma senha separada para o dispositivo e para o perfil de trabalho. Antes dessa configuração, os usuários controlavam esse comportamento com a configuração **Usar um bloqueio** no dispositivo. Quando **Habilitar senha unificada** está **Ativado**, os usuários podem usar a mesma senha para o dispositivo e para o perfil de trabalho. Se **Habilitar senha unificada** estiver **Desativado**, os usuários não podem usar a mesma senha para o dispositivo e para o perfil de trabalho. O padrão é **Desativado**. A configuração **Habilitar bloqueio unificado** está disponível para dispositivos Android Enterprise que executam o Android 9.0 ou posterior. Consulte Política de dispositivo de senha.

Mostrar os aplicativos e atalhos em dispositivos Android Enterprise que não estão em conformidade

A política de dispositivo de senha para Android Enterprise tem uma nova configuração **Mostrar aplicativos e atalhos enquanto a senha não estiver em conformidade**. Habilite a configuração para fazer com que os aplicativos e atalhos permaneçam visíveis quando a senha do dispositivo não estiver mais em conformidade. A Citrix recomenda que você crie uma ação automatizada para marcar o dispositivo como fora de conformidade quando a senha não estiver em conformidade. Consulte Política de dispositivo de senha.

Desabilitar a capacidade de imprimir em dispositivos de perfil de trabalho Android Enterprise ou dispositivos totalmente gerenciados

Na política de dispositivo de Restrições, a configuração **Não permitir impressão** permite especificar se os usuários podem imprimir em qualquer impressora acessível a partir do dispositivo Android Enterprise. Consulte Configurações do Android Enterprise.

Permitir aplicativos em dispositivos dedicados adicionando seu nome de pacote na política de Quiosque

Agora você pode inserir o nome do pacote que deseja permitir na plataforma Android Enterprise. Consulte Configurações do Android Enterprise.

Gerenciar recursos do keyguard para perfil de trabalho Android Enterprise e dispositivos totalmente gerenciados

O keyguard do Android gerencia as telas de bloqueio de desafio do dispositivo e do trabalho. Use a política de dispositivo de Gerenciamento de Keyguard para controlar:

- Gerenciamento de Keyguard em dispositivos de perfil de trabalho. Você pode especificar os recursos disponíveis para os usuários antes que eles desbloqueiem o keyguard do dispositivo e o keyguard de desafio de trabalho. Por exemplo, por padrão, os usuários podem usar o desbloqueio por impressão digital e visualizar notificações não editadas na tela de bloqueio. Você também pode usar a política de gerenciamento de keyguard para desabilitar toda a autenticação biométrica para dispositivos que executam o Android 9.0 e posterior.
- Gerenciamento de Keyguard em dispositivos totalmente gerenciados e dedicados. Você pode especificar os recursos disponíveis, como agentes de confiança e câmera segura, antes que eles desbloqueiem a tela do keyguard. Ou, você pode optar por desabilitar todos os recursos do keyguard.

Consulte Política de dispositivo de Gerenciamento de Keyguard.

Publicar aplicativos empresariais para Android Enterprise no console do XenMobile

Você não precisa mais se registrar para uma conta de desenvolvedor do Google Play ao adicionar um aplicativo privado do Android Enterprise. O console do XenMobile abre uma interface de usuário da loja Google Play gerenciada para você carregar e publicar o arquivo APK. Para obter mais informações, consulte Adicionar um aplicativo empresarial.

Publicar aplicativos web para Android Enterprise no console do XenMobile

Você não precisa mais ir ao Google Play gerenciado ou ao portal do Google Developer para publicar aplicativos web do Android Enterprise para XenMobile. Ao clicar em **Carregar** em **Configurar > Aplicativos > Link da Web**, uma interface de usuário da loja Google Play gerenciada é aberta para você carregar e salvar o arquivo. A aprovação e publicação do aplicativo pode levar cerca de 10 minutos. Para obter mais informações, consulte Adicionar um link da Web.

Carregar certificados para dispositivos iOS em massa com a API REST do XenMobile Server

Se carregar certificados um por um não for prático, use a API REST do XenMobile Server para carregar os certificados para dispositivos iOS em massa.

1. Configure uma política de dispositivo VPN iOS com o tipo de conexão **Sempre ativado IKEv2**.
2. Selecione **Certificado de Dispositivo Baseado na Identidade do Dispositivo** como o método de autenticação do dispositivo.
3. Selecione o **Tipo de identidade do dispositivo** a ser usado.

4. Importe em massa seus certificados de dispositivo com a API REST.

Para obter informações sobre como configurar a política de dispositivo VPN, consulte Política de dispositivo VPN. Para obter informações sobre como importar certificados em massa, consulte Carregar certificados para dispositivos iOS em massa com a API REST.

Atualizar chaves de criptografia

A opção **Atualizar chaves de criptografia** foi adicionada nas Configurações Avançadas da CLI do XenMobile. Você pode usar esta opção para atualizar as chaves de criptografia um nó por vez. Consulte Opções do sistema.

Suporte ao ESXi 7.0

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de atualizar para 10.13 antes de instalar ou atualizar o ESXi 7.0.

Novas propriedades do servidor

As seguintes propriedades do servidor estão agora disponíveis:

- **Permitir nomes de host para links da App Store do iOS:** Para adicionar aplicativos públicos da App Store para iOS usando as APIs públicas em vez do console, configure uma lista de nomes de host permitidos, se desejar.
- **Limite de bloqueio de conta de usuário local:** Configure o número de tentativas de login que um usuário local tem antes que sua conta seja bloqueada.
- **Tempo de bloqueio de conta de usuário local:** Configure por quanto tempo um usuário local é bloqueado após muitas tentativas de login falhas.
- **Restrição de tamanho máximo de upload de arquivo ativada:** Ative a restrição do tamanho máximo de arquivo para arquivos carregados.
- **Tamanho máximo de upload de arquivo permitido:** Defina o tamanho máximo de arquivo para arquivos carregados.

Para obter informações mais detalhadas sobre essas propriedades, consulte Propriedades do servidor.

Limpeza de disco de autoatendimento

Uma nova opção de interface de linha de comando chamada **Uso do Disco** está disponível no **Menu de Solução de Problemas**. Esta opção permite que você veja uma lista de arquivos de despejo de memória e arquivos de pacote de suporte. Após visualizar a lista, você pode optar por

excluir todos esses arquivos através da linha de comando. Para obter mais informações sobre as ferramentas da interface de linha de comando, consulte Opções da interface de linha de comando.

Novidades no XenMobile Server 10.12

XenMobile Server 10.12 (Download em PDF)

Anúncios de descontinuação

Para aviso prévio dos recursos do Citrix XenMobile que estão sendo desativados, consulte Descontinuação.

Prepare seus dispositivos Android para as próximas mudanças

Estas descontinuações anunciadas anteriormente afetam seus dispositivos Android e Android Enterprise:

- Registros de administração de dispositivos (DA) para Android 10:
  - **July 31, 2020:** A Citrix® descontinua novos registros para o modo de administração de dispositivos Android herdado.
  - **November 1, 2020:** O Google descontinua a API de administração de dispositivos herdada. Dispositivos Android 10 executando no modo de administração de dispositivos herdado não funcionarão mais.
- Criptografia MDX:
  - **August 1, 2020:** A Citrix começa a aplicar a migração da criptografia MDX para a criptografia de plataforma para aplicativos de produtividade móvel da Citrix e aplicativos MDX de terceiros.
  - **September 1, 2020:** A criptografia MDX atinge o fim da vida útil.

Para dispositivos registrados no DA herdado

- Se você não usa criptografia MDX, nenhuma ação é necessária.
- Se você usa criptografia MDX, migre os dispositivos Android para o Android Enterprise antes de July 31, 2020. Os dispositivos que executam o Android 10 devem se registrar ou se registrar novamente usando o Android Enterprise. Este requisito inclui dispositivos Android no modo somente MAM. Consulte Migrar da administração de dispositivos para o Android Enterprise.

Para dispositivos já inscritos no Android Enterprise a partir de 31 de julho

- Se você publicou os aplicativos usando a plataforma Android Enterprise, a criptografia já é tratada pelo Android Enterprise. Nenhuma ação é necessária.
- Se você publicou os aplicativos usando a plataforma Android legada, republique os aplicativos usando o Android Enterprise antes de July 31, 2020.

Antes de fazer upgrade para o XenMobile 10.12 (no local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos de sistema e compatibilidade e Compatibilidade do XenMobile.

1. Atualize seu Citrix License Server para a versão 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.12.

   A versão mais recente do XenMobile requer o Citrix License Server 11.16 (versão mínima).

   > **Nota:**
   >
   > Se você quiser usar sua própria licença para a Visualização, saiba que a data do Customer Success Services (anteriormente, data do Subscription Advantage) no XenMobile 10.12 é January 20, 2020. A data do Customer Success Services em sua licença Citrix deve ser posterior a esta data.
   >
   > Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile® a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.
   >
   > Para renovar a data em sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte Customer Success Services.

2. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm os seguintes requisitos. Se o Citrix Gateway estiver configurado para persistência SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.

3. Se a máquina virtual que executa o XenMobile Server a ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a RAM mínima recomendada é de 8 GB para ambientes de produção.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante um upgrade, backups completos permitirão que você se recupere.

Para fazer upgrade

Você pode fazer upgrade diretamente para o XenMobile 10.12 a partir do XenMobile 10.11.x ou 10.10.x. Para fazer o upgrade, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar até **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para seu hypervisor, clique em **Download File**.

Para carregar o upgrade, use a página **Release Management** no console do XenMobile. Para obter mais informações, consulte Para fazer upgrade usando a página Release Management.

Após o upgrade

Após o upgrade para o XenMobile 10.12 (local):

Se a funcionalidade que envolve conexões de saída parar de funcionar e você não tiver alterado sua configuração de conexão, verifique o **log do XenMobile Server** para erros como o seguinte: "Não é possível conectar ao servidor VPP: O nome do host '192.0.2.0' não corresponde ao assunto do certificado fornecido pelo par".

O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor PKI da Microsoft. Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão desta propriedade é `false`.

Suporte adicional para iOS 13

O XenMobile Server oferece suporte a dispositivos atualizados para iOS 13. O upgrade afeta seus usuários da seguinte forma:

- Durante o registro, algumas novas telas de Opções do Assistente de Configuração do iOS aparecem. A Apple adicionou uma nova tela de Opções do Assistente de Configuração do iOS

ao iOS 13. As novas opções estão incluídas na página **Settings > Apple Device Enrollment Program (DEP)** nesta versão. Você pode configurar o XenMobile Server para pular essas telas. Essas páginas aparecem para os usuários em dispositivos iOS 13.

- Algumas configurações de política de dispositivo de Restrições que estavam disponíveis em dispositivos supervisionados ou não supervisionados para versões anteriores do iOS estão disponíveis apenas em dispositivos supervisionados para iOS 13+. As dicas de ferramentas atuais do console do XenMobile Server ainda não indicam que essas configurações são apenas para dispositivos supervisionados para iOS 13+.
    - Permitir controles de hardware:
        - FaceTime
        - Instalando aplicativos
    - Permitir aplicativos:
        - iTunes Store
        - Safari
        - Safari > Preenchimento Automático
    - Rede - Permitir ações do iCloud:
        - Documentos e dados do iCloud
    - Configurações somente para dispositivos supervisionados - Permitir:
        - Game Center > Adicionar amigos
        - Game Center > Jogos multiplayer
    - Conteúdo de mídia - Permitir:
        - Música explícita, podcasts e material do iTunes U

Estas restrições aplicam-se da seguinte forma:

- Se um dispositivo iOS 12 (ou inferior) já estiver registrado no XenMobile Server e, em seguida, for atualizado para iOS 13, as restrições anteriores se aplicam a dispositivos não supervisionados e supervisionados.
- Se um dispositivo iOS 13+ não supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas a dispositivos supervisionados.

- Se um dispositivo iOS 13+ supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas a dispositivos supervisionados.

Migração do Programa de Compra por Volume da Apple para o Apple Business Manager (ABM) e Apple School Manager (ASM)

Empresas e instituições que utilizam o Programa de Compra por Volume da Apple (VPP) precisam migrar para Aplicativos e Livros no Apple Business Manager ou Apple School Manager antes de December 1, 2019.

Antes de migrar contas VPP no XenMobile, consulte este artigo de suporte da Apple.

Se sua organização ou escola usa apenas o Programa de Compra por Volume (VPP), você pode se inscrever no ABM/ASM e, em seguida, convidar os Compradores VPP existentes para sua nova conta ABM/ASM. Para ASM, navegar para `<https://school.apple.com>`. Para ABM, navegar para `<https://business.apple.com>`.

Para atualizar sua conta VPP no XenMobile:

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Configurações do iOS**. A página de configuração do **Programa de Compra por Volume** é exibida.
3. Certifique-se de que sua conta ABM ou ASM tenha a mesma configuração de aplicativo que sua conta VPP anterior.
4. No portal ABM ou ASM, baixe um token atualizado.
5. No console do XenMobile, faça o seguinte:

    a. Edite a conta existente do Volume Purchase com as informações de token atualizadas para esse local.

    b. Edite suas credenciais ABM ou ASM. Não altere o sufixo.

    c. Clique em **Salvar** duas vezes.

Para obter mais informações, consulte:

- Programa de Implantação da Apple
- Registro em massa de dispositivos Apple

Suporte para dispositivos COPE do Android Enterprise

O XenMobile Server oferece suporte a dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho, anteriormente conhecidos como dispositivos COPE (corporate-owned personally enabled). Esses dispositivos são um tipo de dispositivos Android Enterprise totalmente gerenciados que também possuem um perfil de trabalho. Você pode aplicar configurações de política separadas ao dispositivo e ao perfil de trabalho. Para esta versão:

- Você pode aplicar configurações separadas ao dispositivo e ao perfil de trabalho usando estas políticas de dispositivo: Credenciais, Senha e Restrições.
- Você pode aplicar a configuração de modo de localização da política de dispositivo Localização ao próprio dispositivo COPE, mas não ao perfil de trabalho do dispositivo COPE. Outras configurações na política de dispositivo Localização não estão disponíveis para dispositivos COPE.
- Você pode aplicar a ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho.

Políticas de dispositivo

Para dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho (dispositivos COPE), algumas políticas de dispositivo podem aplicar configurações separadas a todo o dispositivo e ao perfil de trabalho. No console do XenMobile Server, algumas políticas de dispositivo permitem que você aplique as configurações separadas. Você pode usar outras políticas de dispositivo para aplicar configurações apenas a todo o dispositivo ou apenas ao perfil de trabalho de dispositivos totalmente gerenciados com perfis de trabalho.

Ações de segurança

Para dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho (dispositivos COPE), você pode aplicar:

- A ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho.
- Todas as outras ações de segurança ao dispositivo.

Perfis de registro controlam as opções de registro para dispositivos Android

Os perfis de registro agora controlam como os dispositivos Android são registrados se o Android Enterprise estiver habilitado para sua implantação do XenMobile. Os perfis de registro determinam se os dispositivos Android são registrados no modo Android Enterprise padrão (totalmente gerenciado ou perfil de trabalho) ou no modo herdado (administrador do dispositivo).

Por padrão, o perfil de registro Global registra dispositivos Android Enterprise novos e redefinidos de fábrica como dispositivos totalmente gerenciados e registra dispositivos Android Enterprise BYOD como dispositivos de perfil de trabalho. Para obter mais informações, consulte Android Enterprise.

Preparando dispositivos Android herdados para o Android Enterprise como registro padrão

O Google está descontinuando o modo de administrador do dispositivo de gerenciamento de dispositivos e incentivando os clientes a gerenciar todos os dispositivos Android no modo proprietário do dispositivo ou no modo proprietário do perfil. (Consulte Descontinuação do administrador do dispositivo nos guias do desenvolvedor do Google Android Enterprise.) Para oferecer suporte a essa mudança, o Android Enterprise agora é a opção de registro padrão para dispositivos Android.

Essa mudança significa que, se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise.

Para se preparar para essa mudança, o XenMobile agora permite que você crie perfis de registro que controlam como os dispositivos Android são registrados.

Sua organização pode não estar pronta para começar a gerenciar dispositivos Android legados no modo de proprietário do dispositivo ou no modo de proprietário do perfil. Nesse caso, você pode continuar a gerenciá-los no modo de administrador do dispositivo. Crie um perfil de registro para dispositivos legados e registre novamente todos os dispositivos legados registrados.

Para criar um perfil de registro para dispositivos legados:

1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro.
3. Clique em **Avançar** ou selecione **Android Enterprise** em **Plataformas**. A página Configuração de Registro é exibida.
4. Defina **Gerenciamento** como **Legado (administração de dispositivo)**. Clique em **Avançar** ou selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.

   Tela de configuração de Perfis de Registro(/en-us/xenmobile/server/media/enrollment-profile-android-legacy.png)

5. Escolha o grupo de entrega ou os grupos de entrega que possuem os administradores que registram os dispositivos dedicados. Em seguida, clique em **Salvar**.

Para continuar gerenciando um dispositivo legado no modo de administrador do dispositivo, registre-o ou registre-o novamente usando este perfil. Você registra dispositivos de administrador de dispositivo de forma semelhante aos dispositivos de perfil de trabalho, fazendo com que os usuários baixem o Secure Hub e fornecendo uma URL de servidor de registro.

Para obter mais informações sobre o suporte do Endpoint Management para a transição para o Android Enterprise, consulte o blog, Android Enterprise como padrão para o serviço Citrix Endpoint Management.

Gerenciamento simplificado de aplicativos para Android Enterprise

Você não precisa mais ir ao Google Play gerenciado ou ao portal do Google Developer para aprovar ou publicar aplicativos para o XenMobile Server. Como resultado, a aprovação e a publicação de aplicativos levam cerca de 10 minutos em vez de horas.

Aprove aplicativos Android Enterprise para a Public App Store no console do XenMobile Server. Agora você pode aprovar aplicativos da Google Play Store gerenciada sem sair do console do XenMobile Server. Depois de inserir um nome de aplicativo no campo de pesquisa, a interface do usuário da Google Play Store gerenciada é aberta com as instruções para você aprovar e salvar o aplicativo. Seu aplicativo então preenche os resultados, permitindo que você configure seus detalhes. Consulte Adicionar um aplicativo da loja de aplicativos pública.

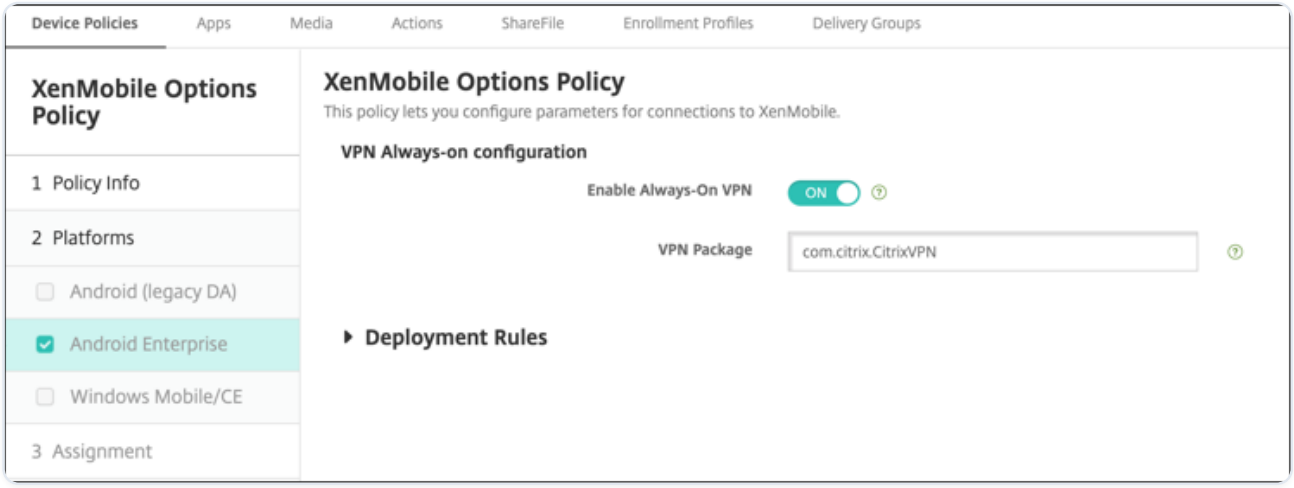
Adicionar aplicativos MDX para Android Enterprise. O console do XenMobile Server agora oferece suporte ao Android Enterprise como plataforma para implantação de aplicativos MDX. Consulte Adicionar um aplicativo MDX.

Aprovar aplicativos MDX para Android Enterprise no console do XenMobile Server. Agora você pode aprovar aplicativos da Google Play Store gerenciada para Android Enterprise sem sair do console do XenMobile Server. Depois de carregar um arquivo MDX, a interface do usuário da Google Play Store gerenciada é aberta com as instruções para você aprovar e salvar o aplicativo. Consulte Adicionar um aplicativo MDX.

Suporte para VPN Always-On para Android Enterprise

A política de dispositivo de opções do XenMobile Server agora permite habilitar a VPN Always-On para Android Enterprise.

Ao configurar perfis VPN para Android Enterprise, em **Perfil VPN padrão**, digite o nome do perfil VPN. O XenMobile usa esse perfil quando os usuários tocam no botão de conexão na interface do usuário do aplicativo Citrix SSO em vez de tocar em um perfil específico. Se este campo for deixado em branco, o perfil principal será usado para a conexão. Se apenas um perfil for configurado, ele será marcado como o perfil padrão. Para uma VPN sempre ativa, este campo deve ser definido com o nome do perfil VPN a ser usado para estabelecer uma VPN sempre ativa.



Configurar a trilha do produto para seus aplicativos Android Enterprise

Ao adicionar um aplicativo de loja pública ou um aplicativo MDX para Android Enterprise, configure a trilha do produto que você deseja enviar para os dispositivos do usuário. Por exemplo, se você tiver uma trilha projetada para testes, poderá selecioná-la e atribuí-la a um grupo de entrega específico. Para saber mais sobre como lançar sua versão, consulte a Central de Ajuda do Google Play. Para obter informações sobre como configurar a trilha do produto, consulte Adicionar um aplicativo MDX ou Adicionar um aplicativo de loja pública.

Forçar redefinição de senha para usuários macOS

Quando um dispositivo macOS recebe um perfil de configuração com uma política de senha, os usuários devem fornecer uma senha que atenda às configurações da política. Agora você pode forçar uma redefinição de senha na próxima vez que um usuário se autenticar. Na política de dispositivo de senha para macOS (10.13 e posterior), habilite a nova configuração **Forçar redefinição de senha**. Para obter mais informações sobre a política, consulte Política de dispositivo de senha.

O que há de novo no XenMobile Server 10.11

XenMobile Server 10.11 (Download em PDF)

Migração do Programa de Compra por Volume da Apple para o Apple Business Manager (ABM) e Apple School Manager (ASM)

Empresas e instituições que usam o Programa de Compra por Volume da Apple (VPP) devem migrar para Aplicativos e Livros no Apple Business Manager ou Apple School Manager antes de December 1, 2019.

Antes de migrar contas VPP no XenMobile, consulte este artigo de suporte da Apple.

Se sua organização ou escola usa apenas o Programa de Compra por Volume (VPP), você pode se inscrever no ABM/ASM e, em seguida, convidar os Compradores VPP existentes para sua nova conta ABM/ASM. Para ASM, navegar para `<https://school.apple.com>`. Para ABM, navegar para `<https://business.apple.com>`.

Para atualizar sua conta de Compra por Volume (anteriormente VPP) no XenMobile®:

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Compra por Volume**. A página de configuração de **Compra por Volume** é exibida.
3. Certifique-se de que sua conta ABM ou ASM tenha a mesma configuração de aplicativo que sua conta VPP anterior.
4. No portal ABM ou ASM, baixe um token atualizado.
5. No console do XenMobile, faça o seguinte:
    a. Edite a conta de Compra por Volume existente com as informações de token atualizadas para esse local.
    b. Edite suas credenciais ABM ou ASM. Não altere o sufixo.
    c. Clique em **Salvar** duas vezes.

Suporte adicional para iOS 13

> **Importante:**

> Para se preparar para atualizações de dispositivos para iOS 12+: O tipo de conexão Citrix VPN na política de dispositivo VPN para iOS não oferece suporte a iOS 12+. Exclua sua política de dispositivo VPN e crie uma política de dispositivo VPN com o tipo de conexão Citrix SSO.

> A conexão Citrix VPN continua a operar em dispositivos implantados anteriormente depois que você exclui a política de dispositivo VPN. Sua nova configuração de política de dispositivo VPN entra em vigor no XenMobile Server 10.11, durante o registro do usuário.

> O XenMobile Server oferece suporte a dispositivos atualizados para iOS 13. A atualização afeta seus usuários da seguinte forma:

- Durante o registro, algumas novas telas de Opções do Assistente de Configuração do iOS aparecem. A Apple adicionou novas telas de Opções do Assistente de Configuração do iOS ao iOS 13. As novas opções não estão incluídas na página **Configurações > Programa de Registro de Dispositivos Apple (DEP)** nesta versão. Como resultado, você não pode configurar o XenMobile Server para ignorar essas telas. Essas páginas aparecem para os usuários em dispositivos iOS 13.
- Algumas configurações de política de dispositivo de Restrições que estavam disponíveis em dispositivos supervisionados ou não supervisionados para versões anteriores do iOS estão disponíveis apenas em dispositivos supervisionados para iOS 13+. As dicas de ferramentas atuais do console do XenMobile Server ainda não indicam que essas configurações são apenas para dispositivos supervisionados para iOS 13+.
    - Permitir controles de hardware:
        - FaceTime
        - Instalar aplicativos
    - Permitir aplicativos:
        - iTunes Store
        - Safari
        - Safari > Preenchimento automático
    - Rede - Permitir ações do iCloud:
        - Documentos e dados do iCloud
    - Configurações somente supervisionadas - Permitir:
        - Game Center > Adicionar amigos
        - Game Center > Jogos multiplayer
    - Conteúdo de mídia - Permitir:

- Música explícita, podcasts e material do iTunes U

Estas restrições se aplicam da seguinte forma:

- Se um dispositivo iOS 12 (ou inferior) já estiver registrado no XenMobile Server e, em seguida, for atualizado para iOS 13, as restrições anteriores se aplicarão a dispositivos não supervisionados e supervisionados.
- Se um dispositivo iOS 13+ não supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicarão somente a dispositivos supervisionados.
- Se um dispositivo iOS 13+ supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicarão somente a dispositivos supervisionados.

Requisitos para certificados confiáveis no iOS 13 e macOS 15

A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, `<https://support.apple.com/pt-br/HT210176>`. Para obter ajuda com o gerenciamento de certificados, consulte Carregar certificados no XenMobile.

Atualizar de GCM para FCM

A partir de April 10, 2018, o Google descontinuou o Google Cloud Messaging (GCM). O Google removeu as APIs de servidor e cliente GCM em May 29, 2019.

> **Requisitos importantes:**
>
> - Atualize para a versão mais recente do XenMobile Server.
> - Atualize para a versão mais recente do Secure Hub.

> O Google recomenda atualizar para o Firebase Cloud Messaging (FCM) imediatamente para começar a aproveitar os novos recursos disponíveis no FCM. Para obter informações do Google, consulte `<https://developers.google.com/cloud-messaging/faq>` e `<https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html>`.

Para continuar o suporte a notificações push para seus dispositivos Android: Se você usa GCM com o XenMobile Server, migre para o FCM. Em seguida, atualize o XenMobile Server com a nova chave FCM disponível no Firebase Cloud Messaging Console.

As etapas a seguir refletem o fluxo de trabalho de registro ao usar certificados confiáveis.

Etapas de atualização:

1. Siga as informações do Google para atualizar do GCM para o FCM.
2. No Firebase Cloud Messaging Console, copie sua nova chave FCM. Você precisará dela para a próxima etapa.
3. No console do XenMobile Server, vá para **Settings > Firebase Cloud Messaging** e configure suas definições.

Os dispositivos mudam para o FCM na próxima vez que proteger com o XenMobile Server e realizam uma atualização de política. Para forçar o Secure Hub a atualizar as políticas: No Secure Hub, vá para **Preferences > Device Information** e toque em **Refresh Policy**. Para obter mais informações sobre como configurar o FCM, consulte Firebase Cloud Messaging.

Antes de atualizar para o XenMobile 10.11 (local)

Alguns requisitos de sistema foram alterados. Para obter informações, consulte Requisitos de sistema e compatibilidade e Compatibilidade do XenMobile.

1. Atualize seu Citrix License Server para 11.15 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.11.

   A versão mais recente do XenMobile requer o Citrix License Server 11.15 (versão mínima).

   > **Nota:**
   >
   > Se você quiser usar sua própria licença para a Prévia, saiba que a data dos Serviços de Sucesso do Cliente (anteriormente, data de Vantagem da Assinatura) no XenMobile 10.11 é April 9, 2019. A data dos Serviços de Sucesso do Cliente em sua licença Citrix deve ser posterior a esta data.
   >
   > Você pode ver a data ao lado da licença no Servidor de Licenças. Se você conectar a versão mais recente do XenMobile a um ambiente de Servidor de Licenças mais antigo, a verificação de conectividade falhará e você não poderá configurar o Servidor de Licenças.

> Para renovar a data da sua licença, baixe o arquivo de licença mais recente do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte Serviços de Sucesso do Cliente.

2. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm os seguintes requisitos. Se o Citrix Gateway estiver configurado para persistência SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
3. Se a máquina virtual que executa o XenMobile Server a ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a RAM mínima recomendada é de 8 GB para ambientes de produção.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do banco de dados de configuração do seu sistema. Se você tiver problemas durante uma atualização, backups completos permitem que você se recupere.

Para atualizar

Você pode atualizar diretamente para o XenMobile 10.11 a partir do XenMobile 10.10.x ou 10.9.x. Para fazer a atualização, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para seu hipervisor, clique em **Download File**.

Para carregar a atualização, use a página **Gerenciamento de Versões** no console do XenMobile. Para obter mais informações, consulte Para atualizar usando a página Gerenciamento de Versões.

Após a atualização

Após a atualização para o XenMobile 10.11 (on-premises):

Se a funcionalidade envolvendo conexões de saída parar de funcionar e você não tiver alterado a configuração de suas conexões, verifique o log do XenMobile Server em busca de erros como o seguinte: “Não é possível conectar ao Servidor VPP: O nome do host '192.0.2.0' não corresponde ao assunto do certificado fornecido pelo par”.

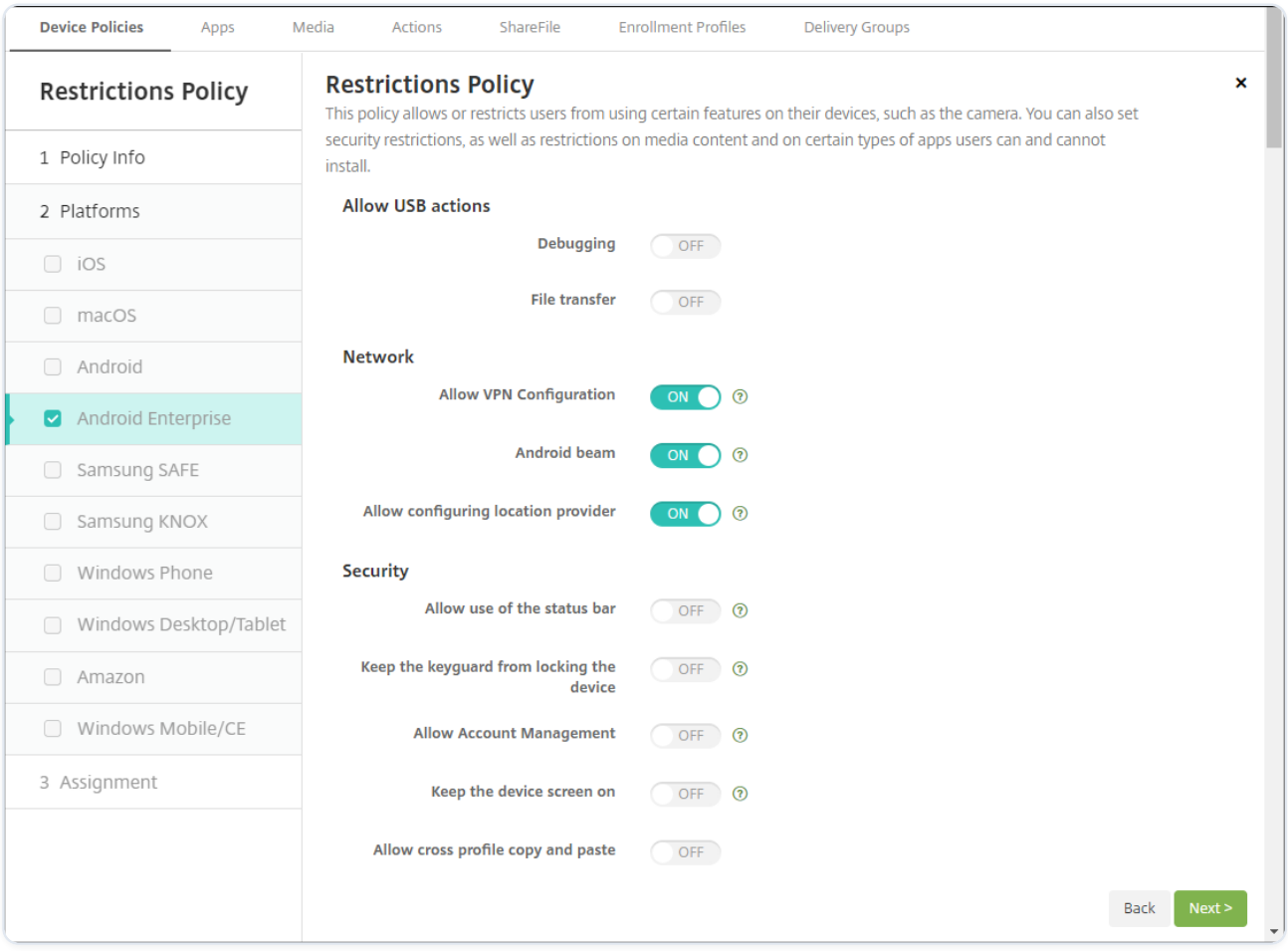
O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor PKI da Microsoft. Se a verificação do nome do host quebrar sua

implantação, altere a propriedade do servidor `disable.hostname.verification` para `true`. O valor padrão desta propriedade é `false`.

Novas e atualizadas configurações de política de dispositivo para dispositivos Android Enterprise

Unificação da política Samsung Knox e Android Enterprise. Para dispositivos Android Enterprise executando Samsung Knox 3.0 ou posterior e Android 8.0 ou posterior: Knox e Android Enterprise são combinados em uma solução unificada de gerenciamento de dispositivos e perfis. Configure as configurações do Knox na página Android Enterprise das seguintes políticas de dispositivo:

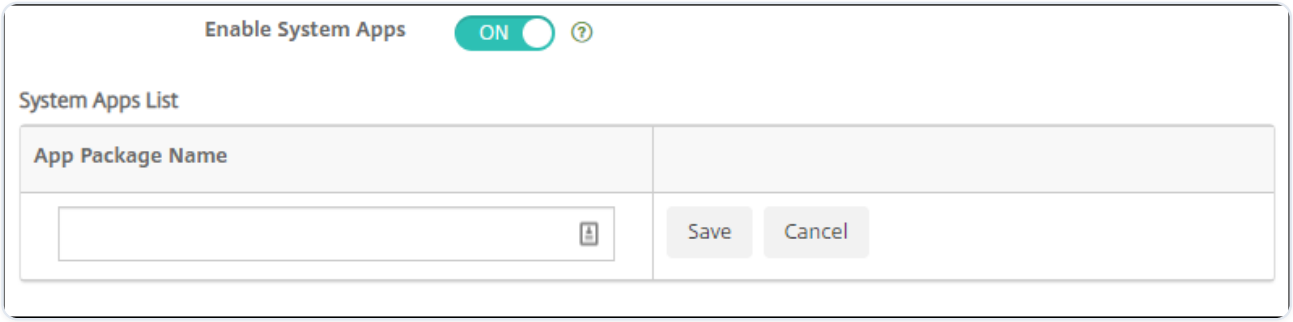
- Política de dispositivo de atualização do SO**.** Inclui configurações para atualizações FOTA do Samsung Enterprise.
- Política de dispositivo de senha**.**
- **Política de dispositivo de chave de licença MDM Samsung.** Configura a chave de licença Knox.
- Configurações da política de dispositivo de restrições**.**



Política de dispositivo de inventário de aplicativos para Android Enterprise. Agora você pode coletar um inventário dos aplicativos Android Enterprise em dispositivos gerenciados. Consulte Política de dispositivo de inventário de aplicativos.

Acessar todos os aplicativos do Google Play na loja gerenciada do Google Play. A propriedade de servidor **Acessar todos os aplicativos na loja gerenciada do Google Play** torna todos os aplicativos da loja pública do Google Play acessíveis a partir da loja gerenciada do Google Play. Definir esta propriedade como **true** permite os aplicativos da loja pública do Google Play para todos os usuários do Android Enterprise. Os administradores podem então usar a Política de dispositivo de restrições para controlar o acesso a esses aplicativos.

Habilitar aplicativos do sistema em dispositivos Android Enterprise. Para permitir que os usuários executem aplicativos do sistema pré-instalados no modo de perfil de trabalho do Android Enterprise ou no modo totalmente gerenciado, configure a Política de dispositivo de restrições. Essa configuração concede ao usuário acesso a aplicativos padrão do dispositivo, como câmera, galeria e outros. Para restringir o acesso a um aplicativo específico, defina as permissões do aplicativo usando a Política de dispositivo de permissões de aplicativos do Android Enterprise.



Suporte para dispositivos dedicados do Android Enterprise. O XenMobile agora oferece suporte ao gerenciamento de dispositivos dedicados, anteriormente chamados de dispositivos de uso único de propriedade corporativa (COSU).

Dispositivos Android Enterprise dedicados são dispositivos totalmente gerenciados que são dedicados a cumprir um único caso de uso. Você restringe esses dispositivos a um aplicativo ou a um pequeno conjunto de aplicativos necessários para realizar as tarefas exigidas para este caso de uso. Você também impede que os usuários habilitem outros aplicativos ou realizem outras ações no dispositivo.

Para obter informações sobre o provisionamento de dispositivos Android Enterprise, consulte Provisionamento de dispositivos Android Enterprise dedicados.

Política renomeada. Para se alinhar à terminologia do Google, a política de dispositivo de restrição de aplicativos do Android Enterprise agora é chamada de política de dispositivo de configurações gerenciadas. Consulte Política de dispositivo de configurações gerenciadas.

Bloquear e redefinir senha para Android Enterprise

O XenMobile agora oferece suporte à ação de segurança Bloquear e Redefinir senha para dispositivos Android Enterprise. Esses dispositivos devem estar registrados no modo de perfil de trabalho executando Android 8.0 ou superior.

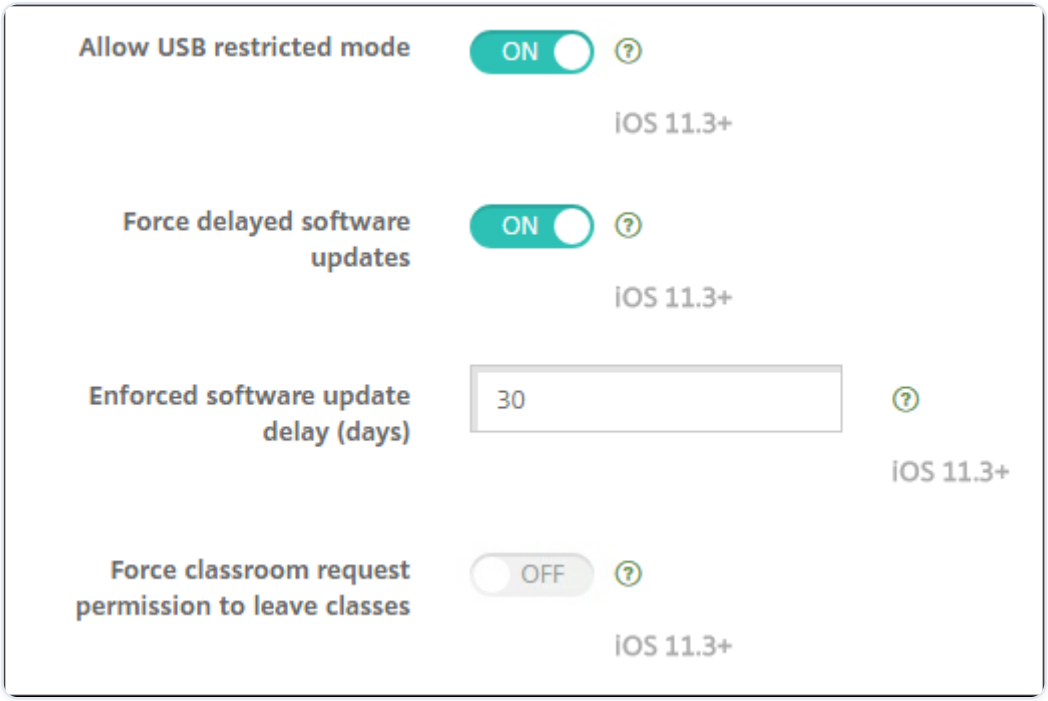
- A senha enviada bloqueia o perfil de trabalho. O dispositivo não é bloqueado.
- Se nenhuma senha for enviada ou a senha enviada não atender aos requisitos de senha:
  - E nenhuma senha já estiver definida no perfil de trabalho, o dispositivo é bloqueado.
  - E uma senha já estiver definida no perfil de trabalho. O perfil de trabalho é bloqueado, mas o dispositivo não é bloqueado.

Para obter mais informações sobre as ações de segurança de bloqueio e redefinição de senha, consulte Ações de segurança.

Novas configurações de política de dispositivo de Restrições para iOS ou macOS

- **Aplicativos não gerenciados leem contatos gerenciados:** Opcional. Disponível apenas se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver desabilitado. Se esta política estiver habilitada, aplicativos não gerenciados podem ler dados dos contatos de contas gerenciadas. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Aplicativos gerenciados gravam contatos não gerenciados:** Opcional. Se habilitado, permite que aplicativos gerenciados gravem contatos nos contatos de contas não gerenciadas. Se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver habilitado, esta restrição não terá efeito. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Preenchimento Automático de Senha:** Opcional. Se desabilitado, os usuários não podem usar os recursos de Preenchimento Automático de Senhas ou Senhas Fortes Automáticas. O padrão é **Ativado**. Disponível a partir do iOS 12 e macOS 10.14.
- **Solicitações de proximidade de senha:** Opcional. Se desabilitado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do iOS 12 e macOS 10.14.
- **Compartilhamento de Senha:** Opcional. Se desabilitado, os usuários não podem compartilhar suas senhas usando o recurso Senhas do AirDrop. O padrão é **Ativado**. Disponível a partir do iOS 12 e macOS 10.14.

- **Forçar data e hora automáticas:** Supervisionado. Se habilitado, os usuários não podem desabilitar a opção **Geral > Data e Hora > Definir Automaticamente**. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Permitir modo restrito USB:** Disponível apenas para dispositivos supervisionados. Se definido como Desativado, o dispositivo pode sempre se conectar a acessórios USB enquanto bloqueado. O padrão é **Ativado**. Disponível a partir do iOS 11.3.
- **Forçar atualizações de software atrasadas:** Disponível apenas para dispositivos supervisionados. Se definido como **Ativado**, atrasa a visibilidade das Atualizações de Software para o usuário. Com esta restrição em vigor, o usuário não verá uma atualização de software até o número especificado de dias após a data de lançamento da atualização de software. O padrão é **Desativado**. Disponível a partir do iOS 11.3 e macOS 10.13.4.
- **Atraso forçado da atualização de software (dias):** Disponível apenas para dispositivos supervisionados. Esta restrição permite ao administrador definir por quanto tempo atrasar uma atualização de software no dispositivo. O máximo é 90 dias e o valor padrão é **30**. Disponível a partir do iOS 11.3 e macOS 10.13.4.
- **Forçar solicitação de permissão da sala de aula para sair das turmas:** Disponível apenas para dispositivos supervisionados. Se definido como **Ativado**, um aluno matriculado em um curso não gerenciado com o Classroom deve solicitar permissão ao professor ao tentar sair do curso. O padrão é **Desativado**. Disponível a partir do iOS 11.3.



Consulte Política de dispositivo de restrições.

Atualizações da política de dispositivo do Exchange para iOS ou macOS

Mais configurações de assinatura e criptografia S/MIME do Exchange a partir do iOS 12. A política de dispositivo do Exchange agora inclui configurações para configurar a assinatura e a criptografia S/MIME.

Para assinatura S/MIME:

- **Credencial de identidade de assinatura:** Escolha a credencial de assinatura a ser usada.
- **S/MIME Assinatura Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**.
- **S/MIME Certificado de Assinatura UUID Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Desativado**.

Para criptografia S/MIME:

- **Credencial de identidade de criptografia:** Escolha a credencial de criptografia a ser usada.
- **Habilitar alternância S/MIME por mensagem:** Quando definido como **Ativado**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que eles compõem. O padrão é **Desativado**.
- **S/MIME Criptografar por Padrão Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem, nas configurações de seus dispositivos, selecionar se o S/MIME está ativado por padrão. O padrão é **Desativado**.
- **S/MIME Certificado de Criptografia UUID Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a identidade e a criptografia S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**.

Configurações do Exchange OAuth a partir do iOS 12. Agora você pode configurar a conexão com o Exchange para usar o OAuth para autenticação.

Configurações de OAuth do Exchange a partir do macOS 10.14. Agora você pode configurar a conexão com o Exchange para usar OAuth para autenticação. Para autenticação usando OAuth, você pode especificar a URL de login para uma configuração que não usa AutoDiscovery.

Consulte Política de dispositivo do Exchange.

Atualizações da política de dispositivo de e-mail para iOS

Mais configurações de assinatura e criptografia S/MIME do Exchange a partir do iOS 12. A política de dispositivo de e-mail inclui mais configurações para configurar a assinatura e a criptografia S/MIME.

Para assinatura S/MIME:

- **Habilitar Assinatura S/MIME:** Selecione se esta conta oferece suporte à assinatura S/MIME. O padrão é **Ativado**. Quando definido como **Ativado**, os seguintes campos aparecem.
  - **Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
  - **UUID do Certificado de Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.

Para criptografia S/MIME:

- **Habilitar Criptografia S/MIME:** Selecione se esta conta oferece suporte à criptografia S/MIME. O padrão é **Desativado**. Quando definido como **Ativado**, os seguintes campos aparecem.
  - **Habilitar alternância S/MIME por mensagem:** Quando definido como **Ativado**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que eles compõem. O padrão é **Desativado**.
  - **Criptografia S/MIME por Padrão Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem, nas configurações de seus dispositivos, selecionar se o S/MIME está ativado por padrão. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
  - **UUID do Certificado de Criptografia S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a identidade e a criptografia S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.

Consulte Política de dispositivo de e-mail.

Atualizações da política de dispositivo de notificações de aplicativos para iOS

As seguintes configurações de notificações de aplicativos estão disponíveis a partir do iOS 12.

- **Mostrar no CarPlay:** Se **Ativado**, as notificações são exibidas no Apple CarPlay. O padrão é **Ativado**.
- **Habilitar Alerta Crítico:** Se **Ativado**, um aplicativo pode marcar uma notificação como uma notificação crítica que ignora as configurações de Não Perturbe e de toque. O padrão é **Desativado**.

Consulte Política de dispositivo de notificações de aplicativos

Suporte para iPads compartilhados usados com o Apple Education

A integração do XenMobile com os recursos do Apple Education agora oferece suporte a iPads compartilhados. Vários alunos em uma sala de aula podem compartilhar um iPad para diferentes disciplinas ensinadas por um ou vários instrutores.

Você ou os instrutores registram os iPads compartilhados e, em seguida, implantam políticas de dispositivo, aplicativos e mídia nos dispositivos. Depois disso, os alunos fornecem suas credenciais de ID Apple gerenciada para fazer login em um iPad compartilhado. Se você implantou anteriormente uma política de Configuração de Educação para os alunos, eles não fazem mais login como um "Outro Usuário" para compartilhar dispositivos.

Pré-requisitos para iPads compartilhados:

- Qualquer iPad Pro, iPad de 5ª geração, iPad Air 2 ou posterior, e iPad mini 4 ou posterior
- Pelo menos 32 GB de armazenamento
- Supervisionado

Para obter mais informações, consulte Configurar iPads compartilhados.

Alteração nas permissões de controle de acesso baseado em função (RBAC)

A permissão RBAC Adicionar/Excluir Usuários Locais agora está dividida em duas permissões: Adicionar Usuários Locais e Excluir Usuários Locais.

Para obter mais informações, consulte Configurar funções com RBAC.

Avisos de terceiros

Esta versão do XenMobile® pode incluir software de terceiros licenciado sob os termos definidos nos seguintes documentos:

Avisos de Terceiros do XenMobile

Descontinuação

Os anúncios neste artigo têm como objetivo fornecer um aviso prévio sobre os recursos do XenMobile Server que estão sendo desativados. Fornecemos essas informações para que você possa tomar decisões de negócios oportunas. A Citrix monitora o uso e o feedback dos clientes para determinar quando eles serão retirados. Os anúncios podem mudar em versões subsequentes e podem não incluir todos os recursos ou funcionalidades descontinuados. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo Política de Suporte ao Ciclo de Vida do Produto.

Descontinuações e remoções

A lista a seguir mostra os recursos do XenMobile® Server que foram descontinuados ou removidos.

Itens *descontinuados* não são removidos imediatamente. A Citrix® continua a oferecer suporte a um item descontinuado até removê-lo em uma versão futura.

Itens *removidos* são removidos ou não são mais suportados no XenMobile Server.

Para obter informações sobre os aplicativos de produtividade móvel que atingiram o Fim da Vida Útil, consulte Aplicativos EOL e descontinuados.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
Licenciamento baseado em arquivo	O licenciamento baseado em arquivo não funcionará mais após April 15, 2026.	Outubro de 2025	Abril de 2026	License Activation Service (LAS) é a tecnologia de próxima geração para ativações de produtos em todo o conjunto de produtos Citrix. Os clientes que usam licenciamento baseado em arquivo são

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
				obrigados a atualizar para uma versão compatível e realizar esta transição tecnológica antes de April 15, 2026. O LAS será a única forma de ativar e licenciar componentes Citrix on-premises após April 15, 2026.
XenMobile Mail Manager (XMM)/ XenMobile NetScaler Connector (XNC)	Suporte descontinuado para XMM e XNC.	Junho de 2025	Setembro de 2025	Nenhuma alternativa.
Hypervisores	Suporte descontinuado para Citrix XenServer 8.2 e anteriores, VMware ESXi 6.x e anteriores, e Hyper-V 2016.	Março de 2025	Maio de 2025	Atualize o sistema para uma das seguintes versões suportadas: Citrix Hypervisor 8.2 CU1 e posteriores, VMware (ESXi 7.0, ESXi 8.0), ou Hyper-V

XENMOBILE® SERVER

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
				(Windows Server 2019 ou Windows Server 2022).
Integração com ShareFile	A integração com o ShareFile será descontinuada se o ShareFile (agora Progress) descontinuar o suporte.	Janeiro de 2025		Sem alternativa
XML personalizado para Zebra	Suporte descontinuado para XML personalizado em dispositivos Zebra	Janeiro de 2022	Meta: Junho de 2022	Use a configuração gerenciada do Android Enterprise.
Windows Information Protection (WIP)	Suporte descontinuado para Windows Information Protection conforme o anúncio da Microsoft aqui.	Agosto de 2022	Meta: Outubro de 2022	Sem alternativa
XenMobile Analyzer	Suporte descontinuado para a ferramenta XenMobile Analyzer.	Julho de 2022	Meta: March 31, 2023	Sem alternativa

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
Identidades PKI: Genérica, PKI Symantec, DigiCert e adaptador Entrust	Suporte preterido para entidades PKI genéricas, gerenciadas pela DigiCert e de adaptador Entrust.	Junho de 2021	Janeiro de 2022	Sem alternativa
Configuração de convite de inscrição	Suporte preterido para usar IMEI, número de série e UDID de um dispositivo para criar um convite de inscrição.	Janeiro de 2022	Maio de 2022	Ao criar um convite de inscrição, configure as configurações disponíveis em **Gerenciar > Convites de Inscrição** no console do XenMobile.
Gateway SMS da operadora	Suporte preterido para notificações do gateway SMS Nexmo	Janeiro de 2022	Abril de 2022	Usar notificações do servidor SMTP
Provedor de Serviços Móveis (MSP)	Suporte obsoleto para a interface MSP para consultar dispositivos Blackberry e outros dispositivos Exchange ActiveSync e emitir operações	Janeiro de 2022	Abril de 2022	Sem alternativa

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
Modo Kiosk da Samsung	Descontinuar o suporte para o modo Kiosk Samsung herdado baseado no modo Administrador de Dispositivo (DA).	Janeiro de 2022	Março de 2022	Usar o modo Kiosk do Android Enterprise (AE).
Permitir restrição de conexão automática a pontos de acesso Wi-Fi Sense para dispositivos Windows	Remover o suporte para a restrição de conexão automática a pontos de acesso Wi-Fi Sense para dispositivos Windows 10. O Windows 10 não oferece mais suporte a esse recurso. Para obter informações, consulte a documentação da Microsoft.	Outubro de 2021	Fevereiro de 2022	Sem alternativa
Plataformas Samsung SAFE/Samsung Knox	Suporte descontinuado para SAFE e Plataforma Knox.	Janeiro de 2022	Junho de 2022	Utilize o plug-in do Knox Service via política de configuração de aplicativo gerenciado para configurar

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
				políticas Knox usando o Android Enterprise.
Modo de registro de Alta Segurança	Suporte descontinuado para gerar convites de registro com o modo de segurança de registro de **Alta Segurança**.	Julho de 2021	Fevereiro de 2022	Consulte Registrar dispositivos para uma lista de modos de segurança de registro suportados.
Função RBAC - Registrador de dispositivos compartilhados e registrador de dispositivos COSU	Descontinuar o suporte para configurações predefinidas de Controle de Acesso Baseado em Função para o registrador de dispositivos compartilhados e o registrador de dispositivos COSU	Julho de 2021	Dezembro de 2021	Configure dispositivos iOS através de Métodos de registro suportados. Configure dispositivos Android COSU (dedicados) através de Perfis de registro.
Knox Mobile Enrollment (DA legado)	Suporte descontinuado para Knox Mobile Enrollment (KME) no modo de Administrador de Dispositivo legado em	Maio de 2021	Junho de 2021	Use o KME para registrar no modo Android Enterprise. Android 9, 10, 11 suportam o Android Enterprise.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	todas as versões do Android.			
Aplicativos de mobilidade Citrix e aplicativos Workspace para Android 7.x e iOS 12.x	Suporte descontinuado para as versões Android 7.x e iOS 12.x de Secure Hub, Secure Mail, Secure Web e o aplicativo Citrix Workspace.	Abril de 2021	Junho de 2021	Use, no mínimo, a versão atual e a anterior de cada plataforma de sistema operacional principal. Dispositivos mais antigos permanecem registrados. No entanto, a Citrix não testa nem oferece suporte aos dispositivos legados.
Credenciais derivadas	Suporte descontinuado para credenciais derivadas e o aplicativo Citrix Derived Credentials Manager.	Março de 2021	Dezembro de 2021	Consulte iOS para obter uma lista dos tipos de autenticação compatíveis com iOS.
Internet Explorer 11	Suporte descontinuado para o uso do Internet Explorer com o console do	Janeiro de 2021	Janeiro de 2021	Use a versão mais recente destes navegadores da web: Google Chrome, Mozilla Firefox,

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	XenMobile Server.			Microsoft Edge, Apple Safari
Suporte a token de software RSA para Android	Suporte descontinuado para a importação direta de tokens de software RSA para o Secure Hub para Android.	Janeiro de 2021	Fevereiro de 2021	Você pode importar o token de software RSA dentro do aplicativo RSA Secure ID disponível no Google Play. Em seguida, você pode usar o token para autenticação do Citrix Gateway.
Android - Sony	Suporte descontinuado para dispositivos Android Sony e políticas específicas da Sony.	Janeiro de 2021	Fevereiro de 2022	Usar Android Enterprise
Android - HTC	Suporte descontinuado para dispositivos Android HTC e políticas específicas da HTC.	Janeiro de 2021	Fevereiro de 2022	Usar Android Enterprise
Android - Amazon	Suporte descontinuado para dispositivos	Janeiro de 2021	Fevereiro de 2022	Usar Android Enterprise

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	Android Amazon e políticas específicas da Amazon.			
Componente de terceiros do painel do XenMobile	Descontinuaremos um componente de terceiros usado como parte do painel do XenMobile.	Dezembro de 2020	Janeiro de 2021	Para continuar usando o painel, atualize para o XenMobile 10.12 ou posterior
Aplicativos publicados para o modo legado de Administrador de Dispositivo em dispositivos Android Enterprise	Não entregamos mais aplicativos publicados para a plataforma DA legada a dispositivos registrados no Android Enterprise.	Outubro de 2020	Novembro de 2020	Para dispositivos Android Enterprise, publique aplicativos para a plataforma Android Enterprise. Para continuar a publicar aplicativos DA legados em dispositivos no modo DA, crie um grupo de entrega separado para esses aplicativos.
Portas de saída APNs	O suporte da Apple para o protocolo binário legado APNs termina a	Outubro de 2020	Março de 2021	Use a porta 443 ou 2197 em vez disso. Consulte Abrir portas XenMobile para

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	partir de March 31, 2021. A Apple recomenda que você use a API do provedor APNs baseada em HTTP/2 em vez disso. Como parte dessa mudança, estamos descontinuando o suporte para as portas 2195 e 2196, usadas para enviar notificações APNs para `*.push.apple.com`.			gerenciar dispositivos.
Contêiner Samsung SEAMS	Suporte descontinuado para o contêiner Samsung SEAMS.	Junho de 2020	Agosto de 2020	Use o aplicativo Samsung Knox Service Plug-in (KSP) para Android Enterprise. Consulte Adicionar o aplicativo de plug-in de serviço Knox.
Certificados SSL (Secure Sockets Layer) autoassinados	Suporte obsoleto para certificados SSL	Maio de 2020		Substitua seu certificado autoassinado existente por

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	autoassinados para todas as plataformas de dispositivos.			um certificado SSL confiável de uma autoridade de certificação (CA) conhecida.
Algoritmos de assinatura de autenticação baseados em certificado (não-FIPS e cifras fracas)	Suporte obsoleto para os seguintes algoritmos de assinatura: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	Maio de 2020	Junho de 2021	Ao criar um CSR para um provedor de credenciais no console do XenMobile (**Configurações > Provedores de Credenciais > Solicitação de Assinatura de Certificado**), escolha uma cifra mais forte.
Servidores de banco de dados	Suporte obsoleto para Microsoft SQL Server 2014 e anteriores.	Outubro de 2021	Agosto de 2022	Atualize o sistema para uma das seguintes versões suportadas: Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 ou

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
				Microsoft SQL Server 2019 CTP 3.2. Consulte a lista de servidores suportados em Requisitos de sistema e compatibilidade.
Hipervisores	Suporte obsoleto para Citrix XenServer 6.5.x e anteriores, VMware ESXi 5.5 Update 3 e anteriores, e Hyper-V 2012.	Maio de 2020	Agosto de 2020	Atualize o sistema para uma das seguintes versões suportadas: Citrix Hypervisor 8.0 e posterior, Citrix XenServer 7.0 e posterior, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 patch 10 ou ESXi 7.0), ou Hyper-V (Windows Server 2016 ou Windows Server 2019).
Citrix Launcher	Suporte obsoleto para o aplicativo	Maio de 2020	Agosto de 2020 (remover da loja de aplicativos)	Use dispositivos de provisionamento como

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	Legacy Citrix Launcher.			quiosques (dispositivos dedicados) e Citrix Launcher para Android Enterprise. Para obter mais informações, consulte a substituição do Citrix Launcher.
Aplicativos de mobilidade Citrix e aplicativos Workspace para Android 6.x e iOS 11.x	Suporte obsoleto para as versões Android 6.x e iOS 11.x de Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace.	Abril de 2020	Junho de 2020	Use, no mínimo, a versão atual e a anterior de cada plataforma de sistema operacional principal.
MDX Toolkit e MDX Service	Suporte descontinuado para o MDX Toolkit e MDX Service em favor do SDK de Gerenciamento de Aplicativos Móveis (MAM). Durante o período de transição, você pode usar aplicativos empacotados	Março de 2020	Meta: Julho de 2023	Para continuar gerenciando seus aplicativos corporativos, use o SDK MAM.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	com MDX e aplicativos desenvolvidos com o SDK MAM.			
MDX: Servidor Gateway Alternativo	Autenticação de etapa adicional descontinuada para dispositivos iOS e Android.	Março de 2020	Setembro de 2021	Sem alternativa
MDX: Micro VPN (modo de túnel completo)	Túnel de rede virtual privada (VPN) completo descontinuado para dispositivos iOS e Android.	Março de 2020	Setembro de 2021	Use o modo SSO Web do SDK MAM ou crie uma política de VPN por aplicativo com o tipo de conexão Citrix SSO.
MDX: suporte a arquivo PAC	Suporte descontinuado para um arquivo de Configuração Automática de Proxy (PAC) com uma implantação de túnel VPN completo para dispositivos iOS e Android.	Março de 2020	Setembro de 2021	Use o Citrix Gateway para se conectar através de um servidor proxy para acesso a redes internas.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
MDX: suporte a dispositivo compartilhado	Suporte a dispositivo compartilhado descontinuado para aplicativos MDX.	Março de 2020	Setembro de 2021	Para Android Enterprise, use o suporte a dispositivo compartilhado para MDM. Para iOS, use o Apple School Manager ou GroundControl.
Novas inscrições de Administrador de Dispositivo para Android 10	Suporte descontinuado para novas inscrições ou reinscrições no modo Administrador de Dispositivo legado em dispositivos Android 10. Dispositivos já inscritos continuam funcionando.	Fevereiro de 2020	Setembro de 2020	Inscreva novos dispositivos Android 10+ no Android Enterprise.
Modo de Administrador de Dispositivo Legado para dispositivos Android 10	O Google descontinuou algumas APIs de Administrador de Dispositivo. A Citrix não oferece suporte a dispositivos Android 10 registrados no modo de	Fevereiro de 2020	Novembro de 2020	Migre dispositivos Android 10 para o Android Enterprise.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	Administrador de Dispositivo a partir da atualização para o Citrix Secure Hub™ que visa o nível 29 da API do Android.			
Criptografia MDX	Criptografia MDX descontinuada e o recurso de criptografia MDX no console do XenMobile.	Outubro de 2019	Setembro de 2020	Habilite a criptografia da plataforma iOS ou Android usando nosso recurso de Gerenciamento de Criptografia com verificação de conformidade adicional. Certifique-se de ter testado e planejado a migração da criptografia MDX até julho de 2020.
Política de dispositivo de senha: A configuração **Sem Restrições** para Android Enterprise	Dispositivos Android Enterprise executando Android 7 ou superior suportam apenas uma senha criada	Fevereiro de 2019	Abril de 2019	Essa alteração não afeta a experiência atual de login do usuário.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	com restrições de caracteres. Se você definiu anteriormente **Caracteres obrigatórios** como **Sem Restrições**, esta atualização altera esse valor para **Somente números**.			
Suporte Remoto	Descontinuado o cliente de Suporte Remoto para implantações de XenMobile Server on-premises em cluster.	Janeiro de 2019	Agosto de 2020	Sem alternativa
Extensões de Rede do Secure Hub para iOS	Descontinuado o framework de Extensão de Rede que permitia personalizar recursos de rede para dispositivos iOS a partir da versão 20.3.0 do Secure Hub.	Outubro de 2018	Março de 2020	Sem alternativa

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
Versões 1.0 e 1.1 do TLS	Para melhorar a segurança do XenMobile, a Citrix agora bloqueia qualquer comunicação via Transport Layer Security (TLS) 1.0 e 1.1. Como resultado de sua segurança enfraquecida, o PCI Council está descontinuando o TLS 1.0 e o TLS 1.1.	Junho de 2018	Março de 2019	Atualize para TLS 1.2.
Windows Mobile/CE	Suporte descontinuado para dispositivos Windows Mobile/CE.	Abril de 2018	Setembro de 2020	Use Windows 10 Desktop e Laptop.
Android TouchDown	A DigiCert parou de oferecer suporte ao Android TouchDown. A Citrix removerá a página da plataforma Android TouchDown da política de	Julho de 2018	2021	Recomendação: Use o Citrix Secure Mail.

ITEM	DESCRIÇÃO	DESCONTINUAÇÃO ANUNCIADA	REMOVIDO	ALTERNATIVA
	dispositivo do Exchange.			
Túnel VPN completo - Android	Suporte descontinuado para túnel VPN completo do Android.	Março de 2020	Setembro de 2021	Modo SSO da Web do MAM SDK.
Permitir troca de modo VPN - Android	Suporte descontinuado para troca de modo VPN Permitir Android.	Março de 2020	Setembro de 2021	Nenhuma alternativa
Troca de Documentos de Entrada - Android	Suporte descontinuado para Troca de Documentos de Entrada do Android.	Março de 2020	Setembro de 2021	Nenhuma alternativa

Problemas corrigidos

O XenMobile 10.16 inclui os seguintes problemas corrigidos:

- Após a atualização para a versão 10.16 do XenMobile Server, o XenMobile Server parou de enviar logs para o Syslog Server.
- O Firebase Cloud Messaging usando a API HTTP v1 não funciona corretamente quando um proxy é configurado.
- Nos dispositivos iOS registrados no modo **somente MAM**, você não consegue instalar aplicativos empresariais ou MDX da loja Secure Hub.
- Um erro é exibido ao editar ou implantar a **política de configurações gerenciadas** em dispositivos Android Enterprise.
- Após configurar o ID de rastreamento de um aplicativo, você não consegue ver a versão de visualização esperada do aplicativo no console do XenMobile® Server. Em vez disso, você vê a versão de produção do aplicativo.
- No XenMobile Server, você não consegue instalar os aplicativos empacotados MDX da loja Secure Hub quando a política de dispositivo de perfil de provisionamento está em status pendente.
- Após a renovação do perfil MDM, os iPads compartilhados do ABM passam para o status não gerenciado.
- Você não consegue configurar os aplicativos Enterprise na plataforma Android ao usar o algoritmo APK Signature Scheme v2 e posterior.
- Você não consegue exportar dispositivos usando a API device/filter.
- Se você estiver registrando dispositivos Android ou iOS com MAM e MDM usando políticas de autenticação nFactor no NetScaler®, o dispositivo será registrado apenas com MDM.
- Ao exportar os scripts de configuração da Autenticação do Citrix Gateway nas versões 10.14 ou posteriores do XenMobile Server, os scripts são truncados e não funcionam.
- No XenMobile Server, você não consegue reeditar os aplicativos VPP sincronizados cuja descrição contém **\b**.
- Nas versões 10.15 e posteriores do XenMobile Server, o Online Certificate Status Protocol (OCSP) não está respondendo às solicitações.

- No XenMobile Server, não é possível registrar os dispositivos que estão executando o Windows 11.
- Em dispositivos Android, ao alternar do MDX Toolkit legado para o MAM SDK, o aplicativo Secure Mail é removido da Secure Hub Store.
- No console do XenMobile Server, não é possível ver a versão do Rapid Security Response (RSR).
- Não é possível baixar aplicativos de **Contas do Google Play Gerenciadas**.
- Após a atualização para o XenMobile Server 10.16, as políticas de dispositivo de Restrições do iOS existentes que usam "Uso de aplicativo restrito" falham ao serem implantadas nos dispositivos iOS.
- Não é possível implantar a política de dispositivo Webclip em dispositivos iOS compartilhados ao usar configurações ABM ou ASM.
- Não é possível ver o botão **Organizar Aplicativos** na página **Configurar** > **Aplicativos** para **Android Enterprise** > **Aplicativos da Google Play Store Gerenciada**.
- Não é possível ver nenhum valor no menu suspenso **Certificado CA** ao configurar a política de Wi-Fi para a plataforma **Android Enterprise**. Apenas a opção **Selecionar certificado** é exibida.
- Para problemas corrigidos na versão 10.15.0 do lançamento de patch contínuo, consulte:
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 8
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 7
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 6
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 5
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 4
  - Notas de Versão para XenMobile Server 10.15 Rolling Patch 3

Informações relacionadas

Central de Conhecimento de Suporte do XenMobile

Problemas conhecidos

Não há problemas conhecidos no XenMobile 10.16.

- Para problemas conhecidos relacionados a aplicativos de produtividade móvel, consulte Secure Hub, Secure Mail e Secure Web.
- Para problemas conhecidos na versão mais recente do patch cumulativo 10.15.0, consulte Release Notes for XenMobile Server 10.15 Rolling Patch 7.

Informações relacionadas

XenMobile Support Knowledge Center

Arquitetura

Os requisitos de gerenciamento de dispositivos e aplicativos da sua organização determinam os componentes do XenMobile® em sua arquitetura XenMobile. Os componentes do XenMobile são modulares e se complementam. Por exemplo, sua implantação inclui o Citrix Gateway:

- O Citrix Gateway oferece aos usuários acesso remoto a aplicativos móveis e rastreia os tipos de dispositivos dos usuários.
- O XenMobile é onde você gerencia esses aplicativos e dispositivos.

Implantação de componentes do XenMobile: Você pode implantar o XenMobile para permitir que os usuários se conectem a recursos em sua rede interna das seguintes maneiras:

- Conexões com a rede interna. Se seus usuários estiverem remotos, eles podem se conectar usando uma conexão VPN ou micro VPN através do Citrix Gateway. Essa conexão fornece acesso a aplicativos e desktops na rede interna.
- Registro de dispositivos. Os usuários podem registrar dispositivos móveis no XenMobile para que você possa gerenciar os dispositivos no console do XenMobile que se conectam aos recursos da rede.
- Aplicativos web, SaaS e móveis. Os usuários podem acessar seus aplicativos web, SaaS e móveis do XenMobile através do Secure Hub.
- Aplicativos baseados em Windows e desktops virtuais. Os usuários podem se conectar com o Citrix Receiver™ ou um navegador da web para acessar aplicativos baseados em Windows e desktops virtuais do StoreFront ou da Web Interface.

Para obter qualquer uma dessas funcionalidades para um XenMobile Server local, a Citrix recomenda implantar os componentes do XenMobile na seguinte ordem:

- Citrix Gateway. Você pode configurar as definições no Citrix Gateway para habilitar a comunicação com o XenMobile, StoreFront™ ou a Web Interface usando o assistente de Configuração Rápida. Antes de usar o assistente de Configuração Rápida no Citrix Gateway, você deve instalar um dos seguintes componentes para configurar as comunicações: XenMobile, StoreFront ou a Web Interface.
- XenMobile. Depois de instalar o XenMobile, você pode configurar políticas e definições no console do XenMobile que permitem aos usuários registrar seus dispositivos móveis. Você

também pode configurar aplicativos móveis, web e SaaS. Os aplicativos móveis podem incluir aplicativos da Apple App Store ou Google Play. Os usuários também podem se conectar a aplicativos móveis que você empacota com o MDX Toolkit e carrega para o console.

- MAM SDK ou MDX Toolkit. A tecnologia de empacotamento MDX está programada para atingir o fim da vida útil (EOL) em julho de 2023. Para continuar gerenciando seus aplicativos corporativos, você deve incorporar o MAM SDK.

  O SDK de Gerenciamento de Aplicativos Móveis (MAM) fornece funcionalidade MDX que não é coberta pelas plataformas iOS e Android. Você pode habilitar MDX e proteger aplicativos iOS ou Android. Você disponibiliza esses aplicativos em uma loja interna ou em lojas de aplicativos públicas. Consulte SDK de Aplicativos MDX.
- StoreFront (opcional). Você pode fornecer acesso a aplicativos baseados em Windows e desktops virtuais do StoreFront através de conexões com o Receiver.
- Citrix Files (opcional). Se você implantar o Citrix Files, poderá habilitar a integração de diretório corporativo por meio do XenMobile, que atua como um provedor de identidade SAML (Security Assertion Markup Language). Para obter mais informações sobre como configurar provedores de identidade para o ShareFile, consulte o site de suporte do ShareFile.

O XenMobile fornece gerenciamento de dispositivos e gerenciamento de aplicativos por meio do console do XenMobile. Esta seção descreve a arquitetura de referência para a implantação do XenMobile.

Em um ambiente de produção, a Citrix recomenda implantar a solução XenMobile em uma configuração de cluster para escalabilidade e redundância de servidor. Além disso, o uso do recurso de descarregamento SSL do Citrix ADC pode reduzir ainda mais a carga no XenMobile Server e aumentar o throughput. Para obter mais informações sobre como configurar o clustering para o XenMobile configurando dois endereços IP virtuais de balanceamento de carga no Citrix ADC, consulte Clustering.

Para obter mais informações sobre como configurar o XenMobile para uma implantação de recuperação de desastres, consulte o artigo do Guia de Implantação Recuperação de Desastres. Esse artigo inclui um diagrama de arquitetura.

As seções a seguir descrevem diferentes arquiteturas de referência para a implantação do XenMobile. Para diagramas de arquitetura de referência, consulte os artigos do Guia de Implantação do XenMobile, Arquitetura de Referência para Implantações Locais e Arquitetura. Para obter uma lista completa de portas, consulte Requisitos de porta (local) e Requisitos de porta (nuvem).

Modo de gerenciamento de dispositivos móveis (MDM)

> **Importante:**
>
> Se você configurar o modo MDM e depois mudar para o modo ENT, certifique-se de usar a mesma autenticação (Active Directory). O XenMobile não oferece suporte à alteração do modo de autenticação após o registro do usuário. Para obter mais informações, consulte Atualizar do XenMobile MDM Edition para o Enterprise Edition.

> O XenMobile MDM Edition fornece gerenciamento de dispositivos móveis. Para suporte de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. Se você planeja usar apenas os recursos MDM do XenMobile, implante o XenMobile no modo MDM. Por exemplo, se você quiser fazer o seguinte.

- Implantar políticas de dispositivo e aplicativos.
- Recuperar inventários de ativos.
- Executar ações em dispositivos, como a limpeza de um dispositivo.

No modelo recomendado, o XenMobile Server é posicionado na DMZ com um Citrix ADC opcional na frente, o que oferece mais proteção para o XenMobile.

Modo de gerenciamento de aplicativos móveis (MAM)

O MAM, também chamado de modo somente MAM, fornece gerenciamento de aplicativos móveis. Para suporte de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. Se você planeja usar apenas os recursos MAM do XenMobile sem que os dispositivos se registrem para MDM, implante o XenMobile no modo MAM. Por exemplo, se você quiser fazer o seguinte.

- Proteger aplicativos e dados em dispositivos móveis BYO.
- Entregar aplicativos móveis corporativos.
- Bloquear os aplicativos e apagar seus dados.

Os dispositivos não podem ser registrados no MDM.

Neste modelo de implantação, o XenMobile Server é posicionado com o Citrix Gateway à frente, o que oferece mais proteção para o XenMobile.

Modo MDM+MAM

O uso conjunto dos modos MDM e MAM oferece gerenciamento de aplicativos e dados móveis e gerenciamento de dispositivos móveis. Para suporte de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. Se você planeja usar os recursos MDM+MAM do XenMobile, implanta o XenMobile no modo ENT (enterprise). Por exemplo, se você quiser:

- Gerenciar um dispositivo corporativo usando MDM
- Implantar políticas e aplicativos de dispositivo
- Recuperar um inventário de ativos
- Apagar dispositivos
- Entregar aplicativos móveis corporativos
- Bloquear aplicativos e apagar os dados nos dispositivos

No modelo de implantação recomendado, o XenMobile Server é posicionado na DMZ com o Citrix Gateway à frente, o que oferece mais proteção para o XenMobile.

XenMobile na rede interna: Outra opção de implantação é posicionar um XenMobile Server local na rede interna, em vez de na DMZ. Essa implantação é usada se sua política de segurança exige que apenas dispositivos de rede possam ser colocados na DMZ. Nesta implantação, o XenMobile Server não está na DMZ. Portanto, não há necessidade de abrir portas no firewall interno para permitir o acesso a servidores SQL Server e PKI a partir da DMZ.

Requisitos do sistema e compatibilidade

Nota:

Este artigo aborda os requisitos do sistema e a compatibilidade para o XenMobile Server 10.16. Para requisitos do sistema para o Endpoint Management, consulte Requisitos do sistema.

Para mais informações sobre requisitos e compatibilidade, consulte os seguintes artigos:

- Compatibilidade do XenMobile
- Sistemas operacionais de dispositivos compatíveis
- Requisitos de porta
- Escalabilidade
- Licenciamento
- Conformidade com FIPS 140-2
- Suporte a idiomas

Para executar o XenMobile 10.16, você precisa dos seguintes requisitos mínimos de sistema:

- Um dos seguintes:
  - Citrix Hypervisor 8.2 CU1 e 8.4; para obter detalhes, consulte XenServer. As versões 8.2 CU1 e posteriores do Citrix Hypervisor não oferecem mais suporte a VMs paravirtualizadas (PV); migre para o modo de virtualização de hardware (HVM) antes de atualizar o XenServer. Consulte Usar imagens HVM nas versões 8.2 CU1 e posteriores do Citrix Hypervisor para obter detalhes. Para obter mais informações sobre a atualização do XenServer, consulte Atualização do XenServer.
  - VMware (versões compatíveis: ESXi 6.0, ESXi 6.5.0 Update 3 ou ESXi 6.7 Update 2 patch 10, ESXi 7.0 Update 3g, ESXi 8.0 Update 2); para obter detalhes, consulte Solução alternativa para ESXi 6.7 e VMware

    - Hyper-V (versões suportadas: Windows Server 2016 e Windows Server 2019); para detalhes, consulte Hyper-V

- Conector do Endpoint Management para Exchange ActiveSync 10.1.10 ou conector do Citrix Gateway para Exchange ActiveSync 8.5.3.19
- Processador dual core
- Quatro CPUs virtuais
- 8 GB de RAM para ambientes de produção; 4 GB de RAM para ambientes de prova de conceito e teste
- 50 GB de espaço em disco
- Citrix License Server 11.16.

  Atualize seu Servidor de Licenças antes de fazer upgrade do seu XenMobile® Server.

Solução alternativa para ESXi 6.7

Para que o ESXi 6.7 funcione, você deve executar a seguinte solução alternativa.

1. Usando a ferramenta OVF fornecida pela VMware, extraia o arquivo OVA baixado de citrix.com. Obtenha a ferramenta OVF na página da VMware (https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491).
2. Dos três arquivos extraídos, carregue o arquivo .vmdk para seu armazenamento de dados.
3. Crie uma nova máquina virtual.
    a. Nomeie a máquina virtual e selecione **máquina virtual ESX/ESXi 4.x** como a opção de compatibilidade.
    b. Para a família do SO Convidado, selecione **Linux**.
    c. Para a versão do SO Convidado, selecione **Other 2.6.x Linux (64-bit)**.
    d. Para o armazenamento de dados, selecione **Default**.
    e. Durante a personalização, remova o disco rígido padrão, o controlador USB e a unidade de CD/DVD.
    f. Em Rede, como tipo de adaptador, selecione **VMXNET3**.
    g. No ESXi, se seus discos forem locais, selecione **SCSI Controller** e **LSI Logic Parallel**. Se você estiver usando um disco compartilhado, selecione **VMware Paravirtual**.
    h. Clique em Próximo para finalizar a criação da VM.

4. navegar para seu armazenamento de dados e copie o arquivo .vmdk que você carregou anteriormente. Copie-o para o diretório da VM que você criou para o XenMobile.
5. Na interface web do ESXi, selecione a VM e edite as configurações.
6. Clique em **Adicionar disco rígido**.
7. Selecione o arquivo .vmdk copiado anteriormente e anexe-o à VM.
8. Clique em **Salvar**.
9. Ligue sua VM.

Requisitos de sistema do Citrix Gateway

Para executar o Citrix Gateway com o XenMobile 10.16, você precisa dos seguintes requisitos mínimos de sistema.

- Citrix Gateway (local). Versões suportadas: 12.1 ou posterior
- Você também deve ser capaz de se comunicar com o Active Directory, o que requer uma conta de serviço. Você só precisa de acesso de consulta e leitura.

Requisitos de banco de dados do XenMobile 10.16

O XenMobile requer um dos seguintes bancos de dados:

- Microsoft SQL Server

  O XenMobile oferece suporte a um banco de dados Microsoft SQL Server executando uma das seguintes versões compatíveis. Para obter mais informações sobre bancos de dados Microsoft SQL Server e seus requisitos de hardware, consulte a documentação da Microsoft.

  - Microsoft SQL Server 2016 SP3
  - Microsoft SQL Server 2017 CU 31
  - Microsoft SQL Server 2019 CU 25
  - Microsoft SQL Server 2022 CU 12

  Os requisitos do seu banco de dados Microsoft SQL Server também dependem do tamanho da sua implantação. Para obter mais informações sobre os requisitos do banco de dados Microsoft SQL Server para o tamanho da sua implantação, consulte Escalabilidade.

  O XenMobile oferece suporte a Grupos de Disponibilidade Básica do SQL (Grupos de Disponibilidade Always On) e Clustering SQL para alta disponibilidade de banco de dados.

A Citrix recomenda usar o Microsoft SQL remotamente.

Para obter informações sobre como atualizar o Microsoft SQL, consulte o artigo da Microsoft Atualizar SQL Server.

- PostgreSQL (somente para ambientes de teste). O PostgreSQL está incluído no XenMobile. Você pode usá-lo localmente ou remotamente em ambientes de teste. A migração de banco de dados não é suportada. Você não pode mover bancos de dados criados em um ambiente de teste para um ambiente de produção.

  Todas as edições do XenMobile oferecem suporte ao PostgreSQL Remoto 9.5.1 e 9.5.11 para Windows com as seguintes limitações: Não recomendado para ambientes de produção. Suporte para até 300 dispositivos. Use o SQL Server local para mais de 300 dispositivos. Sem suporte para clustering.

Requisitos da conta de serviço do SQL Server

Certifique-se de que a conta de serviço do SQL Server a ser usada com o XenMobile tenha a permissão de função `DBcreator`. Registre a senha da conta do SQL Server que você especificar durante a instalação do XenMobile Server. Essa senha é necessária se você precisar clonar o banco de dados do XenMobile durante a recuperação do XenMobile Server.

Proteja seus bancos de dados do SQL Server usando a Criptografia Transparente de Dados (TDE). Não permita acesso externo às portas do SQL Server, conforme mostrado na arquitetura de referência em Arquitetura de Referência para Implantações Locais.

Para obter mais informações sobre as contas de serviço do SQL Server, consulte as seguintes páginas no site de documentação da Microsoft. Esses links apontam para informações do SQL Server 2014. Se você estiver usando uma versão diferente, escolha a versão do seu servidor na lista **Outras Versões**:

- Configurar Contas de Serviço e Permissões do Windows
- Funções de Nível de Servidor

Compatibilidade com Virtual Apps and Desktops

- Aplicativos e Desktops Virtuais 7.15 LTSR CU3
- Aplicativos e Desktops Virtuais 7.1811
- Virtual Apps e Desktops 7 1906
- Virtual Apps e Desktops 7 1909

- Aplicativos e Desktops Virtuais 7 2006

Compatibilidade com StoreFront™

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

Outras compatibilidades

- Conector do Endpoint Management para Exchange ActiveSync 10.1.10
  - Versões mais antigas não são testadas
- Conector do Citrix Gateway para Exchange ActiveSync 8.5.3.19
  - Versões mais antigas não são testadas

Compatibilidade do XenMobile®

> **Nota:**

> Este artigo aborda a compatibilidade do XenMobile Server. Para componentes testados com o Endpoint Management, consulte Compatibilidade do Endpoint Management.

> Para usar os novos recursos, correções e atualizações de política, a Citrix® recomenda que você instale a versão mais recente do seguinte:

- A Citrix recomenda que você integre o SDK de Gerenciamento de Aplicativos Móveis (MAM) com aplicativos iOS e Android corporativos para aplicar os recursos MDX aos aplicativos.

  O MDX Toolkit está programado para atingir o fim da vida útil (EOL) em julho de 2023. Para continuar gerenciando seus aplicativos corporativos, você deve incorporar o SDK MAM.

Este artigo resume as versões dos componentes XenMobile suportados que você pode integrar.

Caminhos de compatibilidade e atualização

As versões mais recentes do Secure Hub, MDX Toolkit e aplicativos de produtividade móvel são compatíveis com a versão atual e anterior do XenMobile Server.

A versão mais recente dos aplicativos de produtividade móvel requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente. Para detalhes, consulte a Matriz de Produtos Citrix.

A Citrix oferece suporte à distribuição de aplicativos de produtividade XenMobile apenas a partir de uma loja de aplicativos pública.

XenMobile Server (local)

- A Citrix oferece suporte a atualizações das duas últimas versões do XenMobile Server.
- Versão mais recente do XenMobile Server: XenMobile Server 10.16
- Atualizar de:
  - XenMobile Server 10.15.x
  - XenMobile Server 10.14.x

Aplicativos de produtividade móvel

Os usuários acessam os aplicativos de produtividade móvel nas lojas de aplicativos públicas. A versão mais recente dos aplicativos de produtividade móvel requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente.

Para obter mais informações sobre a cadência de lançamento faseado de duas semanas dos aplicativos de produtividade móvel, consulte Cronograma de lançamento. Para obter detalhes de suporte, consulte Suporte para aplicativos de produtividade móvel.

MAM SDK

O MAM SDK fornece funcionalidade MDX que não é coberta pelas plataformas iOS e Android. Você disponibiliza esses aplicativos em uma loja interna ou em lojas de aplicativos públicas. Consulte MDX App SDK.

MDX Toolkit

A tecnologia de empacotamento MDX está programada para atingir o fim da vida útil (EOL) em julho de 2023. Para continuar gerenciando seus aplicativos corporativos, você deve incorporar o MAM SDK.

A Citrix oferece suporte às três últimas versões (n.n.n) do MDX Toolkit. Consulte Novidades no MDX Toolkit.

Suporte a navegadores

O console do XenMobile Server requer um dos seguintes navegadores da web compatíveis:

- Versão mais recente do Google Chrome
- Versão mais recente do Mozilla Firefox
- Versão mais recente do Microsoft Edge
- Última versão do Apple Safari

Sistemas operacionais de dispositivos compatíveis

Nota:

Este artigo aborda os sistemas operacionais de dispositivos compatíveis com o XenMobile Server. Para sistemas operacionais compatíveis com o Endpoint Management, consulte Sistemas operacionais de dispositivos compatíveis.

O XenMobile® oferece suporte a dispositivos que executam as seguintes plataformas e sistemas operacionais para gerenciamento de mobilidade empresarial, incluindo gerenciamento de aplicativos e dispositivos. Devido a restrições de plataforma e recursos de segurança, o XenMobile não oferece suporte a todas as funcionalidades em todas as plataformas.

Nota:

O XenMobile Server oferece suporte ao gerenciamento de dispositivos para dispositivos Windows x86 e ARM.

> As informações de plataforma de dispositivo compatíveis neste artigo também se aplicam ao conector XenMobile para Exchange ActiveSync e ao Citrix Gateway connector™ para Exchange ActiveSync.

Para as versões mais recentes dos aplicativos de produtividade móvel e os dispositivos compatíveis com a criptografia MDX, consulte Suporte para aplicativos de produtividade móvel.

> **Nota:**
>
> A Citrix® oferece suporte, no mínimo, à versão atual e à versão anterior de cada plataforma de sistema operacional principal. Nem todos os recursos da versão mais recente do Endpoint Management funcionam em versões de plataforma mais antigas.
>
> Para anúncios de descontinuação, consulte Descontinuação.

Lista de suporte a sistemas operacionais

O Citrix XenMobile oferece suporte aos seguintes sistemas operacionais:

- **Android:** 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, 16.x, 17.x

  Para Android 10 ou posterior, consulte Considerações sobre Android.

- **iOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  Os aplicativos móveis XenMobile e Citrix são compatíveis com iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x e iOS 27.x, mas atualmente não oferecem suporte a todos os novos recursos do iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x e iOS 27.x. Para empacotar aplicativos corporativos internos para iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x e iOS 27.x, use o MDX Toolkit 21.8.5 ou posterior ou prepare os aplicativos usando o MAM SDK.

- **iPadOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  Os aplicativos móveis XenMobile e Citrix são compatíveis com iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, iPadOS 18.x, iPadOS 26.x e iPadOS 27.x, mas atualmente não oferecem suporte a todos os novos recursos do iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, iPadOS 18.x, iPadOS 26.x e iPadOS 27.x.

- **macOS:** 11.x, 12.x, 13.x, 14.x, 15.x

Os aplicativos móveis XenMobile e Citrix são compatíveis com macOS 11, macOS 12, macOS 13, macOS 14 e macOS 15, mas atualmente não oferecem suporte a todos os novos recursos do macOS 11, macOS 12, macOS 13, macOS 14 e macOS 15.

- **Desktops e Tablets Windows:** (somente MDM). Windows 10 e Windows 11

Considerações sobre Android

> **Importante:**
>
> O modo de administração de dispositivo não é mais compatível. Para obter informações, consulte Migrar da administração de dispositivo para o Android Enterprise.

- A Citrix recomenda que você evite registrar dispositivos Android no modo de administração de dispositivo herdado. O Google descontinuou as APIs de Administração de Dispositivo, o que afeta dispositivos que executam Android 10 ou posterior. O registro de dispositivos Android no modo de administração de dispositivo herdado falha. A Citrix não oferece suporte ao registro de dispositivos Android 11 no modo de administração de dispositivo.
- A Citrix recomenda o uso do Android Enterprise para dispositivos Android 10. Para obter mais informações, consulte Migrar da administração de dispositivo para o Android Enterprise.
- A alteração da API do Google não afeta dispositivos registrados no modo somente MAM.

Antes de atualizar:

- Certifique-se de que sua infraestrutura de servidor esteja em conformidade com os certificados de segurança que possuem um nome de host correspondente na extensão subjectAltName (SAN).
- Para verificar um nome de host, o servidor deve apresentar um certificado com um SAN correspondente. A Citrix confia em certificados apenas se eles tiverem um SAN que corresponda ao nome do host.

Requisitos de porta

Para permitir que dispositivos e aplicativos se comuniquem com o XenMobile®, você abre portas específicas em seus firewalls. As tabelas a seguir listam as portas que devem estar abertas.

Abrir portas para Citrix Gateway e XenMobile gerenciarem aplicativos

Abra as seguintes portas para permitir conexões de usuário do Citrix Secure Hub™, Citrix Receiver e do plug-in do Citrix Gateway através do Citrix Gateway para os seguintes componentes:

- XenMobile
- StoreFront™
- Citrix Aplicativos Virtuais e Desktops™
- Conector do Citrix Gateway™ para Exchange ActiveSync
- Outros recursos de rede internos, como sites de intranet

Para habilitar o tráfego para Launch Darkly do Citrix ADC, você pode usar os endereços IP mencionados neste artigo da Central de Conhecimento de Suporte.

Para obter mais informações sobre o Citrix Gateway, consulte a documentação do Citrix Gateway. Essa documentação inclui informações sobre os endereços IP do Citrix ADC (NSIP), IP do servidor virtual (VIP) e IP da sub-rede (SNIP).

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
21 ou 22	Usado para enviar pacotes de suporte para um servidor FTP ou SCP.	XenMobile	Servidor FTP ou SCP
53 (TCP e UDP)	Usado para conexões DNS.	Citrix Gateway, XenMobile	Servidor DNS
80	O Citrix Gateway passa a conexão VPN para o recurso de rede interno através do segundo firewall. Essa situação geralmente ocorre se os usuários fizerem logon com o plug-in do Citrix Gateway.	Citrix Gateway	Sites da intranet

XENMOBILE® SERVER

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
80 ou 8080; 443	Porta XML e Secure Ticket Authority (STA) usada para enumeração, emissão de tíquetes e autenticação. A Citrix recomenda usar a porta 443.	Tráfego de rede XML do StoreFront e Web Interface; STA do Citrix Gateway	Aplicativos Virtuais ou Desktops
123 (TCP e UDP)	Usado para serviços de Network Time Protocol (NTP).	Citrix Gateway; XenMobile	Servidor NTP
389	Usado para conexões LDAP não seguras	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou Microsoft Active Directory
443	Usado para conexões com o StoreFront a partir do Citrix Receiver™ ou Receiver for Web para Aplicativos Virtuais e Desktops.	Internet	Citrix Gateway
443	Usado para conexões com o XenMobile para entrega de aplicativos web, móveis e SaaS.	Internet	Citrix Gateway
443	Usado para comunicação geral de dispositivos com o XenMobile Server.	XenMobile	XenMobile
443	Usado para conexões de dispositivos móveis	Internet	XenMobile

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
	com o XenMobile para registro.		
443	Usado para conexões do XenMobile com o conector do Citrix Gateway para Exchange ActiveSync.	XenMobile	Conector do Citrix Gateway para Exchange ActiveSync
443	Usado para conexões do conector do Citrix Gateway para Exchange ActiveSync com o XenMobile.	Conector do Citrix Gateway para Exchange ActiveSync	XenMobile
443	Usado para URL de retorno de chamada em implantações sem autenticação de certificado.	XenMobile	Citrix Gateway
514	Usado para conexões entre o XenMobile e um servidor syslog.	XenMobile	Servidor syslog
636	Usado para conexões LDAP seguras.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou Active Directory
1494	Usado para conexões ICA® a aplicativos baseados em Windows na rede interna. A Citrix recomenda manter esta porta aberta.	Citrix Gateway	Virtual Apps ou Desktops

XENMOBILE® SERVER

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
1812	Usado para conexões RADIUS.	Citrix Gateway	Servidor de autenticação RADIUS
2598	Usado para conexões a aplicativos baseados em Windows na rede interna usando a confiabilidade da sessão. A Citrix recomenda manter esta porta aberta.	Citrix Gateway	Virtual Apps ou Desktops
3268	Usado para conexões LDAP inseguras do Microsoft Global Catalog.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou Active Directory
3269	Usado para conexões LDAP seguras do Catálogo Global da Microsoft.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou Active Directory
9080	Usado para tráfego HTTP entre o Citrix ADC e o conector do Citrix Gateway para Exchange ActiveSync.	Citrix ADC	Conector do Citrix Gateway para Exchange ActiveSync
30001	API de gerenciamento para preparação inicial do serviço HTTPS	LAN interna	XenMobile Server
9443	Usado para tráfego HTTPS entre o Citrix ADC e o conector do Citrix Gateway para	Citrix ADC	Conector do Citrix Gateway para Exchange ActiveSync

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
	Exchange ActiveSync.		
45000; 80	Usado para comunicação entre duas VMs do XenMobile quando implantadas em um cluster. A porta 80 é para comunicação internós e para descarregamento SSL.	XenMobile	XenMobile
8443	Usado para registro, XenMobile Store e gerenciamento de aplicativos móveis (MAM).	XenMobile; Citrix Gateway; Dispositivos; Internet	XenMobile
4443	Usado para acessar o console do XenMobile por um administrador através do navegador. Também usado para baixar logs e pacotes de suporte para todos os nós do cluster XenMobile a partir de um nó.	Ponto de acesso (navegador); XenMobile	XenMobile
27000	A porta padrão usada para acessar o Citrix License Server externo.	XenMobile	Citrix License Server
7279	A porta padrão usada para verificar	XenMobile	Citrix Vendor Daemon

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
	a entrada e saída de licenças Citrix.		
161	Usado para tráfego SNMP usando o protocolo UDP.	Gerenciador SNMP	XenMobile
162	Usado para enviar alertas de trap SNMP para o gerenciador SNMP do XenMobile. A origem é o XenMobile e o destino é o Gerenciador SNMP.	XenMobile	Gerenciador SNMP

Abrir portas do XenMobile para gerenciar dispositivos

Abra as seguintes portas para permitir que o XenMobile se comunique em sua rede.

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
25	Porta SMTP padrão para o serviço de notificação do XenMobile. Se o seu servidor SMTP usar uma porta diferente, certifique-se de que seu firewall não bloqueie essa porta.	XenMobile	Servidor SMTP
80 e 443	Conexão da Enterprise App Store com a Apple iTunes App Store ou Google Play (deve usar 80). Usado para compra por volume da Apple. Usado para publicar	XenMobile	`ax.apps.apple.com` e `*.mzstatic.com`; `vpp.itunes.apple.com`; `login.live.com`; `*.notify.windows.com`;

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
	aplicativos das lojas de aplicativos do iOS ou Secure Hub para Android.		`play.google.com`, `android.clients.google.com`, `android.l.google.com`
80 ou 443	Usado para conexões de saída entre o XenMobile e o Nexmo SMS Notification Relay.	XenMobile	Servidor de Retransmissão de SMS Nexmo
389	Usado para conexões LDAP inseguras.	XenMobile	Servidor de autenticação LDAP ou Active Directory
443	Usado para registro e configuração de agente para Android.	Internet	XenMobile
443	Usado para registro e configuração de agente para dispositivos Android e Windows e para o Cliente de Suporte Remoto MDM.	Internet LAN e Wi-Fi	XenMobile
1433	Usado por padrão para conexões com um servidor de banco de dados remoto (opcional).	XenMobile	SQL Server
443 ou 2197	Usado para enviar notificações APNs para `*.push.apple.com`	XenMobile	Internet (hosts APNs usando o endereço IP público 17.0.0.0/8
5223	Usado para conexões de saída APNs de dispositivos	Dispositivos iOS	Internet (hosts APNs usando o endereço IP público 17.0.0.0/8)

PORTA TCP	DESCRIÇÃO	ORIGEM	DESTINO
	iOS para `*.push.apple.com` .		
8081	Usado para túneis de aplicativos do Cliente de Suporte Remoto MDM opcional. O padrão é 8081.	Cliente de Suporte Remoto	XenMobile
8443	Usado para o registro de dispositivos iOS.	Internet; LAN e Wi-Fi	XenMobile

Requisito de porta para conectividade do serviço AutoDiscovery

Esta configuração de porta garante que os dispositivos Android que se conectam do Secure Hub para Android possam acessar o Serviço de Descoberta Automática da Citrix (ADS) de dentro da rede interna. Você precisa de acesso ao ADS para baixar as atualizações de segurança disponibilizadas por meio do ADS.

> **Nota:**

> As conexões ADS podem não oferecer suporte ao seu servidor proxy. Nesse cenário, permita que a conexão ADS ignore o servidor proxy.

> Se você quiser habilitar a fixação de certificado, faça os seguintes pré-requisitos:

- **Colete os certificados do XenMobile Server e do Citrix ADC.** Os certificados devem estar no formato PEM e devem ser um certificado público, não a chave privada.
- **Entre em contato com o Suporte Citrix e faça uma solicitação para habilitar a fixação de certificado.** Durante esse processo, você será solicitado a fornecer seus certificados.

A fixação de certificado exige que os dispositivos se conectem ao ADS antes que o dispositivo seja registrado. Esse requisito garante que as informações de segurança mais recentes estejam disponíveis para o Secure Hub. Para que o Secure Hub registre um dispositivo, o dispositivo deve

alcançar o ADS. Portanto, abrir o acesso ao ADS dentro da rede interna é fundamental para permitir que os dispositivos sejam registrados.

Para permitir o acesso ao ADS para o Secure Hub para Android ou iOS, abra a porta 443 para o seguinte FQDN:

FQDN	PORTA	USO DE IP E PORTA
`discovery.cem.cloud.us`	443	Secure Hub - Comunicação ADS via CloudFront

Para obter informações sobre os endereços IP suportados, consulte Centros de armazenamento baseados em nuvem da AWS.

Requisitos de rede do Android Enterprise

Para obter informações sobre as conexões de saída a serem consideradas ao configurar ambientes de rede para o Android Enterprise, consulte o artigo de suporte do Google, Requisitos de Rede do Android Enterprise.

Requisitos de porta para XenMobile

Os seguintes hosts de destino devem estar acessíveis a partir da rede para criar um Managed Google Play Enterprise e para acessar o Managed Google Play iFrame. O Google disponibilizou o Managed Play iFrame para desenvolvedores EMM para simplificar a pesquisa e aprovação de aplicativos. Para usar o Managed Play iFrame, o navegador a partir do qual você acessa o console do XenMobile deve ter acesso ao Google Play.

HOST DE DESTINO	PORTA	DESCRIÇÃO
`play.google.com`	TCP/443	Usado para Google Play Store, inscrição no Play Enterprise
`*.googleapis.com`	TCP/443	Usado para Google Mobile Management, APIs do Google, APIs da Google Play Store, FCM
`accounts.youtube.com`, `accounts.google.com`	TCP/443	Usado para a autenticação da conta

XENMOBILE® SERVER

HOST DE DESTINO	PORTA	DESCRIÇÃO
`apis.google.com`	TCP/443	Usado para serviços web do Google
`ogs.google.com`	TCP/443	Usado para elementos da interface do usuário iFrame
`notifications.google.com`	TCP/443	Usado para notificações de desktop e móveis
`fonts.googleapis.com`, `*.gstatic.com`, `*.googleusercontent.com`	TCP/443	Usado para conteúdo gerado pelo usuário do Google Fonts. Por exemplo, os ícones de aplicativos na loja
`cri.pki.goog`, `ocsp.pki.goog`	TCP/443	Usado para a validação do certificado

Escalabilidade e desempenho

Compreender a escala da sua infraestrutura XenMobile® desempenha um papel significativo na forma como você decide implantar e configurar o XenMobile. Este artigo contém os dados de testes de escalabilidade e orientação sobre como determinar os requisitos de infraestrutura para desempenho e escalabilidade para implantações empresariais XenMobile locais de pequena a grande escala.

A escalabilidade é definida aqui como a capacidade de dispositivos já inscritos na implantação de se reconectarem à implantação ao mesmo tempo.

- *Escalabilidade* é definida como o número máximo de dispositivos inscritos na implantação.
- *Taxa de Login* é definida como a taxa máxima na qual os dispositivos existentes podem se reconectar à implantação.

Os dados neste artigo são derivados de testes em implantações que variam em tamanho de 10.000 a 75.000 dispositivos. Os testes incluíram dispositivos móveis usando cargas de trabalho conhecidas.

Todos os testes foram realizados no XenMobile Advanced Edition (local) ou no Citrix Endpoint Management™ (nuvem).

Os testes foram realizados usando o Citrix Gateway 8200. Espera-se que um appliance Citrix ADC com capacidade semelhante ou superior produza escalabilidade e desempenho semelhantes ou superiores.

Um resumo dos resultados dos testes de escalabilidade segue.

Resumo dos resultados dos testes de escalabilidade para implantações de até 75.000 dispositivos

Taxa de login (taxa de reconexão de usuários existentes) — até 9.375 dispositivos por hora

Configuração utilizada:

- Citrix Gateway
- MPX 8200
- XenMobile Advanced Edition (local) ou Citrix Endpoint Management (nuvem)
- Cluster de 7 nós do XenMobile Server
- Banco de dados: Banco de dados externo do Microsoft SQL Server

Resultados do teste por população de dispositivos e configuração de hardware

NÚMERO DE DISPOSITIVOS	12.500	30.000	60.000	75.000
Taxa de reconexão de dispositivos existentes por hora	1.250	3.750	7.500	9.375
XenMobile Server – modo	Autônomo	Cluster	Cluster	Cluster
XenMobile Server – agrupamento	N/A	3	5	7
XenMobile Server –	Memória = 8 GB RAM; vCPUs = 4	Memória = 16 GB RAM; vCPUs = 6	Memória = 24 GB RAM; vCPUs = 8	Memória = 24 GB RAM; vCPUs = 8

NÚMERO DE DISPOSITIVOS	12.500	30.000	60.000	75.000
appliance virtual				
Active Directory	Memória = 4 GB RAM; vCPUs = 2	Memória = 8 GB RAM; vCPUs = 4	Memória = 16 GB RAM; vCPUs = 4	Memória = 16 GB RAM; vCPUs = 4
Banco de dados externo do Microsoft SQL Server	Memória = 8 GB RAM; vCPUs = 4	Memória = 16 GB RAM; vCPUs = 8	Memória = 24 GB RAM; vCPUs = 16	Memória = 24 GB RAM; vCPUs = 16

Perfil de escalabilidade

CONFIGURAÇÃO DO ACTIVE DIRECTORY	PERFIL USADO
Usuários	100.000
Grupos	200.000
Níveis de aninhamento	5

CONFIGURAÇÃO DO SERVIDOR XENMOBILE	TOTAL	POR USUÁRIO
Políticas	20	20
Aplicativos	270	50
Aplicativo público	200	0
MDX	50	30
Web e SaaS	20	20
Ações	50	
Grupos de entrega	20	

CONFIGURAÇÃO DO SERVIDOR XENMOBILE	TOTAL	POR USUÁRIO
Grupos do Active Directory por grupo de entrega	10	
SQL		
Número de bancos de dados	1	

Conexões de dispositivos e atividades de aplicativos

Este teste de escalabilidade coletou dados sobre a capacidade de dispositivos inscritos em uma implantação de se reconectarem durante um período de 8 horas.

Os testes simularam um intervalo de reconexão durante o qual os dispositivos que se reconectam obtêm todas as políticas de segurança autorizadas, sujeitando os nós do XenMobile Server a condições de carga mais altas do que o normal. Durante as reconexões subsequentes, apenas políticas alteradas ou novas são enviadas para dispositivos iOS, diminuindo a carga nos nós do XenMobile Server.

Esses testes usaram uma mistura de 50% de dispositivos iOS e 50% de dispositivos Android.

Esses testes assumem que os dispositivos Android que se reconectam receberam notificações GCM anteriores.

Durante o intervalo de teste de 8 horas, as seguintes atividades relacionadas a aplicativos ocorreram:

- O Secure Hub foi aberto uma vez para enumerar os aplicativos autorizados
- 2 aplicativos web SAML foram abertos
- 4 aplicativos MAM foram baixados
- 1 STA foi gerado para uso pelo Secure Mail
- 240 validações de ticket STA, uma para cada evento de reconexão do Secure Mail por meio de uma micro VPN, foram realizadas.

Arquitetura de referência

Para a arquitetura de referência para implantações usadas nestes testes de escalabilidade, consulte "Arquitetura de Referência Core MAM+MDM" em Arquitetura de Referência para Implantações Locais.

Ressalvas e limitações

Observe o seguinte ao considerar os resultados do teste de escalabilidade neste artigo:

- A plataforma Windows não foi testada.
- O envio de políticas foi testado para dispositivos iOS e Android.
- Cada nó do XenMobile Server suporta um máximo de 12.000 dispositivos simultaneamente.

Licenciamento

O XenMobile Server agora oferece suporte ao mecanismo de licenciamento do Serviço de Ativação de Licenças (LAS). O LAS é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa moderna ao licenciamento tradicional baseado em arquivo em todo o conjunto de produtos Citrix. Registre seu Citrix License Server com o Citrix Cloud para usar as licenças e direitos que seu Serviço de Ativação de Licenças possui. Para obter mais informações, consulte Serviço de Ativação de Licenças.

> **Importante:**
>
> - Adote o novo modelo de licenciamento até April 15, 2026. Para obter mais informações, consulte Anúncio de Licenciamento Moderno da Citrix.
> - O processo para devolver e modificar licenças Citrix® mudou a partir de November 4, 2020. Para obter mais informações, consulte os seguintes artigos:
>   - Como Devolver uma Licença usando Minha Conta
>   - Como Realocar um Arquivo de Licença

> O XenMobile® usa o Citrix Licensing para gerenciar licenças. O XenMobile Server e o Citrix Gateway exigem licenças.

Para obter mais informações sobre o licenciamento do Citrix Gateway, consulte a documentação do Citrix Gateway. Para obter mais informações sobre o Citrix Licensing, consulte O Sistema de Licenciamento Citrix.

Ao adquirir o XenMobile Server, você recebe uma mensagem de e-mail de confirmação de pedido contendo instruções para ativar sua licença. Novos clientes devem se registrar em um programa

de licença antes de fazer um pedido. Para obter mais informações sobre os modelos e programas de licenciamento do XenMobile, consulte Licenciamento do XenMobile.

Requisitos

- Atualize seu Citrix License Server para 11.16.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server. Versões mais antigas do servidor de licenças não oferecem suporte à versão mais recente do XenMobile.
- Você deve instalar o Citrix Licensing antes de baixar suas licenças do XenMobile. O nome do servidor no qual você instalou o Citrix Licensing é necessário para gerar o arquivo de licença. Ao instalar o XenMobile, o Citrix Licensing é instalado no servidor por padrão. Alternativamente, você pode usar uma implantação existente do Citrix Licensing para gerenciar suas licenças do XenMobile. Para obter mais informações sobre como instalar, implantar e gerenciar o Citrix Licensing, consulte Licenciando seu Produto.
- Se você pretende agrupar nós, ou instâncias, do XenMobile, deve usar o Citrix Licensing em um servidor remoto.
- A Citrix recomenda que você mantenha cópias locais de todos os arquivos de licença que receber. Ao salvar uma cópia de backup do arquivo de configuração, todos os arquivos de licença são incluídos no backup. Se, no entanto, você reinstalar o XenMobile sem primeiro fazer backup do arquivo de configuração, precisará dos arquivos de licença originais.

Considerações sobre licenciamento do XenMobile

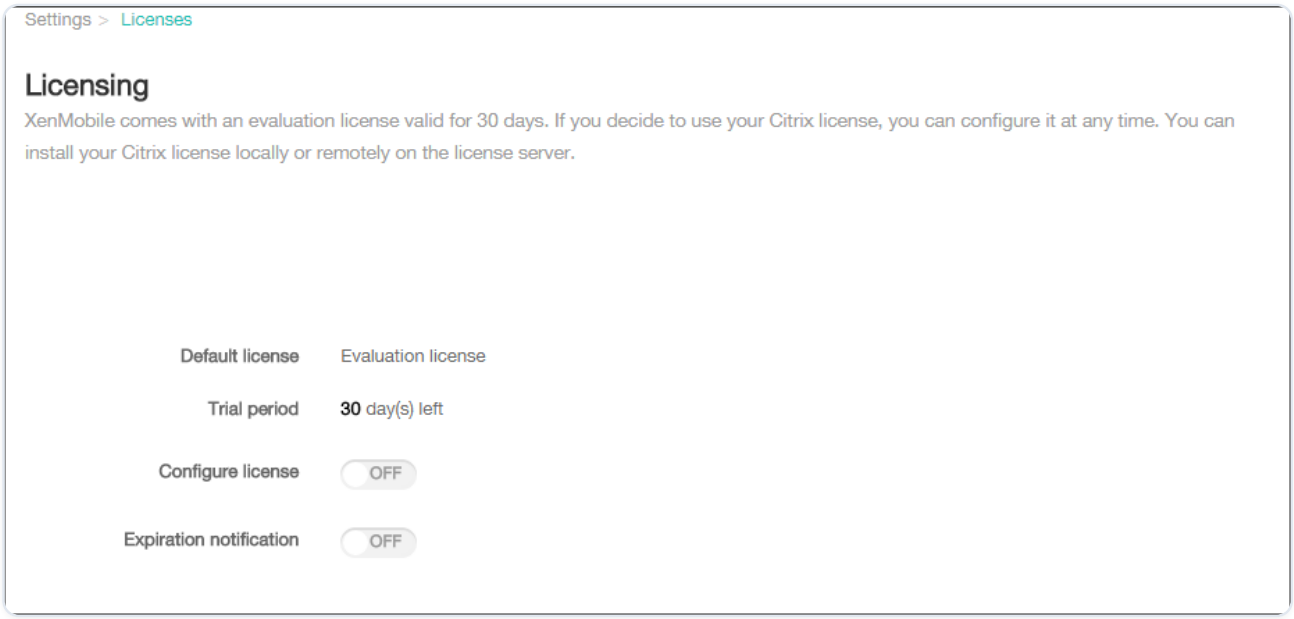
Na ausência de uma licença, o XenMobile opera com todos os recursos no modo de avaliação por um período de carência de 30 dias. Este modo de avaliação pode ser usado apenas uma vez, com o período de 30 dias começando quando você instala o XenMobile. O acesso ao console web do XenMobile nunca é bloqueado, independentemente de uma licença XenMobile válida estar disponível ou não. No console do XenMobile, você pode ver quantos dias restam no seu período de avaliação.

Embora o XenMobile permita fazer upload de várias licenças, apenas uma licença pode ser ativada por vez.

Quando uma licença do XenMobile expira, você não pode mais realizar nenhuma função de gerenciamento de dispositivos. Por exemplo, novos usuários ou dispositivos não podem ser registrados, e aplicativos e configurações implantados em dispositivos registrados não podem ser atualizados. Para obter mais informações sobre modelos e programas de licenciamento do XenMobile, consulte Licenciamento do XenMobile.

Para encontrar a página de Licenciamento no console do XenMobile

Quando a página **Licenciamento** aparece pela primeira vez após a instalação do XenMobile, a licença é definida para o modo de avaliação padrão de 30 dias e ainda não está configurada. Você pode adicionar e configurar licenças nesta página.



1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Licenciamento**. A página **Licenciamento** é exibida.

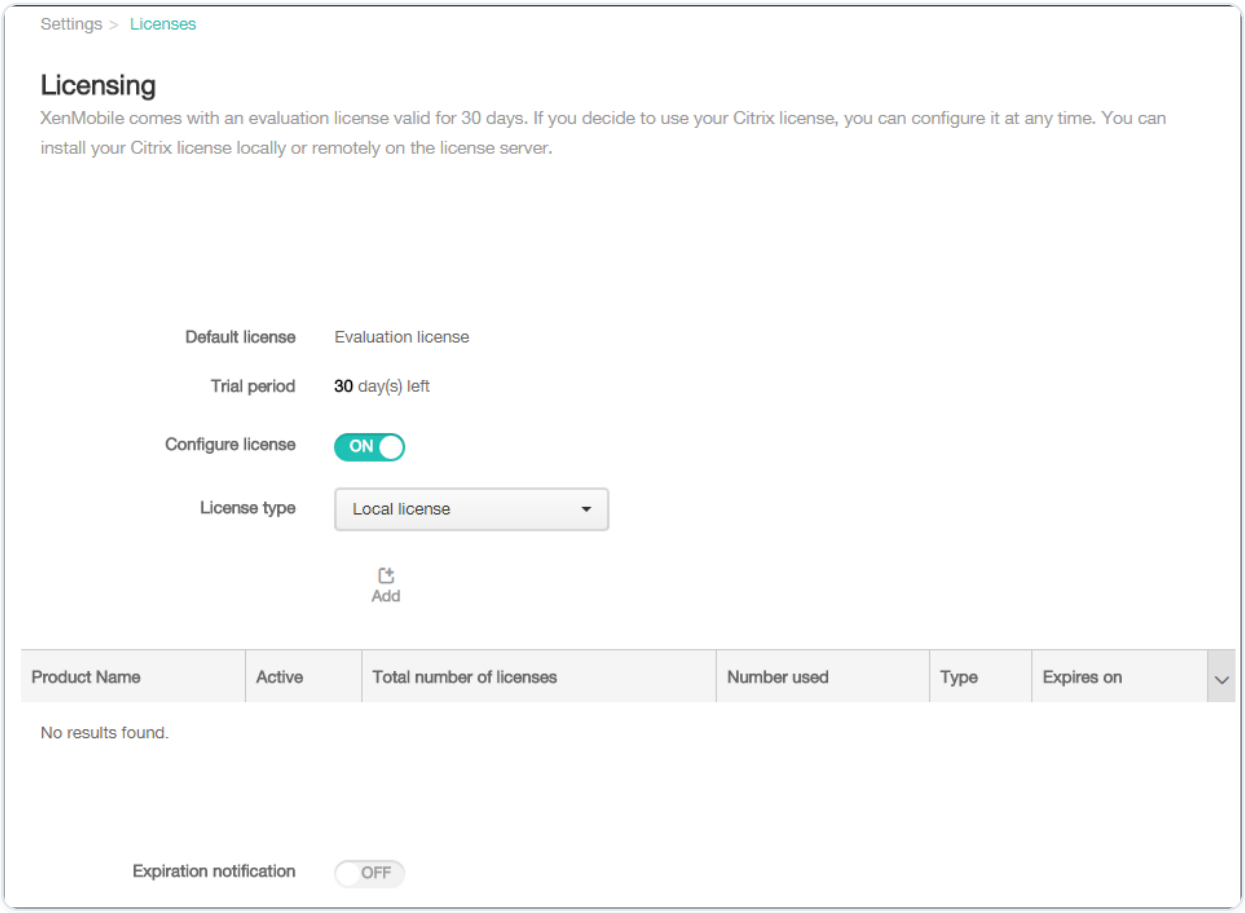
Para adicionar uma licença local

Ao adicionar novas licenças, elas aparecem na tabela. A primeira licença adicionada é ativada automaticamente. Se você adicionar várias licenças da mesma categoria, como Enterprise e tipo, essas licenças aparecerão em uma única linha da tabela. Nesses casos, o **Número total de licenças** e o **Número usado** refletem a quantidade combinada para as licenças comuns. A data de **Expira em** mostra a data de expiração mais recente entre as licenças comuns.

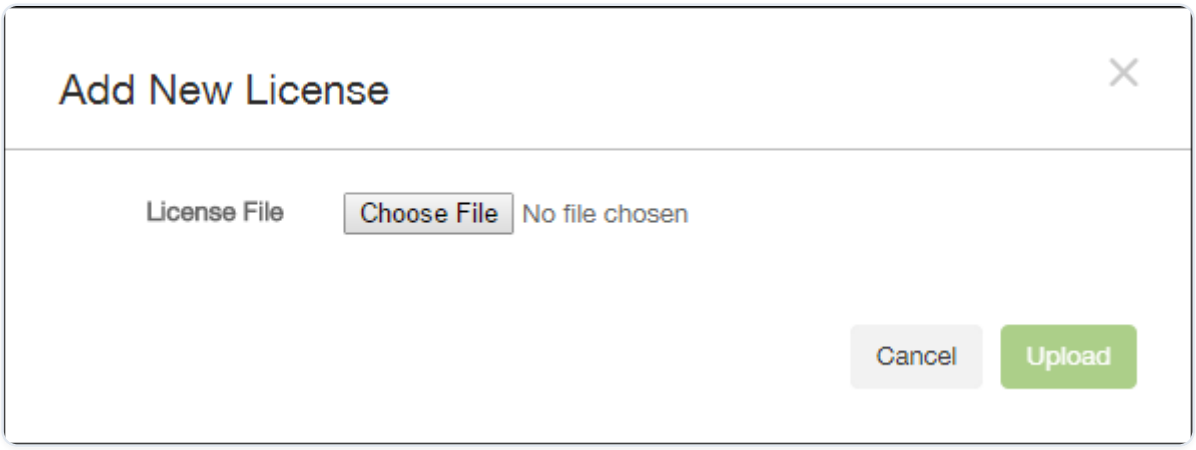
Você gerencia todas as licenças locais através do console do XenMobile.

1. Obtenha um arquivo de licença do Simple License Service, através do License Administration Console ou diretamente da sua conta em Citrix.com. Para obter detalhes, consulte a documentação de Licenciamento da Citrix.
2. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
3. Clique em **Licenciamento**. A página **Licenciamento** é exibida.

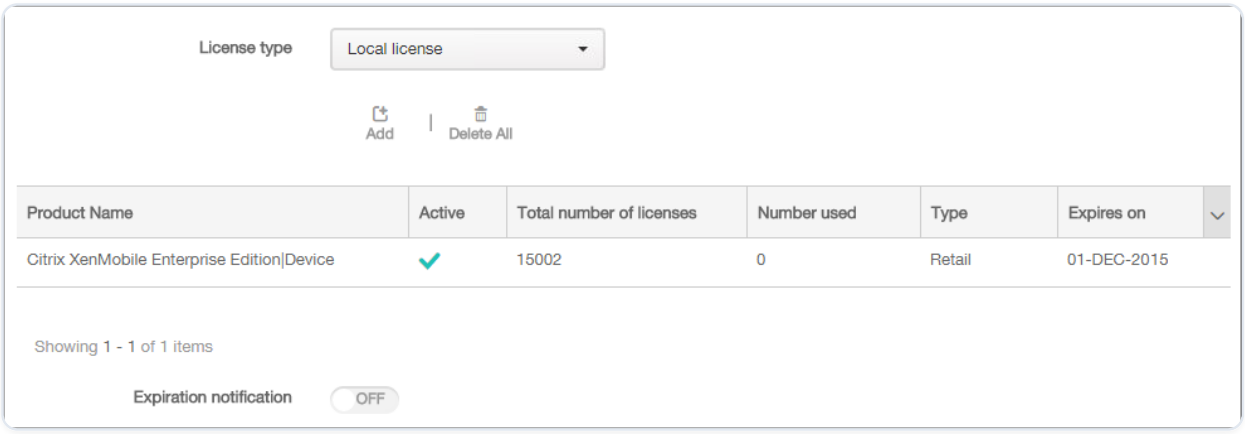
4. Defina **Configurar licença** como **Ativado**. A lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento** são exibidos. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não adicionou uma licença Citrix, a tabela estará vazia.



5. Certifique-se de que **Tipo de licença** esteja definido como **Licença local** e clique em **Adicionar**. A caixa de diálogo **Adicionar Nova Licença** é exibida.



6. Na caixa de diálogo **Adicionar Nova Licença**, clique em **Escolher Arquivo** e navegue até o local do seu arquivo de licença.
7. Clique em **Carregar**. A licença é carregada localmente e aparece na tabela.



8. Quando a licença aparecer na tabela na página **Licenciamento**, ative-a. Se a licença for a primeira na tabela, ela será ativada automaticamente.

Para adicionar uma licença remota

Se você estiver usando o servidor de Licenciamento Citrix remoto, você usa o servidor de Licenciamento Citrix para gerenciar *toda* a atividade de licenciamento. Para obter detalhes, consulte Licenciando seu produto.

1. Importe o certificado do servidor de licenças para o XenMobile Server (**Configurações > Certificados**).
2. Por padrão, a verificação de nome de host está habilitada em conexões de saída, exceto para o servidor PKI da Microsoft. Se a verificação de nome de host interromper sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **true**. O valor padrão desta propriedade é **false**.

   Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar ao servidor de compra por volume: O nome do host '192.0.2.0' não corresponde ao assunto do certificado fornecido pelo par”
3. Na página **Licenciamento**, defina **Configurar licença** como **Ativado**. A lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento** são exibidos. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não adicionou uma licença Citrix, a tabela estará vazia.
4. Defina **Tipo de licença** como **Licença remota**. Os campos **Servidor de licenças** e **Porta** e o botão **Testar Conexão** substituem o botão **Adicionar**.



5. Configure estas definições:

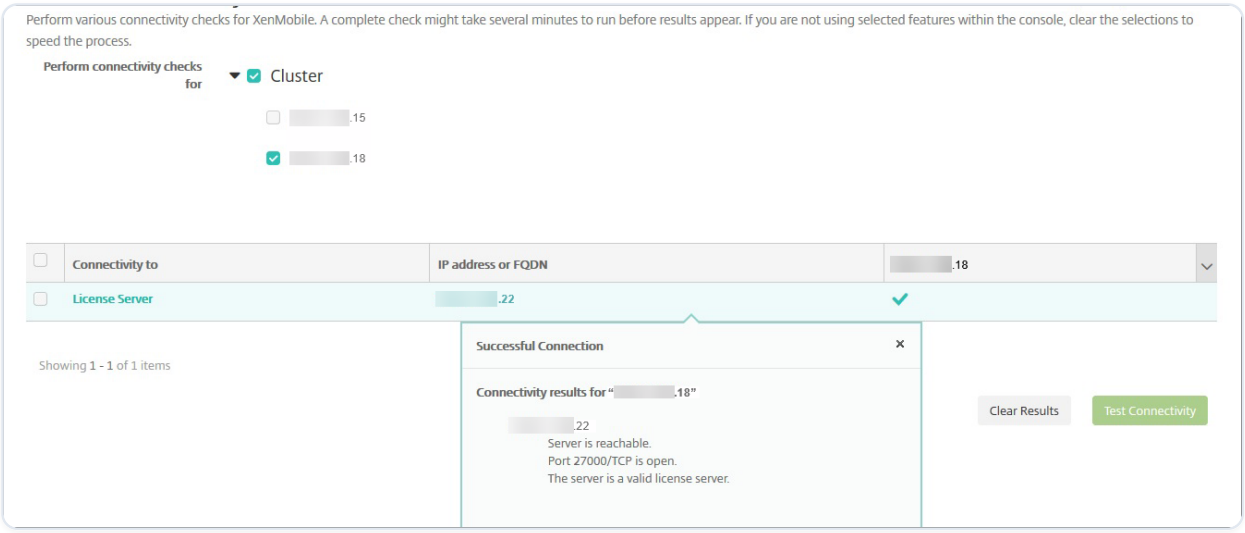
   - **Servidor de licenças:** Digite o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do seu servidor de licenciamento remoto.
   - **Porta:** Aceite a porta padrão ou digite o número da porta usado para se comunicar com o servidor de licenciamento.

6. Clique em **Testar Conexão**. Se a conexão for bem-sucedida, o XenMobile se conectará ao servidor de Licenciamento e a tabela de Licenciamento será preenchida com as licenças disponíveis. Se houver apenas uma licença, ela será ativada automaticamente.

   Ao clicar em **Testar Conexão**, o XenMobile confirma o seguinte:

   - O XenMobile pode se comunicar com o servidor de licenças.
   - As licenças no servidor de licenças são válidas.
   - O servidor de licenças é compatível com o XenMobile.

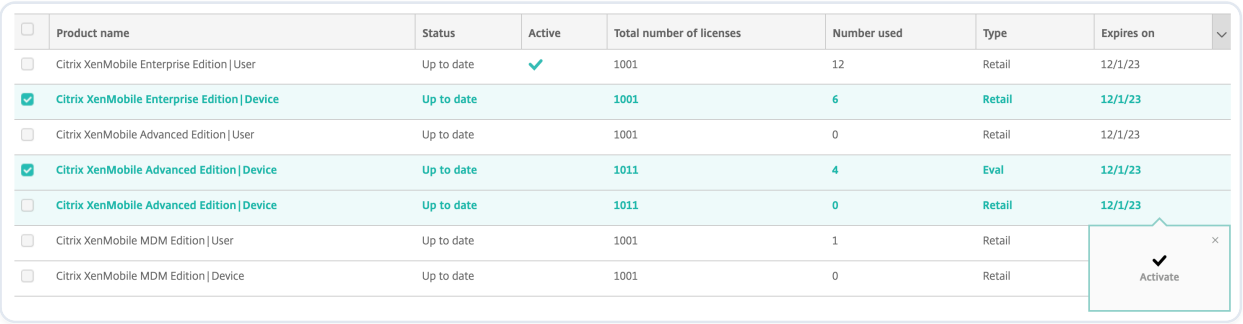
   Se a conexão não for bem-sucedida, revise a mensagem de erro exibida, faça as correções necessárias e clique em **Testar Conexão**.



Para ativar uma licença diferente

Se você tiver várias licenças, poderá escolher as licenças que deseja ativar.

1. Na página **Licenciamento**, na **tabela de Licenciamento**, selecione as licenças que deseja ativar. Clique em qualquer linha da lista; a caixa de diálogo **Ativar** será exibida.



2. Clique em **Ativar**.
3. Quando você vir uma marca de seleção na linha **Ativo** para as licenças, clique em **Salvar**.

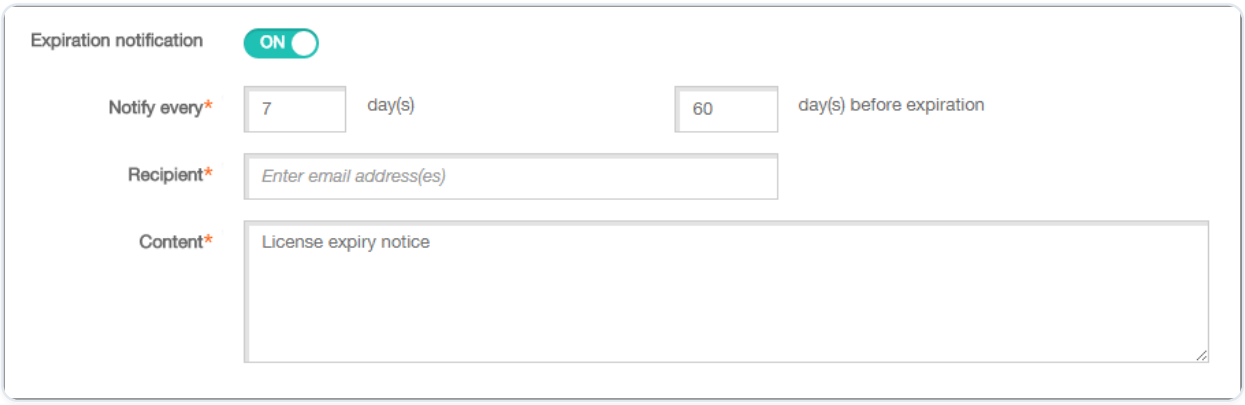
Importante:

- A licença por **Usuário** e a licença por **Dispositivo** são mutuamente exclusivas e não podem ser ativadas simultaneamente.
- Somente as licenças ADV Edition e ENT Edition podem ser misturadas. As licenças MDM Edition não podem ser misturadas com as licenças ADV Edition ou ENT Edition.
- Certifique-se de que os arquivos de licença da mesma edição tenham o mesmo status. Por exemplo, se um arquivo da edição ADV for ativado, os demais arquivos ADV serão ativados automaticamente.
- Para versões anteriores ao XenMobile Server 10.15 Rolling Patch 3, você pode ter apenas uma licença ativa por vez. Ao ativar a licença selecionada, a licença atualmente ativa é desativada.

Para automatizar uma notificação de expiração

Depois de ativar licenças remotas ou locais, você pode configurar o XenMobile para notificar você ou um designado quando a data de expiração da licença se aproximar.

1. Na página **Licenciamento**, defina **Notificação de expiração** como **Ativado**. Novos campos relacionados à notificação aparecem.



2. Configure estas configurações:

   - **Notificar a cada:** Digite:
   - A frequência com que as notificações são enviadas, como a cada **7** dias.
   - Quando começar a enviar a notificação, como 60 dias antes da expiração da licença.
   - **Destinatário:** Digite seu endereço de e-mail ou o endereço de e-mail da pessoa responsável pela licença.
   - **Conteúdo:** Digite uma mensagem de notificação de expiração que o destinatário vê na notificação.

3. Clique em **Salvar**. Com base em suas configurações, o XenMobile começa a enviar mensagens de e-mail que contêm o texto digitado em **Conteúdo** para o destinatário digitado em **Destinatário**. As notificações são enviadas com a frequência que você definiu.

Serviço de Ativação de Licenças

> **Importante:**

> Estamos fazendo a transição para uma arquitetura de licenciamento baseada em nuvem e padrão da indústria para a plataforma Citrix. Essa mudança automatiza o direito e a ativação, trazendo os seguintes benefícios importantes para o cliente:

> - **Sem gerenciamento de arquivos de licença:** Elimina a necessidade de baixar, alocar ou gerenciar arquivos de licença, simplificando suas tarefas administrativas.
> - **Atualizações automáticas de direitos:** Os direitos são atualizados automaticamente em segundo plano após a renovação do contrato, garantindo um serviço ininterrupto.

- **Maior resiliência:** O Servidor de Licenças não é mais um único ponto de falha para as sessões de usuário, aumentando a estabilidade do seu ambiente.

Nós o encorajamos a usar o tempo que antecede a mudança para planejar e executar sua transição para adotar o novo modelo de licenciamento até April 15, 2026, e estamos comprometidos em apoiá-lo em cada etapa do processo. Para obter mais informações, consulte Anúncio de Licenciamento Moderno da Citrix.

O Serviço de Ativação de Licenças (LAS) é uma nova solução de licenciamento baseada em nuvem que oferece uma alternativa ao licenciamento legado tradicional da Citrix. O LAS introduz novos módulos para ativação, garantindo uma abordagem moderna e contínua para o gerenciamento de licenças.

O LAS simplifica a experiência de Licenciamento Citrix. Não há mais códigos de acesso ou arquivos de licença para gerar, baixar ou instalar no servidor de licenças. Você só precisa atualizar seu servidor de licenças e se registrar no Citrix Cloud. Uma vez que os produtos compatíveis são apontados para o servidor de licenças, eles podem ser ativados automaticamente.

Após a ativação, o Servidor de Licenças se comunica regularmente com o Serviço de Ativação de Licenças para manter sua ativação atualizada. O LAS é construído com tecnologia de nuvem, o que melhora o desempenho e garante que não haja tempo de inatividade. Se, por qualquer motivo, o Servidor de Licenças ou o LAS estiver inacessível, o sistema entra no modo de cache de licenças, que é projetado para proteger o sistema de ficar sem licença e evitar uma interrupção. Para obter mais informações, consulte Modo de cache de licenças.

Para servidores de licença que não podem se conectar à nuvem, o LAS também oferece uma opção de ativação offline, garantindo flexibilidade para vários ambientes de rede. Este serviço introduz uma abordagem contínua e moderna para gerenciar suas licenças de produtos Citrix.

Para mais detalhes sobre o LAS, consulte a documentação de Licenciamento Serviço de Ativação de Licenças.

Compatibilidade do LAS

As versões mínimas necessárias do XenMobile Server que são compatíveis com o LAS são:

- 10.16 Rolling Patch 7
- 10.15 Rolling Patch 13

> **Observação:**
>
> Em April 15, 2026, o licenciamento herdado baseado em arquivo deixará de funcionar. Implantações que usam os mecanismos de licenciamento herdados baseados em arquivo terão impactos para o usuário final.

Pré-requisitos

- Instale ou atualize o License Server para a versão 11.17.2 build 51000 ou posterior.
- Uma conta do Citrix Cloud com o OrgID associado aos seus direitos do XenMobile Server.
- Configurar o License Server para Ativação Online.

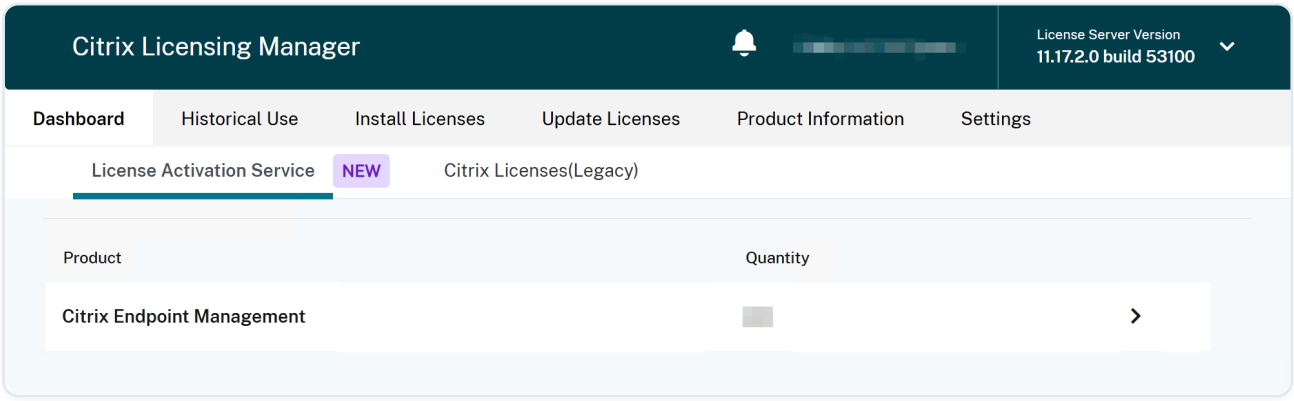
Configurar o Serviço de Ativação de Licença

Etapa 1: Instalar ou atualizar o License Server

Instale ou atualize o License Server para a versão 11.17.2 build 51000 ou posterior. Você pode baixar o Citrix License Server para Windows na página de downloads de licenciamento da Citrix.

Etapa 2: Configurar o LAS

Configure o LAS conforme as instruções mencionadas em Como Configurar o License Server para o Serviço de Ativação de Licença, certifique-se de que o direito do XenMobile Server esteja incluído na sua Conta de Cliente do Citrix Cloud que foi usada na integração do License Server.



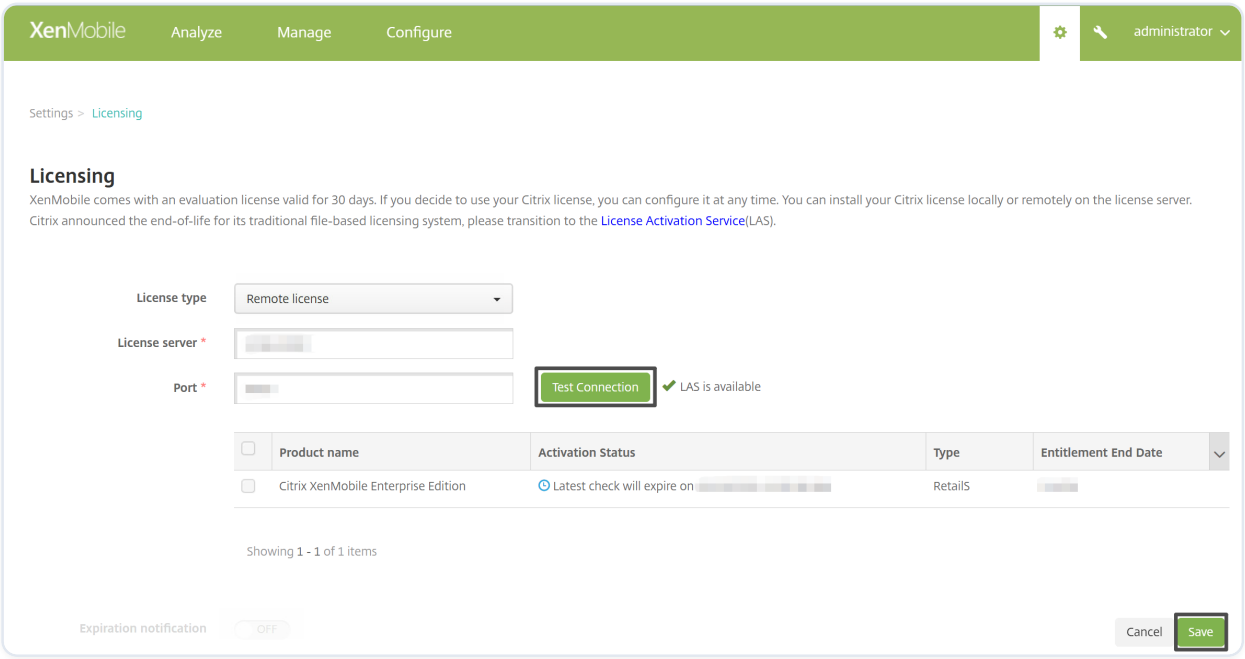
Etapa 3: Atualizar o XenMobile Server

Atualize o XenMobile Server para uma versão compatível com LAS. As versões mínimas necessárias do XenMobile Server são:

- 10.16 Rolling Patch 7
- 10.15 Rolling Patch 13

Passo 4: Configurar o XenMobile Server para usar o LAS

1. Faça login no console do XenMobile Server e navegar para **Settings > Licensing**.
2. Defina **License Type** como **Remote License**.
3. Configure **License server** e **Port**:
   - **License server:** Digite o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do seu servidor de licenciamento remoto.
   - **Port:** Aceite a porta padrão (8083 para LAS) ou digite o número da porta personalizada usada para se comunicar com o servidor de licenciamento LAS.
4. Clique em **Test Connection**. Se a conexão for bem-sucedida, isso indica que o LAS está disponível e a tabela de Licenciamento é preenchida com as licenças disponíveis; certifique-se de que o Status de Ativação esteja íntegro, sem erros.



5. Clique em **Save**. As configurações são salvas e o XenMobile Server passa a usar o Serviço de Ativação de Licença.

Solução de problemas

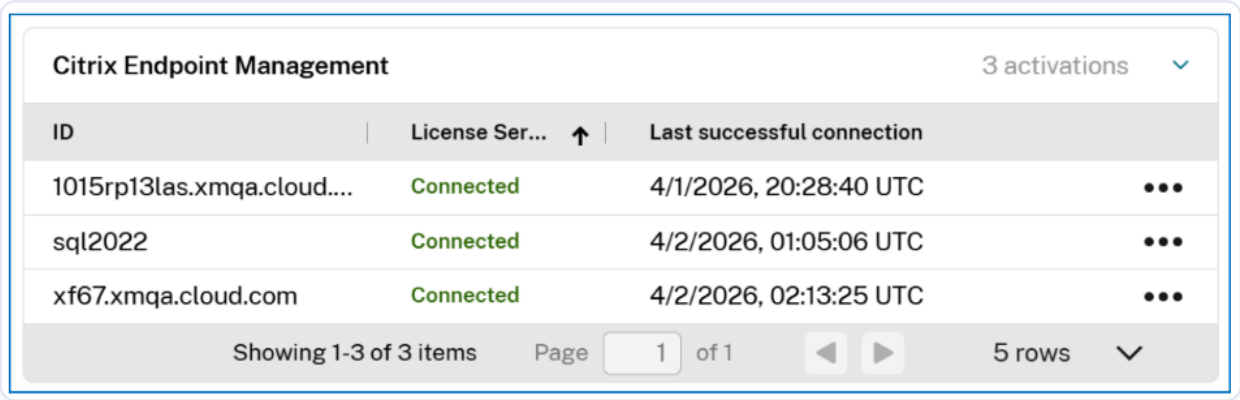
Se o status do servidor de licenças não estiver verde, siga estas etapas para visualizar os detalhes de ativação e solucionar quaisquer problemas.

Para verificar os detalhes de ativação do XenMobile Server no Citrix Cloud, execute as seguintes etapas:

1. navegar para **Licensing** > **Licensed Deployments** > **License Servers**.

2. Encontre o servidor de licenças usado pelo XenMobile Server e, em seguida, clique em **Exibir detalhes**.
3. Na página de detalhes do servidor de licenças, expanda **Citrix Endpoint Management** para ver a lista de ativações.

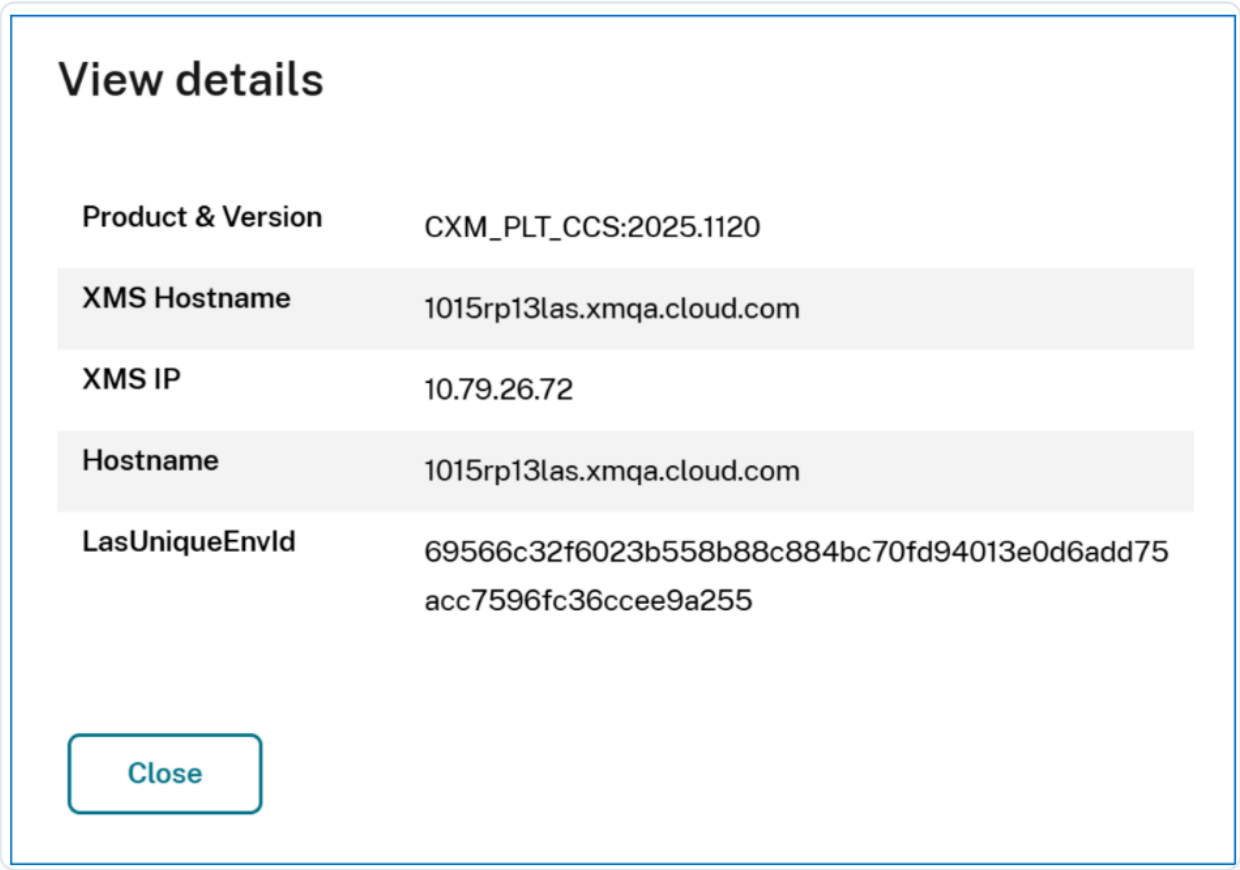
   O **ID** mostrado para cada ativação é o nome do host do XenMobile Server.



4. Clique em **Exibir detalhes** para a ativação necessária.

   A página de detalhes mostra as seguintes informações:

   - **Nome do host XMS:** Nome do host do XenMobile Server.
   - **IP do XMS:** Endereço IP do XenMobile Server.
   - **Nome do host:** Nome do host do XenMobile Server.



Conformidade com FIPS 140-2

O Federal Information Processing Standard (FIPS) é emitido pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST). O FIPS especifica os requisitos de segurança para módulos criptográficos usados em sistemas de segurança. O FIPS 140-2 é a segunda versão desse padrão. Para obter mais informações sobre os módulos FIPS 140 validados pelo NIST, consulte o NIST Computer Security Resource Center.

Importante:

- Você pode habilitar o modo FIPS do XenMobile® somente durante a instalação inicial.
- Somente o gerenciamento de dispositivos móveis do XenMobile, somente o gerenciamento de aplicativos móveis do XenMobile e o XenMobile MDM+MAM são todos compatíveis com FIPS se nenhum aplicativo HDX™ for usado.

Todas as operações criptográficas de dados em repouso e dados em trânsito no iOS usam módulos criptográficos validados por FIPS fornecidos pela Citrix® e Apple. No Android, todas as operações criptográficas de dados em repouso usam módulos criptográficos validados

> por FIPS fornecidos pelos módulos criptográficos da plataforma fornecidos pelo fabricante do dispositivo. Entre em contato com seu representante Citrix para obter mais informações sobre os módulos do fabricante do dispositivo.

Todas as operações criptográficas de dados em repouso e dados em trânsito para Gerenciamento de Dispositivos Móveis (MDM) em dispositivos Windows compatíveis usam módulos criptográficos validados por FIPS.

Todas as operações criptográficas de dados em repouso e dados em trânsito para o XenMobile MDM usam módulos criptográficos validados por FIPS. Todos os dados em repouso e dados em trânsito para fluxos MDM usam módulos criptográficos compatíveis com FIPS de ponta a ponta. Essa segurança inclui as operações criptográficas descritas anteriormente para dispositivos móveis, além das operações criptográficas entre dispositivos móveis e o Citrix Gateway.

O MDX Vault criptografa aplicativos empacotados em MDX e dados em repouso associados em dispositivos iOS e Android usando módulos criptográficos validados por FIPS.

Suporte a idiomas

Os aplicativos de produtividade móvel e o console do XenMobile são adaptados para uso em outros idiomas além do inglês. O suporte inclui caracteres não ingleses e entrada de teclado, mesmo quando o aplicativo não está localizado no idioma preferencial de um usuário. Para obter mais informações sobre o suporte à globalização para todos os produtos Citrix, consulte `<https://support.citrix.com/article/CTX119253>`.

Este artigo lista os idiomas suportados na versão mais recente do XenMobile.

Console do XenMobile e o Portal de Autoatendimento

- Francês
- Alemão
- Espanhol
- Japonês
- Coreano
- Português
- Chinês Simplificado

Aplicativos de produtividade móvel

Um X indica que o aplicativo está disponível nesse idioma específico.

iOS e Android

IDIOMA	SECURE HUB	SECURE MAIL	SECURE WEB	QUICKEDIT
Japonês	X	X	X	X
Chinês Simplificado	X	X	X	X
Chinês Tradicional	X	X	X	X
Francês	X	X	X	X
Alemão	X	X	X	X
Espanhol	X	X	X	X
Coreano	X	X	X	X
Português	X	X	X	X
Holandês	X	X	X	X
Italiano	X	X	X	X
Dinamarquês	X	X	X	X
Sueco	X	X	X	X
Hebraico	X	X	X	Somente iOS
Árabe	X	X	X	X
Russo	X	X	X	X
Turco	X	X	Somente Android	-
Polonês	X	X	X	-

Windows

IDIOMA	SECURE HUB	SECURE MAIL	SECURE WEB
Francês	X	X	X
Alemão	X	X	X
Espanhol	X	X	X
Italiano	X	X	X
Dinamarquês	X	X	X
Sueco	X	X	X

Suporte a idiomas da direita para a esquerda

A tabela a seguir resume o suporte para texto em idiomas do Oriente Médio para cada aplicativo. Um X indica que o recurso está disponível para essa plataforma. O suporte a idiomas da direita para a esquerda não está disponível para dispositivos Windows.

APP	IOS	ANDROID
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

Instalar e configurar

Antes de começar

Você pode usar a seguinte lista de verificação de pré-instalação para anotar os pré-requisitos e configurações para instalar o XenMobile® no local. Cada tarefa ou nota inclui uma coluna indicando o componente ou função para a qual o requisito se aplica.

O planejamento de uma implantação do XenMobile envolve muitas considerações. Para recomendações, perguntas comuns e casos de uso para seu ambiente XenMobile completo, consulte o Manual de Implantação do XenMobile.

Para as etapas de instalação, consulte a seção Instalar o XenMobile mais adiante neste artigo.

Lista de verificação de pré-instalação

Conectividade de Rede Básica

A seguir estão as configurações de rede necessárias para a solução XenMobile.

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO	
Anote o nome de domínio totalmente qualificado (FQDN) ao qual os usuários remotos se conectam.	XenMobile e Citrix Gateway		
Anote o endereço IP público e local.			

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO		
Você precisa desses endereços IP para configurar o firewall para configurar a tradução de endereços de rede (NAT).	XenMobile e Citrix Gateway			
Anote a máscara de sub-rede.	XenMobile e Citrix Gateway			
Anote os endereços IP do DNS.	XenMobile e Citrix Gateway			
Anote os endereços IP do servidor WINS (se aplicável).	Citrix Gateway			
Identifique e anote o nome do host do Citrix Gateway.	Citrix Gateway	Este item não é o FQDN. O FQDN está contido no certificado de servidor assinado que está vinculado ao servidor virtual e ao qual os usuários se conectam. Você pode configurar o nome do host	Citrix Gateway	

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO		
		usando o Assistente de Configuração no Citrix Gateway.		
Anote o endereço IP do XenMobile. Reserve um endereço IP se você instalar uma instância do XenMobile. Se você configurar um cluster, anote todos os endereços IP de que precisa.	XenMobile			
Um endereço IP público configurado no Citrix Gateway	Citrix Gateway			
Uma entrada DNS externa para Citrix Gateway	Citrix Gateway			
Anote o endereço IP do servidor proxy web, a porta, a lista de hosts proxy e o nome de usuário e senha do	Citrix Gateway	Você pode usar o sAMAccountName ou o Nome Principal do Usuário (UPN) ao configurar o nome de	XenMobile e Citrix Gateway	

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO		
administrador. Essas configurações são opcionais se você implantar um servidor proxy em sua rede (se aplicável).		usuário para o proxy web.		
Anote o endereço IP do gateway padrão.	XenMobile e Citrix Gateway			
Anote o endereço IP do sistema (NSIP) e a máscara de sub-rede.	Citrix Gateway			
Anote o endereço IP da sub-rede (SNIP) e a máscara de sub-rede.	Citrix Gateway			
Anote o endereço IP do servidor virtual do Citrix Gateway e o FQDN do certificado. Para configurar vários servidores virtuais, anote	Citrix Gateway			

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO	
todos os endereços IP virtuais e FQDNs dos certificados.			
Anote as redes internas que os usuários podem acessar através do Citrix Gateway. Exemplo: 10.10.0.0/24. Insira todas as redes internas e segmentos de rede aos quais os usuários precisam de acesso nestes casos: Quando os usuários se conectam com o Secure Hub ou o Plug-in do Citrix Gateway quando o split tunneling está definido como Ativado.	Citrix Gateway		
Certifique-se de que a conectividade de rede entre o XenMobile Server, o Citrix Gateway, o	XenMobile e Citrix Gateway		

PRÉ-REQUISITO OU CONFIGURAÇÃO	COMPONENTE OU FUNÇÃO	ANOTE A CONFIGURAÇÃO	
Microsoft SQL Server externo e o servidor DNS esteja acessível.			

Licenciamento

O XenMobile exige que você adquira opções de licenciamento para Citrix Gateway e XenMobile. Para obter mais informações sobre o Licenciamento Citrix, consulte O Sistema de Licenciamento Citrix.

PRÉ-REQUISITO	COMPONENTE	ANOTE O LOCAL
Obtenha licenças Universais no site da Citrix. Para obter detalhes, consulte Licenciamento na documentação do Citrix Gateway.	Citrix Gateway, XenMobile e Citrix License Server	

Certificados

O XenMobile e o Citrix Gateway exigem certificados para habilitar conexões com outros produtos e aplicativos Citrix e de dispositivos de usuário. Para obter detalhes, consulte a seção Certificados e Autenticação na documentação do XenMobile.

PRÉ-REQUISITO	COMPONENTE	OBSERVAÇÕES
Obtenha e instale os certificados necessários.	XenMobile e Citrix Gateway	

Portas

Abra as portas para permitir a comunicação com os componentes do XenMobile.

PRÉ-REQUISITO	COMPONENTE	OBSERVAÇÕES
Abrir portas para o XenMobile	XenMobile e Citrix Gateway	

Banco de dados

O XenMobile requer configuração de conexão com o banco de dados. O repositório do XenMobile requer um banco de dados Microsoft SQL Server executando em uma das versões compatíveis mencionadas em Requisitos de sistema e compatibilidade. A Citrix recomenda usar o Microsoft SQL remotamente. O PostgreSQL está incluído no XenMobile. Use o PostgreSQL localmente ou remotamente *apenas* em ambientes de teste.

Por padrão, o XenMobile usa o driver de banco de dados jTDS. Para usar o driver Microsoft JDBC para instalações locais do XenMobile Server, consulte Drivers do SQL Server.

PRÉ-REQUISITO	COMPONENTE	OBSERVAÇÕES
Endereço IP e porta do Microsoft SQL Server. Certifique-se de que a conta de serviço do SQL Server a ser usada no XenMobile tenha a permissão de função DBcreator.	XenMobile	

Configurações do Active Directory

PRÉ-REQUISITO	COMPONENTE	NOTAS
Anote o endereço IP e as portas do Active Directory para os servidores primário e secundário. Se você usar a porta 636, instale um certificado raiz de uma CA no XenMobile e altere a opção Usar conexões seguras para Sim.	XenMobile e Citrix Gateway	

PRÉ-REQUISITO	COMPONENTE	NOTAS
Anote o nome de domínio do Active Directory.	XenMobile e Citrix Gateway	
Anote a conta de serviço do Active Directory, que requer um ID de usuário, senha e alias de domínio.		
A conta de serviço do Active Directory é a conta que o XenMobile usa para consultar o Active Directory.	XenMobile e Citrix Gateway	
Anote o DN Base do Usuário (User Base DN), que é o nível de diretório sob o qual os usuários estão localizados. Por exemplo: `cn=users,dc=ace,dc=com`. O Citrix Gateway e o XenMobile usam o DN Base do Usuário para consultar o Active Directory.	XenMobile e Citrix Gateway	
Observe o DN Base do Grupo, que é o nível de diretório sob o qual os grupos estão localizados. O Citrix Gateway e o XenMobile usam este DN para consultar o Active Directory.	XenMobile e Citrix Gateway	

Conexões entre XenMobile e Citrix Gateway

PRÉ-REQUISITO	COMPONENTE	OBSERVE A CONFIGURAÇÃO
Observe o nome do host do XenMobile.	XenMobile	

PRÉ-REQUISITO	COMPONENTE	OBSERVE A CONFIGURAÇÃO
Observe o FQDN ou o endereço IP do XenMobile.	XenMobile	
Identifique os aplicativos que os usuários podem acessar.	Citrix Gateway	
Observe a URL de Retorno.	XenMobile	

Conexões de Usuário: Acesso a Citrix Virtual Apps and Desktops™ e Citrix Secure Hub

A Citrix recomenda que você use o assistente de Configuração Rápida no Citrix ADC para configurar as definições de conexão entre o XenMobile e o Citrix Gateway e entre o XenMobile e o Secure Hub. Você cria um segundo servidor virtual para habilitar as conexões de usuário do Citrix Receiver™ e de navegadores da web. Essas conexões são para aplicativos baseados em Windows e desktops virtuais no Virtual Apps and Desktops. A Citrix recomenda que você também use o assistente de Configuração Rápida no Citrix ADC para configurar essas definições.

PRÉ-REQUISITO	COMPONENTE	ANOTE A CONFIGURAÇÃO
Anote o nome do host do Citrix Gateway e o URL externo. O URL externo é o endereço da web com o qual os usuários se conectam.	XenMobile	
Anote o URL de retorno de chamada do Citrix Gateway.	XenMobile	
Anote os endereços IP e as máscaras de sub-rede para o servidor virtual.	Citrix Gateway	
Anote o caminho para o Program Neighborhood Agent ou um Site do Virtual Apps and Desktops.	Citrix Gateway e XenMobile	

PRÉ-REQUISITO	COMPONENTE	ANOTE A CONFIGURAÇÃO
Anote o FQDN ou endereço IP do servidor Citrix Virtual Apps™ and Desktops executando a Secure Ticket Authority (STA) (somente para conexões ICA).	Citrix Gateway	
Anote o FQDN público para o XenMobile.	Citrix Gateway	
Anote o FQDN público para o Secure Hub.	Citrix Gateway	

Fluxograma para implantação do XenMobile

Você pode usar este fluxograma para guiá-lo pelas principais etapas de implantação do XenMobile. Links para tópicos sobre cada etapa seguem a figura.

1: Requisitos do sistema e compatibilidade

2: Instalar e configurar

3 e 4: Lista de verificação de pré-instalação (este artigo)

5: Configurar o XenMobile na Janela do Prompt de Comando (este artigo)

6: Configurar o XenMobile em um navegador da web (este artigo)

7: Configurando as Configurações para o Seu Ambiente XenMobile

8: Requisitos de porta

Instalar o XenMobile

A máquina virtual (VM) do XenMobile é executada no Citrix XenServer, VMware ESXi ou Microsoft Hyper-V. Você pode usar os consoles de gerenciamento XenCenter® ou vSphere para instalar o XenMobile.

> **Nota:**

> Certifique-se de que o hipervisor esteja configurado com a hora correta – usando um servidor NTP ou uma configuração manual – porque o XenMobile usa essa hora. Se você tiver problemas de fuso horário ao sincronizar a hora do XenMobile com um hipervisor, poderá evitar os problemas apontando o XenMobile para um servidor NTP. Para fazer isso, use a CLI do XenMobile, conforme descrito em Opções da interface de linha de comando.

> **Pré-requisitos do XenServer ou VMware ESXi**. Antes de instalar o XenMobile no XenServer ou VMware ESXi, você deve fazer o seguinte. Para obter detalhes, consulte a documentação do XenServer ou VMware.

- Instale o XenServer® ou VMware ESXi em um computador com recursos de hardware adequados.
- Instale o XenCenter ou vSphere em um computador separado. O computador que hospeda o XenCenter ou vSphere se conecta ao host XenServer ou VMware ESXi através da rede.

Pré-requisitos do Hyper-V. Antes de instalar o XenMobile no Hyper-V, você deve fazer o seguinte. Para obter detalhes, consulte a documentação do Hyper-V.

- Instale o Windows Server 2016 ou Windows Server 2019 com o Hyper-V ativado, função ativada, em um computador com recursos de sistema adequados. Ao instalar a função Hyper-V, certifique-se de especificar as NICs no servidor que o Hyper-V usa para criar as redes virtuais. Você pode reservar algumas NICs para o host.
- Exclua o arquivo Virtual Machines/<*build-specific UUID*>.xml
- Mova o arquivo Legacy/<*build-specific UUID*>.exp para Virtual Machines

Modo FIPS 140-2. Para instalar o XenMobile Server no modo FIPS, conclua um grupo de pré-requisitos, conforme discutido em Configurar FIPS com XenMobile.

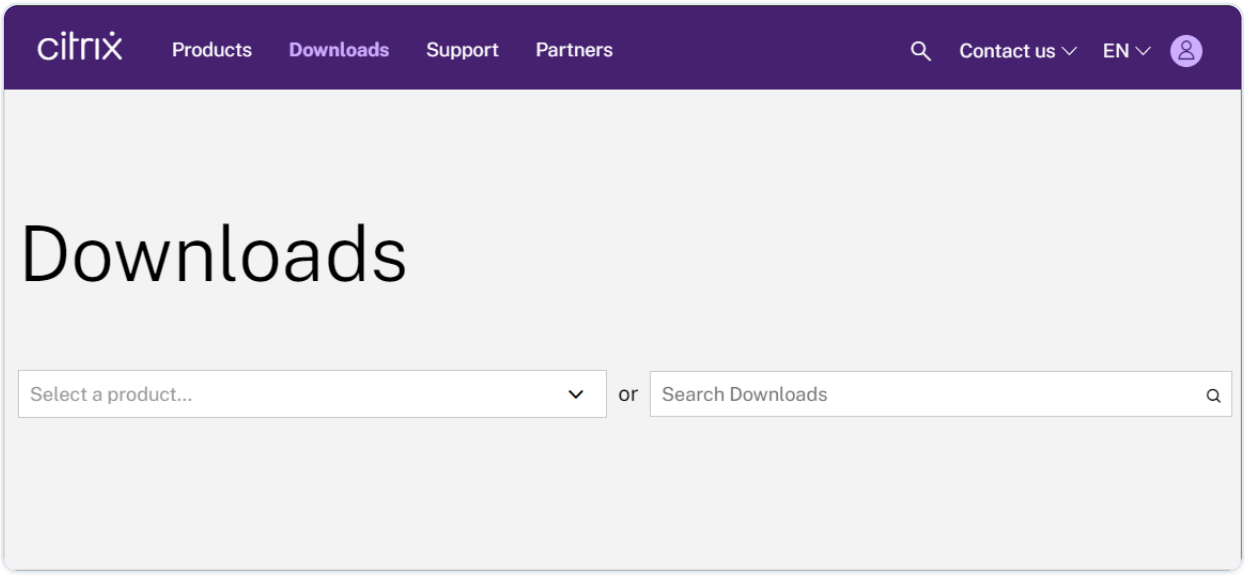
Baixar software de produto XenMobile

Você pode baixar o software do produto no site da Citrix. Faça login no site e use o link Downloads para navegar até a página que contém o software que você deseja baixar.

Para baixar o software para XenMobile

1. Vá para o site da Citrix.
2. Ao lado da caixa de pesquisa, clique em **Log On** e faça login na sua conta.
3. Clique na guia **Downloads**.

4. Na página Downloads, na lista **selecionar um produto**, clique em **Citrix Endpoint Management™ (and Citrix XenMobile Server)**. A página Citrix Endpoint Management (and Citrix XenMobile Server) aparece automaticamente.



5. Expanda **XenMobile Server (on-premises)**.
6. Expanda **Product Software**.
7. Clique em **XenMobile Server 10**.
8. Clique no menu **Jump to Download** e escolha a imagem virtual apropriada para usar para instalar o XenMobile. Alternativamente, role a página para baixo para localizar o botão **Download File** para a imagem que você deseja instalar.
9. Siga as instruções na tela para baixar o software.

Para baixar o software para Citrix Gateway

Você pode usar este procedimento para baixar o dispositivo virtual Citrix Gateway ou atualizações de software para seu dispositivo Citrix Gateway existente.

1. Vá para o site da Citrix.
2. Se você ainda não estiver conectado ao site da Citrix, ao lado da caixa Pesquisar, clique em **Log On** e faça login em sua conta.
3. Clique na guia **Downloads**.
4. Na página Downloads, na lista de seleção de produtos, clique em **Citrix Gateway**.
5. Clique em **Go**. A página Citrix Gateway é exibida.
6. Na página Citrix Gateway, expanda a versão do Citrix Gateway que você está executando.
7. Em **Firmware**, clique na versão do software do appliance que você deseja baixar.

> **Nota:**
>
> Você também pode clicar em **Virtual Appliances** para baixar o Citrix ADC VPX. Ao selecionar esta opção, você receberá uma lista de software para a máquina virtual para cada hypervisor.

8. Clique na versão do software do appliance que você deseja baixar.
9. Na página do software do appliance para a versão que você deseja baixar, clique em **Download** para o appliance virtual apropriado.
10. Siga as instruções na tela para baixar o software.

Configurar o XenMobile para o Primeiro Uso

1. Para configurar o endereço IP e a máscara de sub-rede, gateway padrão, servidores DNS e outras configurações para o XenMobile: Use o console de linha de comando do XenCenter ou vSphere.

> **Nota:**
>
> Ao usar um cliente web vSphere: Recomendamos que você não configure as propriedades de rede durante a implantação do modelo OVF na página **Customize template**. Ao fazer isso em uma configuração de alta disponibilidade: Você evita um problema com o endereço IP que ocorre ao clonar e reiniciar a segunda máquina virtual XenMobile.

2. Acesse o console de gerenciamento do XenMobile apenas através do nome de domínio totalmente qualificado do XenMobile Server ou dos endereços IP do nó.
3. Faça logon e siga as etapas na tela de logon inicial.

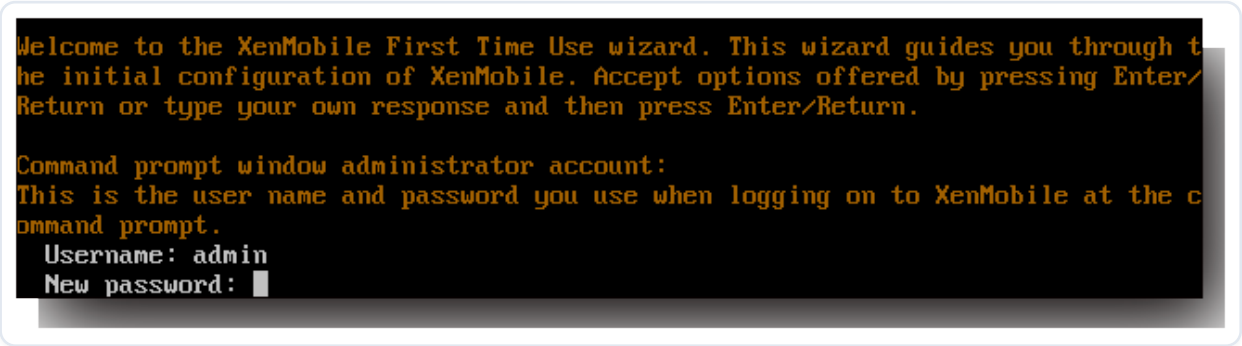
Configurar o XenMobile na Janela do Prompt de Comando

1. Importe a máquina virtual XenMobile para Citrix XenServer, Microsoft Hyper-V ou VMware ESXi. Para obter detalhes, consulte a documentação de XenServer, Hyper-V ou VMware.
2. No seu hypervisor, selecione a máquina virtual XenMobile importada e inicie a visualização do prompt de comando. Para obter detalhes, consulte a documentação do seu hypervisor.

3. Na página do console do hipervisor, crie uma conta de administrador para o XenMobile na janela do prompt de comando digitando o nome de usuário e a senha do administrador.

   Ao criar ou alterar senhas para a conta de administrador do prompt de comando, certificados de servidor de Infraestrutura de Chave Pública (PKI) e FIPS: o XenMobile impõe as seguintes regras para todos os usuários, exceto usuários do Active Directory cujas senhas são gerenciadas fora do XenMobile.

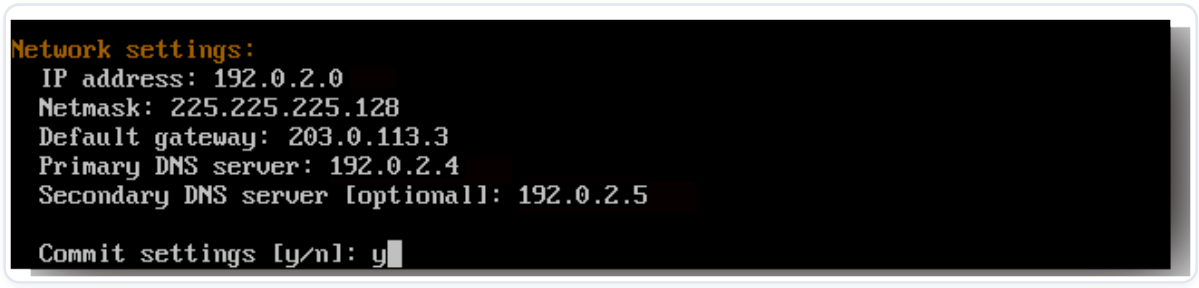
   - A senha deve ter pelo menos oito caracteres.
   - A senha deve atender a pelo menos três dos seguintes critérios de complexidade:
     - Letras maiúsculas (A a Z)
     - Letras minúsculas (a a z)
     - Numerais (0 a 9)
     - Caracteres especiais (como `! # $ %`)

   Nenhum caractere, como asteriscos, aparece ao digitar a nova senha.

4. Forneça as seguintes informações de rede e, em seguida, digite **y** para confirmar as configurações:

   a. Endereço IP do XenMobile Server
   b. Máscara de rede
   c. Gateway padrão, que é o endereço IP do gateway padrão na DMZ
   d. Servidor DNS primário, que é o endereço IP do servidor DNS
   e. Servidor DNS secundário (opcional)



> **Nota:**
>
> Os endereços mostrados nesta e nas imagens a seguir não funcionam e são fornecidos apenas como exemplos.

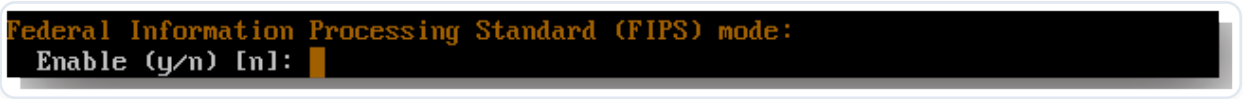
5. Digite **y** para aumentar a segurança gerando uma frase secreta de criptografia aleatória ou **n** para fornecer sua própria frase secreta. A Citrix recomenda digitar **y** para gerar uma frase secreta aleatória.

   A frase secreta é usada como parte da proteção das chaves de criptografia usadas para proteger seus dados confidenciais. Um hash da frase secreta, armazenado no sistema de arquivos do servidor, é usado para recuperar as chaves durante a criptografia e descriptografia dos dados. A frase secreta não pode ser visualizada.

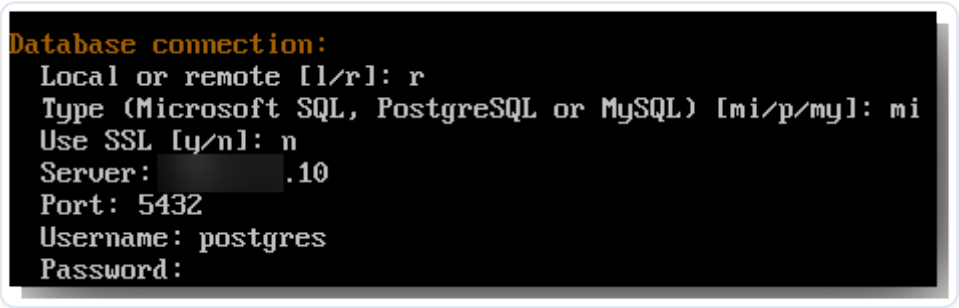
   > **Nota:**
   >
   > Se você pretende estender seu ambiente e configurar mais servidores, forneça sua própria frase secreta. Se você selecionar uma frase secreta aleatória, não poderá visualizá-la.

6. Opcionalmente, habilite o Padrão Federal de Processamento de Informações (FIPS). Para obter detalhes sobre FIPS, consulte FIPS. Além disso, certifique-se de concluir um grupo de pré-requisitos, conforme discutido em Configurar FIPS com XenMobile.

7. Forneça as seguintes informações para configurar a conexão do banco de dados.



- Seu banco de dados pode ser local ou remoto. Digite **l** para local ou **r** para remoto.
- Selecione o tipo de banco de dados. Digite **mi** para Microsoft SQL ou digite **p** para PostgreSQL.

> **Importante:**
>
> - A Citrix recomenda usar o Microsoft SQL remotamente. O PostgreSQL está incluído no XenMobile. Use o PostgreSQL localmente ou remotamente *apenas* em ambientes de teste.
> - A migração de banco de dados não é suportada. Bancos de dados criados em um ambiente de teste não podem ser movidos para um ambiente de produção.

- Opcionalmente, digite **y** para usar a autenticação SSL para seu banco de dados.
- Forneça o nome de domínio totalmente qualificado (FQDN) para o servidor que hospeda o XenMobile. Este servidor de host único fornece serviços de gerenciamento de dispositivos e de aplicativos.
- Digite o número da porta do seu banco de dados se for diferente do número da porta padrão. A porta padrão para Microsoft SQL é 1433 e a porta padrão para PostgreSQL é 5432.
- Digite o nome de usuário do administrador do seu banco de dados.
- Digite a senha do administrador do seu banco de dados.
- Digite o nome do banco de dados.
- Pressione **Enter** para confirmar as configurações do banco de dados.

8. Opcionalmente, digite **y** para habilitar o clustering de nós XenMobile, ou instâncias.

> **Importante:**

> Se você habilitar um cluster XenMobile, após a conclusão da configuração do sistema, abra a porta 80 para habilitar a comunicação em tempo real entre os membros do cluster. Conclua essa configuração em todos os nós do cluster.

9. Digite o nome de domínio totalmente qualificado (FQDN) do XenMobile Server.

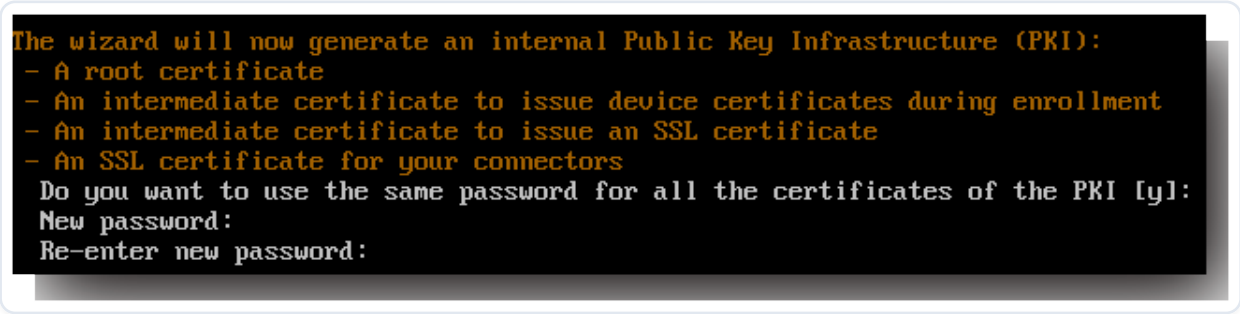


10. Pressione **Enter** para confirmar as configurações.
11. Identifique as portas de comunicação. Para obter detalhes sobre as portas e seus usos, consulte Requisitos de Porta.

> **Nota:**
>
> Aceite as portas padrão pressionando **Enter** (Return em um Mac).



12. Pule a próxima pergunta sobre a atualização de uma versão anterior do XenMobile, pois você está instalando o XenMobile pela primeira vez.
13. Digite **y** se quiser usar a mesma senha para cada certificado de Infraestrutura de Chave Pública (PKI). Para obter detalhes sobre o recurso PKI do XenMobile, consulte Carregando Certificados.



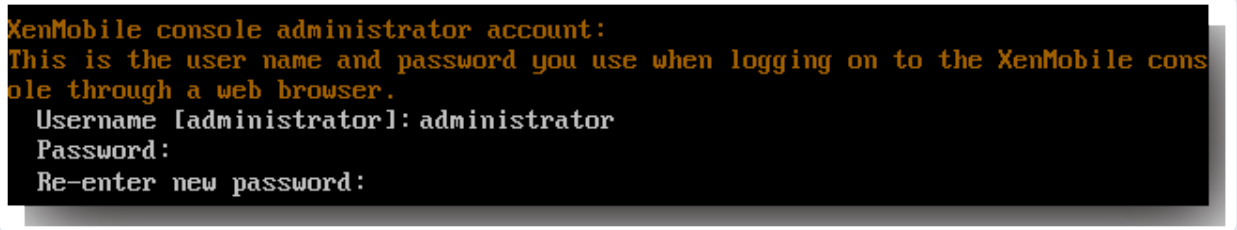
> **Importante:**

> Se você pretende agrupar nós, ou instâncias, do XenMobile, forneça senhas idênticas para os nós subsequentes.

14. Digite a nova senha e, em seguida, digite a nova senha novamente para confirmá-la.

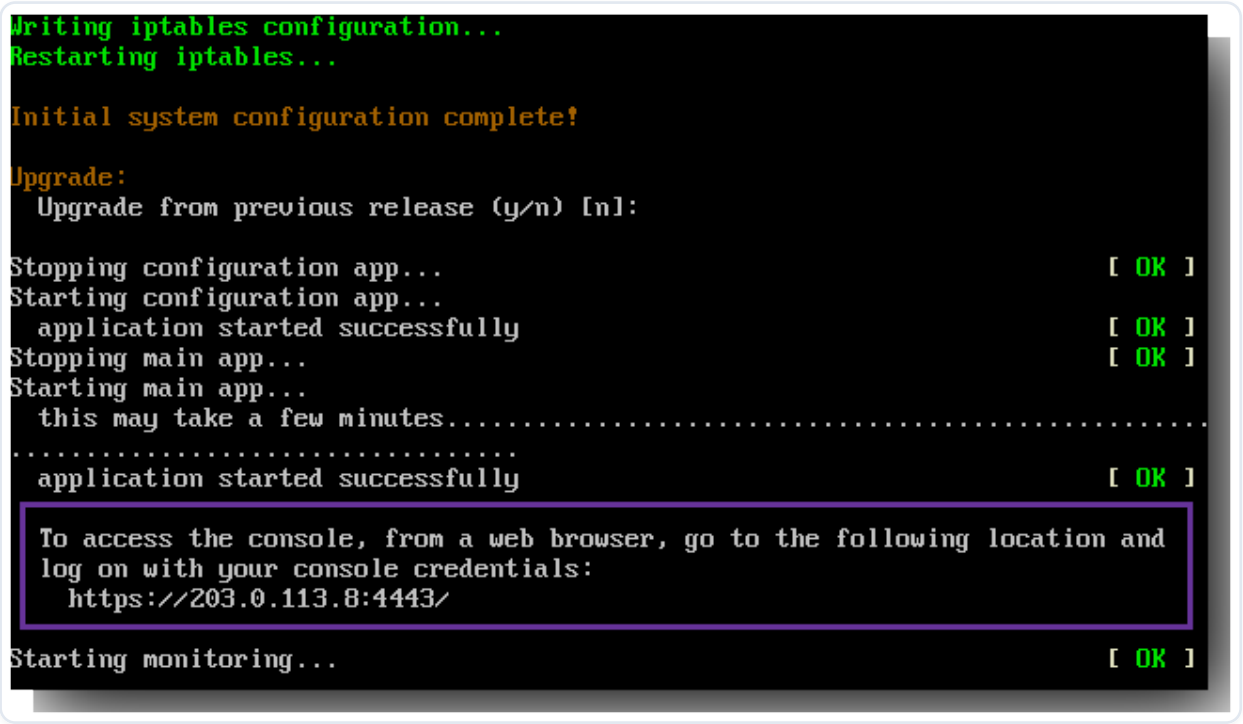
    Nenhum caractere, como asteriscos, aparece ao digitar a nova senha.

15. Pressione **Enter** para confirmar as configurações.
16. Crie uma conta de administrador para fazer logon no console do XenMobile com um navegador da web. Certifique-se de registrar essas credenciais para uso posterior.



> **Nota:**
>
> Nenhum caractere, como asteriscos, aparece ao digitar a nova senha.

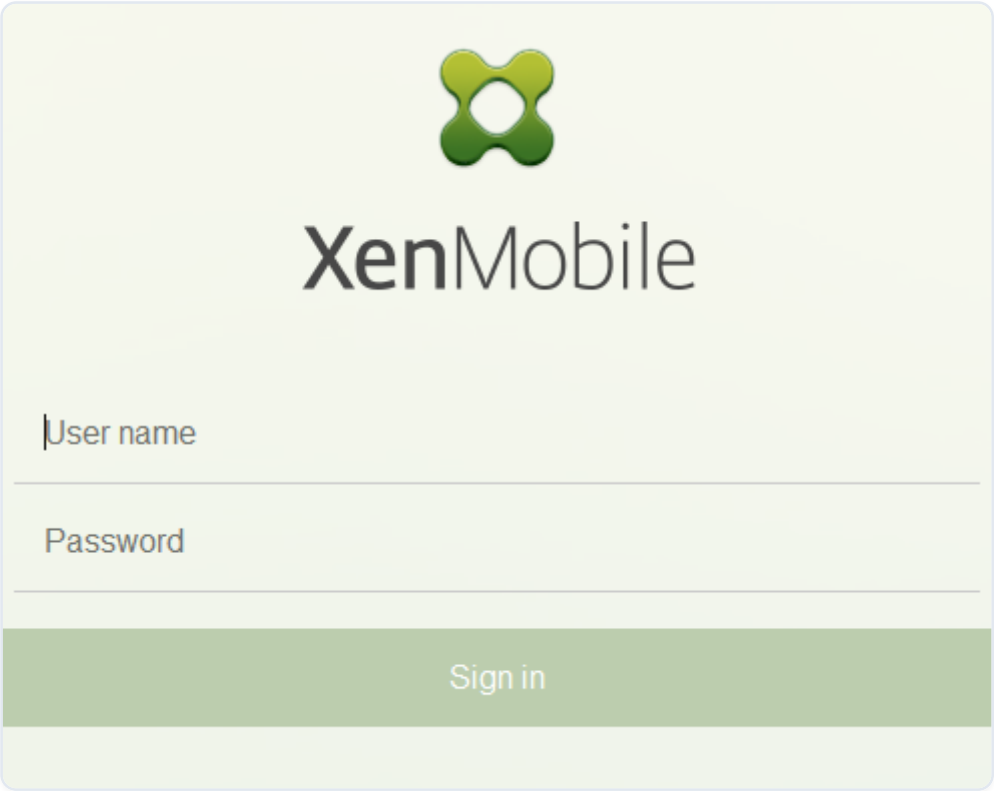
17. Pressione **Enter** para confirmar as configurações. A configuração inicial do sistema é salva.
18. Quando perguntado se você está atualizando, digite **n** porque é uma nova instalação.
19. Copie o URL completo que aparece na tela e continue esta configuração inicial do XenMobile em seu navegador da web.



Configurar o XenMobile em um navegador da web

Após concluir a parte inicial da configuração do XenMobile na janela de prompt de comando do seu hipervisor, conclua o processo em seu navegador da web.

1. No seu navegador da web, navegar até o local fornecido ao final da configuração da janela de prompt de comando.
2. Digite o nome de usuário e a senha da conta de administrador do console do XenMobile que você criou na janela de prompt de comando.



3. Na página Introdução, clique em **Iniciar**. A página **Licenciamento** é exibida.
4. Configure a licença. Se você não carregar uma licença, usará uma licença de avaliação válida por 30 dias. Para obter detalhes sobre como adicionar e configurar licenças e configurar notificações de expiração, consulte Licenciamento.

> **Importante:**
>
> Se você pretende usar o clustering do XenMobile adicionando nós de cluster, ou instâncias, do XenMobile, você deve usar o Citrix Licensing em um servidor remoto.

5. Na página **Certificados**, clique em **Importar**. A caixa de diálogo Importar é exibida.
6. Importe seu certificado APNs e SSL Listener. O gerenciamento de dispositivos iOS requer um certificado APNs. Para obter detalhes sobre como trabalhar com certificados, consulte Certificados.

> **Nota:**
>
> Esta etapa exige a reinicialização do servidor.

7. Se apropriado para o ambiente, configure o Citrix Gateway. Para obter detalhes sobre como configurar o Citrix Gateway, consulte Citrix Gateway e XenMobile e Configurando as Definições para o Seu Ambiente XenMobile.

   Nota:

   - Você pode implantar o Citrix Gateway no perímetro da sua rede interna (ou intranet). Essa implantação fornece um único ponto de acesso seguro aos servidores, aplicativos e outros recursos de rede que residem na rede interna. Nesta implantação, todos os usuários remotos devem se conectar ao Citrix Gateway antes de poderem acessar quaisquer recursos na rede interna.
   - Embora o Citrix Gateway seja uma configuração opcional: depois de inserir dados na página, você deve limpar ou preencher os campos obrigatórios antes de poder sair da página.

8. Conclua a configuração LDAP para acessar usuários e grupos do Active Directory. Para obter detalhes sobre como configurar a conexão LDAP, consulte Configuração LDAP.
9. Configure o servidor de notificação para poder enviar mensagens aos usuários. Para obter detalhes sobre a configuração do servidor de notificação, consulte Notificações.

Pós-requisito. Reinicie o XenMobile Server para ativar seus certificados.

Configurar FIPS com XenMobile®

O modo de Padrões Federais de Processamento de Informações (FIPS) no XenMobile oferece suporte a clientes do governo federal dos EUA usando apenas bibliotecas certificadas FIPS 140-2 para todas as operações de criptografia. A instalação do seu XenMobile Server com o modo FIPS garante que todos os dados para o cliente e servidor XenMobile estejam totalmente em conformidade com o FIPS 140-2. Essa conformidade se aplica a dados em repouso e dados em trânsito.

Antes de instalar um XenMobile Server no modo FIPS, conclua os seguintes pré-requisitos.

- Use um SQL Server 2014 externo para o banco de dados do XenMobile. O SQL Server também deve ser configurado para comunicação SSL segura. Para obter instruções sobre como configurar a comunicação SSL segura com o SQL Server, consulte Habilitar Conexões Criptografadas para o Mecanismo de Banco de Dados (SQL Server Configuration Manager).

- A comunicação SSL segura exige que você instale um certificado SSL confiável de uma autoridade de certificação (CA) conhecida em seu SQL Server. O SQL Server 2014 não pode aceitar um certificado curinga. A Citrix® recomenda que você solicite um certificado SSL com o FQDN do SQL Server.

Configurando o modo FIPS

Você pode habilitar o modo FIPS apenas durante a configuração inicial do XenMobile Server. Não é possível habilitar o FIPS após a conclusão da instalação. Portanto, se você planeja usar o modo FIPS, deve instalar o XenMobile Server com o modo FIPS desde o início. Para clusters XenMobile, todos os nós do cluster devem ter o FIPS habilitado. Você não pode ter uma mistura de XenMobile Servers FIPS e não FIPS no mesmo cluster.

Existe uma opção **Alternar modo FIPS** na interface de linha de comando do XenMobile que não é para uso em produção. Esta opção destina-se a uso não produtivo e diagnóstico e não é suportada em um XenMobile Server de produção.

1. Durante a configuração inicial, habilite o **modo FIPS**.
2. Carregue o certificado raiz da CA para o seu SQL Server.
3. Especifique o nome do servidor e a porta do seu SQL Server, as credenciais para fazer login no SQL Server e o nome do banco de dados a ser criado para o XenMobile.

   > **Nota:**
   >
   > Você pode usar um logon SQL ou uma conta do Active Directory para acessar o SQL Server, mas o logon que você usa deve ter a função DBcreator.

4. Para usar uma conta do Active Directory, insira as credenciais no formato domínio\\nome de usuário.
5. Uma vez que essas etapas estejam concluídas, continue com a configuração inicial do XenMobile.

Para confirmar que a configuração do modo FIPS foi bem-sucedida, faça logon na interface de linha de comando do XenMobile. A frase **In FIPS Compliant Mode** aparece no banner de logon.

Importando Certificados

O procedimento a seguir descreve como configurar o FIPS no XenMobile importando um certificado.

Pré-requisitos do SQL

1. A conexão com a instância SQL a partir do XenMobile deve ser segura e deve ser do SQL Server versão 2012 ou SQL Server 2014. Para proteger a conexão, consulte Como habilitar a criptografia SSL para uma instância do SQL Server usando o Microsoft Management Console.
2. Se o serviço não reiniciar corretamente, verifique o seguinte: Abra **Services.msc**.
    a. Copie as informações da conta de logon usadas para o serviço SQL Server.
    b. Abra MMC.exe no SQL Server.
    c. Vá para **File** > **Add/Remove Snap-in** e, em seguida, clique duas vezes no item de certificados para adicionar o snap-in de certificados. Selecione a conta do computador e o computador local nas duas páginas do assistente.
    d. Clique em **OK**.
    e. Expanda **Certificates (Local Computer) > Personal > Certificates** e encontre o certificado SSL importado.
    f. Clique com o botão direito do mouse no certificado importado (selecionado no SQL Server Configuration Manager) e, em seguida, clique em **All Tasks > Manage Private Keys**.
    g. Em **Group or User names**, clique em **Add**.
    h. Insira o nome da conta de serviço SQL que você copiou na etapa anterior.
    i. Desmarque a opção **Allow Full Control**. Por padrão, a conta de serviço tem permissões de Controle total e Leitura, mas deve ser capaz apenas de ler a chave privada.
    j. Feche **MMC** e inicie o serviço SQL.
3. Certifique-se de que o serviço SQL foi iniciado corretamente.

Pré-requisitos do Internet Information Services (IIS)

1. Baixe o certificado raiz (base 64).
2. Copie o certificado raiz para o site padrão no servidor IIS, C:\\inetpub\\wwwroot.
3. Marque a caixa de seleção **Autenticação** para o site padrão.
4. Defina **Anônimo** como **habilitado**.
5. Selecione a caixa de seleção das regras de **Rastreamento de Solicitações Falhas**.
6. Certifique-se de que o .cer não está bloqueado.
7. Navegue até o local do .cer em um navegador da web a partir do servidor local, `https://localhost/certname.cer`. O texto do certificado raiz aparece no navegador.

8. Se o certificado raiz não aparecer no seu navegador da web, certifique-se de que o ASP esteja habilitado no servidor IIS da seguinte forma.
    a. Abra o Gerenciador do Servidor.
    b. navegar para o assistente em **Gerenciar > Adicionar Funções e Recursos**.
    c. Nas funções do servidor, expanda **Servidor Web (IIS)**, expanda **Servidor Web**, expanda **Desenvolvimento de Aplicativos** e, em seguida, selecione **ASP**.
    d. Clique em **Avançar** até que a instalação seja concluída.
9. Navegue até `https://localhost/cert.cer`.

    Para obter mais informações, consulte Web Server (IIS).

> **Nota:**
>
> Você pode usar a instância do IIS da CA para este procedimento.

Importando o Certificado Raiz Durante a Configuração Inicial do FIPS

Ao concluir as etapas para configurar o XenMobile pela primeira vez no console de linha de comando, você deve concluir estas configurações para importar o certificado raiz. Para obter detalhes sobre as etapas de instalação, consulte Installing XenMobile.

- Habilitar FIPS: Sim
- Carregar Certificado Raiz: Sim
- Copiar(c) ou Importar(i): i
- Insira o URL HTTP para importar: `https://<FQDN of IIS server>/cert.cer`
- Servidor: *FQDN of SQL Server*
- Porta: 1433
- Nome de usuário: Conta de serviço que pode criar o banco de dados (`domain\username`).
- Senha: A senha para a conta de serviço.
- Nome do Banco de Dados: Um nome de sua escolha.

Habilitar o modo FIPS em dispositivos móveis

Por padrão, o modo FIPS está desabilitado em dispositivos móveis. Para habilitar o modo FIPS, vá para **Configurações > Propriedades do Cliente**, edite a propriedade **Habilitar Modo FIPS** e defina o valor como **true**. Para obter mais informações, consulte Propriedades do cliente.

Configurar clustering

Para configurar o clustering, configure os dois endereços IP virtuais de balanceamento de carga a seguir no Citrix ADC.

- **Endereço IP virtual de balanceamento de carga de gerenciamento de dispositivos móveis (MDM):** Um endereço IP virtual de balanceamento de carga MDM é necessário para se comunicar com os nós do XenMobile® configurados em um cluster. Este balanceamento de carga é feito no modo SSL Bridge.
- **Endereço IP virtual de balanceamento de carga de gerenciamento de aplicativos móveis (MAM):** Endereços IP virtuais de balanceamento de carga MAM são necessários para que o Citrix Gateway se comunique com os nós do XenMobile configurados em um cluster. No XenMobile, por padrão, todo o tráfego do Citrix Gateway é roteado para o endereço IP virtual de balanceamento de carga na porta 8443.

Os procedimentos nesta seção explicam como criar uma máquina virtual (VM) do XenMobile e unir a nova VM a uma VM existente. Essas etapas criam uma configuração de cluster.

Pré-requisitos

- Você configurou totalmente o nó XenMobile necessário.
- Configure o NTP em todos os nós do cluster e no banco de dados do XenMobile. Para que o clustering funcione corretamente, todos esses servidores devem ter a mesma hora.
- Um endereço IP público para o balanceador de carga MDM e um endereço IP privado para MAM.
- Certificados de servidor.
- Um IP livre para o endereço IP virtual do Citrix Gateway.
- Com o XenMobile implantado em uma configuração de cluster e no modo somente MDM ou Enterprise (MDM+MAM): Modifique sua configuração de balanceador de carga do Citrix ADC para usar **persistência de IP de origem** para todos os balanceadores de carga MDM do Citrix ADC, ou seja, servidores virtuais configurados para as portas 8443 e 443. Conclua essa configuração antes que os dispositivos do usuário atualizem para o iOS 11. Para obter mais

informações, consulte este artigo do Citrix Knowledge Center: `<https://support.citrix.com/article/CTX227406>`.

- Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no XenMobile Server.

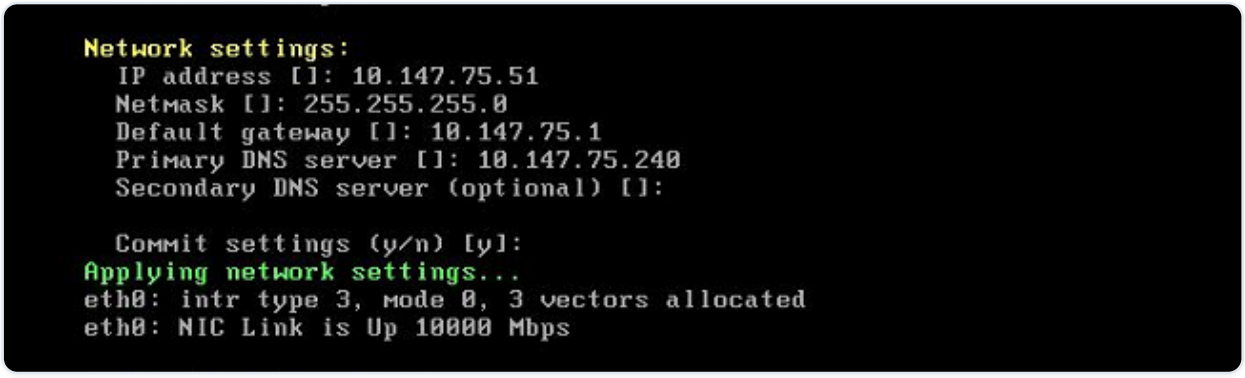
Para diagramas de arquitetura de referência para XenMobile 10.x em configurações de cluster, consulte Arquitetura.

Instalando os Nós do Cluster XenMobile

Com base no número de nós que você precisa, crie VMs do XenMobile. Aponte as novas VMs para o mesmo banco de dados e forneça as mesmas senhas de certificado PKI.

1. Abra o console de linha de comando da nova VM e insira a nova senha para a conta de administrador.

2. Forneça os detalhes de configuração de rede conforme mostrado na figura a seguir.



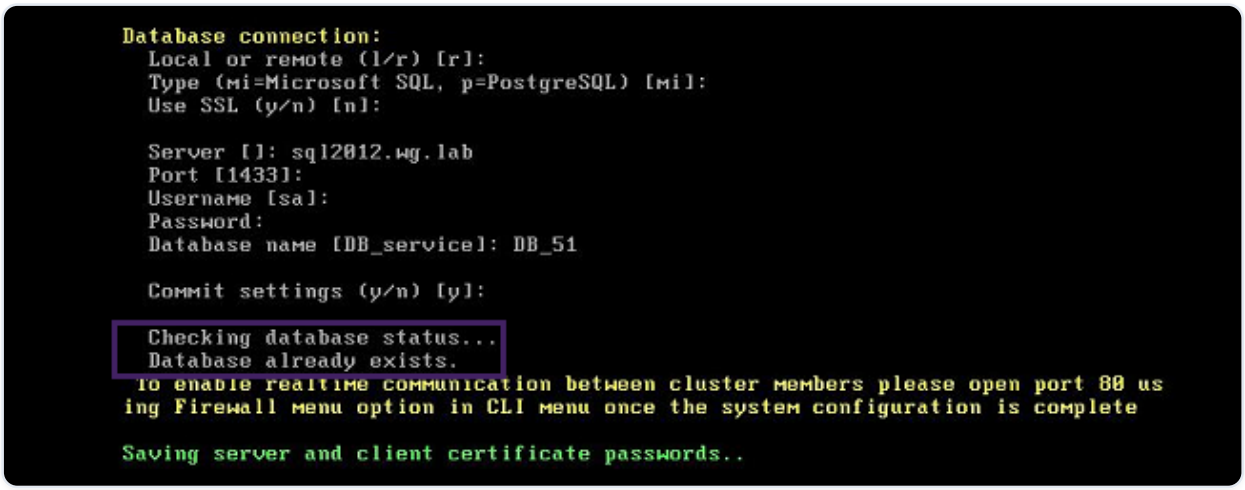
3. Se você quiser usar a senha padrão para proteção de dados, digite **y**; ou, digite **n** e insira uma nova senha.



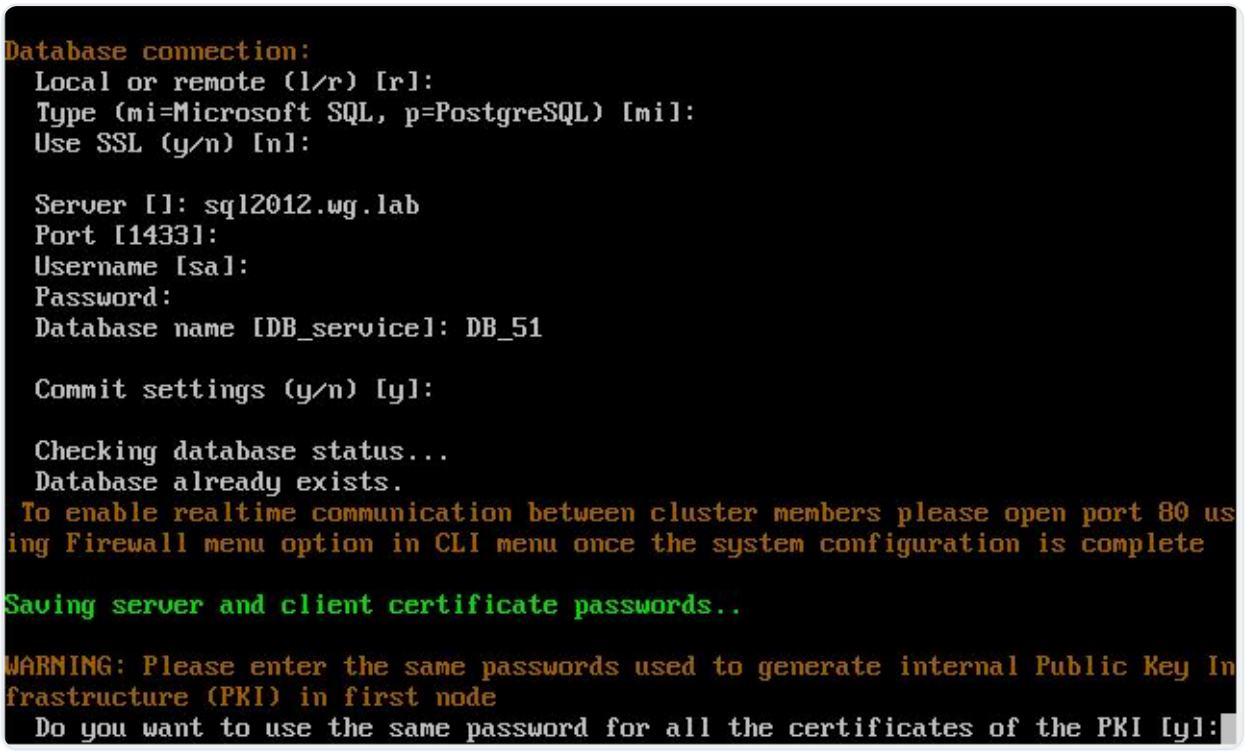
4. Se você quiser usar FIPS, digite **y**; ou, digite **n**.



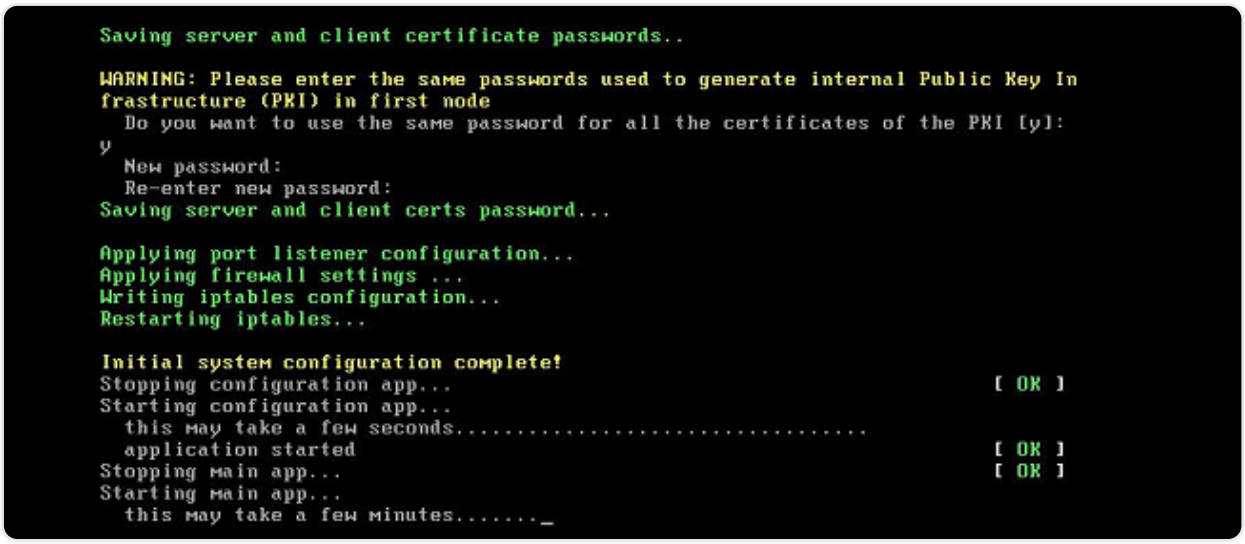
5. Configure o banco de dados para que ele aponte para o mesmo banco de dados para o qual a VM configurada anteriormente apontava. Você verá a mensagem: `Database already exists`.



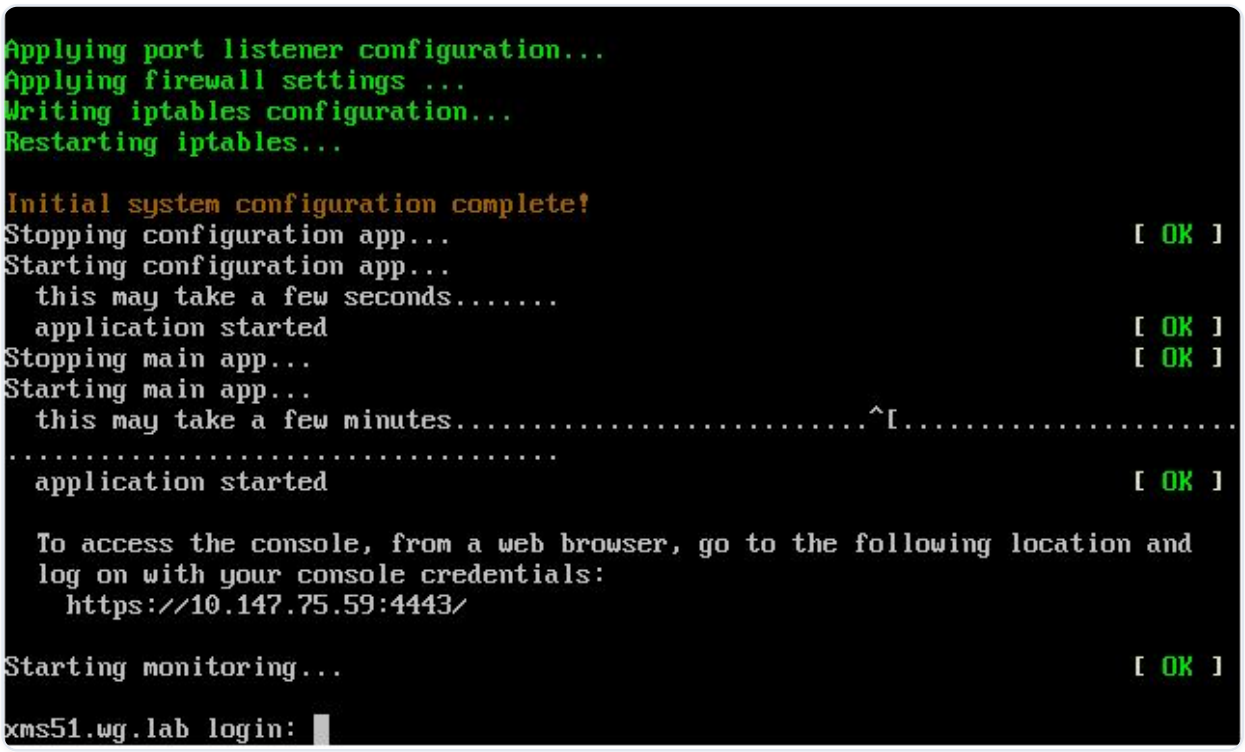
6. Insira as mesmas senhas para os certificados que você forneceu para a primeira VM.



Depois de inserir a senha, a configuração inicial no segundo nó será concluída.



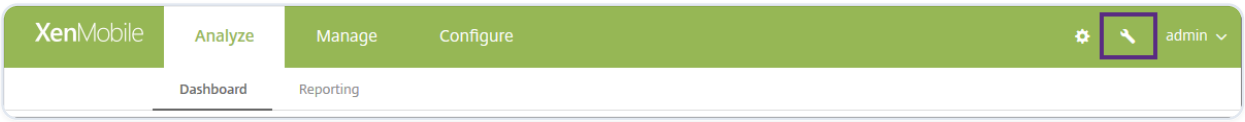
7. Quando a configuração estiver completa, o servidor reinicia e a caixa de diálogo de logon aparece.



> **Nota:**
>
> A caixa de diálogo de logon é semelhante à caixa de diálogo de logon da primeira VM. A correspondência é uma forma de você confirmar que ambas as VMs estão usando o mesmo servidor de banco de dados.

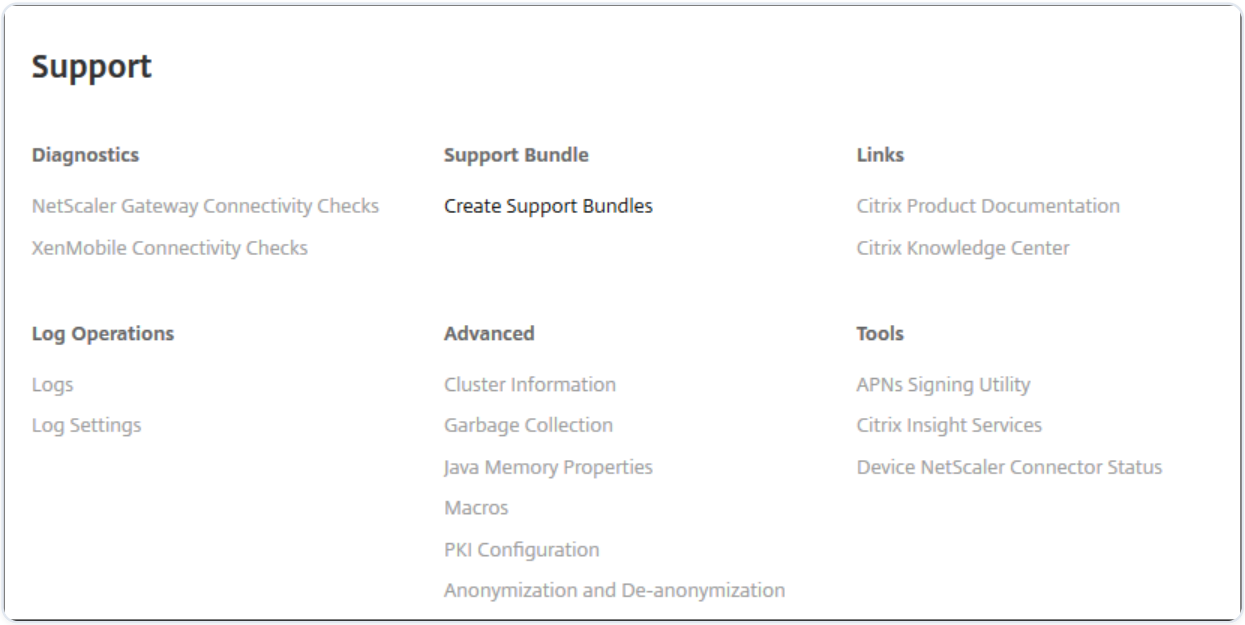
8. Use o nome de domínio totalmente qualificado (FQDN) do XenMobile para abrir o console do XenMobile em um navegador da web.

9. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito do console.

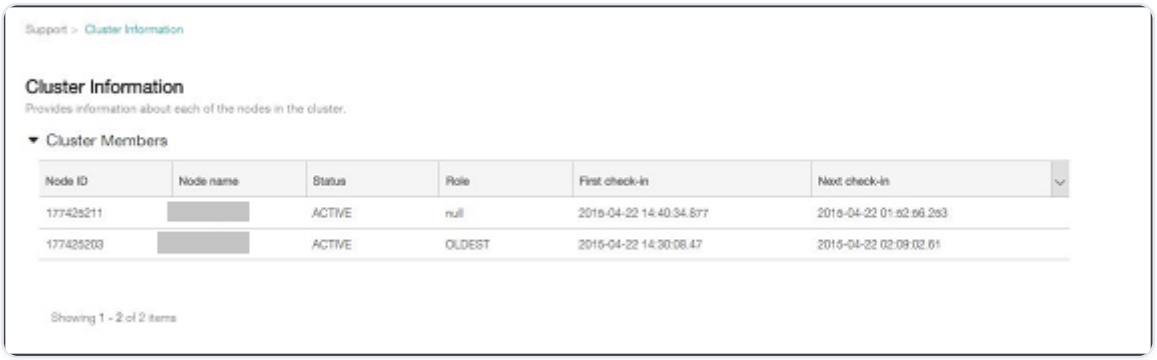


A página **Suporte** é aberta.

10. Em **Avançado**, clique em **Informações do Cluster**.



Todas as informações sobre o cluster, incluindo membro do cluster, informações de conexão do dispositivo, tarefas e assim por diante, aparecem. O novo nó agora é um membro do cluster.

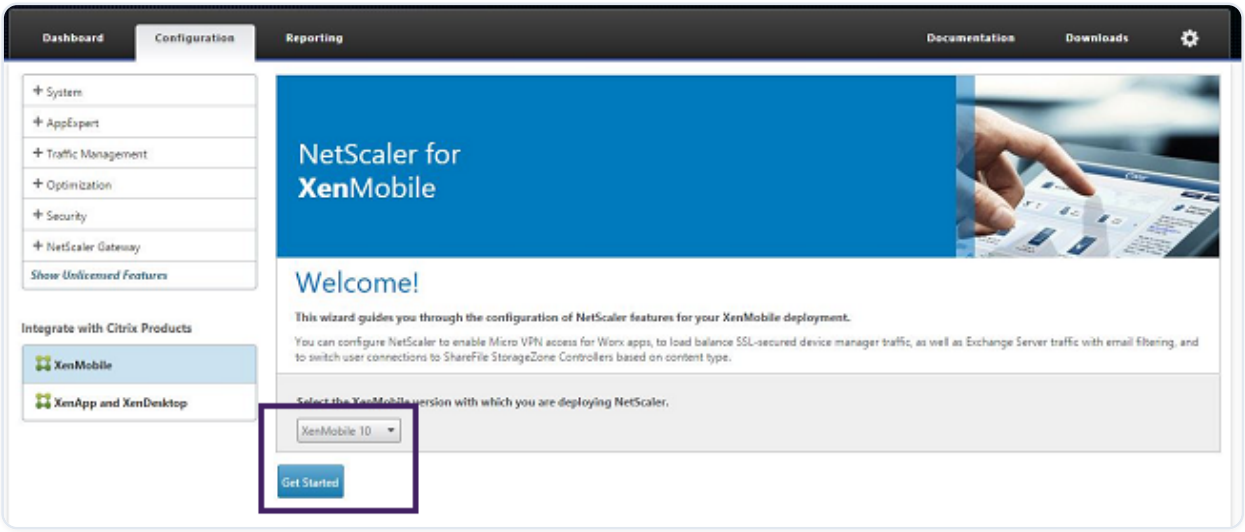


Você pode adicionar outros nós seguindo os mesmos passos. O primeiro nó adicionado ao cluster tem a Função de **OLDEST**. Os nós adicionados depois disso mostram a Função de **NONE** ou **null**.

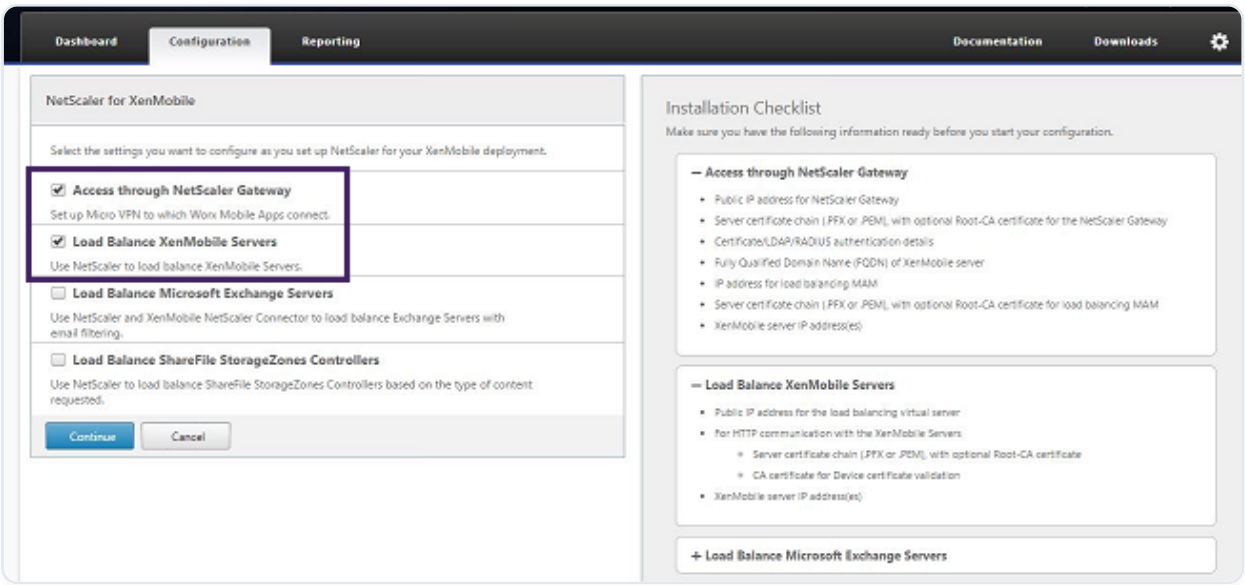
Para configurar o balanceamento de carga para o cluster XenMobile no Citrix ADC

Depois de adicionar os nós necessários como membros do cluster XenMobile, balanceie a carga dos nós para que você possa acessar os clusters. O balanceamento de carga é feito executando o Assistente XenMobile disponível no Citrix ADC. As etapas a seguir descrevem como balancear a carga do XenMobile executando o assistente.

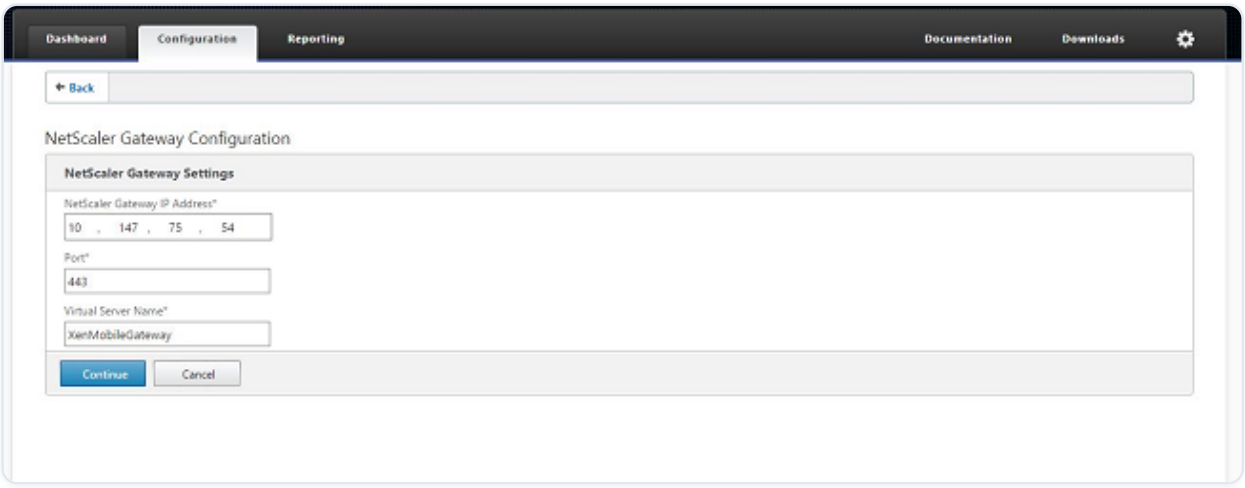
1. Faça logon em Citrix ADC.
2. Na guia Configuração, clique em **XenMobile** e depois clique em **Introdução**.



3. Selecione a caixa de seleção **Acesso via Citrix Gateway** e a caixa de seleção **Balancear Carga dos Servidores XenMobile** e depois clique em **Continuar**.



4. Insira o endereço IP para Citrix Gateway e depois clique em **Continuar**.

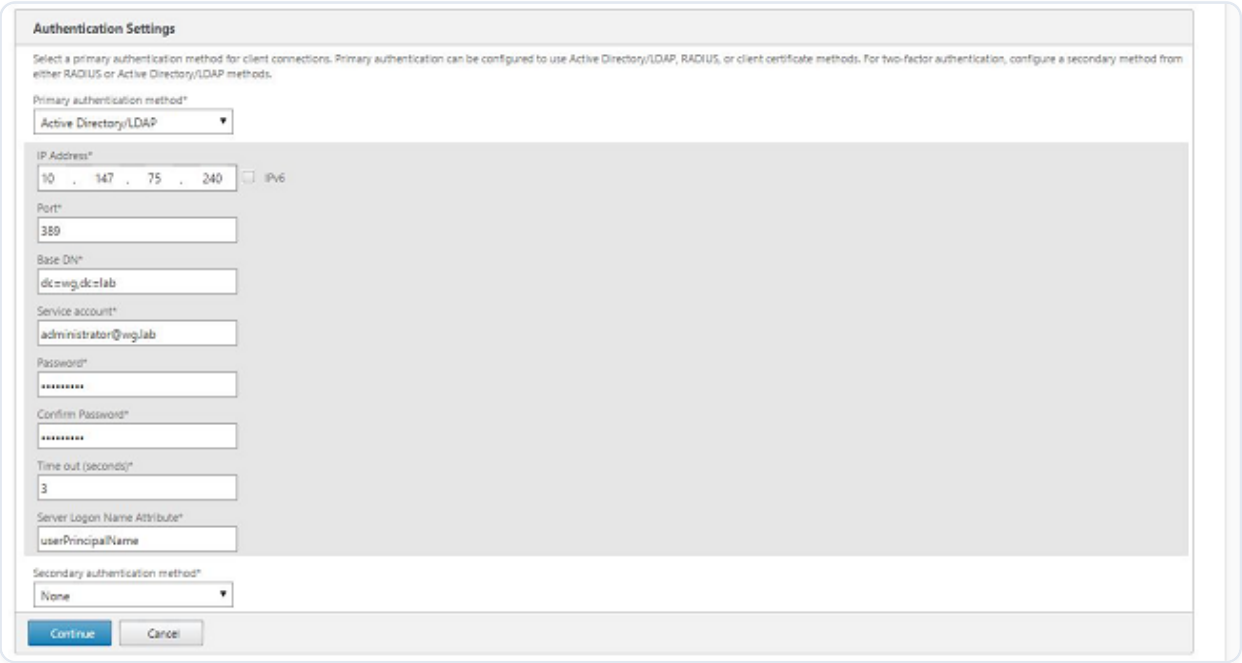


5. Vincule o certificado do servidor ao endereço IP virtual do Citrix Gateway fazendo um dos seguintes e depois clique em **Continuar**.

   - Em **Usar certificado existente**, escolha o certificado do servidor na lista.
   - Clique na guia **Instalar Certificado** para carregar um novo certificado de servidor.



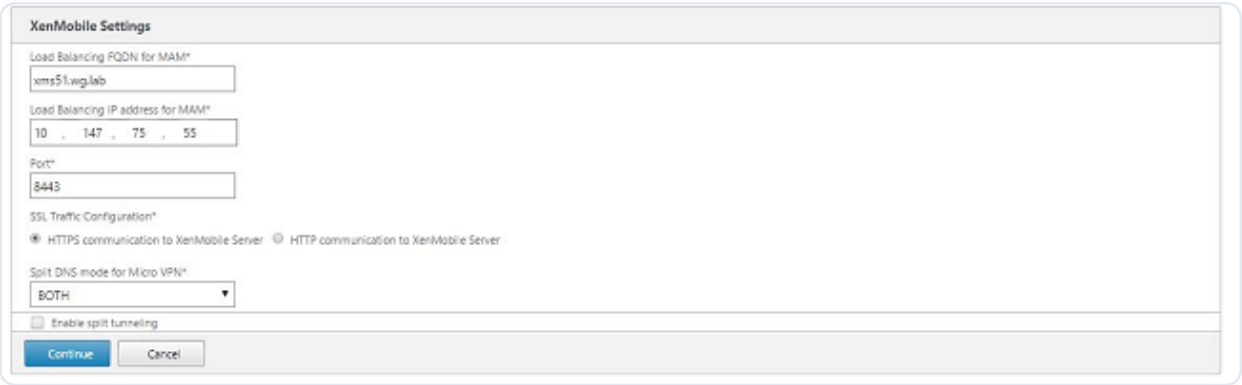
6. Insira os detalhes do servidor de Autenticação e depois clique em **Continuar**.



Nota:

Certifique-se de que o Atributo de Nome de Logon do Servidor seja o mesmo que você forneceu na configuração LDAP do XenMobile.

7. Em configurações do XenMobile, insira o FQDN de Balanceamento de Carga para MAM e clique em **Continuar**.



Nota:

Certifique-se de que o FQDN do endereço IP virtual de balanceamento de carga MAM e o FQDN do XenMobile sejam os mesmos.

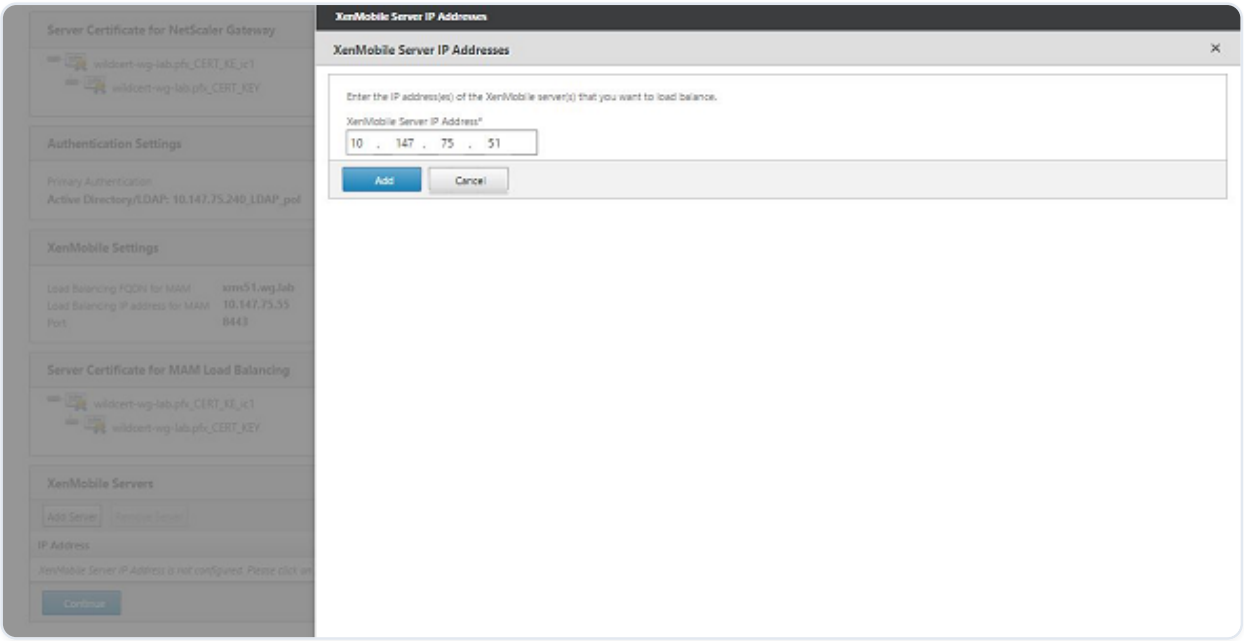
8. Se você quiser usar o modo SSL Bridge (HTTPS), selecione **Comunicação HTTPS para o XenMobile Server**. No entanto, se você quiser usar o descarregamento SSL, selecione **Comunicação HTTP para o XenMobile Server**, conforme mostrado na figura anterior. Para os propósitos deste artigo, a escolha é o modo SSL Bridge (HTTPS).
9. Vincule o certificado do servidor para o endereço IP virtual de balanceamento de carga MAM e clique em Continuar.



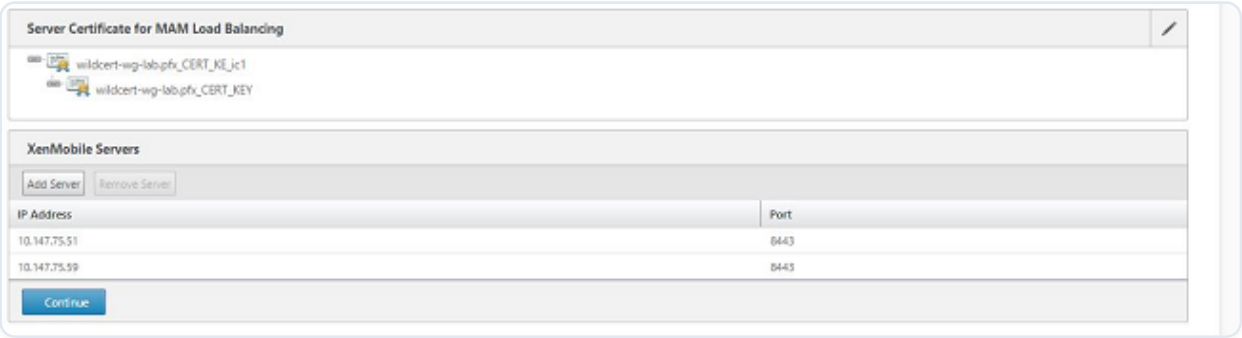
10. Em Servidores XenMobile, clique em **Adicionar Servidor** para adicionar os nós do XenMobile.



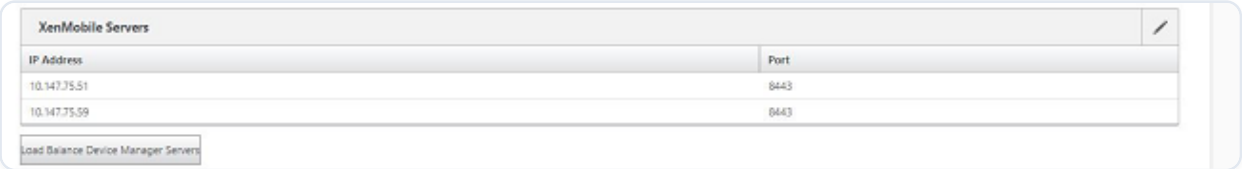
11. Insira o endereço IP do nó do XenMobile e clique em Adicionar.



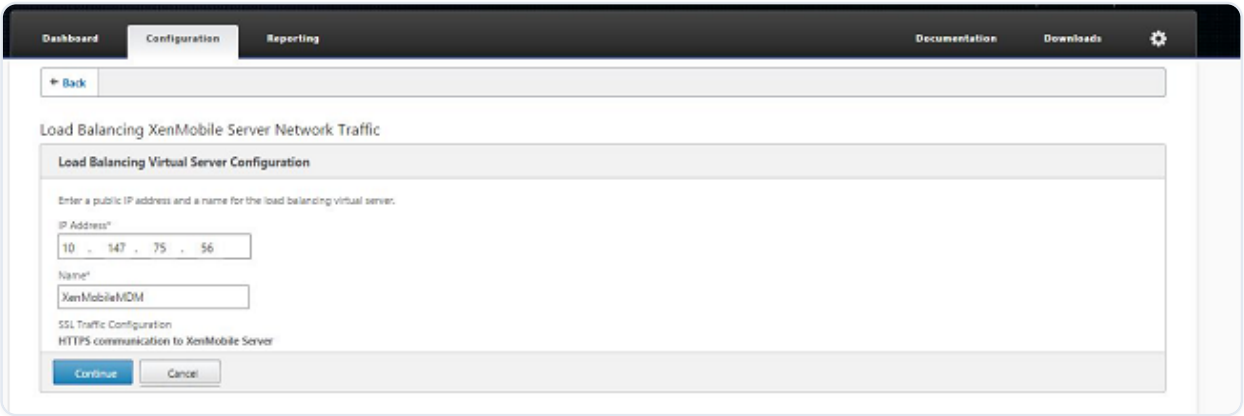
12. Repita as etapas 10 e 11 para adicionar mais nós do XenMobile que fazem parte do cluster XenMobile. Você verá todos os nós do XenMobile que adicionou. Clique em Continuar.



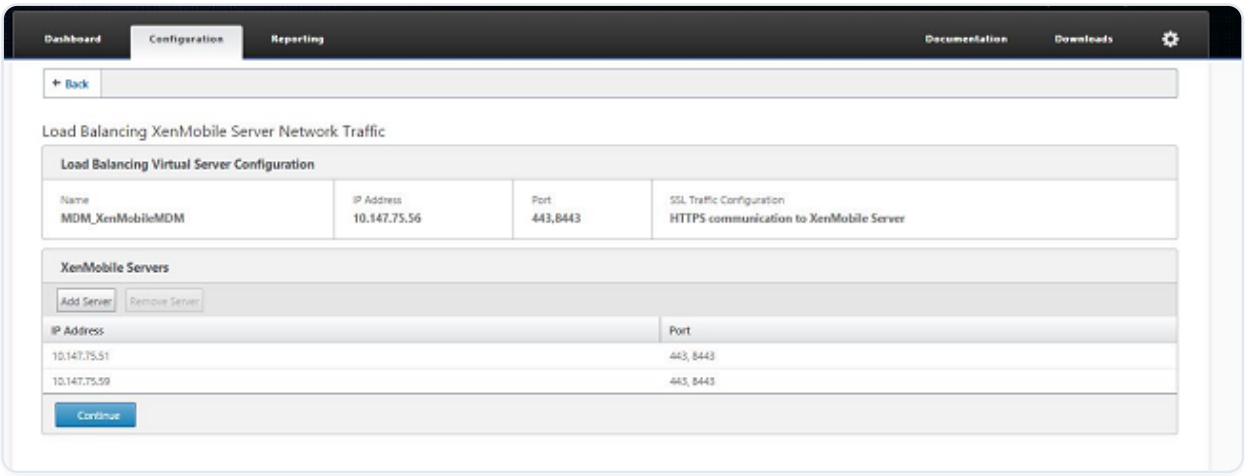
13. Clique em **Balancear Carga dos Servidores do Gerenciador de Dispositivos** para continuar com a configuração de balanceamento de carga MDM.



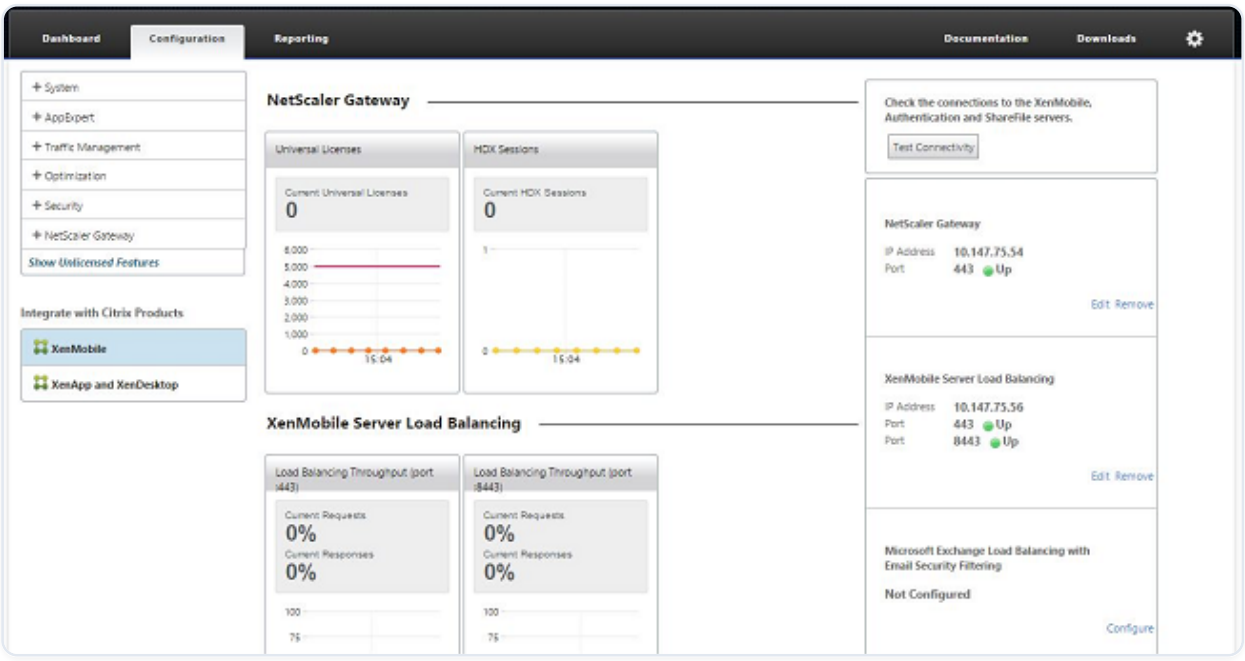
14. Insira o endereço IP a ser usado para o endereço IP de balanceamento de carga MDM e clique em **Continuar**.



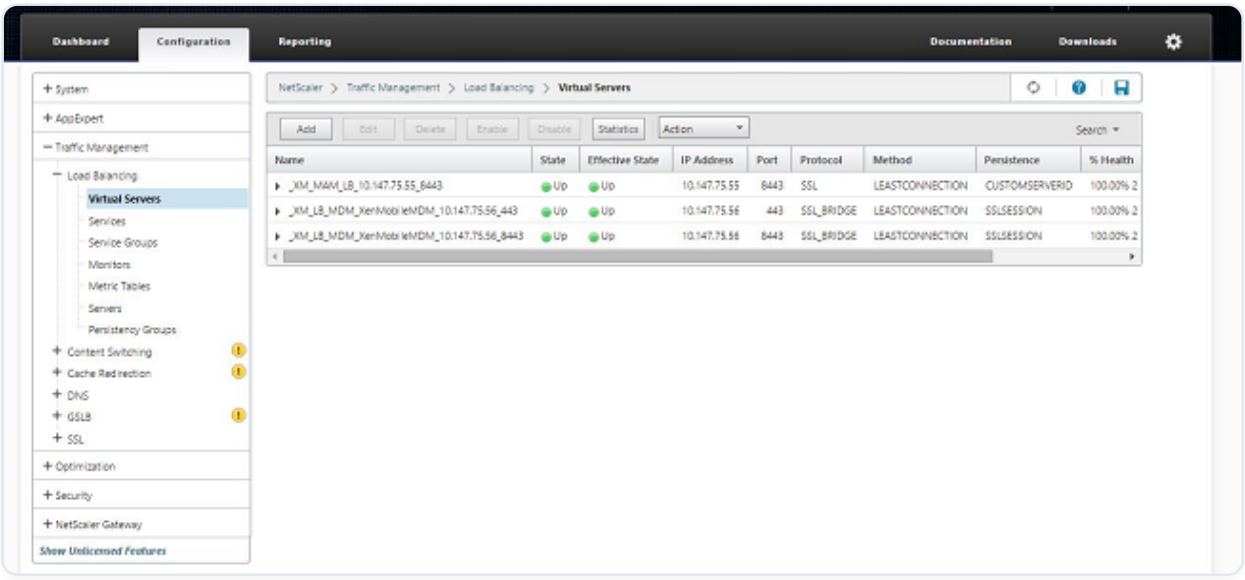
15. Uma vez que você veja os nós do XenMobile na lista, clique em **Continuar** e então clique em Concluído para finalizar o processo.



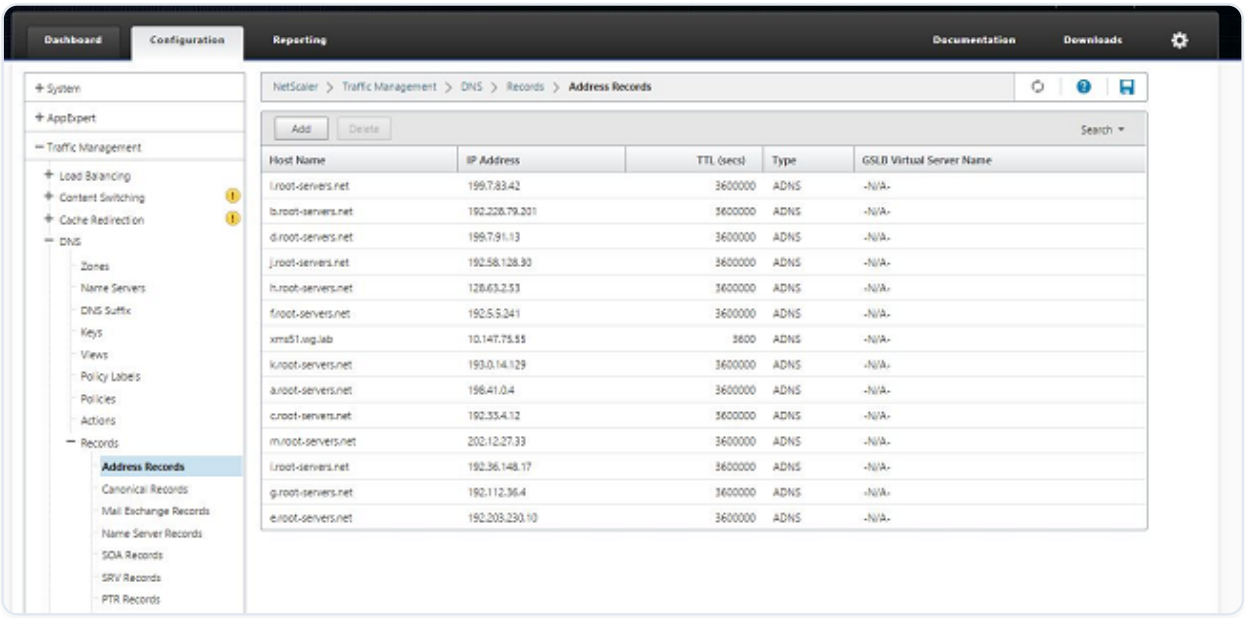
Você verá o status do endereço IP virtual na página do XenMobile.



16. Para confirmar se os endereços IP virtuais estão ativos e funcionando, clique na guia Configuração e então navegar para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores Virtuais**.



Você também verá que a entrada DNS no Citrix ADC aponta para o endereço IP virtual de balanceamento de carga do MAM.



Guia de recuperação de desastres

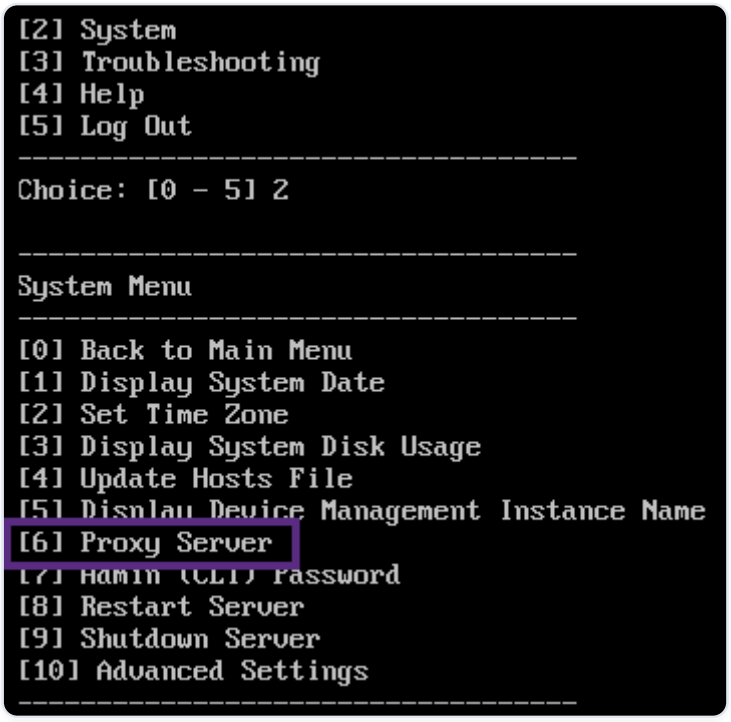
Você pode arquitetar e configurar implantações do XenMobile que incluem vários sites para recuperação de desastres usando uma estratégia de failover ativo-passivo. Para obter detalhes, consulte o Manual de Implantação do XenMobile, artigo Recuperação de Desastres.

Habilitar servidores proxy

Para controlar o tráfego de internet de saída, você pode configurar um servidor proxy no XenMobile® para transportar esse tráfego. Você configura um servidor proxy através da interface

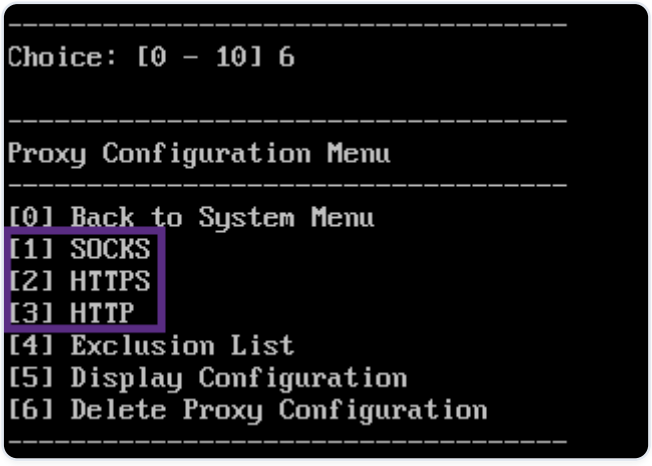
de linha de comando (CLI). A configuração do servidor proxy requer a reinicialização do seu sistema.

1. No menu principal da CLI do XenMobile, digite **2** para selecionar o menu Sistema.
2. No menu Sistema, digite **6** para selecionar o menu Servidor Proxy.



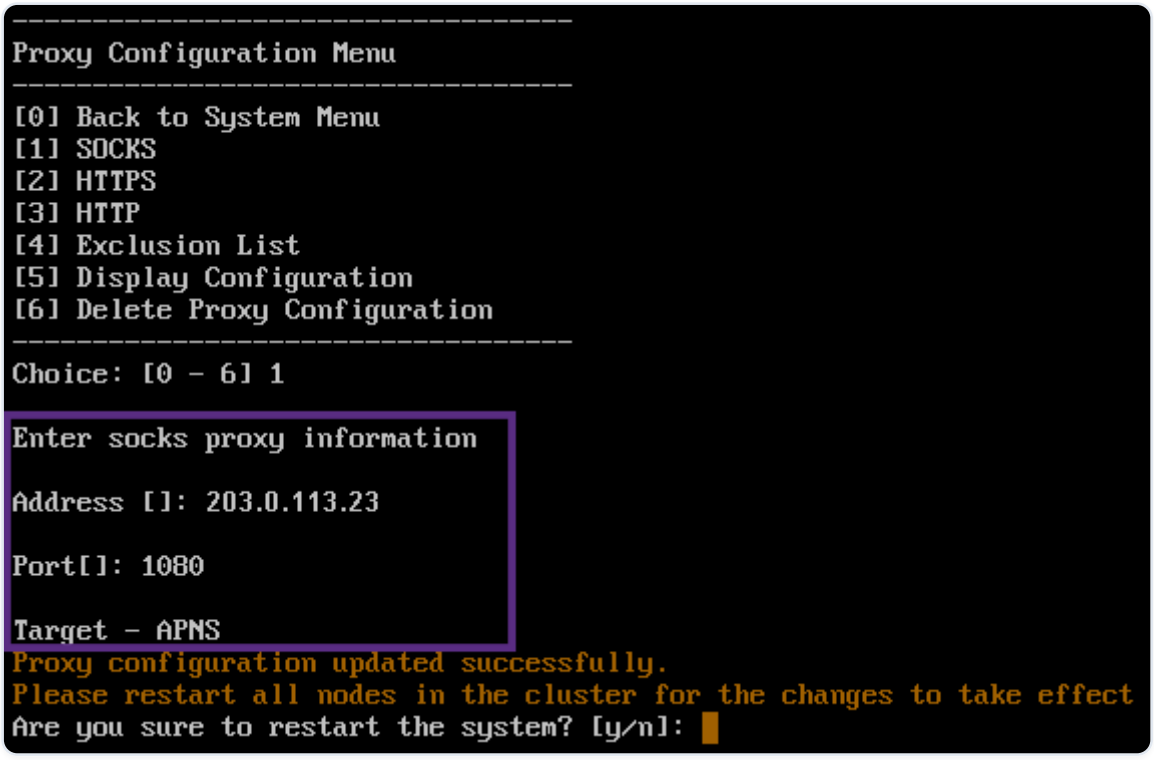
3. No menu Configuração de Proxy, digite **1** para selecionar SOCKS.

   Antes de salvar esta configuração, você também deve configurar o HTTPS. O proxy funciona somente se você salvar as configurações de SOCKS e HTTPS na mesma configuração.

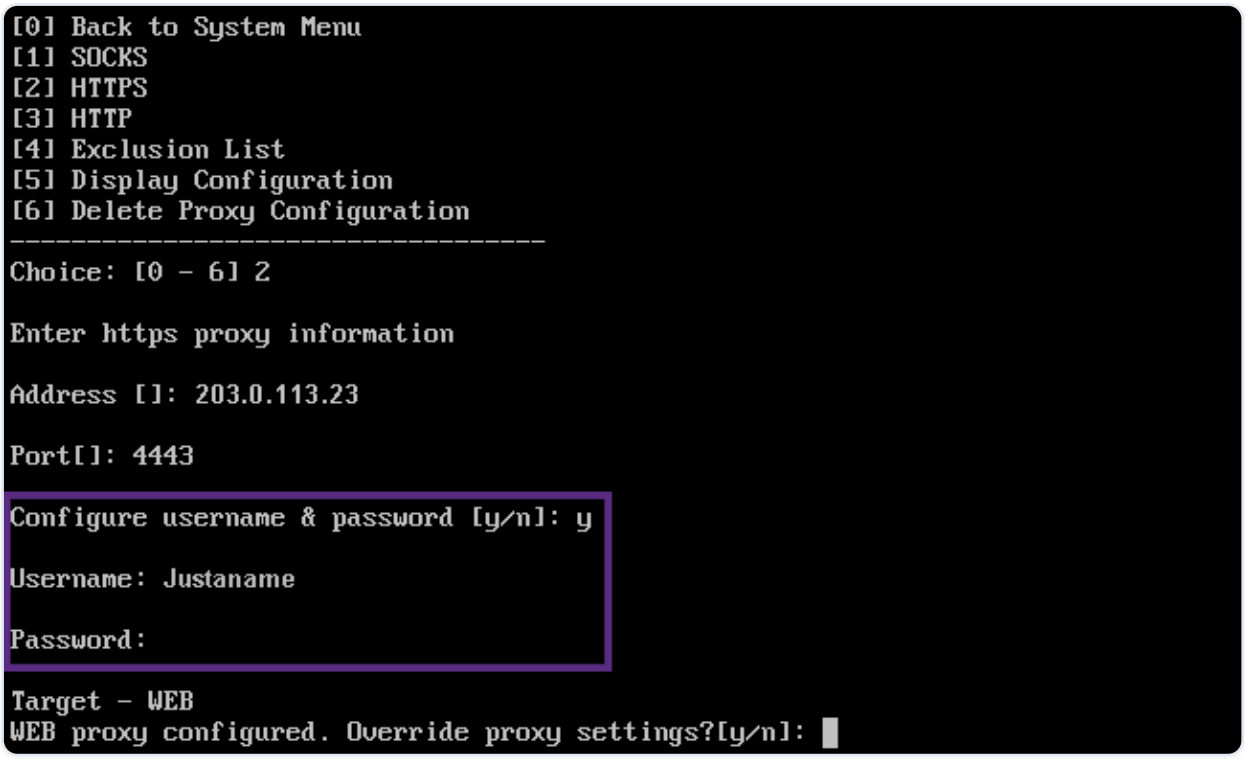


4. Digite o endereço IP do seu servidor proxy, o número da porta e o destino. Consulte a tabela a seguir para ver os tipos de destino suportados para cada tipo de servidor proxy.

Tipo de proxy	Destinos suportados
SOCKS	APNS
HTTP	APNS, Web, PKI
HTTPS	Web, PKI
HTTP com autenticação	Web, PKI
HTTPS com autenticação	Web, PKI



5. Digite **n** e depois digite **2** para selecionar HTTPS.
6. Digite o endereço IP do seu servidor proxy, o número da porta e o destino.
7. Se você optar por configurar um nome de usuário e senha para autenticação no seu servidor proxy, digite **y** e, em seguida, digite o nome de usuário e a senha.



8. Digite **y** para salvar a configuração.

Configurar SQL Server

Para conexões com o SQL Server a partir de um XenMobile® Server local, você pode usar qualquer um dos seguintes drivers:

- O driver padrão
- jTDS
- Driver Microsoft Java Database Connectivity (JDBC)

O driver jTDS é o driver padrão quando você:

- Instala o XenMobile Server localmente.
- Atualiza a partir de um XenMobile Server configurado para usar o driver jTDS.

Para ambos os drivers, o XenMobile oferece suporte à autenticação do SQL Server ou à autenticação do Windows. Para essas combinações de autenticação e driver, o SSL pode estar ativado ou desativado.

Quando você usa a autenticação do Windows com o driver Microsoft JDBC, o driver usa a autenticação integrada com o Kerberos. O XenMobile entra em contato com o Kerberos para obter os detalhes do Centro de Distribuição de Chaves (KDC) do Kerberos. Se os detalhes necessários

não estiverem disponíveis, a CLI do XenMobile solicitará o endereço IP do servidor Active Directory.

Para alternar do driver jTDS para o driver JDBC, faça SSH em todos os seus nós do XenMobile Server e use a CLI do XenMobile para configuração. As etapas variam de acordo com sua configuração atual do driver jTDS, conforme segue.

Alternar para Microsoft JDBC (autenticação do SQL Server)

Para concluir estas etapas, você precisa do nome de usuário e da senha do SQL Server.

1. Faça SSH em todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o **Menu do Sistema**.
3. Digite **12** para selecionar Configurações Avançadas.
4. Digite **7** para selecionar Alternar driver JDBC e, em seguida, digite **m** para Microsoft.

   Imagem de escolha do driver JDBC(/en-us/xenmobile/server/media/cli-choose-jdbc-driver.png)
5. Quando solicitado, digite **y** para escolher a autenticação SQL e, em seguida, digite o nome de usuário e a senha do SQL Server.
6. Repita as etapas para cada nó do XenMobile Server.
7. Reinicie cada nó do XenMobile Server.

Alternar para Microsoft JDBC (SSL desativado; autenticação Windows)

Para concluir estas etapas, você precisa do nome de usuário e senha do Active Directory, do realm KDC do Kerberos e do nome de usuário KDC.

1. Conecte-se via SSH a todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o **Menu do Sistema**.
3. Digite **12** para selecionar Configurações Avançadas.
4. Digite **7** para selecionar Alternar driver JDBC e, em seguida, digite **m**.
5. Quando perguntado se deseja usar a autenticação do SQL Server, digite **n**.
6. Quando solicitado, digite o nome de usuário e a senha do Active Directory configurados para o servidor SQL.
7. Se o XenMobile não descobrir automaticamente o realm KDC do Kerberos, ele solicitará os detalhes do KDC, incluindo o FQDN do servidor SQL.

8. Quando solicitado se deve usar SSL, digite **n**. O XenMobile salva a configuração. Se o XenMobile não conseguir salvar a configuração devido a erros, ele mostrará uma mensagem de erro e os detalhes que você inseriu.
9. Repita as etapas para cada nó do XenMobile Server.
10. Reinicie cada nó do XenMobile Server.

Para alterar a senha do banco de dados do XenMobile

Siga estas orientações para alterar a senha do banco de dados do XenMobile, como quando o Suporte Citrix o instrui a fazer uma alteração de senha.

Se o seu servidor SQL usar autenticação do Windows, faça as alterações de senha do banco de dados no Windows Active Directory. Em seguida, atualize a conta do administrador do banco de dados no servidor de banco de dados para sincronizar a alteração da senha. Você pode então alterar a senha no XenMobile, da seguinte forma.

> **Importante:**
>
> - Planeje uma janela de manutenção programada para alterar a senha do banco de dados no XenMobile. Uma alteração de senha deve ocorrer durante o tempo de inatividade do sistema.
> - Ao alterar a senha, certifique-se de que todos os nós do XenMobile estejam conectados à rede. Depois de alterar a senha, reinicie o XenMobile.
>
>   Se você não reiniciar o XenMobile após uma alteração de senha, o XenMobile entrará no modo de recuperação. Nesse caso, reverta para a senha antiga no servidor SQL, reinicie o XenMobile e altere a senha novamente.

1. Verifique se todos os nós do XenMobile Server estão em execução. Para um ambiente em cluster, ative todos os nós.
2. Bloqueie o tráfego de dispositivos de entrada para o XenMobile no balanceador de carga do Citrix ADC desativando o servidor virtual.
3. Para alterar a senha do banco de dados em um servidor SQL: Faça login na CLI do XenMobile, navegar para **Configuration > Database** e insira a senha alterada quando solicitado:

```
Server []: <ipAddress>

Port [1433]: 1433

Username [sa]: <userName>

Password: <****>
```

4. Escolha **Y** para reiniciar o servidor.
5. Repita as etapas 3 e 4 para todos os outros nós no cluster.
6. Desbloqueie o tráfego de dispositivo de entrada ativando o servidor virtual no balanceador de carga Citrix ADC.

Propriedades do servidor

O XenMobile® possui muitas propriedades que se aplicam a operações em todo o servidor. Este artigo descreve muitas das propriedades do servidor e detalha como adicionar, editar ou excluir propriedades do servidor.

Algumas propriedades são Chaves Personalizadas. Para adicionar uma chave personalizada, clique em **Adicionar** e, em seguida, em **Chave**, escolha **Chave Personalizada**.

Para obter informações sobre as propriedades tipicamente configuradas, consulte Propriedades do Servidor no manual virtual do XenMobile.

Definições de Propriedades do Servidor

Adicionar Dispositivo Sempre

- Se **true**, o XenMobile adiciona um dispositivo ao console do XenMobile, mesmo que a inscrição falhe, para que você possa ver quais dispositivos tentaram se inscrever. O padrão é **false**.

Intervalo de Limitação de Emissão de Certificado de Cliente AG

- O período de carência entre a geração de certificados. Este intervalo impede que o XenMobile gere vários certificados para um dispositivo em um curto período de tempo. A Citrix® recomenda que você não altere este valor. O padrão é **30** minutos.

Hora de Execução da Limpeza do Log de Auditoria

- A hora para iniciar a limpeza do log de auditoria, formatada como HH:MM AM/PM. Exemplo: 04:00 AM. O padrão é **02:00 AM**.

Intervalo de Limpeza do Log de Auditoria (em Dias)

- O número de dias que o XenMobile retém o log de auditoria. O padrão é **1**.

Registrador de Auditoria

- Se **False**, não registra eventos da interface do usuário (UI). O padrão é **False**.

Retenção do Log de Auditoria (em Dias)

- O número de dias que o XenMobile retém o log de auditoria. O padrão é **7**.

auth.ldap.connect.timeout e auth.ldap.read.timeout

- Para compensar respostas lentas do LDAP, a Citrix recomenda que você adicione propriedades de servidor para as seguintes Chaves Personalizadas.
    - Chave: **Chave Personalizada**
    - Chave: **auth.ldap.connect.timeout**
    - Valor: **60000**
    - Nome de Exibição: **auth.ldap.connect.timeout**
    - Descrição: **Tempo limite de conexão LDAP**
    - Chave: **Chave Personalizada**
    - Chave: **auth.ldap.read.timeout**
    - Valor: **60000**
    - Nome de Exibição: **auth.ldap.read.timeout**
    - Descrição: **Tempo limite de leitura LDAP**

Renovação de Certificado em Segundos

- O número de segundos antes que um certificado expire para que o XenMobile comece a renovar certificados. Por exemplo, se um certificado expirar em 30 de dezembro e esta propriedade estiver definida para 30 dias: Se o dispositivo se conectar entre 1º de dezembro e 30 de dezembro, o XenMobile tentará renovar o certificado. O padrão é **2592000** segundos (30 dias).

Tempo Limite de Conexão

- O tempo limite de inatividade da sessão, em minutos, após o qual o XenMobile fecha a conexão TCP com um dispositivo. A sessão permanece aberta. Aplica-se a dispositivos Android e Suporte Remoto. O padrão é **5** minutos.

Tempo Limite de Conexão com o Servidor de Certificação Microsoft

- O número de segundos que o XenMobile aguarda por uma resposta do servidor de certificados. Se o servidor de certificados estiver lento e com muito tráfego, aumente este valor para 60 segundos ou mais. Um servidor de certificados que não responde após 120 segundos requer manutenção. O padrão é **15000** milissegundos (15 segundos).

Canal de implantação padrão

- Determina como o XenMobile implanta um recurso em um dispositivo: No nível do usuário (**DEFAULT_TO_USER**) ou no nível do dispositivo. O padrão é **DEFAULT_TO_DEVICE**.

Limpeza de Log de Implantação (em Dias)

- O número de dias que o XenMobile mantém o log de implantação. O padrão é **7**.

Desabilitar Verificação de Nome de Host

- Por padrão, a verificação de nome de host está habilitada em conexões de saída, exceto para o servidor PKI da Microsoft. Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar ao servidor de compra por volume: O nome de host '192.0.2.0' não corresponde ao assunto do certificado fornecido pelo par”. Se a verificação de nome de host interromper sua implantação, altere esta propriedade para **true**. O padrão é **false**.

Desabilitar Verificação de Servidor SSL

- Se **True**, desabilita a validação do certificado do servidor SSL quando todas as seguintes condições forem atendidas:
  - Você habilitou a autenticação baseada em certificado no seu XenMobile Server.
  - O servidor CA da Microsoft é o emissor do certificado.
  - Uma CA interna, cuja raiz o XenMobile Server não confia, assinou seu certificado.

O padrão é **True**.

Habilitar Console

- Se **true**, habilita o acesso do usuário ao Console do Portal de Autoatendimento. O padrão é **true**.

Habilitar Relatório de Falhas

- Se **true**, a Citrix coleta relatórios de falhas e diagnósticos para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se **false**, nenhum dado é coletado. O valor padrão é **true**.

Habilitar/Desabilitar o registro de estatísticas do Hibernate para diagnósticos

- Se **True**, habilita o registro de estatísticas do Hibernate para auxiliar na solução de problemas de desempenho do aplicativo. Hibernate é um componente usado para conexões do XenMobile com o Microsoft SQL Server. Por padrão, o registro está desabilitado porque afeta o desempenho do aplicativo. Habilite o registro apenas por um curto período para evitar a criação de um arquivo de log enorme. O XenMobile grava os logs em /opt/sas/logs/hibernate_stats.log. O padrão é **False**.

Habilitar OTAE do macOS

- Se **false**, impede o uso de um link de registro para dispositivos macOS, o que significa que os usuários de macOS podem se registrar apenas usando um convite de registro. O padrão é **true**.

Habilitar Gatilho de Notificação

- Habilita ou desabilita as notificações do cliente Secure Hub. O valor **true** habilita as notificações. O padrão é **true**.

force.server.push.required.apps

- Habilita a implantação forçada de aplicativos obrigatórios em dispositivos Android e iOS em situações como as seguintes:
  - Você carrega um novo aplicativo e o marca como obrigatório.
  - Você marca um aplicativo existente como obrigatório.
  - Quando o usuário exclui um aplicativo obrigatório.
  - Uma atualização do Secure Hub está disponível.

A implantação forçada de aplicativos obrigatórios é **false** por padrão. Crie a chave personalizada e defina **Valor** como **true** para habilitar a implantação forçada. Durante a implantação forçada, os aplicativos obrigatórios habilitados para MDX, incluindo aplicativos empresariais e aplicativos de loja de aplicativos públicos, são atualizados imediatamente. A atualização ocorre mesmo se você configurar uma política MDX para um período de carência de atualização de aplicativo e o usuário optar por atualizar o aplicativo mais tarde.

- Chave: **Chave Personalizada**
- Chave: **force.server.push.required.apps**
- Valor: **false**
- Nome de Exibição: **force.server.push.required.apps**
- Descrição: **Forçar a implantação de aplicativos obrigatórios**

Extração Completa de Usuários Permitidos e Negados do ActiveSync

- O intervalo (em segundos) em que o XenMobile extrai uma lista completa (linha de base) de usuários permitidos e negados do ActiveSync. O padrão é **28800** segundos.

hibernate.c3p0.idle_test_period

- Esta propriedade do XenMobile Server, uma Chave Personalizada, determina o tempo ocioso em segundos antes que uma conexão seja automaticamente validada. Configure a chave da seguinte forma. O padrão é **30**.
- Chave: **Chave Personalizada**
- Chave: **hibernate.c3p0. idle_test_period**
- Valor: **30**
- Nome de Exibição: **hibernate.c3p0. idle_test_period =*nnn***
- Descrição: **Período de teste de inatividade do Hibernate**

hibernate.c3p0.max_size

- Esta Chave Personalizada determina o número máximo de conexões que o XenMobile pode abrir para o banco de dados do SQL Server. O XenMobile usa o valor que você especifica para esta chave personalizada como um limite superior. As conexões são abertas apenas se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados. Para obter mais informações, consulte Ajustando Operações do XenMobile. Configure a chave da seguinte forma. O padrão é **1000**.
- Chave: **hibernate.c3p0.max_size**

- Valor: **1000**
- Nome de Exibição: **hibernate.c3p0.max_size**
- Descrição: **Conexões de BD ao SQL**

hibernate.c3p0.min_size

- Esta Chave Personalizada determina o número mínimo de conexões que o XenMobile abre para o banco de dados do SQL Server. Configure a chave da seguinte forma. O padrão é **100**.
- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de Exibição: **hibernate.c3p0.min_size**
- Descrição: **Conexões de BD ao SQL**

hibernate.c3p0.timeout

- Esta Chave Personalizada determina o tempo limite de inatividade, em segundos. O padrão é **120**.
- Chave: **Chave Personalizada**
- Chave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nome de Exibição: **hibernate.c3p0.timeout**
- Descrição: **Tempo limite de inatividade do banco de dados**

Identifica se a telemetria está ativada ou não

- Identifica se a telemetria (Programa de Melhoria da Experiência do Cliente, ou CEIP) está ativada. Você pode optar por participar do CEIP ao instalar ou atualizar o XenMobile. Se o XenMobile tiver 15 uploads falhos consecutivos, ele desativa a telemetria. O padrão é **false**.

Tempo Limite de Inatividade em Minutos

- Se a propriedade de servidor **WebServices timeout type** for **INACTIVITY_TIMEOUT**: Esta propriedade define o número de minutos após os quais o XenMobile desconecta um administrador inativo que fez o seguinte:
  - Usou a API Pública do XenMobile para Serviços REST para acessar o console do XenMobile

- Usou a API Pública do XenMobile para Serviços REST para acessar qualquer aplicativo de terceiros. Um tempo limite de **0** significa que um usuário inativo ainda está conectado.

O padrão é **5**.

Instalação Automática de Registro de Gerenciamento de Dispositivos iOS Ativada

- Se verdadeiro, esta propriedade reduz a quantidade de interação do usuário necessária durante o registro do dispositivo. Os usuários devem clicar em **Instalar CA Raiz** (se necessário) e **Instalar Perfil MDM**.

Atraso na Primeira Etapa do Registro de Gerenciamento de Dispositivos iOS

- Depois que um usuário insere suas credenciais durante o registro do dispositivo, este valor especifica quanto tempo esperar antes de solicitar a CA raiz. A Citrix recomenda que você edite esta propriedade apenas para problemas de latência ou velocidade da rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

Atraso na Última Etapa do Registro de Gerenciamento de Dispositivos iOS

- Durante o registro do dispositivo, este valor de propriedade especifica o tempo de espera entre a instalação do perfil MDM e o início do Agente no dispositivo. A Citrix recomenda que você edite esta propriedade apenas para problemas de latência ou velocidade da rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

Modo de Entrega de Identidade de Gerenciamento de Dispositivos iOS

- Especifica se o XenMobile distribui o certificado MDM para dispositivos usando **SCEP** (recomendado por motivos de segurança) ou **PKCS12**. No modo PKCS12, o par de chaves é gerado no servidor e nenhuma negociação é feita. O padrão é **SCEP**.

Tamanho da Chave de Identidade de Gerenciamento de Dispositivos iOS

- Define o tamanho das chaves privadas para identidades MDM, serviço de perfil iOS e identidades de agente iOS do XenMobile. O padrão é **1024**.

Dias para Renovação da Identidade de Gerenciamento de Dispositivos iOS

- Especifica o número de dias antes da expiração do certificado em que o XenMobile começa a renovar os certificados. Por exemplo: Se um certificado expirar em 10 dias e esta propriedade

for de **10** dias, quando um dispositivo se conectar 9 dias antes da expiração, o XenMobile emitirá um novo certificado. O padrão é **30** dias.

Senha da Chave Privada APNS do MDM iOS

- Esta propriedade contém a senha APNs que é necessária para o XenMobile enviar notificações para os servidores da Apple.

Duração da Inatividade Antes que o Dispositivo Seja Desconectado

- Especifica por quanto tempo um dispositivo pode permanecer inativo, incluindo a última autenticação, antes que o XenMobile o desconecte. O padrão é **7** dias.

Máximo de Dispositivos Somente MAM

- Esta Chave Personalizada limita o número de dispositivos somente MAM que cada usuário pode registrar. Configure a chave da seguinte forma. Um **Valor** de **0** permite registros ilimitados de dispositivos.
- Chave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nome de exibição = **MAM Only Device Max**
- Descrição = **Limita o número de dispositivos MAM que cada usuário pode registrar.**

MaxNumberOfWorker

- O número de threads usados ao importar muitas licenças de compra por volume. O padrão é **3**. Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, com um número maior de threads, como 6, uma importação de compra por volume resulta em alto uso da CPU.

Logon Único do Citrix ADC

- Se **False**, desabilita o recurso de retorno de chamada do XenMobile durante o logon único do Citrix ADC para o XenMobile. Se a configuração do Citrix Gateway incluir uma URL de retorno de chamada, o XenMobile usará o recurso de retorno de chamada para verificar o ID da sessão do Citrix Gateway. O padrão é **False**.

Número de uploads falhos consecutivos

- Exibe o número de falhas consecutivas durante os uploads do Programa de Melhoria da Experiência do Cliente (CEIP). O XenMobile incrementa o valor quando um upload falha. Após 15 falhas de upload, o XenMobile desabilita o CEIP, também chamado de telemetria. Para

obter mais informações, consulte a propriedade do servidor **Identifies if telemetry is enabled or not**. O XenMobile redefine o valor para **0** quando um upload é bem-sucedido.

Número de Usuários Por Dispositivo

- O número máximo de usuários que podem registrar o mesmo dispositivo no MDM. O valor **0** significa que um número ilimitado de usuários pode registrar o mesmo dispositivo. O padrão é **0**.

Extração de Alteração Incremental de Usuários Permitidos e Negados

- O número de segundos que o XenMobile aguarda por uma resposta do domínio ao executar um comando PowerShell para obter um delta de dispositivos ActiveSync. O padrão é **60** segundos.

Tempo Limite de Leitura para o Servidor de Certificação da Microsoft

- O número de segundos que o XenMobile aguarda por uma resposta do servidor de certificados ao fazer uma leitura. Se o servidor de certificados estiver lento e com muito tráfego, você pode aumentar este valor para 60 segundos ou mais. Um servidor de certificados que não responde após 120 segundos requer manutenção. O padrão é **15000** milissegundos (15 segundos).

Serviços Web REST

- Habilita o Serviço Web REST. O padrão é **true**.

Recupera informações de dispositivos em blocos de tamanho especificado

- Este valor é usado internamente para multithreading durante as exportações de dispositivos. Se o valor for maior, um único thread analisa mais dispositivos. Se o valor for menor, mais threads buscam os dispositivos. Reduzir o valor pode aumentar o desempenho das exportações e das buscas de lista de dispositivos, mas pode reduzir a memória disponível. O padrão é **1000**.

Limpeza do Log de Sessão (em Dias)

- O número de dias que o XenMobile mantém o log de sessão. O padrão é **7**.

Modo do Servidor

- Determina se o XenMobile é executado nos modos MAM, MDM ou ENT (empresa), correspondendo a gerenciamento de aplicativos, gerenciamento de dispositivos ou gerenciamento de aplicativos e dispositivos. Defina a propriedade Modo do Servidor de acordo

com a forma como você deseja que os dispositivos se registrem, conforme observado na tabela a seguir. O Modo do Servidor padrão é **ENT**, independentemente do tipo de licença.

Se você tiver uma licença XenMobile MDM Edition, o modo de servidor efetivo será sempre MDM, independentemente de como você definir o modo de servidor em **Propriedades do Servidor**. Se você tiver uma licença MDM Edition, não poderá habilitar o gerenciamento de aplicativos definindo o modo de servidor como MAM ou ENT.

Suas licenças são desta Edição	**Você deseja que os dispositivos se registrem neste modo**	**Defina a propriedade Modo do Servidor como**
Enterprise / Avançado	Modo MDM	MDM
Enterprise / Avançado	Modo MDM+MAM	ENT
MDM	Modo MDM	MDM

O modo de servidor efetivo é uma combinação do tipo de licença e do modo de servidor. Para uma licença MDM, o modo de servidor efetivo é sempre MDM, independentemente da configuração do modo. Para licenças Enterprise e Advanced, o modo de servidor efetivo corresponde ao modo configurado, se este for **ENT** ou **MDM**. Se o modo configurado for **MAM**, o modo de servidor efetivo é ENT.

O XenMobile adiciona o modo de servidor ao log do servidor para cada uma destas atividades: uma licença é ativada, uma licença é excluída e você altera o modo de servidor em **Propriedades do Servidor**. Para obter informações sobre como criar e visualizar arquivos de log, consulte Logs e Visualizar e analisar arquivos de log no XenMobile.

Tipo de configuração do ShareFile

- Especifica o tipo de armazenamento do Citrix Files. **ENTERPRISE** habilita o modo Citrix Files Enterprise. **CONNECTORS** fornece acesso apenas a conectores de zona de armazenamento que você cria através do console do XenMobile. O padrão é **NONE**, que mostra a exibição inicial da tela **Configurar > ShareFile**, onde você escolhe entre Citrix Files Enterprise e Conectores. O padrão é **NONE**.

Tempo limite estático em minutos

- Se a propriedade de servidor **WebServices timeout type** for **STATIC_TIMEOUT**: Esta propriedade define o número de minutos após os quais o XenMobile desconecta um administrador após usar o seguinte:
  - A API Pública do XenMobile para Serviços REST para acessar o console do XenMobile.
  - A API Pública do XenMobile para Serviços REST para acessar qualquer aplicativo de terceiros.

O padrão é **60**.

Supressão de Mensagens do Agente de Gatilho

- Ativa ou desativa as mensagens do cliente Secure Hub. O valor **false** ativa as mensagens. O padrão é **true**.

Supressão de Sons do Agente de Gatilho

- Ativa ou desativa os sons do cliente Secure Hub. O valor **false** ativa os sons. O padrão é **true**.

Download de Aplicativos Não Autenticados para Dispositivos Android

- Se **True**, você pode baixar aplicativos auto-hospedados para dispositivos Android que executam o Android Enterprise. O XenMobile precisa dessa propriedade se a opção do Android Enterprise para fornecer uma URL de download estaticamente na Google Play Store estiver ativada. Nesse caso, as URLs de download não podem incluir um tíquete único (definido pela propriedade do servidor **XAM One-Time Ticket**) que contém o token de autenticação. O padrão é **False**.

Download de Aplicativos Não Autenticados para Dispositivos Windows

- Usado apenas para versões mais antigas do Secure Hub que não validam tíquetes únicos. Se **False**, você pode baixar aplicativos não autenticados do XenMobile para dispositivos Windows. O padrão é **False**.

Usar ID do ActiveSync para Realizar Limpeza de Dispositivo ActiveSync

- Se **true**, o conector do Endpoint Management para Exchange ActiveSync usa o identificador ActiveSync como um argumento para o método asWipeDevice. O padrão é **false**.

Apenas usuários do Exchange

- Se **true**, desativa a autenticação de usuário para usuários do ActiveSync Exchange. O padrão é **false**.

Intervalo de linha de base de VP

- O intervalo mínimo em que o XenMobile reimporta licenças de compra por volume da Apple. A atualização das informações da licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado da compra por volume. Por padrão, o XenMobile atualiza a linha de base da licença de compra por volume no mínimo a cada **720** minutos.

Se você tiver muitas licenças de compra por volume instaladas (por exemplo, mais de 50.000): a Citrix recomenda que você aumente o intervalo da linha de base para reduzir a frequência e a sobrecarga da importação de licenças.

Se você espera alterações frequentes nas licenças de compra por volume da Apple: a Citrix recomenda que você diminua o valor para manter o XenMobile atualizado com as alterações. O intervalo mínimo entre as duas linhas de base é de 60 minutos. Além disso, o XenMobile faz uma importação delta a cada 60 minutos para capturar as alterações desde a última importação. Portanto, se o intervalo da linha de base de compra por volume for de 60 minutos, o intervalo entre as linhas de base poderá ser atrasado em até 119 minutos.

Tipo de tempo limite de WebServices

- Especifica como expirar um token de autenticação recuperado da API pública. Se **STATIC_TIMEOUT**, o XenMobile considera um token de autenticação como expirado após o valor especificado na propriedade do servidor **Static Timeout in Minutes**.

Se **INACTIVITY_TIMEOUT**, o XenMobile considera um token de autenticação como expirado depois que o token fica inativo pelo valor especificado na propriedade do servidor **Inactivity Timeout in Minutes**. O padrão é **STATIC_TIMEOUT**.

Canal WNS do Windows - Número de dias antes da renovação

- A frequência de renovação para o ChannelURI. O padrão é **10** dias.

Intervalo de pulsação do WNS do Windows

- Quanto tempo o XenMobile espera antes de se conectar a um dispositivo depois de se conectar a ele a cada três minutos, cinco vezes. O padrão é **6** horas.

Ticket único XAM

- O número de milissegundos que um token de autenticação único (OTT) é válido para baixar um aplicativo. Esta propriedade e as propriedades **Unauthenticated App download for Android** e **Unauthenticated App download for Windows** funcionam em conjunto. Essas propriedades especificam se devem permitir downloads de aplicativos não autenticados. O padrão é **3600000**.

Intervalo máximo de inatividade do console do Portal de Autoatendimento do XenMobile MDM (minutos)

- O número de minutos após os quais o XenMobile desconecta um usuário inativo do Portal de Autoatendimento do XenMobile. Um tempo limite de **0** significa que um usuário inativo permanece conectado. O padrão é **30**.

Adicionar, Editar ou Excluir Propriedades do Servidor

No XenMobile, você pode aplicar propriedades ao servidor. Após fazer alterações, certifique-se de reiniciar o XenMobile em todos os nós para confirmar e ativar as alterações.

> **Nota:**
>
> Para reiniciar o XenMobile, use o prompt de comando através do seu hipervisor.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Propriedades do Servidor**. A página **Propriedades do Servidor** é exibida. Você pode adicionar, editar ou excluir propriedades do servidor a partir desta página.

   Propriedades do servidor(/en-us/xenmobile/server/media/settings-server-server-properties.png)

Para adicionar uma propriedade de servidor

1. Clique em **Adicionar**. A página **Adicionar Nova Propriedade de Servidor** é exibida.

   Propriedades do servidor(/en-us/xenmobile/server/media/settings-server-server-properties-add.png)
2. Configure estas definições:

- Chave: Na lista, selecione a chave apropriada. As chaves diferenciam maiúsculas de minúsculas. Entre em contato com o Suporte Citrix antes de editar valores de propriedade ou para solicitar uma chave especial.
- Valor: Insira um valor dependendo da chave que você selecionou.
- Nome de Exibição: Insira um nome para o novo valor da propriedade que aparece na tabela **Propriedades do Servidor**.
- Descrição: Opcionalmente, digite uma descrição para a nova propriedade do servidor.

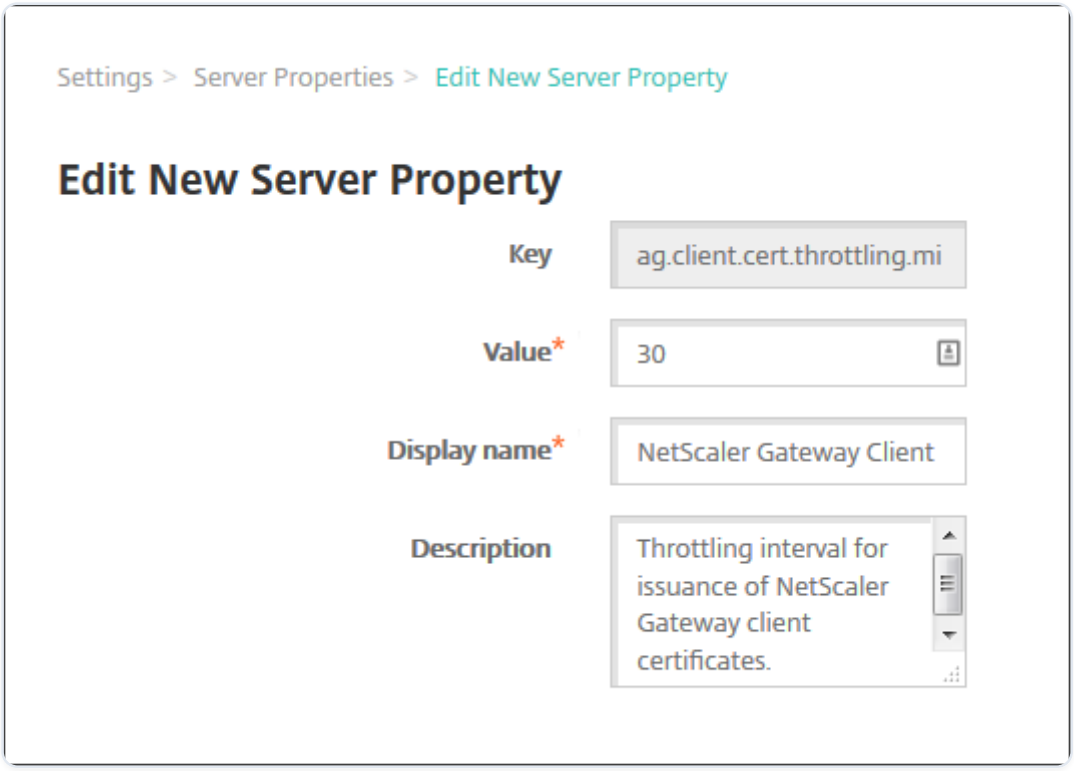
3. Clique em **Salvar**.

Para editar uma propriedade de servidor

1. Na tabela **Propriedades do Servidor**, selecione a propriedade do servidor que você deseja editar.

   Ao selecionar a caixa de seleção ao lado de uma propriedade de servidor, o menu de opções aparece acima da lista de propriedades do servidor. Clique em qualquer outro lugar na lista para abrir o menu de opções no lado direito da listagem.

2. Clique em **Editar**. A página **Editar Nova Propriedade do Servidor** é exibida.



3. Altere as seguintes informações conforme apropriado:

   - Chave: Você não pode alterar este campo.
   - Valor: O valor da propriedade.

- Nome de Exibição: O nome da propriedade.
- Descrição: A descrição da propriedade.

4. Clique em **Salvar** para salvar suas alterações ou **Cancelar** para deixar a propriedade inalterada.

Para excluir uma propriedade de servidor

1. Na tabela **Propriedades do Servidor**, selecione a propriedade do servidor que você deseja excluir.

   Você pode selecionar mais de uma propriedade para excluir selecionando a caixa de seleção ao lado de cada propriedade.

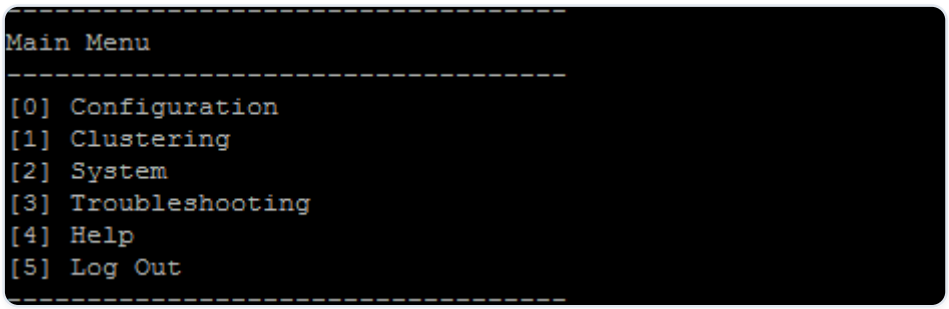
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Opções da interface de linha de comando

Para uma instalação local do XenMobile® Server, você pode acessar as opções da CLI da seguinte forma:

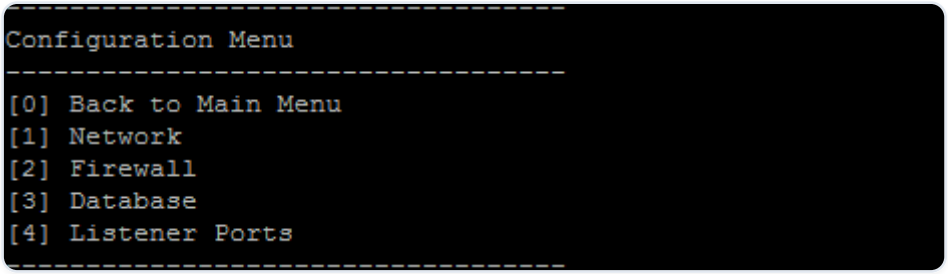
- **Do hipervisor no qual você instalou o XenMobile:** No seu hipervisor, selecione a máquina virtual XenMobile importada, inicie a visualização do prompt de comando e faça login na sua conta de administrador do XenMobile. Para obter detalhes, consulte a documentação do seu hipervisor.
- **Se o SSH estiver habilitado no seu firewall, usando SSH:** Faça login na sua conta de administrador do XenMobile.

Você pode realizar várias tarefas de configuração e solução de problemas usando a CLI. A figura a seguir mostra o menu de nível superior da CLI.

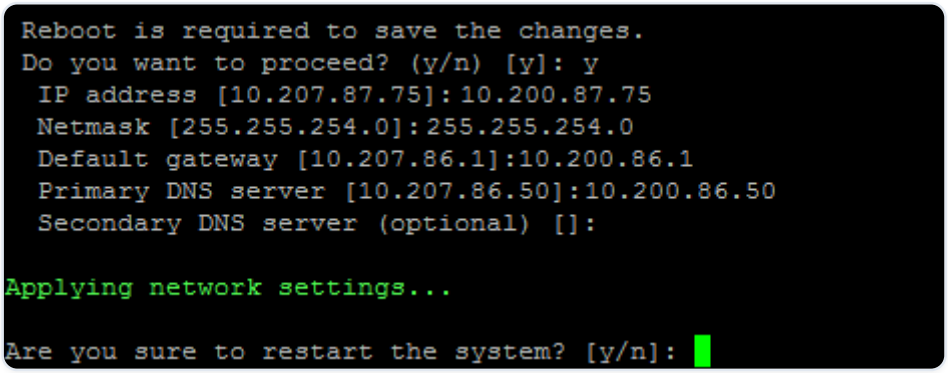


Opções de configuração

A seguir estão exemplos do **Menu de Configuração** e das configurações exibidas para cada opção.



Rede



Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

Banco de dados

```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

Portas do Listener

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

Opções de cluster

A seguir estão exemplos do **Menu de Cluster** e as configurações exibidas para cada opção.

```
-----------------------------------
Clustering Menu
-----------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
```

Mostrar Status do Cluster

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

Habilitar/Desabilitar cluster

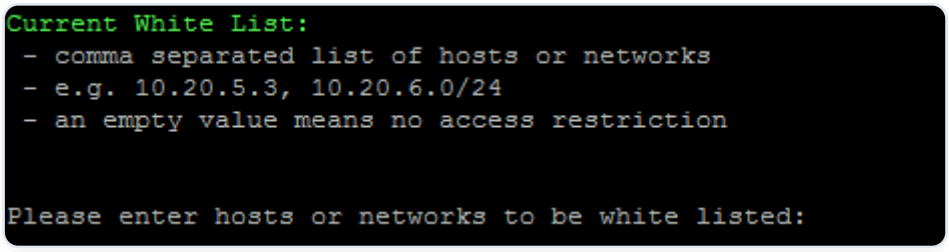
Ao optar por habilitar o cluster, a seguinte mensagem é exibida:

`To enable real-time communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.`.

Ao optar por desabilitar o cluster, a seguinte mensagem é exibida:

`You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.`.

Lista de permissões de membros do cluster



Habilitar ou desabilitar descarregamento SSL

Quando você seleciona para habilitar ou desabilitar o descarregamento SSL, a seguinte mensagem aparece:

`Enabling SSL offload opens port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.`.

Exibir Cluster Hazelcast

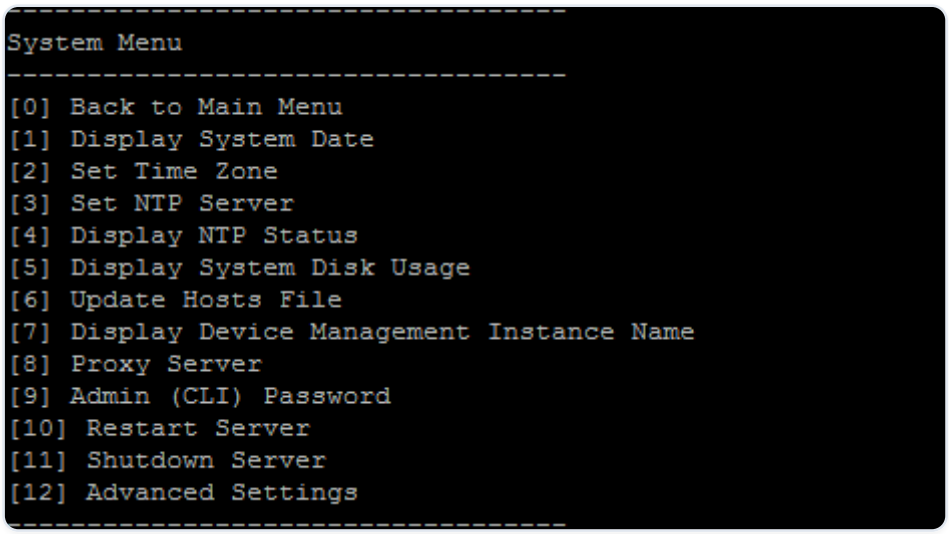
Quando você seleciona para exibir o Cluster Hazelcast, as seguintes opções aparecem:

Membros do Cluster Hazelcast:

> **Nota:**
>
> Se um nó configurado não faz parte do cluster, reinicie esse nó.

Opções do sistema

No **Menu do Sistema**, você pode exibir ou definir informações de nível de sistema, reiniciar ou desligar o servidor, ou acessar as **Configurações Avançadas**.



Definir Servidor NTP permite que você especifique informações do servidor NTP. Se você tiver problemas de fuso horário ao sincronizar o horário do XenMobile com um hypervisor, você pode evitar os problemas apontando o XenMobile para um servidor NTP. Reinicie todos os servidores do cluster após alterar esta opção.

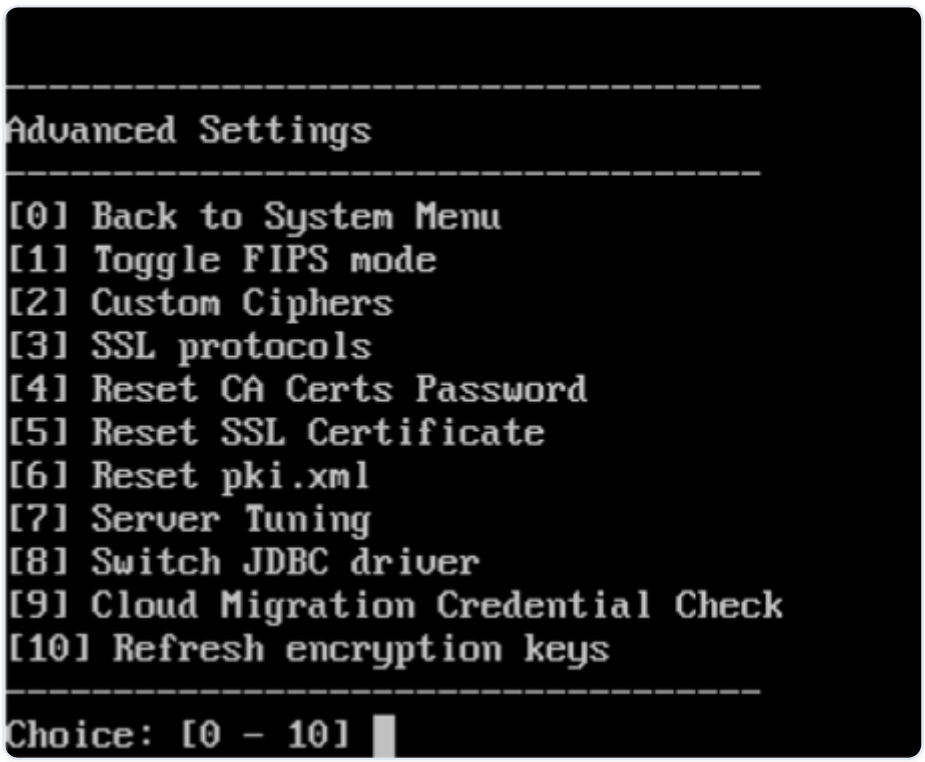
Você também pode verificar o espaço em disco visualizando o item de menu **Exibir Uso do Disco do Sistema**.

Sobre o desligamento de nós do servidor

Quando você desliga um único nó de servidor em um cluster, outros nós geralmente podem manipular a carga de trabalho se atenderem aos requisitos documentados em Escalabilidade e desempenho. O impacto pode variar dependendo de quantos nós estão inativos ao mesmo tempo, o número total de usuários e por quanto tempo os nós ficam inativos.

- Os usuários ainda podem acessar o Secure Hub e a loja.
- Os usuários ainda podem acessar e iniciar aplicativos gerenciados implantados, se um nó disponível puder manipular o número de usuários. As conexões podem ser mais lentas, resultando em check-ins de dispositivos mais lentos.
- As políticas de dispositivo continuam funcionando, a menos que todos os nós estejam inativos. Dependendo dos recursos e do número de dispositivos, as políticas podem ser implantadas mais lentamente.

Configurações Avançadas



As opções de **protocolos SSL** são padronizadas para todos os protocolos permitidos. Após o prompt **Novos protocolos SSL para habilitar**, digite os protocolos que você deseja habilitar. O XenMobile desabilita quaisquer protocolos que você não inclua em sua resposta. Por exemplo: Para desabilitar o TLSv1, digite `TLSv1.2,TLSv1.1` e, em seguida, digite **y** para reiniciar o XenMobile Server.

As opções de **Ajuste do Servidor** incluem o tempo limite de conexão do servidor, o número máximo de conexões (por porta) e o número máximo de threads (por porta).

As opções de **Trocar driver JDBC** são **jTDS** e **Microsoft** JDBC. O driver padrão é jTDS. Para obter informações sobre como mudar para o driver JDBC da Microsoft, consulte Drivers do SQL Server.

Opções de solução de problemas

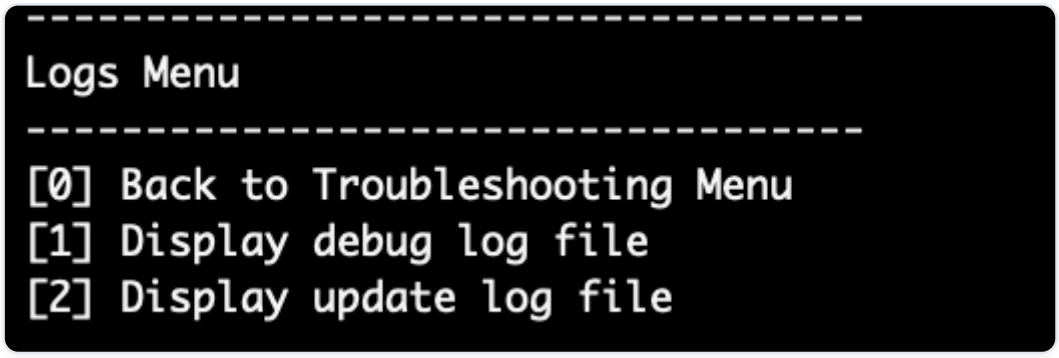
A seguir estão exemplos do **Menu de Solução de Problemas** e das configurações exibidas para cada opção.

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

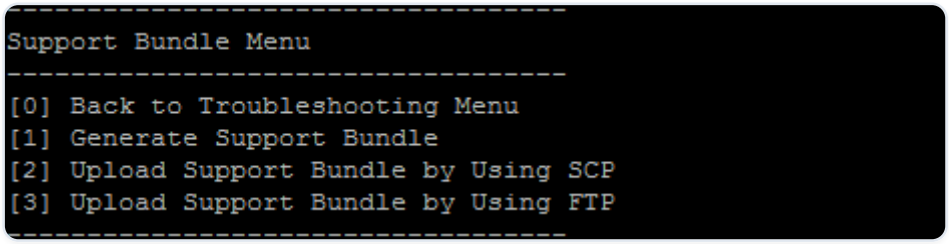
Utilitários de Rede

```
-----------------------------------
Network Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
-----------------------------------
```

Logs



Pacote de Suporte



Uso do Disco



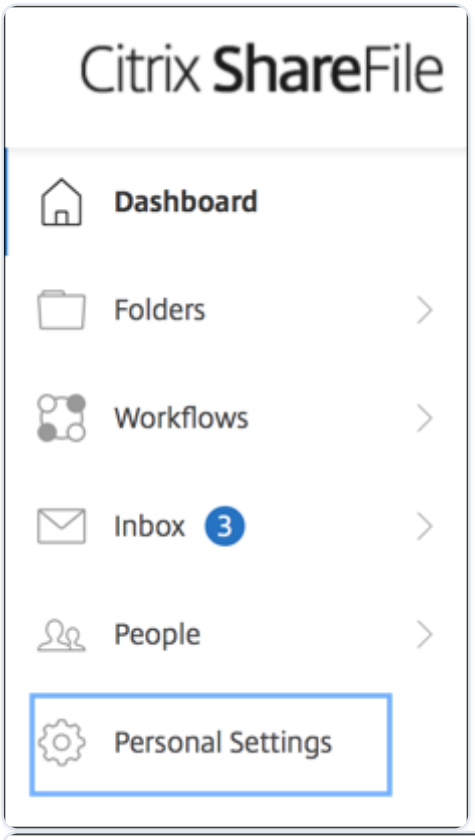
Para carregar um pacote de suporte usando o Citrix Files como site FTP

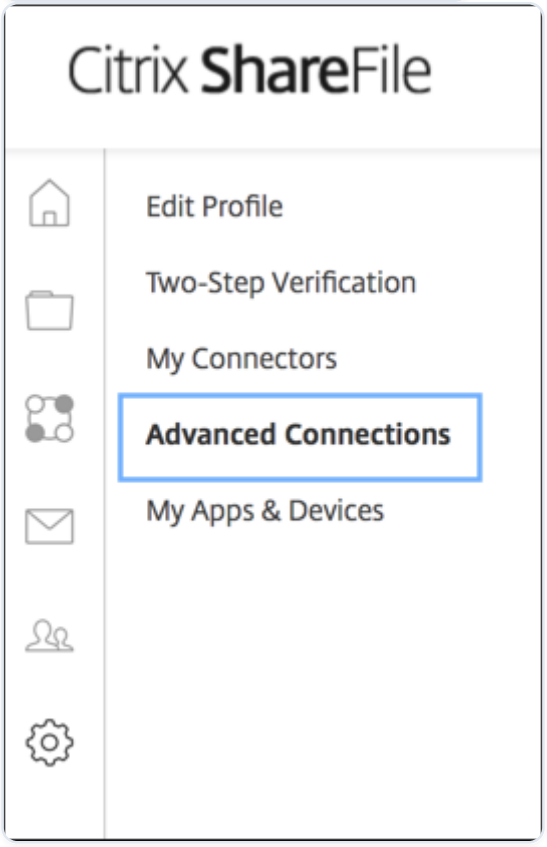
Antes de iniciar o upload de um pacote de suporte, configure os seguintes pré-requisitos no Citrix Files:

1. Verifique os detalhes de logon FTP.

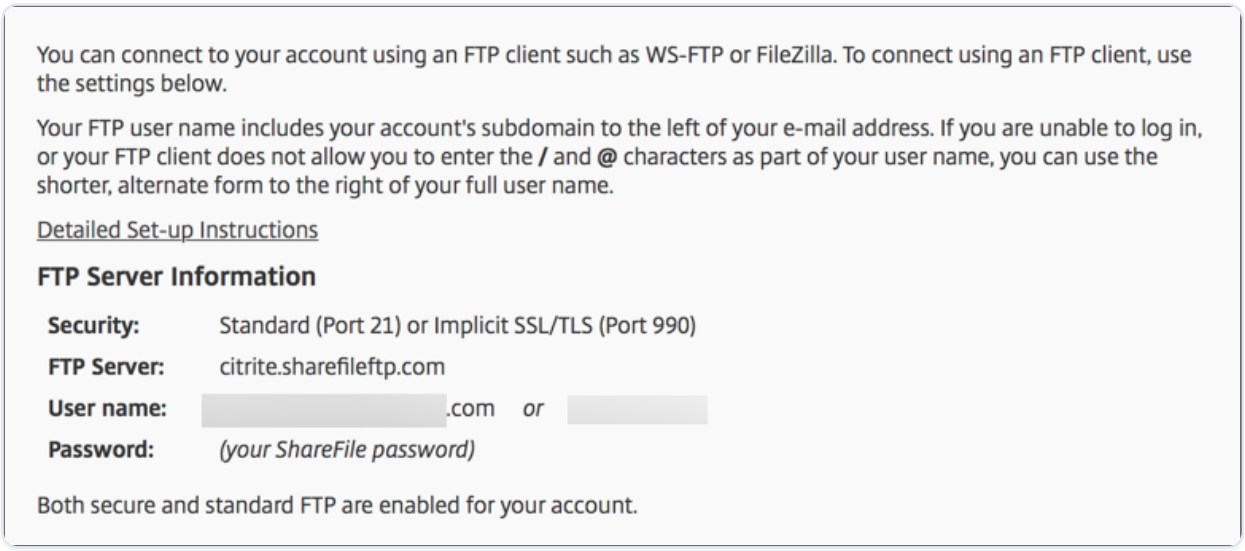
   a. Em um navegador da web, abra `<https://citrix.sharefile.com>`.

   b. Clique em **Configurações Pessoais** e depois clique em **Conexões avançadas**.





c. Em informações do Servidor FTP, para Nome de usuário, verifique se um ID de usuário alfanumérico aparece, juntamente com os detalhes padrão de Subdomínio/nome de usuário.


You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

Detailed Set-up Instructions

FTP Server Information

Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

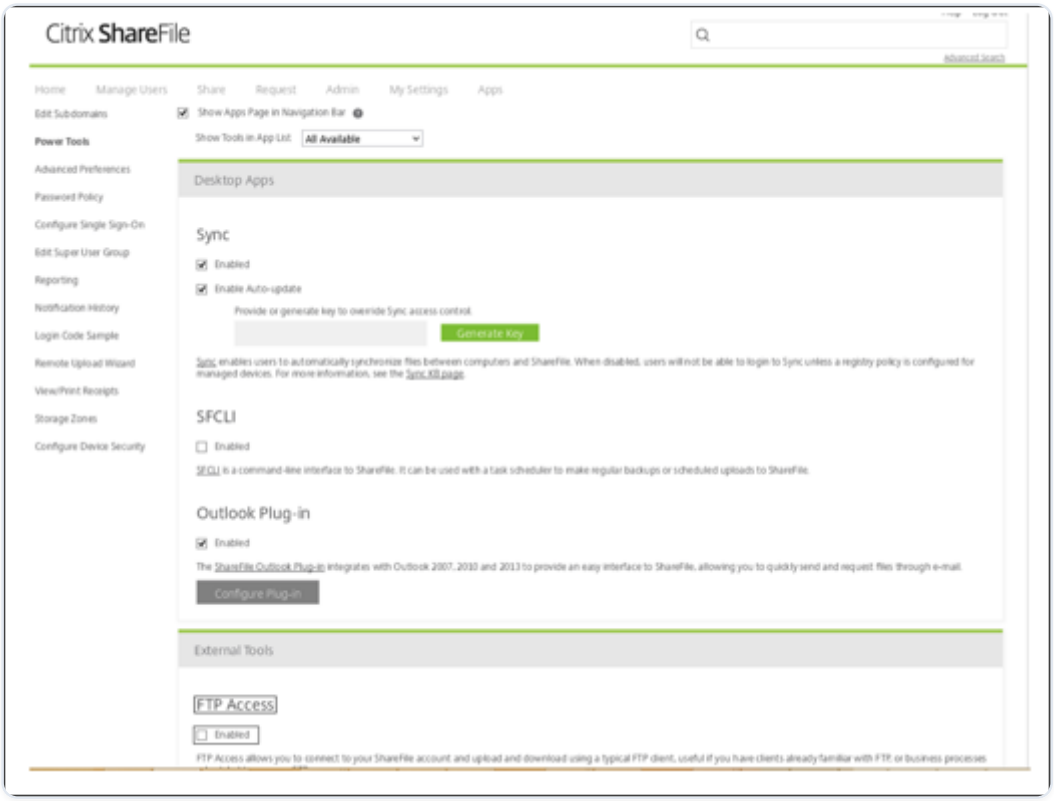
Both secure and standard FTP are enabled for your account.

Observações:

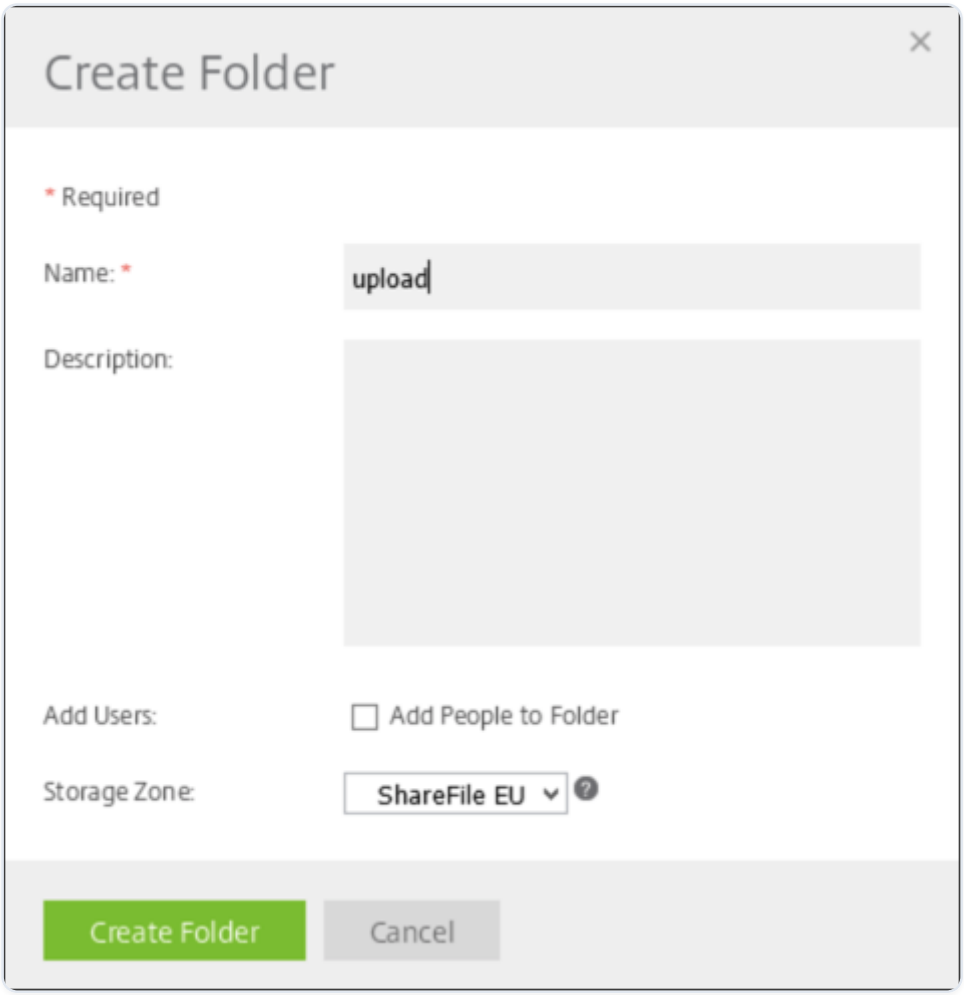
- O arquivo que você está carregando do XenMobile é um cliente FTP baseado em CLI do Linux. Como resultado, você não pode inserir caracteres de barra invertida (\) e arroba (@) como parte do seu nome de usuário.
- Se você não vir o ID de usuário alfanumérico, poderá solicitá-lo ao seu administrador do ShareFile ou ao suporte do ShareFile.

2. Verifique se o servidor Citrix Files está habilitado para comunicação FTP junto com FTPS. Idealmente, os administradores do ShareFile permitem que uma conta de usuário seja aberta para comunicação FTP. Às vezes, no entanto, apenas a comunicação FTPS é permitida.

   Um usuário com direitos de administrador pode verificar e habilitar essa configuração clicando em **Settings** > **Admin Settings** > **Advanced Preferences** > **Enable ShareFile Tools**. Em **External Apps** > **FTP Access**, verifique se a caixa de seleção **Enable** está marcada.



3. Crie uma pasta compartilhada para o cliente FTP usar como diretório para uploads de arquivos. Clique em **Home**, clique em **Folders** e, em seguida, clique em **Personal Folders**.
4. No canto superior direito, clique no ícone de sinal de mais (+), clique em **Create Folder** e, em seguida, insira um nome para a pasta.



5. Na CLI do XenMobile Server, no **Main Menu**, selecione **Troubleshooting > Support Bundle**. Em seguida, no **Support Bundle Menu**, selecione **Generate Support Bundle**.



Nota:

Se um pacote de suporte existir, quando solicitado, digite **y** para substituir o pacote.

6. Carregue o pacote de suporte para o servidor FTP:

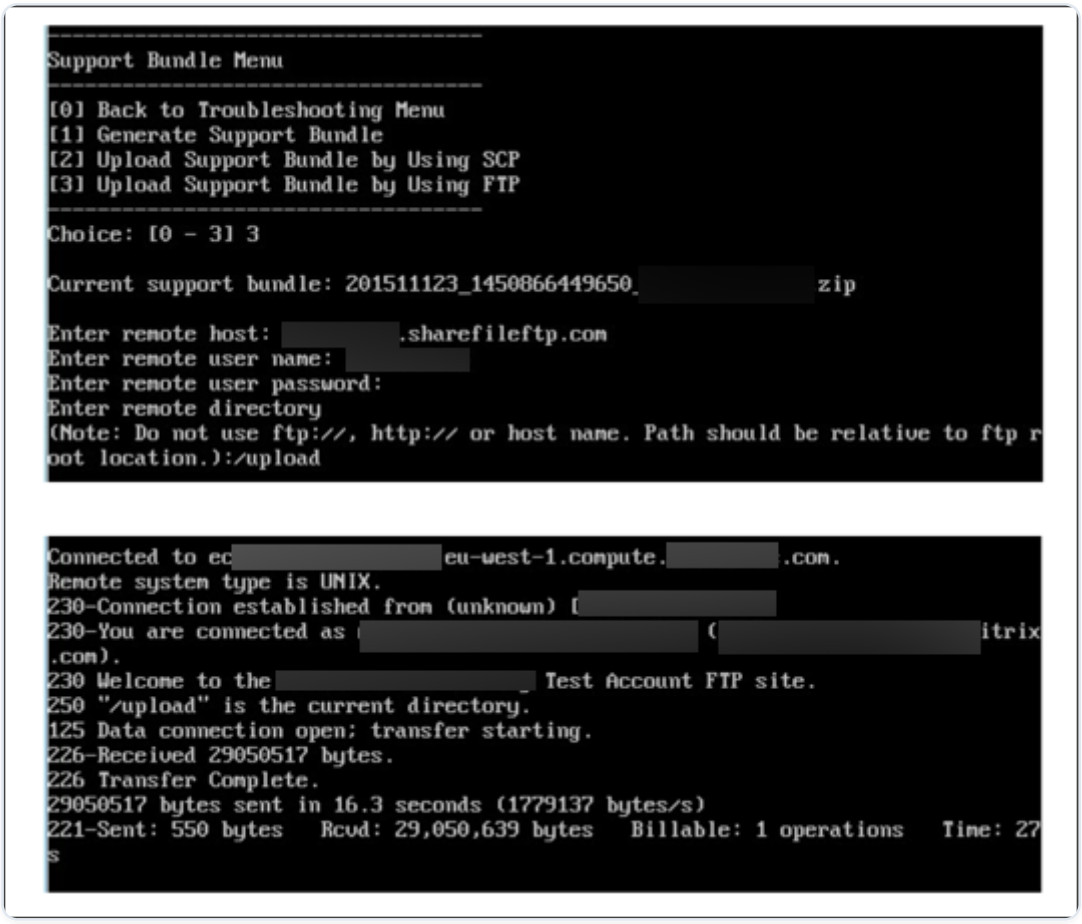
   a. Selecione **Upload Support Bundle by using FTP**.

   b. **Enter remote host:** Quando solicitado, digite o nome do seu servidor FTP. Quando o Citrix Files é usado como servidor FTP, digite o nome da sua empresa seguido pelo nome do site FTP do Citrix Files. Por exemplo, citrix.sharefileftp.com.

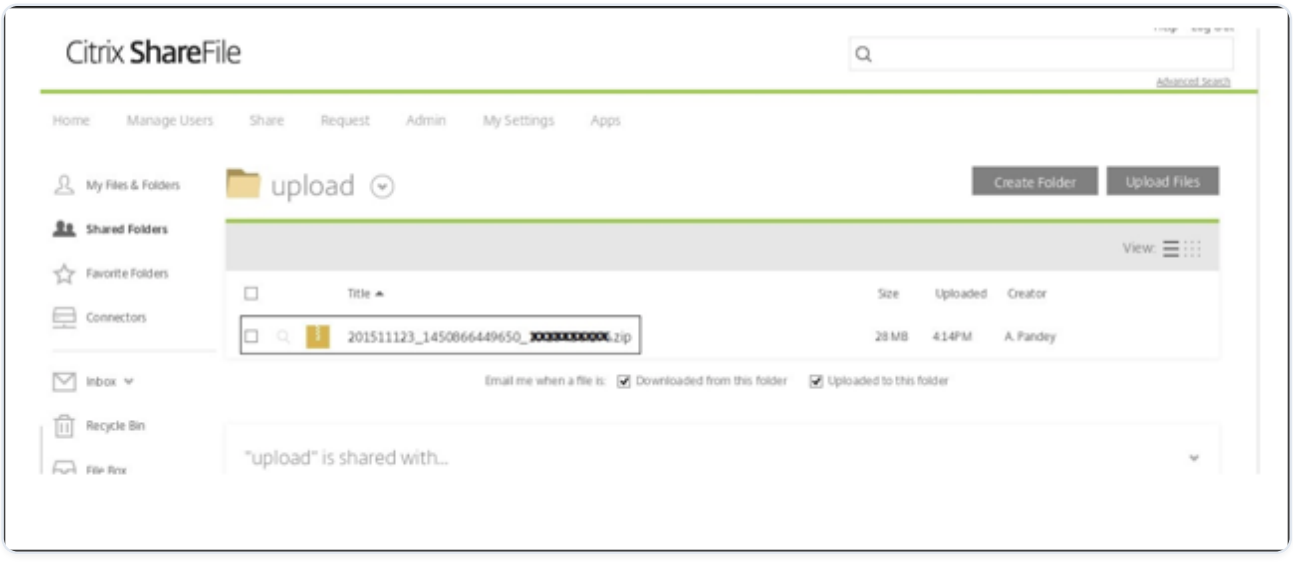
   c. **Enter remote user name:** Quando solicitado, digite o ID de usuário alfanumérico.

d. **Inserir senha do usuário remoto:** Quando solicitado, insira sua senha.

e. **Inserir diretório remoto:** Quando solicitado, insira o nome da pasta compartilhada que você criou no Citrix Files e pressione **Enter**.



Você pode visualizar o pacote de suporte carregado na pasta compartilhada que você criou no Citrix Files.



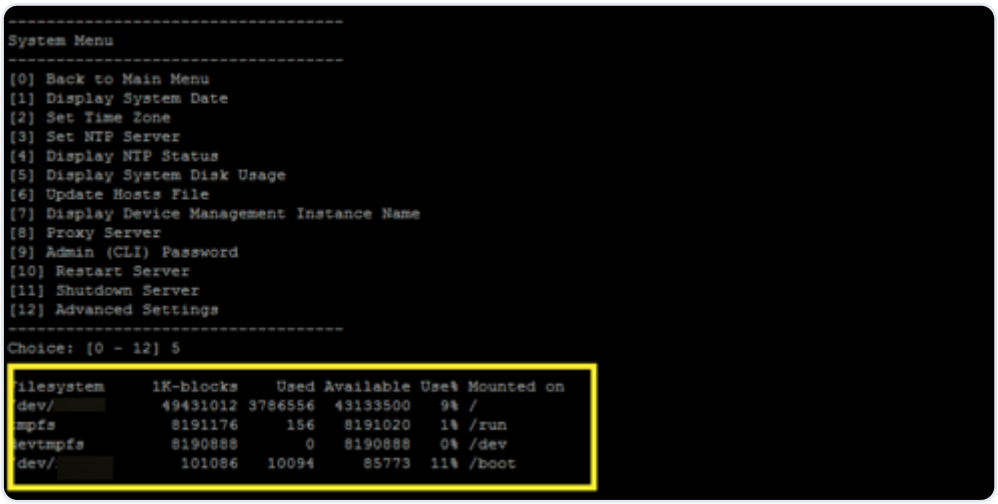
Para obter mais informações sobre o FTP do Citrix Files, consulte este artigo da Central de Conhecimento do Suporte Citrix.

Para verificar o espaço em disco

Você pode verificar o espaço em disco do sistema na CLI da seguinte forma:

1. No menu principal, selecione o menu **Sistema**.
2. No menu **Sistema**, selecione a opção **Exibir Uso do Disco do Sistema**.

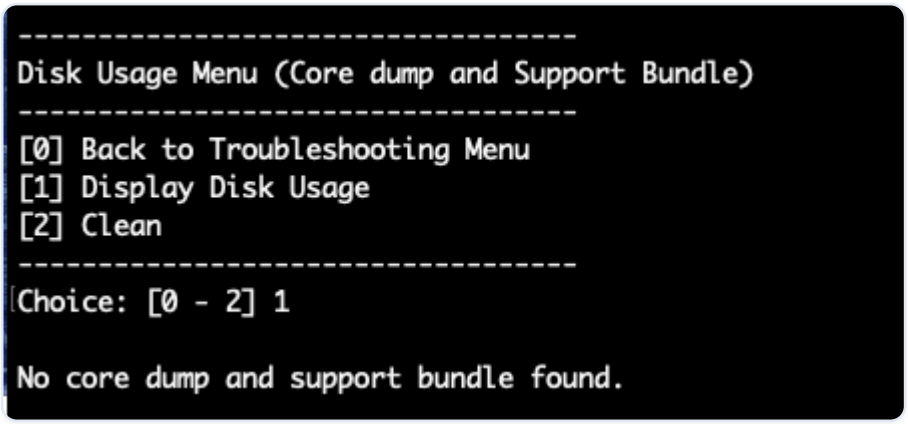
   As informações do sistema de arquivos aparecem.



Para fazer a limpeza de disco de autoatendimento

Você pode limpar o disco na CLI da seguinte forma:

1. No menu **Solução de Problemas**, selecione **Uso do Disco**. A lista **Uso do Disco** tem as seguintes opções:



2. Digite 1 para listar os tipos de arquivo de despejo de memória e de pacotes de suporte. Se não houver arquivos, você receberá a seguinte mensagem: **Nenhum despejo de memória e pacotes de suporte encontrados.**
3. Digite 2 para limpar o arquivo de despejo de memória verificado e o arquivo de pacote de suporte.

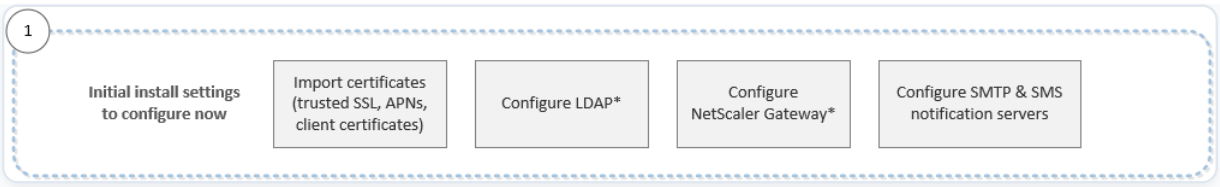
Fluxos de trabalho de introdução para o console XenMobile®

O console XenMobile é a ferramenta de gerenciamento unificada no XenMobile. Este artigo pressupõe que você instalou o XenMobile e está pronto para trabalhar no console. Se você ainda não instalou o XenMobile, consulte Instalando o XenMobile. Para obter detalhes sobre o suporte a navegadores para o console XenMobile, consulte o artigo Compatibilidade do XenMobile.

Fluxo de trabalho de configurações iniciais

Depois de concluir a configuração do XenMobile, primeiro no console de linha de comando e depois no console XenMobile, o painel é aberto. Você não pode retornar às telas de configuração inicial. Se você pulou algumas configurações de instalação, pode configurar as seguintes configurações no console. Antes de começar a adicionar usuários, aplicativos e dispositivos, considere concluir essas configurações de instalação. Para começar, clique no ícone de engrenagem no canto superior direito do console.

> **Nota:**
>
> Os itens com um asterisco são opcionais.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação do Produto Citrix:

- Autenticação
- Citrix Gateway e XenMobile
- Notificações

Para oferecer suporte às plataformas Android, iOS e Windows, você deve ter a seguinte configuração relacionada à conta.

Android

- Crie credenciais do Google Play. Para obter detalhes, consulte Lançamento do Google Play.
- Crie uma conta de administrador do Android Enterprise. Para obter detalhes, consulte Android Enterprise.

- Verifique seu nome de domínio com o Google. Para obter detalhes, consulte Verificar seu domínio para o Google Workspace.
- Habilite as APIs e crie uma conta de serviço para o Android Enterprise. Para obter detalhes, consulte Ajuda do Android Enterprise.

iOS

- Crie um ID Apple e uma conta de desenvolvedor. Para obter detalhes, consulte o site Programa de Desenvolvedores Apple.
- Crie um certificado do Apple Push Notification Service (APNs). Se você planeja gerenciar dispositivos iOS com sua implantação do XenMobile Server, precisará de um certificado APNs da Apple. Se você usa notificação por push para sua implantação do Secure Mail, também precisa de um certificado APNs da Apple. Para obter detalhes sobre como obter certificados APNs da Apple, consulte o Portal de Certificados Push da Apple. Para obter mais informações sobre XenMobile e APNs, consulte Certificados APNs e Notificações por Push para Secure Mail para iOS.
- Crie um token de empresa de compra por volume. Para obter detalhes, consulte Programa de Compra por Volume da Apple.

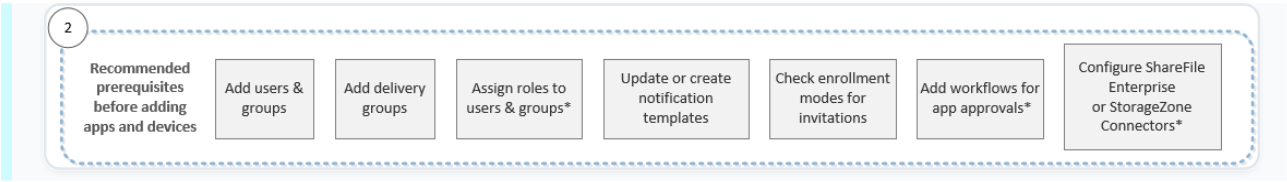
Windows

- Crie uma conta de desenvolvedor da Microsoft Windows Store. Para obter detalhes, consulte Tipos de conta, locais e taxas.
- Obtenha um ID de Editor da Microsoft Windows Store. Para obter detalhes, consulte Gerenciar configurações de conta e informações de perfil.
- Certifique-se de ter um certificado SSL público disponível se planeja usar o XenMobile AutoDiscovery para o registro de seus dispositivos Windows. Para obter detalhes, consulte Serviço XenMobile AutoDiscovery.

Fluxo de trabalho de pré-requisitos do console

Este fluxo de trabalho mostra os pré-requisitos que você deve configurar antes de adicionar aplicativos e dispositivos.

> **Observação:**
>
> Os itens com um asterisco são opcionais.



Para mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação do Produto Citrix:

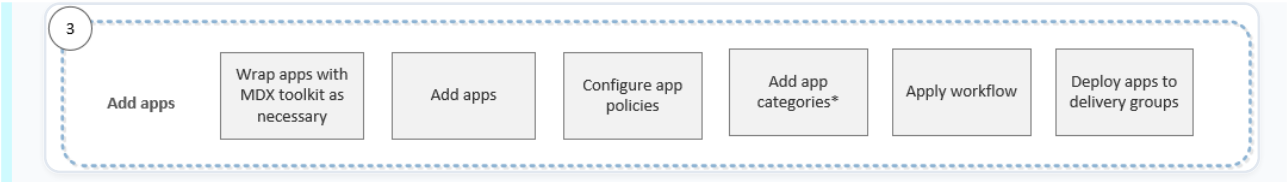
- Contas de usuário, funções e registro
- Implantar recursos
- Configurar funções com RBAC
- Notificações
- Aplicar fluxos de trabalho
- Usar ShareFile com XenMobile

Fluxo de adição de apps

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida ao adicionar aplicativos ao XenMobile.

Nota:

Os itens com um asterisco são opcionais.



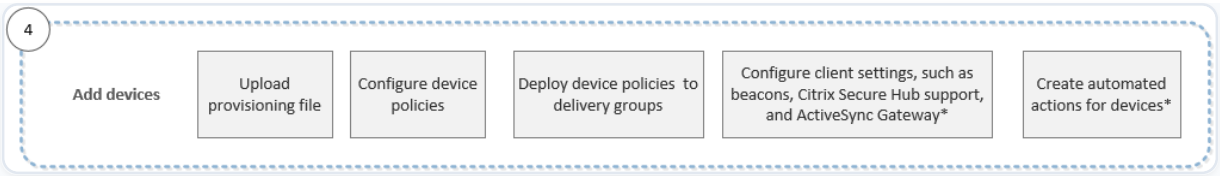
Para mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação do Produto Citrix:

- Sobre o MDX Toolkit
- Adicionar aplicativos
- Visão geral das políticas MDX
- Aplicar fluxos de trabalho
- Implantar recursos

Fluxo de trabalho para adicionar dispositivos

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida ao adicionar e registrar dispositivos no XenMobile.

> **Nota:**
>
> Os itens com um asterisco são opcionais.

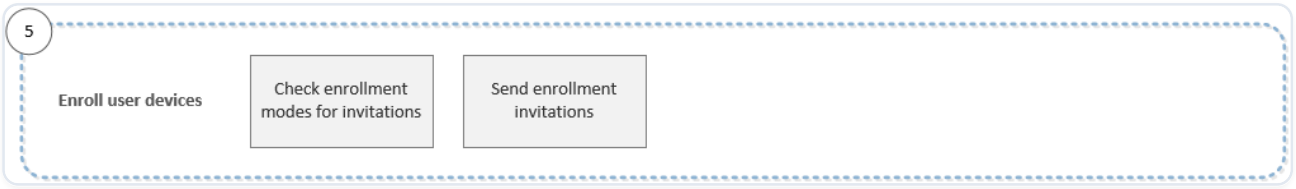


Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação do Produto Citrix:

- Dispositivos
- Sistemas operacionais de dispositivos compatíveis
- Implantar recursos
- Monitorar e dar suporte
- Ações automatizadas

Fluxo de trabalho para registrar dispositivos de usuário

Este fluxo de trabalho mostra uma ordem recomendada a seguir ao registrar dispositivos de usuário no XenMobile.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos da Documentação do Produto Citrix:

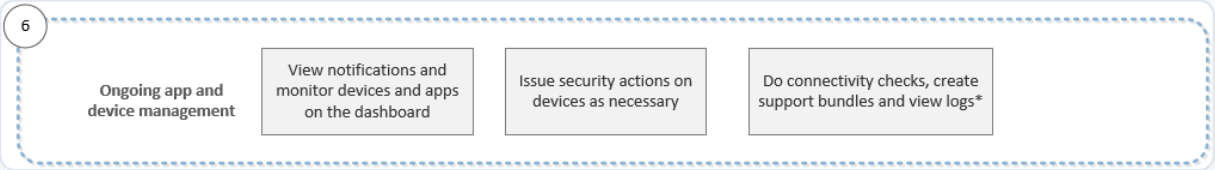
- Contas de usuário, funções e registro
- Notificações

Fluxo de trabalho de gerenciamento contínuo de aplicativos e dispositivos

Este fluxo de trabalho mostra as atividades de gerenciamento de aplicativos e dispositivos que você pode realizar no console.

Nota:

Os itens com um asterisco são opcionais.



Para obter mais informações sobre as opções de suporte encontradas ao clicar no ícone de chave inglesa no canto superior direito do console, consulte Monitorar e dar suporte.

Certificados e autenticação

Vários componentes desempenham um papel na autenticação durante as operações do XenMobile®:

- **XenMobile Server:** O XenMobile Server é onde você define a segurança e a experiência de registro. As opções para integrar usuários incluem:
  - Se o registro deve ser aberto para todos ou apenas por convite.
  - Se é necessário autenticação de dois fatores ou autenticação de três fatores. Através das propriedades do cliente no XenMobile, você pode habilitar a autenticação por PIN da Citrix e configurar a complexidade e o tempo de expiração do PIN.
- **Citrix ADC:** O Citrix ADC fornece terminação para sessões SSL de micro VPN. O Citrix ADC também oferece segurança de rede em trânsito e permite definir a experiência de autenticação usada cada vez que um usuário acessa um aplicativo.
- **Secure Hub:** O Secure Hub e o XenMobile Server trabalham juntos nas operações de registro. O Secure Hub é a entidade em um dispositivo que se comunica com o Citrix ADC: Quando uma sessão expira, o Secure Hub obtém um tíquete de autenticação do Citrix ADC e o passa para os aplicativos MDX. A Citrix recomenda o certificate pinning, que impede ataques man-in-the-middle. Para obter mais informações, consulte esta seção no artigo do Secure Hub: Fixação de certificado.

  O Secure Hub também facilita o contêiner de segurança MDX: o Secure Hub envia políticas, cria uma sessão com o Citrix ADC quando um aplicativo expira e define o tempo limite e a experiência de autenticação do MDX. O Secure Hub também é responsável pela detecção de jailbreak, verificações de geolocalização e quaisquer políticas que você aplique.
- **Políticas MDX:** As políticas MDX criam o cofre de dados no dispositivo. As políticas MDX direcionam as conexões de micro VPN de volta para o Citrix ADC, impõem restrições de modo offline e aplicam políticas de cliente, como tempos limite.

Para obter mais informações sobre como configurar a autenticação, incluindo uma visão geral dos métodos de autenticação de fator único e de dois fatores, consulte o artigo do Guia de Implantação, Autenticação.

Você usa certificados no XenMobile para criar conexões seguras e autenticar usuários. O restante deste artigo discute certificados. Para outros detalhes de configuração, consulte os seguintes artigos:

- Autenticação de domínio ou domínio mais token de segurança
- Certificado de cliente ou certificado mais autenticação de domínio
- Entidades PKI
- Provedores de credenciais
- Certificados APNs
- SAML para logon único com o Citrix Files
- Configurações do servidor Microsoft Azure Active Directory
- Para enviar um certificado para dispositivos para autenticar no servidor Wi-Fi: Política de dispositivo Wi-Fi
- Para enviar um certificado exclusivo não usado para autenticação, como um certificado de autoridade de certificação (CA) raiz interna, ou uma política específica: Política de dispositivo de credenciais

Certificados

O XenMobile gera um certificado Secure Sockets Layer (SSL) autoassinado durante a instalação para proteger os fluxos de comunicação para o servidor. Você deve substituir o certificado SSL por um certificado SSL confiável de uma CA conhecida.

O XenMobile também usa seu próprio serviço de Infraestrutura de Chave Pública (PKI) ou obtém certificados da CA para certificados de cliente. Todos os produtos Citrix suportam certificados curinga e SAN (Subject Alternative Name). Para a maioria das implantações, você só precisa de dois certificados curinga ou SAN.

A autenticação de certificado de cliente fornece uma camada extra de segurança para aplicativos móveis e permite que os usuários acessem aplicativos HDX™ sem problemas. Quando a autenticação de certificado de cliente é configurada, os usuários digitam seu PIN Citrix para acesso de logon único (SSO) a aplicativos habilitados para XenMobile. O PIN Citrix também simplifica a experiência de autenticação do usuário. O PIN Citrix é usado para proteger um certificado de cliente ou salvar credenciais do Active Directory localmente no dispositivo.

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e crie um certificado do Apple Push Notification Service (APNs) da Apple. Para as etapas, consulte Certificados APNs.

A tabela a seguir mostra o formato e o tipo de certificado para cada componente do XenMobile:

COMPONENTE XENMOBILE	FORMATO DO CERTIFICADO	TIPO DE CERTIFICADO NECESSÁRIO
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Raiz (O Citrix Gateway converte PFX para PEM automaticamente.)
XenMobile Server	.p12 (.pfx em computadores baseados em Windows)	SSL, SAML, APNs (O XenMobile também gera uma PKI completa durante o processo de instalação.) Importante: O XenMobile Server não oferece suporte a certificados com extensão .pem. Para usar um certificado .pem, divida o arquivo .pem em um certificado e uma chave e importe cada um para o XenMobile Server.
StoreFront™	PFX (PKCS #12)	SSL, Raiz

O XenMobile oferece suporte a certificados de ouvinte SSL e certificados de cliente com comprimentos de bit de 4096, 2048 e 1024. Certificados de 1024 bits são facilmente comprometidos.

Para o Citrix Gateway e o XenMobile Server, a Citrix recomenda obter certificados de servidor de uma CA pública, como Verisign, DigiCert ou Thawte. Você pode criar uma Solicitação de Assinatura de Certificado (CSR) a partir do Citrix Gateway ou do utilitário de configuração do XenMobile. Depois de criar a CSR, você a envia para a CA para assinatura. Quando a CA retorna o certificado assinado, você pode instalar o certificado no Citrix Gateway ou no XenMobile.

> **Importante: Requisitos para certificados confiáveis no iOS, iPadOS e macOS**

> A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, `<https://support.apple.com/pt-br/HT210176>`.

> A Apple está reduzindo o tempo de vida máximo permitido para certificados de servidor TLS. Essa alteração afeta apenas certificados de servidor emitidos após setembro de 2020. Consulte a publicação da Apple, `<https://support.apple.com/pt-br/HT211025>`.

Carregando certificados no XenMobile

Cada certificado que você carrega tem uma entrada na tabela Certificados, incluindo um resumo de seu conteúdo. Ao configurar componentes de integração PKI que exigem um certificado, você escolhe um certificado de servidor que satisfaça os critérios dependentes do contexto. Por exemplo, você pode querer configurar o XenMobile para integrar-se à sua autoridade de certificação (CA) da Microsoft. A conexão com a CA da Microsoft deve ser autenticada usando um certificado de cliente.

Esta seção fornece procedimentos gerais para upload de certificados. Para obter detalhes sobre como criar, fazer upload e configurar certificados de cliente, consulte Certificado de cliente ou certificado mais autenticação de domínio.

Requisitos de chave privada

O XenMobile pode ou não possuir a chave privada para um determinado certificado. Da mesma forma, o XenMobile pode ou não exigir uma chave privada para certificados carregados.

Upload de certificados

Você tem duas opções para fazer upload de certificados:

- Faça upload dos certificados para o console individualmente.
- Execute um upload em massa de certificados para dispositivos iOS com a API REST.

Ao fazer upload de certificados para o console, você tem duas opções principais:

- Clique para importar um keystore. Em seguida, você identifica a entrada no repositório do keystore que deseja instalar, a menos que esteja fazendo upload de um formato PKCS #12.
- Clique para importar um certificado.

Você pode fazer upload do certificado CA (sem a chave privada) que a CA usa para assinar solicitações. Você também pode fazer upload de um certificado de cliente SSL (com a chave privada) para autenticação de cliente.

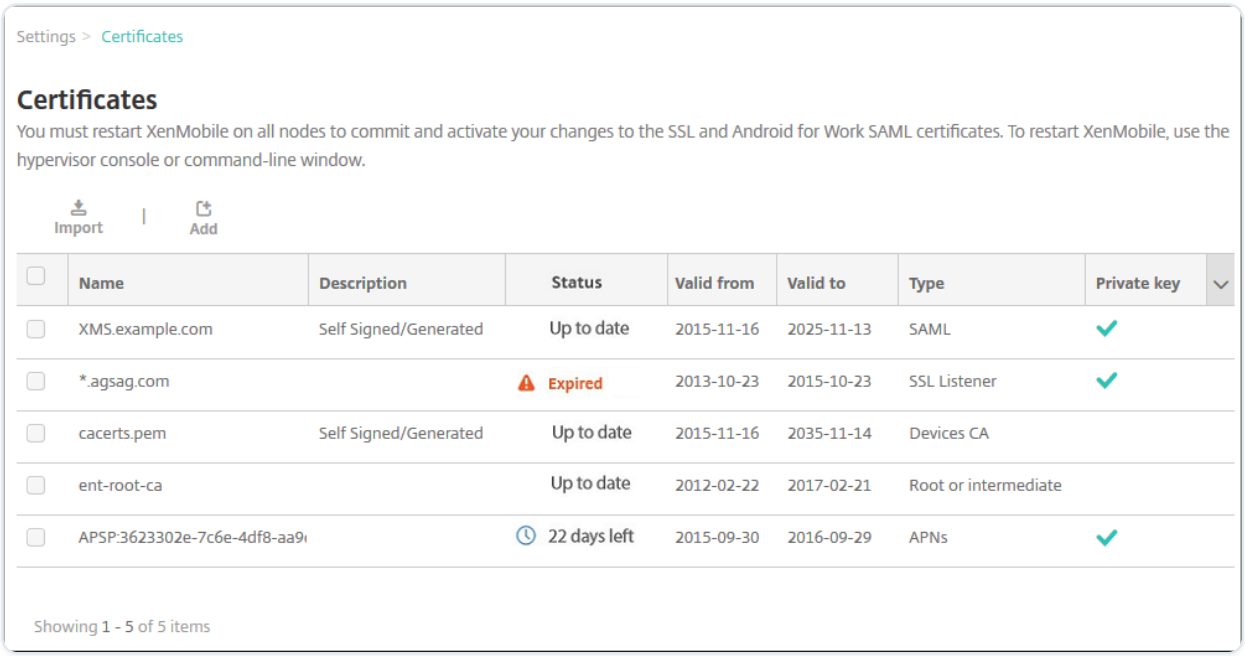
Ao configurar a entidade CA da Microsoft, você especifica o certificado CA. Você seleciona o certificado CA de uma lista de todos os certificados de servidor que são certificados CA. Da

mesma forma, ao configurar a autenticação de cliente, você pode selecionar em uma lista de todos os certificados de servidor para os quais o XenMobile possui a chave privada.

Para importar um keystore

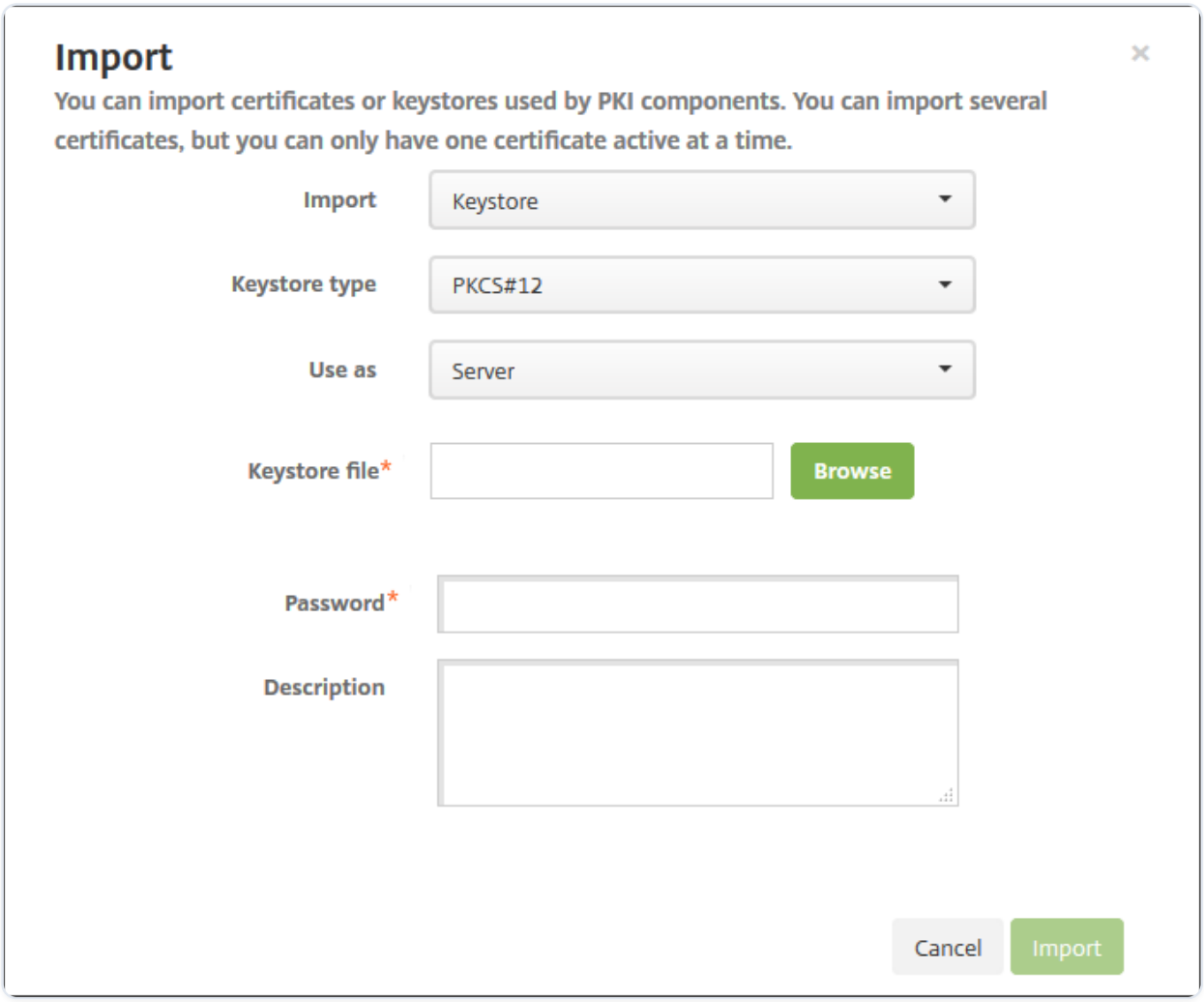
Por design, os keystores, que são repositórios de certificados de segurança, podem conter várias entradas. Ao carregar de um keystore, portanto, você é solicitado a especificar o alias da entrada que identifica a entrada que deseja carregar. Se você não especificar um alias, a primeira entrada do armazenamento será carregada. Como os arquivos PKCS #12 geralmente contêm apenas uma entrada, o campo de alias não aparece quando você seleciona PKCS #12 como o tipo de keystore.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Certificados**. A página **Certificados** é exibida.



3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
4. Configure estas definições:

    - **Importar:** Na lista, clique em **Keystore**. A caixa de diálogo **Importar** muda para refletir as opções de keystore disponíveis.



- **Tipo de keystore:** Na lista, clique em **PKCS #12**.
- **Usar como:** Na lista, clique em como você planeja usar o certificado. As opções disponíveis são:
  - **Servidor**. Certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que são carregados para o console web do XenMobile. Eles incluem certificados CA, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar certificados de servidor como armazenamento para certificados que deseja implantar em dispositivos. Este uso se aplica especialmente a CAs usadas para estabelecer confiança no dispositivo.
  - **SAML**. A certificação Security Assertion Markup Language (SAML) permite que você forneça acesso SSO a servidores, sites e aplicativos.
  - **APNs**. Os certificados APNs da Apple permitem o gerenciamento de dispositivos móveis via Apple Push Network.
  - **Listener SSL**. O Listener Secure Sockets Layer (SSL) notifica o XenMobile sobre a atividade criptográfica SSL.

- **Arquivo de keystore:** Navegue para encontrar o keystore que você deseja importar do tipo de arquivo .p12 (ou .pfx em computadores baseados em Windows).
- **Senha:** Digite a senha atribuída ao certificado.
- **Descrição:** Opcionalmente, digite uma descrição para o keystore para ajudar a distingui-lo de seus outros keystores.

5. Clique em **Importar**. O keystore é adicionado à tabela de Certificados.

Para importar um certificado

Ao importar um certificado, seja de um arquivo ou de uma entrada de keystore, o XenMobile tenta construir uma cadeia de certificados a partir da entrada. O XenMobile importa todos os certificados dessa cadeia para criar uma entrada de certificado de servidor para cada um. Esta operação só funciona se os certificados no arquivo ou na entrada do keystore formarem uma cadeia. Por exemplo, se cada certificado subsequente na cadeia for o emissor do certificado anterior.

Você pode adicionar uma descrição opcional para o certificado importado. A descrição é anexada apenas ao primeiro certificado da cadeia. Você pode atualizar a descrição dos certificados restantes posteriormente.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console e, em seguida, clique em **Certificados**.
2. Na página **Certificados**, clique em **Importar**. A caixa de diálogo **Importar** é exibida.
3. Na caixa de diálogo **Importar**, em **Importar**, se ainda não estiver selecionado, clique em **Certificado**.
4. A caixa de diálogo **Importar** muda para refletir as opções de certificado disponíveis. Em **Usar como**, selecione como você planeja usar o keystore. As opções disponíveis são:

    - **Servidor**. Certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que são carregados para o console web do XenMobile. Eles incluem certificados CA, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar certificados de servidor como armazenamento para certificados que deseja implantar em dispositivos. Esta opção se aplica especialmente a CAs usadas para estabelecer confiança no dispositivo.
    - **SAML**. A certificação Security Assertion Markup Language (SAML) permite que você forneça acesso de logon único (SSO) a servidores, sites e aplicativos.
    - **Ouvinte SSL**. O Ouvinte Secure Sockets Layer (SSL) notifica o XenMobile sobre a atividade criptográfica SSL.

5. Procure o keystore que você deseja importar do tipo de arquivo .p12 (ou .pfx em computadores baseados em Windows).
6. Procure um arquivo de chave privada opcional para o certificado. A chave privada é usada para criptografia e descriptografia junto com o certificado.
7. Digite uma descrição para o certificado, opcionalmente, para ajudar a identificá-lo de seus outros certificados.
8. Clique em **Importar**. O certificado é adicionado à tabela de Certificados.

Carregar certificados para dispositivos iOS em massa com a API REST

Se carregar certificados um por um não for prático, você pode carregá-los em massa para dispositivos iOS com a API REST. Este método suporta certificados no formato .p12. Para obter mais informações sobre a API REST, consulte APIs REST.

1. Renomeie cada um dos arquivos de certificado no formato `device_identity_value.p12`. O `device_identity_value` pode ser o IMEI, Número de Série ou MEID de cada dispositivo.

   Por exemplo, você escolhe usar números de série como seu método de identificação. Um dispositivo tem o número de série `A12BC3D4EFGH`, então nomeie o arquivo de certificado que você espera instalar nesse dispositivo como `A12BC3D4EFGH.p12`.
2. Crie um arquivo de texto para armazenar as senhas dos certificados .p12. Nesse arquivo, digite o identificador do dispositivo e a senha para cada dispositivo em uma nova linha. Use o formato `device_identity_value=password`. Veja o seguinte:

   ```
   A12BC3D4EFGH.p12=password1!

   A12BC3D4EFIJ.p12=password2@

   A12BC3D4EFKL.p12=password3#
   ```
3. Empacote todos os certificados e o arquivo de texto que você criou em um arquivo .zip.
4. Inicie seu cliente de API REST, faça login no XenMobile e obtenha um token de autenticação.
5. Importe seus certificados, garantindo que você coloque o seguinte no corpo da mensagem:

   ```
   {

       "alias": "",

       "useAs": "device",
   ```

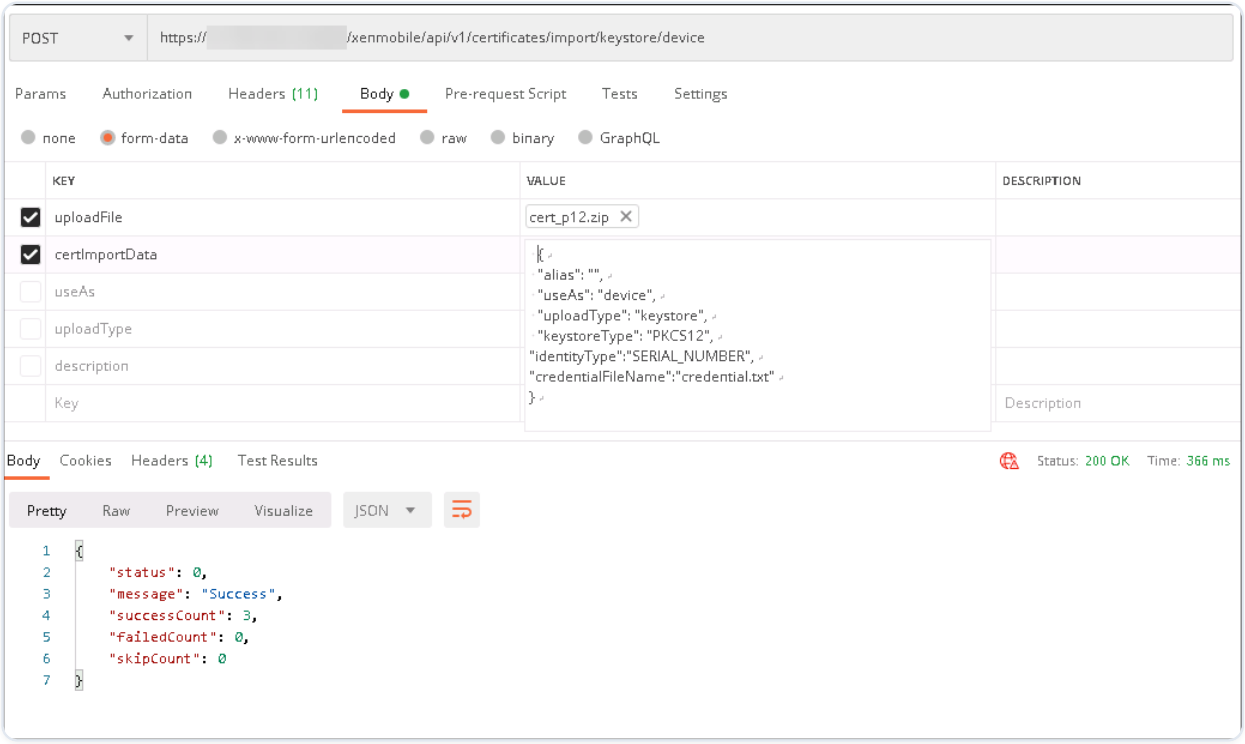
```
    "uploadType": "keystore",

    "keystoreType": "PKCS12",

    "identityType":"SERIAL_NUMBER",        # identity type can be
"SERIAL_NUMBER","IMEI","MEID"

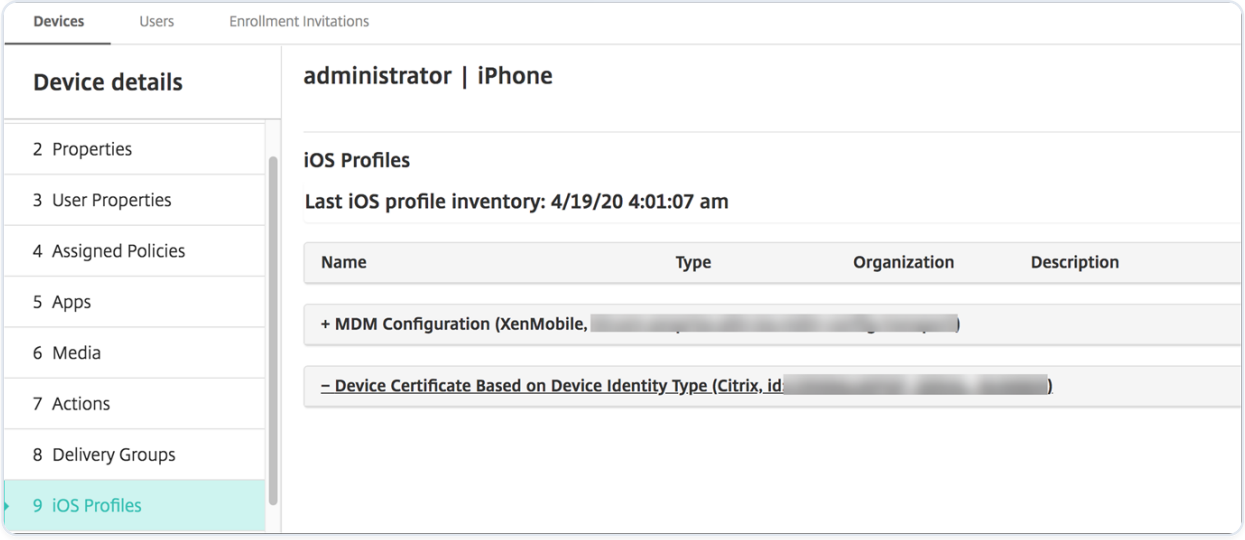
    "credentialFileName":"credential.txt"   # The credential file name
in .zip

}
```



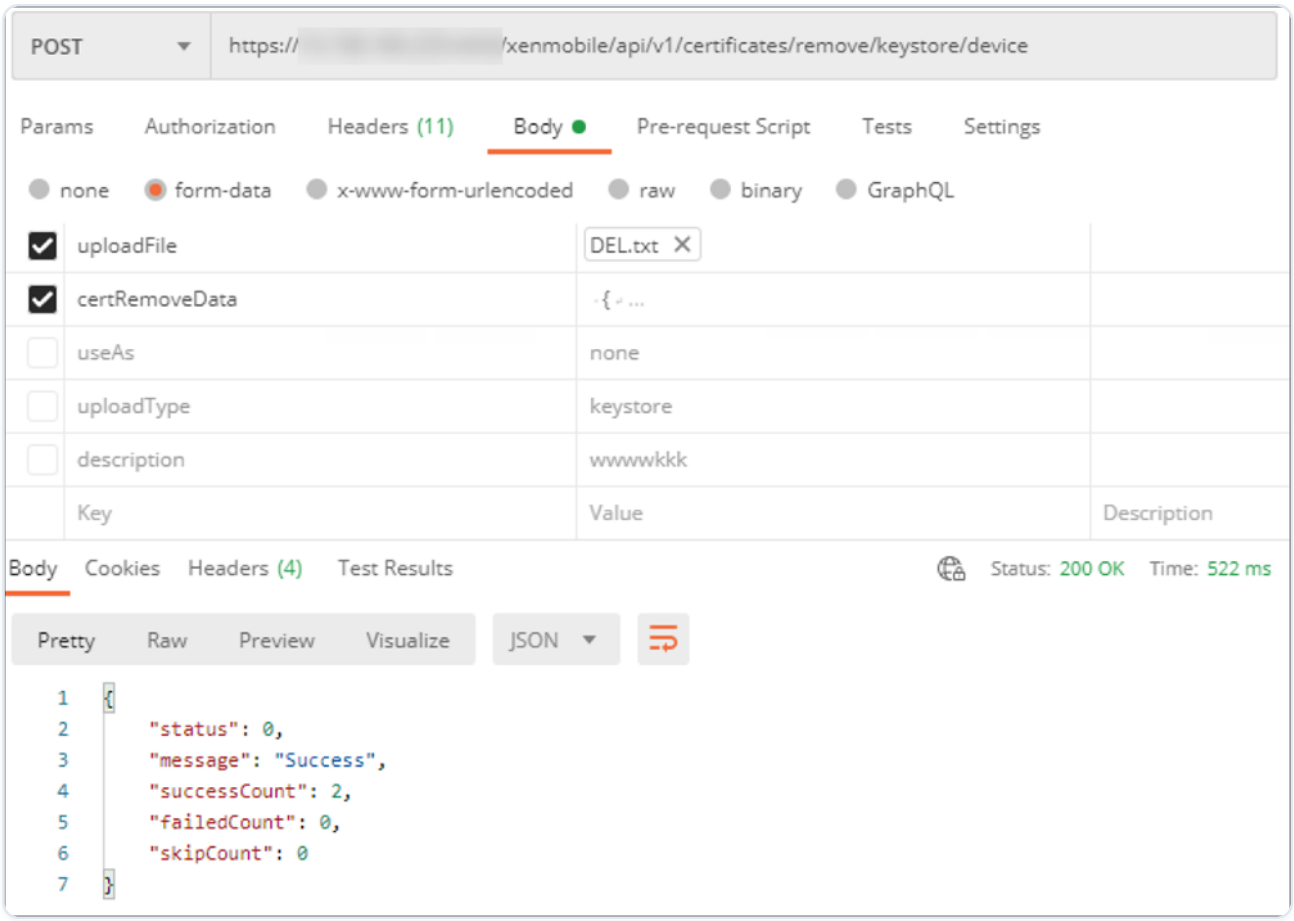
6. Crie uma política VPN com o tipo de credencial **Sempre ativado IKEv2** e o método de autenticação de dispositivo **Certificado de Dispositivo Baseado na Identidade do Dispositivo**. Selecione o **Tipo de identidade do dispositivo** que você usou nos nomes dos arquivos de certificado. Consulte Política de dispositivo VPN.
7. Registre um dispositivo iOS e aguarde a implantação da política VPN. Confirme a instalação do certificado verificando a configuração MDM no dispositivo. Você também pode verificar os detalhes do dispositivo no console do XenMobile.


12:08
Profile
MDM Configuration
MOBILE DEVICE MANAGEMENT
DEVICE IDENTITY CERTIFICATE
XenMobile MDM
Issued by: Devices Certificate Authority
Expires: April 17, 2022
CERTIFICATES (4)
Root Certificate Authority
Issued by: Root Certificate Authority
Expires: February 18, 2038
DigiCert SHA2 Secure Server CA
Issued by: DigiCert Global Root CA
Expires: March 8, 2023
DigiCert Global Root CA
Issued by: DigiCert Global Root CA
Expires: November 10, 2031
cem user02
Issued by:
Expires: February 25, 2021
SIGNING CERTIFICATE


Devices
Users
Enrollment Invitations
Device details
administrator | iPhone
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 iOS Profiles
iOS Profiles
Last iOS profile inventory: 4/19/20 4:01:07 am
Name
Type
Organization
Description
+ MDM Configuration (XenMobile,
– Device Certificate Based on Device Identity Type (Citrix, id

Você também pode excluir certificados em massa criando um arquivo de texto com o `device_identity_value` listado para cada certificado a ser excluído. Na API REST, chame a API de exclusão e use a seguinte solicitação, substituindo `device_identity_value` pelo identificador apropriado:

```
{
    "identityType"="device_identity_value"
}
```



Atualizando um certificado

O XenMobile permite apenas um certificado por chave pública no sistema por vez. Se você tentar importar um certificado para o mesmo par de chaves de um certificado já importado: Você pode substituir a entrada existente ou excluir a entrada.

Para atualizar seus certificados de forma mais eficaz no console do XenMobile, faça o seguinte. Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e, em seguida, clique em **Certificados**. Na caixa de diálogo **Importar**, importe o novo certificado.

Ao atualizar um certificado de servidor, os componentes que estavam usando o certificado anterior mudam automaticamente para usar o novo certificado. Da mesma forma, se você implantou o certificado de servidor em dispositivos, o certificado é atualizado automaticamente na próxima implantação.

Renovando um certificado

O XenMobile Server usa as seguintes autoridades de certificação internamente para PKI: CA Raiz, CA de dispositivo e CA de servidor. Essas CAs são classificadas como um grupo lógico e recebem um nome de grupo. Quando uma nova instância do XenMobile Server é provisionada, as três CAs são geradas e recebem o nome de grupo "default".

Você pode renovar as CAs para dispositivos iOS, macOS e Android compatíveis usando o console do XenMobile Server ou a API REST pública. Para dispositivos Windows registrados, os usuários devem registrar novamente seus dispositivos para receber uma nova CA de dispositivo.

As seguintes APIs estão disponíveis para renovar ou regenerar as CAs PKI internas no XenMobile Server e renovar os certificados de dispositivo emitidos por essas autoridades de certificação.

- Criar autoridades de certificação de grupo (CAs).
- Ativar novas CAs e desativar CAs antigas.
- Renovar o certificado do dispositivo em uma lista configurada de dispositivos. Dispositivos já registrados continuam a funcionar sem interrupção. Um certificado de dispositivo é emitido quando um dispositivo se conecta novamente ao servidor.
- Retornar uma lista de dispositivos que ainda usam a CA antiga.
- Excluir a CA antiga depois que todos os dispositivos tiverem a nova CA.

Para obter informações, consulte as seguintes seções no PDF API Pública para Serviços REST:

- Seção 3.16.58, Renovar Certificado de Dispositivo
- Seção 3.23, Grupos de CA PKI Internos

O console **Gerenciar Dispositivos** inclui a ação de segurança **Renovação de Certificado** usada para renovar o certificado de registro em um dispositivo.

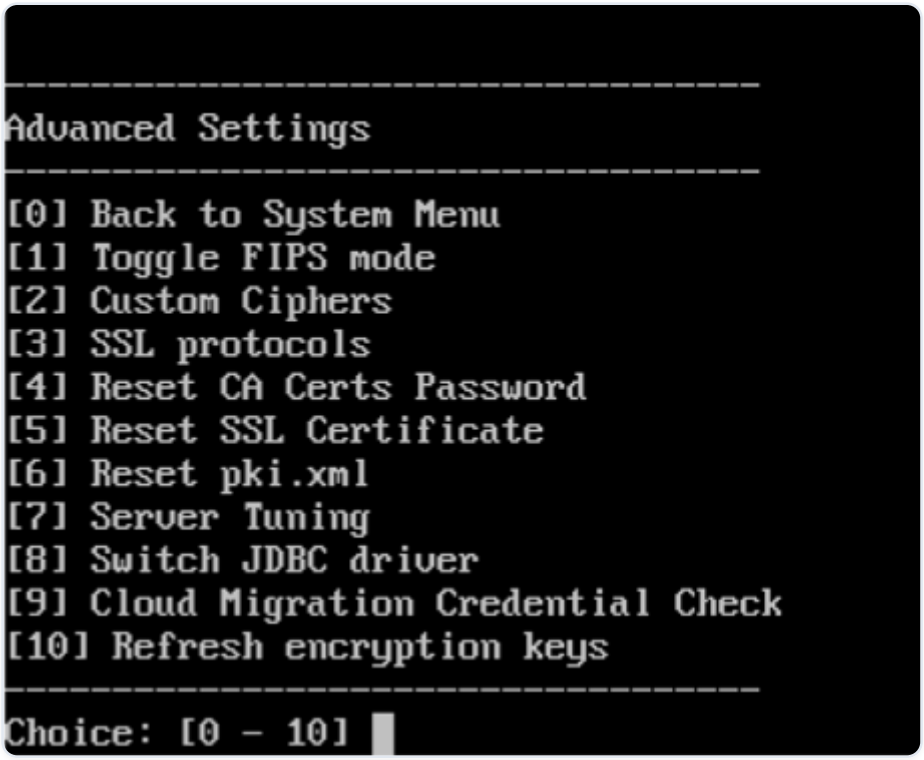
Pré-requisitos

- Por padrão, este recurso de atualização de certificado está desabilitado. Para ativar os recursos de atualização de certificado, defina o valor da propriedade do servidor **refresh.internal.ca** como **True**.

> **Importante:**
>
> Se o seu Citrix ADC estiver configurado para SSL Offload, ao gerar um novo certificado, certifique-se de atualizar seu balanceador de carga com o novo cacert.perm. Para obter mais informações sobre a configuração do Citrix Gateway, consulte Para usar o modo SSL Offload para VIPs do NetScaler.

Opção da CLI para redefinir a senha do certificado CA do servidor para nós de cluster

Depois de gerar um certificado CA do servidor em um nó do XenMobile Server, use a CLI do XenMobile para redefinir a senha do certificado em outros nós do cluster. No menu principal da CLI, escolha **Sistema > Configurações Avançadas > Redefinir senha dos certificados CA**. Se você redefinir a senha quando não houver um novo certificado CA, o XenMobile não redefinirá a senha.



Administração de Certificados do XenMobile

Recomendamos que você liste os certificados que usa em sua implantação do XenMobile, especialmente suas datas de expiração e senhas associadas. Esta seção tem como objetivo ajudá-lo a facilitar a administração de certificados no XenMobile.

Seu ambiente pode incluir alguns ou todos os seguintes certificados:

- Servidor XenMobile
  - Certificado SSL para FQDN MDM
  - Certificado SAML (Para Citrix Files)
  - Certificados de CA Raiz e Intermediários para os certificados precedentes e quaisquer outros recursos internos (StoreFront/Proxy, e assim por diante)
  - Certificado APN para Gerenciamento de Dispositivos iOS
  - Certificado APNs Interno para Notificações do Secure Hub do XenMobile Server
  - Certificado de Usuário PKI para conectividade com PKI
- MDX Toolkit
  - Certificado de Desenvolvedor Apple
  - Perfil de Provisionamento Apple (por aplicativo)
  - Certificado APNs da Apple (para uso com Citrix Secure Mail™)
  - Arquivo Keystore do Android

  O SDK MAM não encapsula aplicativos, portanto, não requer um certificado.
- Citrix ADC
  - Certificado SSL para FQDN MDM
  - Certificado SSL para FQDN do Gateway
  - Certificado SSL para FQDN SZC do ShareFile
  - Certificado SSL para Balanceamento de Carga do Exchange (configuração de descarregamento)
  - Certificado SSL para Balanceamento de Carga do StoreFront
  - Certificados CA Raiz e Intermediários para os certificados anteriores

Política de Expiração de Certificados do XenMobile

Se você permitir que um certificado expire, ele se torna inválido. Você não poderá mais executar transações seguras em seu ambiente e não poderá acessar os recursos do XenMobile.

> **Nota:**
>
> A Autoridade Certificadora (CA) solicita que você renove seu certificado SSL antes da data de expiração.

Certificado APNs para Citrix Secure Mail

Os certificados do Apple Push Notification Service (APNs) expiram anualmente. Certifique-se de criar um certificado SSL APNs e atualizá-lo no portal Citrix antes que o certificado expire. Se o certificado expirar, os usuários enfrentarão inconsistências com as notificações push do Secure Mail. Além disso, você não poderá mais enviar notificações push para seus aplicativos.

Certificado APNs para gerenciamento de dispositivos iOS

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e crie um certificado APNs da Apple. Se o certificado expirar, os usuários não poderão se registrar no XenMobile e você não poderá gerenciar seus dispositivos iOS. Para obter detalhes, consulte certificados APNs.

Você pode visualizar o status e a data de expiração do certificado APNs fazendo login no Portal de Certificados Push da Apple. Certifique-se de fazer login como o mesmo usuário que criou o certificado.

Você também recebe uma notificação por e-mail da Apple 30 e 10 dias antes da data de expiração. A notificação inclui as seguintes informações:

```
The following Apple Push Notification Service certificate, created for
Apple ID CustomerID will expire on Date. Revoking or allowing this
certificate to expire will require existing devices to be re-enrolled with
a new push certificate.



Please contact your vendor to generate a new request (a signed CSR), then
visit https://identity.apple.com/pushcert to renew your Apple Push
Notification Service certificate.
```

```
Thank You,


Apple Push Notification Service
```

MDX Toolkit (certificado de distribuição iOS)

Um aplicativo executado em um dispositivo iOS físico (diferente dos aplicativos da Apple App Store) tem os seguintes requisitos de assinatura:

- Assine o aplicativo com um perfil de provisionamento.
- Assine o aplicativo com um certificado de distribuição correspondente.

Para verificar se você tem um certificado de distribuição iOS válido, faça o seguinte:

1. No portal do Apple Enterprise Developer, crie um ID de Aplicativo explícito para cada aplicativo que você planeja empacotar com o MDX Toolkit. Um exemplo de ID de Aplicativo aceitável é: `com.CompanyName.ProductName`.
2. No portal do Apple Enterprise Developer, vá para **Provisioning Profiles > Distribution** e crie um perfil de provisionamento interno. Repita esta etapa para cada ID de Aplicativo criado na etapa anterior.
3. Baixe todos os perfis de provisionamento. Para obter detalhes, consulte Empacotamento de aplicativos móveis iOS.

Para confirmar que todos os certificados do XenMobile Server são válidos, faça o seguinte:

1. No console do XenMobile, clique em **Settings > Certificates**.
2. Verifique se todos os certificados, incluindo APNs, SSL Listener, Root e Intermediate, são válidos.

Keystore do Android

O keystore é um arquivo que contém certificados usados para assinar seu aplicativo Android. Quando o período de validade da sua chave expira, os usuários não conseguem mais atualizar perfeitamente para novas versões do seu aplicativo.

Citrix ADC

Para obter detalhes sobre como manipular a expiração do certificado para o Citrix ADC, consulte How to manipular certificate expiry on NetScaler no Citrix Support Knowledge Center.

Um certificado Citrix ADC expirado impede que os usuários se registrem e acessem a Store. O certificado expirado também impede que os usuários se conectem ao Exchange Server ao usar o Secure Mail. Além disso, os usuários não podem enumerar e abrir aplicativos HDX (dependendo de qual certificado expirou).

O Expiry Monitor e o Command Center podem ajudar você a rastrear seus certificados Citrix ADC. O Center notifica você quando o certificado expira. Essas ferramentas auxiliam no monitoramento dos seguintes certificados Citrix ADC:

- Certificado SSL para FQDN MDM
- Certificado SSL para FQDN do Gateway
- Certificado SSL para FQDN do ShareFile SZC
- Certificado SSL para Balanceamento de Carga do Exchange (configuração de descarregamento)
- Certificado SSL para Balanceamento de Carga do StoreFront
- Certificados CA Raiz e Intermediários para os certificados anteriores

Citrix Gateway e XenMobile®

Quando você configura o Citrix Gateway usando o XenMobile, você estabelece o mecanismo de autenticação para acesso remoto de dispositivos à rede interna. Essa funcionalidade permite que aplicativos em um dispositivo móvel acessem servidores corporativos na intranet. O XenMobile cria uma micro VPN dos aplicativos no dispositivo para o Citrix Gateway.

Você configura o Citrix Gateway para uso com o XenMobile exportando um script do XenMobile que você executa no Citrix Gateway.

Pré-requisitos para usar o script de configuração do Citrix Gateway

Requisitos do Citrix ADC:

- Citrix ADC (versão mínima 11.0, Build 70.12).
- O endereço IP do Citrix ADC está configurado e tem conectividade com o servidor LDAP, a menos que o LDAP esteja com balanceamento de carga.

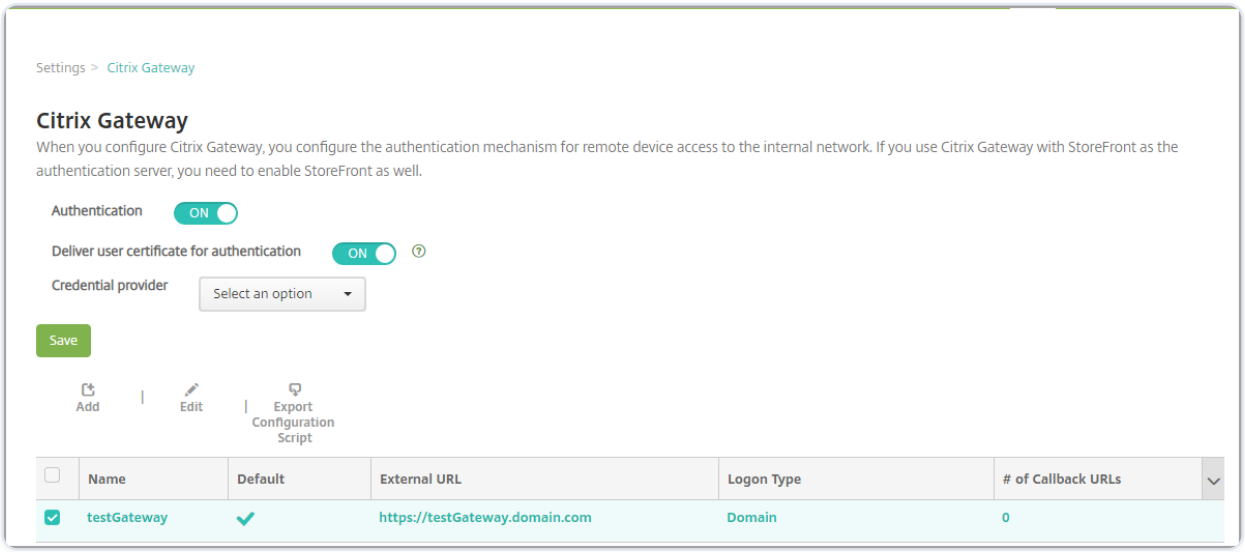
- O endereço IP da sub-rede (SNIP) do Citrix ADC está configurado, tem conectividade com os servidores de back-end necessários e tem acesso à rede pública pela porta 8443/TCP.
- O DNS pode resolver domínios públicos.
- O Citrix ADC está licenciado com licenças Platform/Universal ou Trial. Para obter informações, consulte `<https://support.citrix.com/article/CTX126049>`.
- Um certificado SSL do Citrix Gateway é carregado e instalado no Citrix ADC. Para obter informações, consulte `<https://support.citrix.com/article/CTX136023>`.

Requisitos do XenMobile:

- XenMobile Server (versão mínima 10.6).
- O servidor LDAP está configurado.

Configurar autenticação para acesso remoto de dispositivos à rede interna

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Citrix Gateway**. A página **Citrix Gateway** é exibida. No exemplo a seguir, uma instância do Citrix Gateway já existe.



3. Configure estas configurações:
   - **Autenticação:** Selecione se deseja habilitar a autenticação. O padrão é **ATIVADO**.
   - **Entregar certificado de usuário para autenticação:** Selecione se deseja que o XenMobile compartilhe o certificado de autenticação com o Secure Hub, para permitir que o Citrix Gateway manipular a autenticação de certificado de cliente. O padrão é **DESATIVADO**.

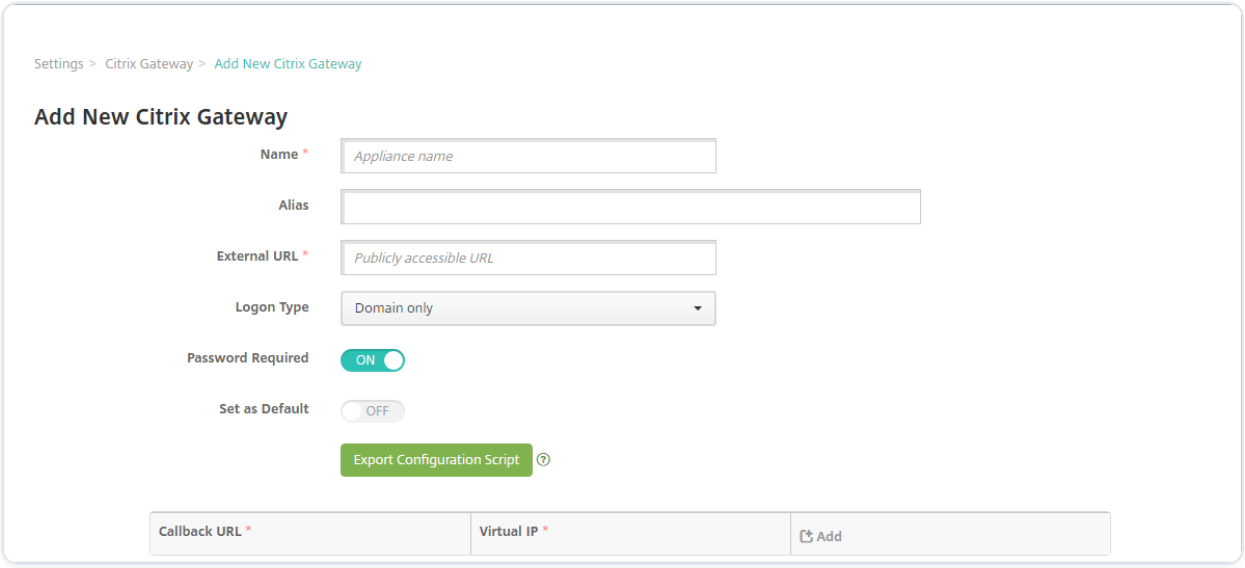
- **Provedor de Credenciais:** Na lista, clique no provedor de credenciais a ser usado. Para obter mais informações, consulte Provedores de Credenciais.

4. Clique em **Salvar**.

Adicionar uma instância do Citrix Gateway

Depois de salvar as configurações de autenticação, você adiciona uma instância do Citrix Gateway ao XenMobile.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é aberta.
2. Em **Servidor**, clique em **Citrix Gateway**. A página **Citrix Gateway** é exibida.
3. Clique em **Adicionar**. A página **Adicionar Novo Citrix Gateway** é exibida.



4. Configure estas configurações:

- **Nome:** Digite um nome para a instância do Citrix Gateway.
- **Alias:** Opcionalmente, inclua um nome de alias para o Citrix Gateway.
- **URL Externa:** Digite a URL publicamente acessível para o Citrix Gateway. Por exemplo, `https://receiver.com`.
- **Tipo de Logon:** Escolha um tipo de logon. Os tipos incluem **Somente domínio**, **Somente token de segurança**, **Domínio e token de segurança**, **Certificado**, **Certificado e domínio** e **Certificado e token de segurança**. A configuração padrão para o campo **Senha Necessária** muda com base no **Tipo de Logon** selecionado. O padrão é **Somente domínio**.

Se você tiver vários domínios, use **Certificado e domínio**. Para obter mais informações sobre como configurar a autenticação de vários domínios com XenMobile e Citrix Gateway, consulte Configurar autenticação para vários domínios.

Se você usar **Certificado e token de segurança**, algumas configurações adicionais são necessárias no Citrix Gateway para oferecer suporte ao Secure Hub. Para obter informações, consulte Configurando o XenMobile para Autenticação de Certificado e Token de Segurança.

Para obter mais informações, consulte Autenticação no Guia de Implantação.

- **Senha Necessária:** Selecione se deseja exigir autenticação por senha. O padrão varia com base no **Tipo de Logon** escolhido.
- **Definir como Padrão:** Selecione se deseja usar este Citrix Gateway como o padrão. O padrão é **DESATIVADO.**
- **Exportar Script de Configuração:** Clique no botão para exportar um pacote de configuração que você carrega para o Citrix Gateway para configurá-lo com as configurações do XenMobile. Para obter informações, consulte "Configurar um Citrix Gateway local para uso com o XenMobile Server" após estas etapas.
- **URL de Retorno** e **IP Virtual:** Salve suas configurações antes de adicionar esses campos. Para obter informações, consulte Adicionar uma URL de retorno e IP virtual de VPN do Citrix Gateway neste artigo.

5. Clique em **Salvar**.

   O novo Citrix Gateway é adicionado e aparece na tabela. Para editar ou excluir uma instância, clique no nome na lista.

Configurar o Citrix Gateway para uso com o XenMobile Server

Para configurar um Citrix Gateway local para uso com o XenMobile, você executa as seguintes etapas gerais, detalhadas neste artigo:

1. Baixe um script e arquivos relacionados do XenMobile Server. Consulte o arquivo readme fornecido com o script para obter as instruções detalhadas mais recentes.
2. Verifique se seu ambiente atende aos pré-requisitos.
3. Atualize o script para seu ambiente.
4. Execute o script no Citrix ADC.
5. Teste a configuração.

O script configura estas definições do Citrix Gateway exigidas pelo XenMobile:

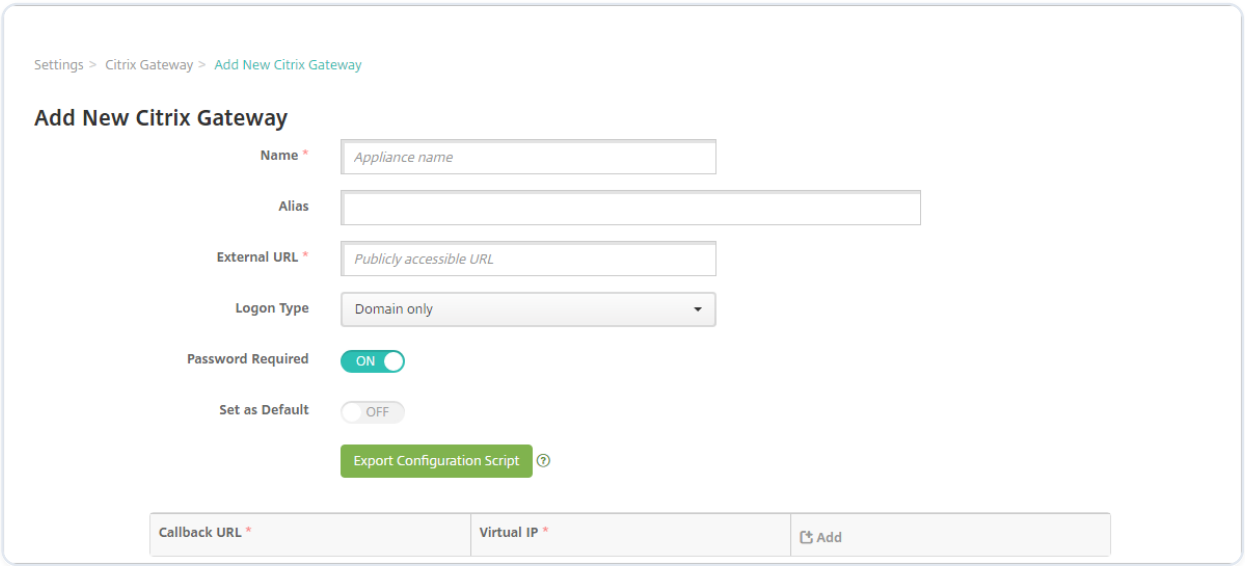
- Servidores virtuais do Citrix Gateway necessários para MDM e MAM
- Políticas de sessão para os servidores virtuais do Citrix Gateway
- Detalhes do XenMobile Server
- Políticas e Ações de Autenticação para o servidor virtual do Citrix Gateway. O script descreve as configurações de configuração LDAP.
- Ações e políticas de tráfego para o servidor proxy
- Perfil de acesso sem cliente
- Registro DNS local estático no Citrix ADC
- Outras vinculações: Política de serviço, certificado CA

O script não manipular a seguinte configuração:

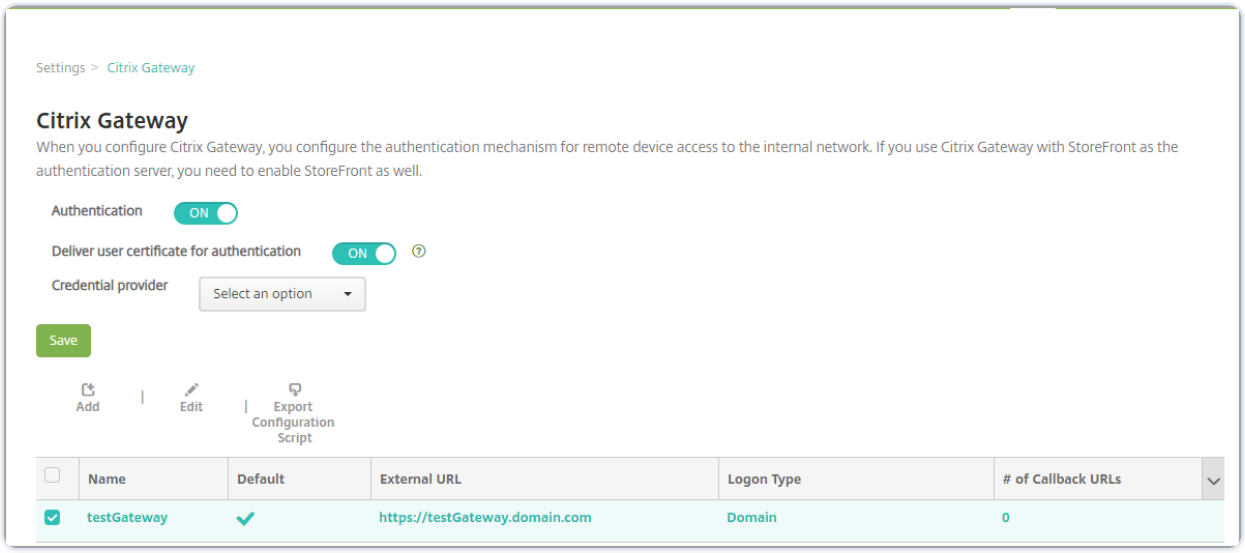
- Balanceamento de carga do Exchange
- Balanceamento de carga do Citrix Files
- Configuração do Proxy ICA®
- Descarregamento SSL

Para baixar, atualizar e executar o script

1. Se você estiver adicionando um Citrix Gateway, clique em **Export Configuration Script** na página **Add New Citrix Gateway**.



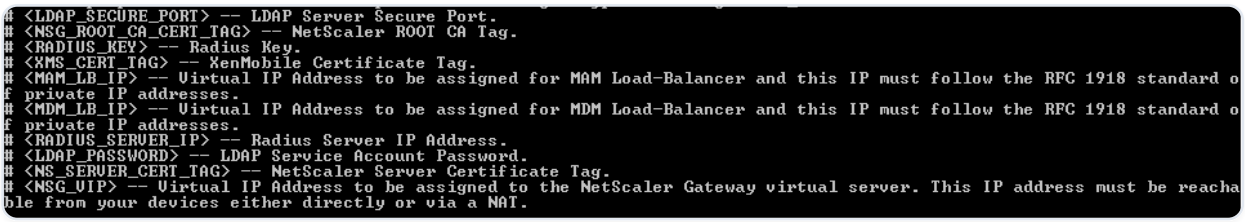
Ou, se você adicionar uma instância do Citrix Gateway e clicar em **Save** antes de exportar o script: Retorne a **Settings > Citrix Gateway**, selecione o Citrix ADC, clique em **Export Configuration Script** e, em seguida, clique em **Download**.



Depois de clicar em **Export Configuration Script**, o XenMobile cria um pacote de script .tar.gz. O pacote de script inclui:

- Arquivo Readme com instruções detalhadas
- Script que contém os comandos CLI do Citrix ADC usados para configurar os componentes necessários no Citrix ADC
- Certificado de CA Raiz Pública e o certificado de CA Intermediária do XenMobile Server (esses certificados, para descarregamento SSL, não são necessários para a versão atual)
- Script que contém os comandos CLI do Citrix ADC usados para remover a configuração do Citrix ADC

2. Edite o script (NSGConfigBundle_CREATESCRIPT.txt) para substituir todos os espaços reservados por detalhes do seu ambiente.



3. Execute seu script editado no shell bash do Citrix ADC, conforme descrito no arquivo readme incluído no pacote de script. Por exemplo:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

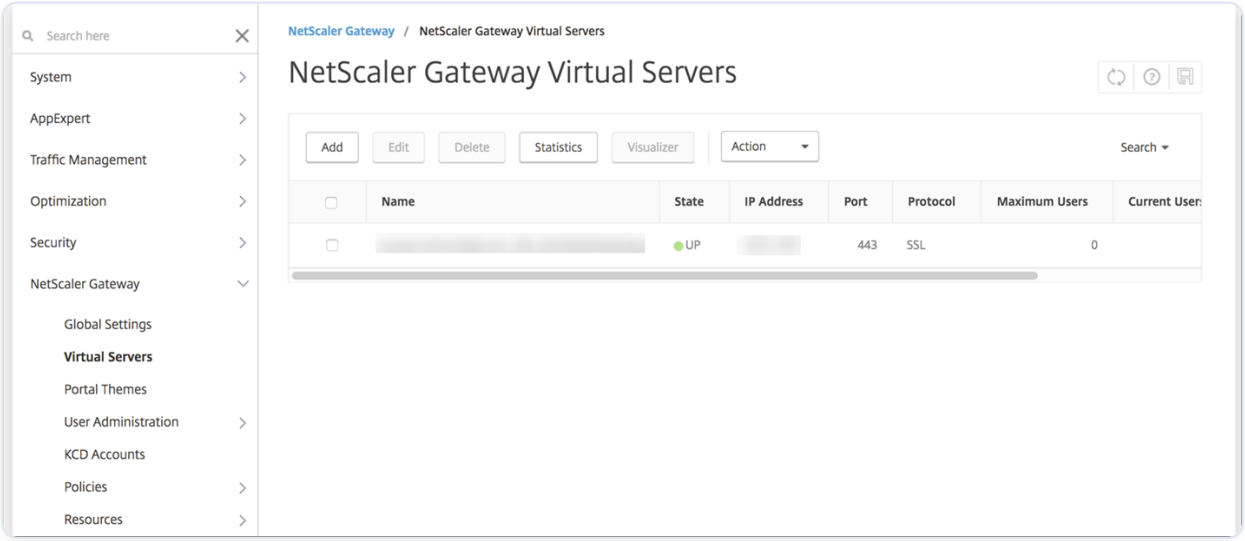
root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

Quando o script for concluído, as seguintes linhas aparecerão.

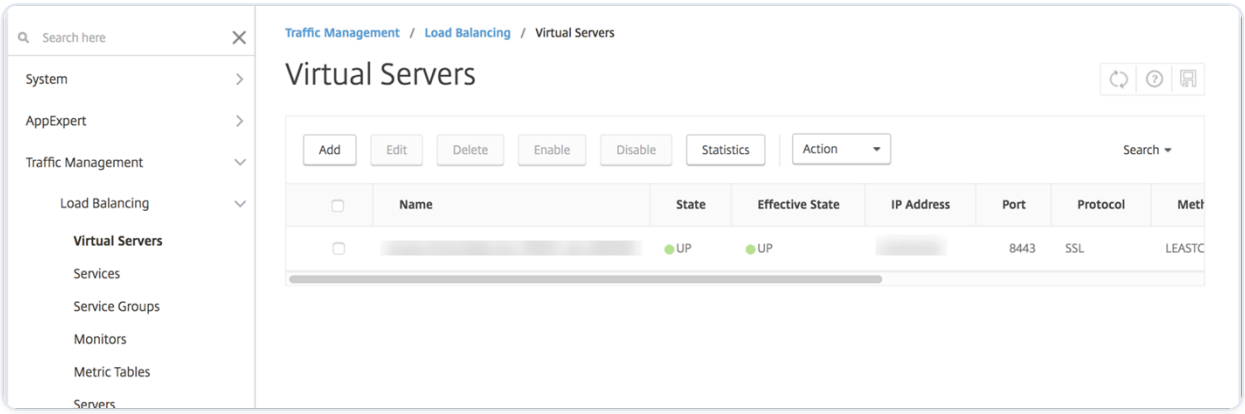
```
exec: save ns config
 Done
 Done
root@ns#
```

Testar a configuração

1. Valide se o Servidor Virtual do Citrix Gateway mostra um estado de **UP**.



2. Valide se o Servidor Virtual de Balanceamento de Carga de Proxy mostra um estado de **UP**.



3. Abra um navegador da web, conecte-se à URL do Citrix Gateway e tente autenticar. Se a autenticação falhar, esta mensagem aparecerá: HTTP Status 404 - Not Found
4. Registre um dispositivo e certifique-se de que ele obtenha o registro MDM e MAM.

Adicionar uma URL de retorno e IP virtual VPN do Citrix Gateway

Após adicionar a instância do Citrix Gateway, você pode adicionar uma URL de retorno e especificar um endereço IP virtual do Citrix Gateway. Essas configurações são opcionais, mas podem ser configuradas para segurança extra, especialmente quando o XenMobile Server está na DMZ.

1. Em **Configurações > Citrix Gateway**, selecione o Citrix Gateway e clique em **Editar**.
2. Na tabela, clique em **Adicionar**.
3. Para **URL de Retorno**, digite o nome de domínio totalmente qualificado (FQDN). A URL de retorno verifica se uma solicitação se originou do Citrix Gateway.

   Certifique-se de que a URL de retorno seja resolvida para um endereço IP acessível a partir do XenMobile Server. A URL de retorno pode ser uma URL externa do Citrix Gateway ou alguma outra URL.
4. Digite o endereço **IP Virtual** do Citrix Gateway e clique em **Salvar**.

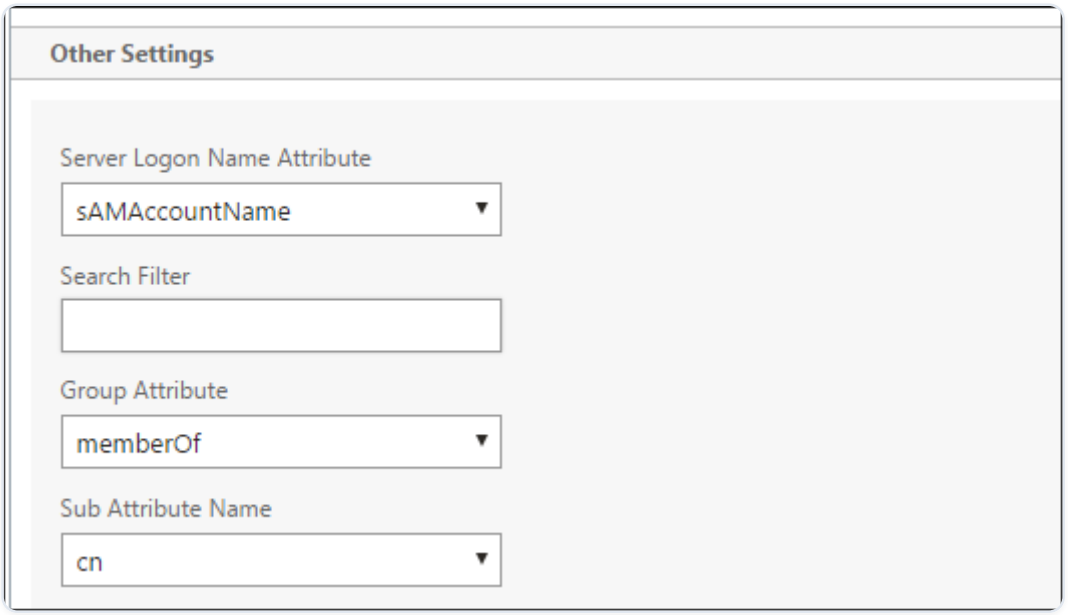
Configurar autenticação para vários domínios

Se você tiver várias instâncias do XenMobile Server, como para ambientes de teste, desenvolvimento e produção, configure o Citrix Gateway para os ambientes adicionais manualmente. (Você pode usar o assistente do Citrix ADC para XenMobile apenas uma vez.)

Configuração do Citrix Gateway

Para configurar políticas de autenticação do Citrix Gateway e uma política de sessão para um ambiente de vários domínios:

1. No utilitário de configuração do Citrix Gateway, na guia **Configuração**, expanda **Citrix Gateway > Políticas > Autenticação**.
2. No painel de navegação, clique em **LDAP**.
3. Clique para editar o perfil LDAP. Altere o **Atributo de Nome de Logon do Servidor** para **userPrincipalName** ou o atributo que você deseja usar para pesquisas. Anote o atributo que você especificar para tê-lo ao configurar as definições de LDAP no console do XenMobile.

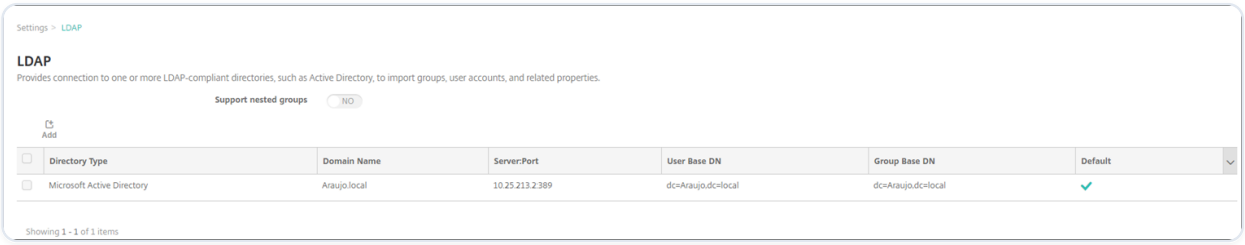


4. Repita essas etapas para cada política LDAP. Uma política LDAP separada é necessária para cada domínio.
5. Na política de sessão vinculada ao servidor virtual do Citrix Gateway, navegar para **Editar perfil de sessão > Aplicativos Publicados**. Certifique-se de que **Domínio de Logon Único** esteja em branco.

Configuração do XenMobile Server

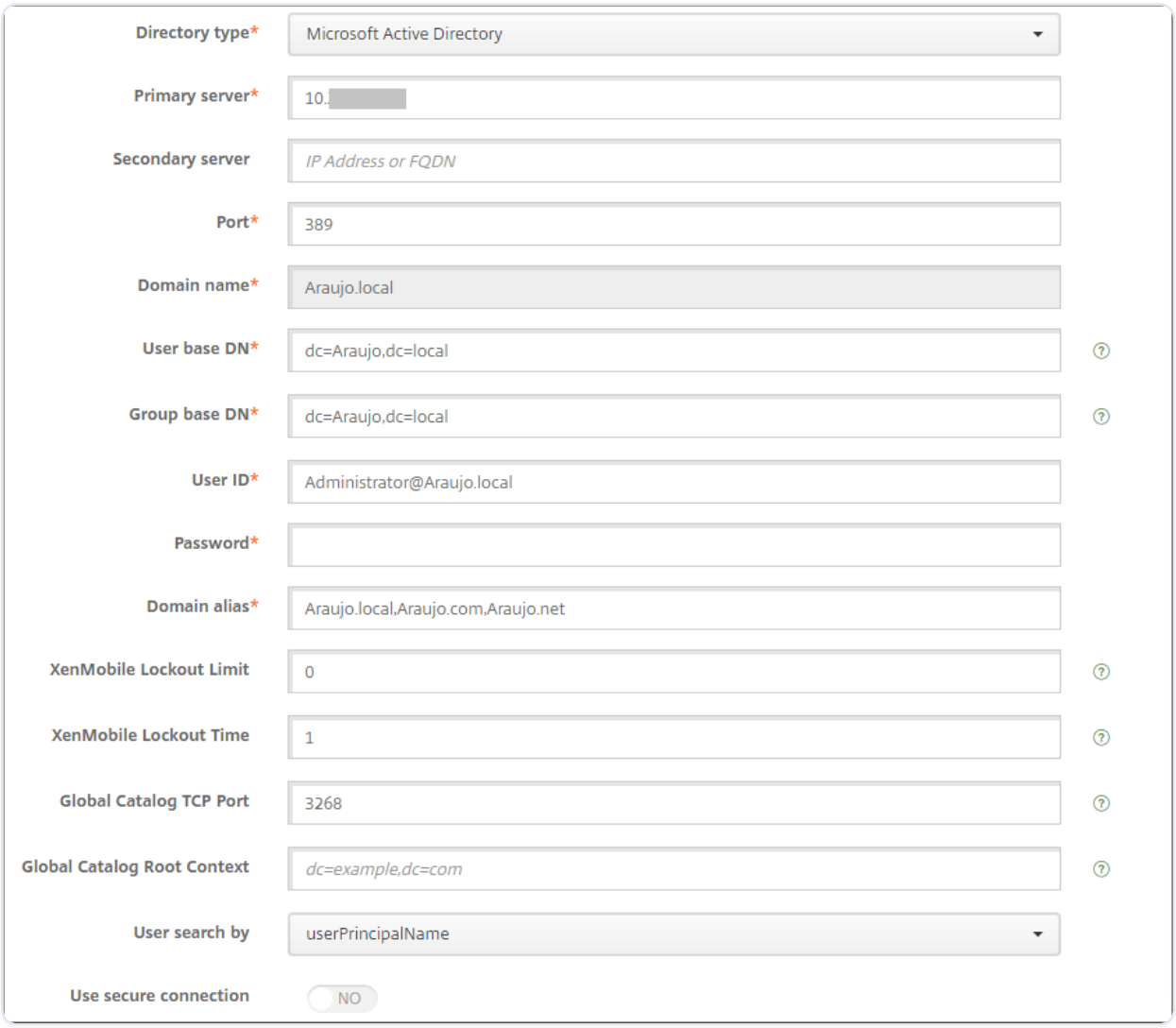
Para configurar o LDAP para um ambiente XenMobile de vários domínios:

1. No console do XenMobile, vá para **Configurações > LDAP** e adicione ou edite um diretório.



2. Forneça as informações.

- Em **Alias de Domínio**, especifique cada domínio a ser usado para autenticação de usuário. Separe os domínios com uma vírgula e não use espaços entre eles. Por exemplo: `domain1.com,domain2.com,domain3.com`
- Certifique-se de que o campo **Pesquisar usuário por** corresponda ao **Atributo de Nome de Logon do Servidor** especificado na política LDAP do Citrix Gateway.



Descartar solicitações de conexão de entrada para URLs específicas

Se o Citrix Gateway em seu ambiente estiver configurado para descarregamento SSL, você pode preferir que o gateway descarte as solicitações de conexão de entrada para URLs específicas.

Se você preferir essa segurança extra, configure os dois servidores virtuais do balanceador de carga MDM (um para a porta 443 e outro para a porta 8443) no Citrix Gateway. Use as informações a seguir como um modelo para suas configurações.

> **Importante:**

> As seguintes atualizações são apenas para um Citrix Gateway configurado para descarregamento SSL.

1. Crie um conjunto de padrões com o nome `XMS_DropURLs`.

```
add policy patset XMS_DropURLs
```

2. Adicione as seguintes URLs ao novo conjunto de padrões. Personalize esta lista conforme necessário.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6


bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5


bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4


bind policy patset XMS_DropURLs /zdm/log.jsp -index 3


bind policy patset XMS_DropURLs /zdm/login.jsp -index 2


bind policy patset XMS_DropURLs /zdm/console -index 1
```

3. Crie uma política para descartar todo o tráfego para esses URLs, a menos que a solicitação de conexão se origine da sub-rede especificada.

```
add responder policy XMS_DROP_pol
“CLIENT.IP.SRC.IN_SUBNET(192.168.0.0/24).NOT &&

HTTP.REQ.URL.CONTAINS_ANY(”XMS_DropURLs”)” DROP -comment "Allow only
```

```
subnet 192.168.0.0/24 to access these URLs. All other connections are
DROPed"
```

4. Vincule a nova política a ambos os servidores virtuais do balanceador de carga MDM (portas 443 e 8443).

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST



bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST
```

5. Bloquear o acesso à URL MAM através do navegador

   Acessar a URL MAM diretamente pelo navegador solicita que os usuários insiram suas credenciais do Active Directory. Embora atue como uma ferramenta para os usuários validarem suas credenciais, alguns usuários podem considerá-lo uma violação de segurança. A seção a seguir ajuda a restringir o acesso do navegador à URL MAM (VIP do NetScaler® Gateway), usando o recurso de Política de Resposta no NetScaler.

   Crie uma das seguintes Políticas de Resposta e vincule-a ao seu Servidor Virtual do NetScaler Gateway:

   - `add responder policy Resp_Brow_Pol "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Mozilla\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`
   - `add responder policy Resp_Brow_Pol_CR "!HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`
   - `add responder policy Resp_Brow_Pol_CR "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`

   Vincular ao Servidor Virtual do NetScaler Gateway usando `bind vpn vserver _XM_XenMobileGateway -policy Resp_Brow_Pol_CR -priority 100 -gotoPriorityExpression END -type REQUEST`

> **Nota:**
>
> `_XM_XenMobileGateway` é um nome de exemplo de um Servidor Virtual do NetScaler Gateway.

Autenticação de domínio ou domínio mais token de segurança

O XenMobile® oferece suporte à autenticação baseada em domínio contra um ou mais diretórios compatíveis com o Lightweight Directory Access Protocol (LDAP). Você pode configurar uma conexão no XenMobile para um ou mais diretórios e, em seguida, usar a configuração LDAP para importar grupos, contas de usuário e propriedades relacionadas.

LDAP é um protocolo de aplicativo de código aberto e independente de fornecedor para acessar e manter serviços de informações de diretório distribuídos em uma rede de Protocolo de Internet (IP). Os serviços de informações de diretório são usados para compartilhar informações sobre usuários, sistemas, redes, serviços e aplicativos disponíveis em toda a rede.

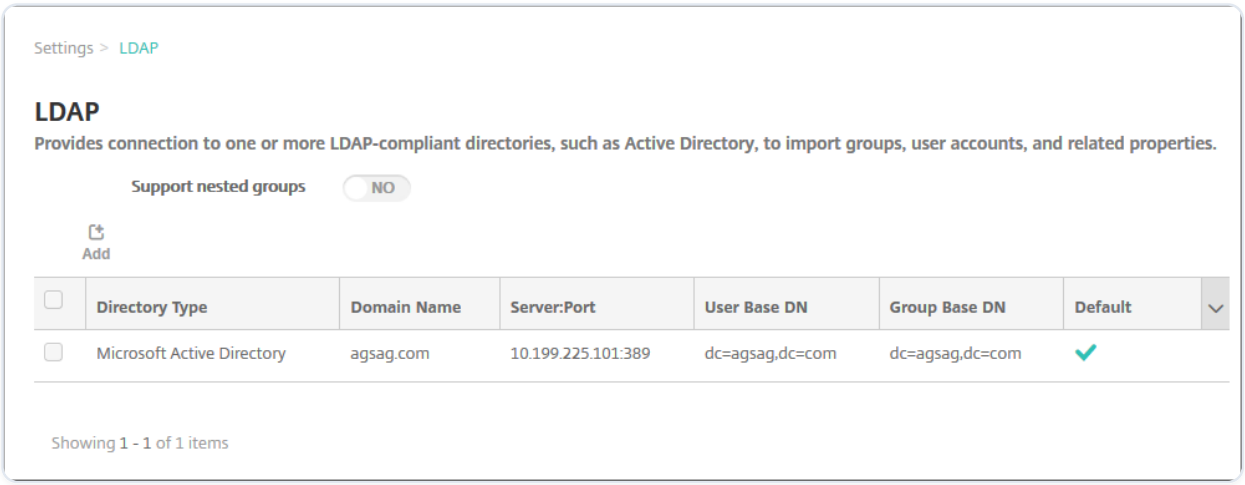
Um uso comum do LDAP é fornecer logon único (SSO) para usuários, onde uma única senha (por usuário) é compartilhada entre vários serviços. O logon único permite que um usuário faça logon uma vez em um site da empresa, para acesso autenticado à intranet corporativa.

Um cliente inicia uma sessão LDAP conectando-se a um servidor LDAP, conhecido como Agente de Sistema de Diretório (DSA). O cliente então envia uma solicitação de operação ao servidor, e o servidor responde com a autenticação apropriada.

> **Importante:**
>
> O XenMobile não oferece suporte à alteração do modo de autenticação de autenticação de domínio para um modo de autenticação diferente depois que os usuários registram dispositivos no XenMobile.

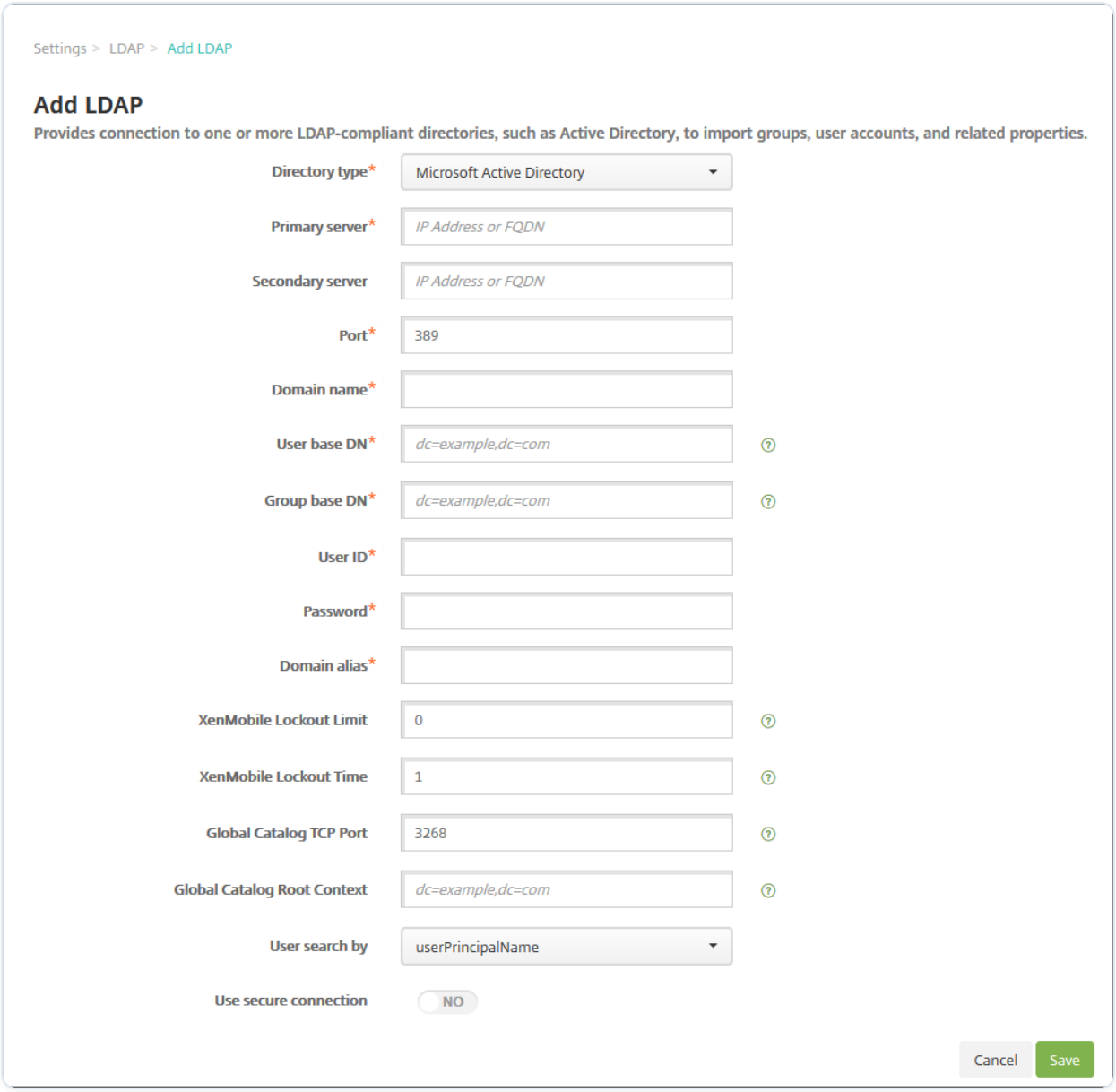
Para adicionar conexões LDAP no XenMobile

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **LDAP**. A página **LDAP** é exibida. Você pode adicionar, editar ou excluir diretórios compatíveis com LDAP, conforme descrito neste artigo.



Para adicionar um diretório compatível com LDAP

1. Na página **LDAP**, clique em **Adicionar**. A página **Adicionar LDAP** é exibida.



2. Configure estas configurações:

- **Tipo de diretório:** Na lista, clique no tipo de diretório apropriado. O padrão é **Microsoft Active Directory**.
- **Servidor primário:** Digite o servidor primário usado para LDAP; você pode inserir o endereço IP ou o nome de domínio totalmente qualificado (FQDN).
- **Servidor secundário:** Opcionalmente, se um servidor secundário tiver sido configurado, insira o endereço IP ou FQDN para o servidor secundário. Este servidor é um servidor de failover usado se o servidor primário não puder ser alcançado.
- **Porta:** Digite o número da porta usado pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número da porta **636** para conexões LDAP seguras, use **3268** para conexões LDAP não seguras da Microsoft ou **3269** para conexões LDAP seguras da Microsoft.
- **Nome de domínio:** Digite o nome de domínio.
- **DN base do usuário:** Digite o local dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users`, `dc=example` ou `dc=com`.
- **DN base do grupo:** Digite o local dos grupos no Active Directory. Por exemplo, `cn=users, dc=domain, dc=net` onde `cn=users` representa o nome do contêiner dos grupos e `dc` representa o componente de domínio do Active Directory.
- **ID do usuário:** Digite o ID do usuário associado à conta do Active Directory.
- **Senha:** Digite a senha associada ao usuário.
- **Alias de domínio:** Digite um alias para o nome de domínio. Se você alterar a configuração de **Alias de domínio** após o registro, os usuários deverão se registrar novamente.
- **Limite de bloqueio do XenMobile:** Digite um número entre **0** e **999** para o número de tentativas de logon com falha. Um valor de **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de logon com falha.
- **Tempo de bloqueio do XenMobile:** Digite um número entre **0** e **99999** representando o número de minutos que um usuário deve esperar após exceder o limite de bloqueio. Um valor de **0** significa que o usuário não é forçado a esperar após um bloqueio.
- **Porta TCP do Catálogo Global:** Digite o número da porta TCP para o servidor de Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número da porta **3269**.

- **Contexto Raiz do Catálogo Global:** Opcionalmente, digite o valor do Contexto Raiz Global usado para habilitar uma pesquisa de catálogo global no Active Directory. Esta pesquisa é um adicional à pesquisa LDAP padrão, em qualquer domínio sem a necessidade de especificar o nome de domínio real.
- **Pesquisa de usuário por:** Na lista, clique em **userPrincipalName** ou **sAMAccountName**. O padrão é **userPrincipalName**. Se você alterar a configuração de **Pesquisa de usuário por** após o registro, os usuários deverão se registrar novamente.
- **Usar conexão segura:** Selecione se deseja usar conexões seguras. O padrão é **NÃO**.

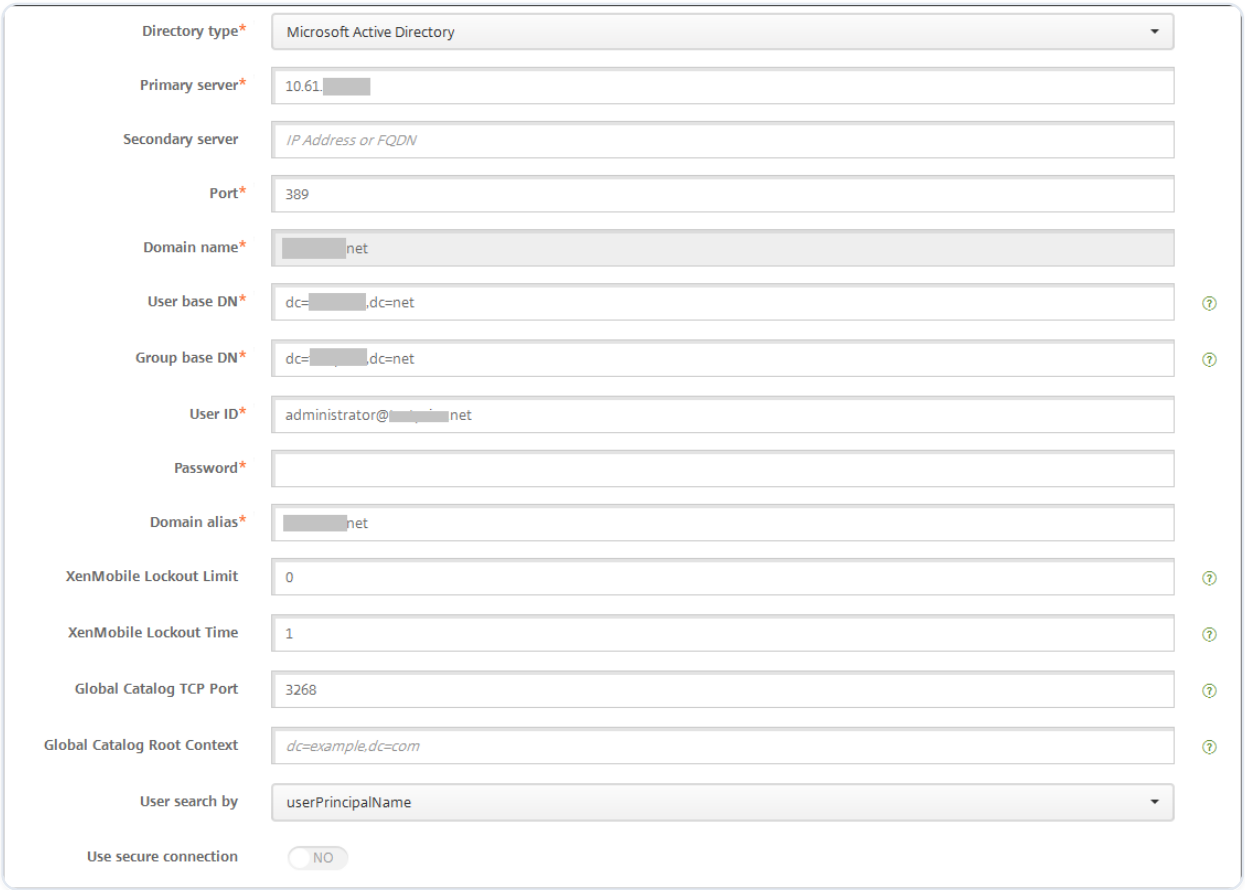
3. Clique em **Salvar**.

Para editar um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório a ser editado.

   Ao selecionar a caixa de seleção ao lado de um diretório, o menu de opções aparece acima da lista LDAP. Clique em qualquer outro lugar na lista e o menu de opções aparecerá no lado direito da listagem.

2. Clique em **Editar**. A página **Editar LDAP** é exibida.



3. Altere as seguintes informações conforme apropriado:

- **Tipo de diretório:** Na lista, clique no tipo de diretório apropriado.
- **Servidor primário:** Digite o servidor primário usado para LDAP; você pode inserir o endereço IP ou o nome de domínio totalmente qualificado (FQDN).
- **Servidor secundário:** Opcionalmente, digite o endereço IP ou FQDN para o servidor secundário (se um tiver sido configurado).
- **Porta:** Digite o número da porta usado pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número da porta **636** para conexões LDAP seguras, use **3268** para conexões LDAP não seguras da Microsoft ou **3269** para conexões LDAP seguras da Microsoft.
- **Nome de domínio:** Você não pode alterar este campo.
- **DN base do usuário:** Digite o local dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users`, `dc=example` ou `dc=com`.
- **DN base do grupo:** Digite o nome do grupo DN base do grupo especificado como `cn=groupname`. Por exemplo, `cn=users, dc=servername, dc=net` onde `cn=users` é o nome do grupo. `DN` e `servername` representam o nome do servidor que executa o Active Directory.
- **ID de usuário:** Digite o ID de usuário associado à conta do Active Directory.
- **Senha:** Digite a senha associada ao usuário.
- **Alias de domínio:** Digite um alias para o nome de domínio. Se você alterar a configuração de **Alias de domínio** após o registro, os usuários deverão se registrar novamente.
- **Limite de bloqueio do XenMobile:** Digite um número entre **0** e **999** para o número de tentativas de logon com falha. Um valor de **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de logon com falha.
- **Tempo de bloqueio do XenMobile:** Digite um número entre **0** e **99999** representando o número de minutos que um usuário deve esperar após exceder o limite de bloqueio. Um valor de **0** significa que o usuário não é forçado a esperar após um bloqueio.
- **Porta TCP do Catálogo Global:** Digite o número da porta TCP para o servidor de Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número da porta **3269**.
- **Contexto Raiz do Catálogo Global:** Opcionalmente, digite o valor do Contexto Raiz Global usado para habilitar uma pesquisa de catálogo global no Active Directory. Esta pesquisa é um complemento à pesquisa LDAP padrão, em qualquer domínio, sem a necessidade de especificar o nome de domínio real.

- **Pesquisa de usuário por:** Na lista, clique em **userPrincipalName** ou **sAMAccountName**. Se você alterar a configuração de **Pesquisa de usuário por** após o registro, os usuários deverão se registrar novamente.
- **Usar conexão segura:** Selecione se deseja usar conexões seguras.

4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório que você deseja excluir.

   Você pode selecionar mais de uma propriedade para excluir marcando a caixa de seleção ao lado de cada propriedade.

2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Configurar autenticação para vários domínios

Para configurar o XenMobile Server para usar vários sufixos de domínio em uma configuração LDAP, consulte o procedimento na documentação do Citrix Endpoint Management, Configurar autenticação para vários domínios. As etapas são as mesmas na versão local do XenMobile Server e na versão em nuvem do Endpoint Management.

Configurar autenticação de domínio mais token de segurança

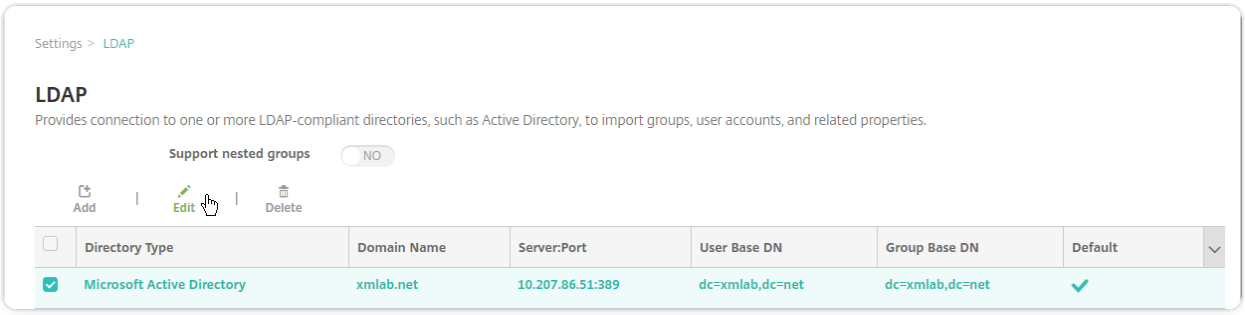
Você pode configurar o XenMobile para exigir que os usuários autenticar com suas credenciais LDAP mais uma senha de uso único, usando o protocolo RADIUS.

Para usabilidade ideal, você pode combinar essa configuração com o PIN do Citrix e o cache de senhas do Active Directory. Com essa configuração, os usuários não precisam inserir seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

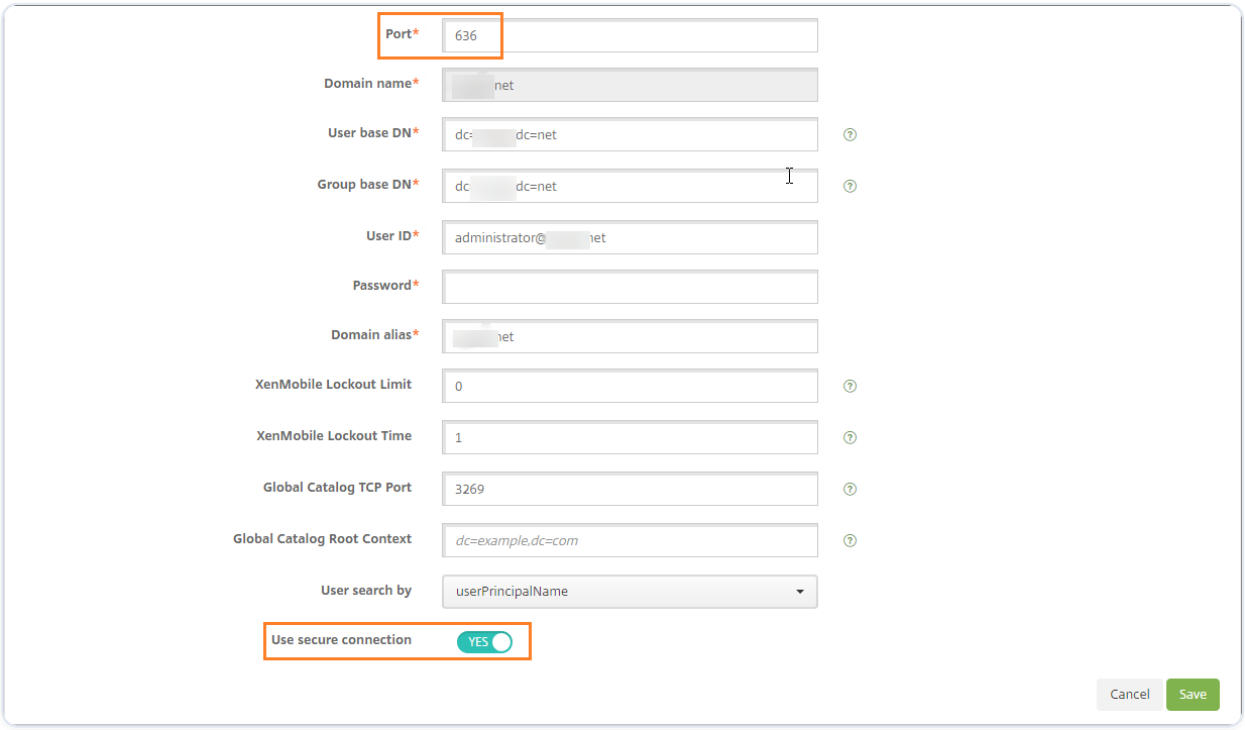
Configurar configurações LDAP

O uso de LDAP para autenticação exige que você instale um certificado SSL de uma Autoridade de Certificação no XenMobile. Para obter informações, consulte Carregando certificados no XenMobile.

1. Em **Configurações**, clique em **LDAP**.
2. Selecione **Microsoft Active Directory** e clique em **Editar**.



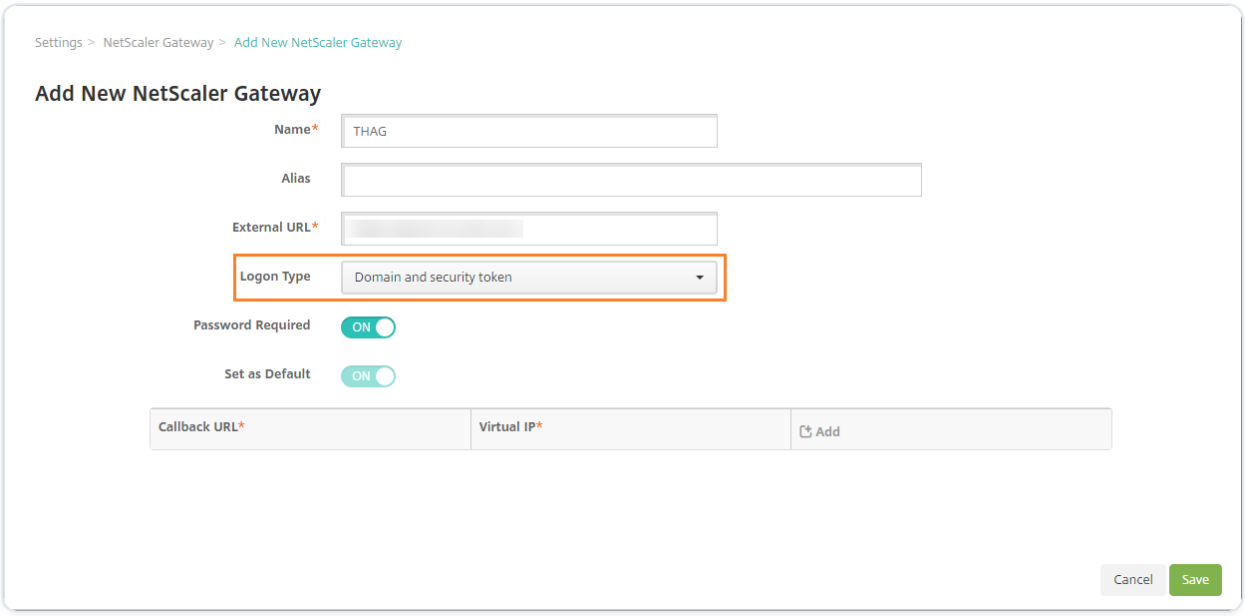
3. Verifique se a Porta é **636**, que é para conexões LDAP seguras, ou **3269** para conexões LDAP seguras da Microsoft.
4. Altere **Usar conexão segura** para **Sim**.



Configurar configurações do Citrix Gateway

As etapas a seguir pressupõem que você já adicionou uma instância do Citrix Gateway ao XenMobile. Para adicionar uma instância do Citrix Gateway, consulte Adicionar uma instância do Citrix Gateway.

1. Em **Configurações**, clique em **Citrix Gateway**.
2. Selecione o **"Citrix Gateway** e depois clique em **Editar**.
3. Em **Tipo de Logon**, selecione **Domínio e token de segurança**.



Habilitar Citrix PIN e cache de senha do usuário

Para habilitar o Citrix PIN e o cache de senha do usuário, vá para **Settings > Client Properties** e selecione estas caixas de seleção: **Enable Citrix PIN Authentication** e **Enable User Password Caching**. Para obter mais informações, consulte Propriedades do cliente.

Configurar o Citrix Gateway para autenticação de domínio e token de segurança

Configure perfis e políticas de sessão do Citrix Gateway para seus servidores virtuais usados com o XenMobile. Para obter informações, consulte a documentação do Citrix Gateway.

Certificado de cliente ou certificado mais autenticação de domínio

A configuração padrão para XenMobile® é autenticação de nome de usuário e senha. Para adicionar outra camada de segurança para registro e acesso ao ambiente XenMobile, considere usar a autenticação baseada em certificado. No ambiente XenMobile, essa configuração é a melhor combinação de segurança e experiência do usuário. A autenticação de certificado mais domínio tem as melhores possibilidades de SSO, juntamente com a segurança fornecida pela autenticação de dois fatores no Citrix ADC.

Para usabilidade ideal, você pode combinar a autenticação de certificado mais domínio com o PIN do Citrix e o cache de senha do Active Directory. Como resultado, os usuários não precisam inserir seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

> **Importante:**

> O XenMobile não oferece suporte à alteração do modo de autenticação de autenticação de domínio para algum outro modo de autenticação depois que os usuários registram dispositivos no XenMobile.

> Se você não permitir LDAP e usar cartões inteligentes ou métodos semelhantes, a configuração de certificados permite representar um cartão inteligente para o XenMobile. Os usuários então se registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que um usuário tem acesso, o XenMobile cria e implanta o certificado usado para autenticar no ambiente XenMobile.

Você pode usar o assistente Citrix ADC para XenMobile para realizar a configuração necessária para o XenMobile ao usar a autenticação somente por certificado do Citrix ADC ou a autenticação por certificado mais domínio. Você pode executar o assistente Citrix ADC para XenMobile apenas uma vez.

Em ambientes altamente seguros, o uso de credenciais LDAP fora de uma organização em redes públicas ou inseguras é considerado uma grande ameaça à segurança da organização. Para ambientes altamente seguros, a autenticação de dois fatores que usa um certificado de cliente e um token de segurança é uma opção. Para obter informações, consulte Configuring XenMobile for Certificate and Security Token Authentication.

A autenticação por certificado de cliente está disponível para o modo MAM do XenMobile (somente MAM) e modo ENT (quando os usuários se registram no MDM). A autenticação por certificado de cliente não está disponível para o modo ENT do XenMobile quando os usuários se registram no modo MAM herdado. Para usar a autenticação por certificado de cliente para os modos ENT e MAM do XenMobile, você deve configurar o servidor Microsoft, o XenMobile Server e, em seguida, o Citrix Gateway. Siga estas etapas gerais, conforme descrito neste artigo.

No servidor Microsoft:

1. Adicione um snap-in de certificado ao Microsoft Management Console.
2. Adicione o modelo à Autoridade de Certificação (CA).
3. Crie um certificado PFX a partir do servidor CA.

No XenMobile Server:

1. Carregue o certificado para o XenMobile.
2. Criar a entidade PKI para autenticação baseada em certificado.

3. Configurar provedores de credenciais.
4. Configurar o Citrix Gateway para entregar um certificado de usuário para autenticação.

Para obter informações sobre a configuração do Citrix Gateway, consulte estes artigos na documentação do Citrix ADC:

- Autenticação de cliente
- Infraestrutura de perfil SSL
- Configurando e Vinculando uma Política de Autenticação de Certificado de Cliente

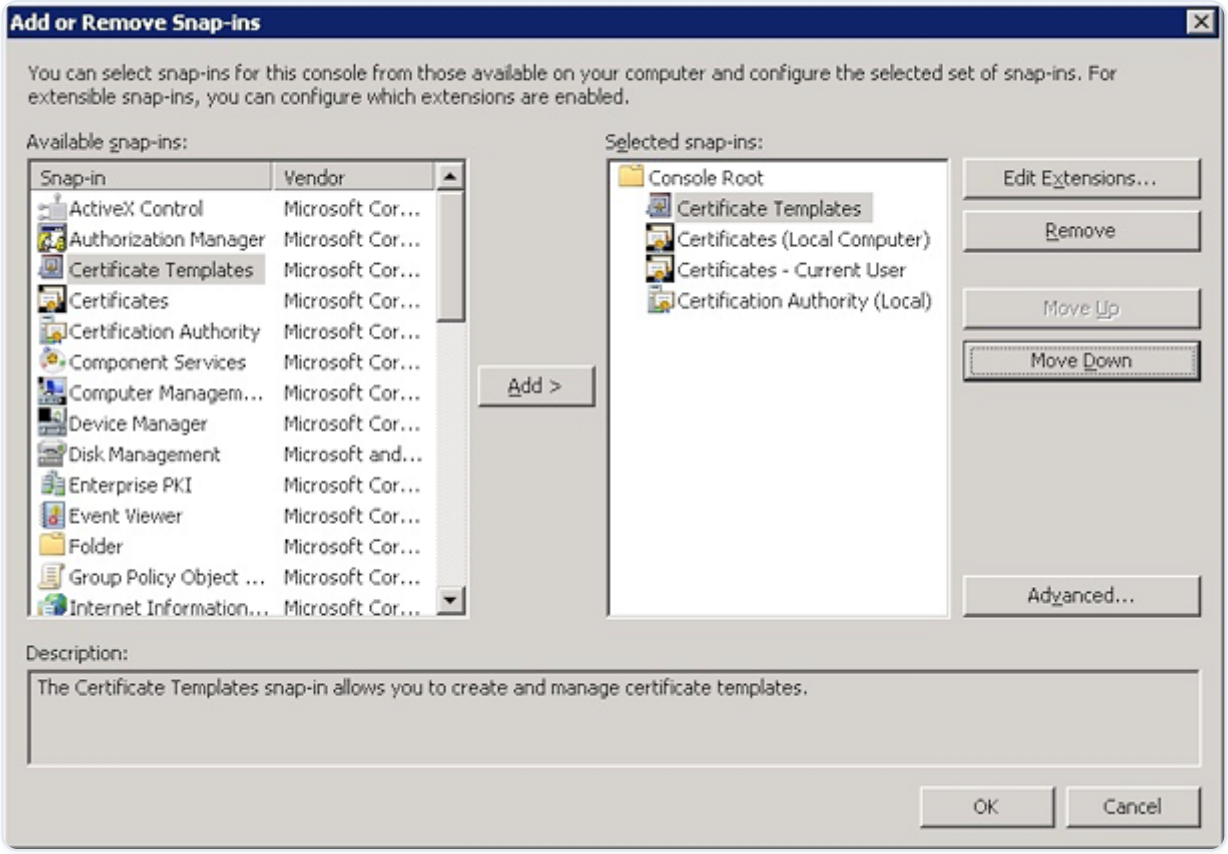
Pré-requisitos

- Ao criar um modelo de Entidade de Serviços de Certificado da Microsoft, evite possíveis problemas de autenticação com dispositivos registrados, excluindo caracteres especiais. Por exemplo, não use estes caracteres no nome do modelo: `: ! $ () # % + * ~ ? | {} []`
- Para configurar a Autenticação baseada em Certificado para o Exchange ActiveSync, consulte este blog da Microsoft. Configure o site do servidor da autoridade de certificação (CA) para que o Exchange ActiveSync exija certificados de cliente.
- Se você usar certificados de servidor privados para proteger o tráfego do ActiveSync para o Exchange Server, certifique-se de que os dispositivos móveis tenham todos os certificados Raiz/Intermediários necessários. Caso contrário, a autenticação baseada em certificado falhará durante a configuração da caixa de correio no Secure Mail. No Console do IIS do Exchange, você deve:
  - Adicionar um site para uso do XenMobile com o Exchange e vincular o certificado do servidor web.
  - Usar a porta 9443.
  - Para esse site, você deve adicionar dois aplicativos, um para "Microsoft-Server-ActiveSync" e outro para "EWS". Para ambos os aplicativos, em **Configurações SSL**, selecione **Exigir SSL**.

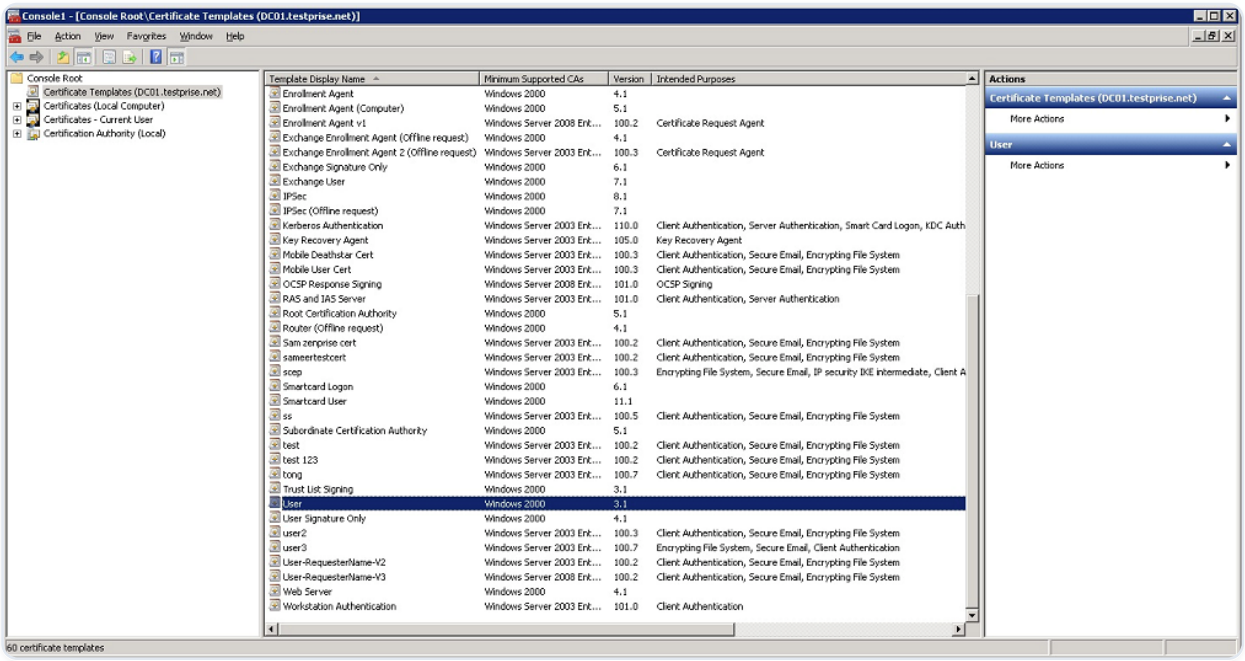
Adicionar um snap-in de certificado ao Microsoft Management Console

1. Abra o console e clique em **Adicionar/Remover Snap-ins**.
2. Adicione os seguintes snap-ins:
   - Modelos de Certificado
   - Certificados (Computador Local)

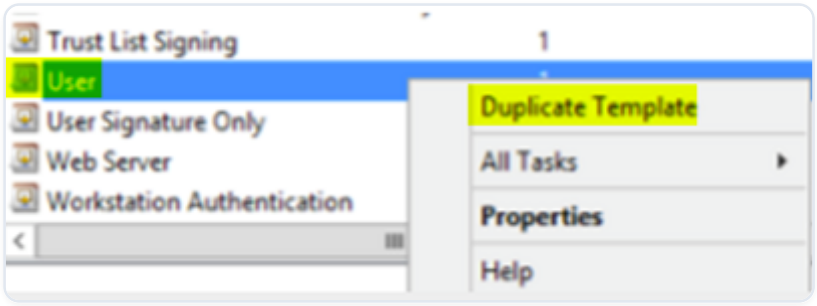
- Certificados - Usuário Atual
- Autoridade de Certificação (Local)



3. Expanda **Modelos de Certificado**.



4. Selecione o modelo **Usuário** e **Duplicar Modelo**.



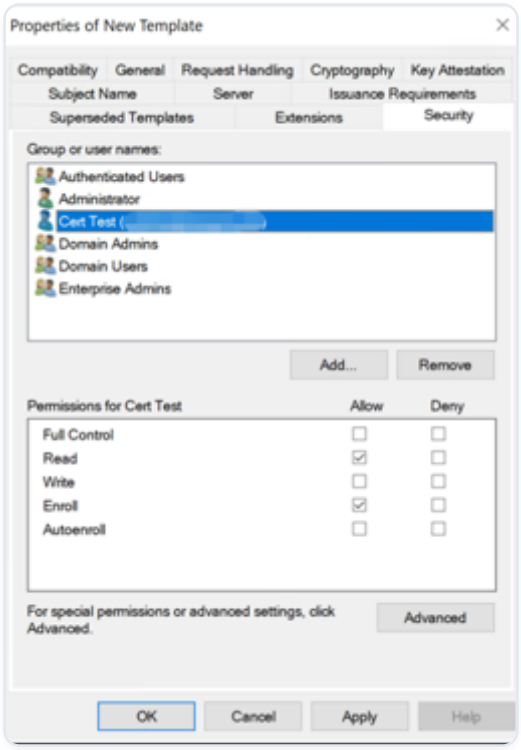
5. Forneça o nome de exibição do Modelo.

> **Importante:**
>
> Não é recomendado selecionar a opção **Publicar certificado no Active Directory**. Se esta opção for selecionada, ela cria certificados de cliente para todos os usuários no Active Directory, o que pode sobrecarregar seu banco de dados do Active Directory.

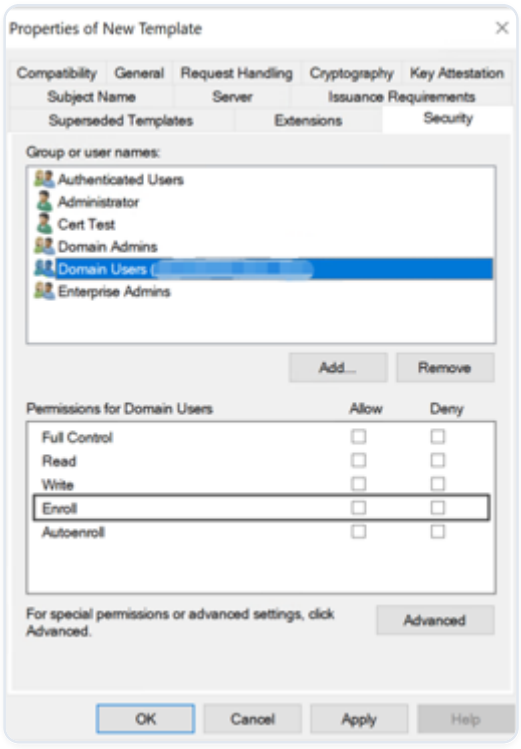
6. Selecione **Windows 2003 Server** para o tipo de modelo. No servidor Windows 2012 R2, em **Compatibilidade**, selecione **Autoridade de certificação** e defina o destinatário como **Windows 2003**.
7. Em **Segurança**, configure o seguinte:

   a. Clique em **Adicionar** e selecione a conta de usuário do AD que o XenMobile Server usa para gerar certificados.

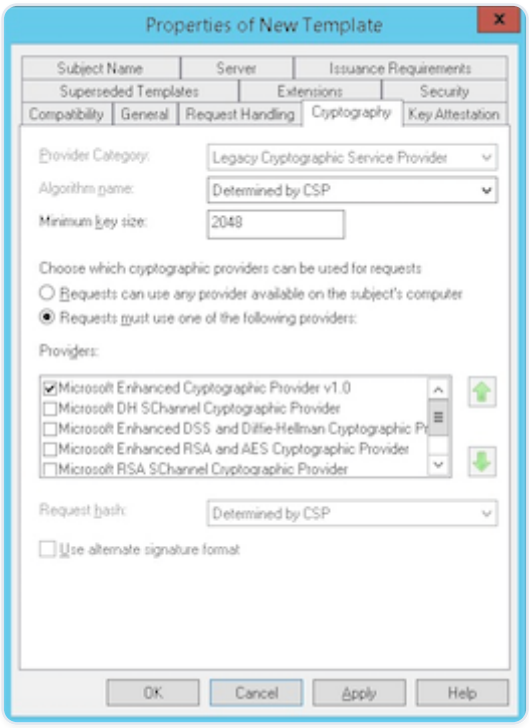
   > **Importante:**
   >
   > Adicione apenas o usuário da conta de serviço aqui. Adicione a permissão de **Registro** apenas a esta conta de usuário do AD.
   >
   > Conforme descrito posteriormente neste artigo, você cria um certificado .pfx de usuário usando a conta de serviço. Para obter informações, consulte Criando um certificado PFX do servidor CA.



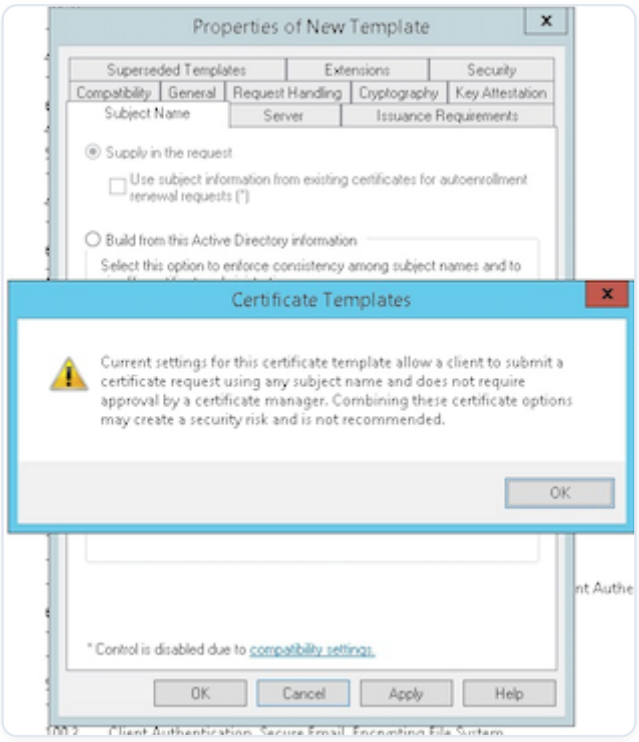
b. Revogue a permissão de **Registro** de **Usuários do Domínio**.



8. Em **Criptografia**, certifique-se de fornecer o tamanho da chave. Você inserirá o tamanho da chave posteriormente ao configurar o XenMobile.

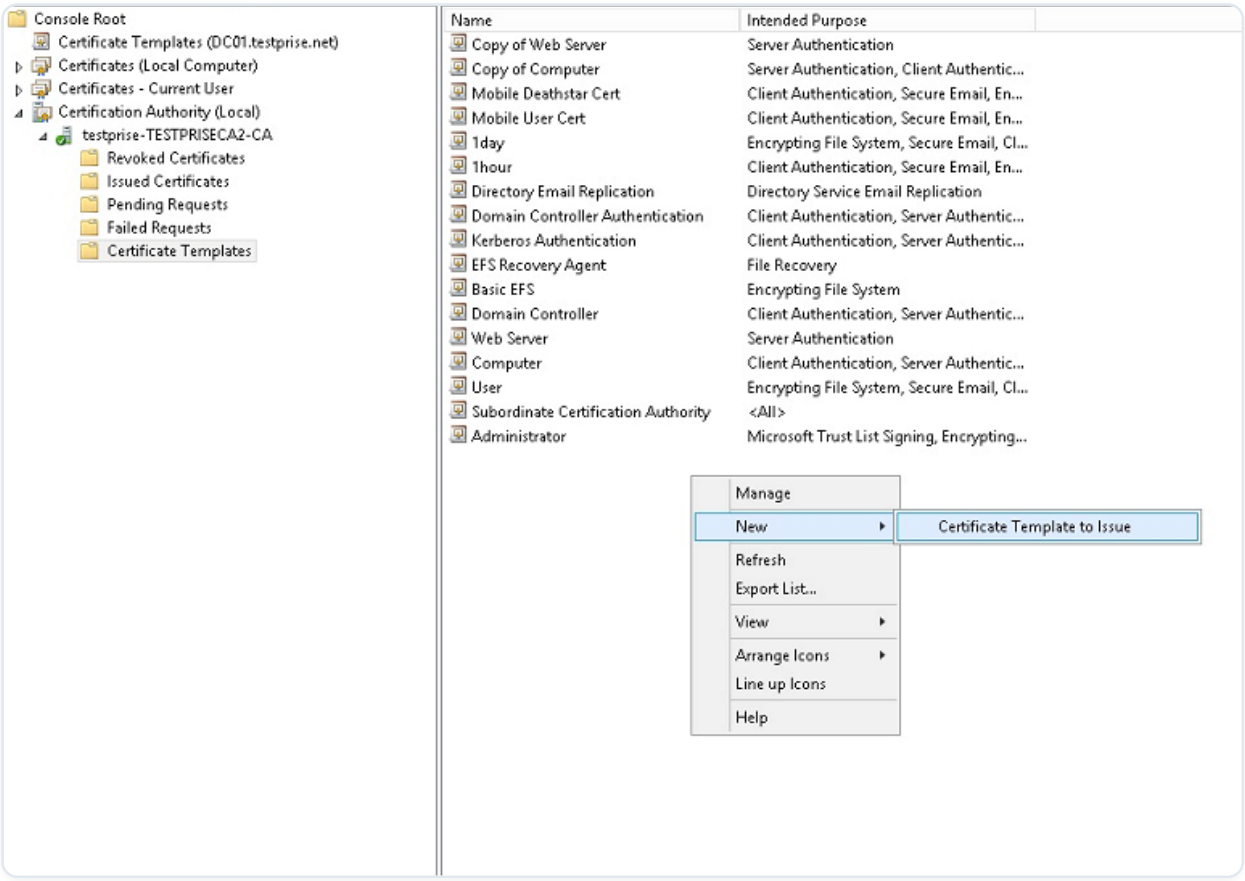


9. Em **Nome do Assunto**, selecione **Fornecer na solicitação**. Aplique as alterações e salve.

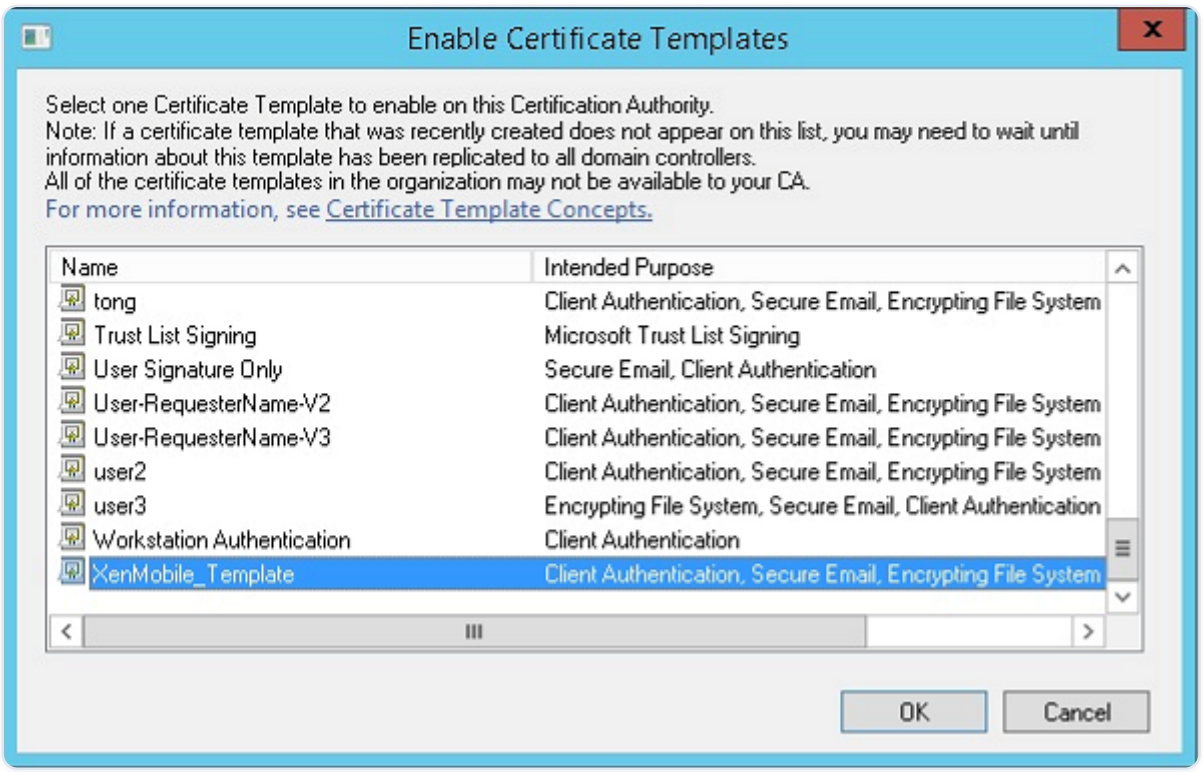


Adicionando o modelo à Autoridade de Certificação

1. Vá para **Autoridade de Certificação** e selecione **Modelos de Certificado**.
2. Clique com o botão direito no painel direito e selecione **Novo > Modelo de Certificado a Ser Emitido**.

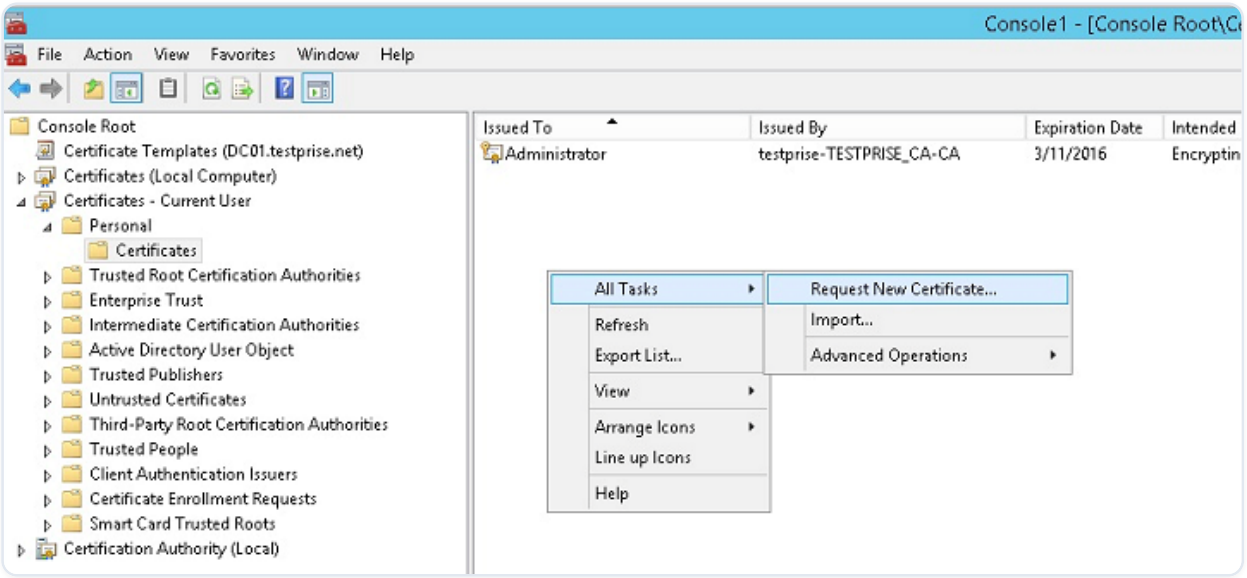


3. Selecione o modelo que você criou na etapa anterior e clique em **OK** para adicioná-lo à **Autoridade de Certificação**.

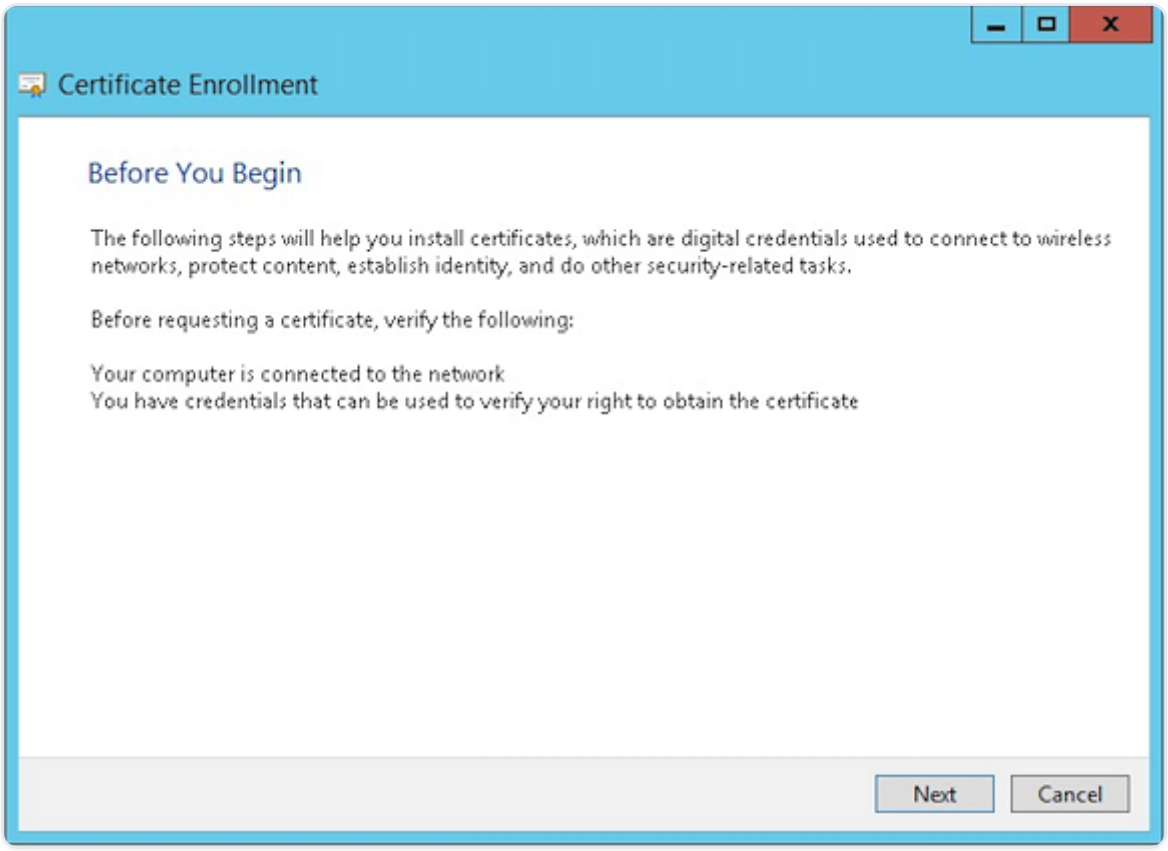


Criando um certificado PFX a partir do servidor CA

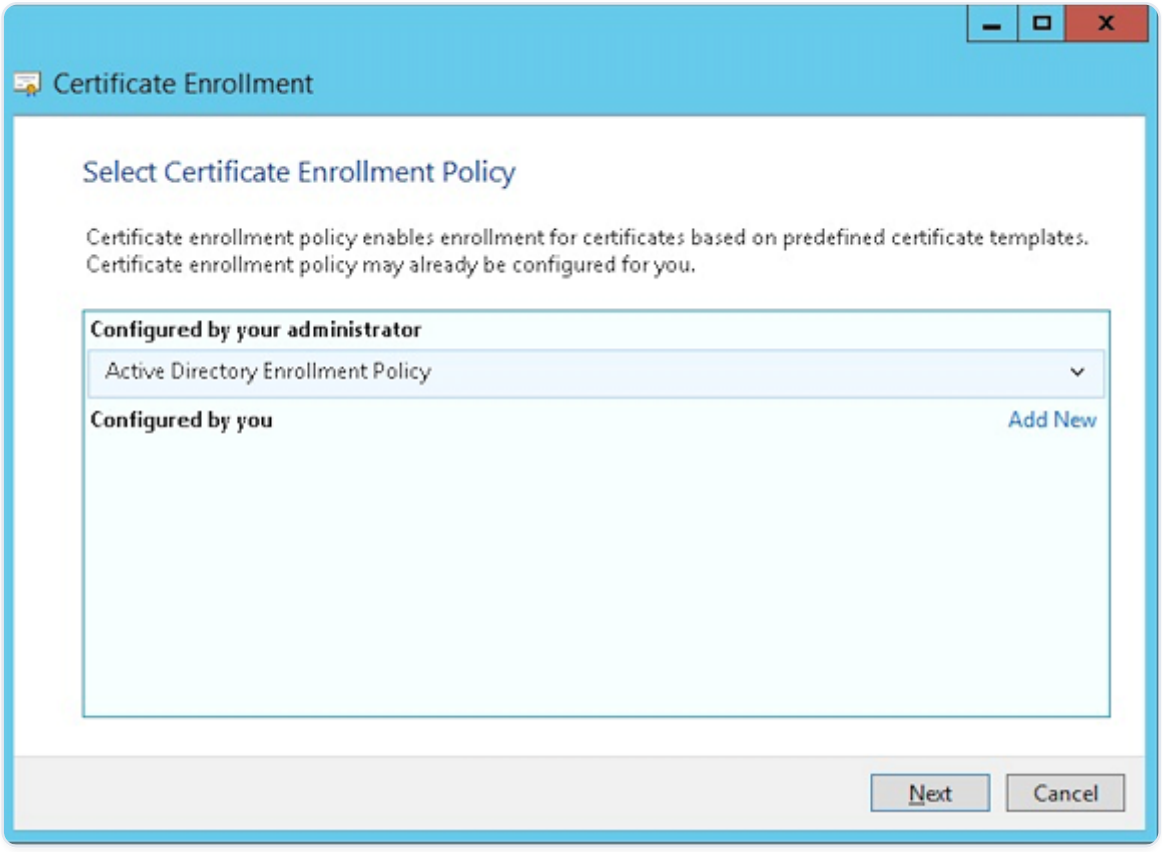
1. Crie um certificado .pfx de usuário usando a conta de serviço com a qual você fez login. O .pfx é carregado para o XenMobile, que então solicita um certificado de usuário em nome dos usuários que registram seus dispositivos.
2. Em **Usuário Atual**, expanda **Certificados**.
3. Clique com o botão direito no painel direito e, em seguida, clique em **Solicitar Novo Certificado**.



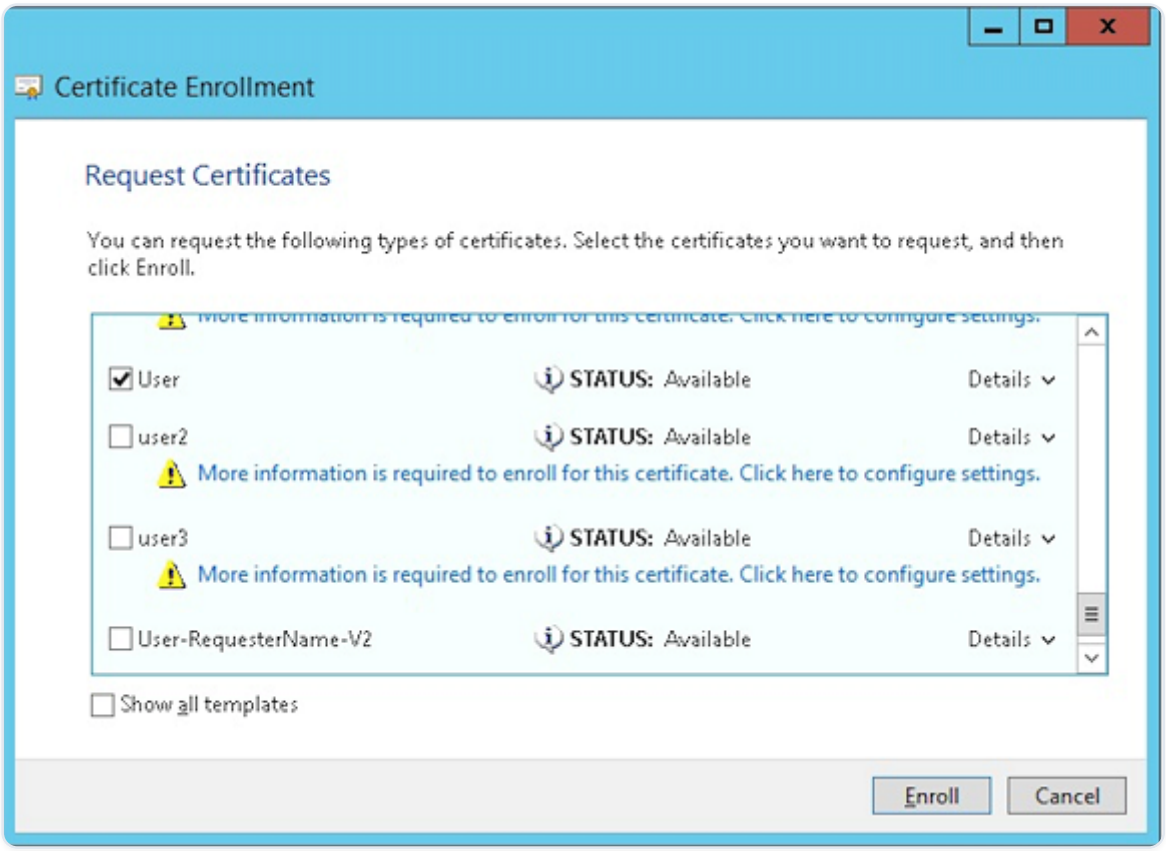
4. A tela **Registro de Certificado** é exibida. Clique em **Avançar**.



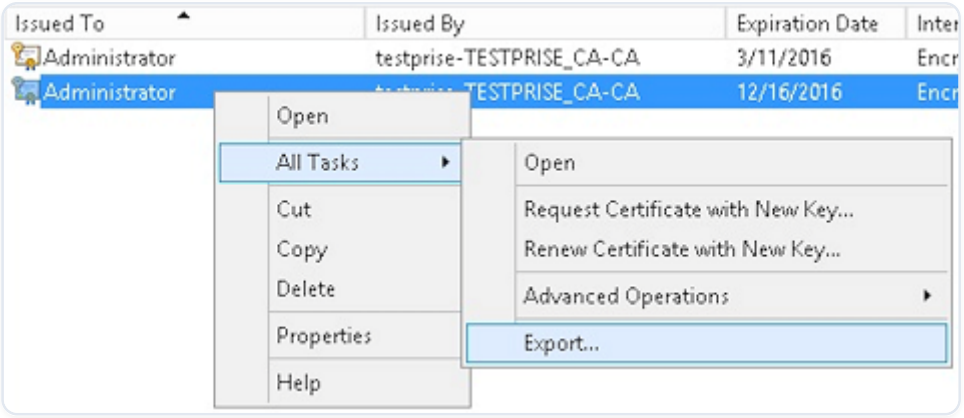
5. Selecione **Política de Registro do Active Directory** e, em seguida, clique em **Avançar**.



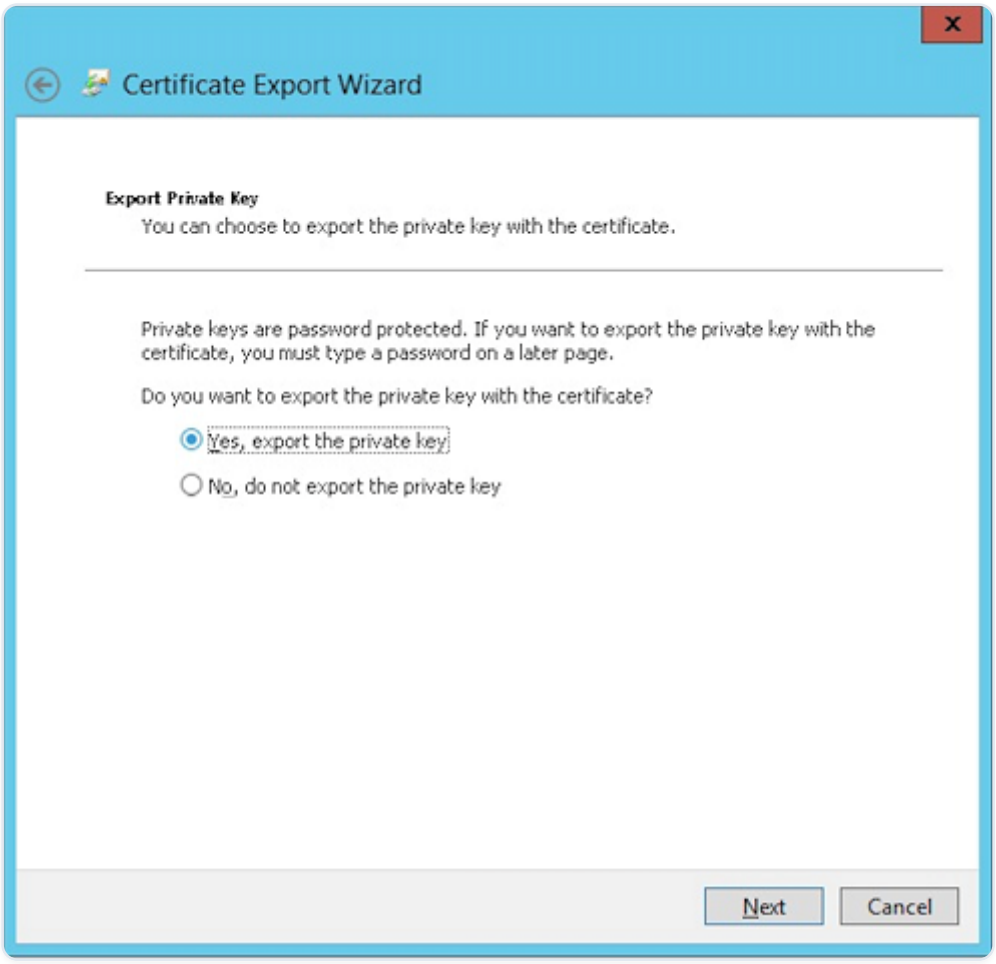
6. Selecione o modelo **Usuário** e, em seguida, clique em **Registrar**.



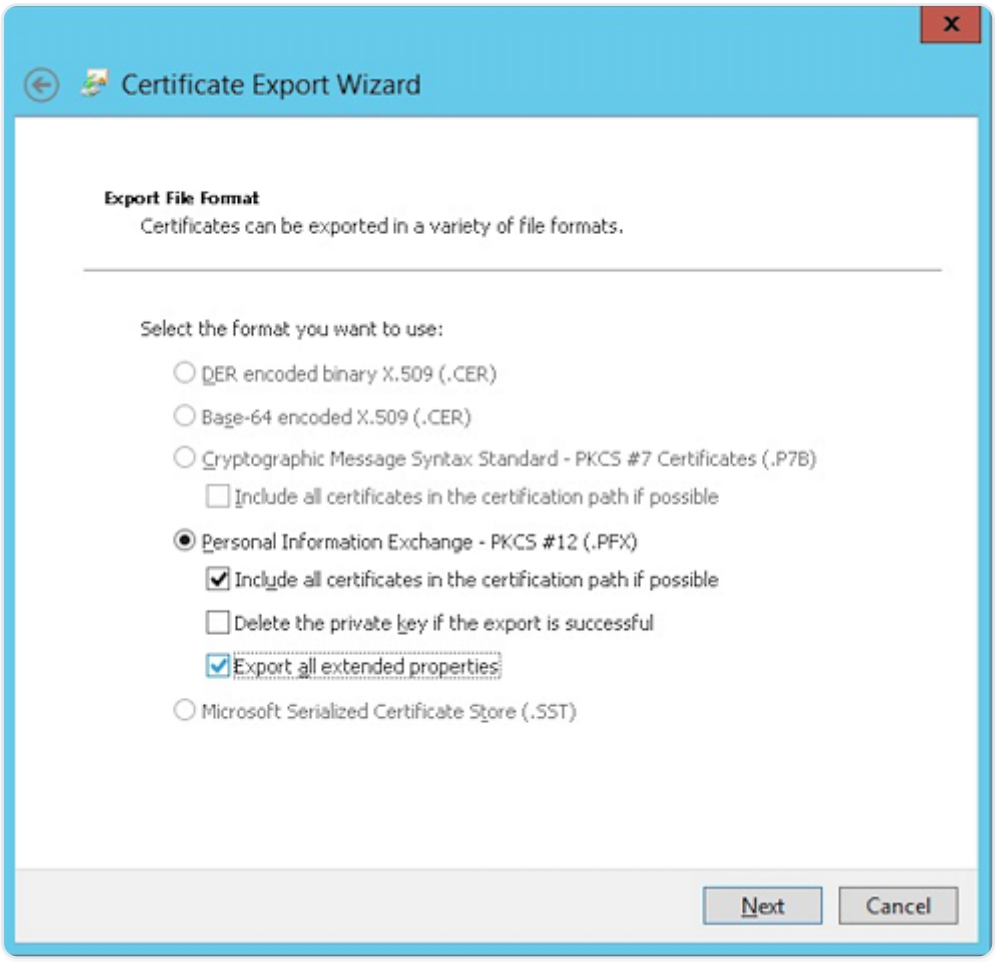
7. Exporte o arquivo .pfx que você criou na etapa anterior.



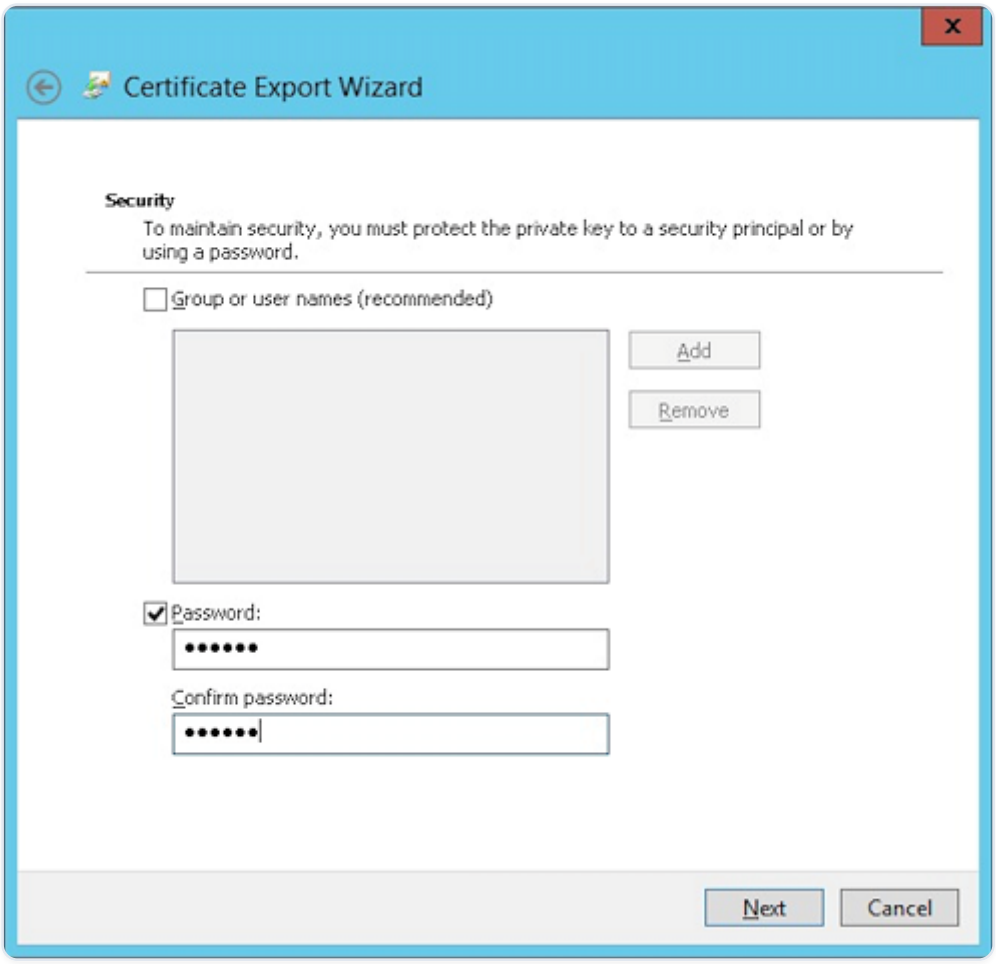
8. Clique em **Sim, exportar a chave privada**.



9. Selecione **Incluir todos os certificados no caminho de certificação, se possível** e marque a caixa de seleção **Exportar todas as propriedades estendidas**.



10. Defina uma senha para usar ao carregar este certificado no XenMobile.

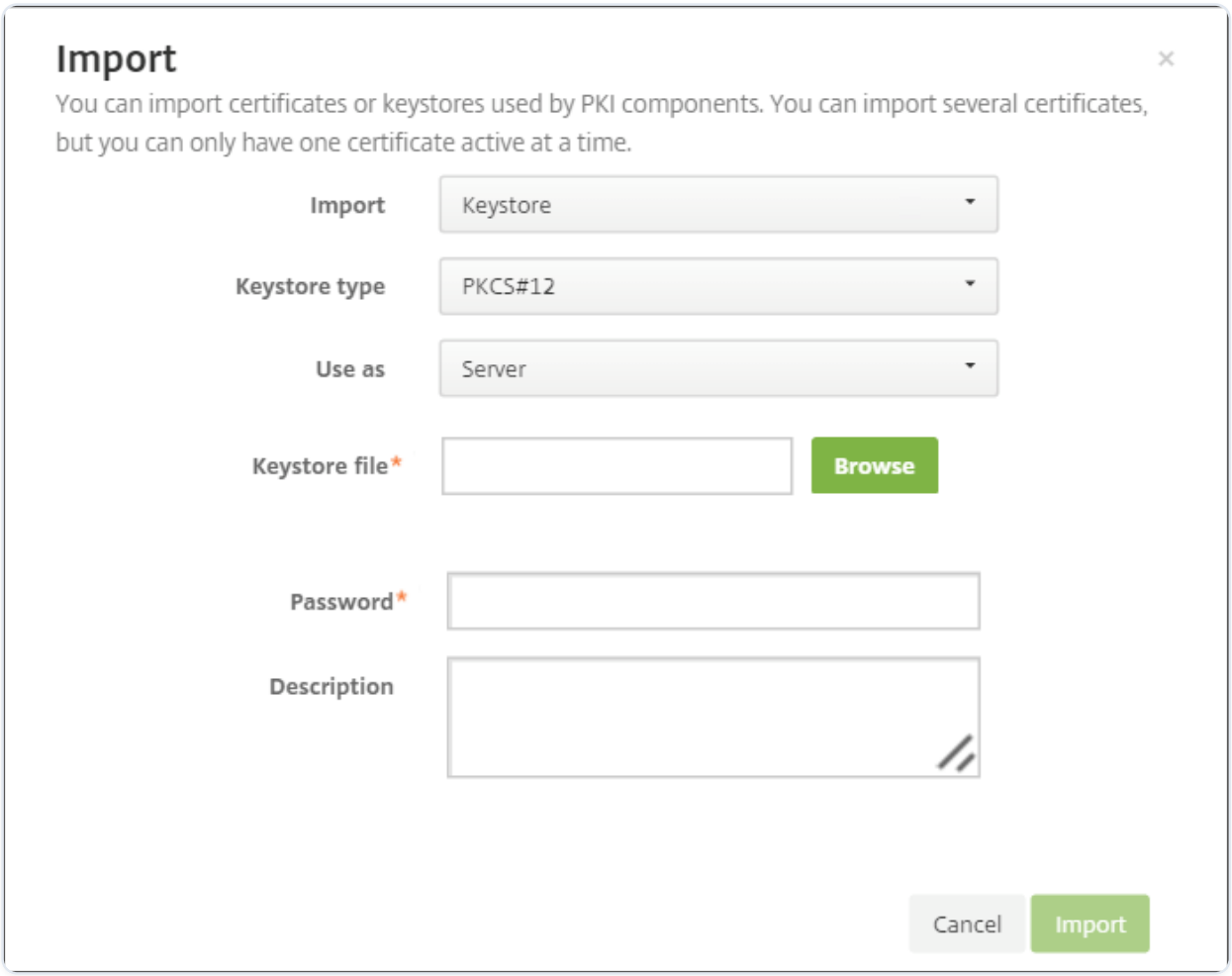


11. Salve o certificado em seu disco rígido.

Carregando o certificado para o XenMobile

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Clique em **Certificados** e, em seguida, clique em **Importar**.
3. Insira os seguintes parâmetros:

   - **Importar:** Keystore
   - **Tipo de Keystore:** PKCS #12
   - **Usar como:** Servidor
   - **Arquivo Keystore:** Clique em **Procurar** para selecionar o certificado `.pfx` que você criou.
   - **Senha:** Insira a senha que você criou para este certificado.



4. Clique em **Importar**.
5. Verifique se o certificado foi instalado corretamente. Um certificado instalado corretamente é exibido como um certificado de Usuário.

Criando a entidade PKI para autenticação baseada em certificado

1. Em **Configurações**, vá para **Mais > Gerenciamento de Certificados > Entidades PKI**.
2. Clique em **Adicionar** e depois clique em **Entidade de Serviços de Certificado Microsoft**. A tela **Entidade de Serviços de Certificado Microsoft: Informações Gerais** é exibida.
3. Insira os seguintes parâmetros:

   - **Nome:** Digite qualquer nome
   - **URL raiz do serviço de registro da Web:** `https://RootCA-URL/certsrv/` (Certifique-se de adicionar a última barra, /, no caminho da URL.)
   - **Nome da página certnew.cer:** certnew.cer (valor padrão)
   - **certfnsh.asp:** certfnsh.asp (valor padrão)
   - **Tipo de autenticação:** Certificado de cliente

- **Certificado de cliente SSL:** Selecione o Certificado de Usuário a ser usado para emitir o certificado de cliente XenMobile.

Tela de configuração de certificados(/en-us/xenmobile/server/media/add-pki-entity-1.png)

4. Em **Modelos**, adicione o modelo que você criou ao configurar o certificado Microsoft. Não adicione espaços.

   Tela de configuração de certificados(/en-us/xenmobile/server/media/add-pki-entity-2.png)

5. Ignore os Parâmetros HTTP e, em seguida, clique em **Certificados CA**.
6. Selecione o nome da CA raiz que corresponde ao seu ambiente. Essa CA raiz faz parte da cadeia importada do certificado de cliente do XenMobile.

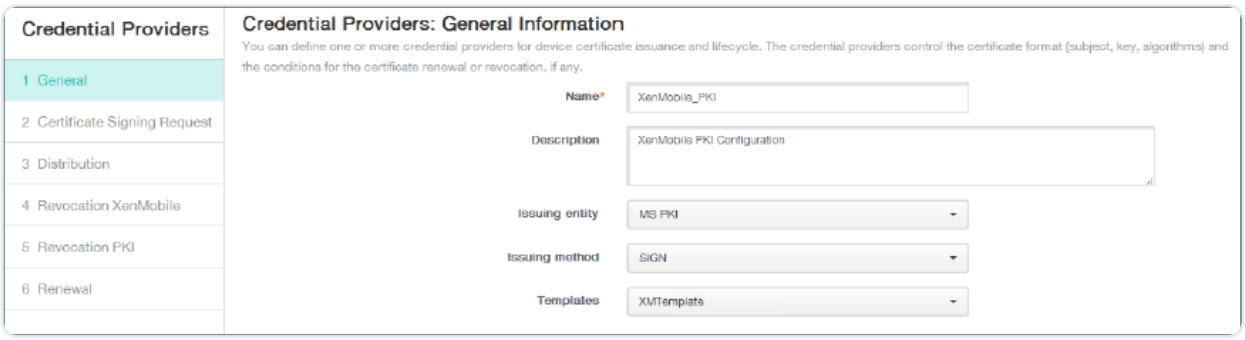
   Tela de configuração de certificados(/en-us/xenmobile/server/media/add-pki-entity-3.png)

7. Clique em **Salvar**.

Configurando provedores de credenciais

1. Em **Configurações**, vá para **Mais > Gerenciamento de Certificados > Provedores de Credenciais**.
2. Clique em **Adicionar**.
3. Em **Geral**, insira os seguintes parâmetros:

   - **Nome:** Digite qualquer nome.
   - **Descrição:** Digite qualquer descrição.
   - **Entidade emissora:** Selecione a entidade PKI criada anteriormente.
   - **Método de emissão:** SIGN
   - **Modelos:** Selecione o modelo adicionado na entidade PKI.



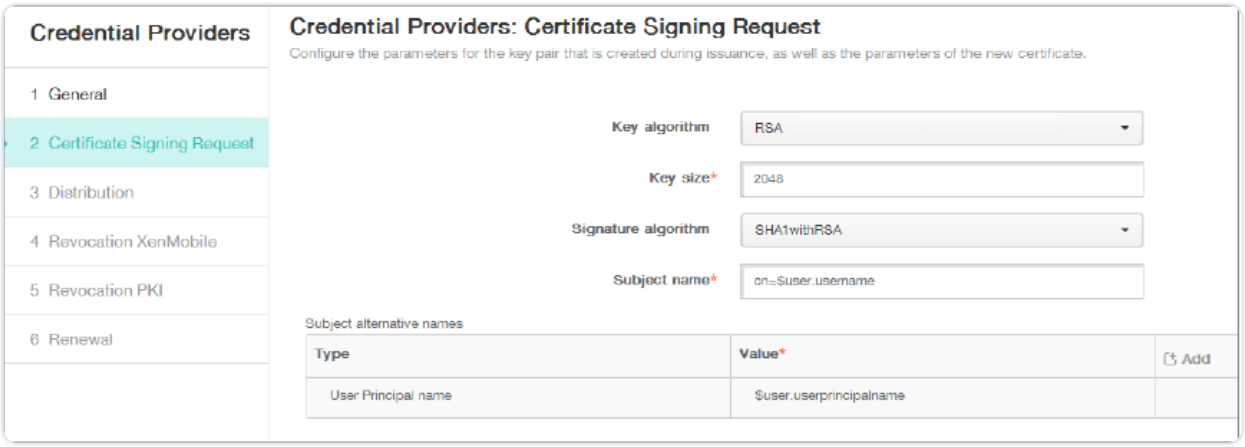
4. Clique em **Solicitação de Assinatura de Certificado** e insira os seguintes parâmetros:

   - **Algoritmo de chave:** RSA

- **Tamanho da chave:** 2048
- **Algoritmo de assinatura:** SHA256withRSA
- **Nome do assunto:** `cn=$user.username`

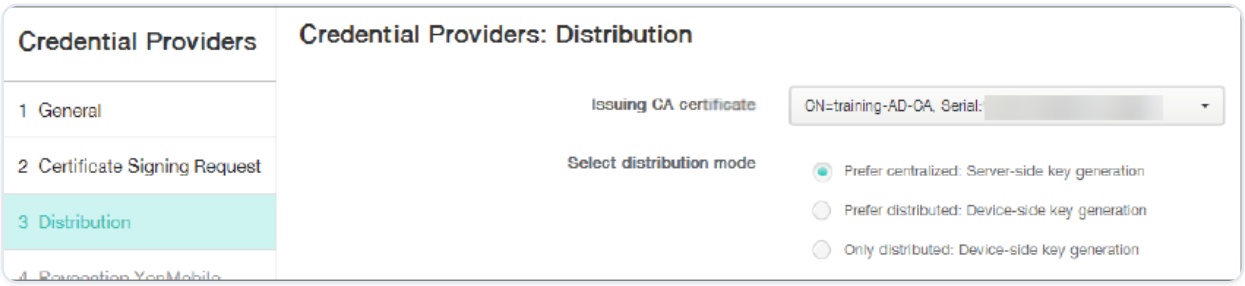
Para **Nomes Alternativos do Assunto**, clique em **Adicionar** e insira os seguintes parâmetros:

- **Tipo:** Nome Principal do Usuário
- **Valor:** `$user.userprincipalname`

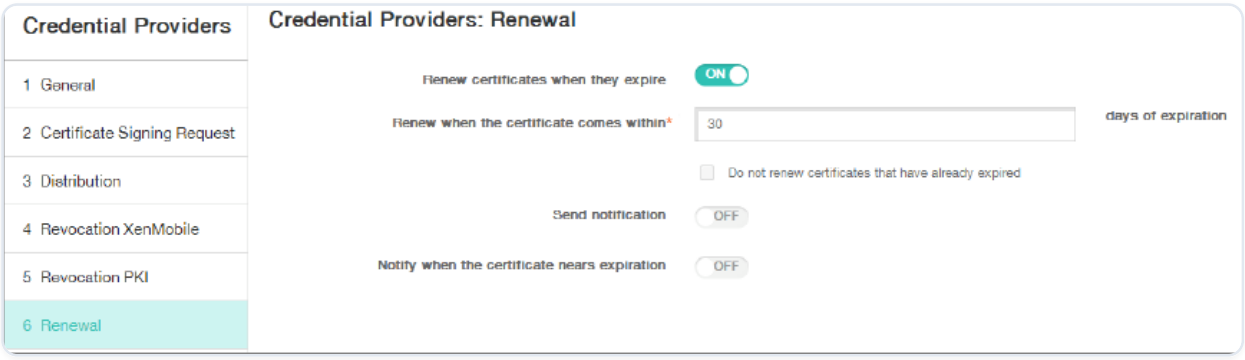


5. Clique em **Distribuição** e insira os seguintes parâmetros:

   - **Certificado da CA Emissora:** Selecione a CA Emissora que assinou o Certificado de Cliente XenMobile.
   - **Selecionar modo de distribuição:** Selecione **Preferir centralizado: Geração de chave no lado do servidor**.



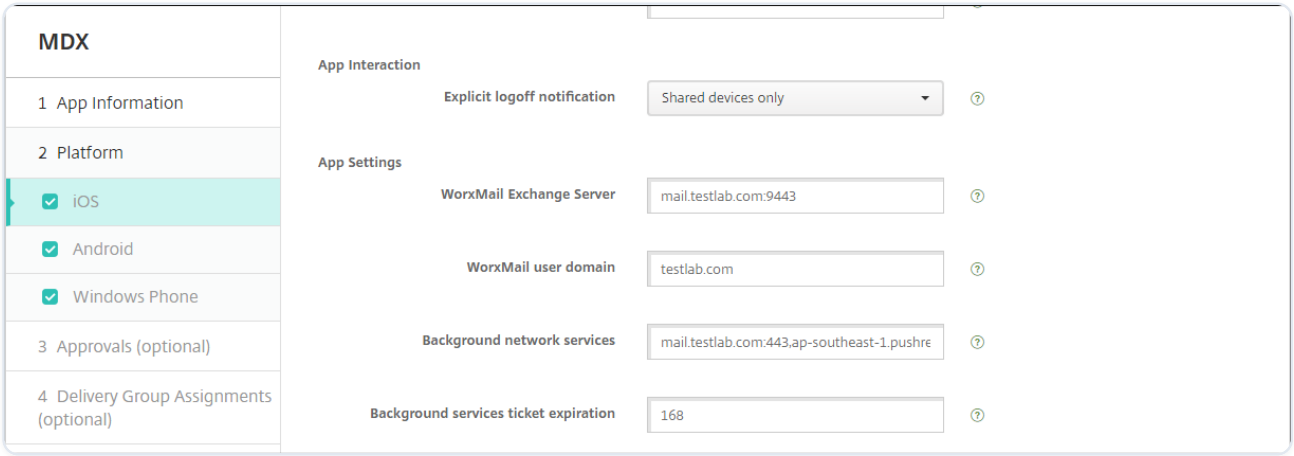
6. Para as próximas duas seções, **Revogação XenMobile** e **Revogação PKI**, defina os parâmetros conforme necessário. Neste exemplo, ambas as opções são ignoradas.
7. Clique em **Renovação**.
8. Para **Renovar certificados quando eles expirarem**, selecione **ATIVADO**.
9. Deixe todas as outras configurações como padrão ou altere-as conforme necessário.



10. Clique em **Salvar**.

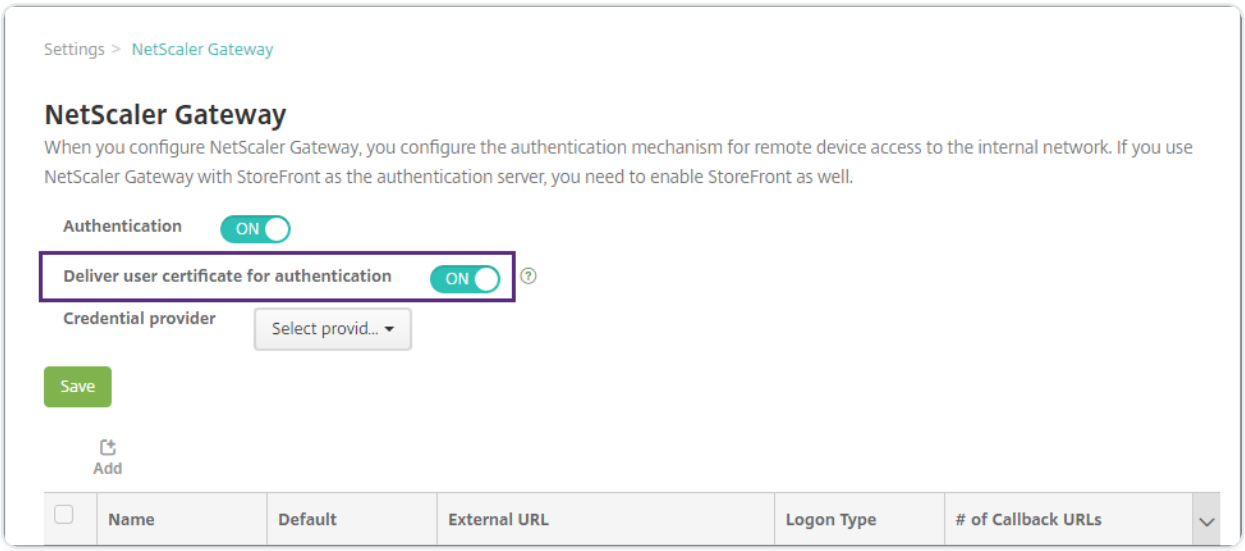
Configurando o Secure Mail para usar autenticação baseada em certificado

Ao adicionar o Secure Mail ao XenMobile, certifique-se de configurar as configurações do Exchange em **Configurações do Aplicativo**.

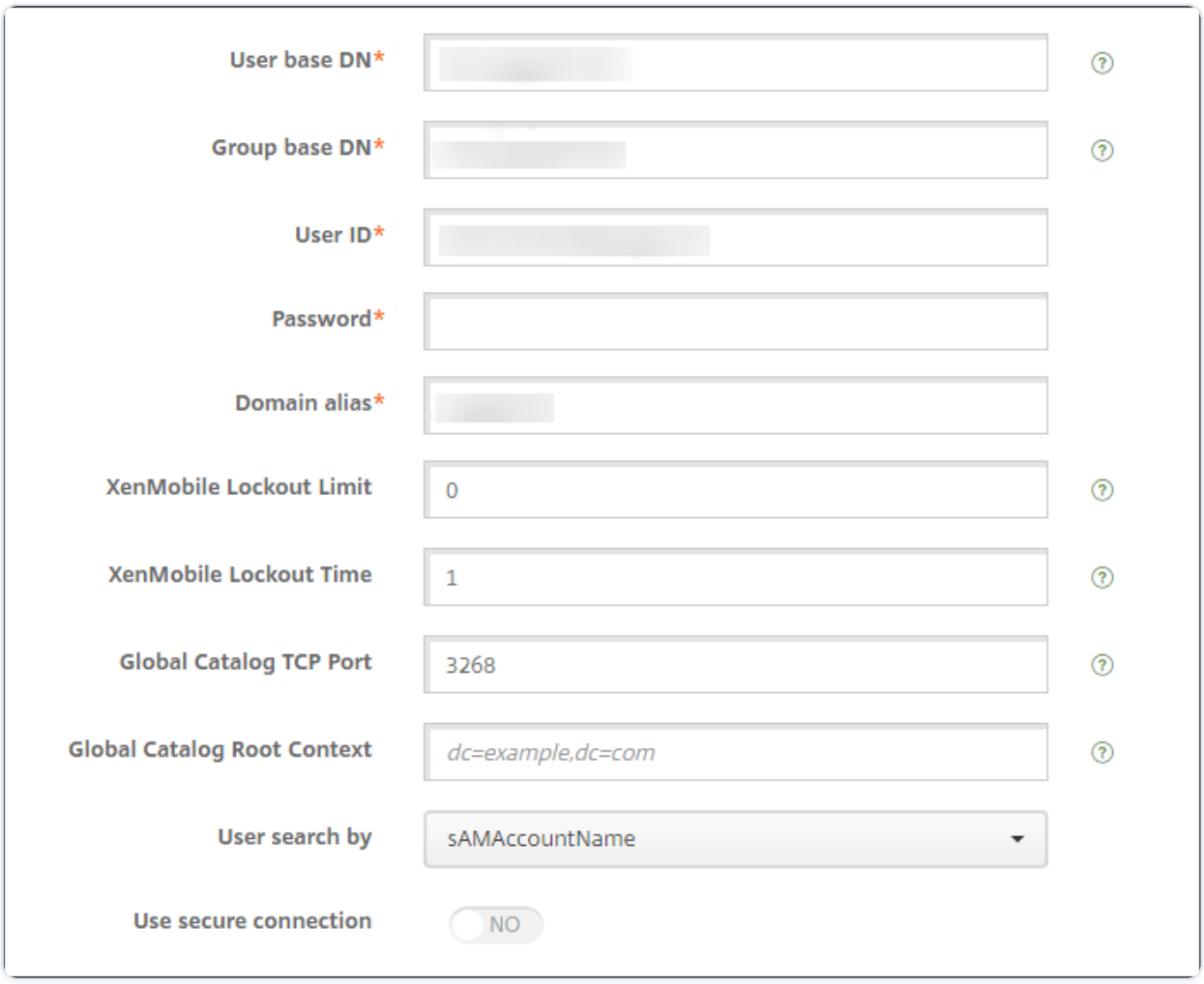


Configurando a entrega de certificado do Citrix ADC no XenMobile

1. Faça logon no console do XenMobile e clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Em **Servidor**, clique em **Citrix Gateway**.
3. Se o Citrix Gateway ainda não tiver sido adicionado, clique em **Adicionar** e especifique as configurações:
   - **URL Externa:** `https://YourCitrixGatewayURL`
   - **Tipo de Logon:** Certificado e domínio
   - **Senha Necessária:** DESATIVADO
   - **Definir como Padrão:** ATIVADO
4. Para **Entregar certificado de usuário para autenticação**, selecione **Ativado**.



5. Para **Provedor de Credenciais**, selecione um provedor e clique em **Salvar**.
6. Para usar os atributos sAMAccount nos certificados de usuário como alternativa ao Nome Principal de Usuário (UPN), configure o conector LDAP no XenMobile da seguinte forma: Vá para **Configurações > LDAP**, selecione o diretório e clique em **Editar**, e selecione **sAMAccountName** em **Pesquisar usuário por**.



Habilitar PIN do Citrix e cache de senha do usuário

Para habilitar o PIN do Citrix e o cache de senha do usuário, vá para **Configurações > Propriedades do Cliente** e selecione estas caixas de seleção: **Habilitar Autenticação por PIN do Citrix** e **Habilitar Cache de Senha do Usuário**. Para obter mais informações, consulte Propriedades do cliente.

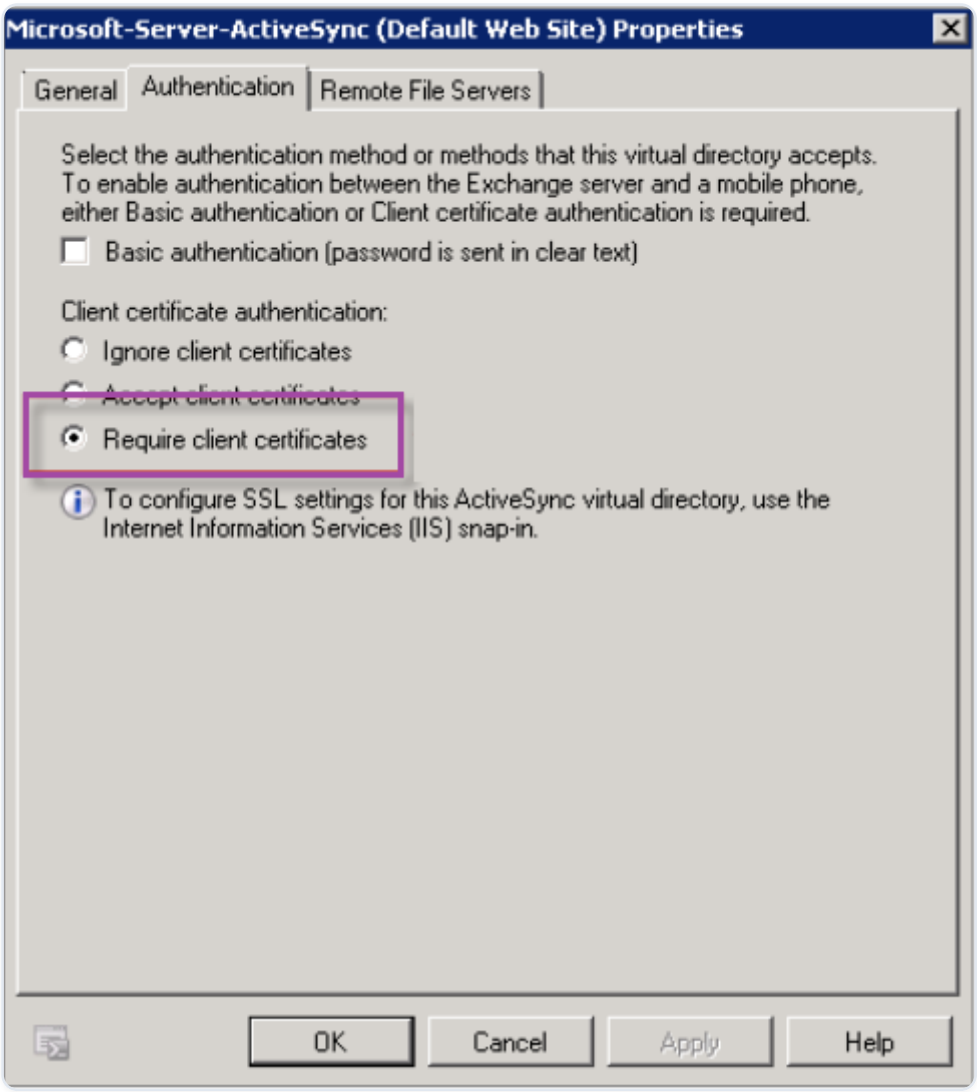
Solução de problemas da sua configuração de certificado de cliente

Após uma configuração bem-sucedida da configuração anterior, mais a configuração do Citrix Gateway, o fluxo de trabalho do usuário é o seguinte:

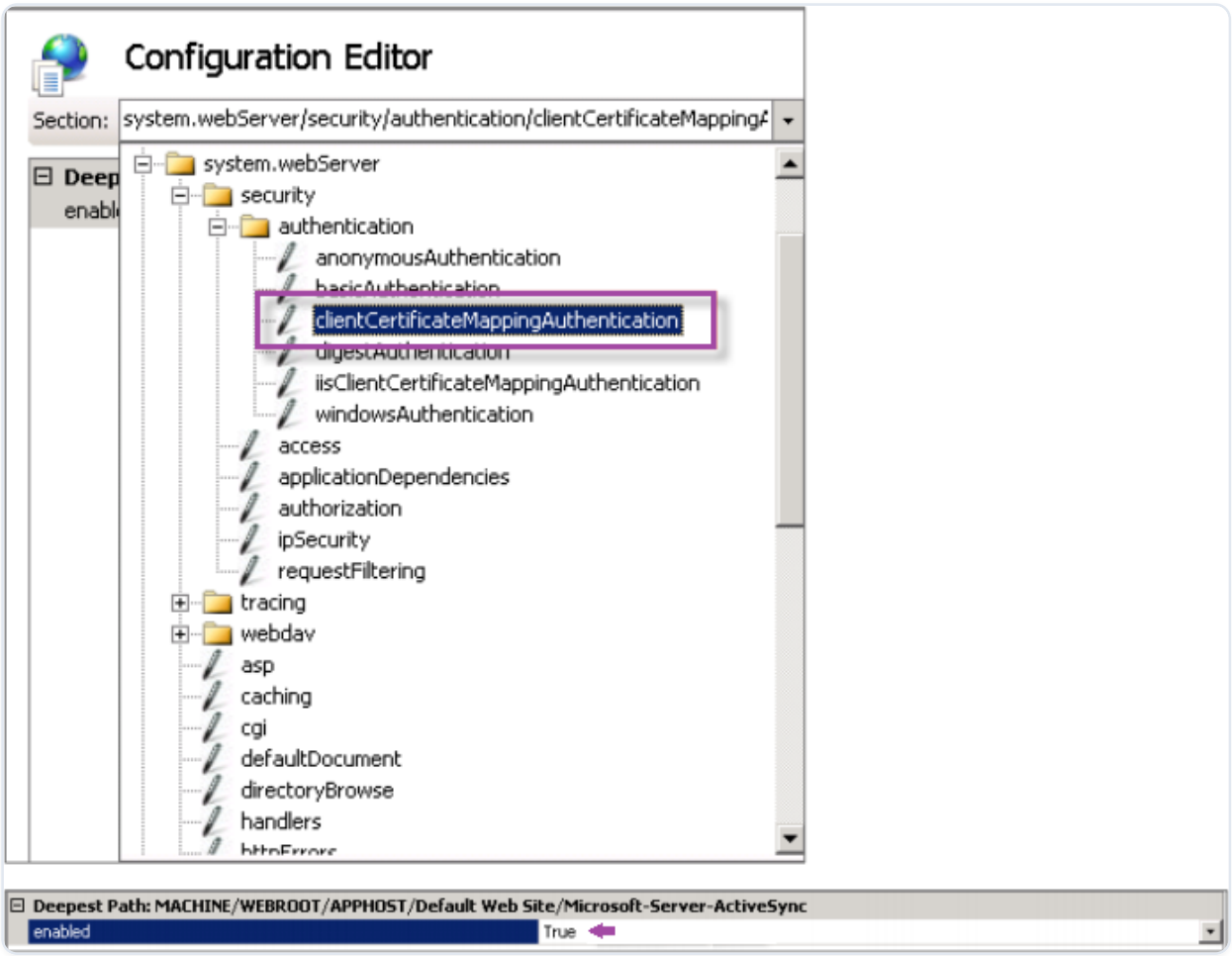
1. Os usuários registram seus dispositivos móveis.
2. O XenMobile solicita que os usuários criem um PIN do Citrix.
3. Os usuários são então redirecionados para a Loja XenMobile.
4. Quando os usuários iniciam o Secure Mail, o XenMobile não solicita credenciais de usuário para a configuração da caixa de correio. Em vez disso, o Secure Mail solicita o certificado do cliente do Secure Hub e o envia para o Microsoft Exchange Server para autenticação. Se o XenMobile solicitar credenciais quando os usuários iniciarem o Secure Mail, verifique sua configuração.

Se os usuários conseguirem baixar e instalar o Secure Mail, mas durante a configuração da caixa de correio o Secure Mail falhar ao concluir a configuração:

1. Se o Microsoft Exchange Server ActiveSync usar certificados de servidor SSL privados para proteger o tráfego, verifique se os certificados Raiz/Intermediário estão instalados no dispositivo móvel.
2. Verifique se o tipo de autenticação selecionado para o ActiveSync é **Exigir certificados de cliente**.



3. No Microsoft Exchange Server, verifique o site **Microsoft-Server-ActiveSync** para verificar se a autenticação de mapeamento de certificado de cliente está ativada. Por padrão, a autenticação de mapeamento de certificado de cliente está desativada. A opção está em **Editor de Configuração > Segurança > Autenticação**.



Depois de selecionar **True**, certifique-se de clicar em **Aplicar** para que as alterações entrem em vigor.

4. Verifique as configurações do Citrix Gateway no console do XenMobile: Certifique-se de que **Entregar certificado de usuário para autenticação** esteja **ATIVADO** e que o **Provedor de credenciais** tenha o perfil correto selecionado.

Para determinar se o certificado de cliente foi entregue a um dispositivo móvel

1. No console do XenMobile, vá para **Gerenciar > Dispositivos** e selecione o dispositivo.
2. Clique em **Editar** ou **Mostrar Mais**.
3. Vá para a seção **Grupos de Entrega** e procure por esta entrada:

   Credenciais do Citrix Gateway: Credencial solicitada, CertId=

Para validar se a negociação de certificado de cliente está ativada

1. Execute este comando `netsh` para mostrar a configuração do Certificado SSL que está vinculada ao site do IIS:

   ```
   netsh http show sslcert
   ```

2. Se o valor para **Negociar Certificado do Cliente** estiver **Desabilitado**, execute o seguinte comando para habilitá-lo:

   ```
   netsh http delete sslcert ipport=0.0.0.0:443
   ```

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable
   ```

   Por exemplo:

   ```
   netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable
   ```

Entidades PKI

A configuração de entidade de Infraestrutura de Chave Pública (PKI) do XenMobile® representa um componente que realiza operações PKI reais (emissão, revogação e informações de status). Esses componentes são internos ou externos ao XenMobile. Os componentes internos são chamados de discricionários. Os componentes externos fazem parte da sua infraestrutura corporativa.

O XenMobile oferece suporte aos seguintes tipos de entidades PKI:

- Serviços de Certificado Microsoft
- Autoridades de Certificação (CAs) Discricionárias

O XenMobile oferece suporte aos seguintes servidores CA:

- Windows Server 2019
- Windows Server 2016

> **Nota:**

> Os Windows Servers 2012 R2, 2012 e 2008 R2 não são mais suportados, pois atingiram o fim da vida útil. Para obter mais informações, consulte documentação do ciclo de vida dos produtos Microsoft.

Conceitos comuns de PKI

Independentemente do seu tipo, cada entidade PKI possui um subconjunto das seguintes capacidades:

- **Assinar:** Emissão de um novo certificado, com base em uma Solicitação de Assinatura de Certificado (CSR).
- **Buscar:** Recuperação de um certificado e par de chaves existentes.
- **Revogar:** Revogação de um certificado de cliente.

Sobre Certificados CA

Ao configurar uma entidade PKI, indique ao XenMobile qual certificado CA é o signatário dos certificados emitidos por (ou recuperados de) essa entidade. Essa entidade PKI pode retornar certificados (obtidos ou recém-assinados) assinados por qualquer número de CAs diferentes.

Forneça o certificado de cada uma dessas CAs como parte da configuração da entidade PKI. Para fazer isso, carregue os certificados para o XenMobile e, em seguida, faça referência a eles na entidade PKI. Para CAs discricionárias, o certificado é implicitamente o certificado CA de assinatura. Para entidades externas, você deve especificar o certificado manualmente.

> **Importante:**

> Ao criar um modelo de Entidade de Serviços de Certificado Microsoft, evite possíveis problemas de autenticação com dispositivos registrados: Não use caracteres especiais no nome do modelo. Por exemplo, não use: `! : $ ( ) # % + * ~ ? | { } [ ]`

Serviços de Certificado Microsoft

O XenMobile se comunica com os Serviços de Certificado Microsoft por meio de sua interface de registro web. O XenMobile suporta apenas a emissão de novos certificados por meio dessa interface. Se a CA da Microsoft gerar um certificado de usuário do Citrix Gateway, o Citrix Gateway suportará a renovação e revogação desses certificados.

Para criar uma entidade PKI de CA Microsoft no XenMobile, você deve especificar a URL base da interface web dos Serviços de Certificado. Se desejar, use a autenticação de cliente SSL para proteger a conexão entre o XenMobile e a interface web dos Serviços de Certificado.

Adicionar uma entidade de Serviços de Certificado Microsoft

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console e, em seguida, clique em **Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

   Um menu de tipos de entidade PKI é exibido.
3. Clique em **Entidade de Serviços de Certificado Microsoft**.

   A página **Entidade de Serviços de Certificado Microsoft: Informações Gerais** é exibida.
4. Na página **Entidade de Serviços de Certificado Microsoft: Informações Gerais**, configure estas definições:

   - **Nome:** Digite um nome para sua nova entidade, que você usará mais tarde para se referir a essa entidade. Os nomes das entidades devem ser únicos.
   - **URL raiz do serviço de registro web:** Digite a URL base do seu serviço de registro web da CA da Microsoft; por exemplo, `https://192.0.2.13/certsrv/`. A URL pode usar HTTP simples ou HTTP-over-SSL.
   - **Nome da página certnew.cer:** O nome da página certnew.cer. Use o nome padrão, a menos que você o tenha renomeado por algum motivo.
   - **certfnsh.asp:** O nome da página certfnsh.asp. Use o nome padrão, a menos que você o tenha renomeado por algum motivo.
   - **Tipo de autenticação:** Escolha o método de autenticação que você deseja usar.
     - **Nenhum**
     - **HTTP Básico:** Digite o nome de usuário e a senha necessários para conectar.
     - **Certificado de cliente:** Escolha o certificado de cliente SSL correto.
5. Clique em **Testar Conexão** para garantir que o servidor esteja acessível. Se não estiver acessível, uma mensagem aparecerá, informando que a conexão falhou. Verifique suas configurações.
6. Clique em **Avançar**.

A página **Entidade de Serviços de Certificado da Microsoft: Modelos** é exibida. Nesta página, você especifica os nomes internos dos modelos que sua CA da Microsoft suporta. Ao criar provedores de credenciais, você seleciona um modelo da lista definida aqui. Cada provedor de credenciais que usa esta entidade utiliza exatamente um desses modelos.

Para os requisitos de modelo dos Serviços de Certificado da Microsoft, consulte a documentação da Microsoft para a sua versão do Microsoft Server. O XenMobile não tem requisitos para os certificados que distribui, além dos formatos de certificado observados em Certificados.

7. Na página **Entidade de Serviços de Certificado da Microsoft: Modelos**, clique em **Adicionar**, digite o nome do modelo e, em seguida, clique em **Salvar**. Repita esta etapa para cada modelo que você deseja adicionar.
8. Clique em **Avançar**.

   A página **Entidade de Serviços de Certificado da Microsoft: Parâmetros HTTP** é exibida. Nesta página, você especifica parâmetros personalizados para o XenMobile adicionar à solicitação HTTP para a interface de Registro Web da Microsoft. Parâmetros personalizados são úteis apenas para scripts personalizados em execução na CA.
9. Na página **Entidade de Serviços de Certificado Microsoft: Parâmetros HTTP**, clique em **Adicionar**, digite o nome e o valor dos parâmetros HTTP que você deseja adicionar e, em seguida, clique em **Avançar**.

   A página **Entidade de Serviços de Certificado Microsoft: Certificados CA** é exibida. Nesta página, você deve informar ao XenMobile os signatários dos certificados que o sistema obtém por meio desta entidade. Quando seu certificado CA for renovado, atualize-o no XenMobile. O XenMobile aplica a alteração à entidade de forma transparente.
10. Na página **Entidade de Serviços de Certificado Microsoft: Certificados CA**, selecione os certificados que você deseja usar para esta entidade.
11. Clique em **Salvar**.

    A entidade aparece na tabela Entidades PKI.

Lista de Revogação de Certificados (CRL) do Citrix ADC

O XenMobile oferece suporte à Lista de Revogação de Certificados (CRL) apenas para uma Autoridade de Certificação de terceiros. Se você tiver uma CA Microsoft configurada, o XenMobile usará o Citrix ADC para gerenciar a revogação.

Ao configurar a autenticação baseada em certificado de cliente, considere configurar a definição da Lista de Revogação de Certificados (CRL) do Citrix ADC **Enable CRL Auto Refresh**. Esta etapa garante que o usuário de um dispositivo no modo somente MAM não possa autenticar usando um certificado existente no dispositivo.

O XenMobile reemite um novo certificado, pois não restringe um usuário de gerar um certificado de usuário depois que um é revogado. Essa configuração aumenta a segurança das entidades PKI quando a CRL verifica entidades PKI expiradas.

CAs discricionárias

Uma CA discricionária é criada quando você fornece ao XenMobile um certificado CA e a chave privada associada. O XenMobile lida com a emissão, revogação e informações de status do certificado internamente, de acordo com os parâmetros que você especificar.

Ao configurar uma CA discricionária, você pode ativar o suporte ao Online Certificate Status Protocol (OCSP) para essa CA. Se e somente se você habilitar o suporte OCSP, a CA adicionará a extensão `id-pe-authorityInfoAccess` aos certificados que a CA emite. A extensão aponta para o respondedor OCSP interno do XenMobile no seguinte local:

`https://<server>/<instance>/ocsp`

Ao configurar o serviço OCSP, especifique um certificado de assinatura OCSP para a entidade discricionária em questão. Você pode usar o próprio certificado CA como signatário. Para evitar a exposição desnecessária de sua chave privada CA (recomendado): Crie um certificado de assinatura OCSP delegado, assinado pelo certificado CA, e inclua esta extensão: `id-kp-OCSPSigning extendedKeyUsage`.

O serviço de respondedor OCSP do XenMobile oferece suporte a respostas OCSP básicas e aos seguintes algoritmos de hash em solicitações:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

As respostas são assinadas com SHA-256 e o algoritmo de chave do certificado de assinatura (DSA, RSA ou ECDSA).

Adicionar CAs discricionárias

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console e, em seguida, clique em **Mais > Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

   Um menu de tipos de entidade PKI é exibido.
3. Clique em **CA discricionária**.

   A página **CA discricionária: Informações gerais** é exibida.
4. Na página **CA discricionária: Informações gerais**, faça o seguinte:

   - **Nome:** Digite um nome descritivo para a CA discricionária.
   - **Certificado CA para assinar solicitações de certificado:** Clique em um certificado para a CA discricionária usar para assinar solicitações de certificado.

     Esta lista de certificados é gerada a partir dos certificados CA com chaves privadas que você carregou no XenMobile em **Configurar > Configurações > Certificados**.
5. Clique em **Avançar**.

   A página **CA discricionária: Parâmetros** é exibida.
6. Na página **CA discricionária: Parâmetros**, faça o seguinte:

   - **Gerador de número de série:** A CA discricionária gera números de série para os certificados que emite. Nesta lista, clique em **Sequencial** ou **Não sequencial** para determinar como os números são gerados.
   - **Próximo número de série:** Digite um valor para determinar o próximo número emitido.
   - **Certificado válido por:** Digite o número de dias de validade do certificado.
   - **Uso da chave:** Identifique a finalidade dos certificados emitidos pela CA discricionária definindo as chaves apropriadas como **Ativado**. Uma vez definido, a CA fica limitada a emitir certificados para essas finalidades.
   - **Uso estendido da chave:** Para adicionar mais parâmetros, clique em **Adicionar**, digite o nome da chave e, em seguida, clique em **Salvar**.
7. Clique em **Avançar**.

   A página **CA discricionária: Distribuição** é exibida.
8. Na página **CA discricionária: Distribuição**, selecione um modo de distribuição:

- **Centralizado: geração de chave no lado do servidor**. A Citrix recomenda a opção centralizada. As chaves privadas são geradas e armazenadas no servidor e distribuídas para os dispositivos do usuário.
- **Distribuído: geração de chave no lado do dispositivo**. As chaves privadas são geradas nos dispositivos do usuário. Este modo distribuído usa SCEP e requer um certificado de criptografia RA com a extensão `keyUsage keyEncryption` e um certificado de assinatura RA com a extensão `keyUsage digitalSignature`. O mesmo certificado pode ser usado para criptografia e assinatura.

9. Clique em **Avançar**.

   A página **CA Discricionária: Protocolo de Status de Certificado Online (OCSP)** é exibida.

   Na página **CA Discricionária: Protocolo de Status de Certificado Online (OCSP)**, faça o seguinte:

   - Se você quiser adicionar uma extensão `AuthorityInfoAccess` (RFC2459) aos certificados assinados por esta CA, defina **Habilitar suporte OCSP para esta CA** como **Ativado**. Esta extensão aponta para o respondedor OCSP da CA em `https://<server>/<instance>/ocsp`.
   - Se você habilitou o suporte OCSP, selecione um certificado de CA de assinatura OSCP. Esta lista de certificados é gerada a partir dos certificados de CA que você carregou no XenMobile.

10. Clique em **Salvar**.

    A CA discricionária aparece na tabela Entidades PKI.

Provedores de credenciais

Os provedores de credenciais são as configurações de certificado reais que você usa nas várias partes do sistema XenMobile®. Os provedores de credenciais definem as fontes, parâmetros e ciclos de vida dos seus certificados. Essas operações ocorrem independentemente de os certificados fazerem parte das configurações do dispositivo ou serem autônomos (ou seja, enviados como estão para o dispositivo).

O registro do dispositivo restringe o ciclo de vida do certificado. Ou seja, o XenMobile não emite certificados antes do registro, embora o XenMobile possa emitir alguns certificados como parte do registro. Além disso, os certificados emitidos da PKI interna no contexto de um registro são

revogados quando o registro é revogado. Após o término da relação de gerenciamento, nenhum certificado válido permanece.

Você pode usar uma configuração de provedor de credenciais em vários lugares, de modo que uma configuração possa governar qualquer número de certificados ao mesmo tempo. A unidade então está no recurso de implantação e na implantação. Por exemplo, se o Provedor de Credenciais P for implantado no dispositivo D como parte da configuração C: As configurações de emissão para P determinam o certificado que é implantado em D. Da mesma forma, as configurações de renovação para D se aplicam quando C é atualizado. E as configurações de revogação para D também se aplicam quando C é excluído ou quando D é revogado.

De acordo com essas regras, a configuração do provedor de credenciais no XenMobile determina o seguinte:

- A fonte dos certificados.
- O método pelo qual os certificados são obtidos: Assinar um novo certificado ou buscar (recuperar) um certificado e par de chaves existentes.
- Os parâmetros para emissão ou recuperação. Por exemplo, parâmetros de Solicitação de Assinatura de Certificado (CSR), como tamanho da chave, algoritmo da chave e extensões de certificado.
- A maneira como os certificados são entregues ao dispositivo.
- Condições de revogação. Embora todos os certificados sejam revogados no XenMobile quando a relação de gerenciamento é interrompida, a configuração pode especificar uma revogação anterior. Por exemplo, a configuração pode especificar a revogação de um certificado quando a configuração do dispositivo associado é excluída. Além disso, sob algumas condições, a revogação do certificado associado no XenMobile pode ser enviada para a infraestrutura de chave pública (PKI) de back-end. Ou seja, a revogação de certificado no XenMobile pode causar a revogação de certificado na PKI.
- Configurações de renovação. Os certificados obtidos por meio de um determinado provedor de credenciais podem ser renovados automaticamente quando se aproximam da expiração. Ou, separadamente dessa situação, notificações podem ser emitidas quando essa expiração se aproxima.

A disponibilidade das opções de configuração depende principalmente do tipo de Entidade PKI e do método de emissão que você seleciona para um provedor de credenciais.

Métodos de emissão de certificado

Você pode obter um certificado, o que é conhecido como método de emissão por assinatura.

Com este método, a emissão envolve a criação de uma nova chave privada, a criação de um CSR e o envio do CSR para uma Autoridade de Certificação (CA) para assinatura. O XenMobile suporta o método de assinatura para entidades de Serviços de Certificado MS e entidades de CA Discricionária.

Um provedor de credenciais usa o método de assinatura de emissão.

Entrega de Certificados

Dois modos de entrega de certificados estão disponíveis no XenMobile: centralizado e distribuído. O modo distribuído usa o Protocolo de Registro Simples de Certificados (SCEP) e está disponível apenas em situações em que o cliente suporta o protocolo (somente iOS). O modo distribuído é obrigatório em algumas situações.

Para que um provedor de credenciais suporte a entrega distribuída (assistida por SCEP), uma etapa de configuração especial é necessária: Configurar certificados da Autoridade de Registro (RA). Os certificados RA são necessários porque, se você usar o protocolo SCEP, o XenMobile atua como um delegado (um registrador) para a autoridade de certificação real. O XenMobile deve provar ao cliente que tem autoridade para atuar como tal. Essa autoridade é estabelecida pelo upload dos certificados mencionados anteriormente para o XenMobile.

São necessárias duas funções de certificado distintas (embora um único certificado possa atender a ambos os requisitos): assinatura RA e criptografia RA. As restrições para essas funções são as seguintes:

- O certificado de assinatura RA deve ter o uso de chave X.509 de assinatura digital.
- O certificado de criptografia RA deve ter o uso de chave X.509 de cifragem de chave.

Para configurar os certificados RA do provedor de credenciais, você faz o upload dos certificados para o XenMobile e, em seguida, os vincula no provedor de credenciais.

Um provedor de credenciais é considerado compatível com a entrega distribuída somente se o provedor tiver um certificado configurado para funções de certificado. Você pode configurar cada provedor de credenciais para preferir o modo centralizado, preferir o modo distribuído ou exigir o modo distribuído. O resultado real depende do contexto: Se o contexto não suportar o modo distribuído, mas o provedor de credenciais exigir este modo, a implantação falhará. Da mesma forma, se o contexto exigir o modo distribuído, mas o provedor de credenciais não suportar o modo distribuído, a implantação falhará. Em todos os outros casos, a configuração preferencial é respeitada.

A tabela a seguir mostra a distribuição SCEP em todo o XenMobile:

CONTEXTO	SCEP SUPORTADO	SCEP EXIGIDO
Serviço de Perfil iOS	Sim	Sim
Registro de gerenciamento de dispositivo móvel iOS	Sim	Não
Perfis de configuração iOS	Sim	Não
Registro SHTP	Não	Não
Configuração SHTP	Não	Não
Registro de Tablet Windows	Não	Não
Configuração de Tablet Windows	Não, exceto para a política de dispositivo Wi-Fi, que é suportada para Windows 10 e Windows 11	Não

Revogação de Certificado

Existem três tipos de revogação.

- **Revogação interna:** A revogação interna afeta o status do certificado conforme mantido pelo XenMobile. O XenMobile considera esse status ao avaliar um certificado apresentado ou ao fornecer informações de status OCSP para um certificado. A configuração do provedor de credenciais determina como esse status é afetado sob várias condições. Por exemplo, o provedor de credenciais pode especificar para sinalizar certificados como revogados quando os certificados são excluídos do dispositivo.
- **Revogação propagada externamente:** Também conhecida como Revogação XenMobile, este tipo de revogação se aplica a certificados obtidos de uma PKI externa. O certificado é revogado na PKI quando o XenMobile revoga internamente o certificado, sob as condições definidas pela configuração do provedor de credenciais.
- **Revogação induzida externamente:** Também conhecida como Revogação PKI, este tipo de revogação também se aplica apenas a certificados obtidos de uma PKI externa. Sempre que o XenMobile avalia um determinado status de certificado, o XenMobile consulta a PKI sobre esse status. Se o certificado for revogado, o XenMobile revoga internamente o certificado. Este mecanismo usa o protocolo OCSP.

Esses três tipos não são exclusivos, mas se aplicam em conjunto. Uma revogação externa ou uma descoberta independente pode causar uma revogação interna. Uma revogação interna pode potencialmente afetar uma revogação externa.

Renovação de Certificado

Uma renovação de certificado é a combinação de uma revogação do certificado existente e uma emissão de outro certificado.

O XenMobile primeiro tenta obter o novo certificado antes de revogar o certificado anterior, para evitar a descontinuação do serviço caso a emissão falhe. Para entrega distribuída (suportada por SCEP), a revogação também só acontece depois que o certificado foi instalado com sucesso no dispositivo. Caso contrário, a revogação ocorre antes que o novo certificado seja enviado ao dispositivo. Essa revogação é independente do sucesso ou falha da instalação do certificado.

A configuração de revogação exige que você especifique uma certa duração (em dias). Quando o dispositivo se conecta, o servidor verifica se a data `NotAfter` do certificado é posterior à data atual, menos a duração especificada. Se o certificado atender a essa condição, o XenMobile tenta renovar o certificado.

Criar um provedor de credenciais

A configuração de um provedor de credenciais varia principalmente em função da entidade emissora e do método de emissão que você seleciona para o provedor de credenciais. Você pode distinguir entre provedores de credenciais que usam uma entidade interna ou uma entidade externa:

- Uma entidade discricionária, que é interna ao XenMobile, é uma entidade interna. O método de emissão para uma entidade discricionária é sempre uma assinatura. Assinar significa que, a cada operação de emissão, o XenMobile assina um novo par de chaves com o certificado CA selecionado para a entidade. Se o par de chaves é gerado no dispositivo ou no servidor depende do método de distribuição que você selecionar.
- Uma entidade externa, que faz parte da sua infraestrutura corporativa, inclui a CA da Microsoft.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito e, em seguida, clique em **Configurações > Provedores de Credenciais**.
2. Na página **Provedores de Credenciais**, clique em **Adicionar**.

   A página **Provedores de Credenciais: Informações Gerais** é exibida.
3. Na página **Provedores de Credenciais: Informações Gerais**, faça o seguinte:

- **Nome:** Digite um nome exclusivo para a nova configuração do provedor. Esse nome é usado posteriormente para identificar a configuração em outras partes do console do XenMobile.
- **Descrição:** Descreva o provedor de credenciais. Embora este campo seja opcional, uma descrição pode fornecer detalhes úteis sobre este provedor de credenciais.
- **Entidade emissora:** Clique na entidade emissora do certificado.
- **Método de emissão:** Clique em **Assinar** ou **Buscar** para servir como o método que o sistema usa para obter certificados da entidade configurada. Para autenticação de certificado de cliente, use **Assinar**.
- Se a lista **Modelo** estiver disponível, selecione o modelo que você adicionou na entidade PKI para o provedor de credenciais.

  Esses modelos ficam disponíveis quando as Entidades de Serviços de Certificado da Microsoft são adicionadas em **Configurações > Entidades PKI**.

4. Clique em **Avançar**.

   A página **Provedores de Credenciais: Solicitação de Assinatura de Certificado** é exibida.

5. Na página **Provedores de Credenciais: Solicitação de Assinatura de Certificado**, configure o seguinte de acordo com a sua configuração de certificado:

   - **Algoritmo de chave:** Escolha o algoritmo de chave para o novo par de chaves. Os valores disponíveis são **RSA**, **DSA** e **ECDSA**.
   - **Tamanho da chave:** Digite o tamanho, em bits, do par de chaves. Este campo é obrigatório.

     Os valores permitidos dependem do tipo de chave. Por exemplo, o tamanho máximo para chaves DSA é de 1024 bits. Para evitar falsos negativos, que dependem do hardware e software subjacentes, o XenMobile não impõe tamanhos de chave. Sempre teste as configurações do provedor de credenciais em um ambiente de teste antes de ativá-las em produção.
   - **Algoritmo de assinatura:** Clique em um valor para o novo certificado. Os valores dependem do algoritmo de chave.
   - **Nome do assunto:** Obrigatório. Digite o Nome Distinto (DN) do novo assunto do certificado. Por exemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation`

     Por exemplo, para autenticação de certificado de cliente, use estas configurações:

- **Algoritmo de chave:** RSA
- **Tamanho da chave:** 2048
- **Algoritmo de assinatura:** SHA256withRSA
- **Nome do assunto:** `cn=$user.username`

- Para adicionar uma entrada à tabela **Nomes alternativos do assunto**, clique em **Adicionar**. Selecione o tipo de nome alternativo e, em seguida, digite um valor na segunda coluna.

  Para autenticação de certificado de cliente, especifique:

  - **Tipo:** Nome Principal do Usuário
  - **Valor:** `$user.userprincipalname`

    Assim como no nome do Assunto, você pode usar macros do XenMobile no campo de valor.

6. Clique em **Avançar**.

   A página **Provedores de Credenciais: Distribuição** é exibida.

7. Na página **Provedores de Credenciais: Distribuição**, faça o seguinte:

   - Na lista **Certificado da CA emissora**, clique no certificado da CA oferecido. Como o provedor de credenciais usa uma entidade de CA discricionária, o certificado da CA para o provedor de credenciais é sempre o certificado da CA configurado na própria entidade. O certificado da CA é apresentado aqui para consistência com as configurações que usam entidades externas.
   - Em **Selecionar modo de distribuição**, clique em uma das seguintes formas de gerar e distribuir chaves:

     - **Preferir centralizado: Geração de chave no lado do servidor:** A Citrix recomenda esta opção centralizada. Ela oferece suporte a todas as plataformas compatíveis com o XenMobile e é necessária ao usar a autenticação do Citrix Gateway. As chaves privadas são geradas e armazenadas no servidor e distribuídas para os dispositivos do usuário.
     - **Preferir distribuído: Geração de chave no lado do dispositivo:** As chaves privadas são geradas e armazenadas nos dispositivos do usuário. Este modo distribuído usa SCEP e requer um certificado de criptografia RA com o keyUsage keyEncryption e um

certificado de assinatura RA com o KeyUsage digitalSignature. O mesmo certificado pode ser usado para criptografia e assinatura.

- **Apenas distribuído: Geração de chave no lado do dispositivo:** Esta opção funciona da mesma forma que Preferir distribuído: Geração de chave no lado do dispositivo, exceto que, como é "Apenas", em vez de "Preferir", nenhuma opção está disponível se a geração de chave no lado do dispositivo falhar ou não estiver disponível.

Se você selecionou **Preferir distribuído: Geração de chave no lado do dispositivo** ou **Apenas distribuído: Geração de chave no lado do dispositivo**, clique no certificado de assinatura RA e no certificado de criptografia RA. O mesmo certificado pode ser usado para ambos. Novos campos aparecem para esses certificados.

8. Clique em **Avançar**.

   A página **Provedores de Credenciais: Revogação XenMobile** é exibida. Nesta página, você configura as condições sob as quais o XenMobile sinaliza internamente os certificados, emitidos por meio desta configuração de provedor, como revogados.

9. Na página **Provedores de Credenciais: Revogação XenMobile**, faça o seguinte:

   - Em **Revogar certificados emitidos**, selecione uma das opções que indicam quando revogar certificados.
   - Para direcionar o XenMobile a enviar uma notificação quando o certificado for revogado: Defina o valor de **Enviar notificação** como **Ativado** e escolha um modelo de notificação.
   - Para revogar o certificado na PKI quando o certificado for revogado do XenMobile: Defina **Revogar certificado na PKI** como **Ativado** e, na **Lista de entidades**, clique em um modelo. A Lista de entidades mostra todas as entidades disponíveis com recursos de revogação. Quando o certificado é revogado do XenMobile, uma chamada de revogação é enviada para a PKI selecionada na Lista de entidades.

10. Clique em **Avançar**.

    A página **Provedores de Credenciais: PKI de Revogação** é exibida. Nesta página, você identifica quais ações tomar na PKI se o certificado for revogado. Você também tem a opção de criar uma mensagem de notificação.

11. Na página **Provedores de Credenciais: PKI de Revogação**, faça o seguinte se quiser revogar certificados da PKI:

    - Altere a configuração de **Habilitar verificações de revogação externas** para **Ativado**. Mais campos relacionados à PKI de revogação aparecem.

- Na lista **Certificado CA do respondedor OCSP**, clique no nome distinto (DN) do assunto do certificado.

  Você pode usar macros do XenMobile para os valores do campo DN. Por exemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

- Na lista **Quando o certificado for revogado**, clique em uma das seguintes ações a serem tomadas na entidade PKI quando o certificado for revogado:
  - Não fazer nada.
  - Renovar o certificado.
  - Revogar e limpar o dispositivo.
- Para direcionar o XenMobile a enviar uma notificação quando o certificado for revogado: Defina o valor de **Enviar notificação** como **Ativado**.

  Você pode escolher entre duas opções de notificação:
- Se você selecionar **Selecionar modelo de notificação**, poderá selecionar uma mensagem de notificação pré-escrita que poderá personalizar. Esses modelos estão na lista de modelos de notificação.
- Se você selecionar **Inserir detalhes da notificação**, poderá escrever sua própria mensagem de notificação. Além de fornecer o endereço de e-mail do destinatário e a mensagem, você pode definir a frequência com que a notificação é enviada.

12. Clique em **Avançar**.

    A página **Provedores de Credenciais: Renovação** é exibida. Nesta página, você pode configurar o XenMobile para fazer o seguinte:

    - Renovar o certificado. Você pode, opcionalmente, enviar uma notificação na renovação e, opcionalmente, excluir certificados já expirados da operação.
    - Emitir uma notificação para certificados que se aproximam da expiração (notificação antes da renovação).

13. Na página **Provedores de Credenciais: Renovação**, faça o seguinte se quiser renovar certificados quando eles expirarem:

    Defina **Renovar certificados** quando eles expirarem como **Ativado**. Mais campos são exibidos.

- No campo **Renovar quando o certificado estiver dentro de**, digite quantos dias antes da expiração para renovar o certificado.
- Opcionalmente, selecione **Não renovar certificados que já expiraram**. Neste caso, "já expirado" significa que a data `NotAfter` está no passado, não que foi revogado. O XenMobile não renova certificados depois que são revogados internamente.

Para direcionar o XenMobile a enviar uma notificação quando o certificado for renovado: Defina **Enviar notificação** como **Ativado**. Para direcionar o XenMobile a enviar uma notificação quando o certificado se aproximar da expiração: Defina **Notificar quando o certificado se aproximar da expiração** como **Ativado**. Para qualquer uma dessas opções, você pode escolher entre duas opções de notificação:

- **Selecionar modelo de notificação:** Selecione uma mensagem de notificação pré-escrita que você pode personalizar. Esses modelos estão na lista de modelos de notificação.
- **Inserir detalhes da notificação:** Escreva sua própria mensagem de notificação. Forneça o endereço de e-mail do destinatário, uma mensagem e uma frequência para o envio da notificação.

No campo **Notificar quando o certificado estiver dentro de**, digite quantos dias antes da expiração do certificado para enviar a notificação.

14. Clique em **Salvar**.

O provedor de credenciais aparece na tabela Provedor de Credenciais.

Certificados APNs

> **Importante:**
>
> O suporte da Apple para o protocolo binário legado APNs termina em March 31, 2021. A Apple recomenda que você use a API de provedor APNs baseada em HTTP/2. A partir da versão 10.13.0, o XenMobile Server oferece suporte à API baseada em HTTP/2. Para obter mais informações, consulte a atualização de notícias, "Apple Push Notification Service Update" em `<https://developer.apple.com/>`. Para obter ajuda com a verificação de conectividade com APNs, consulte Verificações de conectividade.

Para registrar e gerenciar dispositivos iOS e macOS no XenMobile®, você configura um certificado do serviço Apple Push Notification (APNs) da Apple.

Resumo do fluxo de trabalho:

- **Etapa 1:** Criar uma Solicitação de Assinatura de Certificado (CSR) por meio de qualquer um destes métodos:
  - Criar uma CSR usando o Acesso às Chaves no macOS (recomendado pela Citrix®)
  - Criar uma CSR usando o Microsoft IIS
  - Criar uma CSR usando o OpenSSL
- **Etapa 2:** Assinar a CSR nas Ferramentas do XenMobile
- **Etapa 3:** Enviar a CSR assinada para a Apple para obter o certificado APNs
- **Etapa 4:** Usando o mesmo computador usado na Etapa 1, Concluir a CSR e exportar um arquivo PKCS #12:
  - Criar um arquivo PKCS #12 usando o Acesso às Chaves no macOS
  - Criar um arquivo PKCS #12 usando o Microsoft IIS
  - Criar um arquivo PKCS #12 usando o OpenSSL
- **Etapa 5:** Importar um certificado APNs para o XenMobile
- **Etapa 6:** Renovar um certificado APNs

Criar uma Solicitação de Assinatura de Certificado

Recomendamos que você crie um CSR usando o Acesso às Chaves no macOS. Você também pode criar um CSR usando o Microsoft IIS ou o OpenSSL.

> **Importante:**
>
> - Para o ID Apple usado para criar o certificado:
>   - O ID Apple deve ser um ID corporativo e não um ID pessoal.
>   - Registre o ID Apple que você usa para criar o certificado.
>   - Para renovar seu certificado, use o mesmo nome de organização e ID Apple. Usar um ID Apple diferente para renovar o certificado exige o reenrolamento do dispositivo.

- Se você revogar o certificado acidentalmente ou intencionalmente, perderá a capacidade de gerenciar seus dispositivos.
- Se você usou o Programa Empresarial de Desenvolvedores iOS para criar um certificado push do gerenciador de dispositivos móveis: Certifique-se de manipular quaisquer ações para os certificados migrados no Portal de Certificados Push da Apple.

Criar um CSR usando o Acesso às Chaves no macOS

1. Em um computador executando macOS, em **Aplicativos > Utilitários**, inicie o aplicativo Acesso às Chaves.
2. Abra o menu **Acesso às Chaves** e clique em **Assistente de Certificado > Solicitar um Certificado de uma Autoridade de Certificação**.
3. O Assistente de Certificado solicita que você insira as seguintes informações:
   - **Endereço de e-mail:** Endereço de e-mail do indivíduo ou conta de função responsável por gerenciar o certificado.
   - **Nome Comum:** Nome comum do indivíduo ou de uma conta de função responsável por gerenciar o certificado.
   - **Endereço de e-mail da CA:** Endereço de e-mail da Autoridade de Certificação.
4. Selecione as opções **Salvo em disco** e **Permitir que eu especifique as informações do par de chaves** e, em seguida, clique em **Continuar**.
5. Insira um nome para o arquivo CSR, salve o arquivo em seu computador e, em seguida, clique em **Salvar**.
6. Especifique as informações do par de chaves: Selecione o **Tamanho da Chave** de 2048 bits e o **algoritmo RSA** e, em seguida, clique em **Continuar**. O arquivo CSR está pronto para ser carregado como parte do processo de certificado APNs.
7. Clique em **Concluído** quando o Assistente de Certificados concluir o processo de CSR.
8. Para continuar, Assine o CSR.

Criar um CSR usando o Microsoft IIS

O primeiro passo para gerar uma solicitação de certificado APNs é criar uma Solicitação de Assinatura de Certificado (CSR). Para Windows, gere um CSR usando o Microsoft IIS.

1. Abra o Microsoft IIS.
2. Clique duas vezes no ícone Certificados de Servidor para IIS.

3. Na janela **Certificados de Servidor**, clique em **Criar Solicitação de Certificado**.
4. Digite as informações apropriadas do Nome Distinto (DN) e, em seguida, clique em **Avançar**.
5. Selecione **Microsoft RSA SChannel Cryptographic Provider** para o Provedor de Serviços Criptográficos e **2048** para o comprimento do bit e, em seguida, clique em **Avançar**.
6. Insira um nome de arquivo e especifique um local para salvar o CSR e, em seguida, clique em **Concluir**.
7. Para continuar, Assine o CSR.

Criar um CSR usando OpenSSL

Se você não puder usar um dispositivo macOS ou Microsoft IIS para gerar um CSR, use o OpenSSL. Você pode baixar e instalar o OpenSSL no site do OpenSSL.

1. No computador onde você instalou o OpenSSL, execute o seguinte comando a partir de um prompt de comando ou shell.

   `openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048`

2. A seguinte mensagem para informações de nomeação de certificado é exibida. Insira as informações conforme solicitado.

```
You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a
DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. Na próxima mensagem, insira uma senha para a chave privada do CSR.

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

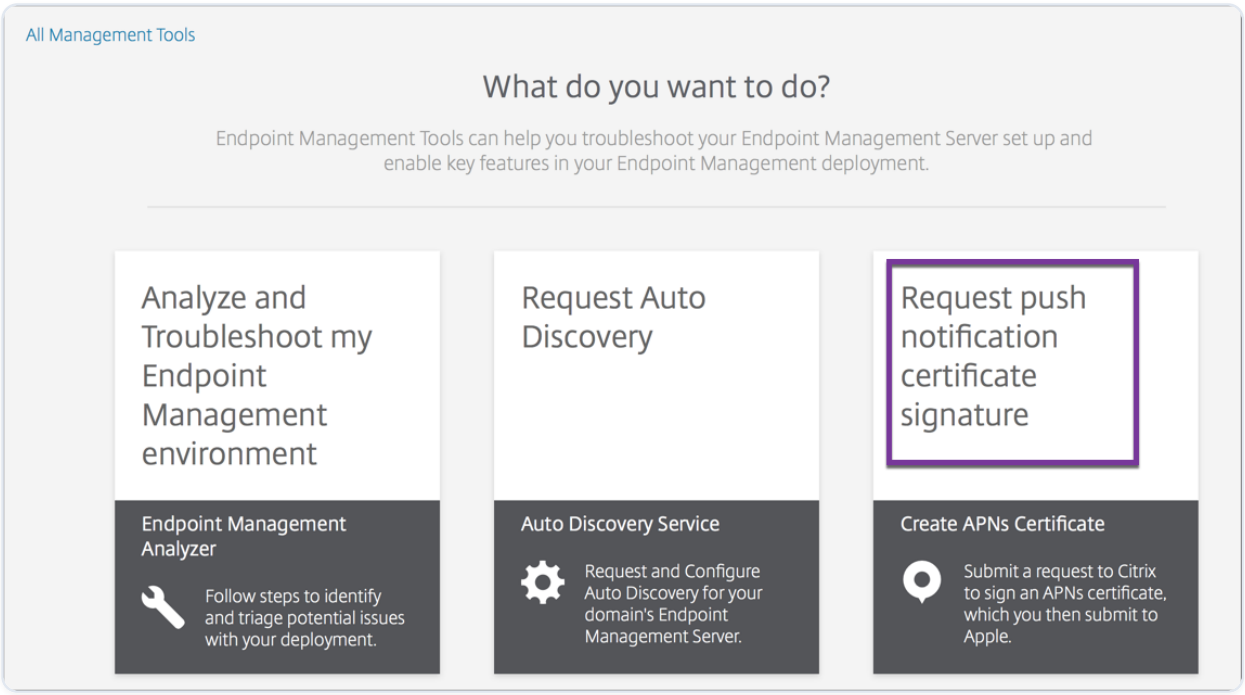
An optional company name []:
```

4. Para continuar, assine o CSR conforme descrito na próxima seção.

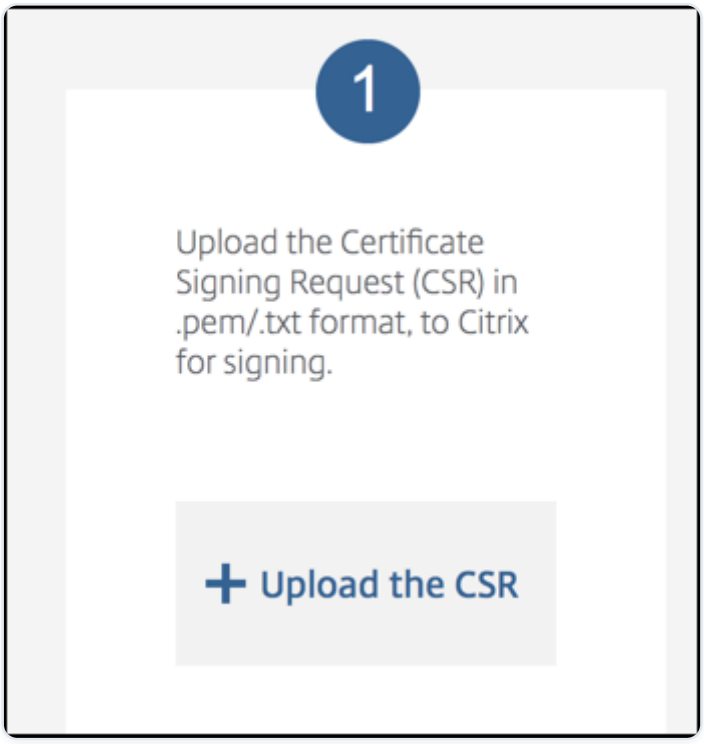
Assinar o CSR

Para usar um certificado com o XenMobile, envie-o à Citrix para assinatura. A Citrix assina o CSR com seu certificado de assinatura de gerenciamento de dispositivo móvel e retorna o arquivo assinado em formato `.plist`.

1. No seu navegador, acesse o site Endpoint Management Tools e clique em **Request push notification certificate signature**.



2. Na **página Criar um novo certificado**, clique em **Carregar o CSR**.



3. Navegue até e selecione o certificado.

   O certificado deve estar no formato .pem/txt.

4. Na página **Assinatura de CSR APNs do Endpoint Management**, clique em **Assinar**. O CSR é assinado e salvo automaticamente na sua pasta de download configurada.
5. Para continuar, envie o CSR assinado conforme descrito na próxima seção.

Envie o CSR assinado para a Apple para obter o certificado APNs

Após receber sua Solicitação de Assinatura de Certificado (CSR) assinada da Citrix, envie o CSR para a Apple para obter o certificado APNs necessário para importar para o XenMobile.

> **Nota:**
>
> Alguns usuários relataram problemas ao fazer login no Portal de Push da Apple. Como alternativa, faça login no Portal do Desenvolvedor da Apple e siga estas etapas:

1. Em um navegador, acesse o Portal de Certificados Push da Apple.
2. Clique em **Criar um Certificado**.
3. Na primeira vez que você criar um certificado com a Apple: Selecione a caixa de seleção **Li e concordo com estes termos e condições** e, em seguida, clique em **Aceitar**.
4. Clique em **Escolher Arquivo**, navegue até o CSR assinado em seu computador e, em seguida, clique em **Carregar**. Uma mensagem de confirmação indica que o upload foi bem-sucedido.
5. Clique em **Baixar** para recuperar o certificado .pem.
6. Para continuar, conclua o CSR e exporte um arquivo PKCS #12 conforme descrito na próxima seção.

Conclua o CSR e exporte um arquivo PKCS #12

Depois de receber o certificado APNs da Apple, retorne ao Acesso às Chaves, Microsoft IIS ou OpenSSL para exportar o certificado para um arquivo PCKS #12.

Um arquivo PKCS #12 contém o arquivo de certificado APNS e sua chave privada. Os arquivos PFX geralmente têm a extensão .pfx ou .p12. Você pode usar arquivos .pfx e .p12 de forma intercambiável.

> **Importante:**
>
> A Citrix recomenda que você salve ou exporte as chaves pessoais e públicas do sistema local. Você precisa das chaves para acessar os certificados APNs para reutilização. Sem as mesmas chaves, seu certificado é inválido e você deve repetir todo o processo de CSR e APNs.

Criar um arquivo PKCS #12 usando o Acesso às Chaves no macOS

Importante:

Use o mesmo dispositivo macOS para esta tarefa que você usou para gerar o CSR.

1. No dispositivo, localize o certificado de identidade de Produção (.pem) que você recebeu da Apple.
2. Inicie o aplicativo Acesso às Chaves e navegar até a guia **Login > Meus Certificados**. Arraste e solte o certificado de identidade do Produto na janela aberta.
3. Clique no certificado e expanda a seta esquerda para verificar se o certificado inclui uma chave privada associada.
4. Para começar a exportar o certificado para um certificado PCKS #12 (.pfx), escolha o certificado e a chave privada, clique com o botão direito e selecione **Exportar 2 itens**.
5. Dê ao arquivo de certificado um nome exclusivo para uso com o XenMobile. Não inclua caracteres de espaço no nome. Em seguida, escolha um local de pasta para o certificado salvo, selecione o formato de arquivo .pfx e clique em **Salvar**.
6. Insira uma senha para exportar o certificado. A Citrix recomenda que você use uma senha única e forte. Além disso, certifique-se de manter o certificado e a senha seguros para uso e referência futuros.
7. O aplicativo Acesso às Chaves solicitará a senha de login ou o conjunto de chaves selecionado. Digite a senha e clique em **OK**. O certificado salvo agora está pronto para uso com o XenMobile Server.
8. Para continuar, consulte Importar um certificado APNs para o XenMobile.

Criar um arquivo PKCS #12 usando o Microsoft IIS

Importante:

Use o mesmo servidor IIS para esta tarefa que você usou para gerar o CSR.

1. Abra o Microsoft IIS.
2. Clique no ícone **Certificados de Servidor**.

3. Na janela **Certificados de Servidor**, clique em **Concluir Solicitação de Certificado**.
4. Navegue até o arquivo Certificate.pem da Apple. Em seguida, digite um nome amigável ou o nome do certificado e clique em **OK**. Não inclua espaços no nome.
5. Selecione o certificado que você identificou na Etapa 4 e clique em **Exportar**.
6. Especifique um local e nome de arquivo para o certificado .pfx e uma senha, e clique em **OK**.

   Você precisará da senha do certificado para importá-lo para o XenMobile.
7. Copie o certificado .pfx para o servidor onde você planeja instalar o XenMobile.
8. Para continuar, consulte Importar um certificado APNs para o XenMobile.

Criar um arquivo PKCS #12 usando o OpenSSL

Se você usar o OpenSSL para criar um CSR, também poderá usar o OpenSSL para criar um certificado APNs .pfx.

1. Em um prompt de comando ou shell, execute o seguinte comando. `Customer.privatekey.pem` é a chave privada do seu CSR. `APNs_Certificate.pem` é o certificado que você acabou de receber da Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```
2. Insira uma senha para o arquivo de certificado .pfx. Lembre-se desta senha porque você a usará novamente ao carregar o certificado para o XenMobile.
3. Anote o local do arquivo de certificado .pfx. Em seguida, copie o arquivo para o XenMobile Server para que você possa usar o console para carregá-lo.
4. Para continuar, importe um certificado APNs para o XenMobile, conforme descrito na próxima seção.

Importar um certificado APNs para o XenMobile

Depois de receber o novo certificado APNs: Importe o certificado APNs para o XenMobile para adicionar o certificado pela primeira vez ou para substituir um certificado.

1. No console do XenMobile, vá para **Configurações > Certificados**.
2. Clique em **Importar > Keystore**.
3. Em **Usar como**, escolha **APNs**.
4. Procure o arquivo .pfx ou .p12 em seu computador.
5. Insira uma senha e clique em **Importar**.

Para obter mais informações sobre certificados no XenMobile, consulte Certificados e Autenticação.

Renovar um certificado APNs

> **Importante:**
>
> Se você usar um ID Apple diferente para o processo de renovação, deverá registrar novamente os dispositivos do usuário.

> Para renovar um certificado APNs, siga as etapas para criar um certificado e, em seguida, vá para o Portal de Certificados Push da Apple. Use esse portal para carregar o novo certificado. Após fazer login, seu certificado existente ou um certificado importado de sua conta anterior de Desenvolvedor Apple aparece.

No Portal de Certificados, a única diferença ao renovar o certificado é que você clica em **Renovar**. Você deve ter uma conta de desenvolvedor com o Portal de Certificados para acessar o site. Para renovar seu certificado, use o mesmo nome de organização e ID Apple.

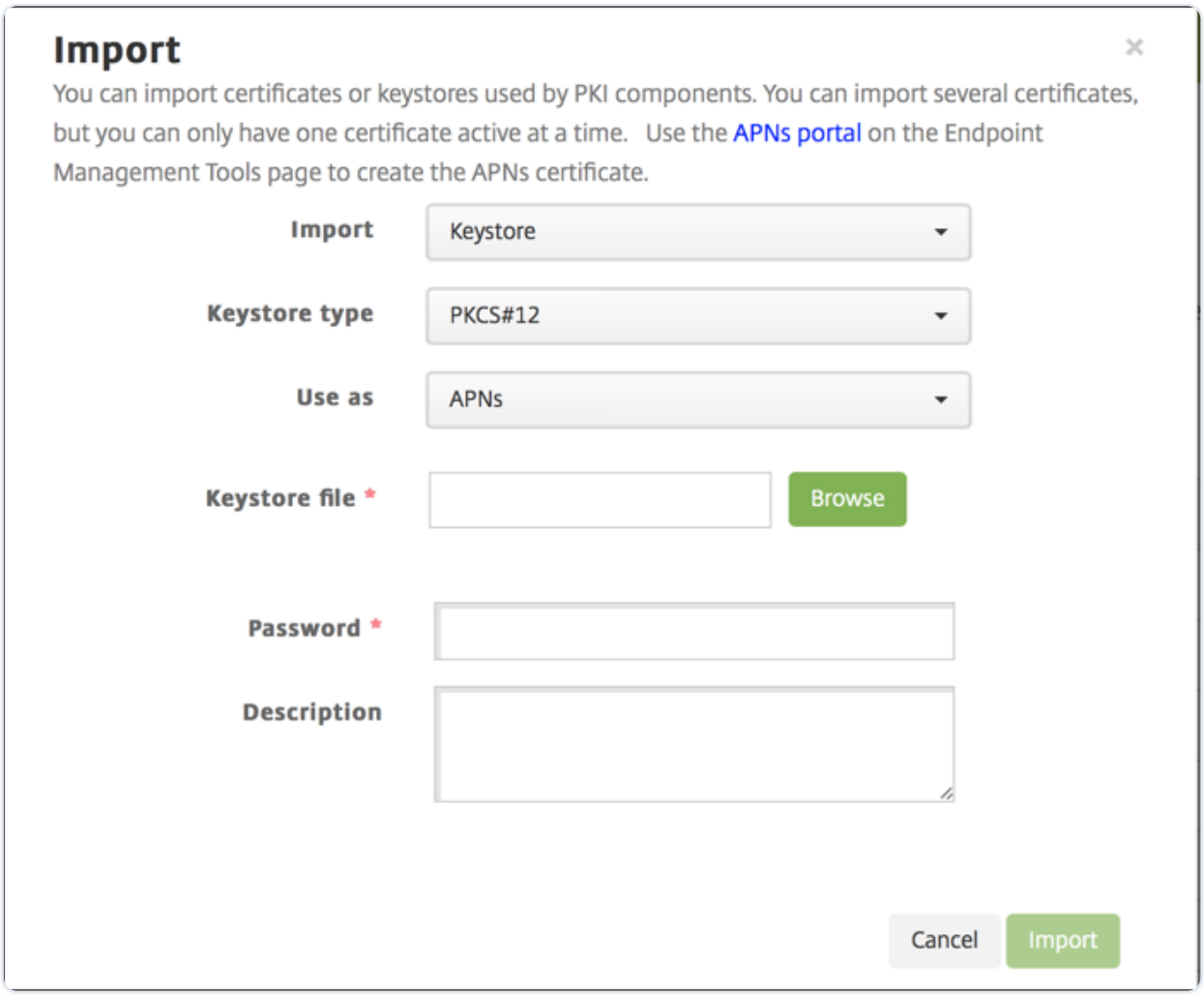
Para determinar quando seu certificado APNs expira no console do XenMobile, vá para **Configurações > Certificados**. Se o certificado expirar, não o revogue.

1. Gere um CSR usando Microsoft IIS, Acesso às Chaves (macOS) ou OpenSSL. Para obter mais informações sobre como gerar um CSR, consulte Criar uma Solicitação de Assinatura de Certificado.
2. No seu navegador, vá para Ferramentas de Gerenciamento de Endpoint. Em seguida, clique em **Solicitar assinatura de certificado de notificação push**.
3. Clique em **+ Carregar o CSR**.
4. Na caixa de diálogo, navegar até o CSR, clique em **Abrir** e clique em **Assinar**.
5. Quando você receber um arquivo `.plist`, salve-o.
6. No título da etapa 3, clique em **Portal de Certificados Push da Apple** e faça login.
7. Selecione o certificado que você deseja renovar e, em seguida, clique em **Renovar**.
8. Carregue o arquivo `.plist`. Você receberá um arquivo .pem como saída. Salve o arquivo .pem.
9. Usando esse arquivo .pem, conclua o CSR (de acordo com o método que você usou para criar o CSR na Etapa 1).

10. Exporte o certificado como um arquivo .pfx.

No console do XenMobile, importe o arquivo .pfx e conclua a configuração da seguinte forma:

1. Vá para **Configurações > Certificados > Importar**.
2. No menu **Importar**, escolha **Keystore**.
3. No menu **Tipo de Keystore**, escolha **PKCS #12.**
4. Em **Usar como**, escolha **APNs**.



5. Para **Arquivo Keystore**, clique em **Procurar** e navegar até o arquivo.
6. Em **Senha**, digite a senha do certificado.
7. Digite uma **Descrição** opcional.
8. Clique em **Importar**.

O XenMobile redireciona você de volta para a página **Certificados**. Os campos **Nome**, **Status**, **Válido de** e **Válido até** são atualizados.

SAML para logon único com o Citrix Files

> **Aviso:**
>
> Este recurso será descontinuado se o ShareFile (agora Progress) descontinuar o suporte.

Você pode configurar o XenMobile® e o ShareFile para usar a Security Assertion Markup Language (SAML) para fornecer acesso de logon único (SSO) aos aplicativos móveis do Citrix Files. Essa funcionalidade inclui:

- Aplicativos Citrix Files habilitados para MAM SDK ou empacotados usando o MDX Toolkit
- Clientes Citrix Files não empacotados, como o site, plug-in do Outlook ou clientes de sincronização
- **Para aplicativos Citrix Files empacotados**. Os usuários que fazem logon no Citrix Files por meio do aplicativo móvel Citrix Files são redirecionados para o Secure Hub para autenticação do usuário e para adquirir um token SAML. Após a autenticação bem-sucedida, o aplicativo móvel Citrix Files envia o token SAML para o ShareFile. Após o logon inicial, os usuários podem acessar o aplicativo móvel Citrix Files por meio de SSO. Eles também podem anexar documentos do ShareFile a e-mails do Secure Mail sem fazer logon a cada vez.
- **Para clientes Citrix Files não empacotados**. Os usuários que fazem logon no Citrix Files usando um navegador da web ou outro cliente Citrix Files são redirecionados para o XenMobile. O XenMobile autentica os usuários, que então adquirem um token SAML que é enviado para o ShareFile. Após o logon inicial, os usuários podem acessar os clientes Citrix Files por meio de SSO sem fazer logon a cada vez.

Para usar o XenMobile como um provedor de identidade SAML (IdP) para o ShareFile, você deve configurar o XenMobile para usar com contas Enterprise, conforme descrito neste artigo. Alternativamente, você pode configurar o XenMobile para funcionar apenas com conectores de zona de armazenamento. Para obter mais informações, consulte Usar ShareFile com XenMobile.

Para um diagrama de arquitetura de referência detalhado, consulte Arquitetura.

Pré-requisitos

Conclua os seguintes pré-requisitos antes de configurar o SSO com o XenMobile e os aplicativos Citrix Files:

- O MAM SDK ou uma versão compatível do MDX Toolkit (para aplicativos móveis Citrix Files).

Para obter mais informações, consulte Compatibilidade do XenMobile.

- Uma versão compatível dos aplicativos móveis Citrix Files e do Secure Hub.
- Conta de administrador do ShareFile.
- Conectividade verificada entre XenMobile e ShareFile.

Configurar acesso ao ShareFile

Antes de configurar o SAML para o ShareFile, forneça as informações de acesso ao ShareFile da seguinte forma:

1. No console web do XenMobile, clique em **Configurar > ShareFile**. A página de configuração do **ShareFile** é exibida.

   Configurações de configuração do ShareFile(/en-us/xenmobile/server/media/configure-content-collaboration-saml-for-non-mdx-apps.png)

2. Configure estas configurações:

   - **Domínio:** Digite o nome do seu subdomínio do ShareFile. Por exemplo: `example.sharefile.com`.
   - **Atribuir a grupos de entrega:** Selecione ou pesquise os grupos de entrega que você deseja que possam usar o SSO com o ShareFile.
   - **Logon da Conta de Administrador do ShareFile**
   - **Nome de usuário:** Digite o nome de usuário do administrador do ShareFile. Este usuário deve ter privilégios de administrador.
   - **Senha:** Digite a senha do administrador do ShareFile.
   - **Provisionamento de conta de usuário:** Deixe esta configuração desabilitada. Use a Ferramenta de Gerenciamento de Usuários do ShareFile para o provisionamento de usuários. Consulte Provisionar contas de usuário e grupos de distribuição.

3. Clique em **Testar Conexão** para verificar se o nome de usuário e a senha da conta de administrador do ShareFile autenticar na conta ShareFile especificada.
4. Clique em **Salvar**.

   - O XenMobile sincroniza com o ShareFile e atualiza as configurações do ShareFile **ShareFile Issuer/Entity ID** e **Login URL**.

- A página **Configurar > ShareFile** mostra o **Nome interno do aplicativo**. Você precisa desse nome para concluir as etapas descritas posteriormente em Modificar as configurações de SSO do Citrix Files.com.

Configurar SAML para aplicativos MDX do Citrix Files empacotados

Você não precisa usar o Citrix Gateway para a configuração de logon único com aplicativos MDX do Citrix Files empacotados. Para configurar o acesso para clientes do Citrix Files não empacotados, como o site, o plug-in do Outlook ou os clientes de sincronização, consulte Configurar o Citrix Gateway para outros clientes do Citrix Files.

As etapas a seguir se aplicam a aplicativos e dispositivos iOS e Android. Para configurar o SAML para aplicativos MDX do Citrix Files empacotados:

1. Com o MDX Toolkit, empacote o aplicativo móvel Citrix Files. Para obter mais informações sobre como empacotar aplicativos com o MDX Toolkit, consulte Empacotando aplicativos com o MDX Toolkit.
2. No console do XenMobile, carregue o aplicativo móvel Citrix Files empacotado. Para obter informações sobre como carregar aplicativos MDX, consulte Para adicionar um aplicativo MDX ao XenMobile.
3. Verifique as configurações do SAML: Faça logon no ShareFile com o nome de usuário e a senha de administrador que você configurou anteriormente.
4. Verifique se o ShareFile e o XenMobile estão configurados para o mesmo fuso horário. Certifique-se de que o XenMobile mostre a hora correta para o fuso horário configurado. Caso contrário, o SSO pode falhar.

Validar o aplicativo móvel Citrix Files

1. No dispositivo do usuário, instale e configure o Secure Hub.
2. Na XenMobile Store, baixe e instale o aplicativo móvel Citrix Files.
3. Inicie o aplicativo móvel Citrix Files. O Citrix Files é iniciado sem solicitar nome de usuário ou senha.

Validar com o Secure Mail

1. No dispositivo do usuário, se ainda não tiver sido feito, instale e configure o Secure Hub.
2. Na Loja XenMobile, baixe, instale e configure o Secure Mail.
3. Abra um novo formulário de e-mail e toque em **Anexar do Citrix Files**. Os arquivos disponíveis para anexar ao e-mail são exibidos sem solicitar nome de usuário ou senha.

Configurar o Citrix Gateway para Outros Clientes do Citrix Files

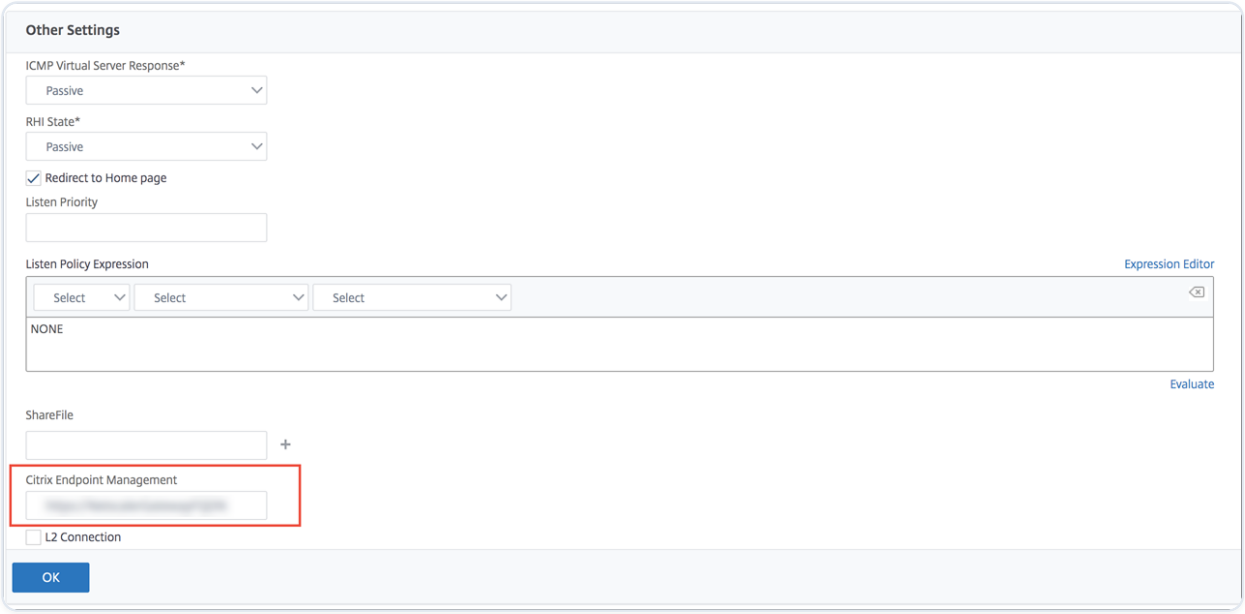
Para configurar o acesso para clientes do Citrix Files não encapsulados, como o site, o plug-in do Outlook ou os clientes de sincronização: Configure o Citrix Gateway para oferecer suporte ao uso do XenMobile como um provedor de identidade SAML da seguinte forma.

- Desativar o redirecionamento da página inicial.
- Crie uma política e um perfil de sessão do Citrix Files.
- Configure políticas no servidor virtual do Citrix Gateway.

Desativar o redirecionamento da página inicial

Desative o comportamento padrão para solicitações que chegam pelo caminho /cginfra. Essa ação permite que os usuários vejam a URL interna original solicitada em vez da página inicial configurada.

1. Edite as configurações do servidor virtual do Citrix Gateway que é usado para logons do XenMobile. No Citrix ADC, vá para **Outras Configurações** e desmarque a caixa de seleção rotulada **Redirecionar para a Página Inicial**.



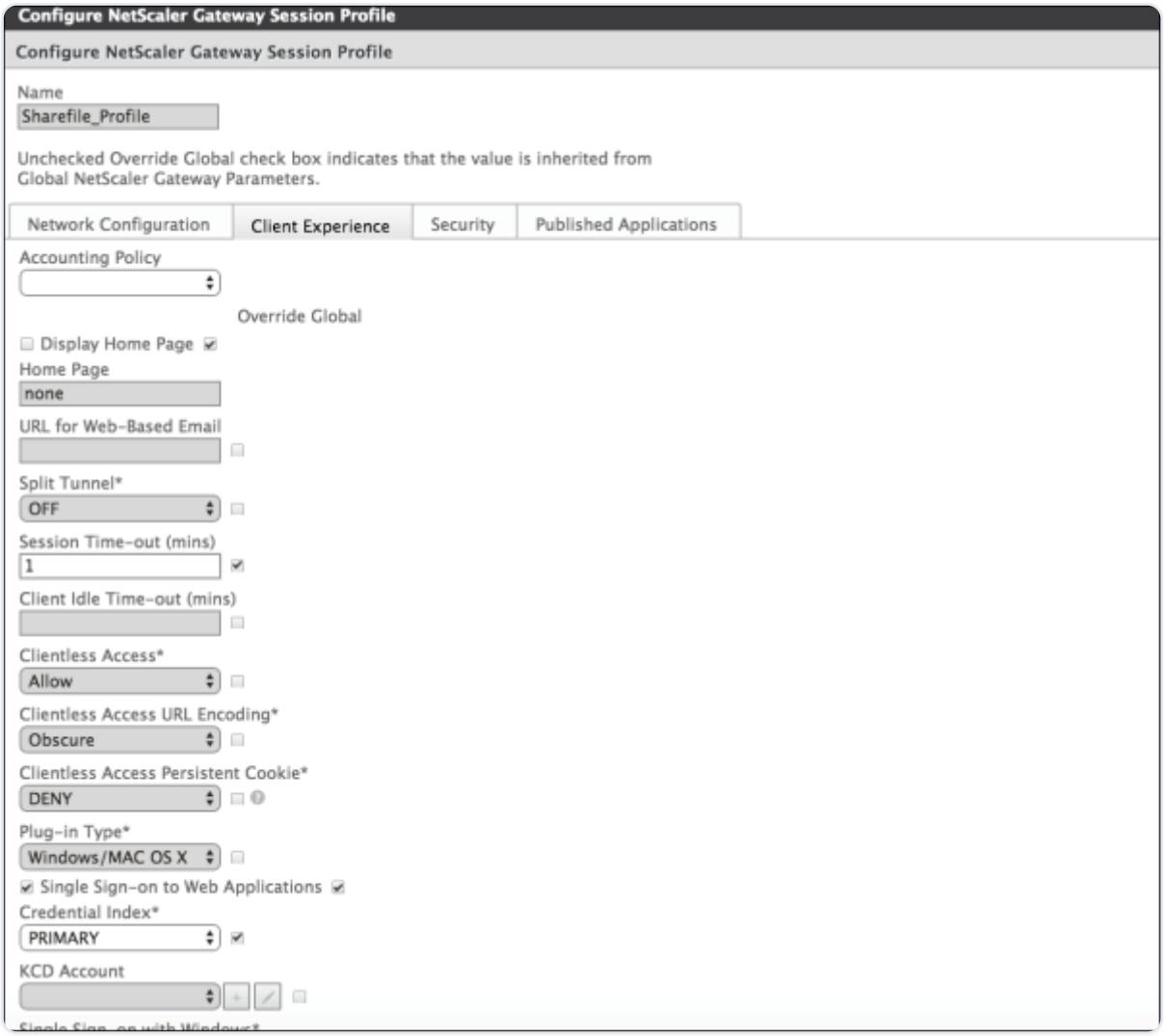
2. Em **ShareFile** (agora chamado ShareFile), digite o nome do seu servidor interno XenMobile e o número da porta.
3. Em **Citrix Endpoint Management™**, digite sua URL do XenMobile. Sua versão do Citrix Gateway pode se referir ao nome do produto mais antigo **AppController**.

   Essa configuração autoriza solicitações para a URL que você inseriu através do caminho / cginfra.

Crie uma política de sessão e um perfil de solicitação do Citrix Files

Configure estas configurações para criar uma política de sessão e um perfil de solicitação do Citrix Files:

1. No utilitário de configuração do Citrix Gateway, no painel de navegação esquerdo, clique em **Citrix Gateway > Policies > Session**.
2. Crie uma política de sessão. Na guia **Policies**, clique em **Add**.
3. No campo **Name**, digite **ShareFile_Policy**.
4. Crie uma ação clicando no botão **+**. A página **Create Session Profile** é exibida.

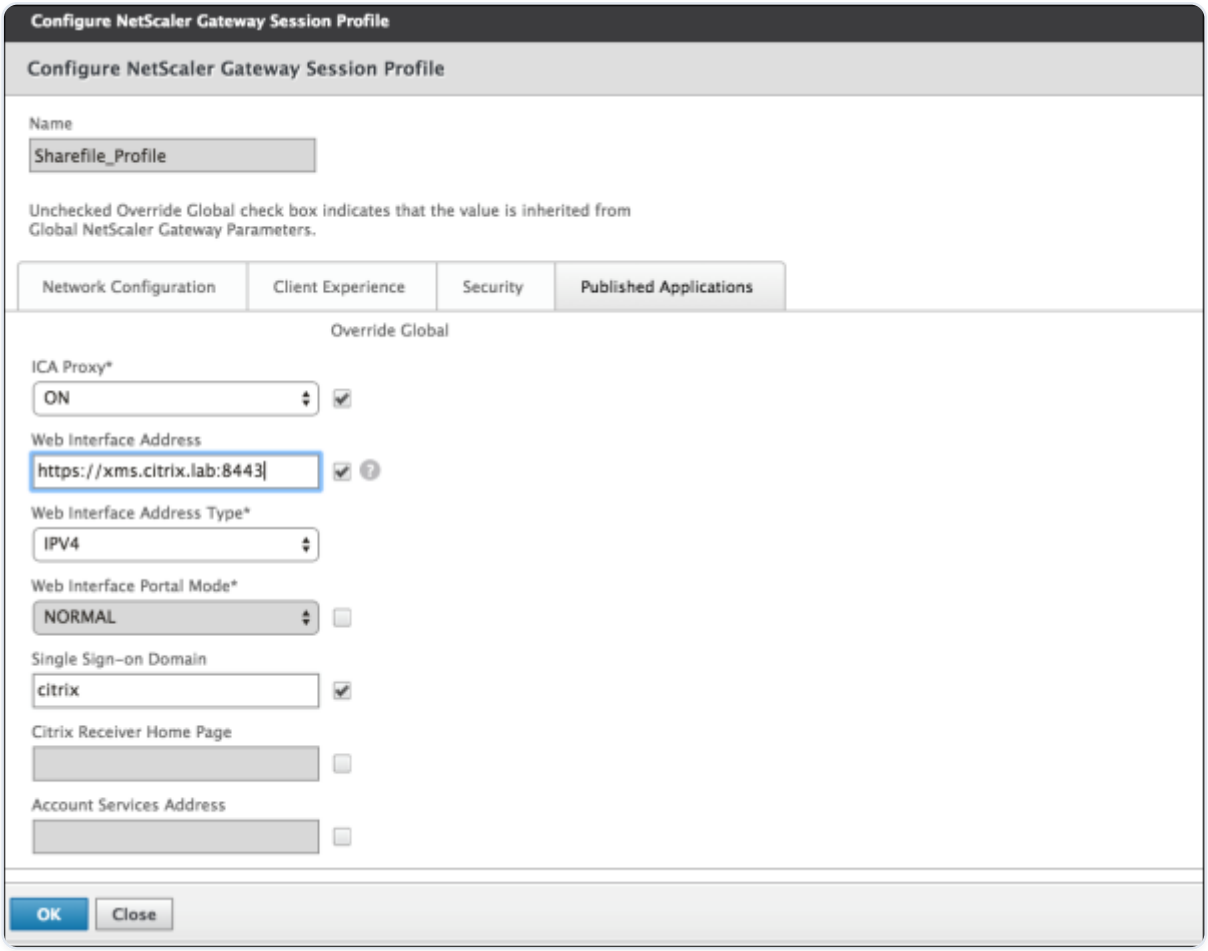


Configure estas configurações:

- **Nome:** Digite **ShareFile_Profile**.
- Clique na guia **Client Experience** e configure estas configurações:
  - **Página inicial:** Digite **none**.
  - **Tempo limite da sessão (min):** Digite **1**.

- **Logon único para aplicativos Web:** Selecione esta configuração.
- **Índice de credenciais:** Clique em **PRIMARY**.

- Clique na guia **Published Applications**.

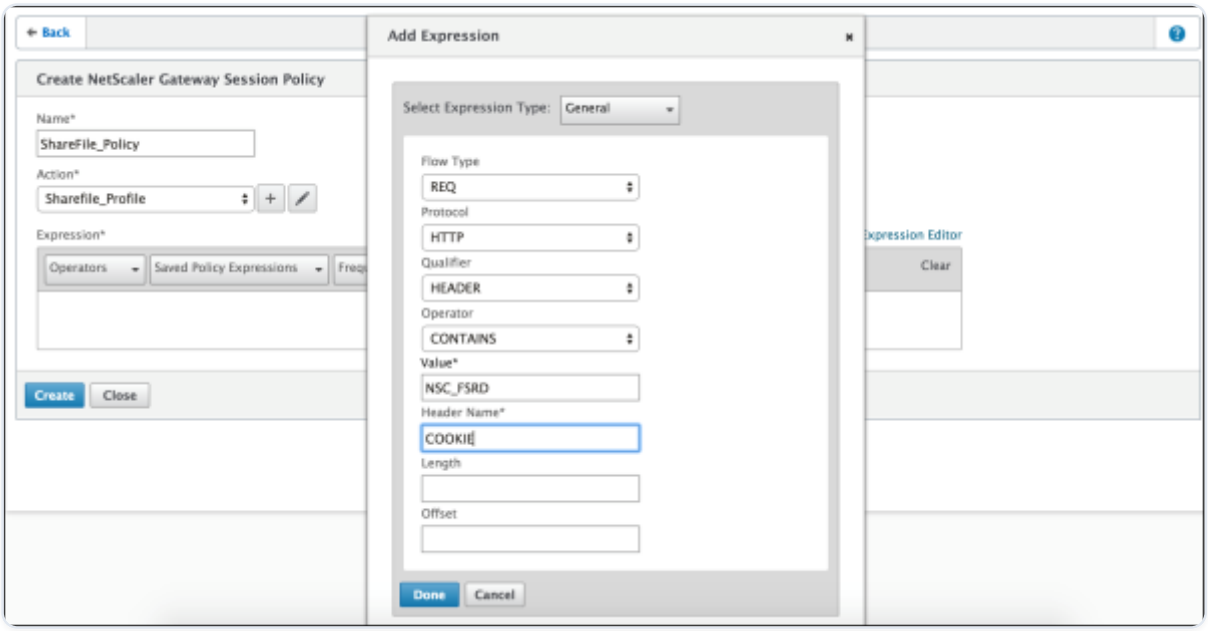


Configure estas configurações:

- **Proxy ICA®:** Clique em **ATIVADO**.
- **Endereço da Interface Web:** Digite a URL do seu XenMobile Server.
- **Domínio de Logon Único:** Digite o nome do seu domínio do Active Directory.

  Ao configurar o Perfil de Sessão do Citrix Gateway, o sufixo de domínio para **Domínio de Logon Único** deve corresponder ao alias de domínio do XenMobile definido no LDAP.

5. Clique em **Criar** para definir o perfil de sessão.
6. Clique em **Editor de Expressões**.



Configure estas configurações:

- **Valor:** Digite **NSC_FSRD**.
- **Nome do Cabeçalho:** Digite **COOKIE**.

7. Clique em **Criar** e depois em **Fechar**.

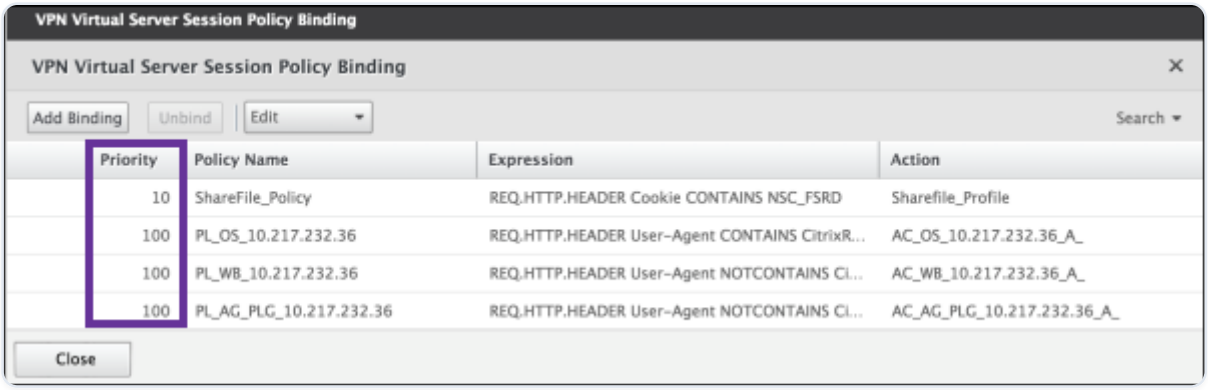


Configurar políticas no servidor virtual do Citrix Gateway

Configure estas configurações no servidor virtual do Citrix Gateway.

1. No utilitário de configuração do Citrix Gateway, no painel de navegação esquerdo, clique em **Citrix Gateway > Virtual Servers**.
2. No painel **Detalhes**, clique no seu servidor virtual do Citrix Gateway.
3. Clique em **Editar**.
4. Clique em **Políticas configuradas > Políticas de sessão** e, em seguida, clique em **Adicionar vinculação**.

5. Selecione **ShareFile_Policy**.
6. Edite o número de **Prioridade** gerado automaticamente para a política selecionada para que ela tenha a prioridade mais alta (o menor número) em relação a quaisquer outras políticas listadas. Por exemplo:



7. Clique em **Concluído** e, em seguida, salve a configuração em execução do Citrix ADC.

Modificar as configurações de SSO do Citrix Files.com

Faça as seguintes alterações para os aplicativos Citrix Files MDX e não MDX.

> **Importante:**

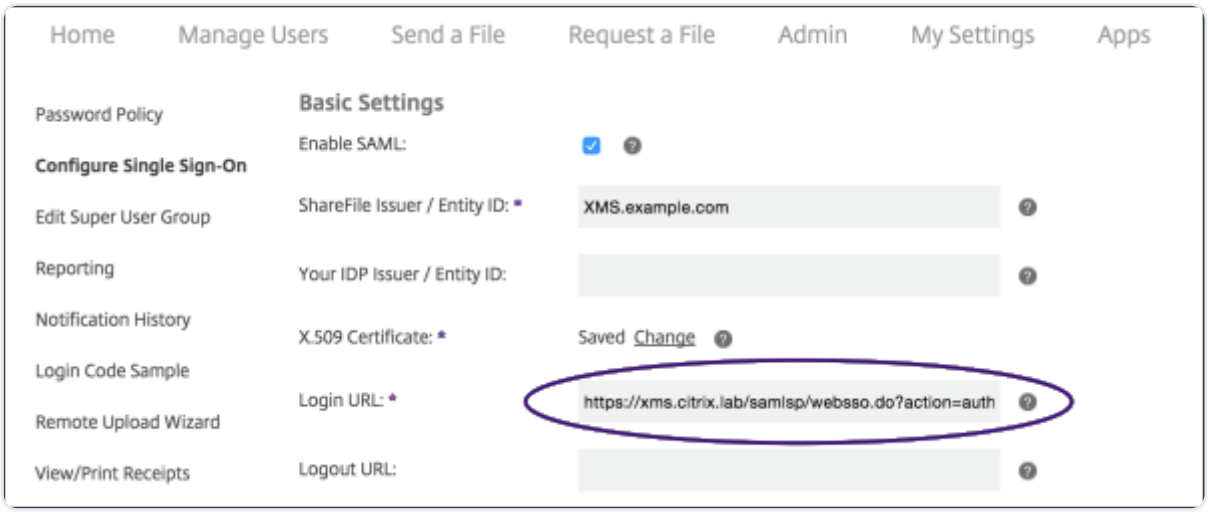
> Um novo número é anexado ao nome interno do aplicativo:

> - Cada vez que você edita ou recria o aplicativo Citrix Files
> - Cada vez que você altera as configurações do ShareFile no XenMobile

> Como resultado, você também deve atualizar a URL de Login no site do Citrix Files para refletir o nome do aplicativo atualizado.

1. Faça logon na sua conta ShareFile (`https://<subdomain>.sharefile.com`) como administrador do ShareFile.
2. Na interface web do ShareFile, clique em **Admin** e selecione **Configurar Logon Único**.
3. Edite a **URL de Logon** da seguinte forma:

   Aqui está um exemplo de **URL de Logon** antes das edições: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.



- Insira o FQDN externo do servidor virtual do Citrix Gateway mais `/cginfra/https/` na frente do FQDN do XenMobile Server e adicione **8443** após o FQDN do XenMobile.

  Aqui está um exemplo de URL editada: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

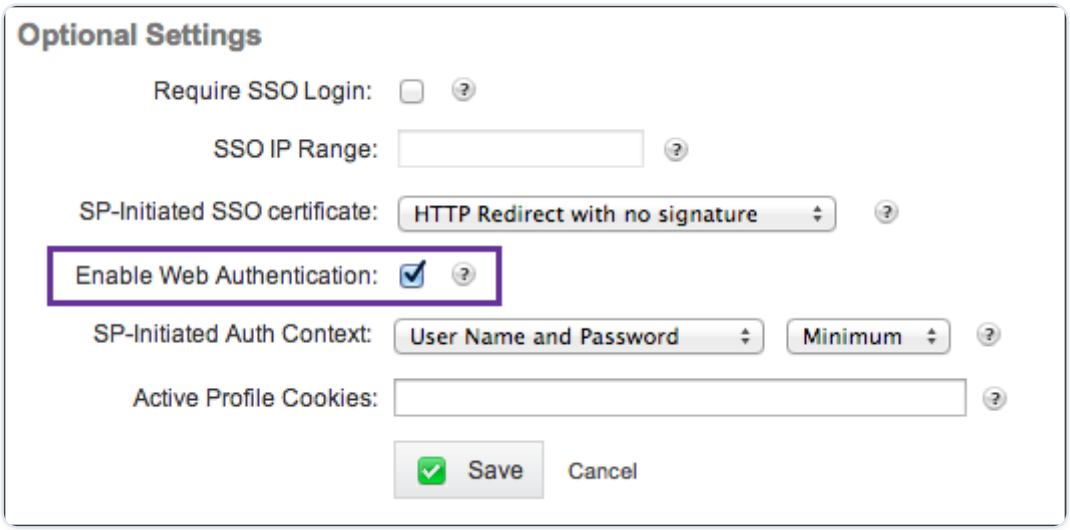
- Altere o parâmetro `&app=ShareFile_SAML_SP` para o nome interno do aplicativo Citrix Files. O nome interno é `ShareFile_SAML` por padrão. No entanto, toda vez que você altera sua configuração, um número é anexado ao nome interno (`ShareFile_SAML_2`, `ShareFile_SAML_3`, e assim por diante). Você pode consultar o **Nome interno do aplicativo** na página **Configurar > ShareFile**.

  Aqui está um exemplo de URL editada: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Adicione `&nssso=true` ao final da URL.

  Aqui está um exemplo da URL final: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. Em **Configurações Opcionais**, selecione a caixa de seleção **Habilitar Autenticação Web**.



Validar a configuração

Faça o seguinte para validar a configuração.

1. Aponte seu navegador para `https://<subdomain>sharefile.com/saml/login`.

   Você é redirecionado para o formulário de logon do Citrix Gateway. Se você não for redirecionado, verifique as configurações de configuração anteriores.

2. Insira o nome de usuário e a senha para o ambiente Citrix Gateway e XenMobile que você configurou.

   Suas pastas do Citrix Files em `<subdomain>.sharefile.com` aparecem. Se você não vir suas pastas do Citrix Files, certifique-se de ter inserido as credenciais de logon corretas.

Azure Active Directory como IdP

Configurar o Azure Active Directory (AAD) como seu provedor de identidade (IdP) permite que os usuários se inscrevam no XenMobile® usando suas credenciais do Azure.

Dispositivos iOS, Android, Windows 10 e Windows 11 são suportados. Dispositivos iOS e Android se inscrevem através do Secure Hub. Este método de autenticação está disponível apenas para usuários que se inscrevem no MDM através do Citrix Secure Hub. Dispositivos que se inscrevem no MAM não podem autenticar usando credenciais AAD. Para usar o Secure Hub com MDM+MAM, configure o XenMobile para usar o Citrix Gateway para inscrição MAM. Para obter mais informações, consulte Citrix Gateway e XenMobile.

Você configura o Azure como seu IdP em **Settings > Authentication > IDP**. A página **IDP** é nova nesta versão do XenMobile. Em versões anteriores do XenMobile, você configurava o Azure em **Settings > Microsoft Azure**.

Requisitos

- Versões e licenças
  - Para inscrever dispositivos iOS ou Android, você precisa do Secure Hub 10.5.5.
  - Para inscrever dispositivos Windows 10 e Windows 11, você precisa de licenças Microsoft Azure Premium.
- Serviços de diretório e autenticação
  - O XenMobile Server deve ser configurado para autenticação baseada em certificado.
  - Se você estiver usando o Citrix ADC para autenticação, o Citrix ADC deve ser configurado para autenticação baseada em certificado.
  - A autenticação do Secure Hub usa o Azure AD e respeita o modo de autenticação definido no Azure AD.
  - O XenMobile Server deve se conectar ao Windows Active Directory (AD) usando LDAP. Configure seu servidor LDAP local para sincronizar com o Azure AD.

Fluxo de autenticação

Quando o dispositivo se inscreve através do Secure Hub e o XenMobile está configurado para usar o Azure como seu IdP:

1. Os usuários inserem seu nome de usuário e senha do Azure Active Directory, em seu dispositivo, na tela de login do Azure AD mostrada no Secure Hub.
2. O Azure AD valida o usuário e envia um token de ID.
3. O Secure Hub compartilha o token de ID com o XenMobile Server.
4. O XenMobile valida o token de ID e as informações do usuário presentes no token de ID. O XenMobile retorna um ID de sessão.

Configuração da conta do Azure

Para usar o Azure AD como seu IdP, primeiro faça login em sua conta do Azure e faça estas alterações:

1. Registre seu domínio personalizado e verifique o domínio. Para obter detalhes, consulte Adicionar nome de domínio personalizado ao Azure Active Directory.
2. Estenda seu diretório local para o Azure Active Directory usando ferramentas de integração de diretório. Para obter detalhes, consulte Integração de Diretório.

Para usar o Azure AD para registrar dispositivos Windows 10 e Windows 11, faça as seguintes alterações em sua conta do Azure:

1. Torne o MDM uma parte confiável do Azure AD. Para fazer isso, clique em **Azure Active Directory > Aplicativos** e, em seguida, clique em **Adicionar**.
2. Selecione **Adicionar um aplicativo** na galeria. Vá para **GERENCIAMENTO DE DISPOSITIVOS MÓVEIS** e, em seguida, selecione **aplicativo MDM local**. Salve as configurações.

   Você escolhe um aplicativo local mesmo que tenha se inscrito no Citrix XenMobile cloud. Na terminologia da Microsoft, qualquer aplicativo não multi-tenant é um aplicativo MDM local.
3. No aplicativo, configure a descoberta do XenMobile Server, os pontos de extremidade dos termos de uso e o URI do ID do aplicativo:

   - **URL de Descoberta do MDM:** `https://<FQDN>:8443/<instanceName>/wpe`
   - **URL dos Termos de Uso do MDM:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **URI do ID do Aplicativo:** `https://<FQDN>:8443/`
4. Selecione o aplicativo MDM local que você criou na etapa 2. Habilite a opção **Gerenciar dispositivos para esses usuários** para habilitar o gerenciamento de MDM para todos os usuários ou qualquer grupo de usuários específico.

   Para obter mais informações sobre como usar o Azure AD com dispositivos Windows 10 e Windows 11, consulte o artigo da Microsoft Integração do Azure Active Directory com MDM.

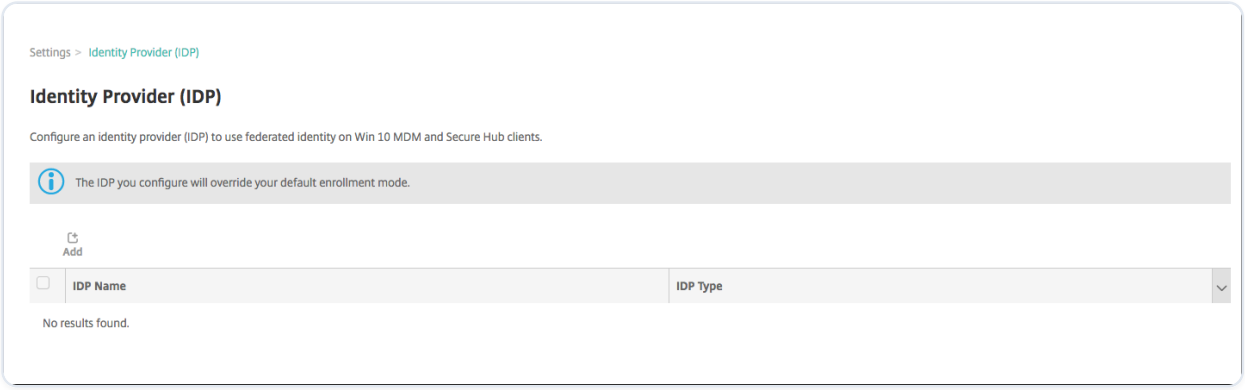
Configurar o Azure AD como seu IdP

1. Localize ou anote as informações de que você precisa da sua conta do Azure:

   - ID do locatário na página de configurações do aplicativo Azure.
   - Se você quiser usar o Azure AD para registrar dispositivos Windows 10 e Windows 11, também precisará:

     - **URI do ID do Aplicativo:** A URL para o servidor que executa o XenMobile.
     - **ID do Cliente:** O identificador exclusivo do seu aplicativo na página Configurar do Azure.
     - **Chave:** Na página de configurações do aplicativo Azure.
2. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.

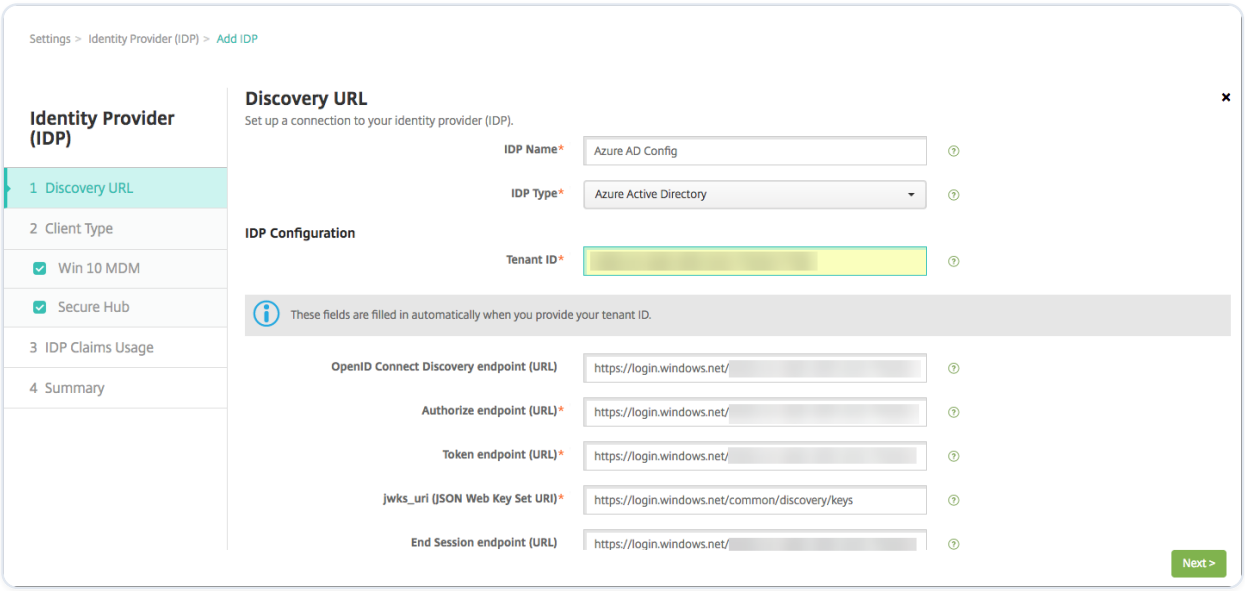
3. Em **Autenticação**, clique em **Provedor de Identidade (IDP)**. A página **Provedor de Identidade** é exibida.



4. Clique em **Adicionar**. A página **Configuração do IDP** é exibida.
5. Configure as seguintes informações sobre seu IdP:

   - **Nome do IdP:** Digite um nome para a conexão IdP que você está criando.
   - **Tipo de IdP:** Escolha Azure Active Directory como seu tipo de IdP.
   - **ID do Locatário:** Copie este valor da página de configurações do aplicativo Azure. Na barra de endereço do navegador, copie a seção composta por números e letras.

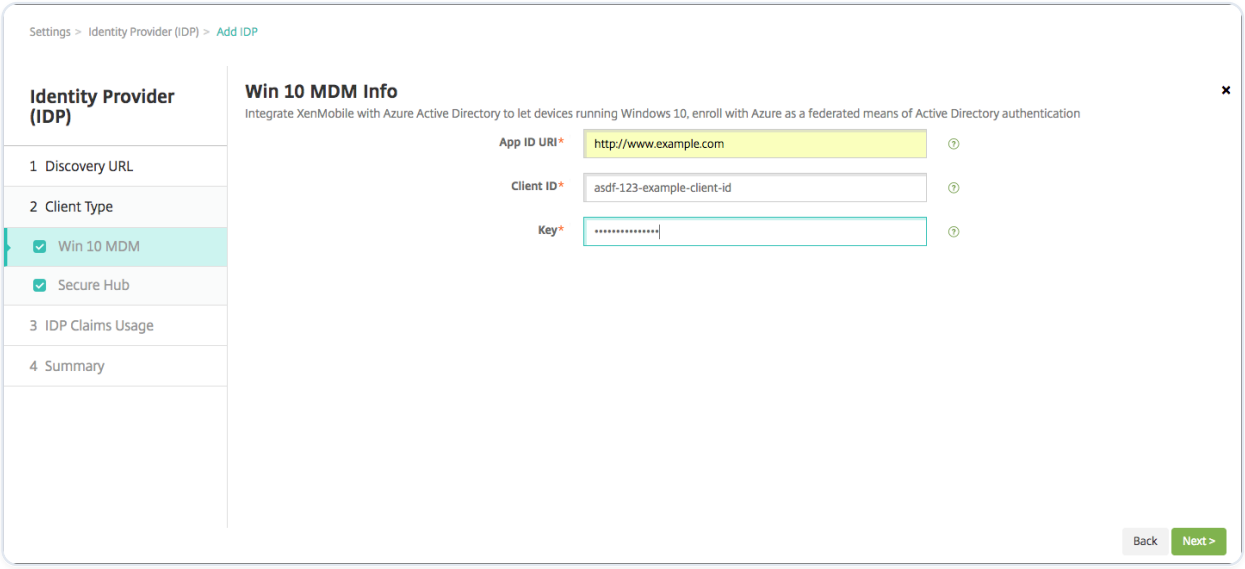
   Por exemplo, em `https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`, o ID do locatário é: `abc123-abc123-abc123`.



6. Os demais campos são preenchidos automaticamente. Quando estiverem preenchidos, clique em **Avançar**.

7. Para configurar o XenMobile para registrar dispositivos Windows 10 e Windows 11 usando o Azure AD para registro MDM, configure as seguintes configurações. Para pular esta etapa opcional, desmarque **Windows MDM**.

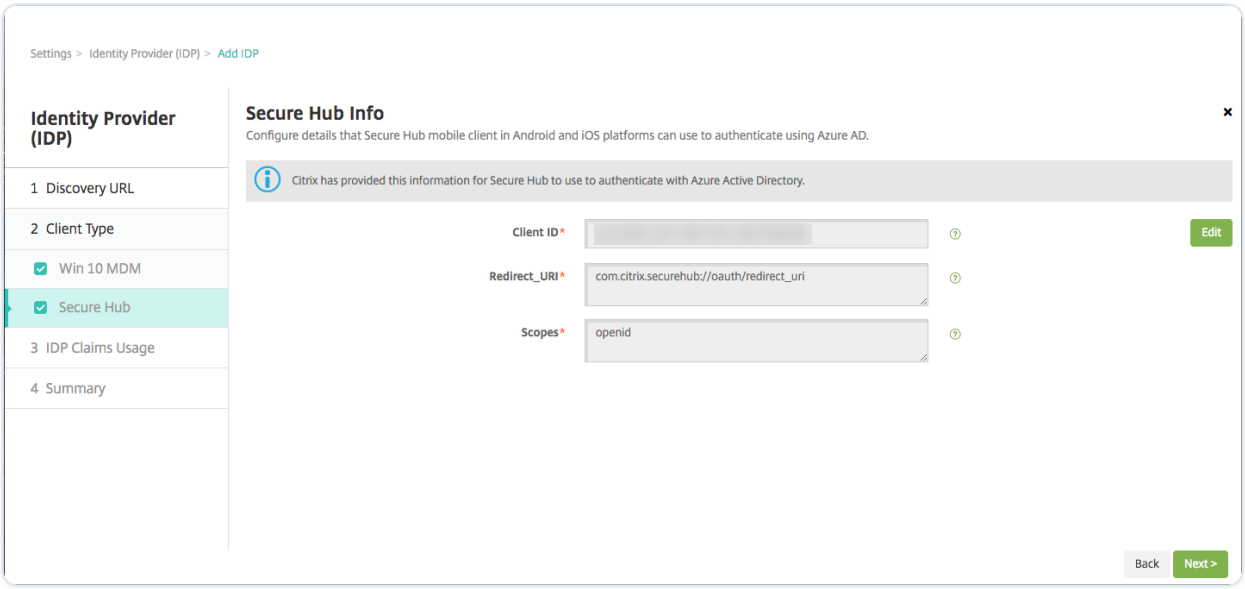
   - **URI da ID do Aplicativo:** Digite a URL do XenMobile Server que você inseriu ao configurar suas configurações do Azure.
   - **ID do Cliente:** Copie e cole este valor da página Configurar do Azure. A ID do cliente é o identificador exclusivo do seu aplicativo.
   - **Chave:** Copie este valor da página de configurações do aplicativo Azure. Em chaves, selecione uma duração na lista e salve a configuração. Você pode então copiar a chave e colá-la neste campo. Uma chave é necessária quando os aplicativos leem ou gravam dados no Microsoft Azure AD.



8. Clique em **Avançar**.

   A Citrix registrou o Secure Hub no Microsoft Azure e mantém as informações. Esta tela mostra os detalhes usados pelo Secure Hub para se comunicar com o Azure Active Directory. Esta página será usada no futuro se alguma dessas informações precisar de alteração. Edite esta página somente se a Citrix o aconselhar.

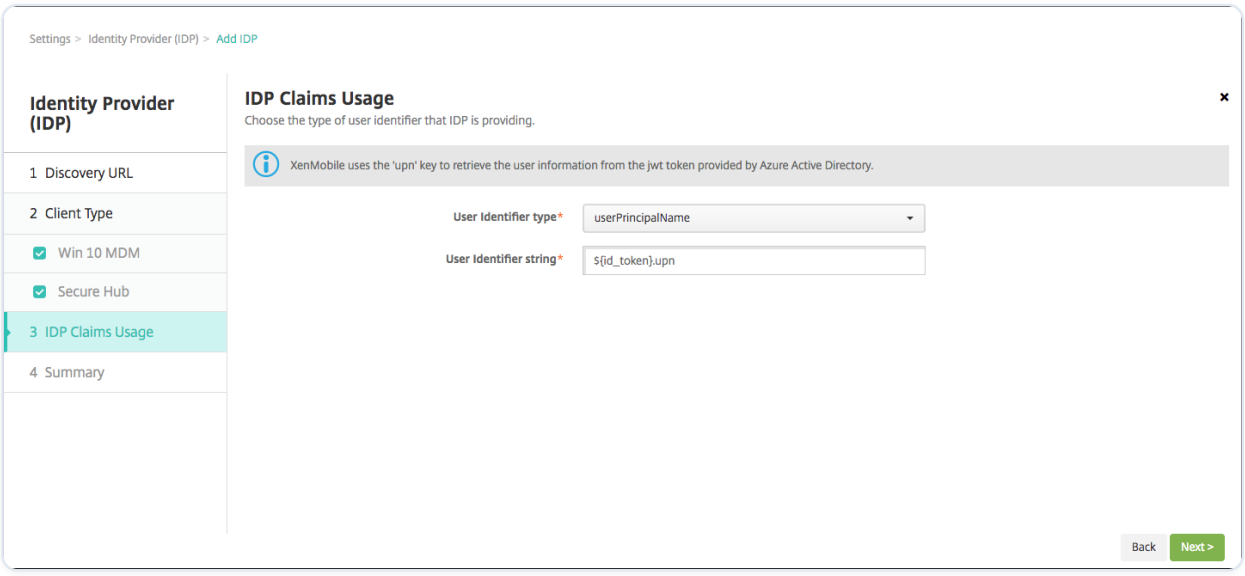
9. Clique em **Avançar**.



10. Configure o tipo de identificador de usuário que seu IdP fornece:

    - **Tipo de identificador de usuário:** Escolha **userPrincipalName** na lista.
    - **Cadeia de caracteres do identificador de usuário:** Este campo é preenchido automaticamente.

11. Clique em **Avançar**.

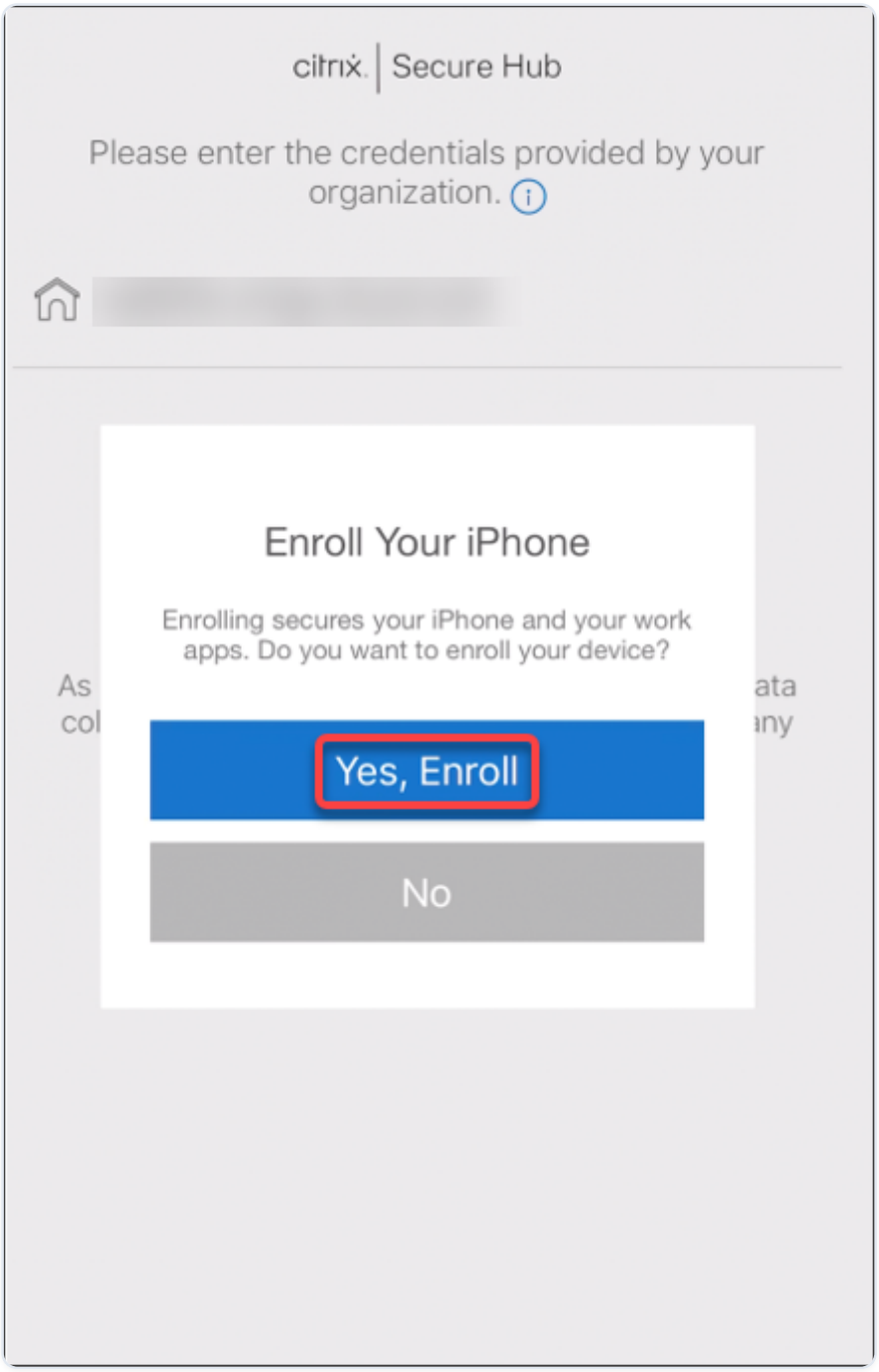


12. Revise a página **Resumo** e clique em **Salvar**.

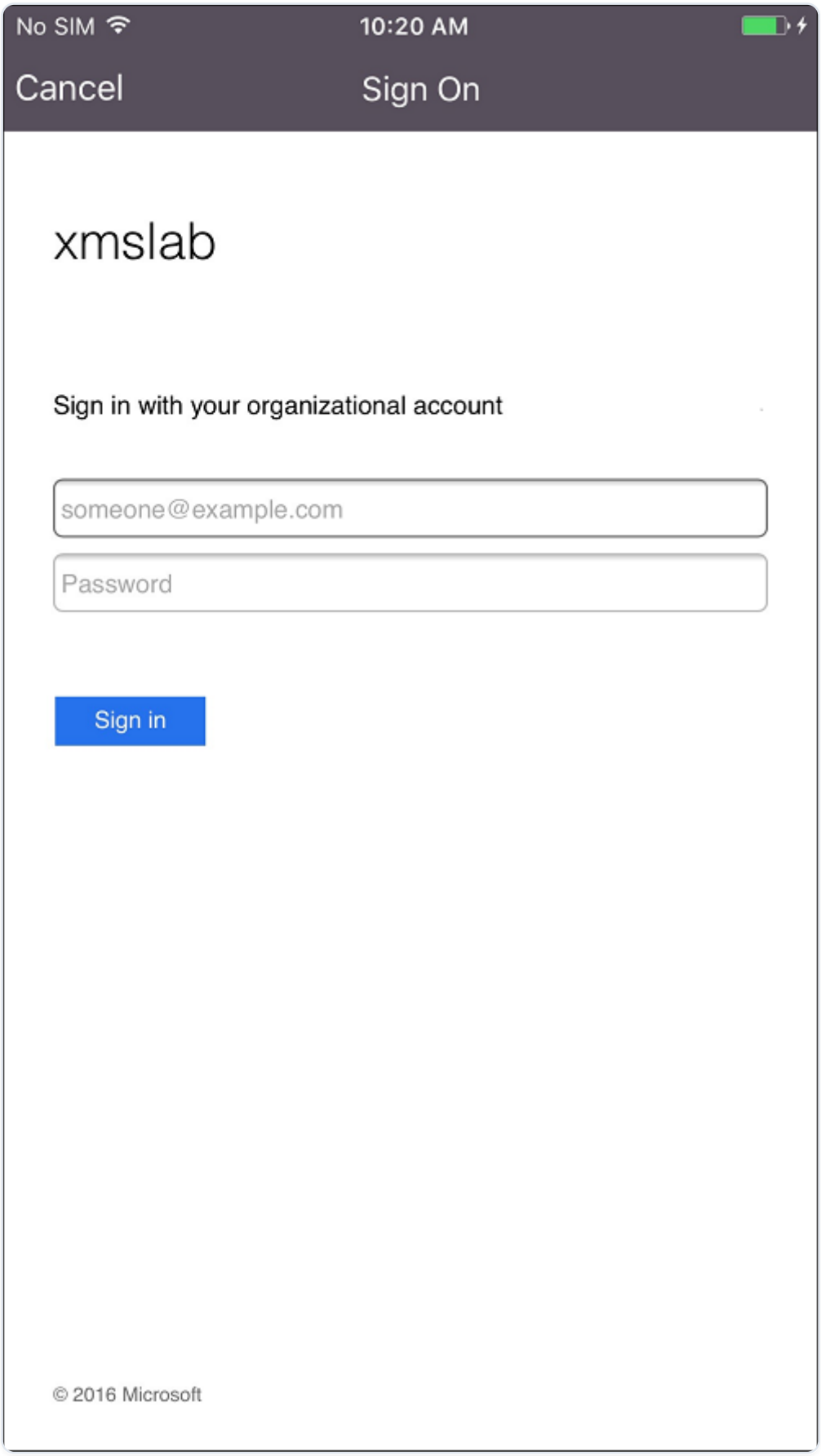


O que os usuários experimentam

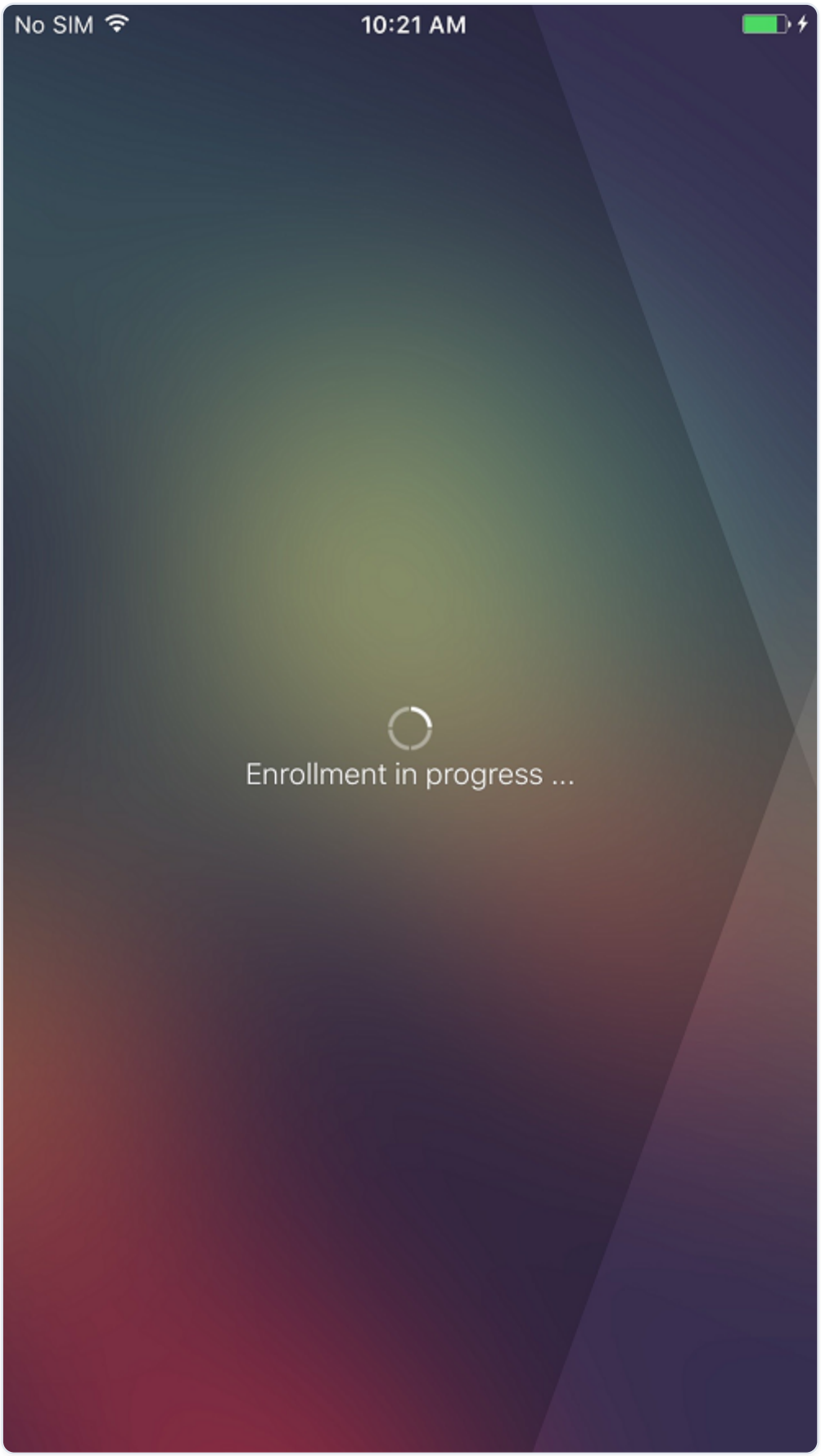
1. Os usuários iniciam o Secure Hub. Em seguida, os usuários inserem o Nome de Domínio Totalmente Qualificado (FQDN) do XenMobile Server, um Nome Principal de Usuário (UPN) ou o endereço de e-mail.

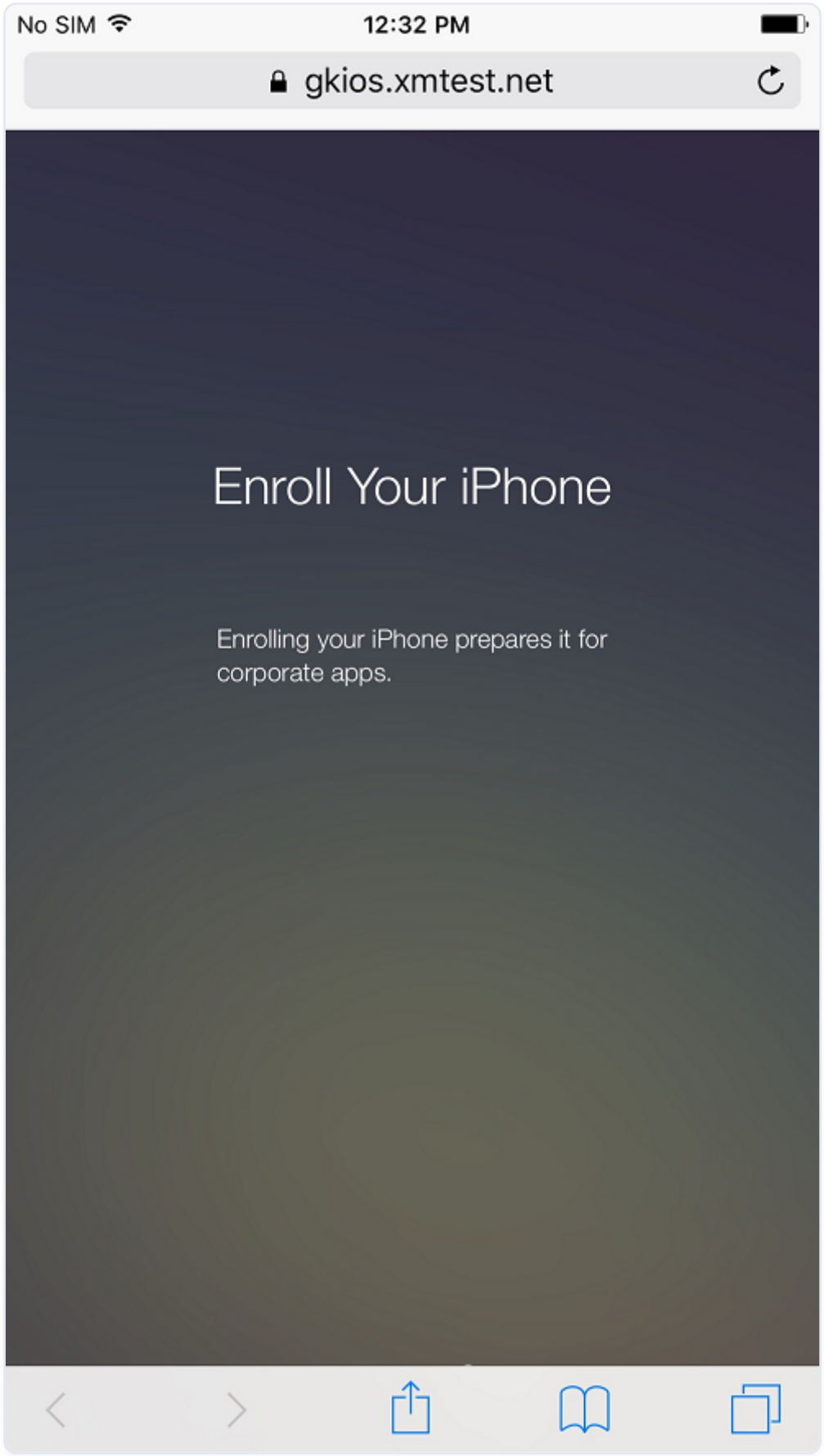


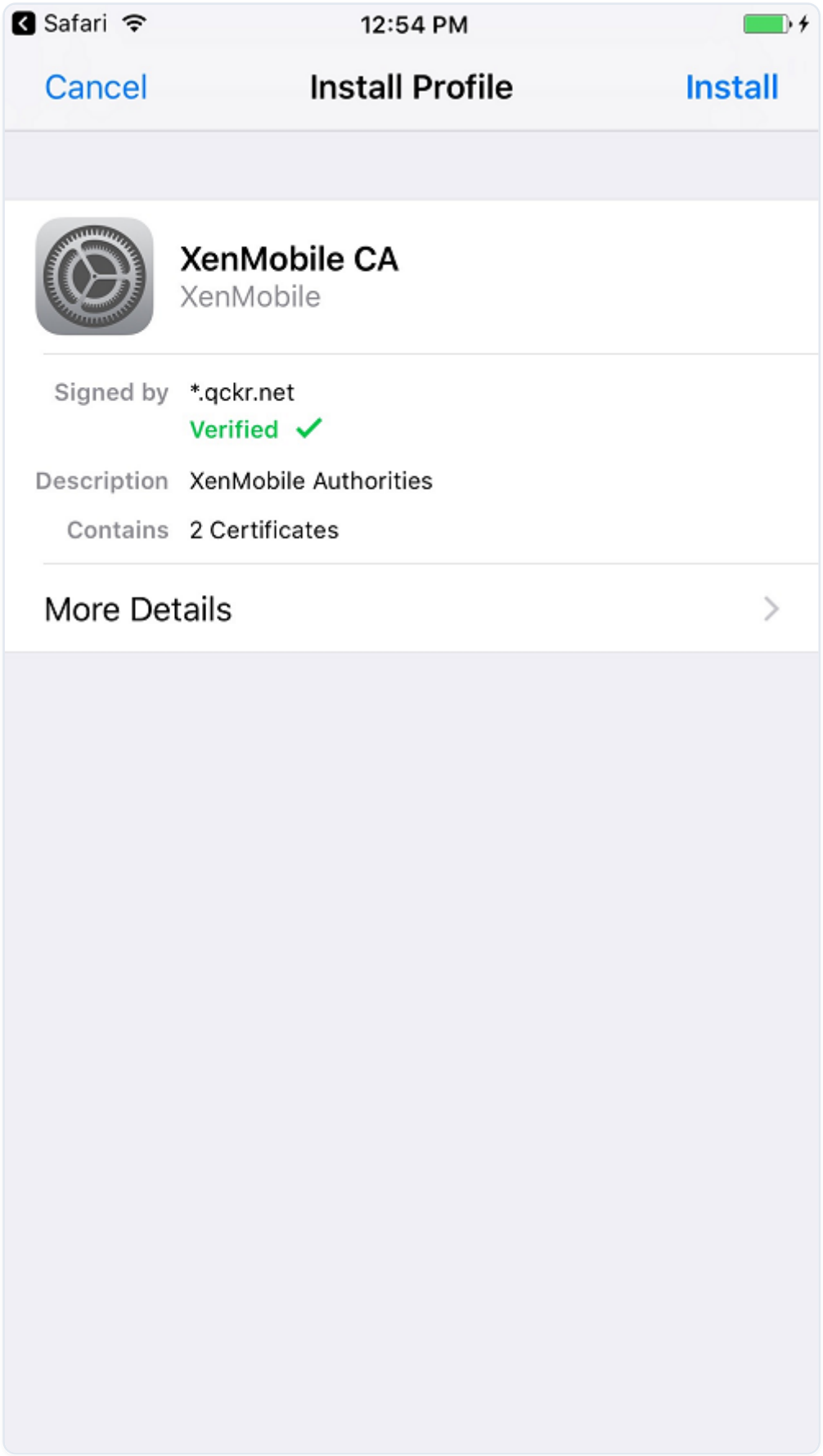
2. Em seguida, os usuários clicam em **Sim, Registrar**.



3. Os usuários fazem logon usando suas credenciais do Azure AD.


No SIM
10:21 AM
Enrollment in progress ...


No SIM
12:32 PM
gkios.xmtest.net
Enroll Your iPhone
Enrolling your iPhone prepares it for corporate apps.



4. Os usuários concluem as etapas de registro da mesma forma que qualquer outro registro através do Secure Hub.

Nota:

O XenMobile não oferece suporte à autenticação via Azure AD para convites de registro. Se você enviar aos usuários um convite de registro que tenha um URL de registro, os usuários autenticar via LDAP em vez do Azure AD.

Atualizar

Antes de atualizar para o XenMobile 10.16

1. Atualize seu Citrix License Server para 11.17.2.0 Build 47000 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.16.

   A versão mais recente do XenMobile requer o Citrix License Server 11.17 (versão mínima).

   A data do Customer Success Services (anteriormente, data do Subscription Advantage) no XenMobile 10.16 é November 15, 2022. A data do Customer Success Services em sua licença Citrix deve ser posterior a esta data. Você pode visualizar a data ao lado da licença no License Server. Se você conectar a versão mais recente do XenMobile a um ambiente de License Server mais antigo, a verificação de conectividade falhará e você não poderá configurar o License Server.

   Para renovar a data em sua licença, baixe o arquivo de licença mais recente do Citrix Portal e carregue o arquivo para o Licensing Server. Para obter mais informações, consulte Customer Success Services.
2. Para um ambiente em cluster: as implantações de políticas e aplicativos iOS para dispositivos que executam iOS 11 e posterior têm os seguintes requisitos. Se o Citrix Gateway estiver configurado para persistência SSL, você deve abrir a porta 80 em todos os nós do XenMobile® Server.
3. Se a máquina virtual que executa o XenMobile Server a ser atualizado tiver menos de 8 GB de RAM, recomendamos que você aumente a RAM para pelo menos 8 GB.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante uma atualização, backups completos permitem que você se recupere.

Para atualizar

Você pode atualizar diretamente para o XenMobile 10.16 a partir do XenMobile 10.15.x ou 10.14.x. Para realizar a atualização, baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (XenMobile) >**

XenMobile Server > Product Software > XenMobile Server 10. No bloco do software XenMobile Server para seu hipervisor, clique em **Download File**. Para carregar a atualização, use a página **Release Management** no console do XenMobile.

Para atualizar usando a página Release Management

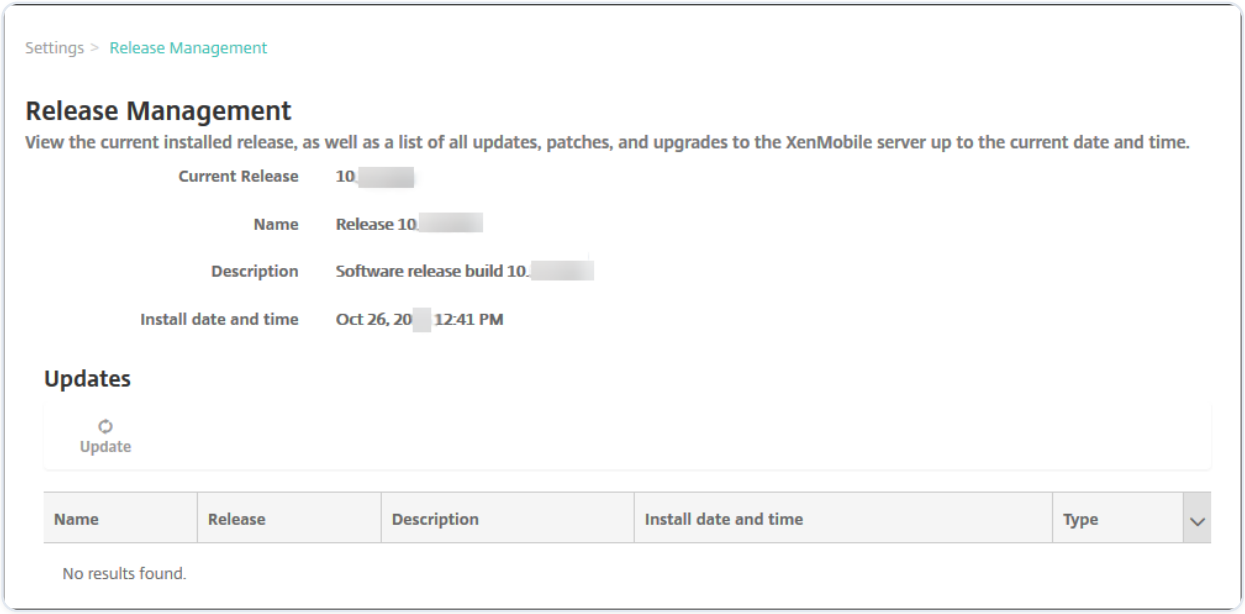
Use a página **Release Management** para atualizar para a versão mais recente do XenMobile Server.

Pré-requisitos:

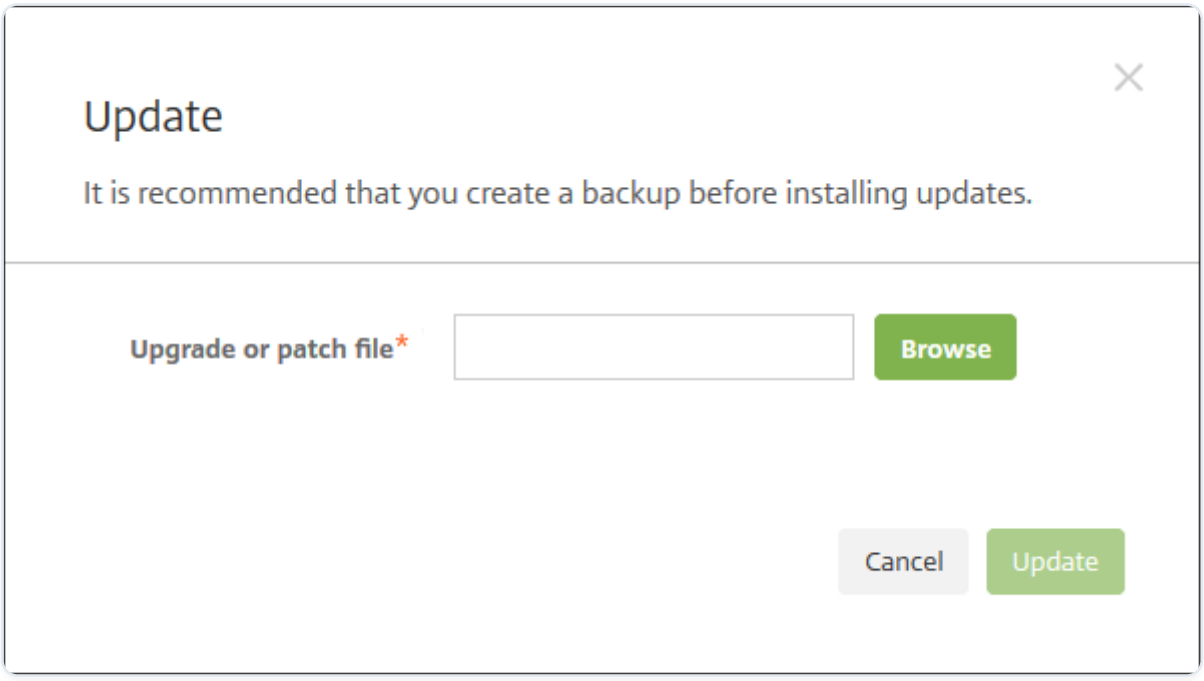
- Revise os Requisitos do Sistema.

Se você tiver uma implantação em cluster, consulte as instruções no final deste artigo.

1. Baixe o binário mais recente disponível: Vá para `<https://www.citrix.com/downloads>`. navegar até **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (local) > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server para seu hipervisor, clique em **Download File**.
2. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
3. Clique em **Release Management**. A página **Release Management** é exibida.



4. Em **Updates**, clique em **Update**. A caixa de diálogo **Update** é exibida.



5. Selecione o arquivo de atualização do XenMobile que você baixou de Citrix.com clicando em **Browse** e navegando até o local do arquivo.
6. Clique em **Update** e, se solicitado, reinicie o XenMobile.

   Se, por algum motivo, a atualização não puder ser concluída com êxito, uma mensagem de erro será exibida para indicar o problema. O sistema é revertido para o estado anterior à tentativa de atualização.

Após a atualização

Após uma atualização, o XenMobile requer uma reinicialização. Use a CLI do XenMobile para reiniciar o XenMobile Server. É importante que você limpe o cache do seu navegador após a reinicialização do sistema.

Se a funcionalidade que envolve conexões de saída parar de funcionar e você não tiver alterado sua configuração de conexão, verifique o **log do XenMobile Server** para erros como o seguinte: "Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer"

O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Por padrão, a verificação do nome do host está habilitada em conexões de saída, exceto para o servidor Microsoft PKI. Se a verificação do nome do host quebrar sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **true**. O valor padrão desta propriedade é **false**.

A Citrix publica novas versões ou atualizações importantes do XenMobile em Citrix.com. Ao mesmo tempo, um aviso é enviado ao contato registrado de cada cliente.

Para atualizar implantações XenMobile em cluster

> **Importante:**
>
> Antes de instalar uma atualização do XenMobile, use a funcionalidade em sua máquina virtual (VM) para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se você tiver problemas durante uma atualização, backups completos permitem que você se recupere.

Se o seu sistema estiver configurado no modo cluster, siga estas etapas para atualizar cada nó de uma versão do XenMobile 10:

1. Carregue o arquivo .bin em todos os nós em **Configurações > Gerenciamento de Versões**.
2. Desligue todos os nós no **Menu do Sistema** na CLI.
3. Inicie um nó, no **Menu do Sistema** na CLI, e verifique se o serviço está em execução.
4. Inicie os outros nós um após o outro.

   Se o XenMobile não conseguir concluir a atualização com sucesso, uma mensagem de erro aparece para indicar o problema. O XenMobile então reverte o sistema para o estado anterior à tentativa de atualização.

Atualizar da Edição XenMobile MDM para a Edição Enterprise

Você pode atualizar a Edição XenMobile MDM para a Edição Avançada do XenMobile (No local) ou Citrix Endpoint Management™ (nuvem) para dispositivos iOS e Android.

Pré-requisitos

- A licença Enterprise correta.
- O Citrix Gateway está configurado.

Para atualizar

1. Vá para **Configurações > Licenciamento** e verifique se o tipo de licença correto da Enterprise Edition foi carregado.

2. Vá para **Configurações > Propriedades do Servidor** e altere a propriedade **Modo do Servidor** de **MDM** para **ENT**.
3. Vá para **Configurações > Citrix Gateway** e configure os detalhes do Citrix Gateway. Defina o modo de autenticação para o mesmo da MDM Edition, ou seja, autenticação de domínio (Active Directory). O XenMobile não oferece suporte à alteração do modo de autenticação após o registro do usuário.
4. Opcional: Vá para **Configurações > Propriedades do Cliente** e habilite a autenticação por PIN do Citrix.

Depois de concluir essas etapas, os usuários devem executar as seguintes etapas para alternar um dispositivo para o modo Enterprise.

Usuários de iOS

1. Feche o Secure Hub: Toque no botão inicial do dispositivo duas vezes (rapidamente) e deslize o aplicativo Secure Hub para cima.
2. Abra o Secure Hub.

Usuários de Android

1. Abra o Secure Hub.
2. Vá para **Preferências > Informações do Dispositivo**.
3. Clique em **Atualizar Política**.

Se você habilitou a autenticação por PIN do Citrix, o Secure Hub solicita que os usuários criem um PIN. Depois que um usuário cria um PIN, o XenMobile configura o dispositivo no modo Enterprise. No console do XenMobile, a página **Gerenciar > Dispositivos** mostra MDM e MAM como ativos para o dispositivo.

Contas de usuário, funções e registro

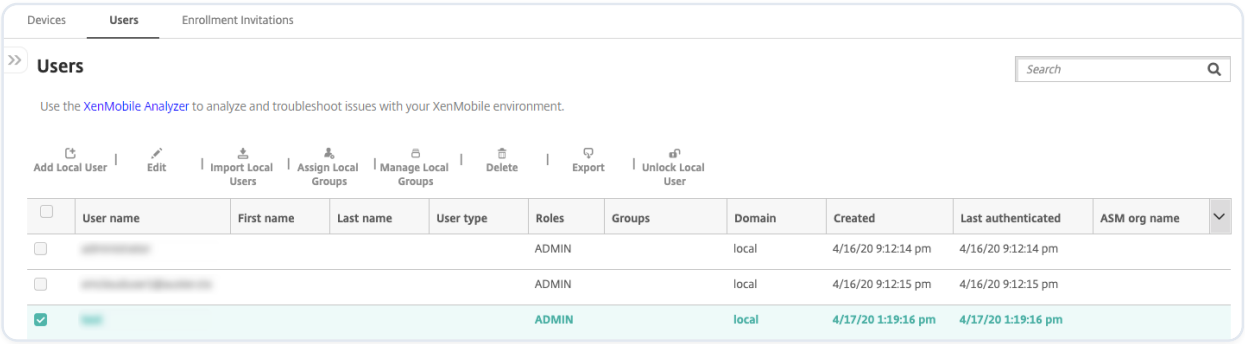
Você configura contas de usuário, funções e registro no console do XenMobile® na guia **Gerenciar** e na página **Configurações**. Salvo indicação em contrário, as etapas para as seguintes tarefas são fornecidas neste artigo.

- Contas de usuário e grupos:
  - Em **Gerenciar > Usuários**, adicione contas de usuário manualmente ou use um arquivo de provisionamento .csv para importar as contas e gerenciar grupos locais.
  - Em **Configurações > Fluxos de trabalho**, use fluxos de trabalho para gerenciar a criação e remoção de contas de usuário.
- Funções para contas de usuário e grupos
  - Em **Configurações > Controle de Acesso Baseado em Função**, atribua funções predefinidas, ou conjuntos de permissões, a usuários e grupos. Essas permissões controlam o nível de acesso que os usuários têm às funções do sistema. Para obter mais informações, consulte Configurar funções com RBAC.
  - Em **Configurações > Modelos de Notificação**, para criar ou atualizar os modelos de notificação a serem usados em ações automatizadas, registro e mensagens de notificação padrão enviadas aos usuários. Você configura os modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS. Para obter mais informações, consulte: Criar e atualizar modelos de notificação.
- Modo de segurança de registro e convites
  - Em **Configurações > Registro**, configure até sete modos de segurança de registro e envie convites de registro. Cada modo de segurança de registro tem seu próprio nível de segurança e etapas que os usuários devem seguir para registrar seus dispositivos.
  - Habilitar AutoDiscovery no XenMobile para registro de usuário

Para adicionar, editar, desbloquear ou excluir contas de usuário locais

Você pode adicionar contas de usuário locais ao XenMobile manualmente ou pode usar um arquivo de provisionamento para importar as contas. Para as etapas de importação de contas de usuário de um arquivo de provisionamento, consulte Importar contas de usuário.

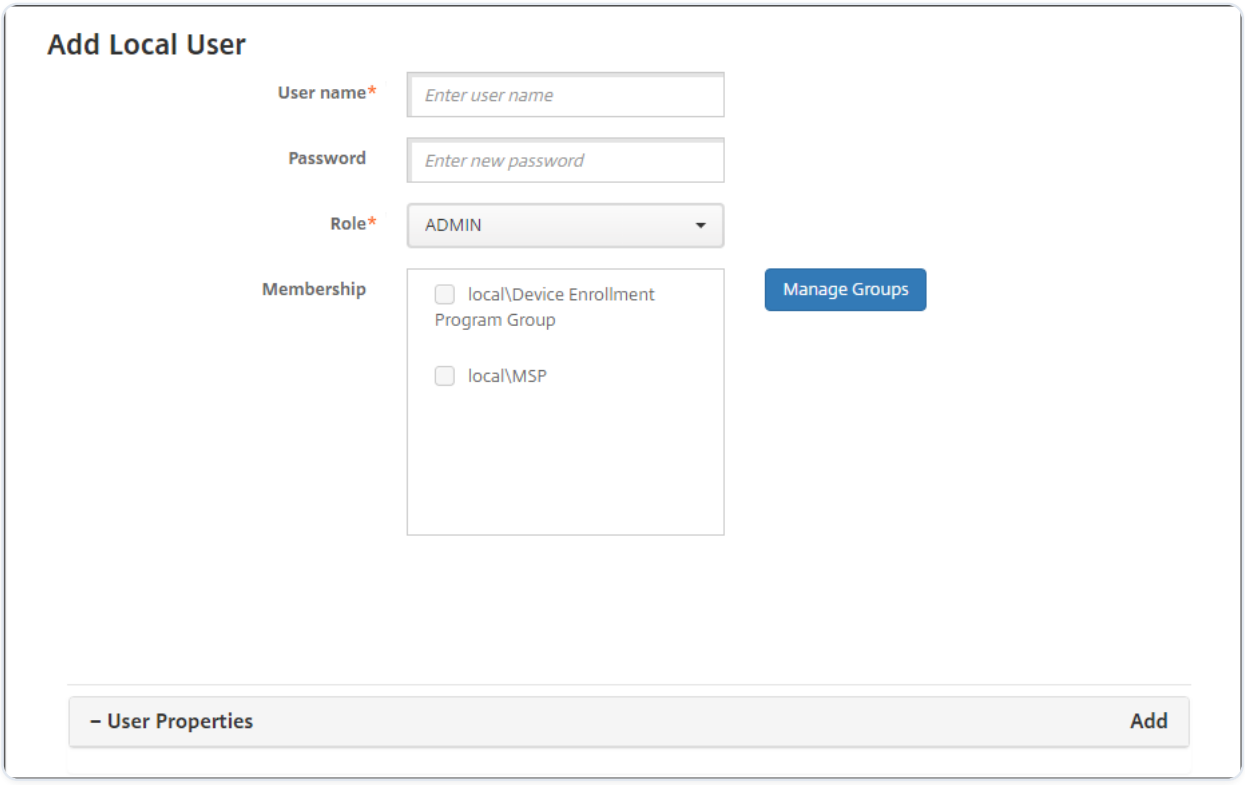
1. No console do XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.



2. Clique em **Mostrar filtro** para filtrar a lista.

Para adicionar uma conta de usuário local

1. Na página **Usuários**, clique em **Adicionar Usuário Local**. A página **Adicionar Usuário Local** é exibida.



2. Configure estas configurações:

- **Nome de usuário:** Digite o nome, um campo obrigatório. Você pode incluir espaços nos nomes, além de letras maiúsculas e minúsculas.
- **Senha:** Digite uma senha de usuário opcional. A senha deve ter pelo menos 14 caracteres e atender a todos os seguintes critérios:
  - Incluir pelo menos dois números
  - Incluir pelo menos uma letra maiúscula e uma minúscula
  - Incluir pelo menos um caractere especial
  - Não inclua palavras de dicionário ou palavras restritas, como seu nome de usuário ou endereço de e-mail Citrix®
  - Não inclua mais de três caracteres sequenciais e repetidos ou padrões de teclado, como 1111, 1234 ou asdf
- **Função:** Na lista, clique na função do usuário. Para obter mais informações sobre funções, consulte Configurar funções com RBAC. As opções possíveis são:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPORTE
  - USUÁRIO
- **Associação:** Na lista, clique no grupo ou grupos aos quais adicionar o usuário.
- **Propriedades do Usuário:** Adicione propriedades de usuário opcionais. Para cada propriedade de usuário que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Propriedades do Usuário:** Na lista, clique em uma propriedade e, em seguida, digite o atributo da propriedade do usuário no campo ao lado da propriedade.
  - Clique em **Concluído** para salvar a propriedade do usuário ou clique em **Cancelar**.

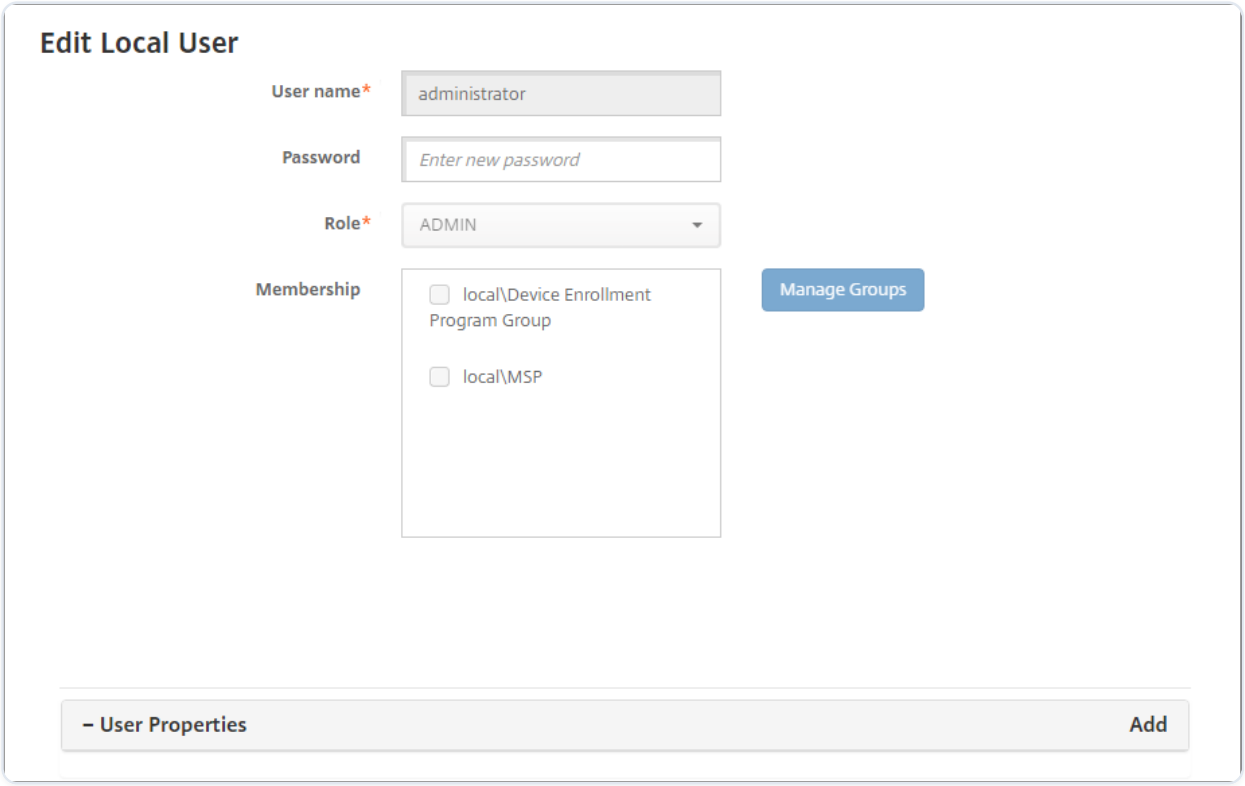
Para excluir uma propriedade de usuário existente, passe o mouse sobre a linha que contém a propriedade e, em seguida, clique no X no lado direito. A propriedade é excluída imediatamente.

Para editar uma propriedade de usuário existente, clique na propriedade e faça as alterações. Clique em **Concluído** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.

3. Clique em **Salvar**.

Para editar uma conta de usuário local

1. Na página **Usuários**, na lista de usuários, clique para selecionar um usuário e, em seguida, clique em **Editar**. A página **Editar Usuário Local** é exibida.



2. Altere as seguintes informações conforme apropriado:

   - **Nome de usuário:** Você não pode alterar o nome de usuário.
   - **Senha:** Altere ou adicione uma senha de usuário.
   - **Função:** Na lista, clique na função do usuário.
   - **Associação:** Na lista, clique no grupo ou grupos aos quais adicionar ou editar a conta de usuário. Para remover a conta de usuário de um grupo, desmarque a caixa de seleção ao lado do nome do grupo.
   - **Propriedades do usuário:** Faça um dos seguintes:
     - Para cada propriedade de usuário que você deseja alterar, clique na propriedade e faça as alterações. Clique em **Concluído** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.
     - Para cada propriedade de usuário que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
       - **Propriedades do Usuário:** Na lista, clique em uma propriedade e, em seguida, digite o atributo da propriedade do usuário no campo ao lado da propriedade.

    - Clique em **Concluído** para salvar a propriedade do usuário ou clique em **Cancelar**.
  - Para cada propriedade de usuário existente que você deseja excluir, passe o mouse sobre a linha que contém a propriedade e, em seguida, clique no **X** no lado direito. A propriedade é excluída imediatamente.

3. Clique em **Salvar** para salvar suas alterações ou clique em **Cancelar** para deixar o usuário inalterado.

Para desbloquear uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuário, clique para selecionar uma conta de usuário.
2. Clique em **Desbloquear Usuário Local**. Uma caixa de diálogo de confirmação é exibida.
3. Clique em **Desbloquear** para desbloquear a conta de usuário ou clique em **Cancelar** para deixar o usuário inalterado.

Para excluir uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuário, clique para selecionar uma conta de usuário.

Você pode selecionar mais de uma conta de usuário para excluir, marcando a caixa de seleção ao lado de cada conta de usuário.

1. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.
2. Clique em **Excluir** para excluir a conta de usuário ou clique em **Cancelar**.

Para excluir usuários do Active Directory

Para excluir um ou mais usuários do Active Directory por vez, selecione os usuários e clique em **Excluir**.

Se um usuário que você excluiu tiver dispositivos registrados e você quiser registrá-los novamente, exclua os dispositivos antes de registrá-los novamente. Para excluir um dispositivo, vá para **Gerenciar > Dispositivos**, selecione o dispositivo e clique em **Excluir**.

Importar contas de usuário

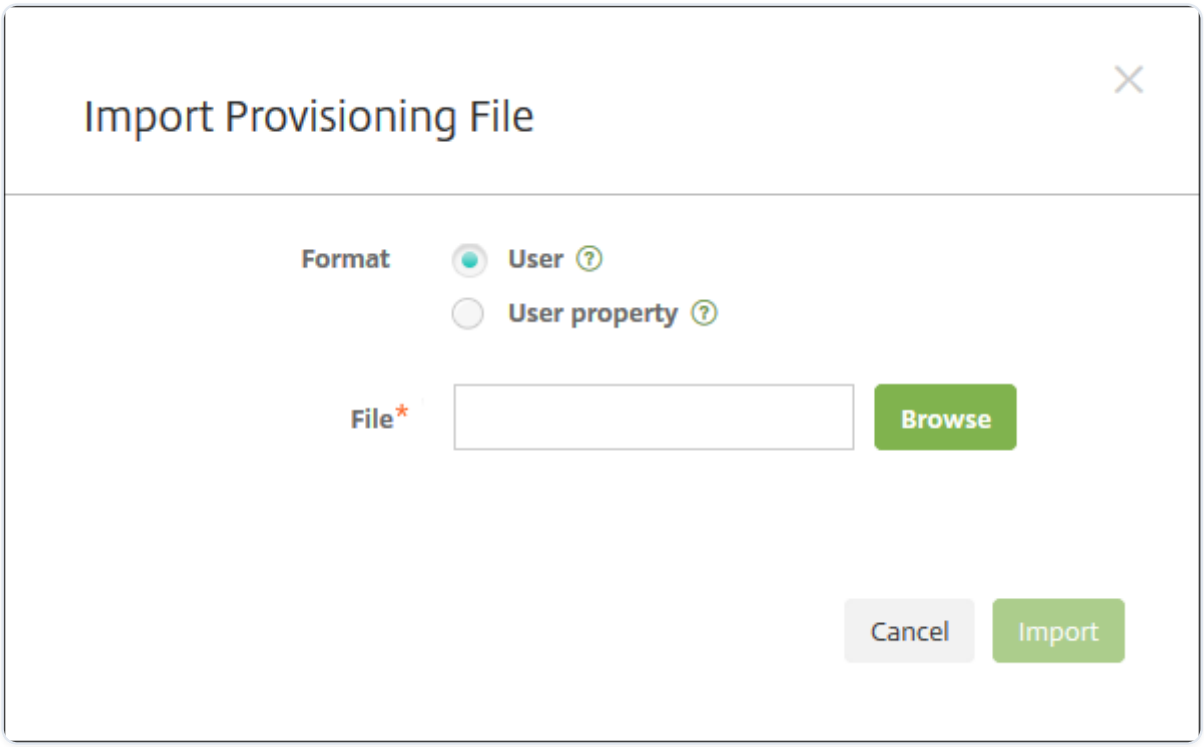
Você pode importar contas de usuário locais e propriedades de um arquivo .csv chamado arquivo de provisionamento, que você pode criar manualmente. Para obter mais informações sobre como formatar arquivos de provisionamento, consulte Formatos de arquivo de provisionamento.

Nota:

- Para usuários locais, use o nome de domínio junto com o nome de usuário no arquivo de importação. Por exemplo, especifique nome_de_usuário@domínio. Se o usuário local que você cria ou importa for para um domínio gerenciado no XenMobile, o usuário não poderá se registrar usando as credenciais LDAP correspondentes.
- Se estiver importando contas de usuário para o diretório de usuários interno do XenMobile, desative o domínio padrão para acelerar o processo de importação. Lembre-se de que a desativação do domínio afeta os registros, portanto, reative o domínio padrão após a conclusão da importação de usuários internos.
- Usuários locais podem estar no formato de Nome Principal de Usuário (UPN). No entanto, a Citrix recomenda que você não use o domínio gerenciado. Por exemplo, se example.com for gerenciado, não crie um usuário local com este formato UPN: user@example.com.

Depois de preparar um arquivo de provisionamento, siga estas etapas para importar o arquivo para o XenMobile.

1. No console do XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.
2. Clique em **Importar Usuários Locais**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.



3. Selecione **Usuário** ou **Propriedade** para o formato do arquivo de provisionamento que você está importando.
4. Selecione o arquivo de provisionamento a ser usado clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
5. Clique em **Importar**.

Formatos de arquivo de provisionamento

Você pode criar manualmente um arquivo de provisionamento para importar contas de usuário e propriedades para o XenMobile. Os formatos válidos são os seguintes:

- **Campos do arquivo de provisionamento de usuário:**
  `user;password;role;group1;group2`
- **Campos do arquivo de provisionamento de atributos de usuário:**
  `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

Observação:

- Separe os campos dentro do arquivo de provisionamento com um ponto e vírgula (;). Se parte de um campo contiver um ponto e vírgula, escape-o com um caractere de barra

invertida (\\). Por exemplo, digite a propriedade `propertyV;test;1;2` como `propertyV\\;test\\;1\\;2` no arquivo de provisionamento.

- Os valores válidos para **Função** são as funções predefinidas USER, ADMIN, SUPPORT e DEVICE_PROVISIONING, além de quaisquer outras funções que você tenha definido.
- Use o caractere de ponto (.) como separador para criar hierarquia de grupo. Não use um ponto em nomes de grupo.
- Use letras minúsculas para atributos de propriedade em arquivos de provisionamento de atributos. O banco de dados diferencia maiúsculas de minúsculas.

Exemplo de conteúdo de provisionamento de usuário

A entrada `user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` significa:

- **Usuário:** `user01`
- **Senha:** `pwd;01`
- **Função:** `USER`
- **Grupos:**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.users.users01`

Como outro exemplo, `AUser0;1.password;USER;ActiveDirectory.test.net` significa:

- **Usuário:** `AUser0`
- **Senha:** `1.password`
- **Função:** `USER`
- **Grupo:** `ActiveDirectory.test.net`

Exemplo de conteúdo de provisionamento de atributos de usuário

A entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

- **Usuário:** `user01`
- **Propriedade 1**

- **nome:** `propertyN`
- **valor:** `propertyV;test;1;2`

- **Propriedade 2:**
  - **nome:** `prop 2`
  - **valor:** `prop2 value`

Configurar modos de segurança de registro

Você configura um modo de segurança de registro de dispositivo para especificar um nível de segurança e um modelo de notificação para o registro de dispositivos no XenMobile.

O XenMobile oferece sete modos de segurança de registro, cada um com seu próprio nível de segurança e etapas que os usuários devem seguir para registrar seus dispositivos. Você configura os modos de segurança de registro no console do XenMobile Server na página **Configurações > Registro**.

Você pode disponibilizar alguns modos no Portal de Autoatendimento. No portal, os usuários geram links de registro que lhes permitem registrar seus dispositivos. Usuários de iOS, iPadOS, macOS, Android Enterprise e Android legado podem optar por enviar a si mesmos um convite de registro do portal. Convites de registro não estão disponíveis para dispositivos Windows.

Você envia convites de registro na página **Gerenciar > Convites de Registro**. Para obter informações, consulte Enviar um convite de registro.

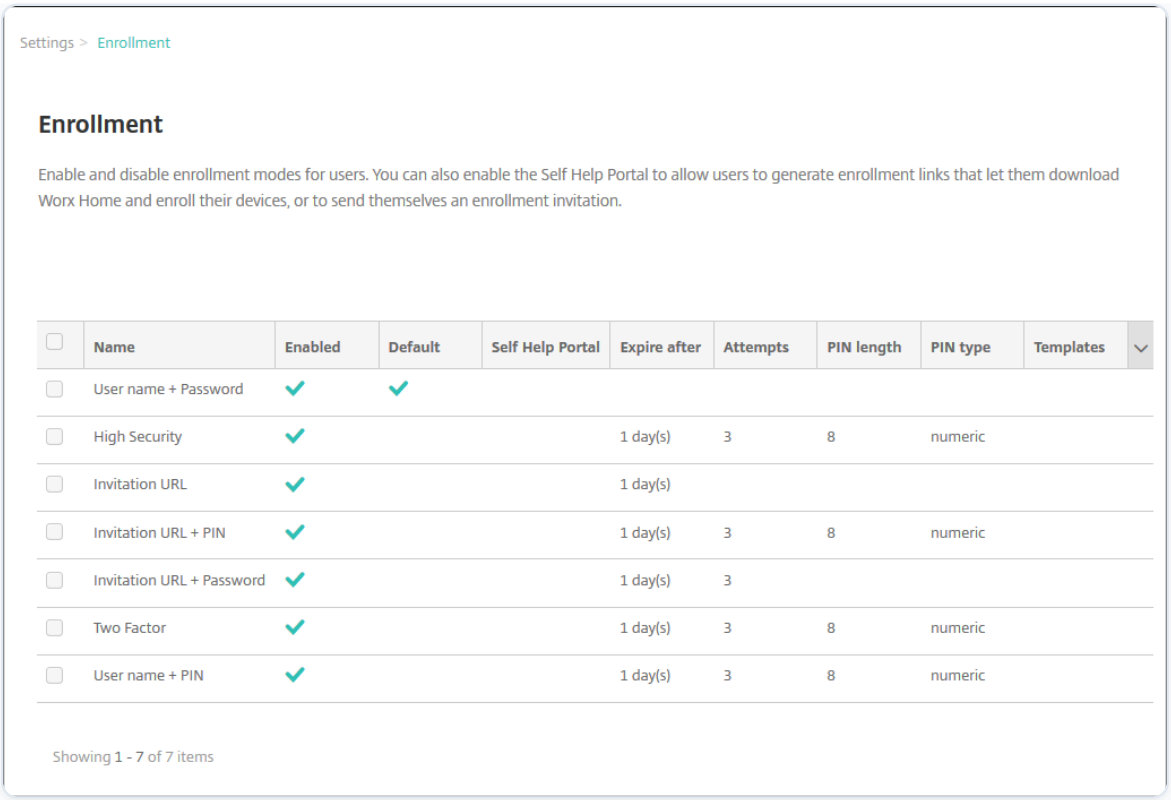
> **Nota:**
>
> Se você planeja usar modelos de notificação personalizados, deve configurar os modelos antes de configurar os modos de segurança de registro. Para obter mais informações sobre modelos de notificação, consulte Criar ou Atualizar Modelos de Notificação.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Registro**. A página **Registro** é exibida, contendo uma tabela de todos os modos de segurança de registro disponíveis. Por padrão, todos os modos de segurança de registro estão habilitados.

3. Selecione qualquer modo de segurança de inscrição na lista para editá-lo. Em seguida, defina o modo como padrão, desative o modo ou permita que os usuários acessem através do Portal de Autoatendimento.

Nota:

Quando você seleciona a caixa de seleção ao lado de um modo de segurança de inscrição, o menu de opções aparece acima da lista de modos de segurança de inscrição. Quando você clica em qualquer outro lugar da lista, o menu de opções aparece no lado direito da listagem.



Escolha entre estes modos de segurança de inscrição:

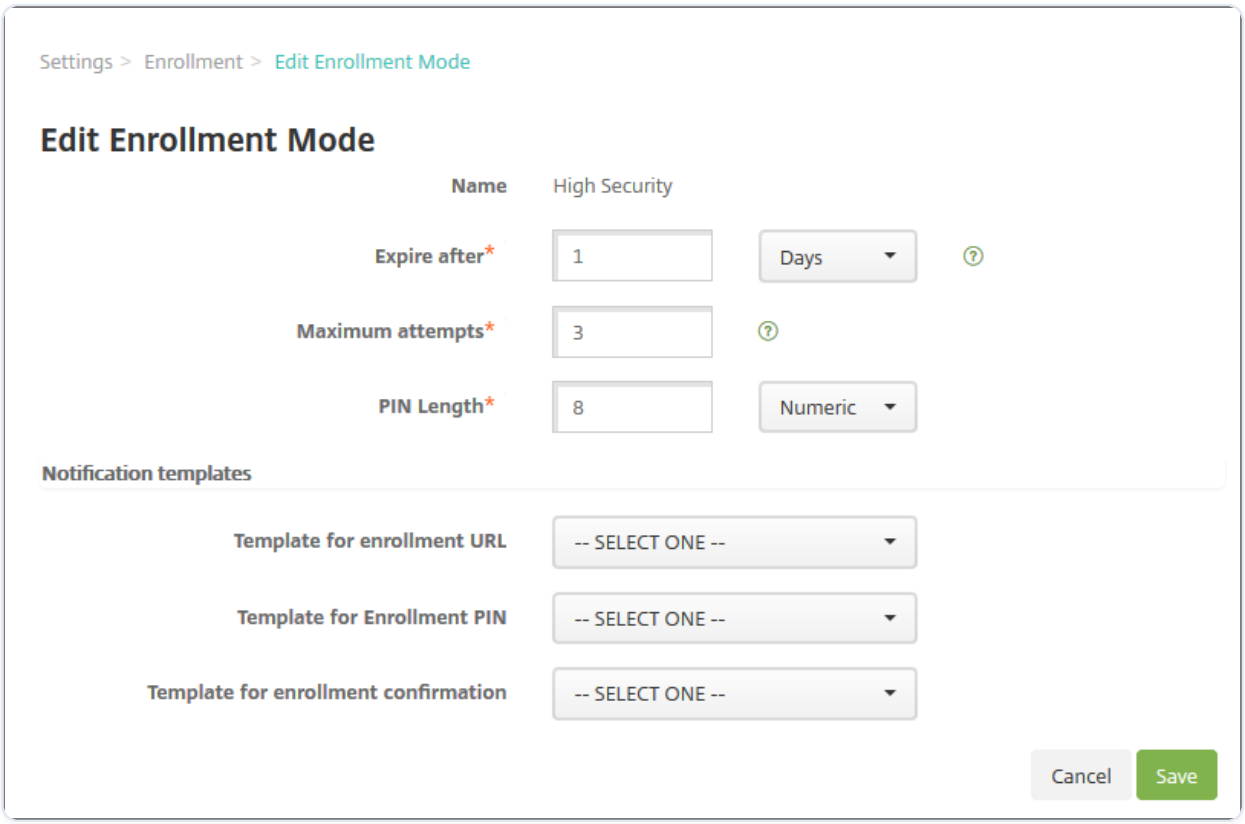
- Nome de usuário + Senha
- Alta Segurança
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Autenticação de dois fatores
- Nome de usuário + PIN

Você pode usar convites de inscrição para restringir a inscrição apenas a usuários com um convite. Para enviar convites de inscrição, você só pode usar os modos de segurança de inscrição **URL de Convite**, **URL de Convite + PIN** ou **URL de Convite + Senha**. Para dispositivos que se inscrevem com **Nome de usuário + Senha**, **Autenticação de dois fatores** ou **Nome de usuário + PIN**, os usuários devem inserir manualmente suas credenciais no Secure Hub.

Você pode usar convites de inscrição de PIN único (OTP) como uma solução de autenticação de dois fatores. Os convites de inscrição OTP controlam o número de dispositivos que um usuário pode inscrever. Os convites OTP não estão disponíveis para dispositivos Windows.

Para editar um modo de segurança de inscrição

1. Na lista **Inscrição**, selecione um modo de segurança de inscrição e clique em **Editar**. A página **Editar Modo de Inscrição** é exibida. O modo selecionado determina as opções exibidas.



2. Altere as seguintes informações conforme apropriado:

   - **Expirar após:** Digite um prazo de expiração após o qual os usuários não poderão inscrever seus dispositivos. Esse valor aparece nas páginas de configuração de convite de inscrição de usuário e grupo.

     Digite **0** para evitar que o convite expire.

- **Dias:** Na lista, clique em **Dias** ou **Horas** para corresponder ao prazo de expiração que você inseriu em **Expirar após**.
- **Tentativas máximas:** Digite o número de tentativas de inscrição que um usuário pode fazer antes de ser bloqueado do processo de inscrição. Esse valor aparece nas páginas de configuração de convite de inscrição de usuário e grupo.

  Digite **0** para permitir tentativas ilimitadas.
- **Comprimento do PIN:** Digite um número para definir o comprimento do PIN gerado.
- **Numérico:** Na lista, clique em **Numérico** ou **Alfanumérico** para o tipo de PIN.
- **Modelos de notificação:**
  - **Modelo para URL de inscrição:** Na lista, clique em um modelo para usar para a URL de inscrição. Por exemplo, o modelo de convite de inscrição envia aos usuários um e-mail ou SMS. O método depende de como você configurou o modelo que permite que eles inscrevam seus dispositivos no XenMobile. Para obter mais informações sobre modelos de notificação, consulte Criação ou atualização de modelos de notificação.
  - **Modelo para PIN de inscrição:** Na lista, clique em um modelo para usar para o PIN de inscrição.
  - **Modelo para confirmação de inscrição:** Na lista, clique em um modelo para usar para informar um usuário de que ele se inscreveu com sucesso.

3. Clique em **Salvar**.

Para definir um modo de segurança de inscrição como padrão

Quando você define um modo de segurança de inscrição como padrão, o modo é usado para todas as solicitações de inscrição de dispositivo, a menos que você selecione um modo de segurança de inscrição diferente. Se nenhum modo de segurança de inscrição for definido como padrão, você deverá criar uma solicitação de inscrição para cada inscrição de dispositivo.

> **Nota:**
>
> Os únicos modos de segurança de inscrição que você pode usar como padrão são **Somente Nome de usuário + Senha**, **Dois Fatores** ou **Nome de usuário + PIN**.

1. Selecione o modo de segurança de inscrição padrão, seja **Nome de usuário + Senha**, **Dois Fatores** ou **Nome de usuário + PIN**.

Para usar um modo como padrão, primeiro habilite-o.

2. Clique em **Padrão**. O modo selecionado agora é o padrão. Se qualquer outro modo de segurança de inscrição foi definido como padrão, o modo não é mais o padrão.

Para desabilitar um modo de segurança de inscrição

Desabilitar um modo de segurança de inscrição o torna indisponível para uso, tanto para convites de inscrição em grupo quanto no Portal de Autoatendimento. Você pode alterar como os usuários podem inscrever seus dispositivos desabilitando um modo de segurança de inscrição e habilitando outro.

1. Selecione um modo de segurança de inscrição.

   Você não pode desabilitar o modo de segurança de inscrição padrão. Se você deseja desabilitar o modo de segurança de inscrição padrão, deve primeiro remover seu status padrão.

2. Clique em **Desabilitar**. O modo de segurança de inscrição não está mais habilitado.

Para habilitar um modo de segurança de inscrição no Portal de Autoatendimento

Habilitar um modo de segurança de inscrição no Portal de Autoatendimento permite que os usuários inscrevam seus dispositivos no XenMobile individualmente.

Nota:

- O modo de segurança de registro deve ser habilitado e vinculado a modelos de notificação para ser disponibilizado no Portal de Autoatendimento.
- Você só pode habilitar um modo de segurança de registro no Portal de Autoatendimento por vez.

1. Selecione um modo de segurança de registro.
2. Clique em **Portal de Autoatendimento**. O modo de segurança de registro que você selecionou agora está disponível para os usuários no Portal de Autoatendimento. Qualquer modo já habilitado no Portal de Autoatendimento não está mais disponível para os usuários.

Adicionar ou remover grupos

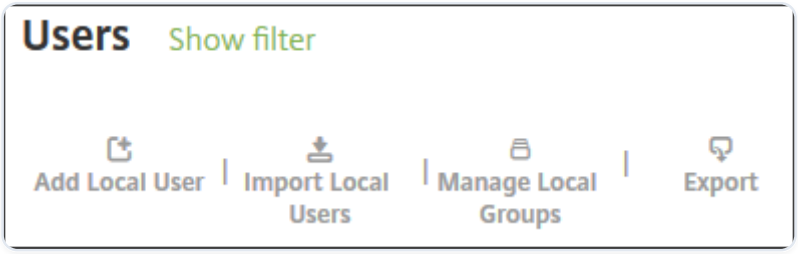
Você gerencia grupos na caixa de diálogo **Gerenciar Grupos** no console do XenMobile nestas páginas: **Usuários**, **Adicionar Usuário Local** ou **Editar Usuário Local**. Não há comando de edição de grupo.

Se você remover um grupo, lembre-se de que a remoção do grupo não tem efeito nas contas de usuário. A remoção de um grupo simplesmente remove a associação do usuário a esse grupo. Os usuários também perdem o acesso a aplicativos ou perfis fornecidos pelos Grupos de Entrega associados a esse grupo; quaisquer outras associações de grupo, no entanto, permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles serão associados no nível superior.

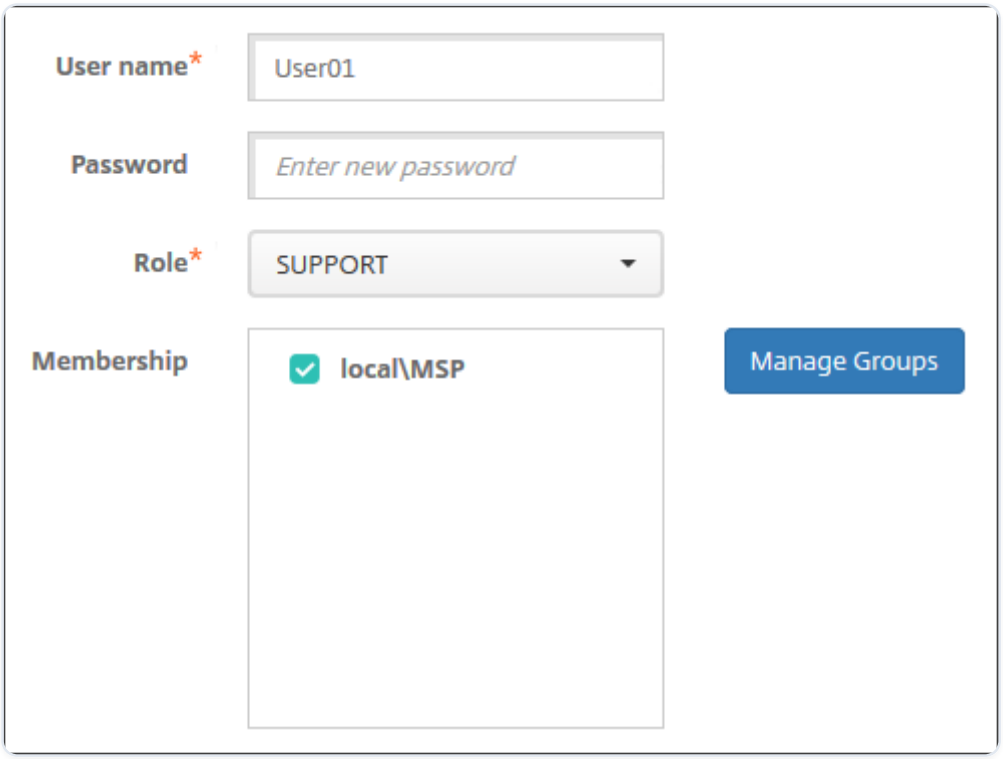
Para adicionar um grupo local

1. Faça um dos seguintes:

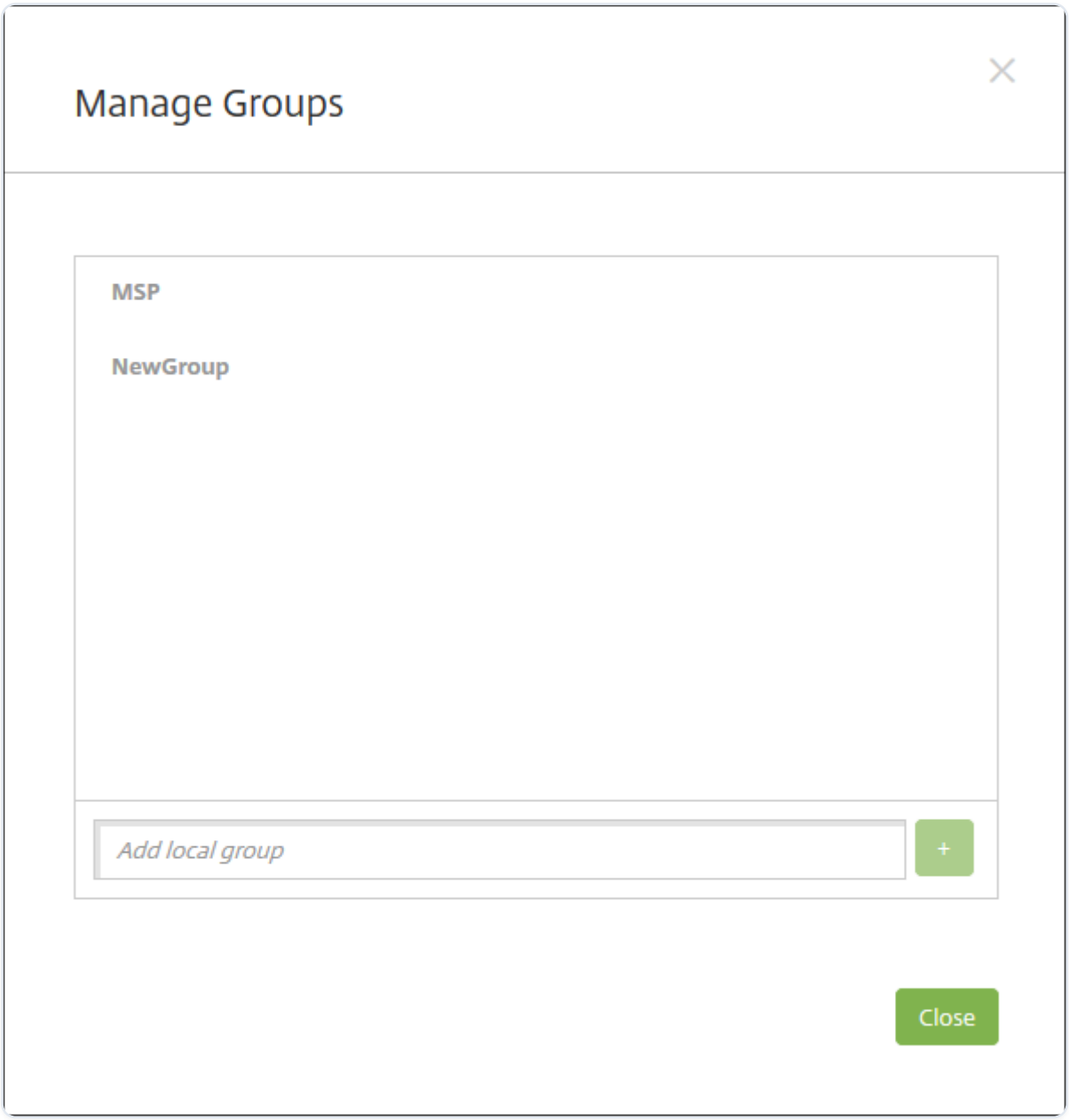
   - Na página **Usuários**, clique em **Gerenciar Grupos Locais**.



   - Na página **Adicionar Usuário Local** ou na página **Editar Usuário Local**, clique em **Gerenciar Grupos**.



A caixa de diálogo **Gerenciar Grupo** é exibida.



2. Abaixo da lista de grupos, digite um novo nome de grupo e clique no sinal de mais (**+**). O grupo de usuários é adicionado à lista.
3. Clique em **Fechar**.

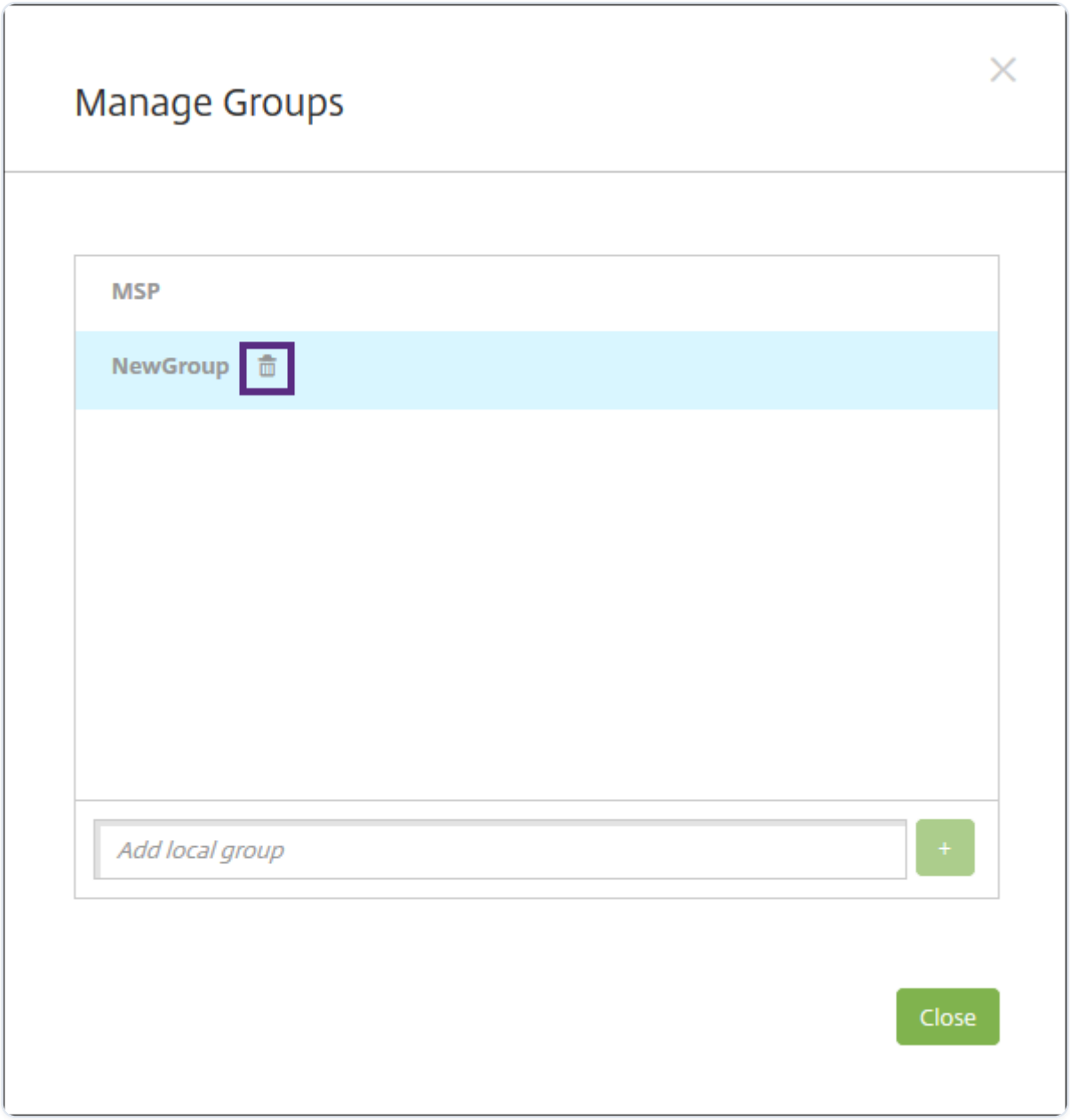
Para remover um grupo

A remoção de um grupo não afeta as contas de usuário. A remoção de um grupo simplesmente remove a associação do usuário com esse grupo. Os usuários também perdem o acesso a aplicativos ou perfis fornecidos pelos Grupos de Entrega associados a esse grupo. No entanto, quaisquer outras associações de grupo permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles serão associados no nível superior.

1. Faça um dos seguintes:

- Na página **Usuários**, clique em **Gerenciar Grupos Locais**.
- Na página **Adicionar Usuário Local** ou na página **Editar Usuário Local**, clique em **Gerenciar Grupos**.

A caixa de diálogo **Gerenciar Grupos** é exibida.



2. Na caixa de diálogo **Gerenciar Grupos**, clique no grupo que você deseja excluir.
3. Clique no ícone da lixeira à direita do nome do grupo. Uma caixa de diálogo de confirmação é exibida.
4. Clique em **Excluir** para confirmar a operação e remover o grupo.

> **Importante:**

> Você não pode desfazer esta operação.

5. Na caixa de diálogo **Gerenciar Grupos**, clique em **Fechar**.

Criar e gerenciar fluxos de trabalho

Você pode usar fluxos de trabalho para gerenciar a criação e remoção de contas de usuário. Antes de usar um fluxo de trabalho, identifique as pessoas em sua organização que têm autoridade para aprovar solicitações de contas de usuário. Em seguida, você pode usar o modelo de fluxo de trabalho para criar e aprovar solicitações de contas de usuário.

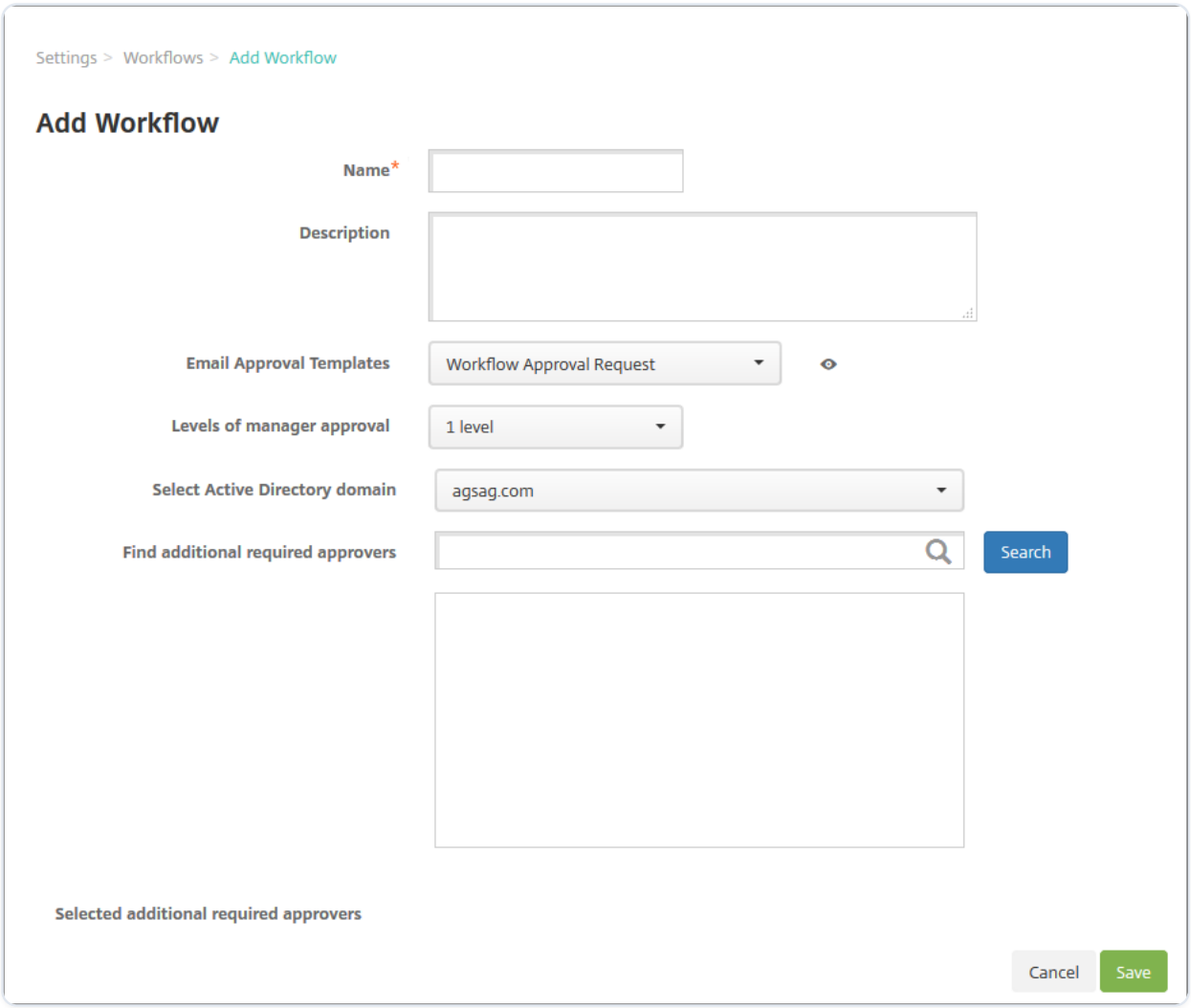
Ao configurar o XenMobile pela primeira vez, você define as configurações de e-mail do fluxo de trabalho, que devem ser definidas antes de você poder usar os fluxos de trabalho. Você pode alterar as configurações de e-mail do fluxo de trabalho a qualquer momento. Essas configurações incluem o servidor de e-mail, a porta, o endereço de e-mail e se a solicitação para criar a conta de usuário requer aprovação.

Você pode configurar fluxos de trabalho em dois locais no XenMobile:

- Na página **Fluxos de Trabalho** no console do XenMobile. Na página **Fluxos de Trabalho**, você pode configurar vários fluxos de trabalho para uso com configurações de aplicativos. Ao configurar fluxos de trabalho na página Fluxos de Trabalho, você pode selecionar o fluxo de trabalho ao configurar o aplicativo.
- Ao configurar um conector de aplicativo no aplicativo, você fornece um nome de fluxo de trabalho e, em seguida, configura os indivíduos que podem aprovar a solicitação de conta de usuário. Consulte Adicionar Aplicativos ao XenMobile.

Você pode atribuir até três níveis para aprovação de contas de usuário pelo gerente. Se você precisar que outras pessoas aprovem a conta de usuário, poderá pesquisá-las e selecioná-las usando o nome ou o endereço de e-mail. Quando o XenMobile encontra a pessoa, você a adiciona ao fluxo de trabalho. Todos os indivíduos no fluxo de trabalho recebem e-mails para aprovar ou negar a nova conta de usuário.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Fluxos de Trabalho**. A página **Fluxos de Trabalho** é exibida.
3. Clique em **Adicionar**. A página **Adicionar Fluxo de Trabalho** é exibida.



4. Configure estas configurações:

- **Nome:** Digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** Opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de Aprovação de E-mail:** Na lista, selecione o modelo de aprovação de e-mail a ser atribuído. Você cria modelos de e-mail na seção **Modelos de Notificação** em **Configurações** no console do XenMobile. Ao clicar no ícone de olho à direita deste campo, você verá uma prévia do modelo que está configurando.
- **Níveis de aprovação do gerente:** Na lista, selecione o número de níveis de aprovação do gerente necessários para este fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
  - Não Necessário
  - 1 nível
  - 2 níveis
  - 3 níveis

- **Selecionar domínio do Active Directory:** Na lista, selecione o domínio do Active Directory apropriado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores adicionais necessários:** Digite um nome no campo de pesquisa e clique em **Pesquisar**. Os nomes são originados no Active Directory.
- Quando o nome aparecer no campo, selecione a caixa de seleção ao lado do nome. O nome e o endereço de e-mail aparecem na lista **Aprovadores adicionais necessários selecionados**.
    - Para remover um nome da lista, faça o seguinte:
        - Clique em **Pesquisar** para ver uma lista de todos no domínio selecionado.
        - Digite um nome completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar os resultados da pesquisa.
        - As pessoas na lista **Aprovadores adicionais necessários selecionados** têm marcas de seleção ao lado de seus nomes na lista de resultados da pesquisa. Role a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

5. Clique em **Salvar**. O fluxo de trabalho criado aparece na página **Fluxos de trabalho**.

Depois de criar o fluxo de trabalho, você pode visualizar seus detalhes, os aplicativos associados a ele ou excluí-lo. Você não pode editar um fluxo de trabalho depois de criá-lo. Se precisar de um com diferentes níveis de aprovação ou aprovadores, crie outro.

Para visualizar detalhes e excluir um fluxo de trabalho

1. Na página **Fluxos de trabalho**, na lista de fluxos de trabalho existentes, selecione um fluxo de trabalho específico. Para fazer isso, clique na linha da tabela ou selecione a caixa de seleção ao lado do fluxo de trabalho.
2. Para excluir um fluxo de trabalho, clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

> **Importante:**
>
> Não é possível desfazer esta operação.

Perfis de registro

Um perfil de registro especifica o seguinte:

- Opções de registro de gerenciamento de dispositivos para dispositivos Android e iOS. Para Android, as opções de registro disponíveis para o modo de servidor MDM+MAM (ENT) diferem das opções para o modo MDM.
- Opções de registro de gerenciamento de aplicativos para dispositivos Android e iOS.
- Outras opções de registro:
  - Se deve limitar o número de dispositivos que um usuário pode registrar.

    Se o limite de dispositivos for atingido, uma mensagem de erro informa ao usuário que ele excedeu o limite de registro de dispositivos.
  - Se deve permitir que um usuário recuse o gerenciamento de dispositivos.

Você pode usar perfis de registro para combinar vários casos de uso e caminhos de migração de dispositivos em um único console do XenMobile® Server. Alguns casos de uso incluem:

- Gerenciamento de Dispositivos Móveis (somente MDM)
- MDM+Gerenciamento de Aplicativos Móveis (MAM)
- Somente MAM
- Registros de propriedade corporativa
- Registro BYOD (a capacidade de optar por não participar do registro MDM)
- Migração de registros do Administrador de Dispositivos Android para registros do Android Enterprise (totalmente gerenciado, perfil de trabalho, dispositivo dedicado)

Ao criar um grupo de entrega, você pode usar o perfil de inscrição padrão chamado Global ou especificar um perfil de inscrição diferente.

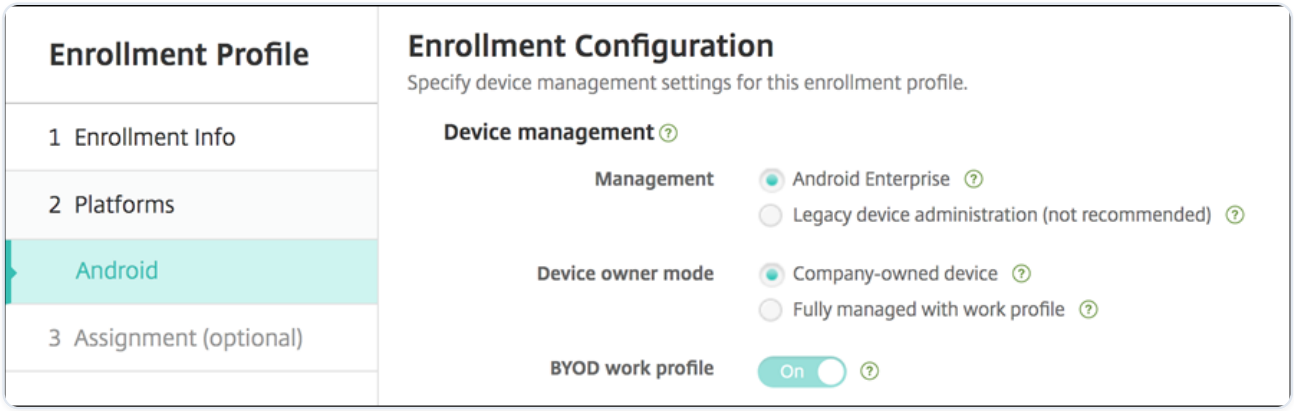
Os recursos do perfil de inscrição por plataforma incluem o seguinte.

- **Para dispositivos Android:** Você especifica o modo de proprietário do dispositivo. Por exemplo: Totalmente gerenciado, totalmente gerenciado com perfil de trabalho e perfil de trabalho BYOD. A opção **Dispositivo dedicado** aparece somente quando você tem uma licença Enterprise ou Advanced para XenMobile. Novos dispositivos são inscritos no Android Enterprise e no gerenciamento de aplicativos por padrão. Os modos de segurança de inscrição **Nome de usuário + PIN**, **URL de convite**, **URL de convite + PIN** e **URL de convite + Senha** não estão disponíveis para Android Enterprise.

- **Para dispositivos iOS:** Você especifica o tipo de inscrição do dispositivo: Inscrição de dispositivo ou não gerenciar dispositivos. As configurações do iOS aparecem somente quando você tem uma licença Enterprise ou Advanced para XenMobile. Novos dispositivos são inscritos no gerenciamento de dispositivos Apple e no gerenciamento de aplicativos por padrão.

Se você não precisar inscrever dispositivos dedicados para dispositivos Android ou inscrição somente MAM para dispositivos Android ou iOS, poderá desabilitar a propriedade do servidor `enable.multimode.xms`. No entanto, manter essa propriedade habilitada significa que você precisa de apenas um XenMobile Server para manipular todos os tipos de perfis de inscrição. Consulte Propriedades do servidor.

Ao desabilitar `enable.multimode.xms`, somente as configurações nesta captura de tela estarão disponíveis:

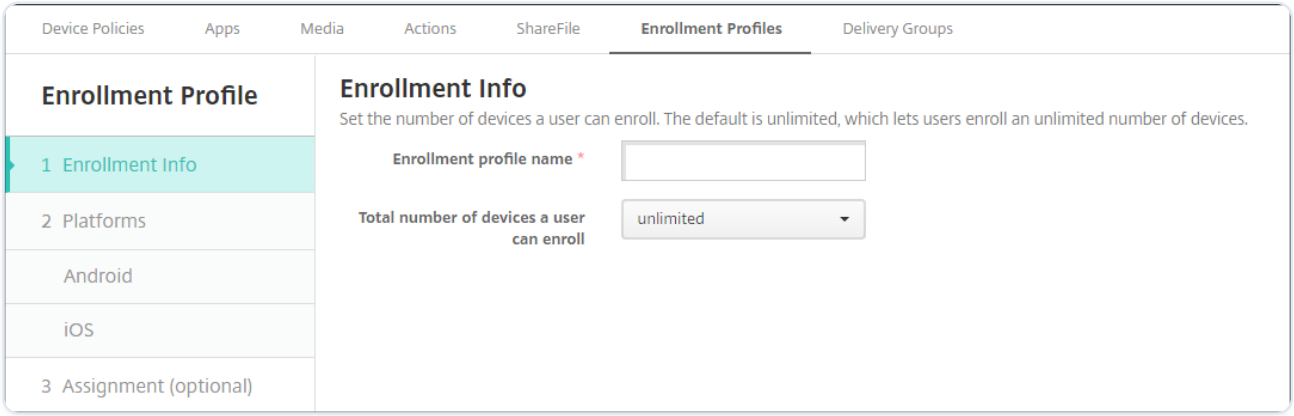


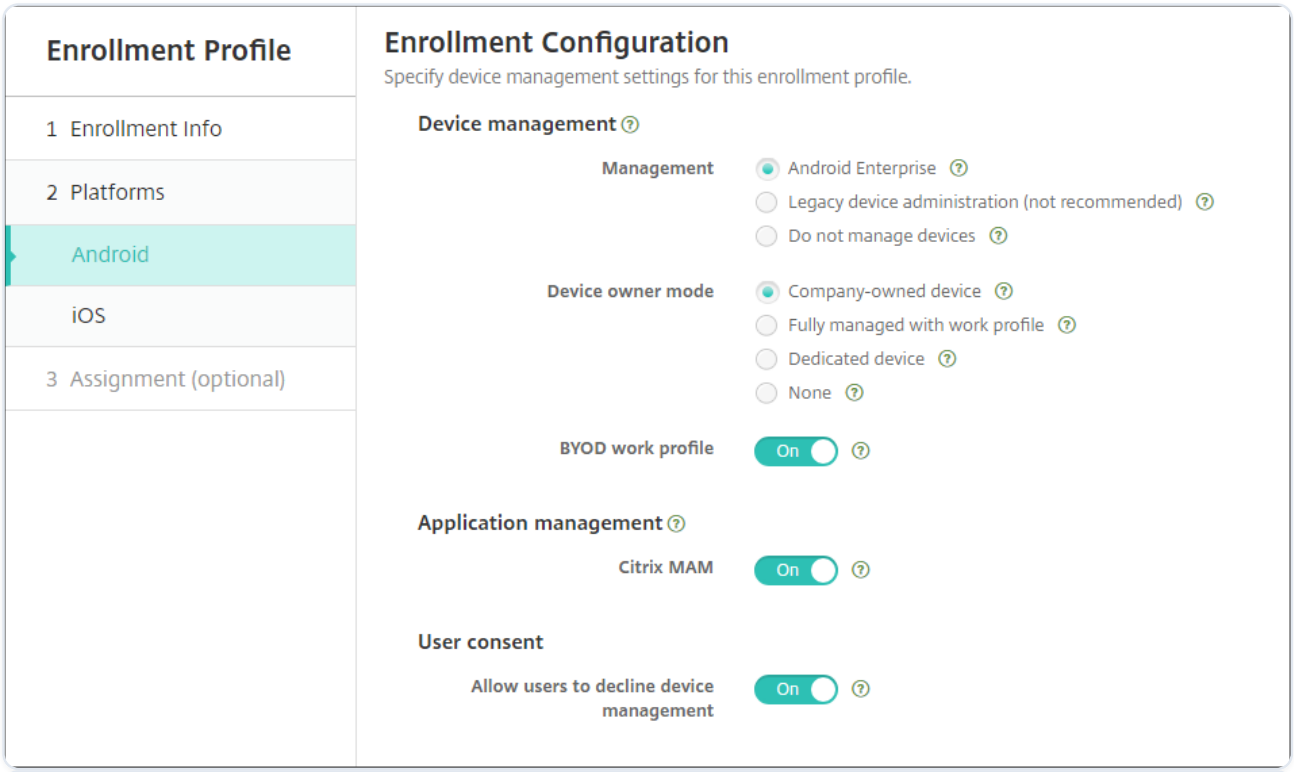
Para obter mais detalhes sobre essas configurações, consulte Android Enterprise.

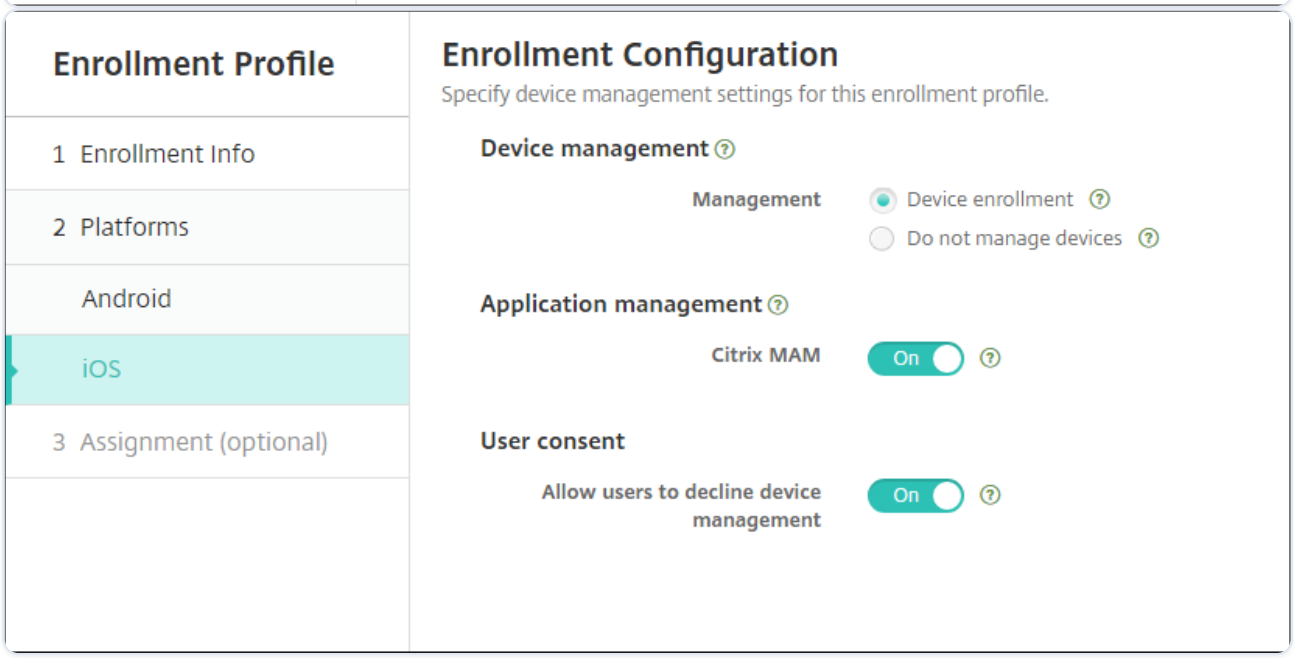
Perfil de inscrição global

O perfil de inscrição padrão é chamado Global. O perfil Global é útil para testes até que você tenha a chance de criar perfis de inscrição.

As capturas de tela a seguir mostram as configurações padrão para o perfil de inscrição Global.







Perfis de inscrição, grupos de entrega e inscrição

Os perfis de inscrição e os grupos de entrega interagem da seguinte forma:

- Você pode anexar um perfil de inscrição a um ou mais grupos de entrega.
- Se um usuário pertencer a vários grupos de entrega que têm perfis de inscrição diferentes, o nome do grupo de entrega determina o perfil de inscrição usado. O XenMobile Server seleciona o grupo de entrega que aparece por último em uma lista alfabetizada de grupos de entrega. Por exemplo, suponha que você tenha o seguinte:

- Dois perfis de inscrição, chamados "EP1" e "EP2".
- Dois grupos de entrega, chamados "DG1" e "DG2".
- "DG1" está associado a "EP1".
- "DG2" está associado a "EP2".

Se o usuário que está se inscrevendo estiver nos grupos de entrega "DG1" e "DG2", o XenMobile Server usará o perfil de inscrição "EP2" para determinar o tipo de inscrição para o usuário.

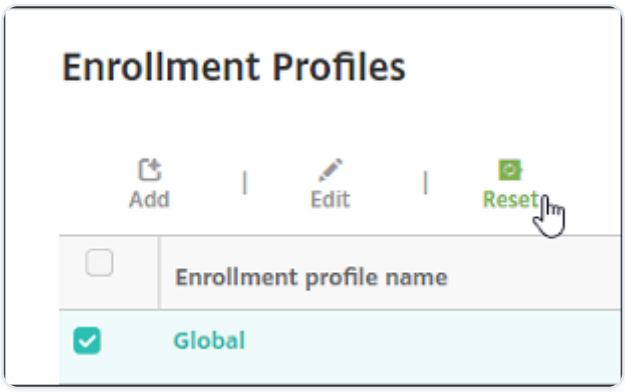
- A ordem de implantação se aplica apenas a dispositivos em um grupo de entrega que tenha um perfil de inscrição configurado para MDM (gerenciamento de dispositivos).
- Depois que um dispositivo é inscrito, algumas alterações em um perfil de inscrição exigem uma nova inscrição:
  - Adicionar MAM a um perfil de inscrição configurado para MDM.
  - Mover um dispositivo inscrito no MDM para um grupo de entrega configurado para MDM+MAM. Essa alteração afeta apenas as novas inscrições de dispositivos. As inscrições de dispositivos existentes não são afetadas.
  - Adicionar MDM a um perfil de inscrição configurado para MAM.
- Mudar para um perfil de inscrição diferente não afeta os dispositivos inscritos existentes. No entanto, os usuários devem cancelar a inscrição e, em seguida, reinscrever esses dispositivos para que as alterações entrem em vigor.

Para criar um perfil de inscrição

1. No console do XenMobile Server, vá para **Configurar > Perfis de Registro**.
2. Na página **Informações de Registro**, digite um nome descritivo para o perfil. Por padrão, um usuário pode registrar um número ilimitado de dispositivos. Selecione um valor para limitar o número de dispositivos por usuário. O limite se aplica à soma de dispositivos Android e iOS gerenciados por MAM ou MDM que um usuário registra.
3. Preencha as páginas da plataforma. Para obter informações sobre as configurações de registro específicas das plataformas, consulte:
   - Android Enterprise
   - iOS: Métodos de registro compatíveis
4. Na página **Atribuição**, anexe um ou mais grupos de entrega ao perfil de registro.

> Um usuário pode pertencer a vários grupos de entrega que têm perfis de registro diferentes. Nesse caso, o nome do grupo de entrega determina o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabetizada de grupos de entrega. Para criar grupos de entrega, vá para **Configurar > Grupos de Entrega**.

Uma lista dos seus perfis de registro aparece na página **Configurar > Perfis de Registro**. Para editar o perfil Global ou redefini-lo para o padrão original, selecione a linha do perfil Global e clique em **Redefinir**. Você não pode excluir o perfil Global.



Configurar funções com RBAC

Cada função de controle de acesso baseado em função (RBAC) predefinida tem certas permissões de acesso e recursos associadas. Este artigo descreve o que cada uma dessas permissões faz. Para uma lista completa das permissões padrão para cada função integrada, baixe Padrões de Controle de Acesso Baseado em Função.

Ao *aplicar permissões*, você está definindo os grupos de usuários que a função RBAC tem permissão para gerenciar. O administrador padrão não pode alterar as configurações de permissão aplicadas. Por padrão, as permissões aplicadas se aplicam a todos os grupos de usuários.

Ao fazer uma *atribuição*, você está atribuindo a função RBAC a um grupo, para que o grupo de usuários possua os direitos de administrador RBAC.

> **Importante:**

> Na permissão Configurações, a permissão RBAC concede aos usuários Administradores acesso total, incluindo a capacidade de atribuir suas próprias permissões. Conceda este acesso apenas aos usuários a quem você pretende dar a capacidade de manipular tudo no sistema Endpoint Management.

> Este artigo possui as seguintes seções:

- Função de Administrador
- Função de Suporte
- Função de Usuário
- Configurar funções com RBAC

Função de Administrador

Usuários com a função de Administrador predefinida têm acesso ou não têm acesso aos seguintes recursos no XenMobile. Por padrão, **Acesso autorizado** (exceto Portal de Autoatendimento), **Recursos do console** e **Aplicar permissões** estão ativados.

Acesso autorizado

Acesso ao console de administração	Os administradores têm acesso a todos os recursos no console do XenMobile.
Acesso ao Portal de Autoatendimento	Os administradores não têm acesso ao Portal de Autoatendimento.
Registrador de dispositivos compartilhados	Os administradores não têm acesso ao registrador de dispositivos compartilhados. Este recurso é destinado a usuários que precisam registrar dispositivos compartilhados.
Acesso ao Suporte Remoto	Os administradores possuem acesso ao Suporte Remoto.*
Acesso à API Pública	Os administradores têm acesso à API pública para realizar ações programaticamente que estão disponíveis no console do XenMobile. As ações incluem a administração de certificados, aplicativos, dispositivos, grupos de entrega e usuários locais.
Registrador de dispositivos COSU	Fornece uma maneira para os administradores registrarem dispositivos Android Enterprise dedicados (também conhecidos como dispositivos COSU) se essa capacidade não

	estiver configurada usando um perfil de registro.

* O suporte remoto permite que seus representantes de help desk assumam o controle remoto de dispositivos móveis Android gerenciados. A transmissão de tela é suportada apenas em dispositivos Samsung Knox. O suporte remoto não está disponível para implantações de servidor XenMobile on-premises em cluster. O Suporte Remoto não está mais disponível para novos clientes a partir de January 1, 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornece aprimoramentos ou correções.

Recursos do console

Os administradores têm acesso irrestrito ao console do XenMobile.

Painel	O **Painel** é a primeira página que os administradores veem após fazer login no console do XenMobile. O **Painel** mostra informações básicas sobre notificações e dispositivos.	
Relatórios	A página **Analisar > Relatórios** fornece relatórios predefinidos que permitem analisar suas implantações de aplicativos e dispositivos.	
Dispositivos	A página **Gerenciar > Dispositivos** é onde você gerencia os dispositivos dos usuários. Você pode adicionar dispositivos individuais na página ou importar um arquivo de provisionamento de dispositivo para adicionar vários dispositivos de uma só vez.	

Usuários e Grupos Locais	A página **Gerenciar > Usuários** é onde você pode adicionar, editar ou excluir usuários locais e grupos de usuários locais.	
Registro	A página **Gerenciar > Convites de Registro** é onde você gerencia como os usuários são convidados a registrar seus dispositivos no XenMobile.	
Políticas	A página **Configurar > Políticas de Dispositivo** é onde você gerencia políticas de dispositivo, como VPN e Wi-Fi.	
Aplicativos	A página **Configurar > Aplicativos** é onde você gerencia os vários aplicativos que os usuários podem instalar em seus dispositivos.	
Mídia	A página **Configurar > Mídia** é onde você gerencia as várias mídias que os usuários podem instalar em seus dispositivos.	
Ação	A página **Configurar > Ações** é onde você gerencia as respostas para acionar eventos.	
Perfis de Inscrição	A página **Configurar > Perfis de Inscrição** é onde você configura perfis de inscrição (modos) para permitir que os usuários inscrevam seus dispositivos.	

Grupos de Entrega	A página **Configurar > Grupos de Entrega** é onde você gerencia grupos de entrega e os recursos associados a eles.	
Configurações	A página **Configurações** é onde você gerencia as configurações do sistema, como propriedades de cliente e servidor, certificados e provedores de credenciais. **Importante:** Essas configurações incluem a permissão RBAC. A permissão RBAC concede aos administradores acesso total, incluindo a capacidade de atribuir suas próprias permissões. Conceda este acesso apenas aos usuários aos quais você pretende dar a capacidade de manipular tudo no sistema Endpoint Management.	
Suporte	A página **Solução de Problemas e Suporte** é onde você realiza atividades de solução de problemas, como executar diagnósticos e gerar logs.	

Dispositivos

Os administradores acessam os recursos do dispositivo em todo o console definindo restrições de dispositivo, configurando e enviando notificações para dispositivos, administrando aplicativos nos dispositivos e assim por diante.

Limpeza completa do dispositivo	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, se o dispositivo tiver um.
Limpar Restrição	Remover uma ou mais restrições de dispositivo.
Limpeza Seletiva do dispositivo	Apagar todos os dados e aplicativos corporativos de um dispositivo, deixando os dados e aplicativos pessoais no lugar.
Visualizar localizações	Ver a localização e definir restrições geográficas em um dispositivo. Inclui: Localizar dispositivo, Ver a localização de um dispositivo, Rastrear dispositivo, Rastrear a localização de um dispositivo ao longo do tempo.
Bloquear dispositivo	Bloquear remotamente um dispositivo para que os usuários não possam usá-lo.
Desbloquear dispositivo	Desbloquear remotamente um dispositivo para que os usuários possam usá-lo.
Bloquear contêiner	Bloquear remotamente o contêiner corporativo em um dispositivo.
Desbloquear contêiner	Desbloquear remotamente o contêiner corporativo em um dispositivo.
Redefinir senha do contêiner	Redefinir a senha do contêiner corporativo.
Ativar bloqueio de ativação ASM DEP/Bypass	Armazene um código de bypass em um dispositivo iOS supervisionado quando o Bloqueio de Ativação estiver ativado. Se precisar apagar o dispositivo, use este código para limpar o Bloqueio de Ativação automaticamente.
Toca o dispositivo	Toca remotamente um dispositivo Windows no volume máximo por 5 minutos.

Reiniciar o dispositivo	Reinicia dispositivos Windows a partir do console do XenMobile.
Implantar no dispositivo	Envie aplicativos, notificações, restrições e assim por diante para um dispositivo.
Editar dispositivo	Altere as configurações no dispositivo.
Notificação para o dispositivo	Envie uma notificação para um dispositivo.
Adicionar/Excluir dispositivo	Adicione ou remova dispositivos do XenMobile.
Importação de dispositivos	Importar um grupo de dispositivos de um arquivo para o XenMobile.
Exportar tabela de dispositivos	Coletar informações do dispositivo na página Dispositivo e exportá-las para um arquivo .csv.
Revogar dispositivo	Proibir que um dispositivo se conecte ao XenMobile.
Bloqueio de app	Negar acesso a todos os aplicativos em um dispositivo. No Android, os usuários não podem fazer login no XenMobile. No iOS, os usuários podem fazer login, mas não podem acessar os aplicativos.
Limpeza de app	No Android, esta ação exclui a conta XenMobile do usuário. No iOS, esta ação exclui a chave de criptografia que os usuários precisam para acessar os recursos do XenMobile.
Visualizar inventário de software	Ver qual software está instalado em um dispositivo.
Solicitar espelhamento AirPlay	Solicitar o início do streaming AirPlay.
Parar espelhamento AirPlay	Parar streaming AirPlay.

Habilitar modo perdido	Em **Gerenciar > Dispositivos**, você pode colocar um dispositivo supervisionado no modo perdido para bloquear um dispositivo supervisionado na tela de bloqueio. O modo perdido também permite localizar o dispositivo quando ele é perdido ou roubado.
Desabilitar modo perdido	Em **Gerenciar > Dispositivos**, você pode desabilitar o modo perdido para um dispositivo que está configurado para o modo perdido.
Atualizar SO do dispositivo	Você pode implantar uma política de dispositivo de Controle de Atualizações de SO para os dispositivos.
Desligar dispositivo	Desligue dispositivos iOS do console XenMobile.
Reiniciar dispositivo	Reinicie dispositivos iOS do console XenMobile.

Usuários e Grupos Locais

Os administradores gerenciam usuários locais e grupos de usuários locais na página **Gerenciar > Usuários** no XenMobile.

Adicionar Usuários Locais
Excluir Usuários Locais
Editar Usuários Locais
Importar Usuários Locais
Exportar Usuários Locais
Grupos de Usuários Locais
Obter ID de Bloqueio de Usuário Local
Excluir Bloqueio de Usuário Local

Registro

Os administradores podem adicionar e excluir convites de registro, enviar notificações aos usuários e exportar a tabela de registro para um arquivo .csv.

Adicionar/Excluir registro	Adicionar ou remover um convite de registro para um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite de registro para um usuário ou grupo de usuários.
Exportar tabela de convites de registro	Coletar informações de registro da página Registro e exportá-las para um arquivo .csv.

Políticas

Adicionar/Excluir política	Adicionar ou remover uma política de dispositivo ou aplicativo.
Editar política	Alterar uma política de dispositivo ou aplicativo.
Carregar política	Carregar uma política de dispositivo ou aplicativo.
Clonar política	Copiar uma política de dispositivo ou aplicativo.
Desativar política	Desativar uma política de aplicativo existente.
Exportar política	Coletar informações de política de dispositivo da página Políticas de Dispositivo e exportá-las para um arquivo .csv.
Atribuir política	Atribuir uma política de dispositivo a um ou mais grupos de entrega.

Aplicativo

Os administradores gerenciam aplicativos na página **Configurar > Aplicativos** no XenMobile.

Adicionar/Excluir loja de aplicativos ou aplicativo empresarial	Adicionar ou remover um aplicativo de loja de aplicativos pública ou um aplicativo empresarial (não habilitado para MDX).
Editar loja de aplicativos ou aplicativo empresarial	Alterar um aplicativo de loja de aplicativos pública ou um aplicativo empresarial (não habilitado para MDX).
Adicionar/Excluir aplicativo MDX, Web e SaaS	Adicionar ou remover um aplicativo habilitado para MDX, um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) ao XenMobile.
Editar aplicativo MDX, Web e SaaS	Alterar um aplicativo habilitado para MDX, um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) ao XenMobile.
Adicionar/Excluir categoria	Adicionar ou excluir uma categoria na qual os aplicativos podem aparecer na XenMobile Store.
Atribuir aplicativo público/empresarial a grupo de entrega	Atribuir um aplicativo de loja de aplicativos pública ou um aplicativo habilitado para MDX a um grupo de entrega para implantação.
Atribuir aplicativo MDX/WebLink/SaaS a grupo de entrega	Atribuir a um grupo de entrega um aplicativo habilitado para MDX, que não requer logon único (WebLink), ou que seja de uma rede pública (SaaS).
Exportar tabela de aplicativos	Coletar informações do aplicativo da página Aplicativo e exportá-las para um arquivo .csv.

Nota:

Quando você seleciona **Recursos do console > Aplicativo**, o endpoint da API `GET <https://XMS_IP:4443/controlpoint/rest/ad>` retorna as informações LDAP por padrão.

Mídia

Gerenciar mídias obtidas de uma loja de aplicativos pública ou por meio de uma licença de Compra por Volume.

Adicionar/Excluir livros da loja de aplicativos ou da empresa
Atribuir livros públicos/empresariais ao grupo de entrega
Editar livros da loja de aplicativos ou da empresa

Ação

Adicionar/excluir ação	Adicionar ou remover uma ação definida por um gatilho (evento, propriedade do dispositivo ou do usuário, ou nome do aplicativo instalado) e resposta associada.
Editar ação	Alterar uma ação definida por um gatilho (evento, propriedade do dispositivo ou do usuário, ou nome do aplicativo instalado) e resposta associada.
Atribuir ação ao grupo de entrega	Atribuir uma ação a um grupo de entrega para implantação em dispositivos de usuário.
Exportar ação	Coletar informações de ação da página Ações e exportá-las para um arquivo .csv.

Grupo de entrega

Os administradores gerenciam grupos de entrega na página **Configurar > Grupos de Entrega**.

Adicionar/excluir grupo de entrega	Criar ou remover um grupo de entrega, que adiciona usuários especificados e políticas, aplicativos e ações opcionais.
Editar grupo de entrega	Alterar um grupo de entrega existente, que modifica usuários e políticas, aplicativos e ações opcionais.

Implantar grupo de entrega	Disponibilizar um grupo de entrega para uso.
Exportar grupo de entrega	Coletar informações do grupo de entrega da página Grupo de entrega e exportá-las para um arquivo .csv.

Perfil de registro

Gerenciar perfis de registro.

Adicionar/excluir perfil de registro
Editar perfil de registro
Atribuir perfil de registro a grupo de entrega

Configurações

Os administradores configuram várias definições nas páginas de **Configurações**.

RBAC	Atribuição de RBAC, Atribuir funções. **Importante:** Esta permissão concede aos administradores acesso total, incluindo a capacidade de atribuir suas próprias permissões. Conceda este acesso apenas aos usuários a quem você pretende dar a capacidade de manipular tudo no sistema Endpoint Management.
LDAP	Administrar um ou mais diretórios compatíveis com LDAP, como o Active Directory, para importar grupos, contas de usuário e propriedades relacionadas.
Licença	Para XenMobile Server local. Administre suas licenças Citrix®.
Registro	Habilitar modos de segurança de registro para usuários e o Portal de Autoatendimento.

Gerenciamento de Lançamentos	Visualizar a versão instalada atual. Inclui: Atualização do Gerenciamento de Lançamentos
Certificados	Editar certificado APNS, Ouvinte SSL de Certificados
Modelos de Notificação	Crie modelos de notificação para usar em ações automatizadas, registro e entrega de mensagens de notificação padrão aos usuários.
Fluxos de Trabalho	Gerencie a criação, aprovação e remoção de contas de usuário para uso com configurações de aplicativos.
Provedores de Credenciais	Adicione um ou mais provedores de credenciais autorizados a emitir certificados de dispositivo. Os provedores de credenciais controlam o formato do certificado e as condições para renovar ou revogar o certificado.
Entidades PKI	Gerencie entidades de infraestrutura de chave pública (genéricas, Serviços de Certificado Microsoft ou CA discricionária).
Testar Conexão PKI	Use o botão **Testar Conexão** na página **Configurações > Entidades PKI** para garantir que o servidor esteja acessível.
Propriedades do Cliente	Gerencie várias propriedades em dispositivos de usuário, como tipo de senha, força ou expiração.
Suporte ao Cliente	Defina as formas pelas quais os usuários podem entrar em contato com seus serviços de suporte (e-mail, telefone ou e-mail de tíquete de suporte).
Marca do Cliente	Crie um nome de loja personalizado e exibições de loja padrão para a XenMobile

	Store. Adicione um logotipo personalizado que aparece em uma XenMobile Store ou no Secure Hub.
Gateway SMS da Operadora	Configure gateways SMS da operadora para configurar notificações que o XenMobile envia por meio de gateways SMS da operadora.
Servidor de Notificação	Configure um servidor de gateway SMTP para enviar um e-mail aos usuários.
Gateway ActiveSync	Gerencie o acesso de usuários a usuários e dispositivos por meio de regras e propriedades.
Programa de Implantação da Apple	Adicione uma conta do Programa de Implantação da Apple ao XenMobile.
Registro de Dispositivo do Apple Configurator	Configure as definições do Apple Configurator no XenMobile.
Configurações de compra por volume do iOS	Adicione contas de Compra por Volume da Apple.
Provedor de Serviços Móveis	Use a interface do Provedor de Serviço Móvel para consultar dispositivos BlackBerry e outros dispositivos Exchange ActiveSync e para emitir operações.
Citrix Gateway	Para XenMobile Server local. Adicione um Citrix Gateway. Escolha se deseja habilitar a autenticação e se deseja enviar um certificado de usuário para autenticação. Escolha um provedor de credenciais.
Controle de Acesso à Rede	Defina as condições que determinam que um dispositivo não está em conformidade e, portanto, tem o acesso à rede negado.
Samsung Knox	Habilite ou desabilite o XenMobile para consultar as APIs REST do servidor de atestado Samsung Knox.

Propriedades do Servidor	Adicione ou modifique as propriedades do servidor. Requer a reinicialização do XenMobile em todos os nós.
Syslog	Para XenMobile Server local. Envie arquivos de log para um servidor de Log do Sistema (syslog) usando o nome do host do servidor ou o endereço IP.
XenApp e XenDesktop®	Permita que os usuários adicionem Aplicativos e Desktops Virtuais através do Secure Hub.
Citrix Files	Ao usar o XenMobile com contas Enterprise: Configure as configurações para conectar-se à conta ShareFile e à conta de serviço de administrador para gerenciar contas de usuário. Requer domínio Citrix Files existente e credenciais de administrador. Ao usar o XenMobile com conectores de zona de armazenamento: Configure o XenMobile para apontar para compartilhamentos de rede e locais do SharePoint definidos nos conectores de zona de armazenamento.
Programa de Melhoria da Experiência	Para XenMobile Server local. Ative ou desative o envio de estatísticas anônimas e informações de uso para a Citrix.
Microsoft Azure	Para XenMobile Server local. Integre o XenMobile com o Microsoft Azure.
Android Enterprise	Configure as configurações do servidor Android Enterprise.
Provedor de Identidade (IdP)	Configure um provedor de identidade.
Ferramentas do XenMobile	Acesse a página Ferramentas do XenMobile.
Configuração SNMP	Habilite o SNMP para nós do XenMobile Server. Edite ou adicione usuários de monitoramento, configure o gerenciador SNMP

	onde as notificações de trap aparecem e configure intervalos e limites de trap.

Suporte

Os administradores podem realizar várias tarefas de suporte.

Verificações de Conectividade do Citrix Gateway	Realiza várias verificações de conectividade para o Citrix Gateway por endereço IP. Requer um nome de usuário e senha.
Verificações de Conectividade do XenMobile	Realiza verificações de conectividade para recursos selecionados do XenMobile, como banco de dados, DNS ou Google Plan.
Criar Pacotes de Suporte	Para o XenMobile Server local. Cria um arquivo para enviar ao Suporte Citrix para solução de problemas. Contém informações do sistema, logs, informações do banco de dados, informações principais, arquivos de rastreamento e as informações de configuração mais recentes para o XenMobile ou Citrix Gateway.
Documentação do Produto Citrix	Acessa o site público de documentação do Citrix XenMobile.
Central de Conhecimento Citrix	Acessa o site de Suporte Citrix para pesquisar artigos da base de conhecimento.
Logs	Acessa e analisa detalhes de arquivos de log para depuração, auditoria de administrador e auditoria de usuário.
Informações do Cluster	Para o XenMobile Server local. Acessa informações sobre cada um dos nós em um ambiente em cluster.
Coleta de Lixo	Para o XenMobile Server local. Acessa informações sobre objetos de memória que não estão mais em uso.

Propriedades de Memória Java	Para XenMobile Server local. Acesse um instantâneo do uso da memória Java, detalhes da memória e detalhes do pool de memória.
Macros	Preencha dados de propriedade de usuário ou dispositivo no campo de texto de um perfil, política, notificação ou modelo de registro. Configure uma única política, implante a política para uma grande base de usuários e tenha valores específicos do usuário exibidos para cada usuário direcionado.
Configuração PKI	Importar e exportar informações de configuração PKI.
Utilitário de Assinatura APNS	Envie uma solicitação para certificados de assinatura da Apple Push Network (APNs) ou carregue um certificado APNs do Secure Mail para iOS.
Serviços Citrix Insight	Carregue logs para os Serviços Citrix Insight (CIS) para obter assistência com vários problemas.
Status do conector Citrix Gateway™ do dispositivo para Exchange ActiveSync	Consulte o XenMobile para verificar o status de um dispositivo conforme enviado ao conector Citrix Gateway para Exchange ActiveSync com base no ID do ActiveSync do dispositivo.
Anonimização e desanonimização	Para XenMobile Server local. Ao criar pacotes de suporte no XenMobile, dados confidenciais de usuário, servidor e rede são anonimizados por padrão. Você pode alterar esse comportamento em **Suporte > Anonimização e Desanonimização** em **Avançado**.
Configurações de Log	Personalize o nível de log ou adicione um registrador personalizado.

Restringir Acesso a Grupos

Usuários administradores podem aplicar permissões a todos os grupos de usuários.

Função de Suporte

Usuários com a função de Suporte têm acesso ao suporte remoto. Suas permissões se aplicam a todos os usuários por padrão e eles não podem editar essa configuração.

Função de Usuário

Usuários com a função de Usuário têm o seguinte acesso limitado ao XenMobile.

Acesso autorizado

Portal de Autoatendimento	Os usuários têm acesso apenas ao Portal de Autoatendimento no XenMobile.

Recursos do console

Os usuários têm o seguinte acesso restrito ao console do XenMobile.

Dispositivos

Limpar dispositivo completamente	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, se o dispositivo tiver um.
Limpeza Seletiva do dispositivo	Apaga todos os dados e aplicativos corporativos de um dispositivo, deixando os dados e aplicativos pessoais no lugar.
Visualizar localizações	Ver a localização e definir restrições geográficas em um dispositivo. Incluído: Localizar dispositivo, Ver a localização de um dispositivo, Rastrear dispositivo, Rastrear localização do dispositivo ao longo do tempo
Bloquear dispositivo	Bloqueia um dispositivo remotamente para que não possa ser usado.
Desbloquear dispositivo	Desbloqueia um dispositivo remotamente para que possa ser usado.

Bloquear contêiner	Bloqueia remotamente o contêiner corporativo em um dispositivo.
Desbloquear contêiner	Desbloqueia remotamente o contêiner corporativo em um dispositivo.
Redefinir senha do contêiner	Redefine a senha do contêiner corporativo.
Habilitar ASM DEP/Ignorar bloqueio de ativação	Armazene um código de bypass em um dispositivo iOS supervisionado quando o Bloqueio de Ativação estiver ativado. Se precisar apagar o dispositivo, use este código para limpar o Bloqueio de Ativação automaticamente.
Toca o dispositivo	Tocar remotamente um dispositivo Windows em volume máximo por 5 minutos.
Reiniciar o dispositivo	Reiniciar um dispositivo Windows.
Visualizar inventário de software	Ver qual software está instalado em um dispositivo.

Registro

Adicionar/Excluir registro	Adicionar ou remover um convite de registro para um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite de registro para um usuário ou grupo de usuários.

Restringir Acesso a Grupo

Para todas as quatro funções padrão, esta permissão é definida por padrão e pode ser aplicada a todos os grupos de usuários. Você não pode editar a função.

Configurar funções com RBAC

O recurso de Controle de Acesso Baseado em Função (RBAC) no XenMobile permite atribuir funções predefinidas, ou conjuntos de permissões, a usuários e grupos. Essas permissões controlam o nível de acesso que os usuários têm às funções do sistema.

O XenMobile implementa quatro funções de usuário padrão para separar logicamente o acesso às funções do sistema:

- **Administrador:** Concede acesso total ao sistema.
- **Suporte:** Concede acesso ao suporte remoto.
- **Usuário:** Usado por usuários que podem registrar dispositivos e acessar o Portal de Autoatendimento.

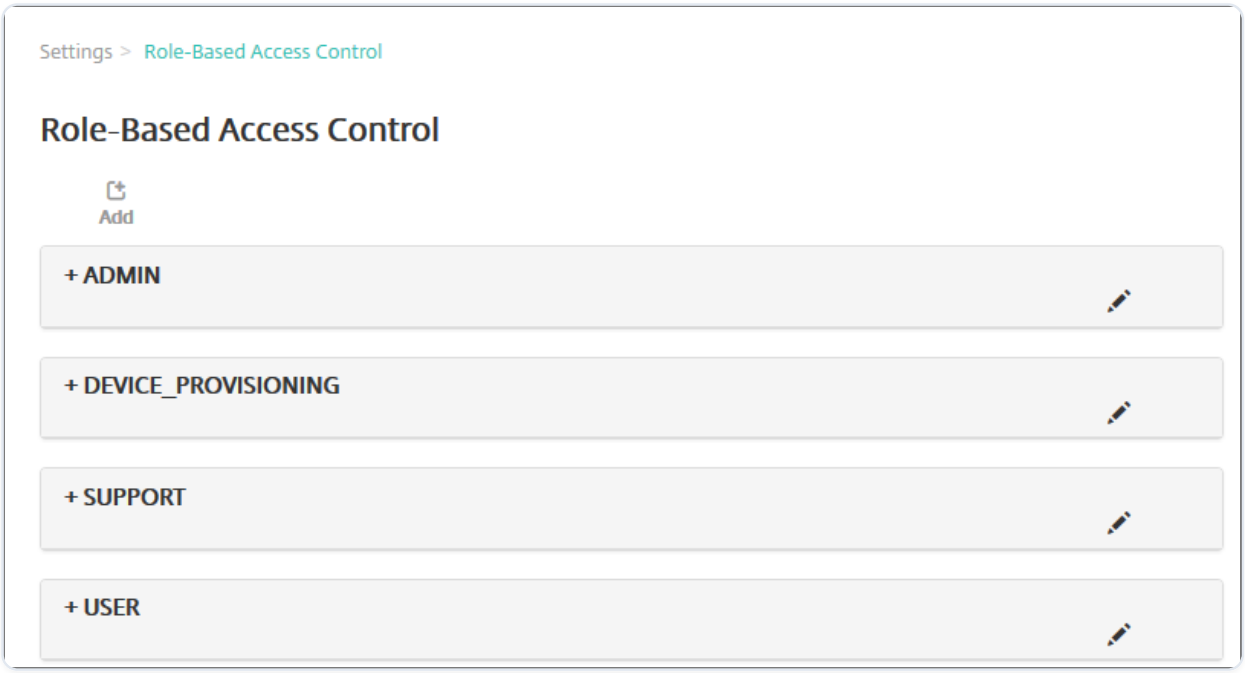
Você também pode usar as funções padrão como modelos que você personaliza para criar funções de usuário. Você pode atribuir permissões às funções para acessar funções específicas do sistema além das funções definidas pelas funções padrão.

As funções podem ser atribuídas a usuários locais (no nível do usuário) ou a grupos do Active Directory (todos os usuários nesse grupo têm as mesmas permissões). Se um usuário pertencer a vários grupos do Active Directory, todas as permissões serão mescladas para definir as permissões para esse usuário. Por exemplo, suponha que os usuários do ADGroupA possam localizar dispositivos de gerentes e os usuários do ADGroupB possam apagar dispositivos de funcionários. Nesse caso, um usuário que pertence a ambos os grupos pode localizar e apagar os dispositivos de gerentes e funcionários.

> **Observação:**
>
> Usuários locais podem ter apenas uma função atribuída a eles.
>
> Você pode usar o recurso RBAC no XenMobile para fazer o seguinte:

- Criar uma função.
- Adicionar grupos a uma função.
- Associar usuários locais a funções.

1. No console do XenMobile, vá para **Configurações > Controle de Acesso Baseado em Função**. A página **Controle de Acesso Baseado em Função** é exibida, mostrando as quatro funções de usuário padrão, além de quaisquer funções que você tenha adicionado anteriormente.



Se você clicar no sinal de mais (+) ao lado de uma função, a função se expandirá para mostrar todas as permissões para essa função, conforme mostrado na figura a seguir.



2. Clique em **Adicionar** para adicionar uma nova função de usuário. Para editar a função, clique no ícone de caneta à direita de uma função existente. Para excluir a função, clique no ícone de lixeira à direita de uma função. Você não pode excluir as funções de usuário padrão.

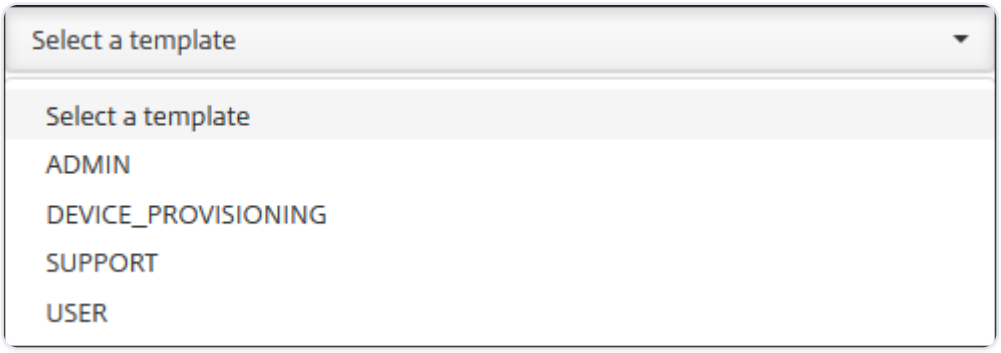
   - Ao clicar em **Adicionar** ou no ícone de caneta, a página **Adicionar Função** ou **Editar Função** é exibida.
   - Ao clicar no ícone de lixeira, uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para remover a função selecionada.

3. Insira as seguintes informações para criar ou editar uma função de usuário:

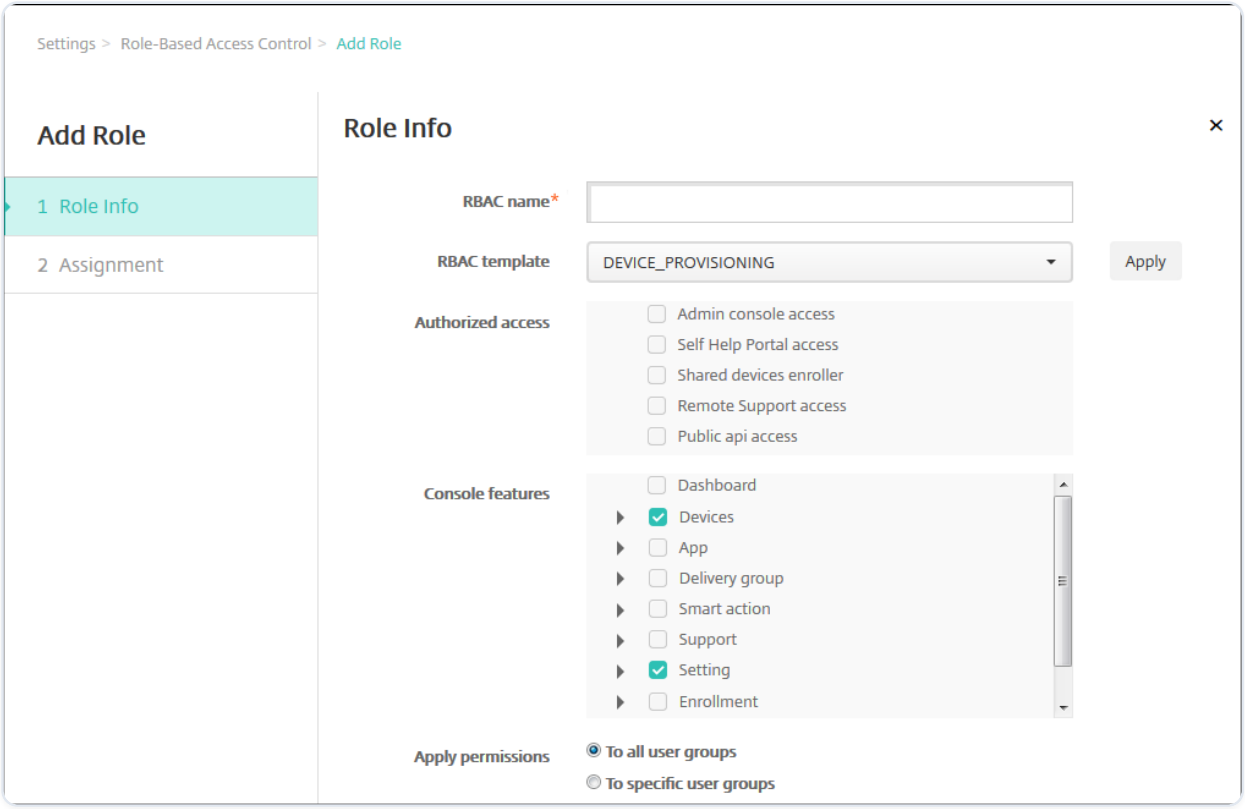
   - **Nome do RBAC:** Insira um nome descritivo para a nova função de usuário. Você não pode alterar o nome de uma função existente.

- **Modelo de RBAC:** Opcionalmente, clique em um modelo como ponto de partida para a nova função. Você não pode selecionar um modelo se estiver editando uma função existente.

Os modelos de RBAC são as funções de usuário padrão. Eles definem o acesso às funções do sistema que os usuários associados a essa função possuem. Depois de selecionar um modelo de RBAC, você pode ver todas as permissões associadas a essa função nos campos **Acesso Autorizado** e **Recursos do Console**. O uso de um modelo é opcional. Você pode selecionar diretamente as opções que deseja atribuir a uma função nos campos **Acesso Autorizado** e **Recursos do Console**.

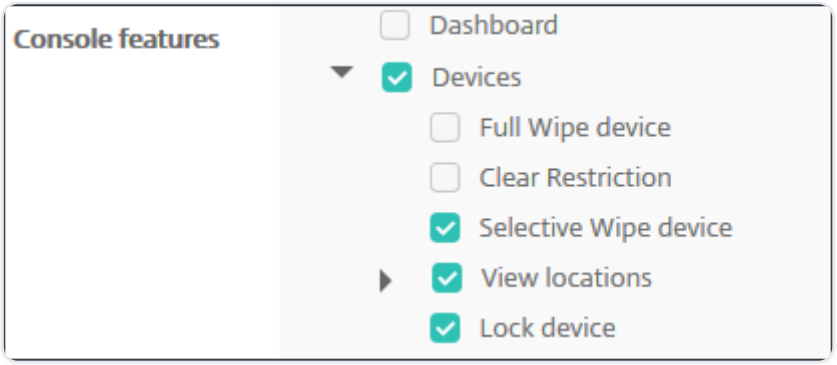


4. Clique em **Aplicar** próximo ao campo **Modelo de RBAC** selecionado para preencher **Acesso autorizado** e **Recursos do console** com as permissões de acesso e recursos predefinidas.



5. Selecione e desmarque as caixas de seleção em **Acesso autorizado** e **Recursos do console** para personalizar a função.

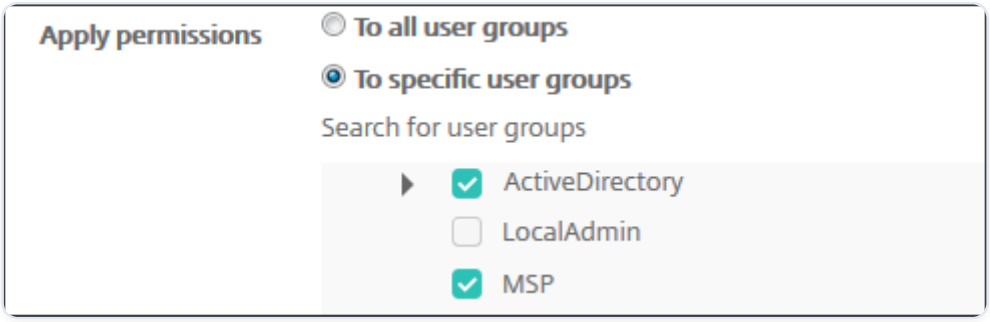
Se você clicar no triângulo ao lado de um recurso do Console, as permissões específicas desse recurso aparecerão e você poderá selecioná-las e desmarcá-las. Clicar na caixa de seleção de nível superior proíbe o acesso a essa área do console. Selecione opções individuais abaixo do nível superior para habilitar essas opções. Por exemplo, na figura a seguir, as opções **Limpar dispositivo completamente** e **Limpar restrições** não aparecem para os usuários atribuídos à função. As opções marcadas aparecem.



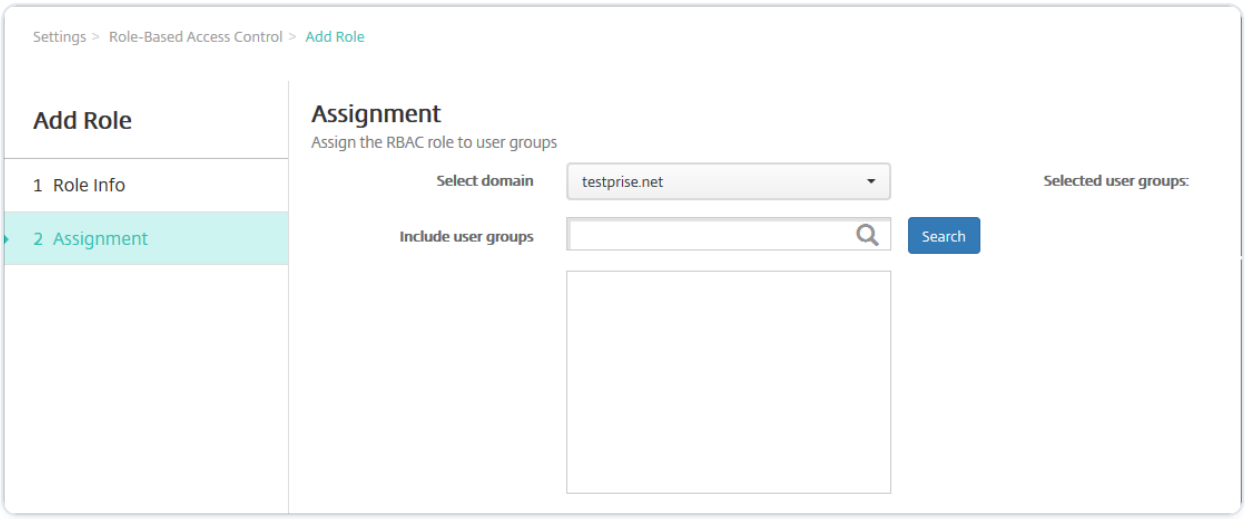
6. **Aplicar permissões:** Selecione um ou mais grupos de usuários para limitar quais grupos o administrador pode gerenciar. Se você clicar em **Para grupos de usuários específicos**, uma lista de grupos aparece da qual você pode selecionar um ou mais grupos.

   Por exemplo, se um administrador RBAC tiver permissões para os grupos de usuários ActiveDirectory e MSP:

   - O administrador pode acessar informações apenas para usuários que estão no grupo ActiveDirectory, no grupo MSP ou em ambos os grupos.
   - O administrador não pode visualizar nenhum outro usuário local ou do AD. O administrador pode visualizar usuários que são membros de grupos filhos de qualquer um desses grupos.
   - O administrador pode enviar convites para:
     - os grupos de permissão e seus grupos filhos
     - os usuários que são membros de grupos de permissão e seus grupos filhos

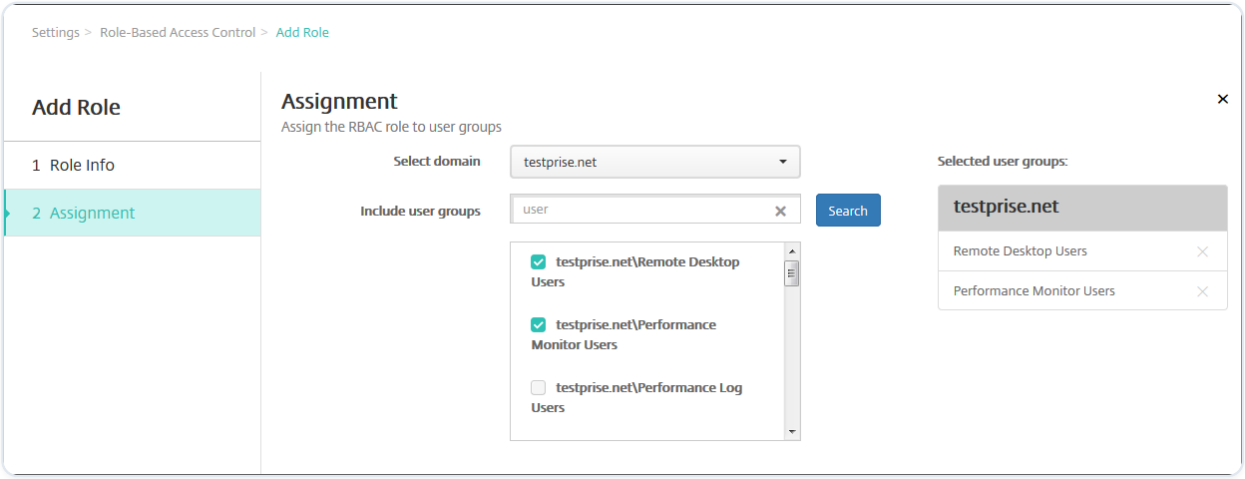


7. Clique em **Avançar**. A página **Atribuição** aparece.



8. Insira as seguintes informações para atribuir a função a grupos de usuários.

   - **Selecionar domínio:** Clique em um domínio na lista suspensa.
   - **Incluir grupos de usuários:** Clique em Pesquisar para ver uma lista de todos os grupos disponíveis ou digite um nome de grupo completo ou parcial para limitar a lista apenas aos grupos com esse nome.
   - Na lista que aparece, selecione os grupos de usuários aos quais você deseja atribuir a função. Ao selecionar um grupo de usuários, o grupo aparece na lista **Grupos de usuários selecionados**.



Nota:

Para remover um grupo de usuários da lista **Grupos de usuários selecionados**, clique no X ao lado do nome do grupo de usuários.

9. Clique em **Salvar**.

Notificações

Você pode usar notificações no XenMobile® para os seguintes propósitos:

- Para se comunicar com grupos selecionados de usuários para várias funções relacionadas ao sistema. Você também pode direcionar essas notificações para determinados usuários. Por exemplo, todos os usuários com dispositivos iOS, usuários cujos dispositivos estão fora de conformidade, usuários com dispositivos de propriedade do funcionário e assim por diante.
- Para registrar usuários e seus dispositivos.
- Para notificar usuários automaticamente (usando ações automatizadas) quando certas condições são atendidas. Por exemplo:
  - Quando um dispositivo de usuário está prestes a ser bloqueado do domínio corporativo devido a um problema de conformidade.
  - Quando um dispositivo foi desbloqueado (jailbroken ou rooted)

Para obter detalhes sobre ações automatizadas, consulte Ações Automatizadas.

Para enviar notificações com o XenMobile, você deve configurar um gateway e um servidor de notificação. Você pode configurar um servidor de notificação no XenMobile para configurar servidores de gateway de Simple Mail Transfer Protocol (SMTP) e Short Message Service (SMS) para enviar notificações por e-mail e texto (SMS) aos usuários. Você pode usar notificações para enviar mensagens por dois canais diferentes: SMTP ou SMS.

- SMTP é um protocolo orientado a conexão e baseado em texto no qual um remetente de e-mail se comunica com um receptor de e-mail emitindo cadeias de comando e fornecendo os dados necessários, tipicamente por meio de uma conexão Transmission Control Protocol (TCP). As sessões SMTP consistem em comandos originados por um cliente SMTP (a pessoa que envia a mensagem) e respostas correspondentes do servidor SMTP.
- SMS é um componente de serviço de mensagens de texto de sistemas de comunicação telefônica, web ou móvel. O SMS usa protocolos de comunicação padronizados para permitir que dispositivos de linha fixa ou móveis troquem mensagens de texto curtas.

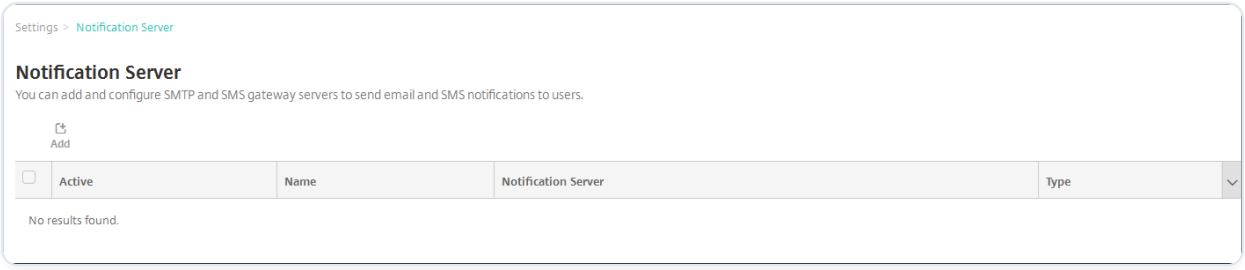
Você também pode configurar um Gateway SMS da Operadora no XenMobile para configurar notificações que são enviadas por meio de um gateway SMS de uma operadora. As operadoras usam gateways SMS para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos de comunicação padronizados para permitir que dispositivos de linha fixa ou móveis troquem mensagens de texto curtas.

Pré-requisitos

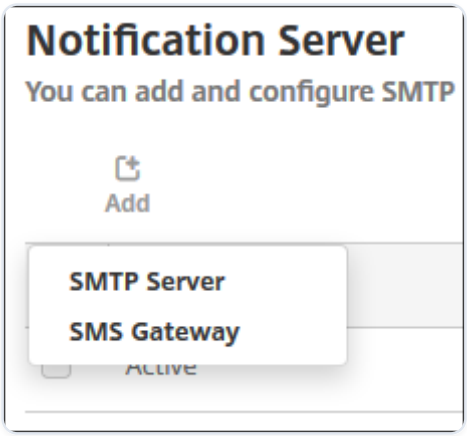
- Antes de configurar o gateway SMS, consulte o administrador do sistema para determinar as informações do servidor. É importante saber se o servidor SMS está hospedado em um servidor corporativo interno ou se o servidor faz parte de um serviço de e-mail hospedado. Nesse caso, você precisa de informações do site do provedor de serviços.
- Configure o servidor de notificações SMTP para enviar mensagens aos usuários. Se o servidor estiver hospedado em um servidor interno, entre em contato com o administrador do sistema para obter informações de configuração. Se o servidor for um serviço de e-mail hospedado, localize as informações de configuração apropriadas no site do provedor de serviços.
- Você pode usar um servidor SMTP ativo e um servidor SMS ativo simultaneamente. Ambos os canais de comunicação permitem uma configuração ativa.
- Abra a porta 25 do XenMobile localizado na DMZ da sua rede para apontar de volta para o servidor SMTP na sua rede interna. Isso permite que o XenMobile envie notificações com sucesso.

Configurar um servidor SMTP e um gateway SMS

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Notificações**, clique em **Servidor de Notificação**. A página **Servidor de Notificação** é exibida.

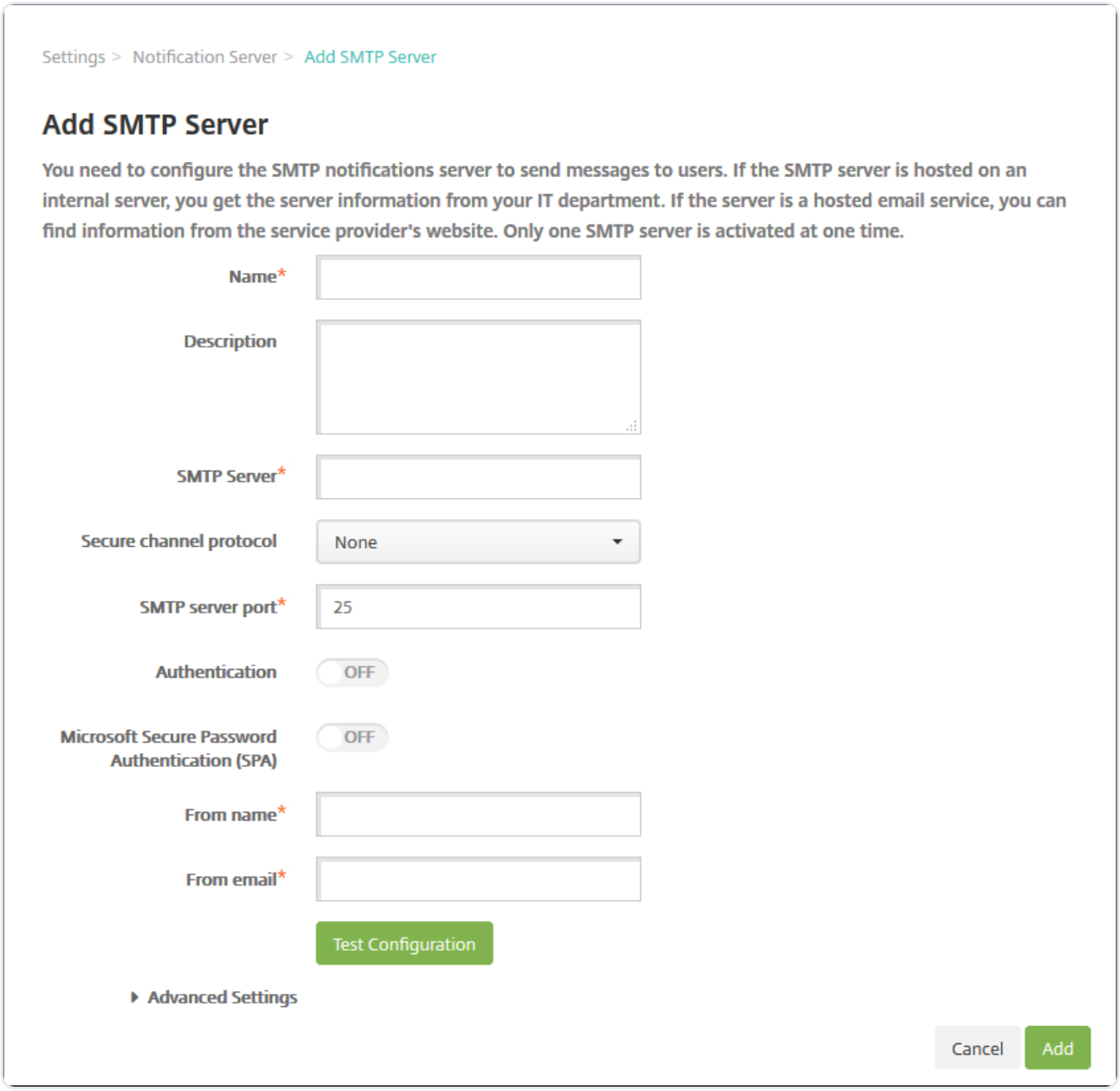


3. Clique em **Adicionar**. Um menu é exibido com opções para configurar um servidor SMTP ou um gateway SMS.



- Para adicionar um servidor SMTP, clique em **Servidor SMTP** e consulte Para adicionar um servidor SMTP para as etapas de configuração desta definição.
- Para um gateway SMS, clique em **Gateway SMS** e consulte Para adicionar um gateway SMS para as etapas de configuração desta definição.

Adicionar um servidor SMTP



1. Configure estas definições:

   - **Nome:** Digite o nome associado a esta conta de servidor SMTP.
   - **Descrição:** Opcionalmente, insira uma descrição do servidor.
   - **Servidor SMTP:** Digite o nome do host para o servidor. O nome do host deve ser um nome de domínio totalmente qualificado (FQDN) ou um endereço IP.
   - **Protocolo de canal seguro:** Clique em **SSL**, **TLS** ou **Nenhum** na lista suspensa para o protocolo de canal seguro usado pelo servidor (se o servidor estiver configurado para usar autenticação segura). O padrão é **Nenhum**.

- **Porta do servidor SMTP:** Digite a porta usada pelo servidor SMTP. Por padrão, a porta é definida como 25. Se as conexões SMTP usarem o protocolo de canal seguro SSL, a porta será definida como 465.
- **Autenticação:** Selecione **ATIVADO** ou **DESATIVADO**. O padrão é **DESATIVADO**.
- Se você habilitar a **Autenticação**, configure estas definições:
  - **Nome de usuário:** Digite o nome de usuário para autenticação
  - **Senha:** Digite a senha do usuário de autenticação.

> **Importante:**
>
> Para usar o OAuth com o Microsoft Exchange Online, você deve primeiro registrar seu aplicativo no Microsoft Entra ID. Após o registro, habilite **Autenticação** e **Microsoft Exchange Online OAuth 2.0**.

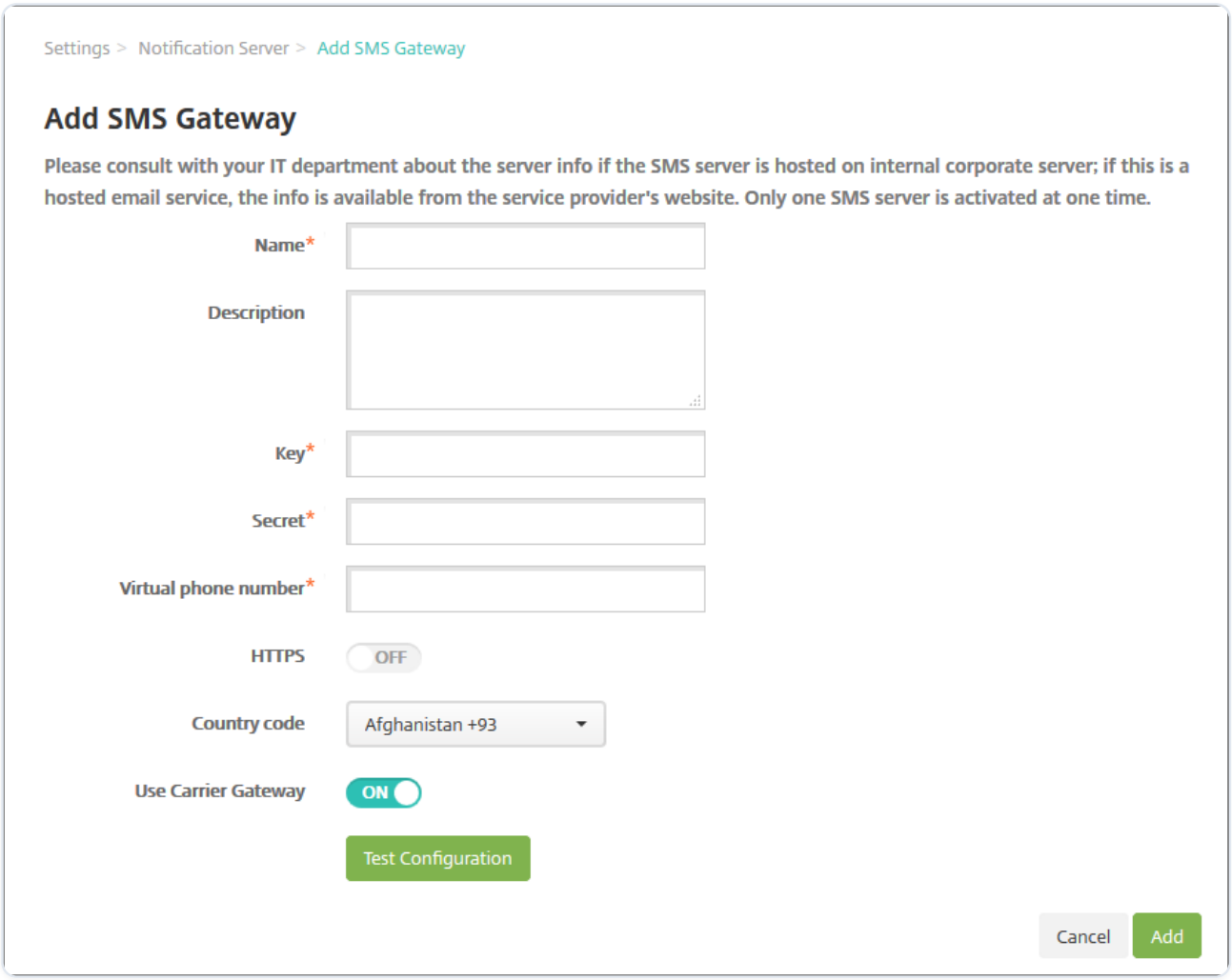
- Se você habilitar a **Autenticação** e o **Microsoft Exchange Online OAuth 2.0**, configure as seguintes definições:
  - **Nome de usuário:** Digite o nome de usuário para autenticação.
  - **ID do locatário:** Digite o ID do locatário do seu diretório Microsoft Entra ID.
  - **ID do cliente:** Digite o ID do cliente (aplicativo) do seu aplicativo registrado. Você pode encontrá-lo no portal do Azure > seu aplicativo registrado > **ID do aplicativo (cliente)**.
  - **Segredo do cliente:** Digite o segredo do cliente do seu aplicativo registrado. Você pode encontrá-lo no portal do Azure > seu aplicativo registrado > **Certificados e segredos**.
- **Autenticação de Senha Segura da Microsoft (SPA):** Se o servidor SMTP estiver usando o SPA, clique em **ATIVADO**. O padrão é **DESATIVADO**.
- **Nome do Remetente:** Digite o nome exibido na caixa **De** quando um cliente recebe um e-mail de notificação deste servidor. Por exemplo, TI Corporativa.
- **E-mail do Remetente:** Digite o endereço de e-mail usado se um destinatário de e-mail responder à notificação enviada pelo servidor SMTP.

2. Clique em **Testar Configuração** para enviar uma notificação de e-mail de teste.
3. Expanda **Configurações Avançadas** e, em seguida, configure estas configurações:

- **Número de tentativas SMTP:** Digite o número de vezes para tentar novamente uma mensagem com falha enviada do servidor SMTP. O padrão é 5.
- **Tempo Limite SMTP:** Digite a duração a aguardar (em segundos) ao enviar uma solicitação SMTP. Aumente este valor se o envio de mensagens estiver falhando continuamente devido a tempos limite. Tenha cuidado ao diminuir este valor; isso pode aumentar o número de mensagens com tempo limite esgotado e não entregues. O padrão é 30 segundos.
- **Número máximo de destinatários SMTP:** Digite o número máximo de destinatários por mensagem de e-mail enviada pelo servidor SMTP. O padrão é 100.

4. Clique em **Adicionar**.

Adicionar um gateway SMS



Observação:

> O XenMobile suporta apenas mensagens SMS da Nexmo. Se você ainda não tem uma conta para usar as mensagens da Nexmo, visite o site deles para criar uma.

1. Configure as seguintes configurações:

   - **Nome:** Digite um nome para a configuração do Gateway SMS. Este campo é obrigatório.
   - **Descrição:** Opcionalmente, digite uma descrição da configuração.
   - **Chave:** Digite o identificador numérico fornecido pelo administrador do sistema ao ativar a conta. Este campo é obrigatório.
   - **Segredo:** Digite um segredo fornecido pelo administrador do sistema que é usado para acessar sua conta quando uma senha é perdida ou roubada. Este campo é obrigatório.
   - **Número de Telefone Virtual:** Este campo é usado ao enviar para números de telefone norte-americanos (com o prefixo +1). Você deve digitar um número de telefone virtual Nexmo e deve usar apenas dígitos neste campo. Você pode comprar números de telefone virtuais no site da Nexmo.
   - **HTTPS:** Selecione se deseja usar HTTPS para transmitir solicitações SMS para a Nexmo. O padrão é **DESATIVADO**.

   > **Importante:**
   >
   > Deixe o HTTPS definido como **ATIVADO**, a menos que você tenha orientação do Suporte Citrix para configurá-lo como **DESATIVADO**.

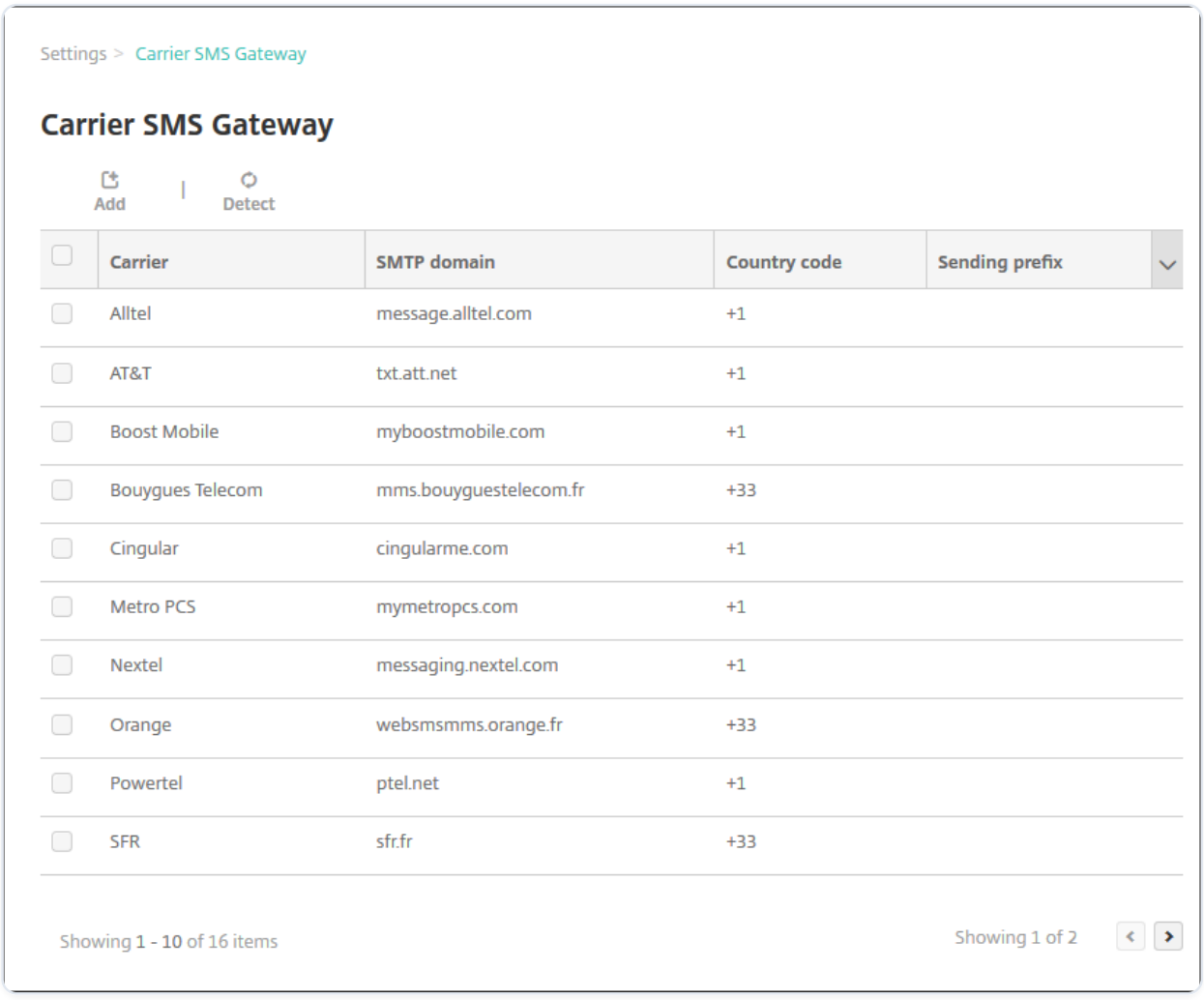
   - **Código do País:** Clique no prefixo de código de país SMS padrão na lista suspensa para destinatários em sua organização. Este campo sempre começa com um símbolo +. O padrão é **Afeganistão +93**.

2. Clique em **Testar Configuração** para enviar uma mensagem de teste usando a configuração atual. Erros de conexão, como erros de autenticação ou de número de telefone virtual, são detectados e aparecem imediatamente. As mensagens são recebidas no mesmo período de tempo que as mensagens enviadas entre telefones celulares.
3. Clique em **Adicionar**.

Adicionar um gateway SMS de operadora

Você pode configurar um Gateway SMS de Operadora no XenMobile para configurar notificações que são enviadas através do gateway SMS de uma operadora. As operadoras usam gateways de Serviço de Mensagens Curtas (SMS) para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos de comunicação padronizados para permitir que dispositivos de linha fixa ou móveis troquem mensagens de texto curtas.

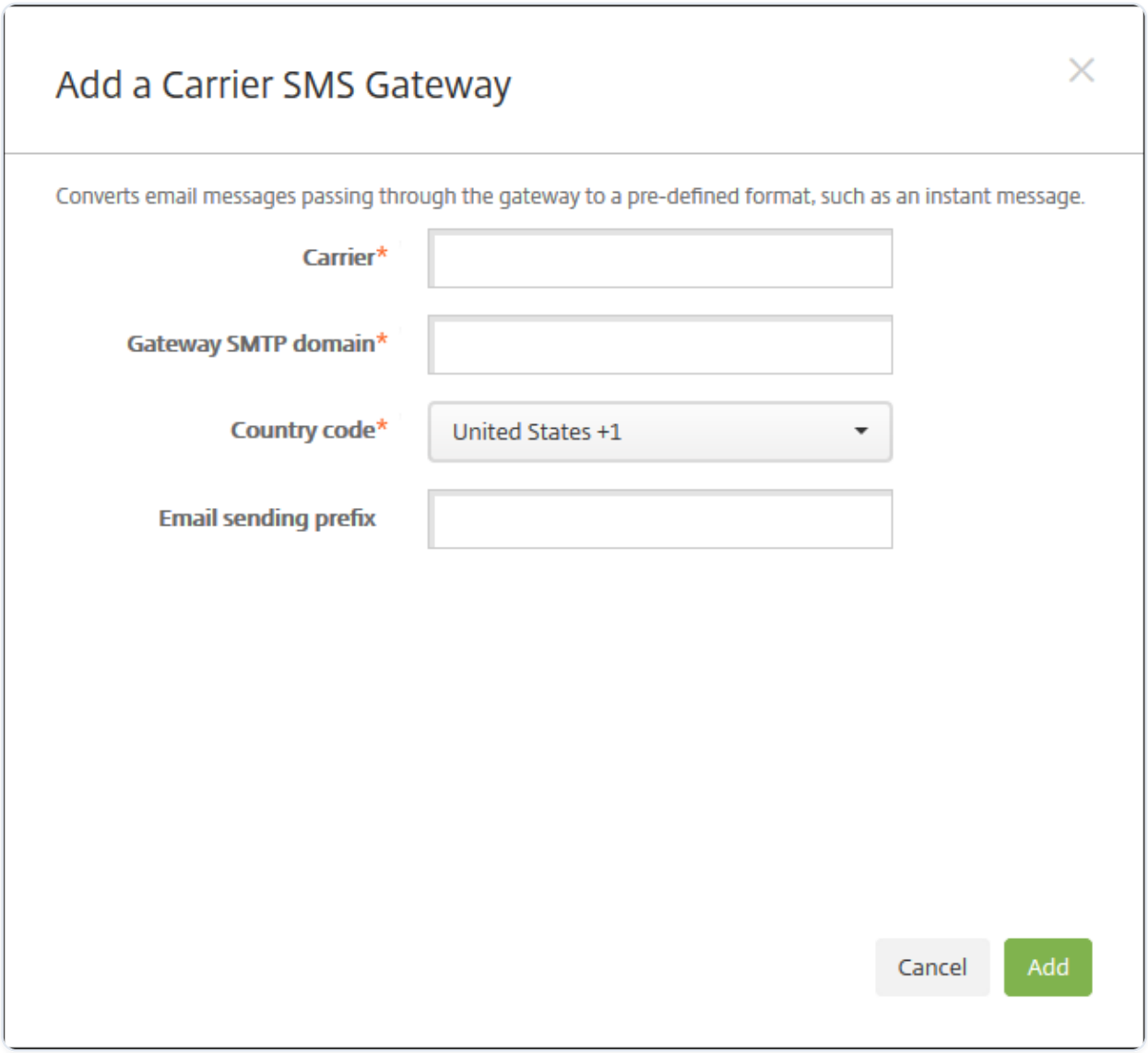
1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Notificações**, clique em **Gateway SMS de Operadora**. A página **Gateway SMS de Operadora** é aberta.



3. Faça um dos seguintes:

   - Clique em **Detectar** para descobrir automaticamente um gateway. Uma caixa de diálogo é exibida indicando que não há novas operadoras detectadas ou listando as novas operadoras detectadas entre os dispositivos registrados.

- Clique em **Adicionar**. A caixa de diálogo **Adicionar um Gateway SMS de Operadora** é exibida.



Observação:

O XenMobile oferece suporte apenas a mensagens SMS do Nexmo. Se você ainda não tem uma conta para usar as mensagens do Nexmo, visite o site deles para criar uma.

4. Configure estas definições:

- **Operadora:** Digite o nome da operadora.
- **Domínio do Gateway SMTP:** Digite o domínio associado ao gateway SMTP.
- **Código do país:** Clique no código do país da operadora na lista suspensa.

- **Prefixo de envio de e-mail:** Opcionalmente, especifique um prefixo de envio de e-mail.

5. Clique em **Adicionar** para adicionar a nova operadora ou clique em **Cancelar** para não adicionar a nova operadora.

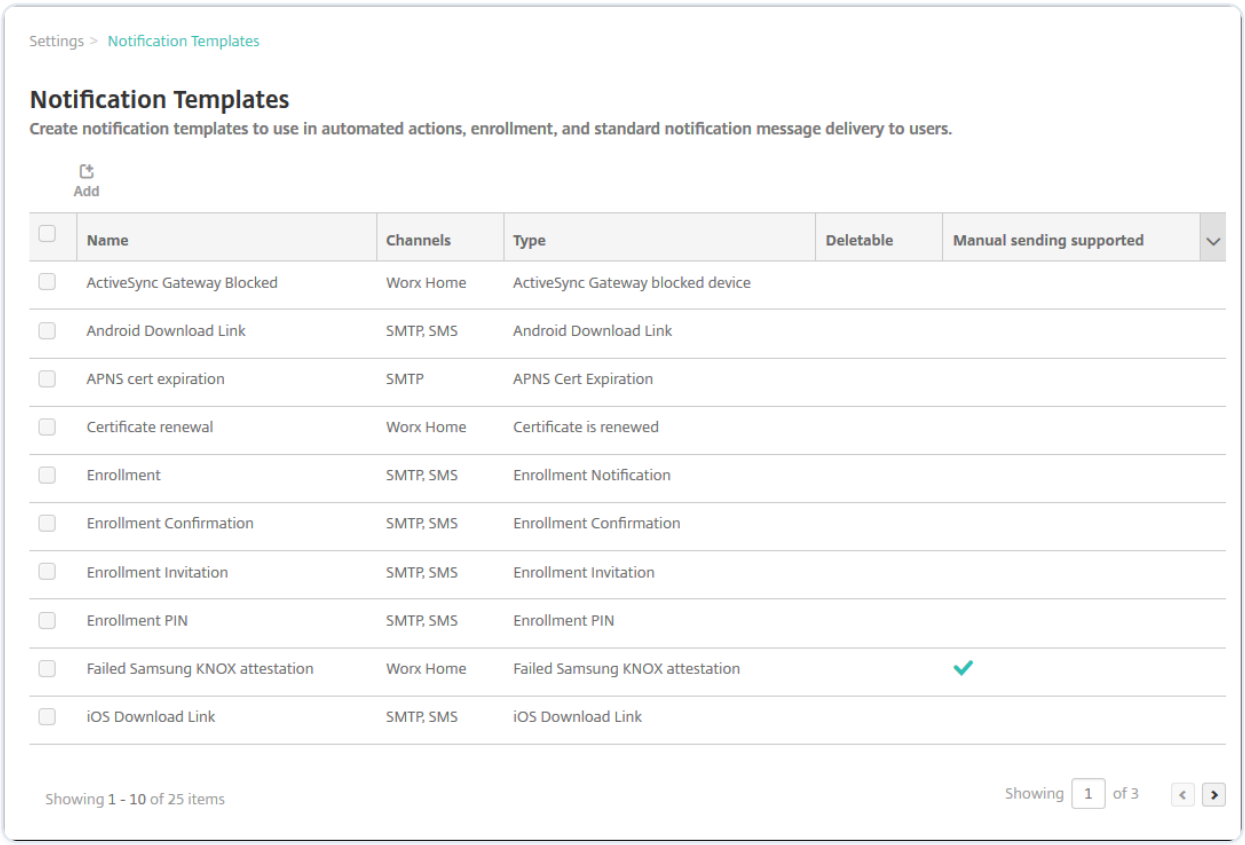
Criar e atualizar modelos de notificação

Você pode criar ou atualizar modelos de notificação no XenMobile para serem usados em ações automatizadas, registro e mensagens de notificação padrão enviadas aos usuários. Você configura os modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS.

O XenMobile inclui muitos modelos de notificação predefinidos que refletem os diferentes tipos de eventos aos quais o XenMobile responde automaticamente para cada dispositivo no sistema.

> **Observação:**
>
> Se você planeja usar canais SMTP ou SMS para enviar notificações aos usuários, você deve configurar os canais antes de poder ativá-los. O XenMobile solicita que você configure os canais ao adicionar modelos de notificação, caso eles ainda não estejam configurados.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Modelos de Notificação**. A página **Modelos de Notificação** é exibida.



Adicionar um modelo de notificação

1. Clique em **Adicionar**. Se nenhum gateway SMS ou servidor SMTP tiver sido configurado, uma mensagem será exibida sobre o uso de notificações SMS e SMTP. Você pode optar por configurar o servidor SMTP ou o gateway SMS agora ou configurá-los mais tarde.

   Se você optar por configurar as configurações do servidor SMS ou SMTP agora, será redirecionado para a página **Servidor de Notificação** na página **Configurações**. Depois de configurar os canais que deseja usar, você pode retornar à página **Modelo de Notificação** para continuar adicionando ou modificando modelos de notificação.

   > **Importante:**
   >
   > Se você optar por configurar as configurações do servidor SMS ou SMTP mais tarde, não poderá ativar esses canais ao adicionar ou editar um modelo de notificação, o que significa que esses canais não estarão disponíveis para o envio de notificações aos usuários.

2. Configure estas configurações:

   - **Nome:** Digite um nome descritivo para o modelo.

- **Descrição:** Digite uma descrição para o modelo.
- **Tipo:** Clique no tipo de notificação na lista suspensa. Apenas os canais suportados para o tipo selecionado aparecem. Apenas um modelo de Expiração de Certificado APNS é permitido, que é um modelo predefinido. Isso significa que você não pode adicionar um novo modelo deste tipo.

> **Nota:**
>
> Para alguns tipos de modelo, a frase Envio manual suportado aparece abaixo do tipo. Isso significa que o modelo está disponível na lista **Notificações** no **Painel** e na página **Dispositivos** para permitir que você envie manualmente a notificação aos usuários. O envio manual não está disponível em nenhum modelo que use as seguintes macros no campo Assunto ou Mensagem em qualquer canal:

- ${outofcompliance.reason(allowlist_blocklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

3. Em **Canais**, configure as informações para cada canal a ser usado com esta notificação. Você pode escolher qualquer um ou todos os canais. Os canais que você escolher dependem de como você deseja enviar as notificações:

   - Se você escolher **Secure Hub**, somente dispositivos iOS e Android recebem as notificações, que aparecem na bandeja de notificações do dispositivo.
   - Se você escolher **SMTP**, a maioria dos usuários recebe a mensagem porque eles se registraram com seus endereços de e-mail.
   - Se você escolher **SMS**, somente usuários que utilizam dispositivos com um cartão SIM recebem a notificação.

   Secure Hub:

   - **Ativar:** Clique para habilitar o canal de notificação.
   - **Mensagem:** Digite a mensagem a ser enviada ao usuário. Este campo é obrigatório se você estiver usando o Secure Hub. Para obter informações sobre como usar macros em uma mensagem, consulte Macros.
   - **Arquivo de Som:** Clique no som de notificação na lista suspensa que o usuário ouve quando a notificação é recebida.

SMTP:

- **Ativar:** Clique para habilitar o canal de notificação.

  Você pode ativar a notificação SMTP somente depois de configurar o servidor SMTP.
- **Remetente:** Digite um remetente opcional para a notificação, que pode ser um nome, um endereço de e-mail ou ambos.
- **Destinatário:** Este campo possui uma macro pré-construída para todas as notificações, exceto as Ad Hoc, para garantir que as notificações sejam enviadas para o endereço de destinatário SMTP correto. A Citrix recomenda que você não modifique macros em modelos. Você também pode adicionar destinatários (por exemplo, o administrador corporativo) além do usuário, adicionando seus endereços separados por um ponto e vírgula (;). Para enviar notificações Ad Hoc, você pode inserir destinatários específicos nesta página, ou pode selecionar dispositivos na página **Gerenciar > Dispositivos** e enviar notificações de lá. Para obter detalhes, consulte Dispositivos.
- **Assunto:** Digite um assunto descritivo para a notificação. Este campo é obrigatório.
- **Mensagem:** Digite a mensagem a ser enviada ao usuário. Para obter informações sobre como usar macros em uma mensagem, consulte Macros.

SMS:

- **Ativar:** Clique para habilitar o canal de notificação.

  Você pode ativar a notificação SMTP somente depois de configurar o servidor SMTP.
- **Destinatário:** Este campo possui uma macro pré-construída para todas as notificações, exceto as Ad Hoc, para garantir que as notificações sejam enviadas para o endereço de destinatário SMS correto. A Citrix recomenda que você não modifique macros em modelos. Para enviar notificações Ad Hoc, você pode inserir destinatários específicos ou selecionar dispositivos na página **Gerenciar > Dispositivos**.
- **Mensagem:** Digite a mensagem a ser enviada ao usuário. Este campo é obrigatório. Para obter informações sobre como usar macros em uma mensagem, consulte Macros.

4. Clique em **Adicionar**. Quando todos os canais estiverem configurados corretamente, eles aparecerão nesta ordem na página **Modelos de Notificação**: SMTP, SMS e Secure Hub. Quaisquer canais não configurados corretamente aparecerão após os canais configurados corretamente.

Editar um modelo de notificação

1. Selecione um modelo de notificação. A página de edição específica para esse modelo aparece, onde você pode fazer alterações em todos os campos, exceto o campo **Tipo**, e ativar ou desativar canais.
2. Clique em **Salvar**.

Excluir um modelo de notificação

Você pode excluir apenas os modelos de notificação que você adicionou. Você não pode excluir modelos de notificação predefinidos.

1. Selecione um modelo de notificação existente.
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.
3. Clique em **Excluir** para excluir o modelo de notificação ou clique em **Cancelar** para cancelar a exclusão do modelo de notificação.

Dispositivos

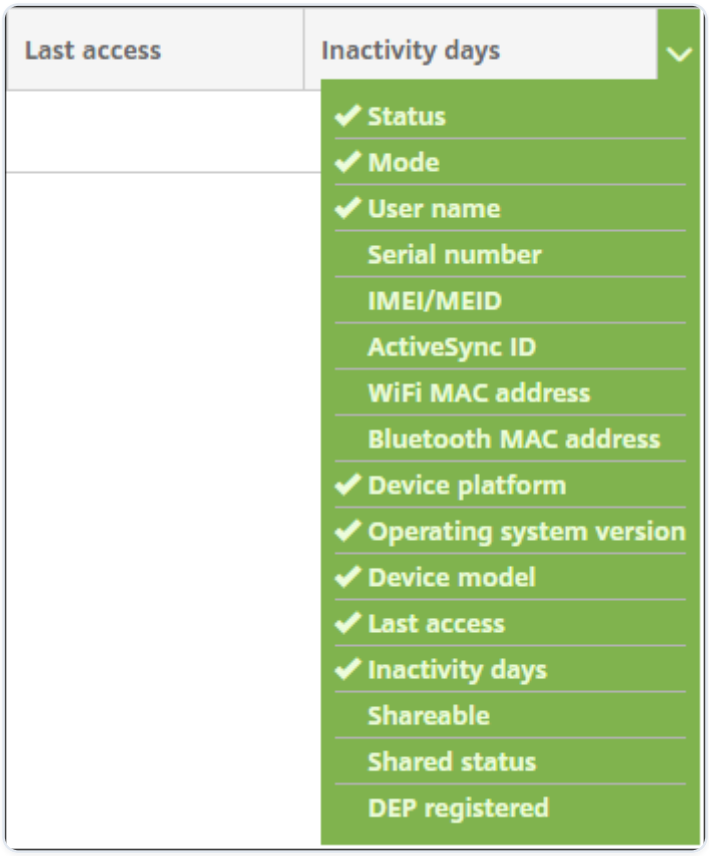
O Citrix XenMobile® pode provisionar, gerenciar, proteger e inventariar uma ampla gama de tipos de dispositivos em um único console de gerenciamento.

O banco de dados do XenMobile Server armazena uma lista de dispositivos móveis. Um número de série exclusivo ou um International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) define de forma exclusiva cada dispositivo móvel. Para preencher o console do XenMobile com seus dispositivos, você pode adicioná-los manualmente ou importar uma lista de dispositivos de um arquivo. Para obter mais informações sobre formatos de arquivo de provisionamento de dispositivos, consulte Formatos de arquivo de provisionamento de dispositivos mais adiante neste artigo.

A página **Dispositivos** no console do XenMobile lista cada dispositivo e as seguintes informações:

- **Status:** Ícones indicam se o dispositivo está com jailbreak, se é gerenciado, se o Active Sync Gateway está disponível e o estado de implantação.
- **Modo:** Se o modo do dispositivo é MDM, MAM ou ambos.
- Outras informações sobre o dispositivo, como **Nome de usuário**, **Plataforma do dispositivo**, **Versão do sistema operacional**, **Modelo do dispositivo**, **Último acesso** e **Dias de inatividade**. Esses cabeçalhos são os padrões exibidos.

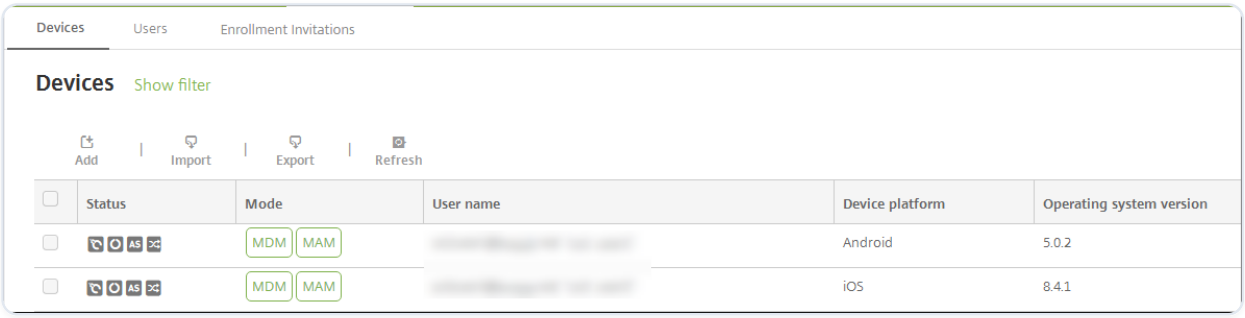
Para personalizar a tabela **Dispositivos**, clique na seta para baixo no último cabeçalho. Em seguida, selecione os cabeçalhos adicionais que você deseja ver na tabela ou desmarque quaisquer cabeçalhos para remover.



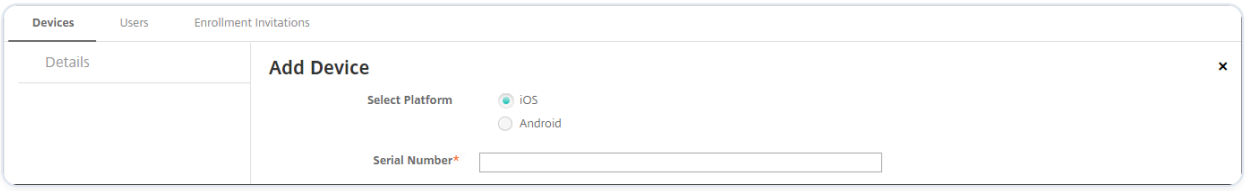
Você pode adicionar dispositivos manualmente, importar dispositivos de um arquivo de provisionamento de dispositivos, editar detalhes do dispositivo, realizar ações de segurança e enviar notificações para dispositivos. Você também pode exportar todos os dados da tabela de dispositivos para um arquivo .csv para criar um relatório personalizado. O servidor exporta todos os atributos do dispositivo. Se você aplicar filtros, o XenMobile usará os filtros ao criar o arquivo .csv.

Adicionar um dispositivo manualmente

1. No console do XenMobile, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



2. Clique em **Adicionar**. A página **Adicionar Dispositivo** é exibida.



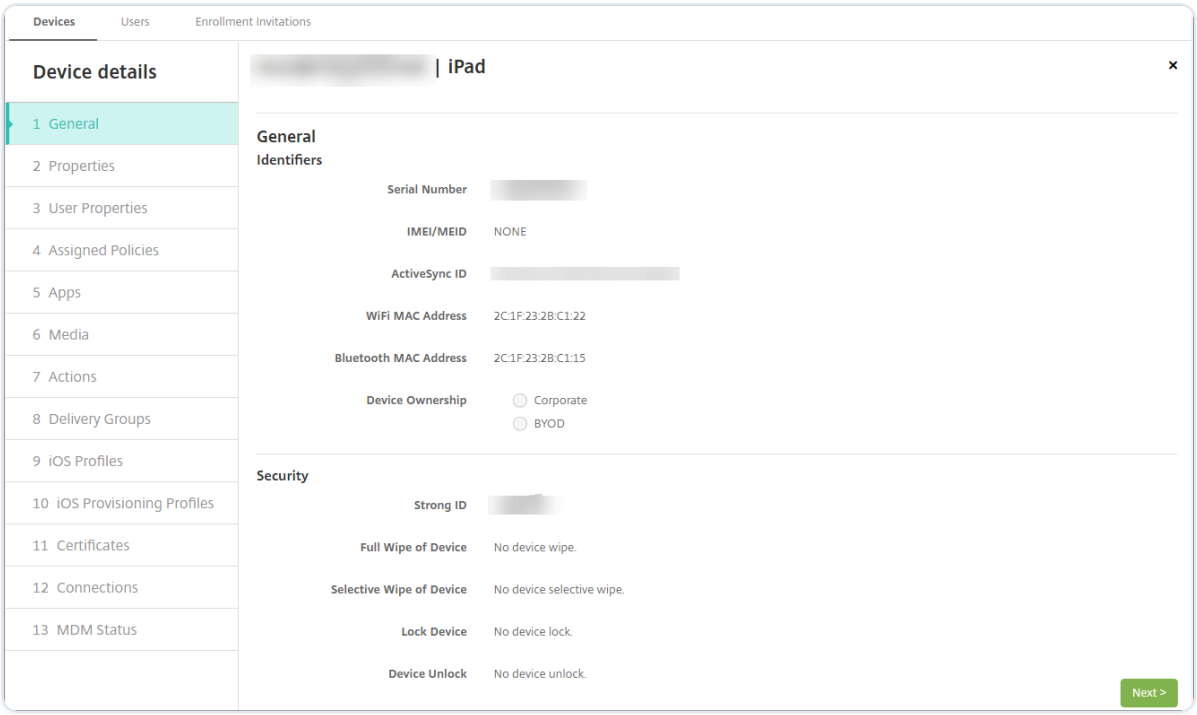
3. Configure estas configurações:

   - **Selecionar plataforma:** Clique em **iOS** ou **Android**.
   - **Número de Série:** Digite o número de série do dispositivo.
   - **IMEI/MEID:** Opcionalmente, apenas para dispositivos Android, digite as informações de IMEI/MEID do dispositivo.

4. Clique em **Adicionar**. A tabela **Dispositivos** aparece com o dispositivo adicionado ao final da lista. Escolha o dispositivo que você adicionou e, no menu que aparece, clique em **Editar** para visualizar e confirmar os detalhes do dispositivo.

> **Observação:**
>
> Quando você seleciona a caixa de seleção ao lado de um dispositivo, o menu de opções aparece acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de opções aparece no lado direito da listagem.

- XenMobile Server configurado no modo Enterprise (XME) ou MDM
- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
  - Um ou mais grupos locais.
  - Usuários locais atribuídos a grupos locais.
  - Grupos de entrega estão associados a grupos locais.
- Se estiver usando o Active Directory:
  - Grupos de entrega estão associados a grupos do Active Directory.



5. A página **Geral** lista os **Identificadores** do dispositivo, como número de série, ID do ActiveSync e outras informações para o tipo de plataforma. Para **Propriedade do Dispositivo**, selecione **Corporativo** ou **BYOD**.

   A página **Geral** também lista as propriedades de **Segurança** do dispositivo, como ID Forte, Bloquear Dispositivo, Ignorar Bloqueio de Ativação e outras informações para o tipo de plataforma. O campo **Limpeza Completa do Dispositivo** inclui o código PIN do usuário. O usuário deve inserir esse código após a limpeza do dispositivo. Se o usuário esquecer o código, você pode consultá-lo aqui.

6. A página **Propriedades** lista as propriedades do dispositivo que o XenMobile deve provisionar. Esta lista mostra todas as propriedades do dispositivo incluídas no arquivo de provisionamento usado para adicionar o dispositivo. Para adicionar uma propriedade, clique em **Adicionar** e selecione uma propriedade na lista. Para valores válidos para cada propriedade, consulte o PDF Nomes e valores das propriedades do dispositivo.

   Ao adicionar uma propriedade, ela aparece inicialmente na categoria onde você a adicionou. Depois de clicar em **Avançar** e retornar à página **Propriedades**, a propriedade aparece na lista apropriada.

   Para excluir uma propriedade, passe o mouse sobre a listagem e clique no **X** no lado direito. O XenMobile exclui o item imediatamente.

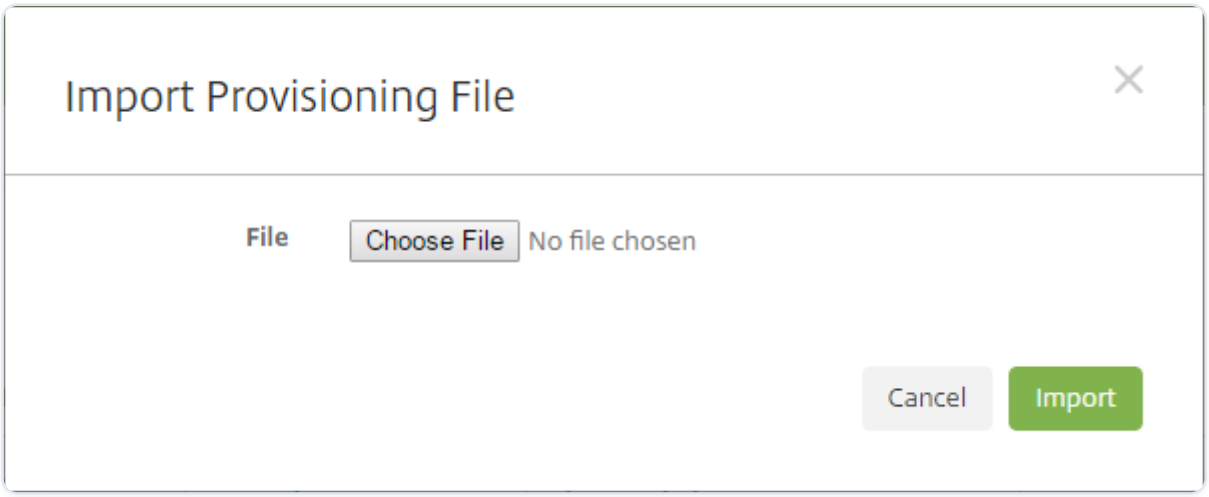
7. As seções restantes de **Detalhes do Dispositivo** contêm informações de resumo para o dispositivo.

- **Propriedades do Usuário:** Exibe funções RBAC, associações de grupo, contas de compra por volume e propriedades para o usuário. Você pode desativar uma conta de compra por volume a partir desta página.
- **Políticas Atribuídas:** Exibe o número de políticas atribuídas, incluindo o número de políticas implantadas, pendentes e com falha. Fornece o nome da política, tipo e informações da última implantação para cada política.
- **Aplicativos:** Exibe, para o último inventário, o número de implantações de aplicativos instaladas, pendentes e com falha. Fornece o nome do aplicativo, identificador, tipo e outras informações.
- **Mídia:** Exibe, para o último inventário, o número de implantações de mídia implantadas, pendentes e com falha.
- **Ações:** Exibe o número de ações implantadas, pendentes e com falha. Fornece o nome da ação e a hora da última implantação.
- **Grupos de Entrega:** Exibe o número de grupos de entrega bem-sucedidos, pendentes e com falha. Para cada implantação, fornece o nome do grupo de entrega e a hora da implantação. Selecione um grupo de entrega para visualizar informações mais detalhadas, incluindo status, ação e canal ou usuário.
- **Perfis iOS:** Exibe o último inventário de perfis iOS, incluindo nome, tipo, organização e descrição.
- **Perfis de Provisionamento iOS:** Exibe informações do perfil de provisionamento de distribuição empresarial, como o UUID, data de expiração e se é gerenciado.
- **Certificados:** Exibe, para certificados válidos, expirados ou revogados, informações como o tipo, provedor, emissor, número de série e o número de dias restantes antes da expiração.
- **Conexões:** Exibe o status da primeira conexão e o status da última conexão. Fornece para cada conexão, o nome de usuário, o tempo de autenticação penúltimo (penúltima) e o tempo da última autenticação.
- **Status do MDM:** Exibe informações como o status do MDM, a hora do último push e a hora da última resposta do dispositivo.

Importar dispositivos de um arquivo de provisionamento

Você pode importar um arquivo fornecido por operadoras de celular ou fabricantes de dispositivos, ou pode criar seu próprio arquivo de provisionamento de dispositivo. Para obter detalhes, consulte Formatos de arquivo de provisionamento de dispositivo mais adiante neste artigo.

1. Vá para **Gerenciar > Dispositivos** e clique em **Importar**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.

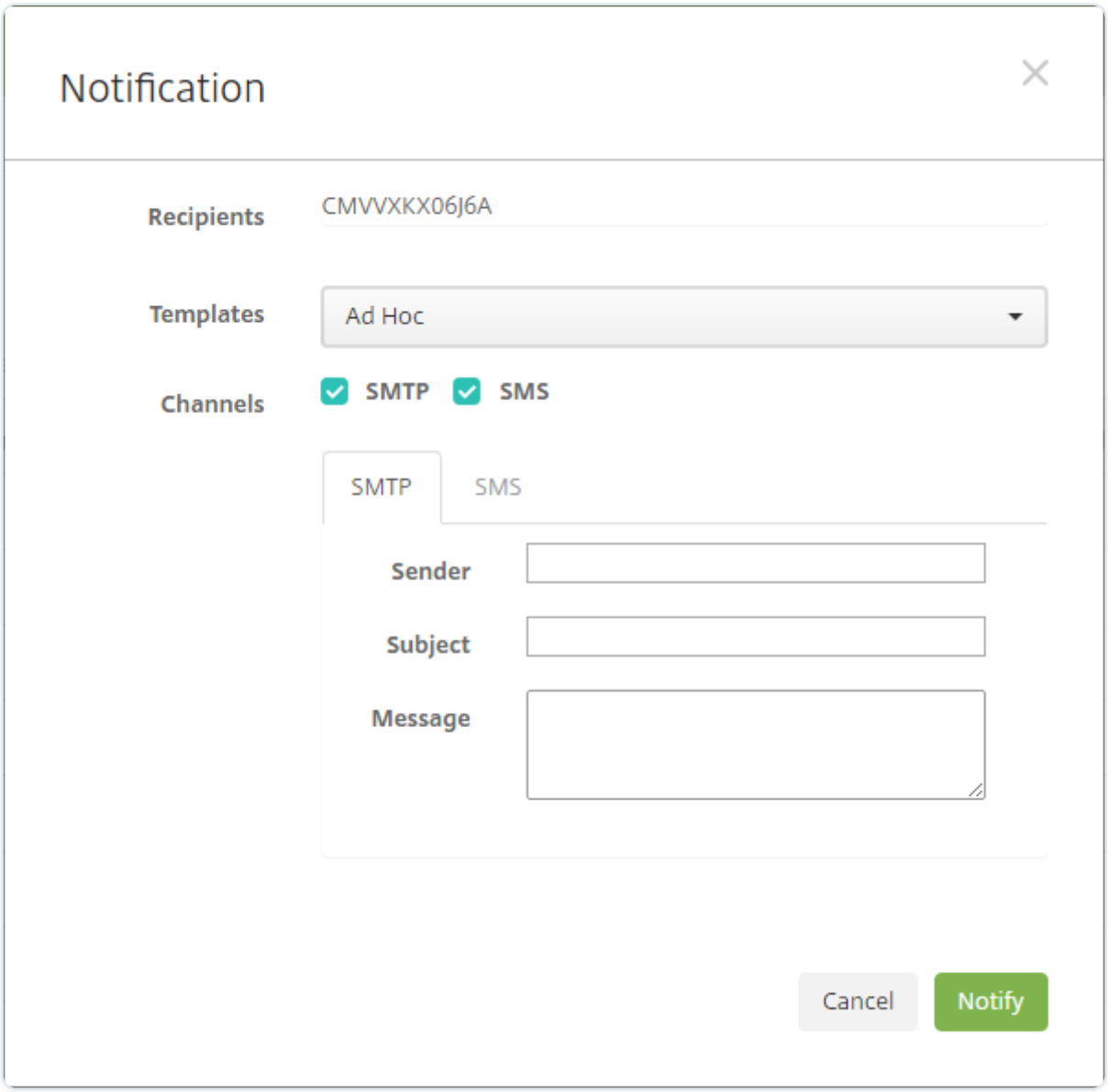


2. Clique em **Escolher Arquivo** e, em seguida, navegar até o arquivo que deseja importar.
3. Clique em **Importar**. A tabela **Dispositivos** lista o arquivo importado.
4. Para editar as informações do dispositivo, selecione-o e clique em **Editar**. Para obter informações sobre as páginas de **Detalhes do dispositivo**, consulte Adicionar um dispositivo manualmente.

Enviar uma notificação para dispositivos

Você pode enviar notificações para dispositivos a partir da página Dispositivos. Para obter mais informações sobre notificações, consulte Notificações.

1. Na página **Gerenciar > Dispositivos**, selecione o dispositivo ou os dispositivos para os quais você deseja enviar uma notificação.
2. Clique em **Notificar**. A caixa de diálogo **Notificação** é exibida. O campo **Destinatários** lista todos os dispositivos que receberão a notificação.



3. Configure estas configurações:

    - **Modelos:** Na lista, clique no tipo de notificação que você deseja enviar. Para cada modelo, exceto **Ad Hoc**, os campos **Assunto** e **Mensagem** mostram o texto configurado para o modelo que você escolher.
    - **Canais:** Selecione como enviar a mensagem. O padrão é **SMTP** e **SMS**. Clique nas abas para ver o formato da mensagem para cada canal.
    - **Remetente:** Insira um remetente opcional.
    - **Assunto:** Insira um assunto para uma mensagem **Ad Hoc**.
    - **Mensagem:** Insira a mensagem para uma mensagem **Ad Hoc**.

4. Clique em **Notificar**.

Exportar a tabela Dispositivos

1. Filtre a tabela **Dispositivos** de acordo com o que você deseja que apareça no arquivo de exportação.
2. Clique no botão **Exportar** acima da tabela **Dispositivos**. O XenMobile extrai as informações da tabela **Dispositivos** filtrada e as converte para um arquivo .csv.
3. Quando solicitado, abra ou salve o arquivo .csv.

Marcar dispositivos de usuário manualmente

Você pode marcar um dispositivo manualmente no XenMobile das seguintes maneiras:

- Durante o processo de registro baseado em convite.
- Durante o processo de registro do Portal de Autoatendimento.
- Ao adicionar a propriedade de posse do dispositivo como uma propriedade do dispositivo

Você tem a opção de marcar o dispositivo como corporativo ou de propriedade do funcionário. Ao usar o Portal de Autoatendimento para auto-registrar um dispositivo, você pode marcar o dispositivo como corporativo ou de propriedade do funcionário. Você também pode marcar um dispositivo manualmente, da seguinte forma.

1. Adicione uma propriedade ao dispositivo na guia **Dispositivos** no console do XenMobile.
2. Adicione a propriedade chamada **Propriedade de** e escolha **Corporativo** ou **BYOD** (de propriedade do funcionário).

   Imagem das configurações da propriedade Propriedade de(/en-us/xenmobile/server/media/manage-devices-properties-owned-by.png)

Formatos de arquivo de provisionamento de dispositivo

Muitas operadoras de celular ou fabricantes de dispositivos fornecem listas de dispositivos móveis autorizados. Você pode usar essas listas para evitar ter que inserir uma longa lista de dispositivos móveis manualmente. O XenMobile suporta um formato de arquivo de importação comum a todos os três tipos de dispositivos suportados: Android, iOS e Windows.

Um arquivo de provisionamento que você cria manualmente e usa para importar dispositivos para o XenMobile deve estar no seguinte formato:

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

Tenha em mente o seguinte:

- Para valores válidos para cada propriedade, consulte o PDF Nomes e valores de propriedades de dispositivo.
- Use o conjunto de caracteres UTF-8.
- Use um ponto e vírgula (;) para separar os campos dentro do arquivo de provisionamento. Se parte de um campo contiver um ponto e vírgula, escape-o com um caractere de barra invertida (\\).

  Por exemplo, para esta propriedade:

  `propertyV;test;1;2`

  Faça o escape da seguinte forma:

  `propertyV\;test\;1\;2`
- O número de série é obrigatório para dispositivos iOS porque o número de série é o identificador do dispositivo iOS.
- Para outras plataformas de dispositivo, você deve incluir o número de série ou o IMEI.
- Os valores válidos para **OperatingSystemFamily** são **WINDOWS**, **ANDROID** ou **iOS**.

Exemplo de um arquivo de provisionamento de dispositivo:

```
`1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;`
```

Cada linha no arquivo descreve um dispositivo. A primeira entrada no exemplo acima significa o seguinte:

- Número de Série: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`

- Família do Sistema Operacional: `WINDOWS`
- Nome da Propriedade: `propertyN`
- Valor da Propriedade: `propertyV\;test\;1\;2;prop 2`

Gateway ActiveSync

ActiveSync é um protocolo de sincronização de dados móveis desenvolvido pela Microsoft. O ActiveSync sincroniza dados com dispositivos portáteis e computadores de mesa (ou laptops).

Você pode configurar as regras do Gateway ActiveSync no XenMobile. Com base nessas regras, você pode permitir ou negar o acesso de dispositivos aos dados do ActiveSync. Por exemplo, se você ativar a regra Aplicativos Necessários Ausentes, o XenMobile verifica a Política de Acesso a Aplicativos para aplicativos necessários e nega o acesso aos dados do ActiveSync se os aplicativos necessários estiverem ausentes. Para cada regra, você pode escolher **Permitir** ou **Negar**. A configuração padrão é **Permitir**.

Para obter mais informações sobre a política de dispositivo de acesso a aplicativos, consulte Política de dispositivo de acesso a aplicativos.

O XenMobile oferece suporte às seguintes regras:

Dispositivos Anônimos: Verifica se um dispositivo está no modo anônimo. Essa verificação está disponível se o XenMobile não conseguir re-autenticar o usuário quando um dispositivo tentar se reconectar.

Atestado Samsung KNOX com falha: Verifica se um dispositivo falhou em uma consulta ao servidor de atestado Samsung KNOX.

Aplicativos Proibidos: Verifica se um dispositivo tem aplicativos proibidos, conforme definido em uma política de Acesso a Aplicativos.

Permissão e Negação Implícitas: Esta ação é o padrão para o Gateway ActiveSync. O gateway cria uma Lista de Dispositivos de todos os dispositivos que não atendem a nenhum dos outros critérios de regra de filtro e permite ou nega conexões com base nessa lista. Se nenhuma regra corresponder, o padrão é Permitir Implícito.

Dispositivos Inativos: Verifica se um dispositivo está inativo conforme definido pela configuração **Limite de Dias de Inatividade do Dispositivo** em **Propriedades do Servidor**.

Aplicativos Necessários Ausentes: Verifica se um dispositivo está sem os aplicativos necessários, conforme definido em uma política de Acesso a Aplicativos.

Aplicativos Não Sugeridos: Verifica se um dispositivo tem aplicativos não sugeridos, conforme definido em uma política de Acesso a Aplicativos.

Senha Não Conforme: Verifica se a senha do usuário está em conformidade. Em dispositivos iOS e Android, o XenMobile pode determinar se a senha atualmente no dispositivo está em conformidade com a política de senha enviada ao dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de senha para o dispositivo. Antes que o usuário defina a senha, a senha pode não estar em conformidade.

Dispositivos Fora de Conformidade: Verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Fora de Conformidade. Essa propriedade geralmente é alterada pelas ações automatizadas ou por terceiros que utilizam as APIs do XenMobile.

Status Revogado: Verifica se o certificado do dispositivo foi revogado. Um dispositivo revogado não pode ser reinscrito até que seja autorizado novamente.

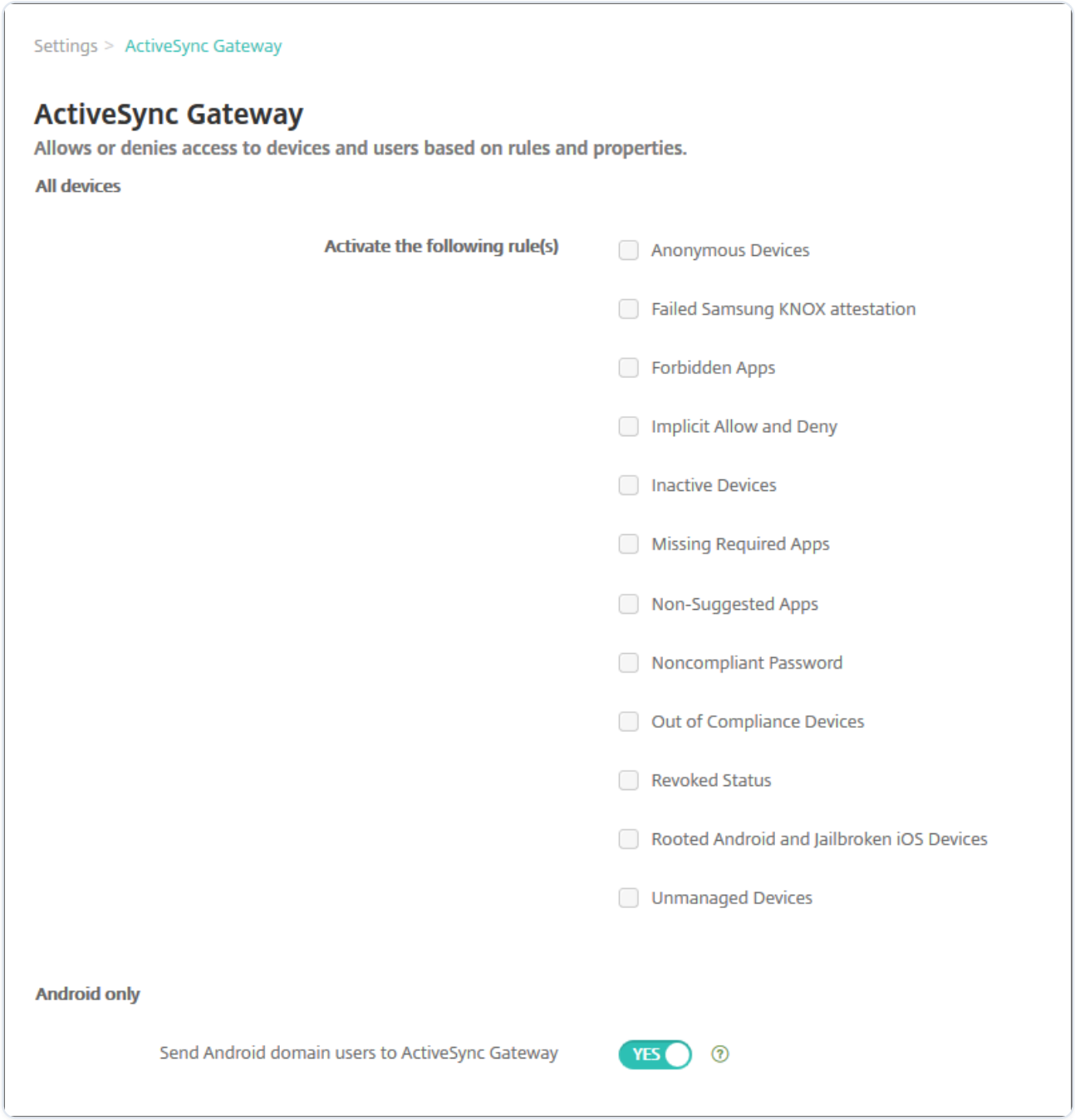
Dispositivos Android com root e iOS com jailbreak: Verifica se um dispositivo Android ou iOS tem jailbreak.

Dispositivos Não Gerenciados: Verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo registrado no MAM ou um dispositivo não registrado não é gerenciado.

Enviar usuários de domínio Android para o ActiveSync Gateway: Clique em **SIM** para garantir que o XenMobile envie informações de dispositivos Android para o ActiveSync Gateway.

Para configurar as definições do ActiveSync Gateway

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **ActiveSync Gateway**. A página **ActiveSync Gateway** é exibida.



1. Em **Ativar as seguintes regras**, selecione uma ou mais regras que você deseja ativar.
2. Em **Somente Android**, em **Enviar usuários de domínio Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie informações de dispositivos Android para o ActiveSync Gateway.
3. Clique em **Salvar**.

Migrar da administração de dispositivos para o Android Enterprise

Este artigo discute considerações e recomendações para migrar da administração de dispositivos Android legada para o Android Enterprise. O Google está descontinuando a API de Administração de Dispositivos Android. Essa API suportava aplicativos corporativos em dispositivos Android. O Android Enterprise é a solução de gerenciamento moderna recomendada pelo Google e pela Citrix.

O XenMobile® está mudando para o Android Enterprise como método de registro padrão para dispositivos Android. Depois que o Google descontinuar as APIs, o registro falhará para dispositivos Android Q no modo de administração de dispositivos.

O Android Enterprise inclui suporte para modos de dispositivo totalmente gerenciado e perfil de trabalho. A publicação do Google, Android Enterprise Migration Bluebook, explica em detalhes como a administração de dispositivos legada e o Android Enterprise diferem. Recomendamos que você leia as informações de migração do Google.

Essa publicação também descreve as quatro fases da migração da administração de dispositivos e inclui o diagrama a seguir. Este artigo inclui recomendações específicas do XenMobile para as fases de migração.

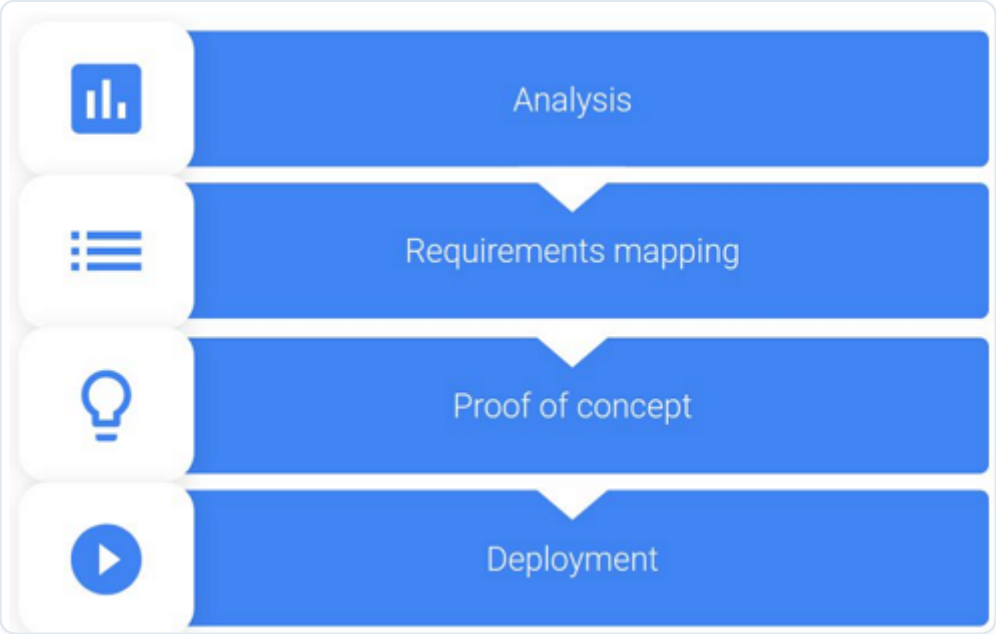


Diagrama do Android Enterprise Migration Bluebook. Republicado com a permissão do Google.

Impacto da descontinuação da administração de dispositivos

O Google descontinua as seguintes APIs de Administração de Dispositivos. Essas APIs não funcionarão em dispositivos que executam o Android Q depois que você atualizar o Secure Hub para ter como alvo o nível da API do Android Q:

- Desativar câmera: Controla o acesso às câmeras do dispositivo.
- Expirar senha: Força os usuários a alterar sua senha após um período configurável.
- Limitar senha: Define requisitos de senha restritivos.

As APIs descontinuadas não têm impacto em dispositivos registrados no modo somente MAM do Citrix.

Recomendações

As seguintes recomendações são para dispositivos já registrados no modo de administração de dispositivos Android legado, dispositivos não registrados e dispositivos registrados no modo somente MAM do Citrix.

STATUS DE REGISTRO DO DISPOSITIVO	AÇÃO RECOMENDADA
Um dispositivo existente está registrado no modo de administração do dispositivo e pode ser atualizado para o Android Q.	Antes de atualizar o dispositivo para o Android Q, migre do modo de administração do dispositivo para o Android Enterprise.
Um dispositivo existente está registrado no modo de administração do dispositivo. O dispositivo não pode ser atualizado para o Android Q.	O dispositivo pode permanecer no modo de administração do dispositivo. No entanto, planeje mover o dispositivo para o Android Enterprise na atualização do dispositivo.
Um dispositivo existente está registrado no modo de administração do dispositivo e foi atualizado para o Android Q.	Migre do modo de administração do dispositivo para o Android Enterprise antes que o Google descontinue as APIs. Uma mensagem de aviso para esses dispositivos aparece no console do XenMobile.
Novo dispositivo entregue com Android Q e registrado no modo de administração do dispositivo.	Migre do modo de administração do dispositivo para o Android Enterprise antes que o Google descontinue as APIs. Uma mensagem de aviso para esses dispositivos aparece no console do XenMobile.

STATUS DE REGISTRO DO DISPOSITIVO	AÇÃO RECOMENDADA
Novo dispositivo entregue com ou atualizável para Android Q. O dispositivo não está registrado.	Use o Android Enterprise para quaisquer novos dispositivos.
Dispositivo novo ou existente no Android Q é registrado no modo de administração do dispositivo depois que o Google descontinua as APIs.	Para evitar os impactos das APIs do Google descontinuadas, a Citrix recomenda migrar para o Android Enterprise antes que o Google descontinue as APIs. Após essa data, os registros desses dispositivos falharão.
Dispositivos novos ou existentes registrados no modo somente MAM do Citrix	Nenhuma ação necessária. As APIs do Google descontinuadas não têm impacto em dispositivos no modo somente MAM.

Análise

A fase de análise da migração consiste em:

- Compreender sua configuração Android legada
- Documentar sua configuração legada para que você possa mapear recursos legados para recursos do Android Enterprise

Análise recomendada

1. Avalie o Android Enterprise no XenMobile: Totalmente gerenciado, totalmente gerenciado com perfil de trabalho, dispositivo dedicado, perfil de trabalho (BYOD).
2. Analise seus recursos atuais de administração de dispositivos em relação ao Android Enterprise.
3. Documente seus casos de uso de administração de dispositivos.

Para documentar seus casos de uso de administração de dispositivos:

1. Crie uma planilha e liste os grupos de políticas atuais em seu console XenMobile.
2. Crie casos de uso separados com base nos grupos de políticas existentes.
3. Para cada caso de uso, documente o seguinte:
    - Nome
    - Proprietário da empresa

- Modelo de identidade do usuário
- Requisitos do dispositivo
  - Segurança
  - Gerenciamento
  - Usabilidade
- Inventário de dispositivos
  - Marca e modelo
  - Versão do SO
- Aplicativos

4. Para cada aplicativo, liste:
   - Nome do aplicativo
   - Nome do pacote
   - Método de hospedagem
   - Se o aplicativo é público ou privado
   - Se o aplicativo é obrigatório (verdadeiro/falso)

Mapeamento de requisitos

Com base na análise concluída, determine seus requisitos de recursos do Android Enterprise.

Mapeamento de requisitos recomendado

1. Determine o modo de gerenciamento e o método de registro:
   - Perfil de trabalho (BYOD): Requer novo registro. Nenhuma redefinição de fábrica é necessária.
   - Totalmente gerenciado: Requer redefinição de fábrica. Registre dispositivos usando código QR, comunicação de campo próximo (NFC) bump, identificador de controlador de política de dispositivo (DPC), zero touch.
2. Crie uma estratégia de migração de aplicativos.
3. Mapeie os requisitos de caso de uso para os recursos do Android Enterprise. Documente o recurso para cada requisito de dispositivo que mais se aproxima do requisito e sua versão Android correspondente.

4. Determine o SO Android mínimo com base nos requisitos de recursos (7.0, 8.0, 9.0).
5. Escolha um modelo de identidade:
    - Recomendado: Conta do Google Play Gerenciada
    - Use contas do Google G-Suite somente se você for um cliente do Google Cloud Identity
6. Crie uma estratégia de dispositivo:
    - Nenhuma ação: Se os dispositivos atenderem ao nível mínimo do SO
    - Atualização: Se os dispositivos suportarem e puderem ser atualizados para o SO compatível
    - Substituir: Se os dispositivos não puderem ser atualizados para o nível de SO compatível

Estratégia de migração de aplicativos recomendada

Depois de concluir o mapeamento de requisitos, mova os aplicativos da plataforma Android para a plataforma Android Enterprise. Para obter detalhes sobre a publicação de aplicativos, consulte Adicionar aplicativos.

- Aplicativos da loja pública

    a. Selecione os aplicativos a serem migrados e, em seguida, edite os aplicativos para desmarcar a configuração do Google Play e selecione **Android Enterprise** como a plataforma.

    b. Selecione o grupo de entrega. Se um aplicativo for obrigatório, mova o aplicativo para a lista **Aplicativos Obrigatórios** no grupo de entrega.

    Depois de salvar um aplicativo, ele aparece na Google Play Store. Se você tiver um perfil de trabalho, os aplicativos aparecerão na Google Play Store no perfil de trabalho.

- Aplicativos privados (corporativos)

    Os aplicativos privados são desenvolvidos internamente ou por um desenvolvedor terceirizado. Recomendamos que você publique aplicativos privados usando o Google Play.

    a. Selecione os aplicativos a serem migrados e, em seguida, edite os aplicativos para selecionar **Android Enterprise** como a plataforma.

    b. Carregue o arquivo APK e, em seguida, configure as configurações do aplicativo.

    c. Publique o aplicativo no grupo de entrega necessário.

- Aplicativos MDX

a. Selecione os aplicativos a serem migrados e, em seguida, edite os aplicativos para selecionar **Android Enterprise** como a plataforma.
b. Carregue o arquivo MDX. Passe pelo processo de aprovação do aplicativo.
c. Selecione as políticas MDX.

Para aplicativos MDX Enterprise, recomendamos alterá-los para aplicativos empacotados no modo MDX SDK:

- Opção 1: Hospede o APK no Google Play com uma conta de desenvolvedor atribuída privadamente à sua organização. Publique o arquivo MDX no XenMobile.
- Opção 2: Publique o aplicativo do XenMobile como um aplicativo empresarial. Publique o APK no XenMobile e selecione a plataforma **Android Enterprise** para o arquivo MDX.

Migração da política de dispositivo Citrix

Para políticas disponíveis para as plataformas Android e Android Enterprise: Edite a política e selecione a plataforma **Android Enterprise**.

Para o Android Enterprise, considere o modo de registro. Algumas opções de política estão disponíveis apenas para dispositivos no modo de perfil de trabalho ou no modo totalmente gerenciado.

Prova de conceito

Após migrar os aplicativos para o Android Enterprise, você pode configurar um teste de migração para verificar se os recursos estão funcionando conforme o esperado.

Configuração recomendada para prova de conceito

1. Configure a infraestrutura de implantação:
   - Crie um Grupo de Entrega para seu teste de Android Enterprise.
   - Configure o Android Enterprise no XenMobile.
2. Configure os aplicativos do usuário.
3. Configure os recursos do Android Enterprise.
4. Atribuir políticas ao grupo de entrega do Android Enterprise.
5. Testar e confirmar recursos.
6. Concluir um passo a passo de configuração do dispositivo para cada caso de uso.
7. Documentar as etapas de configuração do usuário.

Implantação

Agora você pode implantar sua configuração do Android Enterprise e preparar seus usuários para a migração.

Estratégia de implantação recomendada

A estratégia de implantação recomendada pela Citrix é testar todos os seus sistemas de produção para o Android Enterprise e, em seguida, concluir a migração do dispositivo mais tarde.

- Neste cenário, os usuários continuam a usar dispositivos legados com sua configuração atual. Você configura novos dispositivos para o gerenciamento do Android Enterprise.
- Migre os dispositivos existentes apenas quando uma atualização ou substituição for necessária.
- Migre os dispositivos existentes para o gerenciamento do Android Enterprise no final de seu ciclo de vida usual. Ou, migre esses dispositivos quando eles precisarem ser substituídos devido a perda ou quebra.

Android Enterprise

Android Enterprise é um conjunto de ferramentas e serviços fornecidos pelo Google como uma solução de gerenciamento empresarial para dispositivos Android. Com o Android Enterprise:

- Você usa o XenMobile® para gerenciar dispositivos Android de propriedade da empresa e dispositivos Android de uso pessoal (BYOD).
- Você pode gerenciar o dispositivo inteiro ou um perfil separado no dispositivo. O perfil separado isola contas, aplicativos e dados corporativos de contas, aplicativos e dados pessoais.
- Você também pode gerenciar dispositivos dedicados a um único uso, como gerenciamento de inventário. Para uma visão geral dos recursos do Android Enterprise do Google, consulte Gerenciamento do Android Enterprise.

Recursos:

- Para uma lista de termos e definições relacionados ao Android Enterprise, consulte terminologia do Android Enterprise no guia do desenvolvedor do Google Android Enterprise. O Google atualiza esses termos com frequência.
- Para sistemas operacionais Android compatíveis com o XenMobile, consulte Sistemas operacionais de dispositivos compatíveis.

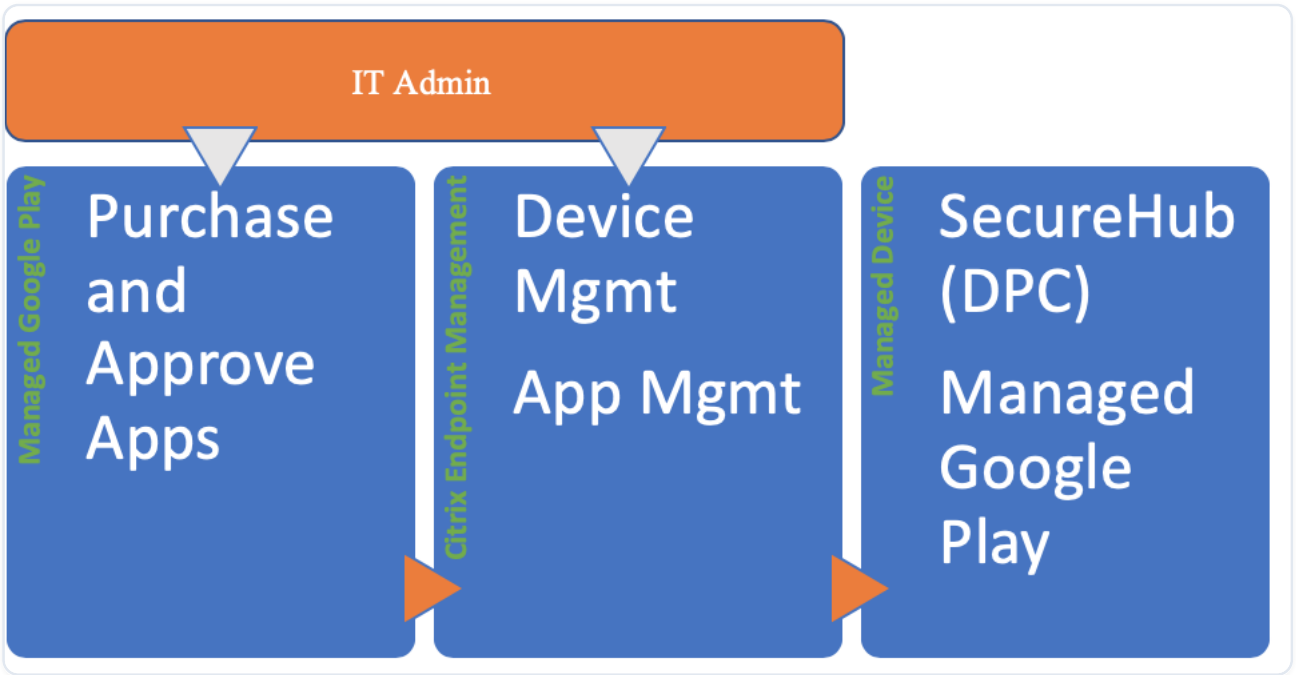
- Para obter informações sobre as conexões de saída a serem consideradas ao configurar ambientes de rede para o Android Enterprise, consulte o artigo de suporte do Google, Requisitos de Rede do Android Enterprise.

Ao integrar o XenMobile com o Google Play gerenciado para usar o Android Enterprise, você cria uma empresa. O Google define uma empresa como uma ligação entre a organização e sua solução de gerenciamento de mobilidade empresarial (EMM). Todos os usuários e dispositivos que a organização gerencia por meio de sua solução pertencem à sua empresa.

Uma empresa para Android Enterprise possui três componentes: uma solução EMM, um aplicativo de controlador de política de dispositivo (DPC) e uma plataforma de aplicativos empresariais do Google. Ao integrar o XenMobile com o Android Enterprise, a solução completa possui estes componentes:

- **XenMobile:** O EMM da Citrix. O XenMobile é a solução unificada do XenMobile para um espaço de trabalho digital seguro. O XenMobile fornece os meios para que os administradores de TI gerenciem dispositivos e aplicativos para suas organizações.
- **Citrix Secure Hub™:** O aplicativo DPC da Citrix. O Secure Hub é o ponto de partida para o XenMobile. O Secure Hub impõe políticas no dispositivo.
- **Google Play Gerenciado:** Uma plataforma de aplicativos empresariais do Google que se integra ao XenMobile. A API EMM do Google Play define políticas de aplicativos e distribui aplicativos.

Esta ilustração mostra como os administradores interagem com esses componentes e como os componentes interagem entre si:



Usando o Google Play gerenciado com o XenMobile

> **Nota:**
>
> Você pode usar o Google Play gerenciado ou o Google Workspace para registrar a Citrix como seu provedor EMM. Este artigo discute o uso do Android Enterprise com o Google Play gerenciado. Se sua organização usa o Google Workspace para fornecer acesso a aplicativos, você pode usá-lo com o Android Enterprise. Consulte Android Enterprise herdado para clientes do Google Workspace (anteriormente G-Suite).

> Ao usar o Google Play gerenciado, você provisiona Contas do Google Play gerenciadas para dispositivos e usuários finais. As Contas do Google Play gerenciadas fornecem acesso ao Google Play gerenciado, permitindo que os usuários instalem e usem os aplicativos que você disponibiliza. Se sua organização usa um serviço de identidade de terceiros, você pode vincular Contas do Google Play gerenciadas às suas contas de identidade existentes.

Como esse tipo de empresa não está vinculado a um domínio, você pode criar mais de uma empresa para uma única organização. Por exemplo, cada departamento ou região dentro de uma organização pode se registrar como uma empresa diferente para gerenciar conjuntos separados de dispositivos e aplicativos.

Para administradores do XenMobile, o Google Play gerenciado combina a experiência do usuário e os recursos da loja de aplicativos do Google Play com um conjunto de recursos de gerenciamento projetados para empresas. Você usa o Google Play gerenciado para adicionar, comprar e aprovar aplicativos para implantação no espaço de trabalho do Android Enterprise em um dispositivo. Você pode usar o Google Play para implantar aplicativos públicos, aplicativos privados e aplicativos de terceiros.

Para usuários de dispositivos gerenciados, o Google Play gerenciado é a loja de aplicativos corporativos. Os usuários podem navegar pelos aplicativos, visualizar detalhes dos aplicativos e instalá-los. Ao contrário da versão pública do Google Play, os usuários só podem instalar aplicativos do Google Play gerenciado que você disponibiliza para eles.

Cenários de implantação de dispositivos e modos de operação

O cenário de implantação de dispositivos refere-se a quem possui os dispositivos que você implanta e como você os gerencia. Os perfis de dispositivo referem-se a como o DPC gerencia e aplica políticas nos dispositivos.

Um perfil de trabalho isola contas comerciais, aplicativos e dados de contas pessoais, aplicativos e dados. Para obter mais detalhes sobre perfis de trabalho, consulte o tópico de ajuda do Google Android Enterprise, O que é um perfil de trabalho.

Importante:

Quando os dispositivos Android Enterprise são atualizados para o Android 11, o Google migra os dispositivos gerenciados como "totalmente gerenciados com um perfil de trabalho" para uma nova experiência de perfil de trabalho com segurança aprimorada. Para obter mais informações, consulte Mudanças futuras para o Android Enterprise totalmente gerenciado com perfil de trabalho.

GERENCIAMENTO DE DISPOSITIVOS	CASOS DE USO	PERFIL DE TRABALHO	PERFIL PESSOAL	NOTAS
Dispositivos de propriedade da empresa (totalmente gerenciados)	Dispositivos de propriedade da empresa destinados apenas para uso profissional	Não	Sim. O DPC pode realizar ações em todo o dispositivo, como configurar a conectividade em todo o dispositivo, configurar as definições globais e fazer uma redefinição de fábrica.	Apenas para dispositivos novos ou redefinidos de fábrica.
Totalmente gerenciado com um perfil de trabalho	Dispositivos de propriedade da empresa destinados para uso	Sim	Sim. Duas cópias do DPC são executadas nesses dispositivos:	Anteriormente conhecidos como dispositivos corporativos habilitados

GERENCIAMENTO DE DISPOSITIVOS	CASOS DE USO	PERFIL DE TRABALHO	PERFIL PESSOAL	NOTAS
	profissional e pessoal		Uma gerencia o dispositivo no modo proprietário do dispositivo e a outra gerencia o perfil de trabalho no modo proprietário do perfil. Você pode aplicar políticas separadas ao dispositivo e ao perfil de trabalho.	para uso pessoal (COPE).
Dispositivos dedicados*	Dispositivos de propriedade da empresa configurados para um único caso de uso, como sinalização digital ou impressão de bilhetes	Não	Sim. Você fornece apenas os aplicativos necessários e impede que os usuários adicionem outros aplicativos.	Anteriormente conhecidos como dispositivos de uso único de propriedade corporativa (COSU).

GERENCIAMENTO DE DISPOSITIVOS	CASOS DE USO	PERFIL DE TRABALHO	PERFIL PESSOAL	NOTAS
Perfil de trabalho BYOD**	Dispositivos pessoais registrados no modo de perfil de trabalho (também conhecido como modo de proprietário de perfil)	Sim	Sim. O DPC gerencia apenas o perfil de trabalho, não o dispositivo inteiro.	Esses dispositivos não precisam ser novos ou ter sido redefinidos de fábrica.

* Os usuários podem compartilhar um dispositivo dedicado. Quando um usuário faz login em um aplicativo em um dispositivo dedicado, o estado do seu trabalho está com o aplicativo, não com o dispositivo.

** O XenMobile não oferece suporte a dispositivos Zebra no modo de perfil de trabalho BYOD. O XenMobile oferece suporte a dispositivos Zebra como dispositivos totalmente gerenciados e no modo legado de dispositivo (também chamado de modo de administrador de dispositivo).

Para obter informações sobre como migrar do modo legado para o modo de proprietário de dispositivo ou proprietário de perfil, consulte Migrar da administração de dispositivo para o Android Enterprise.

Métodos de autenticação

Os perfis de registro determinam se os dispositivos Android são registrados em MAM, MDM ou MDM+MAM, com a opção para os usuários optarem por não usar o MDM.

Para obter informações sobre como especificar o nível de segurança e as etapas de registro necessárias, consulte Configurar modos de segurança de registro.

O XenMobile oferece suporte aos seguintes métodos de autenticação para dispositivos Android registrados em MDM+MAM. Para obter informações, consulte os artigos em Certificados e autenticação.

- Domínio
- Domínio mais token de segurança

- Certificado de cliente
- Certificado de cliente mais domínio
- Provedores de identidade:
  - Azure Active Directory
  - Provedor de identidade Citrix

Outro método de autenticação raramente usado é o certificado de cliente mais token de segurança. Para obter informações, consulte `<https://support.citrix.com/article/CTX215200>`.

Requisitos

Antes de começar a usar o Android Enterprise, você precisa:

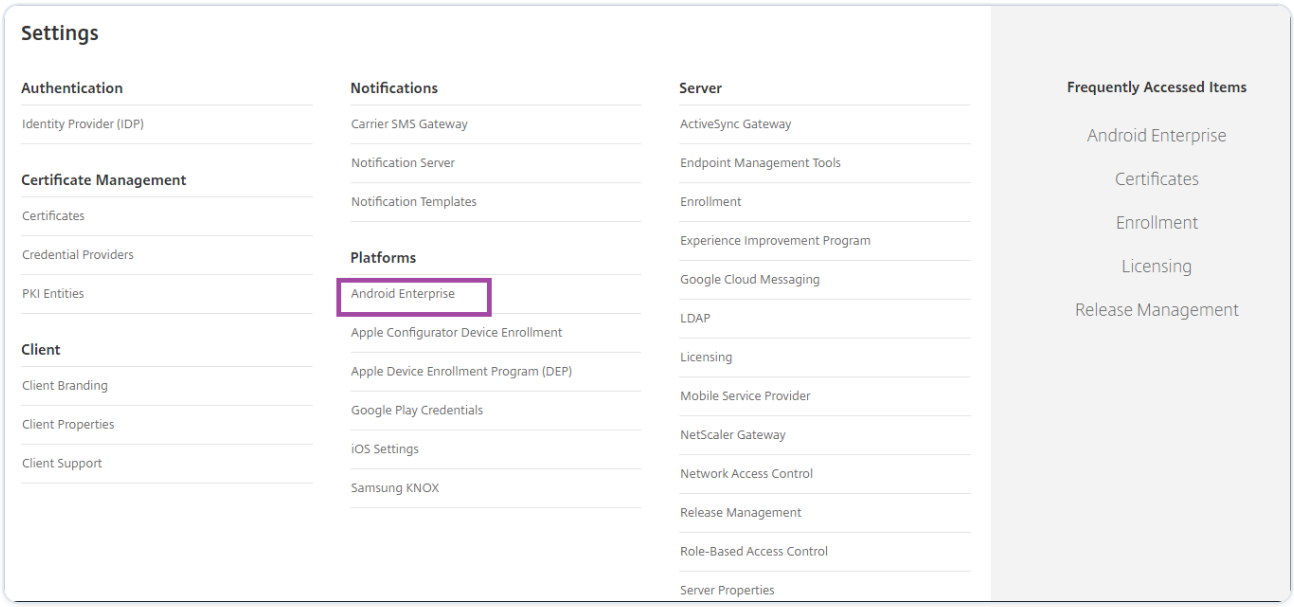
- Contas e credenciais:
  - Para configurar o Android Enterprise com o Google Play gerenciado, uma conta corporativa do Google
  - Para baixar os arquivos MDX mais recentes, uma conta de cliente Citrix
  - Para implantar aplicativos privados (opcional), uma conta de desenvolvedor do Google
- Firebase Cloud Messaging (FCM) configurado para XenMobile. Consulte Firebase Cloud Messaging para obter instruções.
- Para o Samsung Knox Mobile Enrollment (opcional), licenças premium do Knox.

Conectando o XenMobile ao Google Play

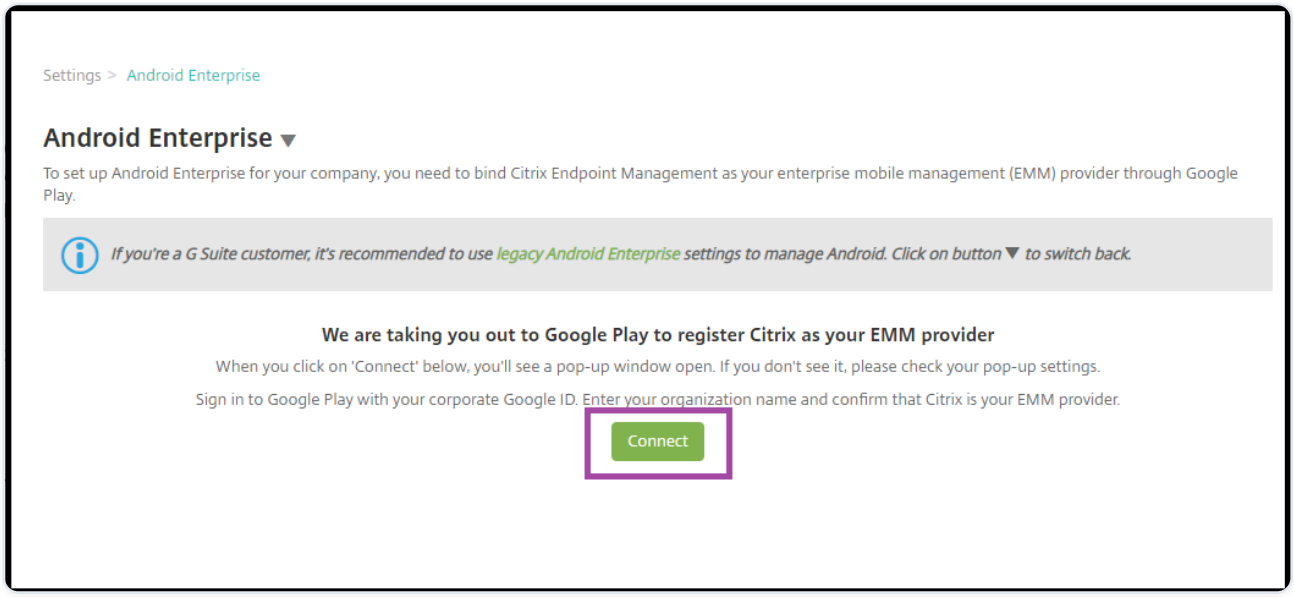
Para configurar o Android Enterprise para sua organização, registre a Citrix como seu provedor EMM através do Google Play gerenciado. Essa configuração conecta o Google Play gerenciado ao XenMobile e cria uma empresa para o Android Enterprise no XenMobile.

Você precisa de uma conta corporativa do Google para fazer login no Google Play.

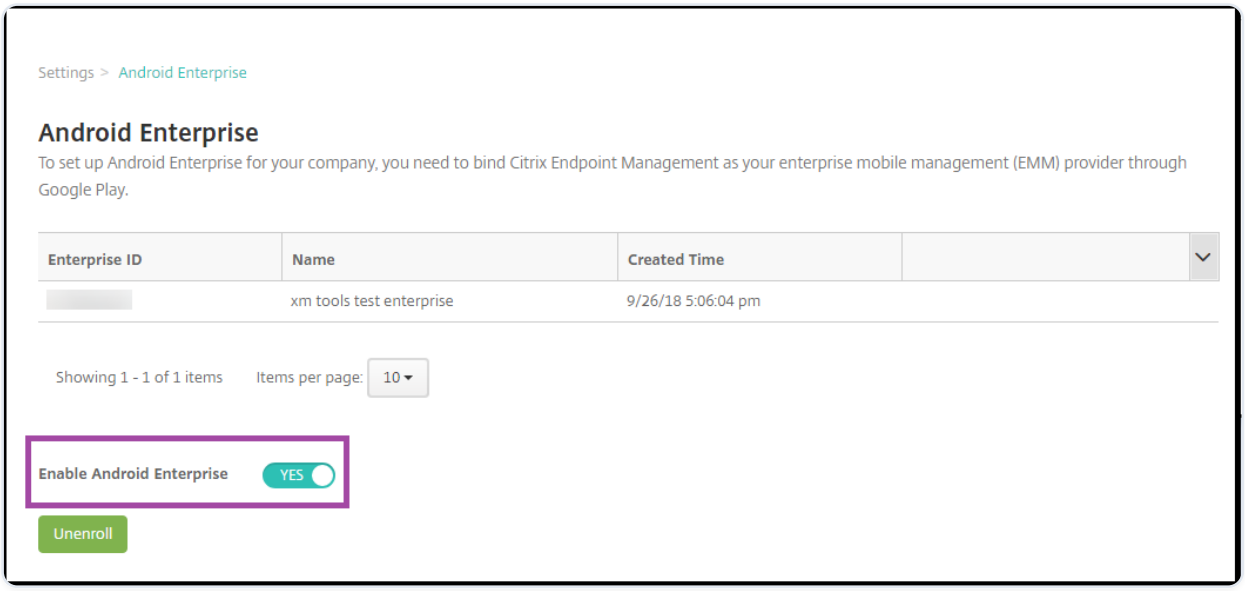
1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Vá para **Configurações > Android Enterprise**.



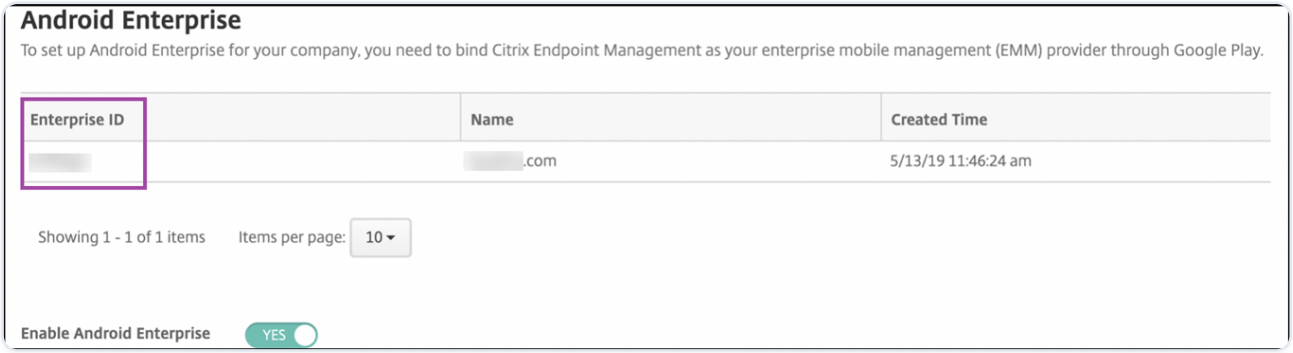
1. Clique em **Conectar**. O Google Play é aberto.



1. Faça login no Google Play com suas credenciais de conta corporativa do Google. Insira o nome da sua organização e confirme que a Citrix é seu provedor EMM.
2. Um ID de empresa é adicionado para o Android Enterprise. Para habilitar o Android Enterprise, deslize **Habilitar Android Enterprise** para **Sim**.



Seu ID de Empresa aparece no console do XenMobile.



Seu ambiente está conectado ao Google e pronto para gerenciar os dispositivos. Agora você pode fornecer aplicativos para os usuários.

O XenMobile pode ser usado para fornecer aos usuários aplicativos de produtividade móvel Citrix, aplicativos MDX, aplicativos de loja de aplicativos públicos, aplicativos web e SaaS, aplicativos corporativos e links da web. Para obter mais informações sobre esses tipos de aplicativos e como fornecê-los aos usuários, consulte Adicionar aplicativos.

A seção a seguir mostra como fornecer aplicativos de produtividade móvel.

Fornecendo aplicativos de produtividade móvel Citrix para usuários do Android Enterprise

O fornecimento de aplicativos de produtividade móvel Citrix para usuários do Android Enterprise requer estas etapas.

1. Publique os aplicativos como aplicativos MDX. Consulte Configurar aplicativos como aplicativos MDX.

2. Configure as regras para os desafios de segurança que seus usuários usam para acessar os perfis de trabalho em seus dispositivos. Consulte Configurar política de desafio de segurança.

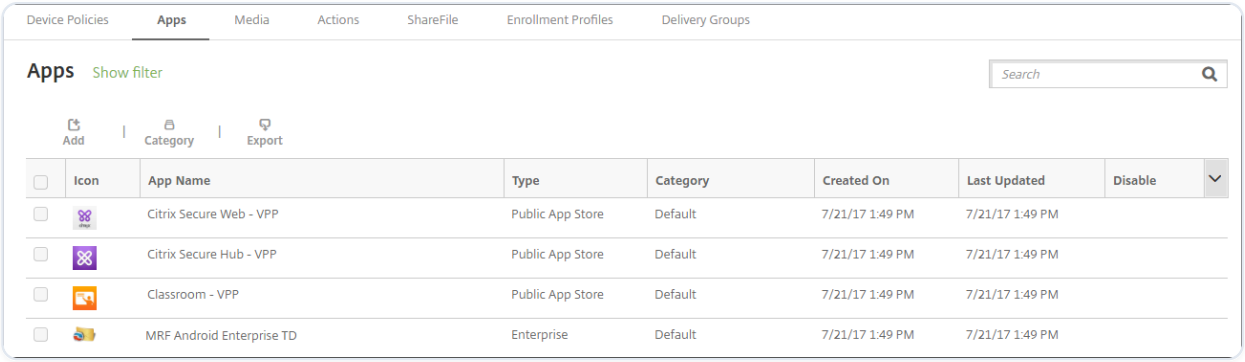
Os aplicativos que você publica estão disponíveis para dispositivos registrados em sua empresa Android Enterprise.

> **Nota:**
>
> Quando você implanta um aplicativo de loja de aplicativos público do Android Enterprise para um usuário Android, esse usuário é automaticamente registrado no Android Enterprise.

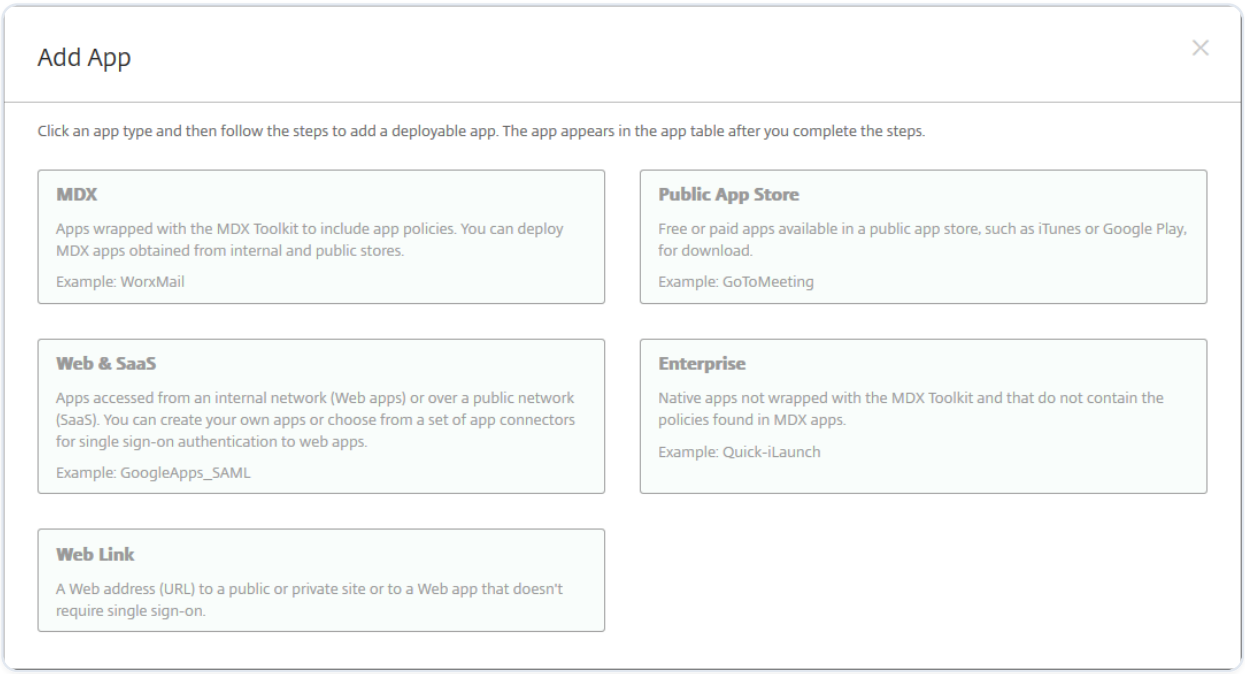
Configurar aplicativos como aplicativos MDX

Para configurar um aplicativo de produtividade Citrix como um aplicativo MDX para Android Enterprise:

1. No console do XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.



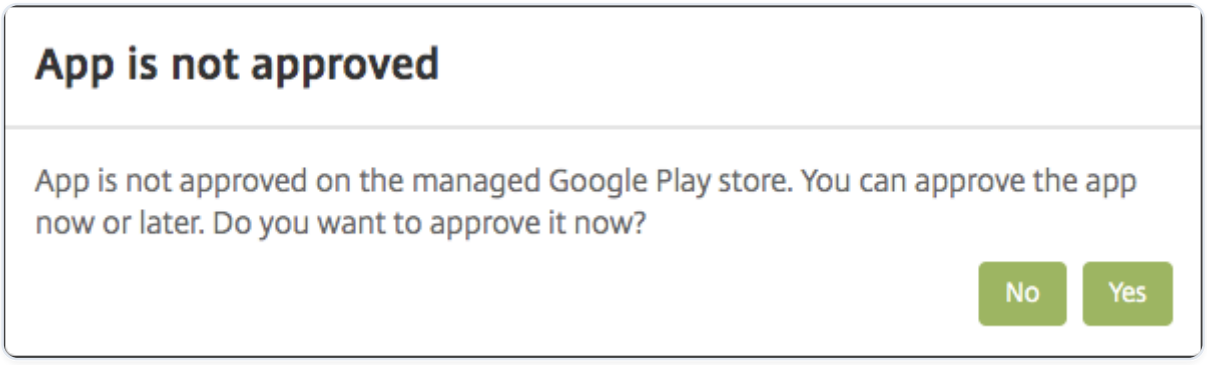
2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.



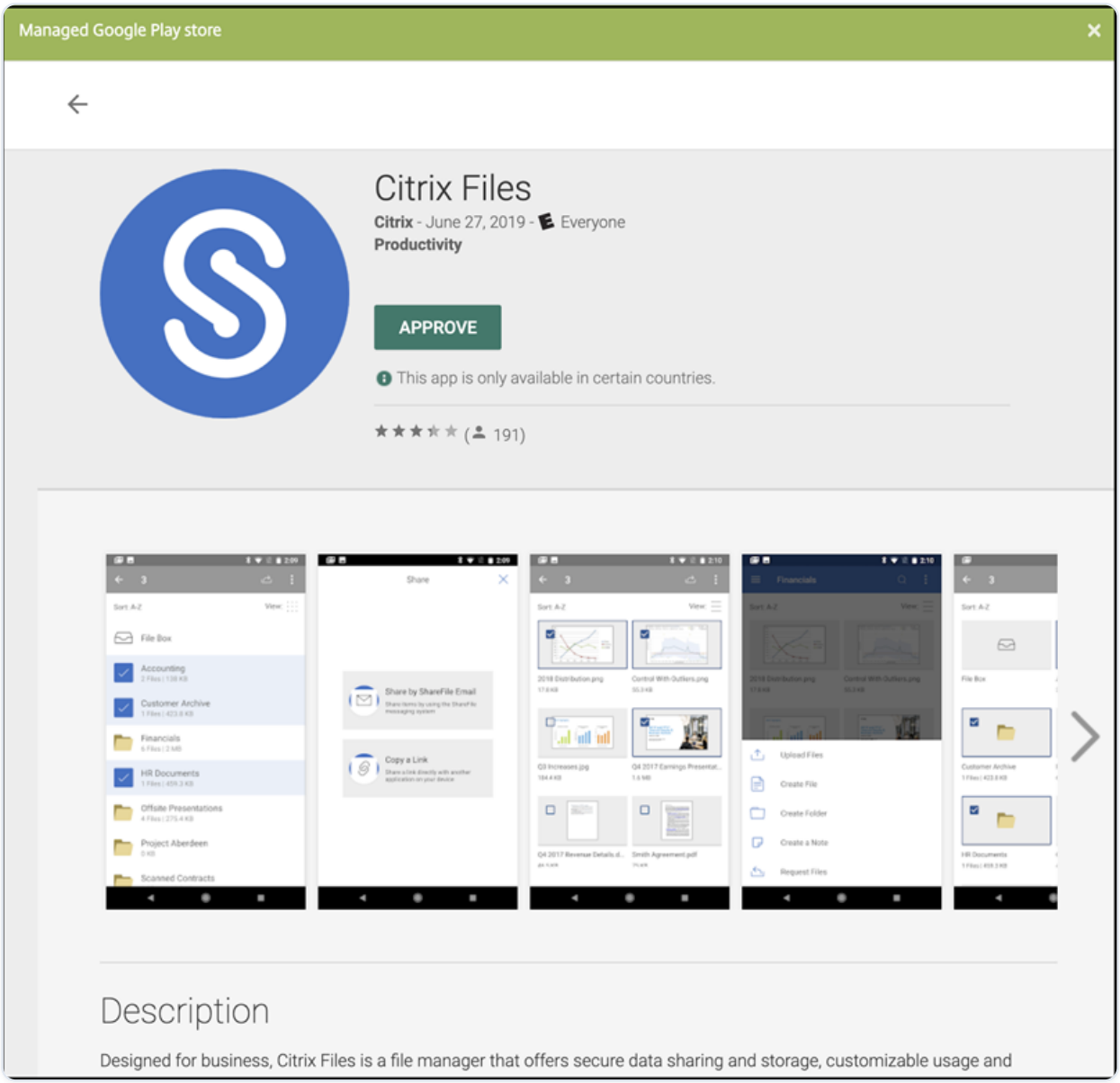
3. Clique em **MDX**. A página **Informações do Aplicativo** é exibida.
4. No lado esquerdo da página, selecione **Android Enterprise** como a plataforma.
5. Na página **Informações do Aplicativo**, digite as seguintes informações:

    - **Nome:** Digite um nome descritivo para o aplicativo. Este nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
    - **Descrição:** Digite uma descrição opcional do aplicativo.
    - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre as categorias de aplicativos.

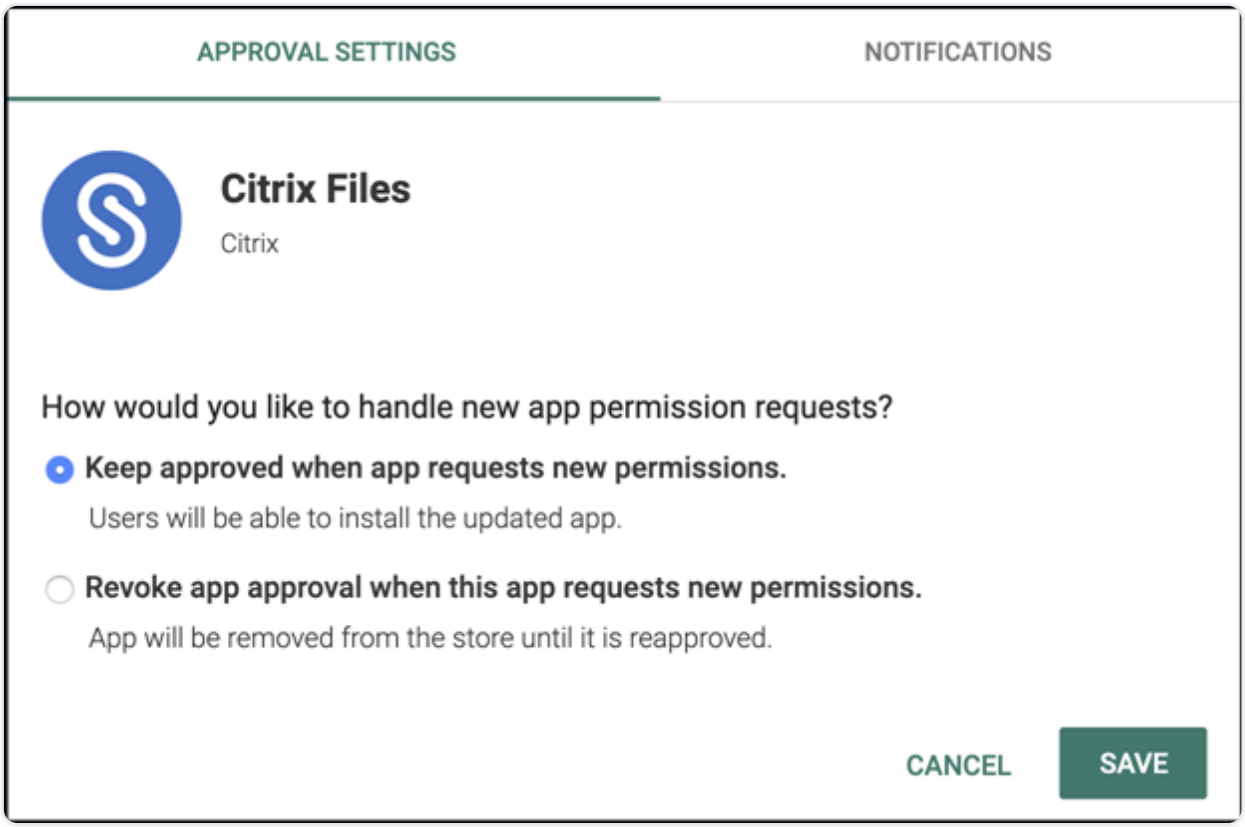
6. Clique em **Avançar**. A página **Aplicativo MDX do Android Enterprise** é exibida.
7. Clique em **Carregar** e navegar até o local do arquivo dos arquivos .mdx para o aplicativo. Selecione o arquivo e clique em **Abrir**.
8. A interface do usuário notifica você se o aplicativo anexado requer aprovação da Google Play Store gerenciada. Para aprovar o aplicativo sem sair do console do XenMobile, clique em **Sim**.



9. Quando a página da Google Play Store gerenciada for aberta, clique em **Aprovar**.



10. Clique em **Aprovar** novamente.
11. Selecione **Manter aprovado quando o aplicativo solicitar novas permissões**. Clique em **Salvar**.

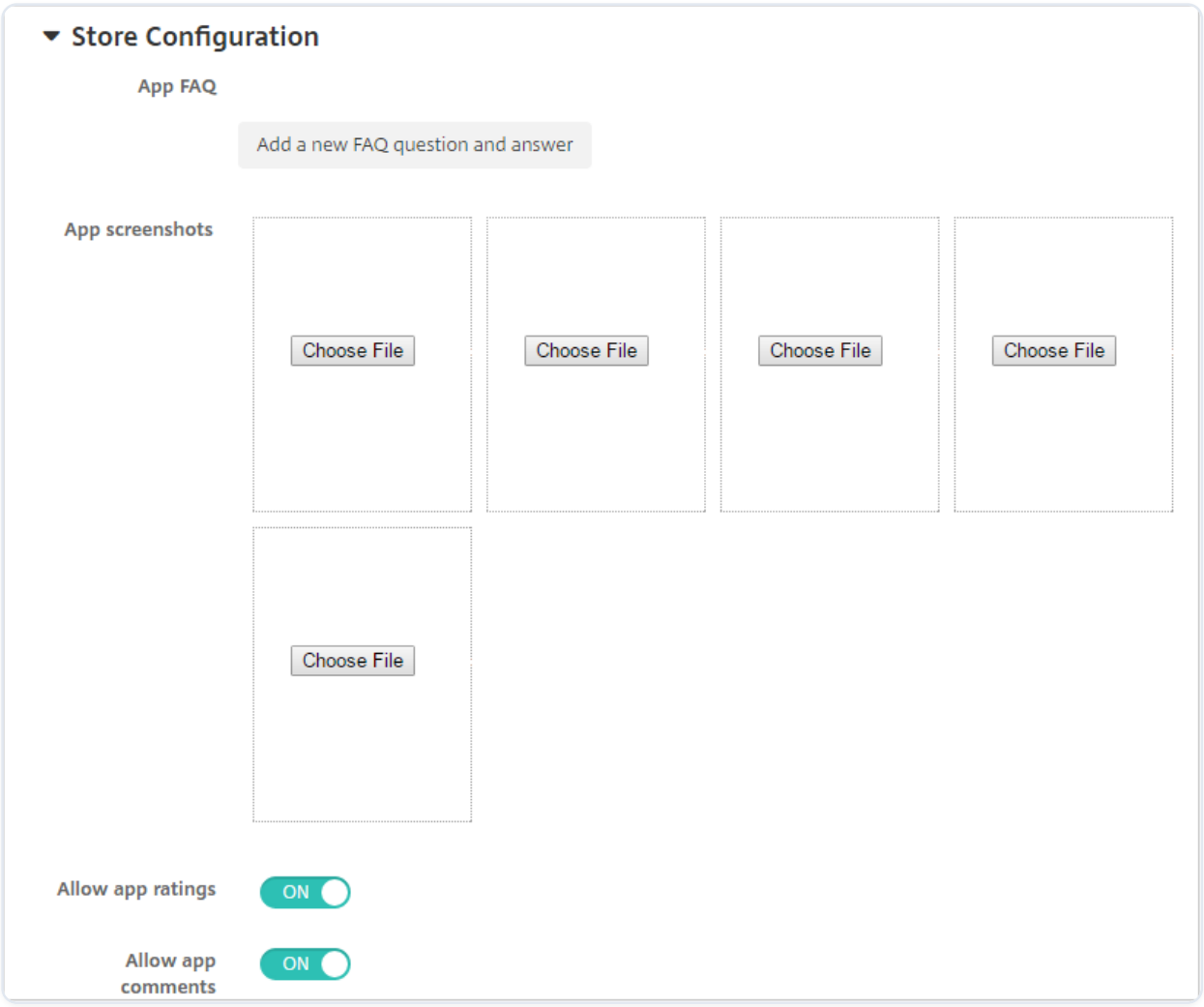


12. Quando o aplicativo é aprovado e salvo, mais configurações aparecem na página. Configure estas configurações:

    - **Nome do arquivo:** Digite o nome do arquivo associado ao aplicativo.
    - **Descrição do aplicativo:** Digite uma descrição para o aplicativo.
    - **Faixa de produto:** Especifique qual faixa de produto você deseja enviar para os dispositivos dos usuários. Se você tiver uma faixa projetada para testes, poderá selecioná-la e atribuí-la aos seus usuários. O padrão é Produção.
    - **Versão do aplicativo:** Opcionalmente, digite o número da versão do aplicativo.
    - **ID do pacote:** A URL do aplicativo na Google Play Store.
    - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
    - **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
    - **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.

13. Configure as **Políticas MDX**. Para obter mais informações sobre políticas de aplicativos para aplicativos MDX, consulte Políticas MDX em um Relance e Visão geral do SDK MAM.
14. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.

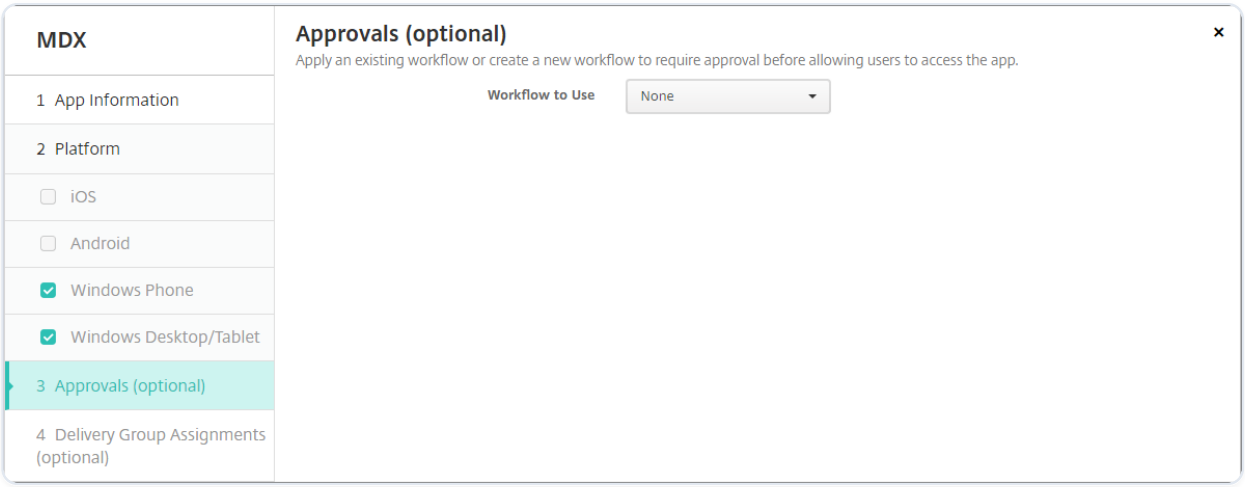
15. Expanda **Configuração da Loja**. Esta configuração não se aplica a aplicativos Android Enterprise, que aparecem apenas no Google Play gerenciado.



Opcionalmente, você pode adicionar um FAQ para o aplicativo ou capturas de tela que aparecem na loja de aplicativos. Você também pode definir se os usuários podem avaliar ou comentar sobre o aplicativo.

- Configure estas configurações:
  - **Perguntas Frequentes do Aplicativo:** Adicione perguntas e respostas frequentes para o aplicativo.
  - **Capturas de tela do aplicativo:** Adicione capturas de tela para ajudar a classificar o aplicativo na loja de aplicativos. O gráfico que você carrega deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
  - **Permitir classificações do aplicativo:** Selecione se deseja permitir que um usuário classifique o aplicativo. O padrão é **ATIVADO**. **Permitir comentários do aplicativo:** Selecione se deseja permitir que os usuários comentem sobre o aplicativo selecionado. O padrão é **ATIVADO**.

16. Clique em **Avançar**. A página **Aprovações** é exibida.



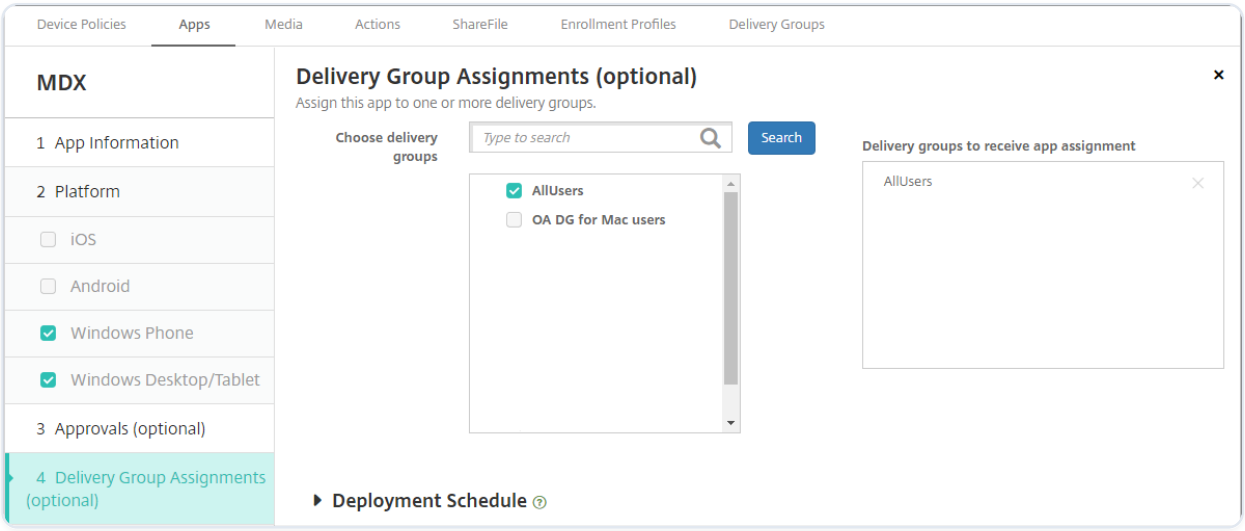
Você usa fluxos de trabalho quando precisa de aprovação ao criar contas de usuário. Se você não quiser configurar fluxos de trabalho de aprovação, pode pular para a Etapa 15.

Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de Trabalho a Usar:** Na lista, clique em um fluxo de trabalho existente ou clique em **Criar um novo fluxo de trabalho**. O padrão é **Nenhum**.
- Se você selecionar **Criar um novo fluxo de trabalho**, configure estas definições. Para obter mais informações, consulte Aplicar fluxos de trabalho.
- **Nome:** Digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** Opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de Aprovação por E-mail:** Na lista, selecione o modelo de aprovação por e-mail a ser atribuído. Ao clicar no ícone de olho à direita deste campo, uma caixa de diálogo é exibida onde você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** Na lista, selecione o número de níveis de aprovação do gerente necessários para este fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
  - Não Necessário
  - 1 nível
  - 2 níveis
  - 3 níveis
- **Selecionar domínio do Active Directory:** Na lista, selecione o domínio do Active Directory apropriado a ser usado para o fluxo de trabalho.

- **Encontrar aprovadores adicionais necessários:** Digite o nome da pessoa adicional necessária no campo de pesquisa e clique em **Pesquisar**. Os nomes são originados no Active Directory.
- Quando o nome aparecer no campo, selecione a caixa de seleção ao lado do nome. O nome e o endereço de e-mail aparecem na lista **Aprovadores adicionais necessários selecionados**.
    - Para remover uma pessoa da lista **Aprovadores adicionais necessários selecionados**, faça o seguinte:
        - Clique em **Pesquisar** para ver uma lista de todas as pessoas no domínio selecionado.
        - Digite um nome completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar os resultados da pesquisa.
        - As pessoas na lista **Aprovadores adicionais necessários selecionados** têm marcas de seleção ao lado de seus nomes na lista de resultados da pesquisa. Role a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

17. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.



18. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um ou mais grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
19. Expanda **Agendamento de Implantação** e configure as seguintes definições:
    - Ao lado de **Implantar**, clique em **ATIVADO** para agendar a implantação ou clique em **DESATIVADO** para impedir a implantação. A opção padrão é **ATIVADO**.

- Ao lado de Agendamento de implantação, clique em **Agora** ou **Mais tarde**. A opção padrão é **Agora**.
- Se você clicar em **Mais tarde**, clique no ícone do calendário e selecione a data e a hora para a implantação.
- Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou clique em **Somente quando a implantação anterior falhou**. A opção padrão é definida como **Em cada conexão**.
- Ao lado de **Implantar para conexão sempre ativa**, certifique-se de que **DESATIVADO** esteja selecionado. A opção padrão é definida como **DESATIVADO**. As conexões sempre ativas não estão disponíveis para o Android Enterprise se você começou a usar o XenMobile com a versão 10.18.19 ou posterior. Não recomendamos as conexões para clientes que começaram a usar o XenMobile antes da versão 10.18.19.

  Esta opção se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

  O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você fizer se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.

20. Clique em **Salvar**.

Repita as etapas para configurar um aplicativo MDX para cada aplicativo de produtividade móvel.

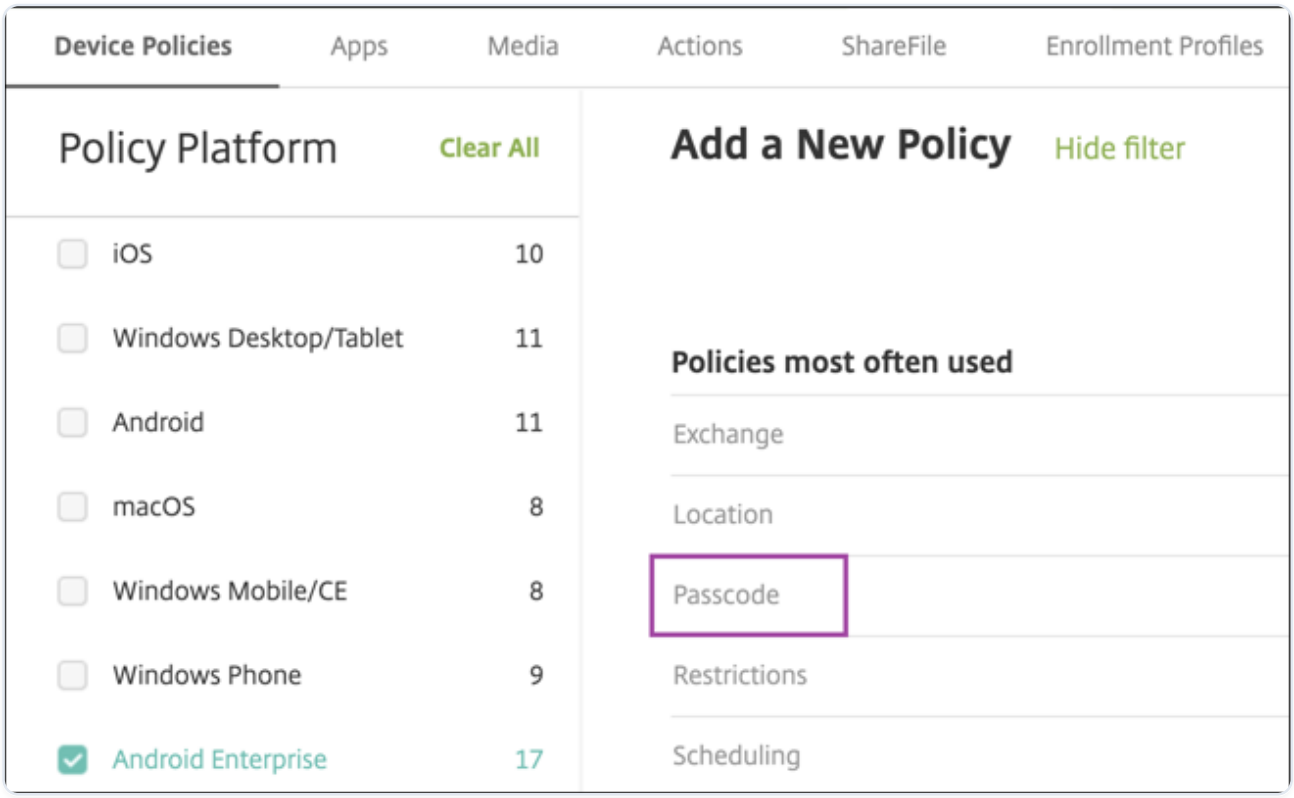
Configurar política de desafio de segurança

A política de dispositivo de senha do XenMobile configura o conjunto de regras para os desafios de segurança que os usuários enfrentam para acessar seus dispositivos ou os perfis de trabalho do Android Enterprise em seus dispositivos. Um desafio de segurança pode ser uma senha ou reconhecimento biométrico. Para obter mais informações sobre a política de senha, consulte Política de dispositivo de senha.

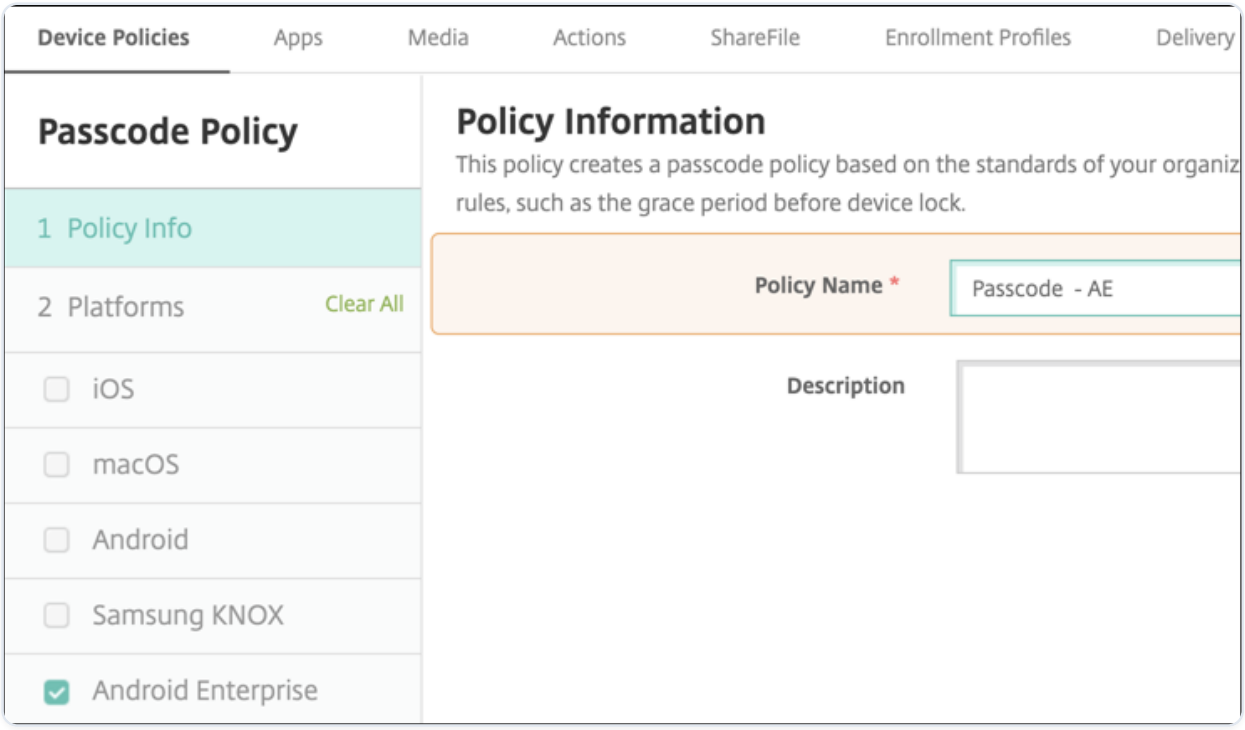
- Se sua implantação do Android Enterprise incluir dispositivos BYOD, configure a política de senha para o perfil de trabalho.
- Se sua implantação incluir dispositivos de propriedade da empresa e totalmente gerenciados, configure a política de senha para o próprio dispositivo.
- Se sua implantação incluir ambos os tipos de dispositivos, configure ambos os tipos de política de senha.

Para configurar a política de senha:

1. No console do XenMobile, vá para **Configurar > Políticas de Dispositivo**.
2. Clique em **Adicionar**.
3. Clique em **Mostrar filtro** para exibir o painel **Plataforma de Política**. No painel **Plataforma de Política**, selecione **Android Enterprise**.
4. Clique em **Senha** no painel direito.



1. Insira um **Nome da Política**. Clique em **Avançar**.



2. Configure as configurações da política de Senha.
    - Defina **Senha do dispositivo necessária** como **Ativado** para ver as configurações disponíveis para desafios de segurança para o próprio dispositivo.
    - Defina **Desafio de segurança do perfil de trabalho** como **Ativado** para ver as configurações disponíveis para desafios de segurança do perfil de trabalho.
3. Clique em **Avançar**.
4. Atribua a política a um ou mais grupos de entrega.
5. Clique em **Salvar**.

Criação de perfis de inscrição

Os perfis de inscrição controlam como os dispositivos Android são inscritos se o Android Enterprise estiver habilitado para sua implantação do XenMobile. Ao criar um perfil de inscrição para inscrever dispositivos Android Enterprise, você pode configurar o perfil de inscrição para inscrever dispositivos novos e redefinidos de fábrica como:

- Dispositivos totalmente gerenciados
- Dispositivos dedicados (dispositivos COSU)
- Dispositivos totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Você também pode configurar cada um desses perfis de registro do Android Enterprise para registrar dispositivos Android BYOD como dispositivos de perfil de trabalho.

Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise. Por padrão, o perfil de registro Global registra dispositivos Android novos e redefinidos de fábrica como dispositivos totalmente gerenciados e registra dispositivos Android BYOD como dispositivos de perfil de trabalho.

Ao criar perfis de registro, você atribui grupos de entrega a eles. Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabetizada de grupos de entrega. Para obter mais informações, consulte Perfis de registro.

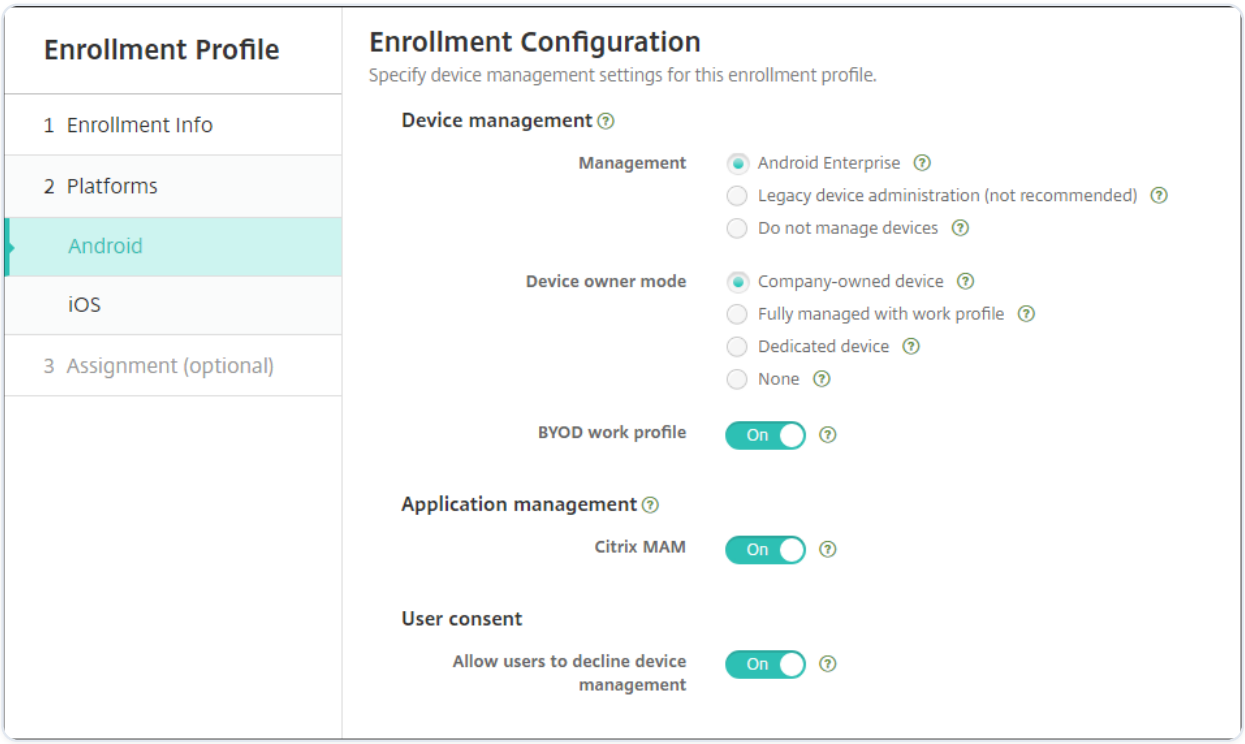
Você pode usar perfis de registro para combinar vários casos de uso, como somente MDM, MDM+MAM e somente MAM. Seu tipo de licença do XenMobile Server, refletido na propriedade

do servidor, `xms.server.mode`, determina as configurações disponíveis em **Configurar > Perfis de Registro**.

Adicionar um perfil de registro para dispositivos totalmente gerenciados

O perfil de registro Global registra dispositivos totalmente gerenciados por padrão, mas você pode criar mais perfis de registro para registrar dispositivos totalmente gerenciados.

1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página Configuração de Registro é exibida.
5. Defina **Gerenciamento** como **Android Enterprise**.
6. Defina **Modo de proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.



7. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e redefinidos de fábrica são registrados como dispositivos totalmente gerenciados.

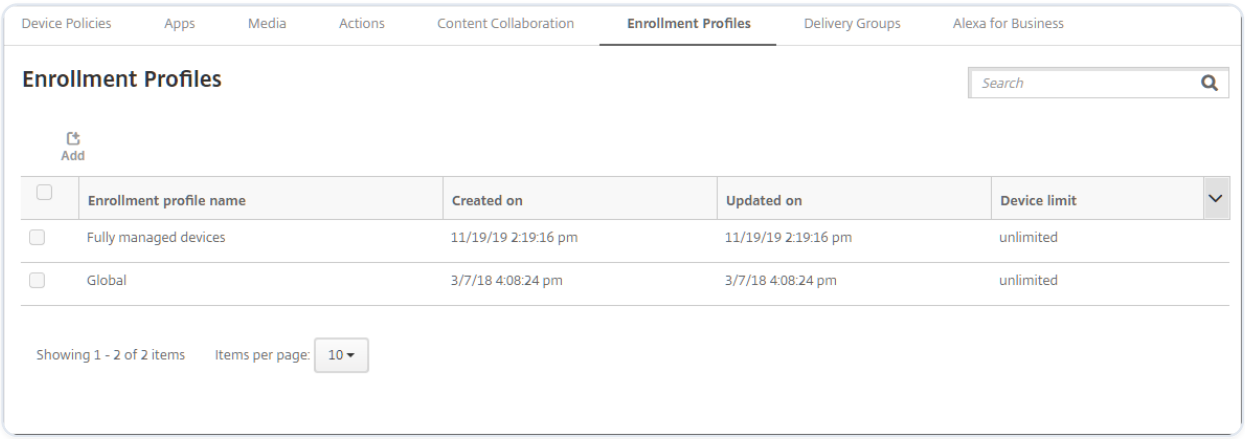
   - Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. O padrão é **Ativado**.

- Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos totalmente gerenciados.

8. Escolha se deseja registrar dispositivos no Citrix MAM.
9. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento de dispositivos ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**.

   Se **Perfil de trabalho BYOD** estiver definido como **Ativado**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** é **Ativado**. Se **Perfil de trabalho BYOD** estiver definido como **Desativado**, então **Permitir que os usuários recusem o gerenciamento de dispositivos** é desabilitado.
10. Selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.
11. Escolha o grupo de entrega ou os grupos de entrega que contêm os administradores que registram dispositivos totalmente gerenciados. Em seguida, clique em **Salvar**.

    A página Perfil de Registro é exibida com o perfil que você adicionou.

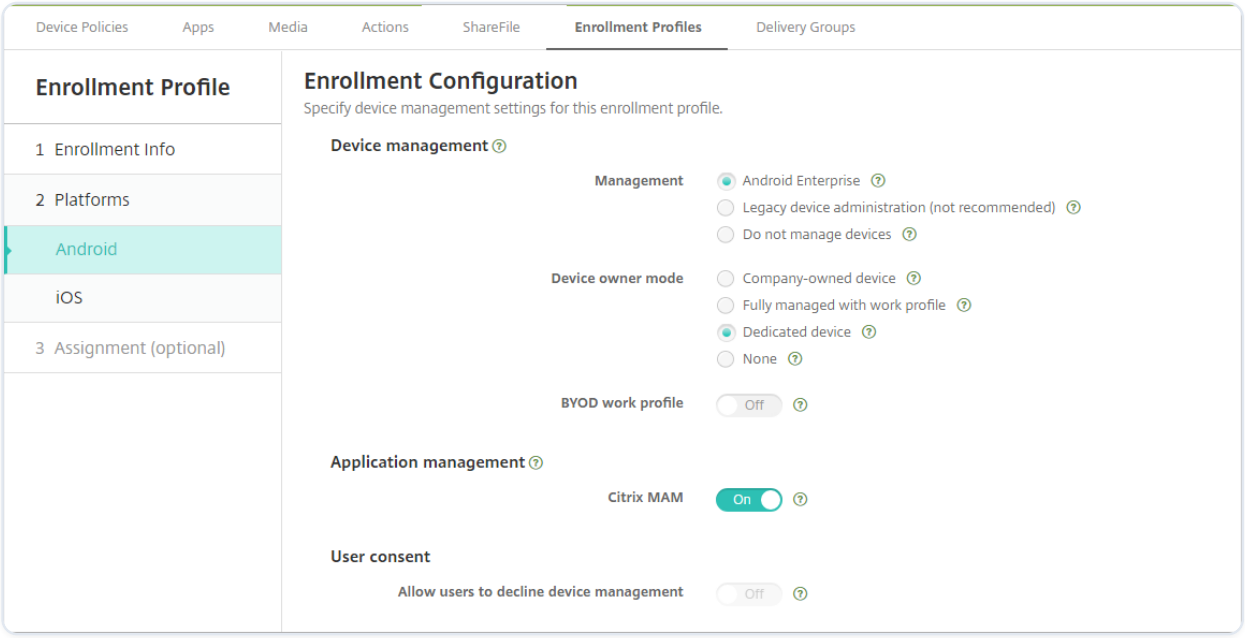


Adicionar um perfil de registro de dispositivo dedicado

Quando sua implantação do XenMobile inclui dispositivos dedicados, um único administrador do XenMobile ou um pequeno grupo de administradores registra muitos dispositivos dedicados. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com um número ilimitado de dispositivos permitidos por usuário.

1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.

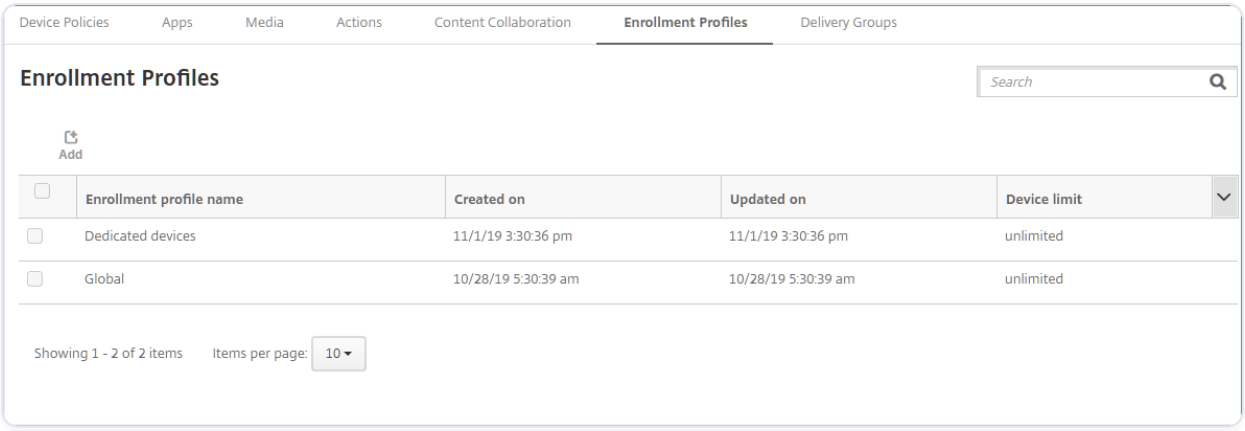
3. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página Configuração de Registro é exibida.
4. Defina **Gerenciamento** como **Android Enterprise**.
5. Defina **Modo de proprietário do dispositivo** como **Dispositivo dedicado**.



6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e redefinidos de fábrica são registrados como dispositivos dedicados. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos de propriedade da empresa. O padrão é **Ativado**.
7. Escolha se deseja registrar dispositivos no Citrix MAM.
8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento de dispositivos ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**.

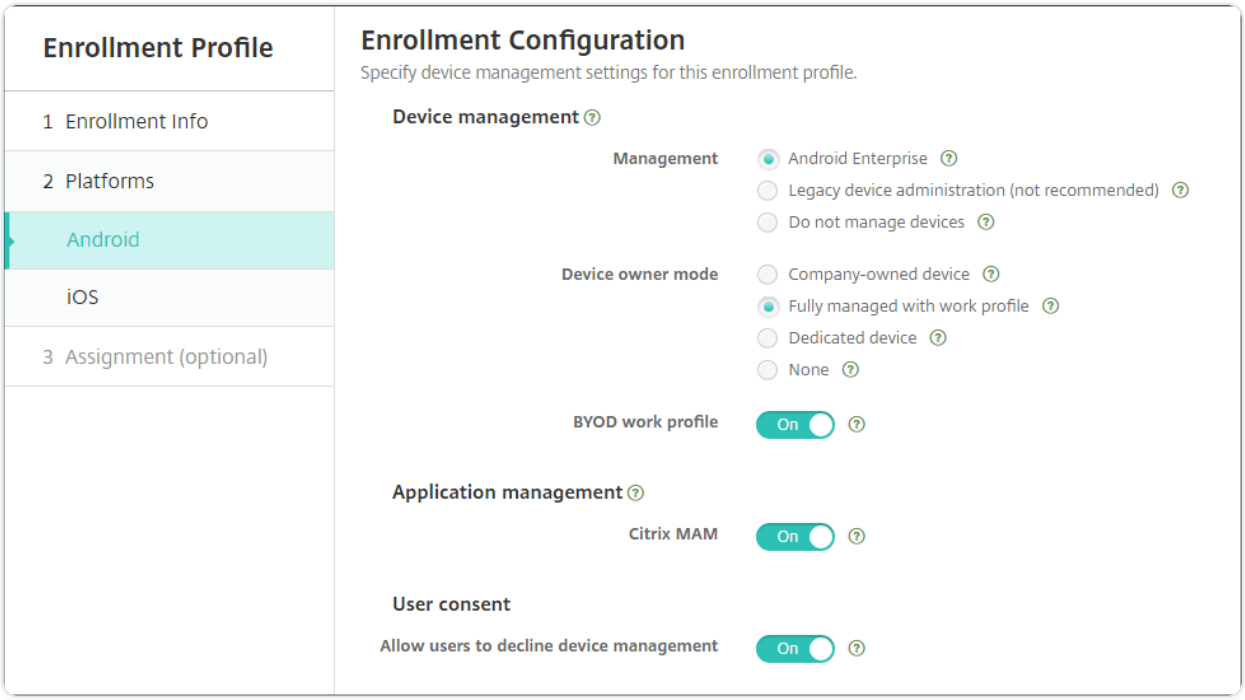
   Se **Perfil de trabalho BYOD** estiver definido como **Ativado**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** é **Ativado**. Se **Perfil de trabalho BYOD** estiver definido como **Desativado**, então **Permitir que os usuários recusem o gerenciamento de dispositivos** é desabilitado.
9. Selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.
10. Escolha o grupo de entrega ou grupos de entrega que possui os administradores que registram os dispositivos dedicados. Em seguida, clique em **Salvar**.

A página Perfil de Registro é exibida com o perfil que você adicionou.



Adicionar um perfil de registro para dispositivos totalmente gerenciados com um perfil de trabalho

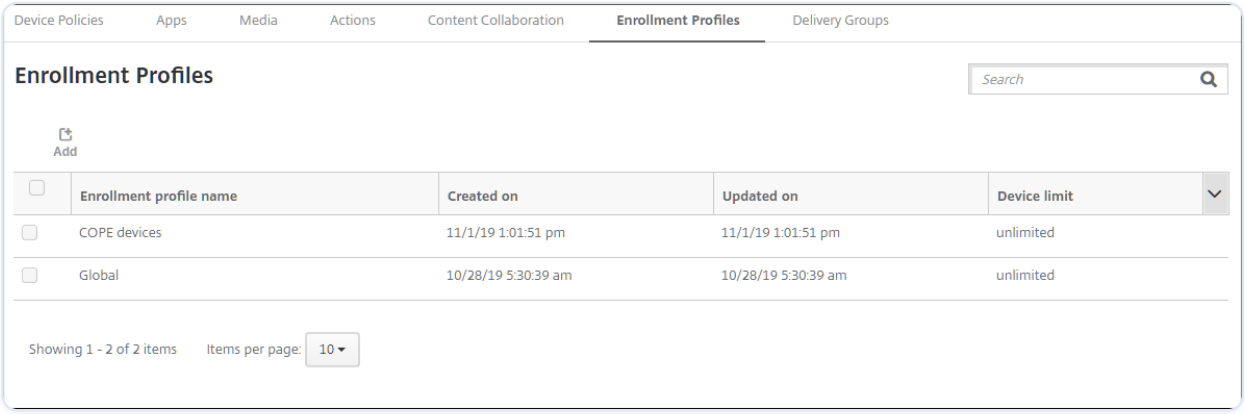
1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página Configuração de Registro é exibida.
5. Defina **Gerenciamento** como **Android Enterprise**. Defina **Modo de proprietário do dispositivo** como **Totalmente gerenciado com perfil de trabalho**.



6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e redefinidos de fábrica são registrados como dispositivos totalmente gerenciados com um perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos dedicados. O padrão é **Desativado**.
7. Escolha se deseja registrar dispositivos no Citrix MAM.
8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento de dispositivos ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**.

   Se **Perfil de trabalho BYOD** estiver definido como **Ativado**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** é **Ativado**. Se **Perfil de trabalho BYOD** estiver definido como **Desativado**, então **Permitir que os usuários recusem o gerenciamento de dispositivos** é desabilitado.
9. Selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.
10. Escolha o grupo de entrega ou os grupos de entrega que possuem os administradores que registram dispositivos totalmente gerenciados com um perfil de trabalho. Em seguida, clique em **Salvar**.

    A página Perfil de Registro é exibida com o perfil que você adicionou.



Adicionando um perfil de registro para dispositivos legados

O Google está descontinuando o modo de administrador de dispositivo de gerenciamento de dispositivos. O Google incentiva os clientes a gerenciar todos os dispositivos Android no modo de proprietário do dispositivo ou modo de proprietário do perfil. (Consulte Descontinuação do administrador do dispositivo nos guias do desenvolvedor do Google Android Enterprise.)

Para oferecer suporte a essa alteração:

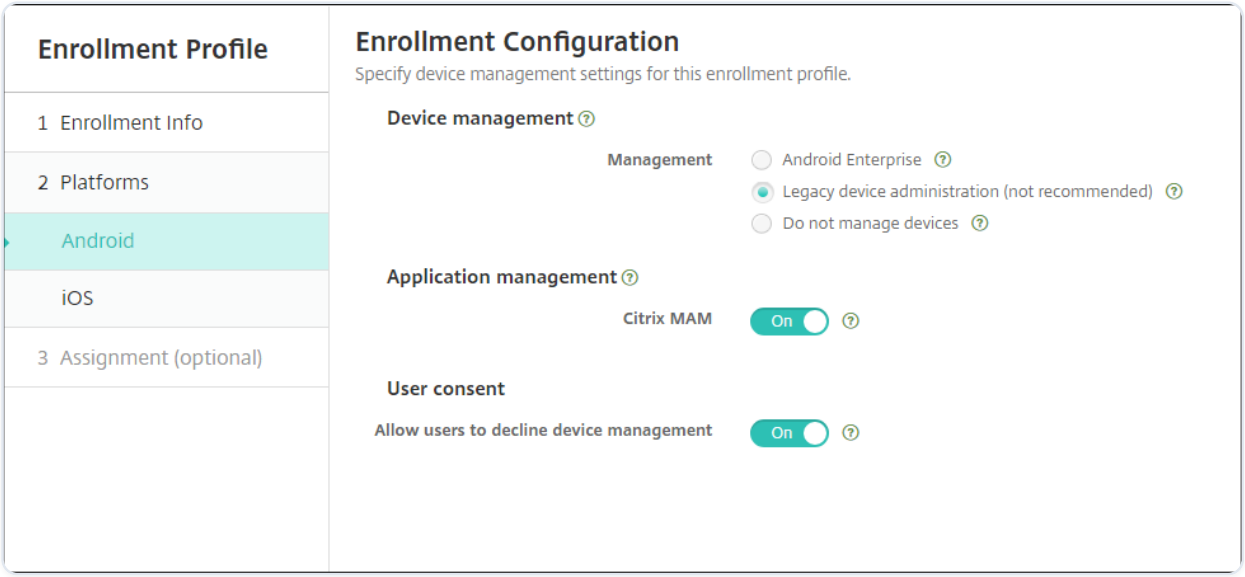
- A Citrix torna o Android Enterprise a opção de registro padrão para dispositivos Android.
- Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise.

Sua organização pode não estar pronta para começar a gerenciar dispositivos Android legados usando o Android Enterprise. Nesse caso, você pode continuar a gerenciá-los no modo de administrador de dispositivo. Para dispositivos já registrados no modo de administrador de dispositivo, o XenMobile continua a gerenciá-los no modo de administrador de dispositivo.

Crie um perfil de registro para dispositivos legados para permitir que novos registros de dispositivos Android usem o modo de administrador de dispositivo.

Para criar um perfil de registro para dispositivos legados:

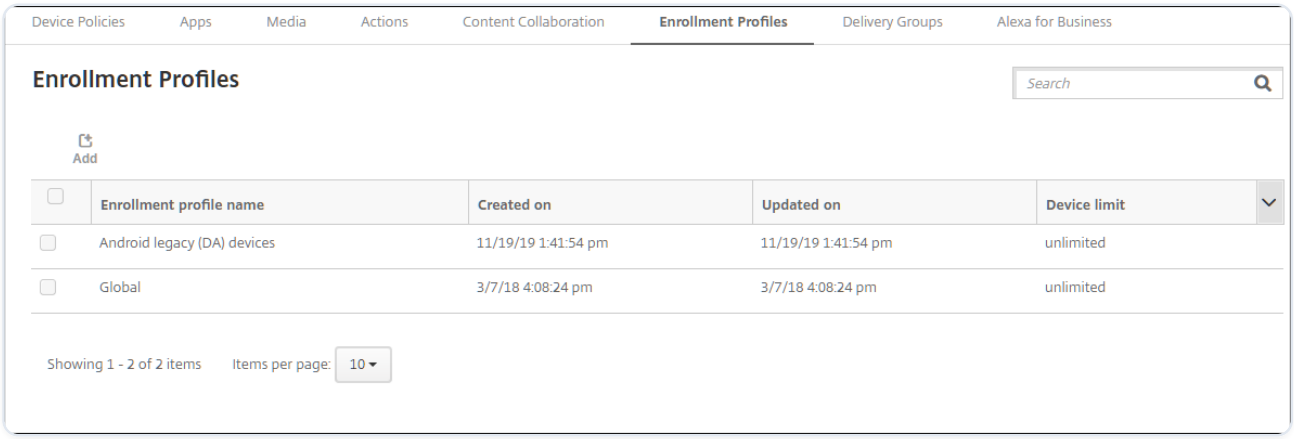
1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página Configuração de Registro é exibida.
5. Defina **Gerenciamento** como **Administração de dispositivo legado (não recomendado)**. Clique em **Avançar**.



6. Escolha se deseja registrar dispositivos no Citrix MAM.

7. Para permitir que os usuários recusem o gerenciamento de dispositivos ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**. O padrão é **Ativado**.
8. Selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.
9. Escolha o grupo de entrega ou os grupos de entrega que contêm os administradores que registram os dispositivos dedicados. Em seguida, clique em **Salvar**.

A página Perfil de Registro é exibida com o perfil que você adicionou.



Para continuar gerenciando um dispositivo legado no modo de administrador de dispositivo, registre-o ou registre-o novamente usando este perfil. Você registra dispositivos de administrador de dispositivo de forma semelhante aos dispositivos de perfil de trabalho, fazendo com que os usuários baixem o Secure Hub e forneçam uma URL de servidor de registro.

Provisionando dispositivos de perfil de trabalho do Android Enterprise

Os dispositivos de perfil de trabalho do Android Enterprise são registrados no modo de proprietário de perfil. Esses dispositivos não precisam ser novos ou redefinidos de fábrica. Dispositivos BYOD são registrados como dispositivos de perfil de trabalho. A experiência de registro é semelhante ao registro Android no XenMobile. Os usuários baixam o Secure Hub do Google Play e registram seus dispositivos.

Por padrão, as configurações de **Depuração USB e Fontes Desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android Enterprise como um dispositivo de perfil de trabalho.

Ao registrar dispositivos no Android Enterprise como dispositivos de perfil de trabalho, sempre vá ao Google Play. A partir daí, habilite o Secure Hub para aparecer no perfil pessoal do usuário.

Provisionando dispositivos totalmente gerenciados do Android Enterprise

Você pode registrar dispositivos totalmente gerenciados na implantação que configurou nas seções anteriores. Dispositivos totalmente gerenciados são dispositivos de propriedade da empresa e são registrados no modo de proprietário do dispositivo. Somente dispositivos novos ou redefinidos de fábrica podem ser registrados no modo de proprietário do dispositivo.

Você pode registrar dispositivos no modo de proprietário do dispositivo usando qualquer um destes métodos de registro:

- **Token de identificador DPC:** Com este método de registro, os usuários inserem os caracteres `afw#xenmobile` ao configurar o dispositivo. `afw#xenmobile` é o token de identificador DPC da Citrix. Este token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub da Google Play Store. Consulte Registrando dispositivos usando o token de identificador DPC da Citrix.
- **Toque de comunicação de campo próximo (NFC):** O método de registro por toque NFC transfere dados entre dois dispositivos usando comunicação de campo próximo. Bluetooth, Wi-Fi e outros modos de comunicação são desativados em um dispositivo novo ou redefinido de fábrica. NFC é o único protocolo de comunicação que o dispositivo pode usar neste estado. Consulte Registrando dispositivos com toque NFC.
- **Código QR:** O registro por código QR pode ser usado para registrar uma frota distribuída de dispositivos que não suportam NFC, como tablets. O método de registro por código QR configura o modo de perfil do dispositivo escaneando um código QR do assistente de configuração. Consulte Registrando dispositivos usando um código QR.
- **Zero touch:** O registro zero touch permite configurar dispositivos para se registrarem automaticamente quando são ligados pela primeira vez. O registro zero touch é suportado em alguns dispositivos Android que executam o Android 9.0 ou posterior. Consulte Registro zero touch.
- **Contas Google:** Os usuários inserem suas credenciais de Conta Google para iniciar o processo de provisionamento. Esta opção é para empresas que usam o Google Workspace.

Registrando dispositivos usando o token de identificador DPC da Citrix

Os usuários inserem `afw#xenmobile` quando solicitados a inserir uma conta Google após ligar dispositivos novos ou redefinidos de fábrica para a configuração inicial. Esta ação baixa e instala o Secure Hub. Os usuários então seguem os prompts de configuração do Secure Hub para concluir o registro.

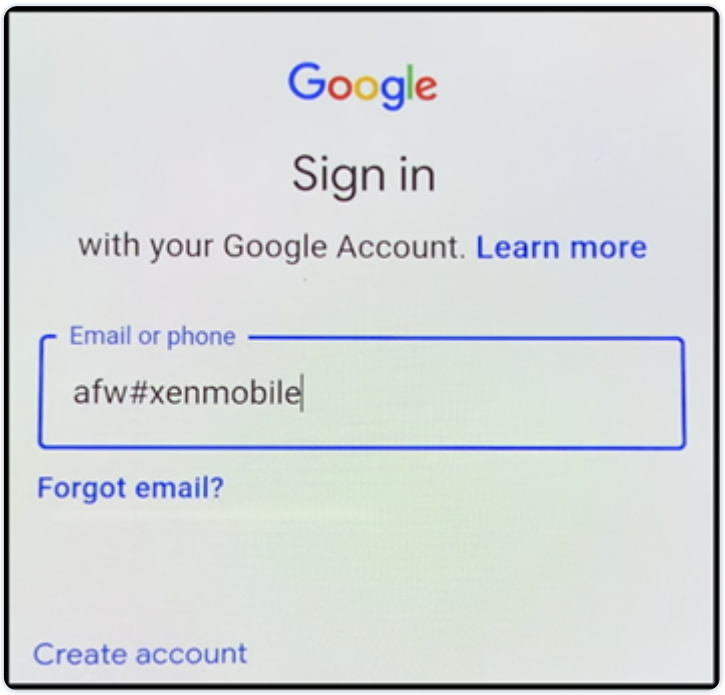
Este método de registro é recomendado para a maioria dos clientes porque a versão mais recente do Secure Hub é baixada da Google Play Store. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download do XenMobile Server.

Requisitos do sistema

- Compatível com todos os dispositivos Android que executam o sistema operacional Android.

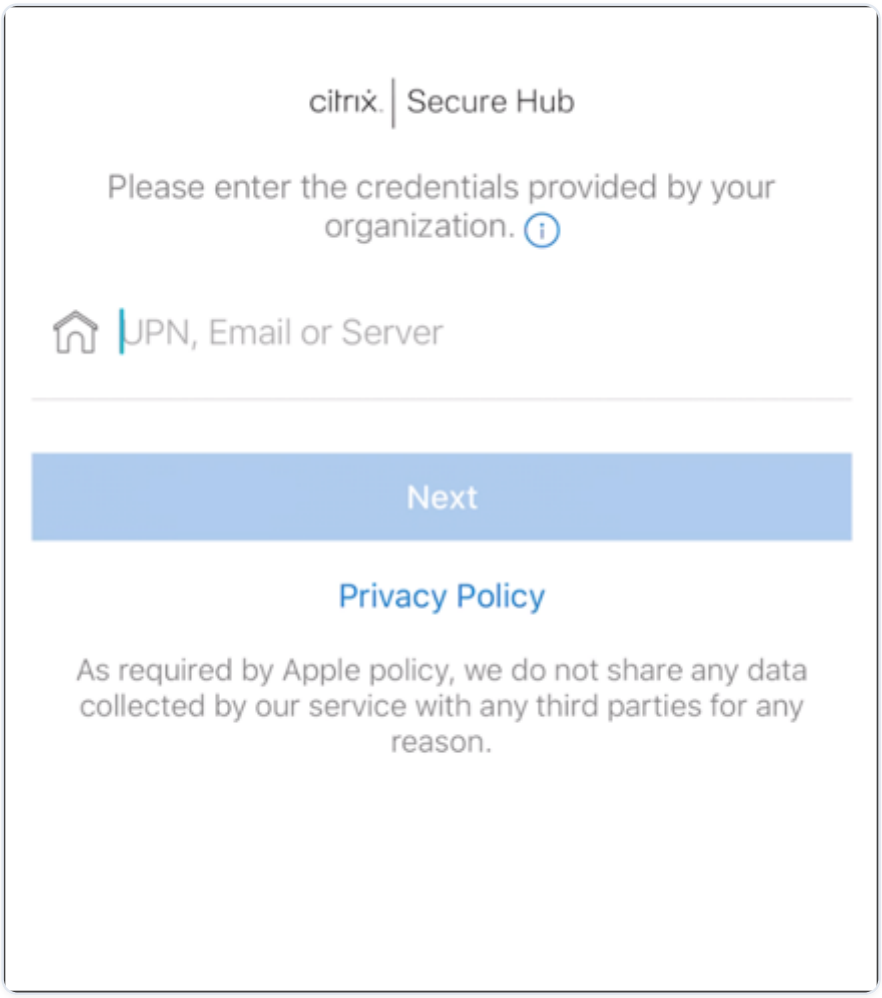
Para registrar o dispositivo

1. Ligue um dispositivo novo ou redefinido de fábrica.
2. A configuração inicial do dispositivo é carregada e solicita uma conta Google. Se o dispositivo carregar a tela inicial, verifique a barra de notificação para uma notificação de **Concluir Configuração**.
3. Insira `afw#xenmobile` no campo **E-mail ou telefone**.

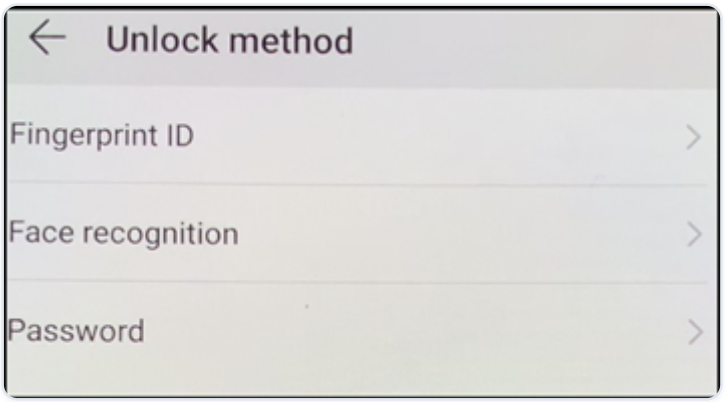


4. Toque em **Instalar** na tela do Android Enterprise que solicita a instalação do Secure Hub.
5. Toque em **Instalar** na tela do instalador do Secure Hub.
6. Toque em **Permitir** para todas as solicitações de permissão do aplicativo.
7. Toque em **Aceitar e Continuar** para instalar o Secure Hub e permitir que ele gerencie o dispositivo.
8. O Secure Hub está agora instalado e na tela de registro padrão. Neste exemplo, o AutoDiscovery não está configurado. Se estivesse, o usuário poderia inserir seu nome de

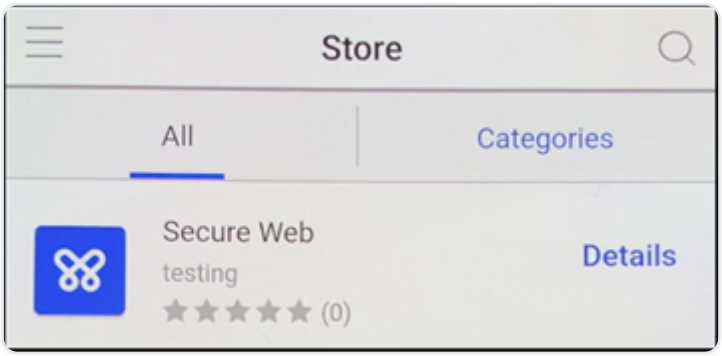
usuário/e-mail e um servidor seria encontrado para ele. Em vez disso, insira o URL de registro para o ambiente e toque em **Avançar**.



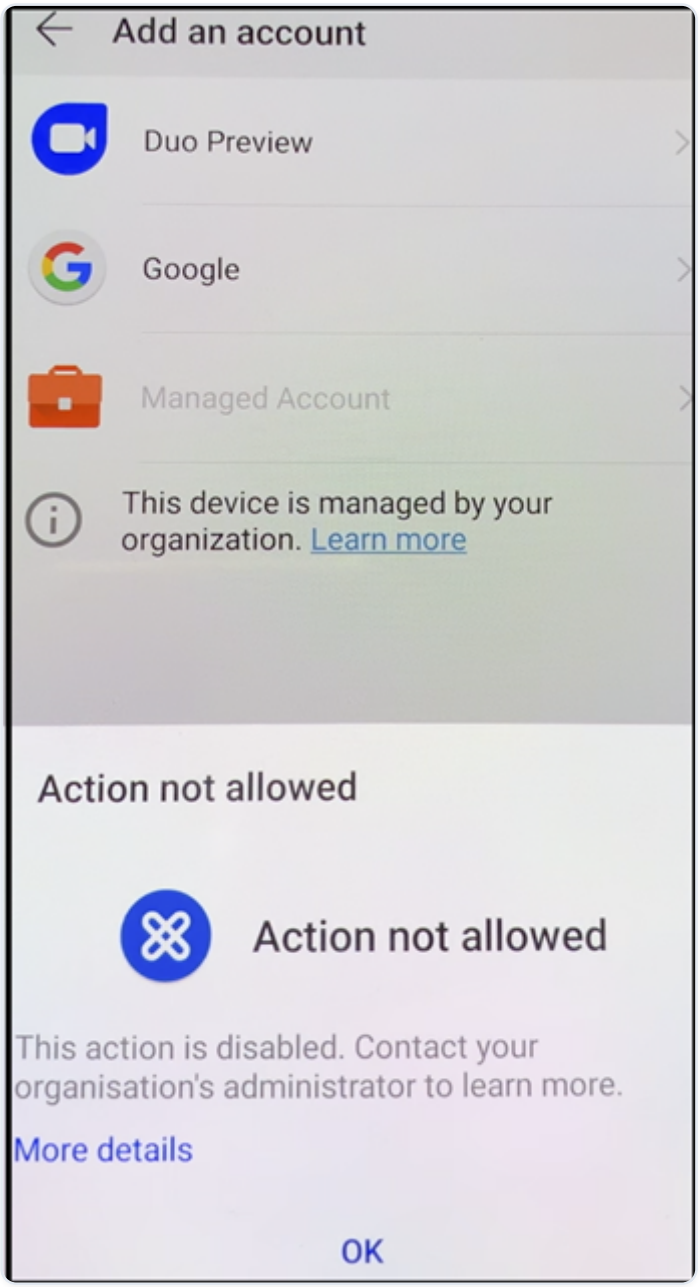
9. A configuração padrão do XenMobile permite que os usuários escolham se usam MAM ou MDM+MAM. Se solicitado dessa forma, toque em **Sim, Registrar** para escolher MDM+MAM.
10. Insira o nome de usuário e a senha e, em seguida, toque em **Avançar**.
11. O usuário é solicitado a configurar uma senha de dispositivo. Toque em **Definir** e insira uma senha.
12. O usuário é solicitado a configurar um método de desbloqueio de perfil de trabalho. Para este exemplo, toque em **Senha**, toque em **PIN** e insira um PIN.



13. O dispositivo está agora na tela inicial **Meus Aplicativos** do Secure Hub. Toque em **Adicionar aplicativos da Loja**.
14. Para adicionar o Secure Web, toque em **Secure Web**.



15. Toque em **Adicionar**.
16. O Secure Hub direciona o usuário para a Google Play Store para instalar o Secure Web. Toque em **Instalar**.
17. Após a instalação do Secure Web, toque em **Abrir**. Insira um URL de um site interno na barra de endereços e verifique se a página é carregada.
18. Vá para **Configurações > Contas** no dispositivo. Observe que a **Conta Gerenciada** não pode ser modificada. As opções de desenvolvedor para compartilhamento de tela ou depuração remota também estão bloqueadas.



Registrando dispositivos com NFC bump

Para registrar um dispositivo como um dispositivo totalmente gerenciado usando NFC bumps, são necessários dois dispositivos: um que foi redefinido para as configurações de fábrica e outro executando a Ferramenta de Provisionamento do XenMobile.

Requisitos de sistema e pré-requisitos

- Dispositivos Android compatíveis.
- Um dispositivo novo ou redefinido de fábrica, provisionado para Android Enterprise como um dispositivo totalmente gerenciado. Você pode encontrar as etapas para concluir este pré-requisito mais adiante neste artigo.

- Outro dispositivo com capacidade NFC, executando a Ferramenta de Provisionamento configurada. A Ferramenta de Provisionamento está disponível no Secure Hub ou na página de downloads da Citrix.

Cada dispositivo pode ter apenas um perfil do Android Enterprise, gerenciado pelo Secure Hub. Apenas um perfil é permitido em cada dispositivo. Tentar adicionar um segundo aplicativo DPC remove o Secure Hub instalado.

Dados transferidos através do toque NFC

O provisionamento de um dispositivo redefinido de fábrica exige que você envie os seguintes dados por meio de um toque NFC para inicializar o Android Enterprise:

- Nome do pacote do aplicativo DPC que atua como proprietário do dispositivo (neste caso, Secure Hub).
- Localização na Intranet/Internet de onde o dispositivo pode baixar o aplicativo DPC.
- Hash SHA1 do aplicativo DPC para verificar se o download foi bem-sucedido.
- Detalhes da conexão Wi-Fi para que um dispositivo redefinido de fábrica possa se conectar e baixar o aplicativo DPC. Observação: o Android agora não oferece suporte a Wi-Fi 802.1x para esta etapa.
- Fuso horário para o dispositivo (opcional).
- Localização geográfica para o dispositivo (opcional).

Quando os dois dispositivos são tocados, os dados da Ferramenta de Provisionamento são enviados para o dispositivo redefinido de fábrica. Esses dados são então usados para baixar o Secure Hub com as configurações de administrador. Se você não inserir os valores de fuso horário e localização, o Android configurará automaticamente os valores no novo dispositivo.

Configurando a Ferramenta de Provisionamento do XenMobile

Antes de fazer um toque NFC, você deve configurar a Ferramenta de Provisionamento. Essa configuração é então transferida para o dispositivo redefinido de fábrica durante o toque NFC.

A configuração da Ferramenta de Provisionamento(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no próximo procedimento descrevem como configurar o arquivo de texto e contêm descrições para cada campo. O aplicativo não salva as informações depois que você as digita, então você pode querer criar um arquivo de texto para guardar as informações para uso futuro.

PARA CONFIGURAR A FERRAMENTA DE PROVISIONAMENTO USANDO UM ARQUIVO DE TEXTO

Nomeie o arquivo nfcprovisioning.txt e coloque o arquivo na pasta `/sdcard/` no cartão SD do dispositivo. O aplicativo pode então ler o arquivo de texto e preencher os valores.

O arquivo de texto deve ter os seguintes dados:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Esta linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo redefinido de fábrica se conecta ao Wi-Fi após o NFC bump, o dispositivo deve ter acesso a este local para download. A URL é uma URL regular, sem necessidade de formatação especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

Esta linha é o checksum do aplicativo do provedor EMM. Este checksum é usado para verificar se o download foi bem-sucedido. As etapas para obter o checksum são discutidas posteriormente neste artigo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esta linha é o SSID Wi-Fi conectado do dispositivo no qual a Ferramenta de Provisionamento está sendo executada.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Os valores suportados são WEP e WPA2. Se o Wi-Fi não estiver protegido, este campo deve estar vazio.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Se o Wi-Fi não estiver protegido, este campo deve estar vazio.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO de duas letras minúsculas (como en), conforme definido por ISO 639-1. Os códigos de país são códigos de país ISO de duas letras maiúsculas (como US), conforme definido por ISO 3166-1. Por exemplo, digite en_US para inglês falado nos Estados Unidos. Se você não digitar nenhum código, o país e o idioma serão preenchidos automaticamente.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

O fuso horário em que o dispositivo está sendo executado. Digite um nome Olson no formato área/localização. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir um nome, o fuso horário será preenchido automaticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Esses dados não são necessários, pois o valor é codificado no aplicativo como Secure Hub. É mencionado aqui apenas para fins de conclusão.

Se houver uma rede Wi-Fi protegida usando WPA2, um arquivo nfcprovisioning.txt preenchido pode ser semelhante ao seguinte:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name`

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2`

`android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

Se houver uma rede Wi-Fi desprotegida, um arquivo nfcprovisioning.txt preenchido pode ser semelhante ao seguinte:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

Para obter o checksum do Citrix Secure Hub

O checksum do Secure Hub é um valor constante: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Para baixar um arquivo APK do Secure

Hub, use o seguinte link da Google Play Store: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

Para obter um checksum de aplicativo

Pré-requisitos:

- A ferramenta **apksigner** do Android SDK Build Tools
- Linha de comando OpenSSL

Para obter o checksum de qualquer aplicativo, siga estas etapas:

1. Baixe o arquivo APK do aplicativo na Google Play Store.
2. Na linha de comando OpenSSL, navegar até a ferramenta **apksigner**: `android-sdk/build-tools/<version>/apksigner` e digite o seguinte:

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   O comando retorna um checksum válido.
3. Para gerar o código QR, insira o checksum no campo `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`. Por exemplo:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }
```

```
}
```

Bibliotecas usadas

A Ferramenta de Provisionamento usa as seguintes bibliotecas em seu código-fonte:

- biblioteca v7 `appcompat`, biblioteca de suporte de Design e biblioteca v7 Palette do Google sob licença Apache 2.0

  Para obter informações, consulte Guia de Recursos da Biblioteca de Suporte.

- Butter Knife de Jake Wharton sob licença Apache 2.0

Registrando dispositivos usando um código QR

Para registrar um dispositivo totalmente gerenciado usando um código QR, você gera um código QR criando um JSON e convertendo o JSON em um código QR. As câmeras dos dispositivos escaneiam o código QR para registrar o dispositivo.

Requisitos do sistema

- Compatível com todos os dispositivos Android executando Android 9.0 e superior.

Criar um código QR a partir de um JSON

Crie um JSON com os seguintes campos.

Estes campos são obrigatórios:

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valor: com.zenprise/com.zenprise.configuration.AdminFunction

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valor: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valor: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Estes campos são opcionais:

- **android.app.extra.PROVISIONING_LOCALE:** Insira os códigos de idioma e país.

Os códigos de idioma são códigos de idioma ISO de duas letras minúsculas (como en), conforme definido por ISO 639-1. Os códigos de país são códigos de país ISO de duas letras maiúsculas (como US), conforme definido por ISO 3166-1. Por exemplo, insira en_US para inglês falado nos Estados Unidos.

- **android.app.extra.PROVISIONING_TIME_ZONE:** O fuso horário em que o dispositivo está sendo executado.

  Digite um nome Olson no formato área/localização. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir um, o fuso horário será preenchido automaticamente.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Tempo em milissegundos desde a Época.

  A época Unix (ou tempo Unix, tempo POSIX ou timestamp Unix) é o número de segundos que se passaram desde January 1, 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (em ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Defina como **true** para ignorar a criptografia durante a criação do perfil. Defina como **false** para forçar a criptografia durante a criação do perfil.

Um JSON típico se parece com o seguinte:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Valide o JSON criado usando qualquer ferramenta de validação de JSON, como https://jsonlint.com. Converta essa string JSON em um código QR usando qualquer gerador de código QR online, como https://www.qr-code-generator.com.

Este código QR é escaneado por um dispositivo redefinido de fábrica para registrar o dispositivo como um dispositivo totalmente gerenciado.

Para registrar o dispositivo

Após ligar um dispositivo novo ou redefinido de fábrica:

1. Toque na tela seis vezes na tela de boas-vindas para iniciar o fluxo de registro por código QR.
2. Quando solicitado, conecte-se ao Wi-Fi. O local de download do Secure Hub no código QR (codificado no JSON) é acessível por esta rede Wi-Fi.

   Assim que o dispositivo se conectar com sucesso ao Wi-Fi, ele baixa um leitor de código QR do Google e inicia a câmera.

3. Aponte a câmera para o código QR para escanear o código.

   O Android baixa o Secure Hub do local de download no código QR, valida a assinatura do certificado de assinatura, instala o Secure Hub e o define como proprietário do dispositivo.

Para obter mais informações, consulte este guia do Google para desenvolvedores Android EMM: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`.

Registro zero-touch

O registro zero-touch permite configurar dispositivos para que se provisionem como dispositivos totalmente gerenciados quando são ligados pela primeira vez.

Seu revendedor de dispositivos cria uma conta para você no portal Android zero-touch, uma ferramenta online que permite aplicar configurações a dispositivos. Usando o portal Android zero-touch, você cria uma ou mais configurações de registro zero-touch e as aplica aos dispositivos atribuídos à sua conta. Quando seus usuários ligam esses dispositivos, eles são automaticamente registrados no XenMobile. A configuração atribuída ao dispositivo define seu processo de registro automático.

Requisitos do sistema

- O suporte para registro zero-touch começa com o Android 9.0.

Dispositivos e informações da conta do seu revendedor

- Dispositivos elegíveis para o registro zero-touch são comprados de um revendedor empresarial ou parceiro do Google. Para obter uma lista de parceiros zero-touch do Android Enterprise, consulte o site do Android.
- Uma conta do portal zero-touch do Android Enterprise, criada pelo seu revendedor.
- Informações de login da conta do portal zero-touch do Android Enterprise, fornecidas pelo seu revendedor.

Criar uma configuração zero-touch

Ao criar uma configuração zero-touch, inclua um JSON personalizado para especificar os detalhes da configuração.

Use este JSON para configurar o dispositivo para se registrar no XenMobile Server que você especificar. Substitua o URL do seu servidor por 'URL' neste exemplo.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL",

   }

}
```

Você pode usar um JSON opcional com mais parâmetros para personalizar ainda mais sua configuração. Este exemplo especifica o XenMobile Server e o nome de usuário e senha que os dispositivos que usam esta configuração utilizam para fazer logon no servidor.

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

     {

         "serverURL":"URL",

         "xm_username":"username",

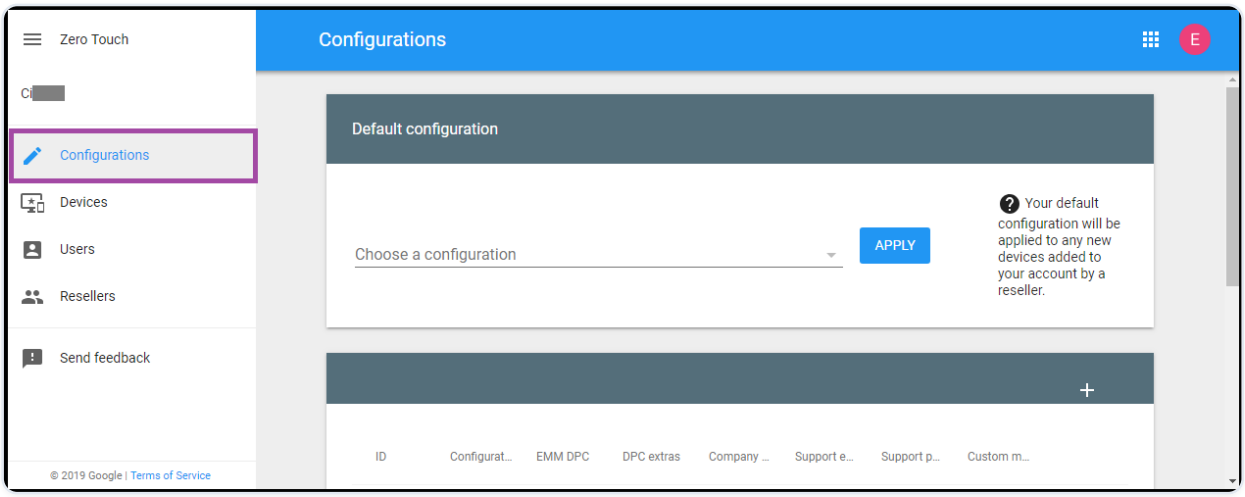
         "xm_password":"password"

     }

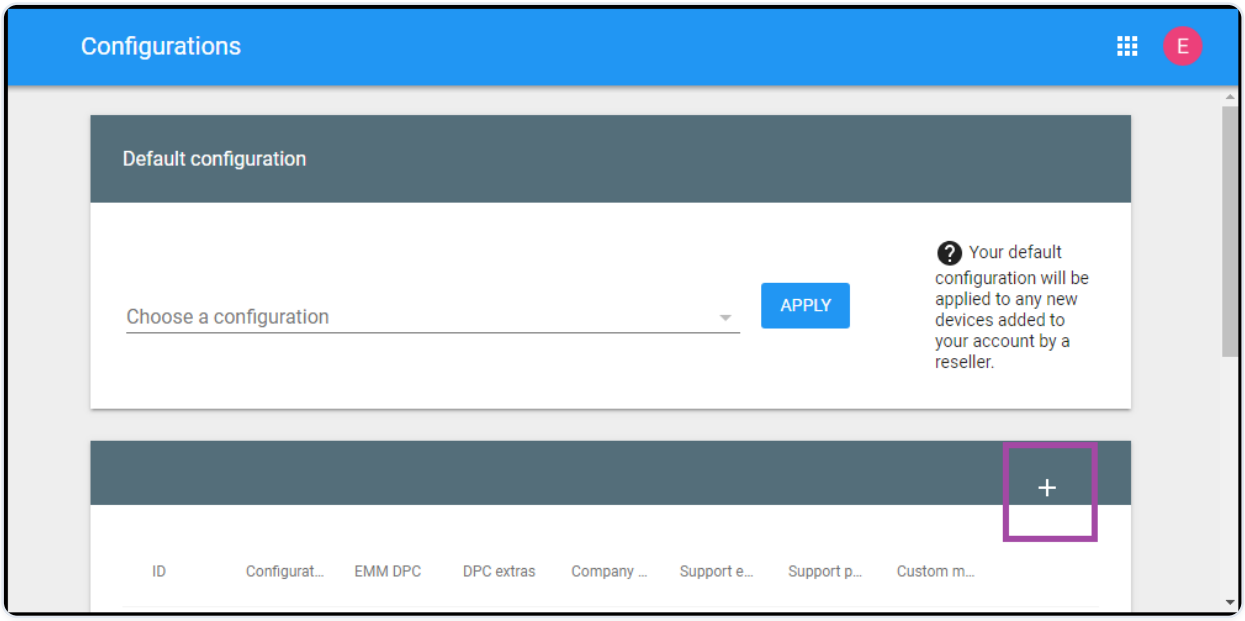
       }
```

1. Vá para o portal zero-touch do Android em https://partner.android.com/zerotouch. Faça login com as informações da conta do seu revendedor de dispositivos zero-touch.

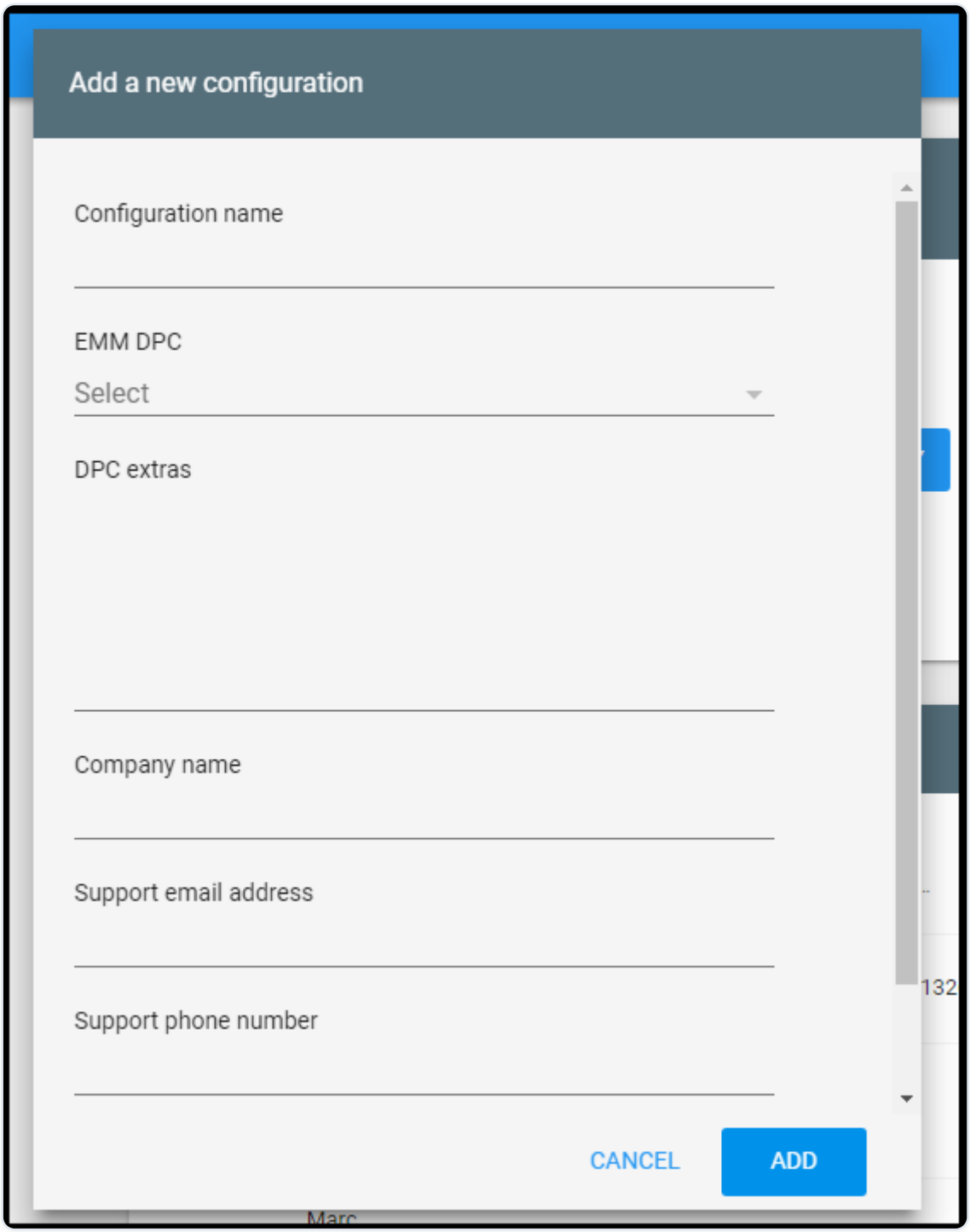
2. Clique em **Configuração**.



3. Clique em **+** acima da tabela de configuração.



4. Insira suas informações de configuração na janela de configuração que aparece.



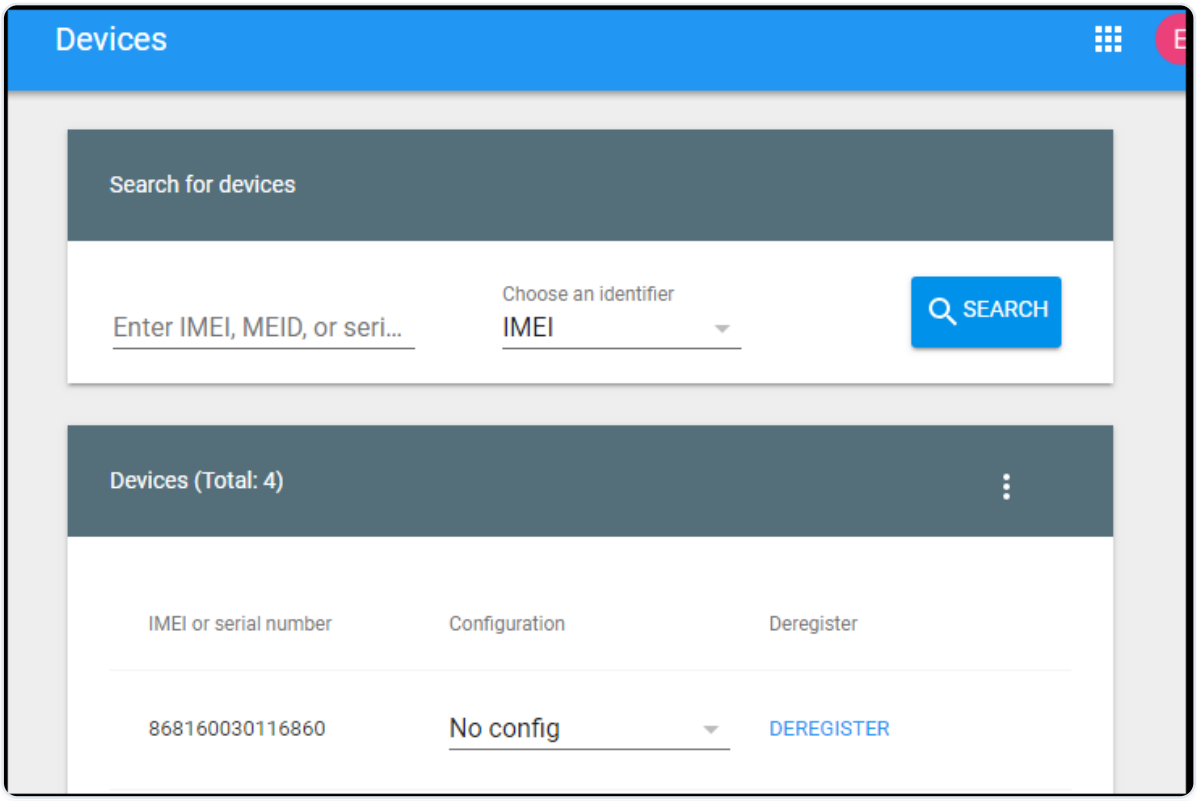
- **Nome da configuração:** Digite o nome que você escolher para esta configuração.
- **EMM DPC:** Escolha **Citrix Secure Hub**.
- **Extras do DPC:** Cole seu texto JSON personalizado neste campo.
- **Nome da empresa:** Digite o nome que você deseja que apareça em seus dispositivos zero-touch do Android Enterprise durante o provisionamento do dispositivo.

- **Endereço de e-mail de suporte:** Digite um endereço de e-mail que seus usuários podem contatar para obter ajuda. Este endereço aparece em seus dispositivos Android Enterprise zero-touch antes do provisionamento do dispositivo.
- **Número de telefone de suporte:** Digite um número de telefone que seus usuários podem contatar para obter ajuda. Este número de telefone aparece em seus dispositivos Android Enterprise zero-touch antes do provisionamento do dispositivo.
- **Mensagem personalizada:** Opcionalmente, adicione uma ou duas frases para ajudar seus usuários a contatá-lo ou para fornecer mais detalhes sobre o que está acontecendo com o dispositivo deles. Esta mensagem personalizada aparece em seus dispositivos Android Enterprise zero-touch antes do provisionamento do dispositivo.

5. Clique em **Adicionar**.
6. Para criar mais configurações, repita as etapas 2 a 4.
7. Para aplicar uma configuração a um dispositivo:

   a. No portal Android zero-touch, clique em **Dispositivos**.

   b. Encontre o dispositivo na lista de dispositivos e escolha a configuração que deseja atribuir a ele.



   c. Clique em **Atualizar**.

Você pode aplicar uma configuração a muitos dispositivos usando um arquivo CSV.

Para obter informações sobre como aplicar uma configuração a muitos dispositivos, consulte o tópico de ajuda do Android Enterprise Inscrição zero-touch para administradores de TI. Este tópico de ajuda do Android Enterprise tem mais informações sobre como gerenciar configurações e aplicá-las a dispositivos.

Provisionamento de dispositivos Android Enterprise dedicados

Dispositivos Android Enterprise dedicados são dispositivos totalmente gerenciados que são dedicados a cumprir um único caso de uso. Dispositivos dedicados também são conhecidos como dispositivos de uso único de propriedade corporativa (COSU). Você restringe esses dispositivos a um aplicativo ou a um pequeno conjunto de aplicativos necessários para realizar as tarefas exigidas para este caso de uso. Você também impede que os usuários habilitem outros aplicativos ou realizem outras ações no dispositivo.

Registre dispositivos dedicados usando qualquer um dos métodos de registro usados para outros dispositivos totalmente gerenciados, conforme descrito em Provisionamento de dispositivos Android Enterprise totalmente gerenciados. O provisionamento de dispositivos dedicados requer mais configuração antes do registro.

Para provisionar dispositivos dedicados:

- Adicione um perfil de registro para administradores do XenMobile que você permite registrar dispositivos dedicados em sua implantação do XenMobile. Consulte Criação de perfis de registro.
- Permita os aplicativos que você deseja que o dispositivo dedicado acesse.
- Opcionalmente, defina o aplicativo permitido para permitir o modo de tarefa bloqueada. Quando um aplicativo está no modo de tarefa bloqueada, ele é fixado na tela do dispositivo quando o usuário o abre. Nenhum botão Início aparece e o botão Voltar é desativado. O usuário sai do aplicativo usando uma ação programada no aplicativo, como sair.
- Registre cada dispositivo no perfil de registro que você adicionou.

Requisitos do sistema

- O suporte para registro de dispositivos dedicados começa com o Android 6.0.

Permitir aplicativos e definir o modo de tarefa bloqueada

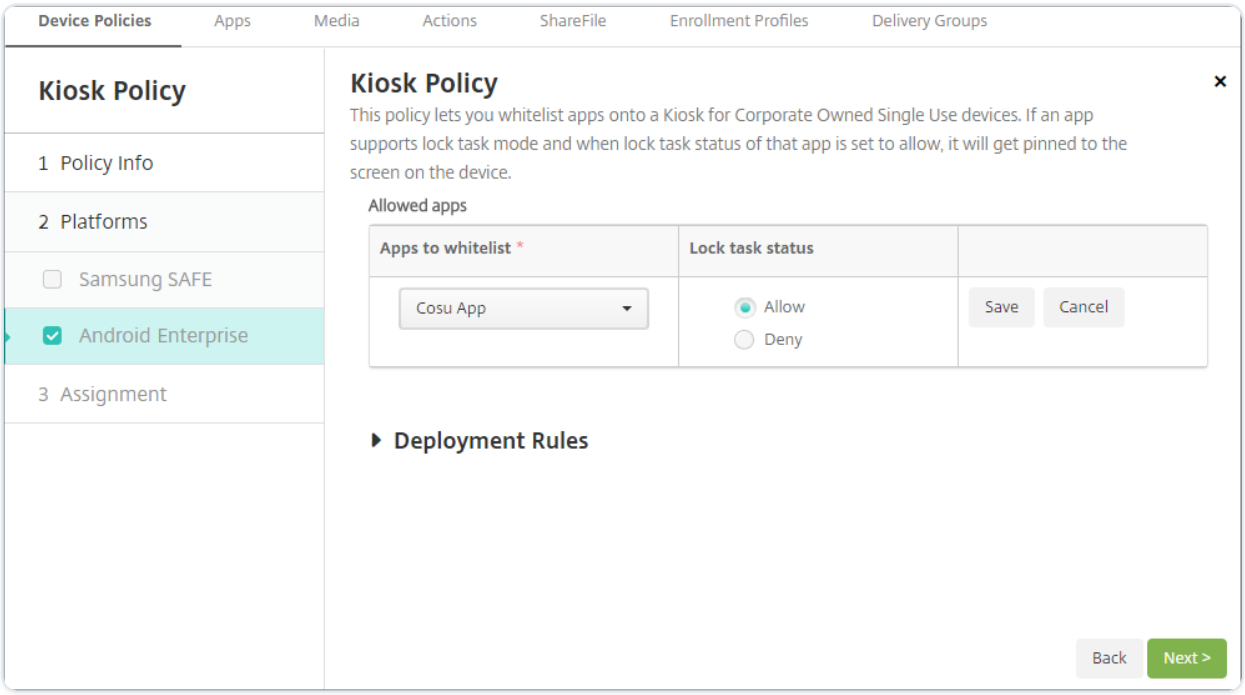
A política de dispositivo Kiosk permite que você permita aplicativos e defina o modo de tarefa bloqueada. Por padrão, o Secure Hub e os serviços do Google Play são permitidos.

Para adicionar a política Kiosk:

1. No console do XenMobile, clique em **Configurar > Políticas de Dispositivo**. A página **Políticas de Dispositivo** é exibida.
2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Nova Política** é exibida.
3. Expanda **Mais** e, em seguida, em Segurança, clique em **Kiosk**. A página **Política de Kiosk** é exibida.
4. Em Plataformas, selecione **Android Enterprise**. Desmarque outras plataformas.
5. No painel Informações da Política, digite o **Nome da Política** e uma **Descrição** opcional.
6. Clique em **Avançar** e, em seguida, clique em **Adicionar**.
7. Para permitir um aplicativo e permitir ou negar o modo de tarefa bloqueada para esse aplicativo:

   Selecione o aplicativo que você deseja permitir na lista.

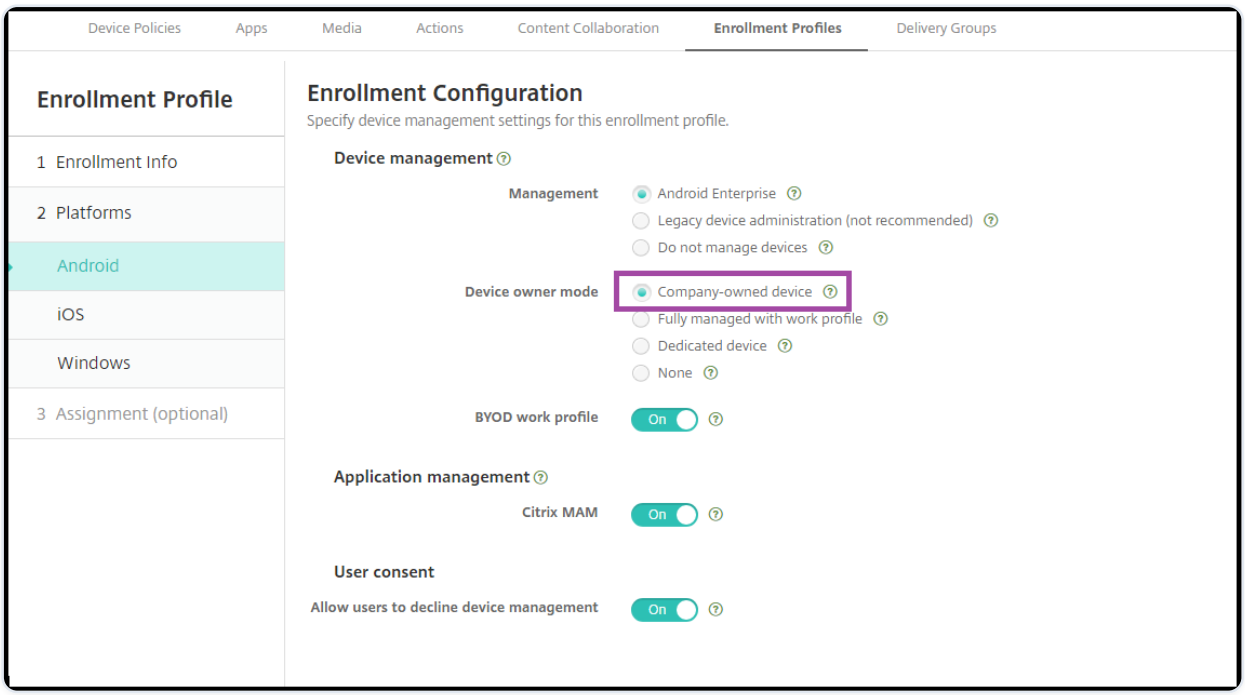
   Escolha **Permitir** para definir que o aplicativo seja fixado na tela do dispositivo quando o usuário o iniciar. Escolha **Negar** para definir que o aplicativo não seja fixado. O padrão é **Permitir**.



8. Clique em **Salvar**.
9. Para permitir outro aplicativo e permitir ou negar o modo de tarefa bloqueada para esse aplicativo, clique em **Adicionar**.
10. Configure as regras de implantação e escolha os grupos de entrega. Para obter mais informações, consulte Políticas de dispositivo.

Para registrar o dispositivo

1. Clique em **Avançar** ou selecione **Android** em **Plataformas**. A página Configuração de Registro é exibida.
2. Defina **Gerenciamento** como **Android Enterprise**.
3. Defina **Modo de proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.



4. Selecione **Atribuição (opções)**. A tela Atribuição de Grupo de Entrega é exibida.
5. Escolha o grupo de entrega ou os grupos de entrega que contêm os administradores que registram os dispositivos dedicados. Em seguida, clique em **Salvar**.

Se você ativou o **perfil de trabalho BYOD** no perfil de registro, os dispositivos que não são novos ou redefinidos de fábrica são registrados como dispositivos de perfil de trabalho. Consulte Provisionamento de dispositivos de perfil de trabalho do Android Enterprise.

Provisionar dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Dispositivos totalmente gerenciados com um perfil de trabalho, anteriormente chamados de dispositivos COPE, são dispositivos de propriedade da empresa que são usados para fins profissionais e pessoais. Sua organização gerencia todos os dispositivos. Você pode aplicar um conjunto de políticas ao dispositivo e um conjunto separado de políticas ao perfil de trabalho.

No console do XenMobile, os dispositivos totalmente gerenciados com um perfil de trabalho aparecem com estes termos:

- A propriedade do dispositivo é "Corporativa".
- O tipo de instalação do Android Enterprise do dispositivo é "Proprietário Corporativo Pessoalmente Habilitado".

Requisitos do sistema

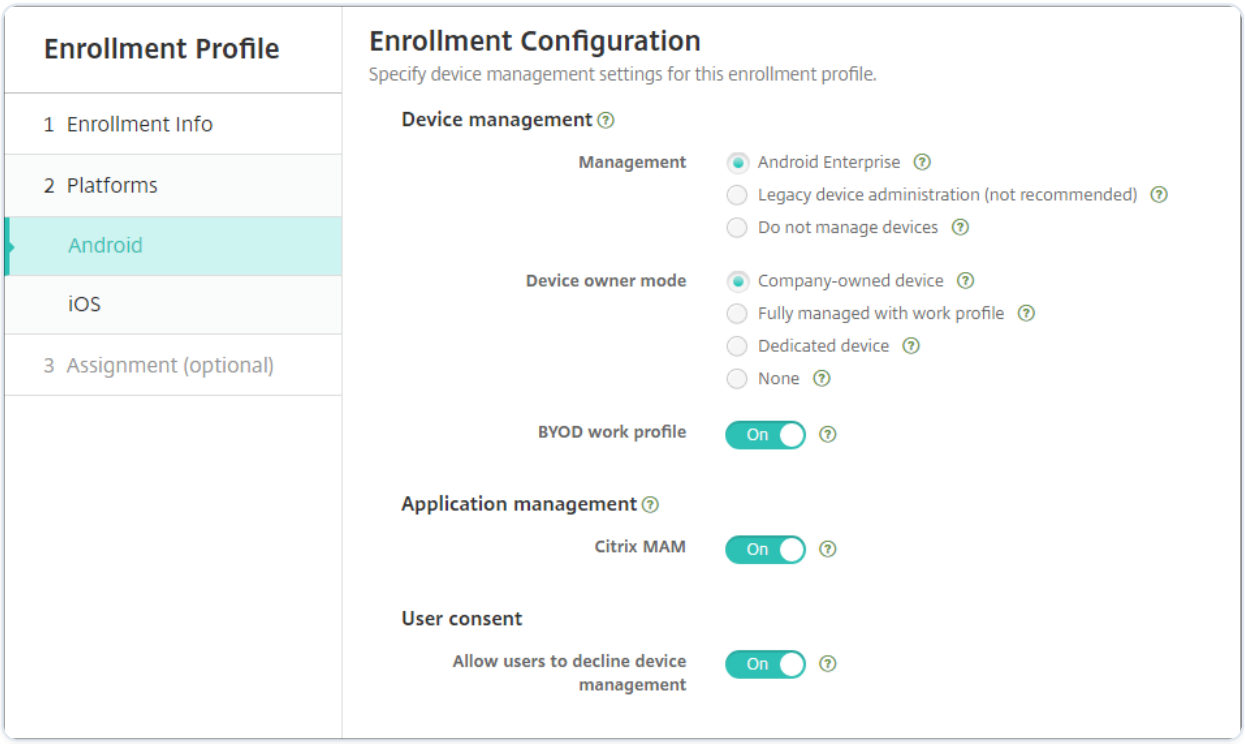
- O suporte para registrar dispositivos totalmente gerenciados com perfis de trabalho começa do Android 9.0 ao Android 10.x.

Adicionar um perfil de registro para dispositivos totalmente gerenciados com perfis de trabalho

Crie um perfil de registro para registrar dispositivos totalmente gerenciados com perfis de trabalho. Os administradores nos grupos de entrega atribuídos a este perfil de registro podem registrar dispositivos totalmente gerenciados com perfis de trabalho. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com dispositivos ilimitados permitidos por usuário. Atribua este perfil a um grupo de entrega que tenha os administradores que registram dispositivos totalmente gerenciados com perfis de trabalho.

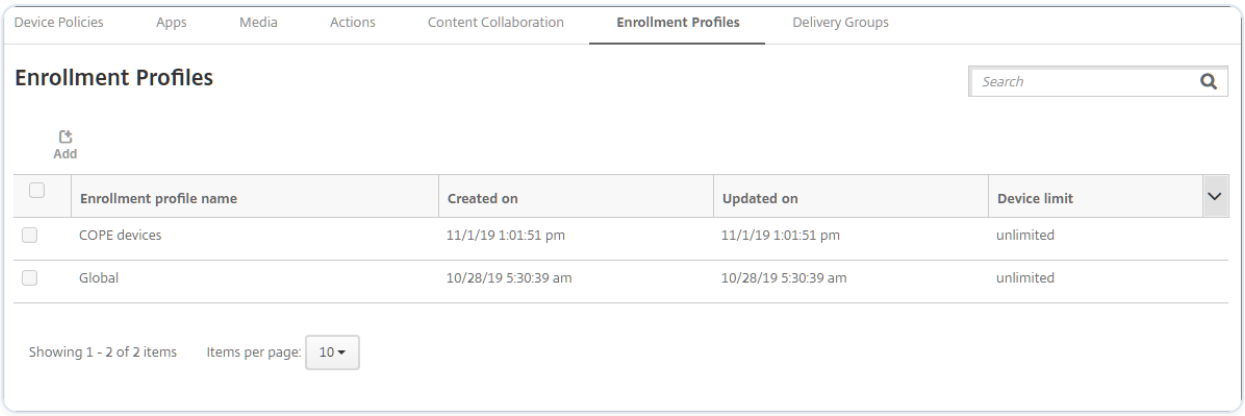
1. No console do XenMobile, vá para **Configurar > Perfis de Registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página Informações de Registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.
3. Clique em **Avançar** ou selecione **Android Enterprise** em **Plataformas**. A página Configuração de Registro é exibida.
4. Defina **Tipo de Registro** como um dos seguintes:

    - **Totalmente gerenciado/Perfil de trabalho:** Novos dispositivos ou dispositivos redefinidos de fábrica são registrados como totalmente gerenciados. Dispositivos BYOD são registrados apenas com um perfil de trabalho gerenciado por você.
    - **COPE/Perfil de trabalho:** Novos dispositivos ou dispositivos redefinidos de fábrica são registrados como totalmente gerenciados com um perfil de trabalho. Dispositivos BYOD são registrados apenas com um perfil de trabalho gerenciado por você.



5. Selecione **Atribuição (opcional)** ou clique em **Avançar**. A tela de Atribuição de Grupo de Entrega é exibida.
6. Escolha o grupo de entrega ou os grupos de entrega que contêm os administradores que registram os dispositivos dedicados. Em seguida, clique em **Salvar**.

   A página Perfil de Registro é exibida com o perfil que você adicionou.



Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabetizada de grupos de entrega.

Para registrar o dispositivo

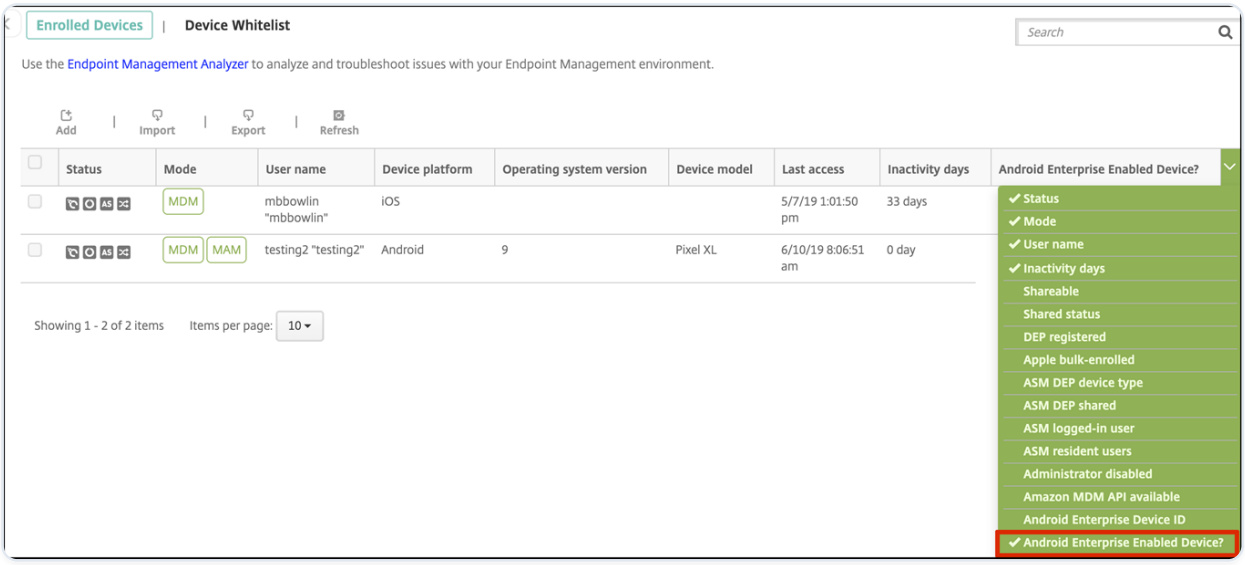
Dispositivos novos e redefinidos de fábrica são registrados como dispositivos totalmente gerenciados com um perfil de trabalho usando o token de identificador DPC, o toque de comunicação de campo próximo (NFC) ou os métodos de código QR. Consulte Registrando

dispositivos usando o token de identificador DPC da Citrix, Registrando dispositivos com toque NFC ou Registrando dispositivos usando um código QR.

Dispositivos que não são novos ou redefinidos de fábrica são registrados como dispositivos de perfil de trabalho, conforme descrito em Provisionando dispositivos de perfil de trabalho do Android Enterprise.

Visualizando dispositivos Android Enterprise no console do XenMobile

1. No console do XenMobile, vá para **Gerenciar > Dispositivos**.
2. Adicione a coluna **Dispositivo Android Enterprise Habilitado?** clicando no menu à direita da tabela nesta página.



3. Para visualizar as ações de segurança disponíveis, selecione um dispositivo totalmente gerenciado e clique em **Proteger**. Quando o dispositivo é totalmente gerenciado, a ação **Limpeza Completa** está disponível, mas a **Limpeza Seletiva** não. Essa diferença ocorre porque o dispositivo permite apenas aplicativos da Google Play Store gerenciada. Não há opção para o usuário instalar aplicativos da loja pública. Sua organização gerencia todo o conteúdo do dispositivo.



Configurar políticas de dispositivo e aplicativo do Android Enterprise

Para uma visão geral das políticas controladas nos níveis de dispositivo e aplicativo, consulte Políticas de dispositivo e políticas MDX compatíveis para Android Enterprise.

O que saber sobre as políticas:

- **Proteção contra perda de dados:** A tecnologia de contêiner MAM do XenMobile protege aplicativos com criptografia e outras tecnologias de Prevenção de Perda de Dados (DLP) móveis. Use o Citrix MAM SDK ou o MDX Toolkit para habilitar aplicativos para MDX.
- **Restrições de dispositivo:** Dezenas de restrições de dispositivo permitem controlar recursos como:
  - Uso da câmera do dispositivo
  - Uso de copiar e colar entre perfis de trabalho e pessoais
- **VPN por aplicativo:** Use a política de dispositivo de configurações gerenciadas para configurar perfis de VPN para Android Enterprise.
- **Política de e-mail:** Recomendamos usar a política de dispositivo de configurações gerenciadas para configurar aplicativos.

Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos Android Enterprise.

> **Importante:**

Para dispositivos que se registram no Android Enterprise e usam aplicativos MDX: Você pode controlar algumas configurações através do MDX e do Android Enterprise. Use as configurações de política menos restritivas para MDX e controle a política através do Android Enterprise.

Permissões de aplicativo do Android Enterprise	Configurações gerenciadas	Inventário de aplicativos
Desinstalação de aplicativo	Atualizar automaticamente aplicativos gerenciados	Controlar atualização do SO
Credenciais	XML personalizado	Exchange
Arquivos	Gerenciamento de tela de bloqueio	Quiosque
Localização	Senha	Restrições
Chave de licença MDM da Samsung	Agendamento	Wi-Fi
Opções do XenMobile		

Políticas de dispositivo para dispositivos totalmente gerenciados com perfil de trabalho (dispositivos COPE)

Para dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE), algumas políticas de dispositivo podem ser usadas para aplicar configurações separadas a todo o dispositivo e ao perfil de trabalho. Você pode usar outras políticas de dispositivo para aplicar configurações apenas a todo o dispositivo ou apenas ao perfil de trabalho de dispositivos totalmente gerenciados com perfis de trabalho.

POLÍTICA	APLICA-SE A
Permissões de aplicativo do Android Enterprise	Perfil de trabalho
Configurações gerenciadas	Perfil de trabalho

POLÍTICA	APLICA-SE A
Inventário de aplicativos	Perfil de trabalho
Desinstalação de aplicativo	Perfil de trabalho
Atualizar automaticamente aplicativos gerenciados	Perfil de trabalho
Controlar atualização do SO	N/A
Credenciais	Perfil de trabalho
XML personalizado	N/A
Exchange	N/A
Arquivos	Perfil de trabalho
Gerenciamento de tela de bloqueio	Dispositivo e perfil de trabalho
Quiosque	N/A
Localização	Dispositivo (somente modo de localização)
Senha	Dispositivo e perfil de trabalho
Restrições	Dispositivo e perfil de trabalho (crie políticas separadas para o dispositivo e o perfil de trabalho)
Chave de licença Samsung MDM	N/A
Agendamento	Perfil de trabalho
Wi-Fi	Dispositivo
Opções do XenMobile	Perfil de trabalho

Consulte também, Políticas de dispositivo e políticas MDX compatíveis para Android Enterprise e Visão geral do SDK MAM.

Ações de segurança

O Android Enterprise oferece suporte às seguintes ações de segurança. Para uma descrição de cada ação de segurança, consulte Ações de segurança.

AÇÃO DE SEGURANÇA	PERFIL DE TRABALHO	TOTALMENTE GERENCIADO
Renovação de certificado	Sim	Sim
Limpeza completa	Não	Sim
Localizar	Sim	Sim
Bloquear	Sim	Sim
Bloquear e Redefinir Senha	Não	Sim
Notificar (Tocar)	Sim	Sim
Revogar	Sim	Sim
Limpeza Seletiva	Sim	Não

Notas sobre ações de segurança

- A ação de segurança de localização falha a menos que a política de dispositivo de Localização defina o modo de localização para o dispositivo como **Alta Precisão** ou **Economia de Bateria**. Consulte Política de dispositivo de Localização.
- Em dispositivos com perfil de trabalho que executam versões do Android anteriores ao Android 9.0:
    - A ação de bloqueio e redefinição de senha não é suportada.
- Em dispositivos com perfil de trabalho com Android 9.0 ou superior:
    - A senha enviada bloqueia o perfil de trabalho. O dispositivo em si não é bloqueado.
    - Se nenhuma senha for definida no perfil de trabalho:
        - Se nenhuma senha for enviada, ou a senha enviada não atender aos requisitos de senha: O dispositivo é bloqueado.
    - Se uma senha for definida no perfil de trabalho:

    - Se nenhuma senha for enviada, ou a senha enviada não atender aos requisitos de senha: O perfil de trabalho é bloqueado, mas o dispositivo em si não é bloqueado.

- Em dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE):
    - Você pode aplicar a ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho

Cancelar o registro de uma empresa Android Enterprise

Se você não quiser mais usar sua empresa Android Enterprise, poderá cancelar o registro da empresa.

> **Aviso:**

> Depois de cancelar o registro de uma empresa, os aplicativos Android Enterprise em dispositivos já registrados por meio dela são redefinidos para seus estados padrão. O Google não gerencia mais os dispositivos. Se você se registrar em uma nova empresa Android Enterprise, deverá aprovar os aplicativos para a nova organização no Google Play gerenciado. Em seguida, você pode atualizar os aplicativos do console XenMobile.

> Depois que o registro da empresa Android Enterprise for cancelado:

- Dispositivos e usuários registrados por meio da empresa têm os aplicativos Android Enterprise redefinidos para o estado padrão. As políticas de Configurações Gerenciadas aplicadas anteriormente não afetam mais as operações.
- O XenMobile gerencia dispositivos registrados através da empresa. Na perspectiva do Google, esses dispositivos não são gerenciados. Você não pode adicionar novos aplicativos do Android Enterprise. Você não pode aplicar políticas de Configurações Gerenciadas. Você pode aplicar outras políticas, como Agendamento, Senha e Restrições, a esses dispositivos.
- Se você tentar registrar dispositivos no Android Enterprise, eles serão registrados como dispositivos Android, e não como dispositivos Android Enterprise.

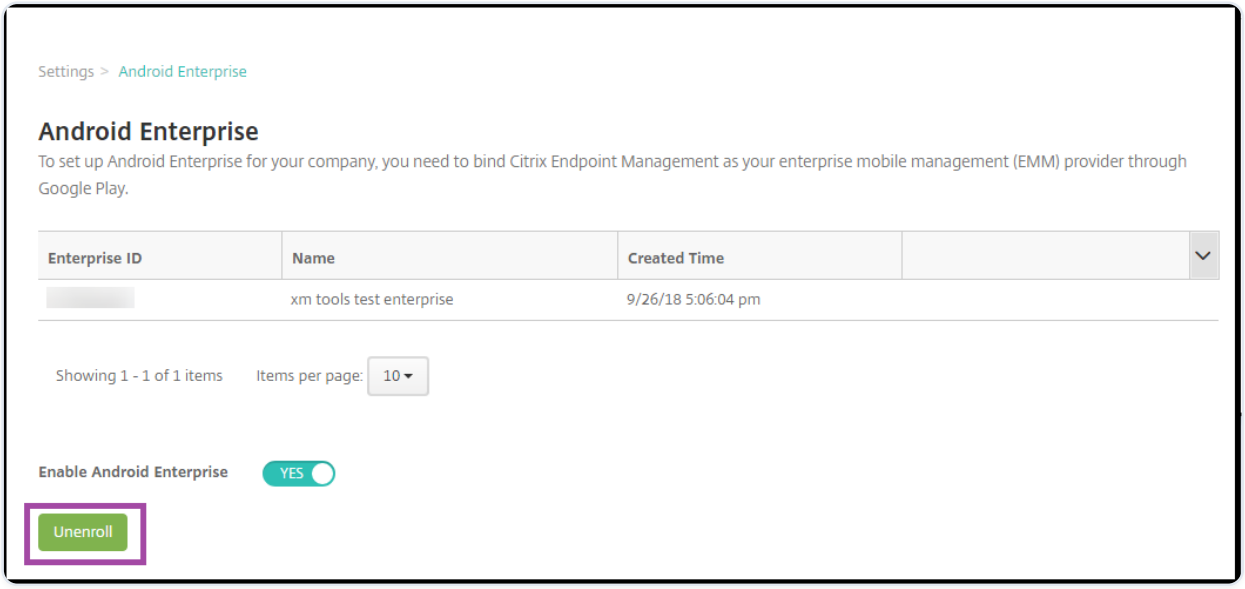
Cancele o registro de uma empresa Android Enterprise usando o console do XenMobile Server e as Ferramentas XenMobile.

Ao realizar esta tarefa, o XenMobile abre uma janela pop-up para as Ferramentas XenMobile. Antes de começar, certifique-se de que o XenMobile tenha permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você

desative o bloqueio de pop-ups e adicione o endereço do site do XenMobile à lista de permissões de bloqueio de pop-ups.

Para cancelar o registro de uma empresa Android Enterprise:

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página Configurações é exibida.
2. Na página Configurações, clique em **Android Enterprise**.
3. Clique em **Cancelar registro**.



Distribuir aplicativos Android Enterprise

O XenMobile® gerencia aplicativos implantados em dispositivos. Você pode organizar e implantar os seguintes tipos de aplicativos Android Enterprise.

- **Aplicativos da loja de aplicativos gerenciada:** Esses aplicativos incluem aplicativos gratuitos disponíveis na Google Play Store gerenciada. Por exemplo, GoToMeeting.
- **MDX:** Aplicativos preparados com o MAM SDK ou empacotados com o MDX Toolkit. Esses aplicativos incluem políticas MDX. Você obtém aplicativos MDX de fontes internas e lojas públicas. Implante aplicativos de produtividade móvel Citrix® como aplicativos MDX.
- **Empresarial:** Aplicativos privados que você desenvolve ou obtém de outra fonte. Você fornece esses aplicativos aos seus usuários por meio da Google Play Store gerenciada. A Google Play Store gerenciada é a loja de aplicativos empresariais do Google.
- **Aplicativos privados habilitados para MDX:** Aplicativos empresariais preparados com o MAM SDK ou empacotados com o MDX Toolkit.

Você pode adicionar aplicativos empresariais e aplicativos privados habilitados para MDX de duas maneiras diferentes.

- Adicione os aplicativos ao console do XenMobile como aplicativos empresariais, conforme descrito nas seções Aplicativos empresariais e Aplicativos privados habilitados para MDX neste artigo.
- Publique os aplicativos diretamente na Google Play Store gerenciada usando sua conta de desenvolvedor do Google. Em seguida, adicione os aplicativos ao console do XenMobile como aplicativos da loja de aplicativos gerenciada. Consulte Aplicativos da loja de aplicativos gerenciada.

Se você publicar aplicativos usando sua conta de desenvolvedor do Google e depois mudar para o console do XenMobile, a propriedade dos aplicativos será diferente. Gerencie seus aplicativos em ambos os locais, neste caso. A Citrix recomenda adicionar seus aplicativos usando um método ou outro.

Se você precisar remover aplicativos autogerenciados da Google Play Store gerenciada, abra um tíquete com o Google. Os desenvolvedores podem desativar, mas não excluir, aplicativos da Google Play Store gerenciada.

As seções a seguir fornecem informações mais detalhadas para a configuração de aplicativos Android Enterprise. Para obter informações sobre a distribuição de aplicativos, consulte Adicionar aplicativos. Esse artigo inclui:

- Os fluxos de trabalho gerais para adicionar aplicativos web e SaaS ou links da web
- O fluxo de trabalho de aplicativo necessário para aplicativos empresariais e de loja pública
- Como entregar aplicativos empresariais da Citrix Content Delivery Network (CDN) for Enterprise Apps

Aplicativos da loja de aplicativos gerenciada

Você pode adicionar aplicativos gratuitos disponíveis na Google Play Store gerenciada ao XenMobile.

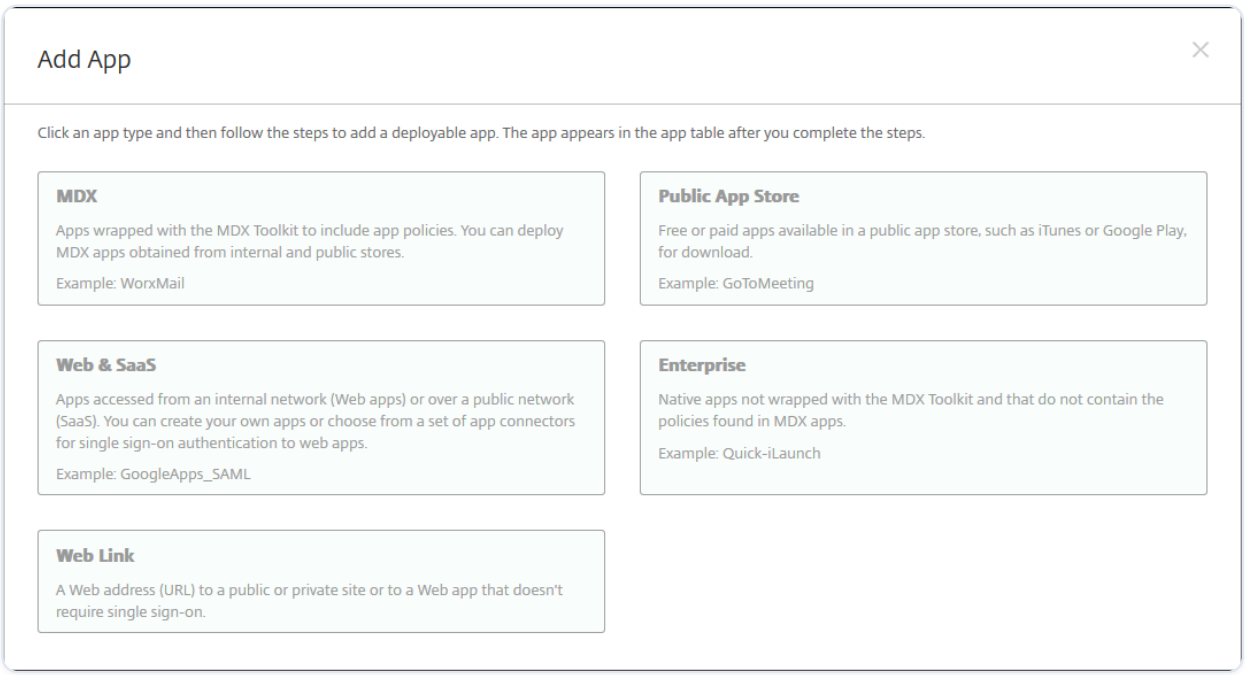
> **Nota:**

> Para tornar todos os aplicativos da Google Play Store acessíveis a partir do Google Play gerenciado, use a propriedade de servidor **Acessar todos os aplicativos na Google Play Store gerenciada**. Consulte Propriedades do servidor. Definir esta propriedade como **true**

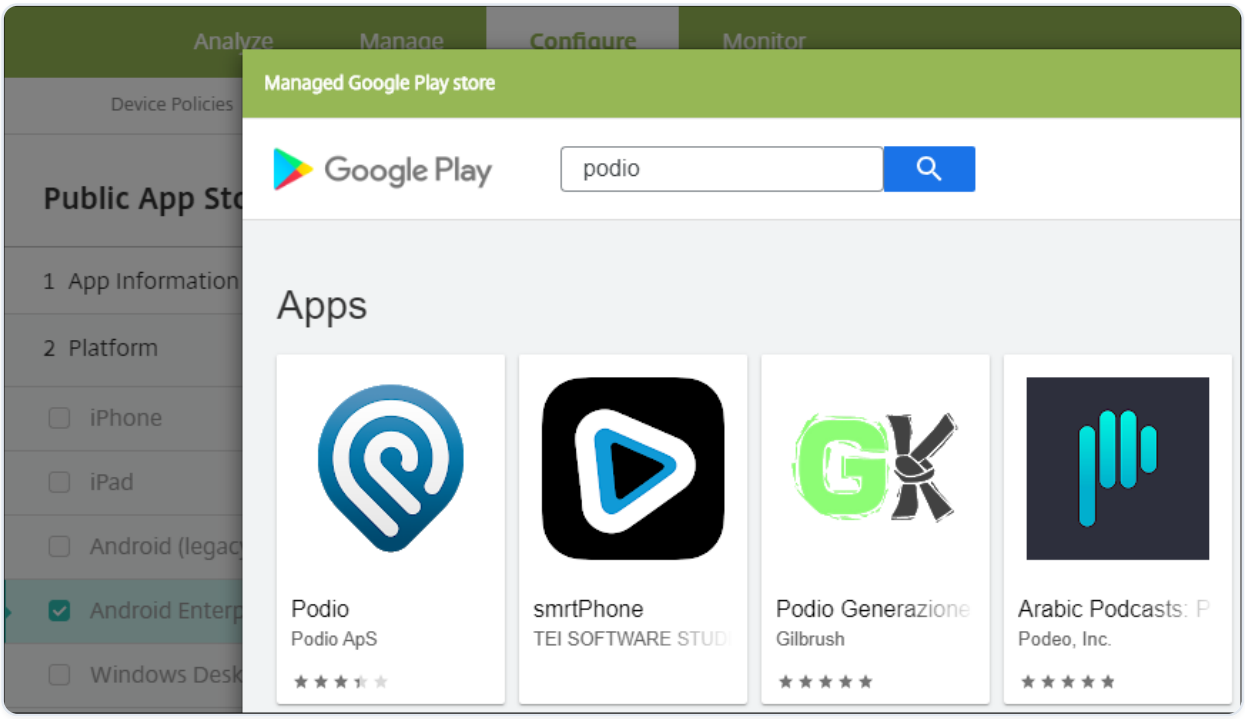
> permite que todos os usuários do Android Enterprise acessem aplicativos públicos da Google Play Store. Você pode então usar a política de dispositivo Restrições para controlar o acesso a esses aplicativos.

Etapa 1: Adicionar e configurar aplicativos

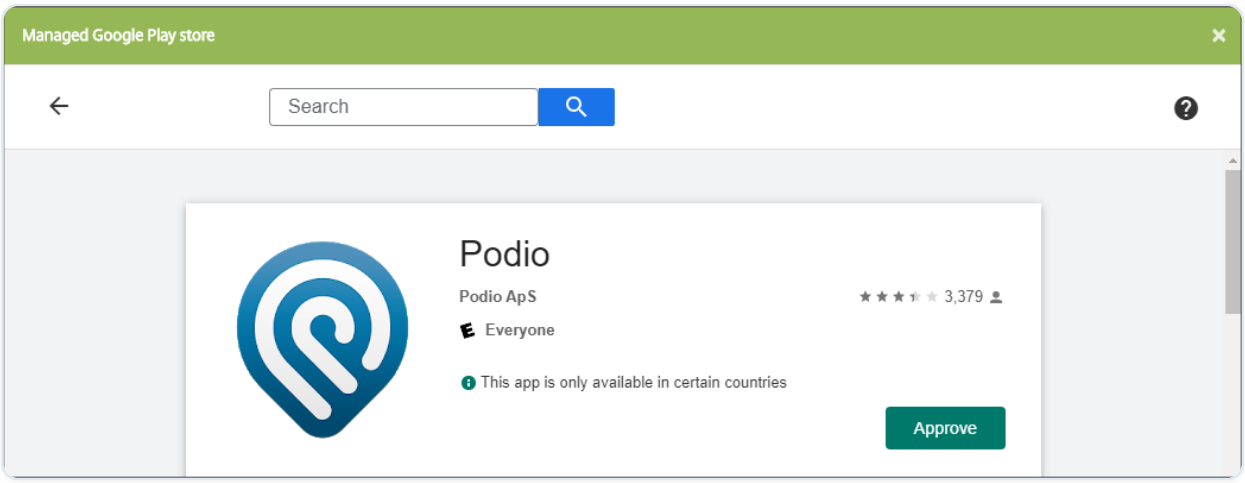
1. No console do XenMobile, navegar até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **Loja de Aplicativos Pública**.



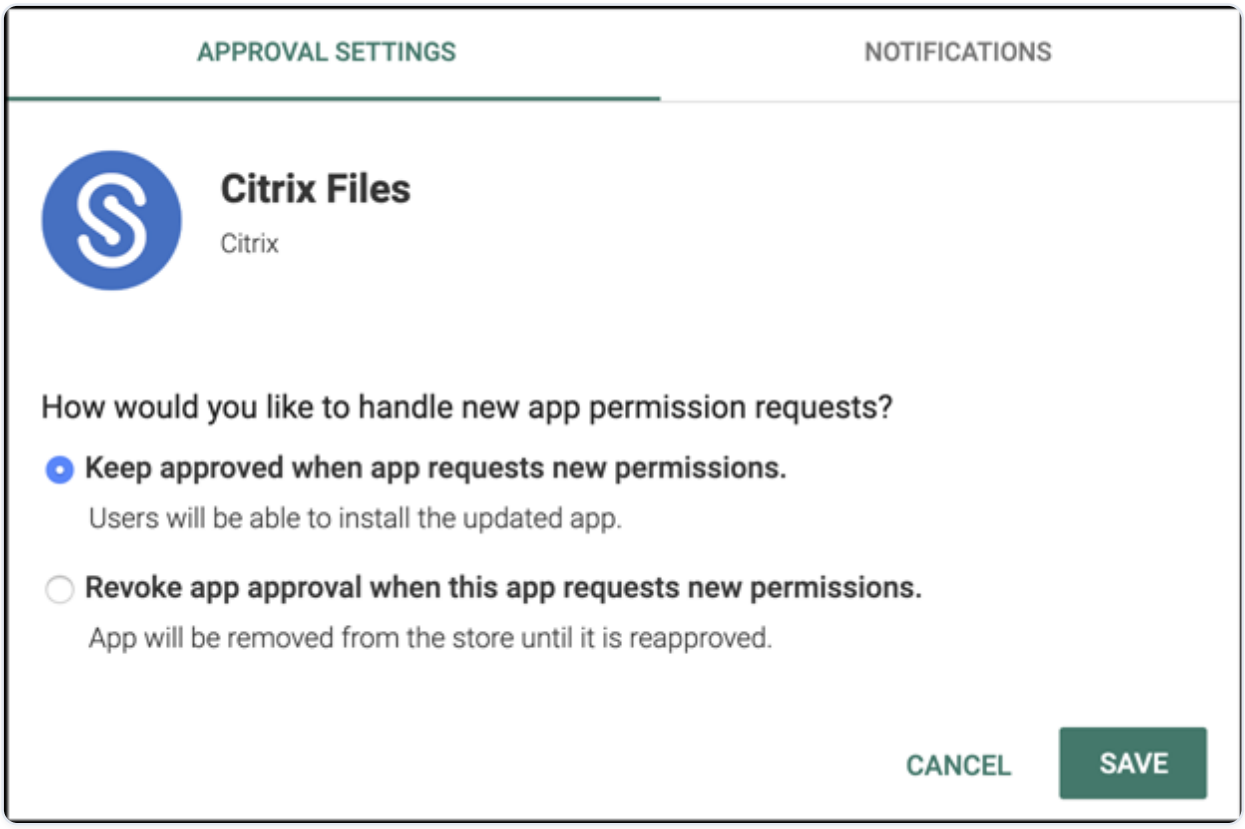
3. No painel **Informações do Aplicativo**, digite as seguintes informações:
   - **Nome:** Digite um nome descritivo para o aplicativo. O nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
   - **Descrição:** Digite uma descrição opcional do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
4. Selecione **Android Enterprise** como a plataforma.
5. Digite o nome do aplicativo ou o ID do pacote na caixa de pesquisa e clique em **Pesquisar**. Você pode localizar o ID do pacote na Google Play Store. O ID está na URL do aplicativo. Por exemplo, `com.Slack` é o ID do pacote em `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.



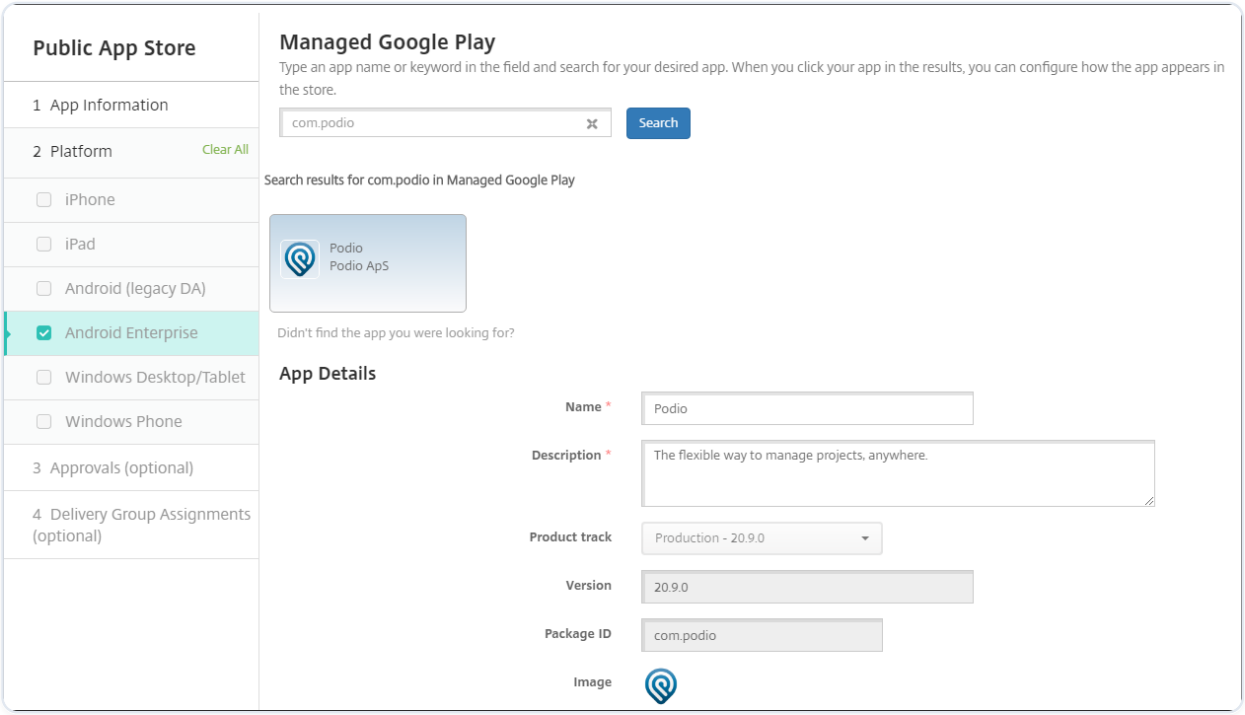
6. Os aplicativos que correspondem aos critérios de pesquisa aparecem. Clique no aplicativo desejado e, em seguida, clique em **Aprovar**.



7. Clique em **Aprovar** novamente.
8. Selecione **Manter aprovado quando o aplicativo solicitar novas permissões**. Clique em **Salvar**.



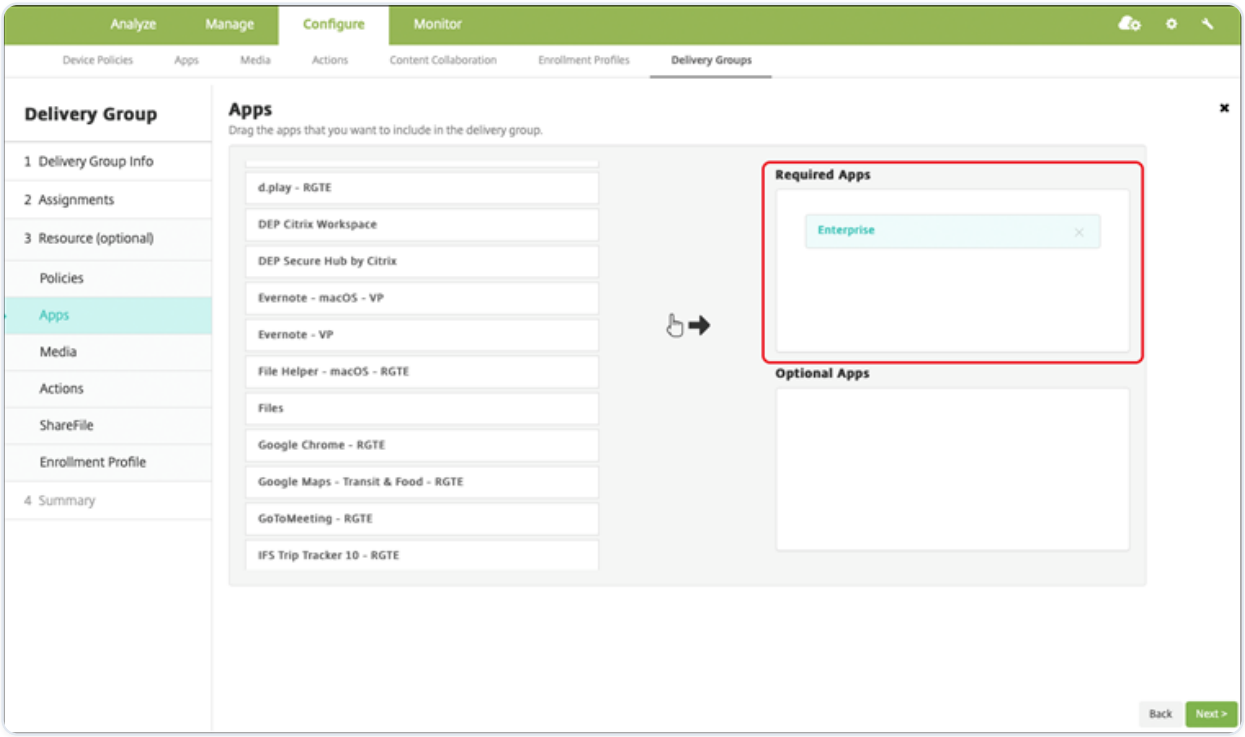
9. Clique no ícone do aplicativo e configure o **Nome** e a **Descrição** do aplicativo.



10. Atribua quaisquer grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte Implantar recursos.

Etapa 2: Configurar a implantação do aplicativo

1. navegar até **Configurar > Grupos de Entrega** e selecione o grupo de entrega que você configurou. Clique em **Editar**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa **Aplicativos Obrigatórios**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

Aplicativos MDX

Adicione arquivos MDX ao XenMobile e configure os detalhes do aplicativo e as configurações de política. Para configurar aplicativos de produtividade móvel Citrix para Android Enterprise, adicione-os como aplicativos MDX. Para obter informações sobre as políticas de aplicativo disponíveis para cada tipo de plataforma de dispositivo, consulte:

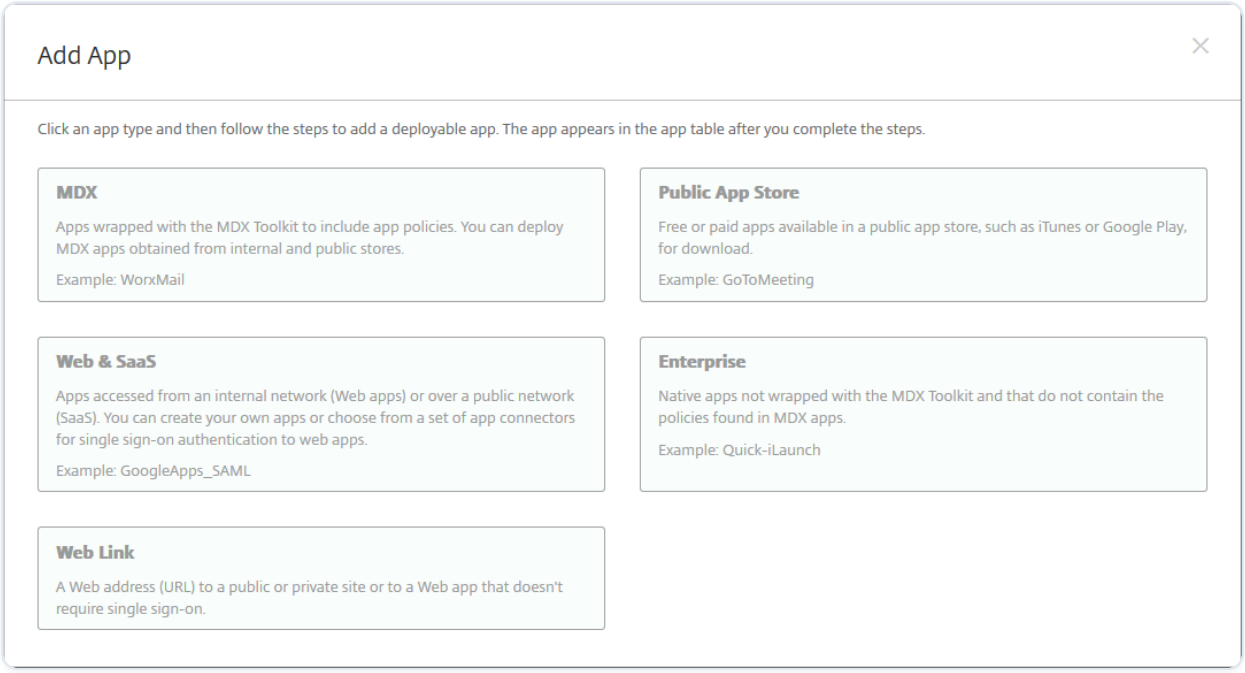
- Visão geral do SDK MAM
- Políticas MDX em um relance

Etapa 1: Adicionar e configurar aplicativos

1. Para aplicativos de produtividade móvel da Citrix, baixe os arquivos MDX da loja pública: Vá para `<https://www.citrix.com/downloads>`. navegar para **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   Para outros tipos de aplicativos MDX, obtenha o arquivo MDX.

2. No console do XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

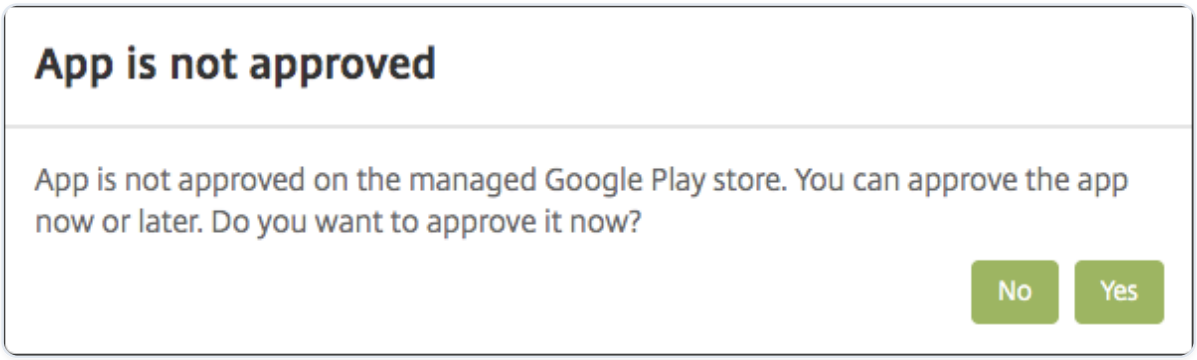


3. Clique em **MDX**. A página **Informações do Aplicativo MDX** é exibida. No painel **Informações do Aplicativo**, digite as seguintes informações:

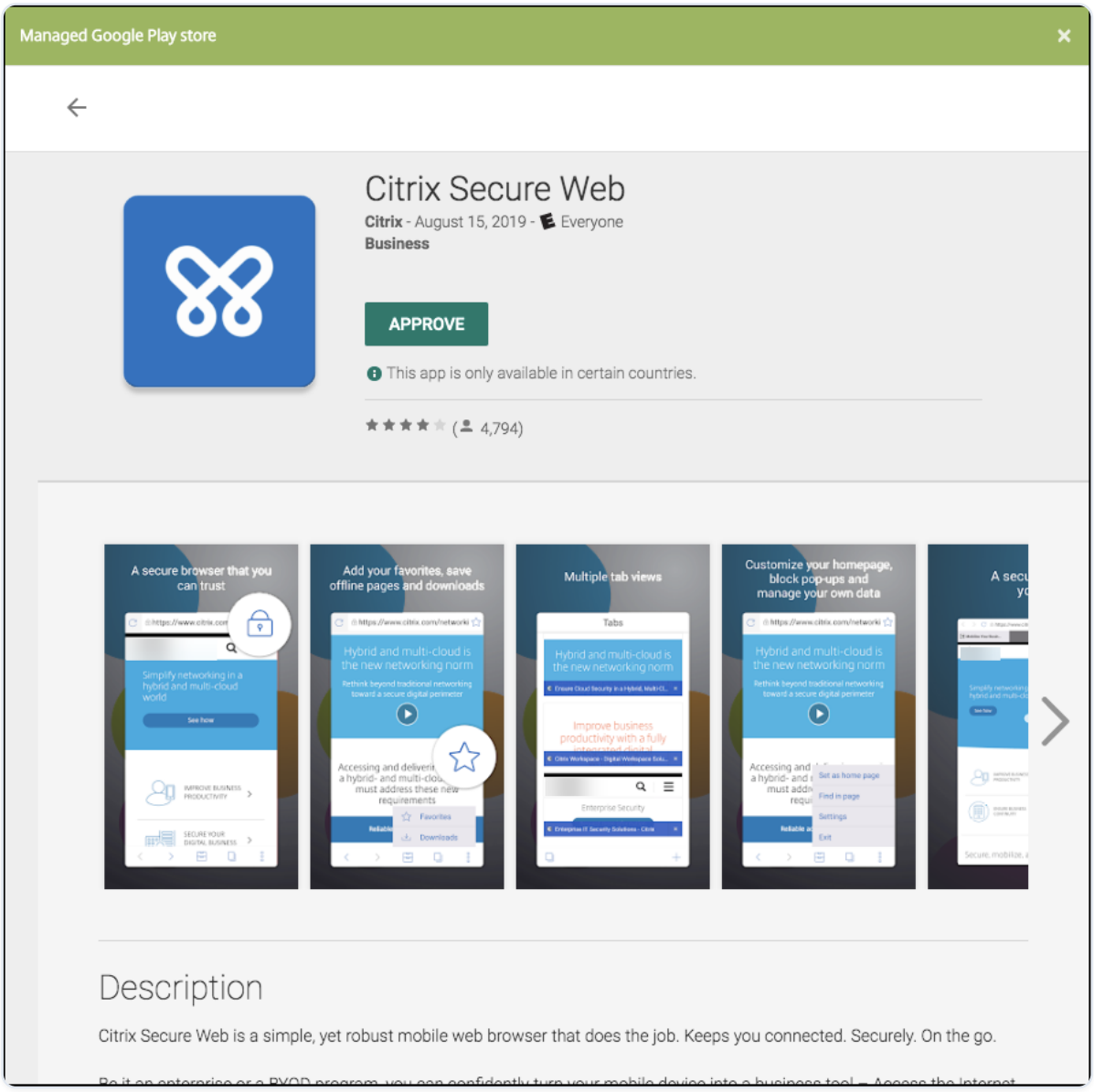
   - **Nome:** Digite um nome descritivo para o aplicativo. O nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
   - **Descrição:** Digite uma descrição opcional do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

4. Selecione **Android Enterprise** como a plataforma.
5. Clique em **Carregar** e navegar até o arquivo MDX. O Android Enterprise oferece suporte apenas a aplicativos preparados com o SDK MAM ou o MDX Toolkit.

   - A interface do usuário notifica você se o aplicativo anexado requer aprovação da Google Play Store gerenciada. Para aprovar o aplicativo sem sair do console do XenMobile, clique em **Sim**.



Depois que a Google Play Store gerenciada abrir, siga as instruções para aprovar e salvar o aplicativo.



Quando você adiciona o aplicativo com sucesso, a página **Detalhes do aplicativo** é exibida.

6. Configure estas configurações:

   - **Nome do arquivo:** Digite o nome do arquivo associado ao aplicativo.

- **Descrição do aplicativo:** Digite uma descrição para o aplicativo.
- **Versão do aplicativo:** Opcionalmente, digite o número da versão do aplicativo.
- **ID do pacote:** Digite o ID do pacote para o aplicativo, obtido na Google Play Store gerenciada.
- **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
- **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
- **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.

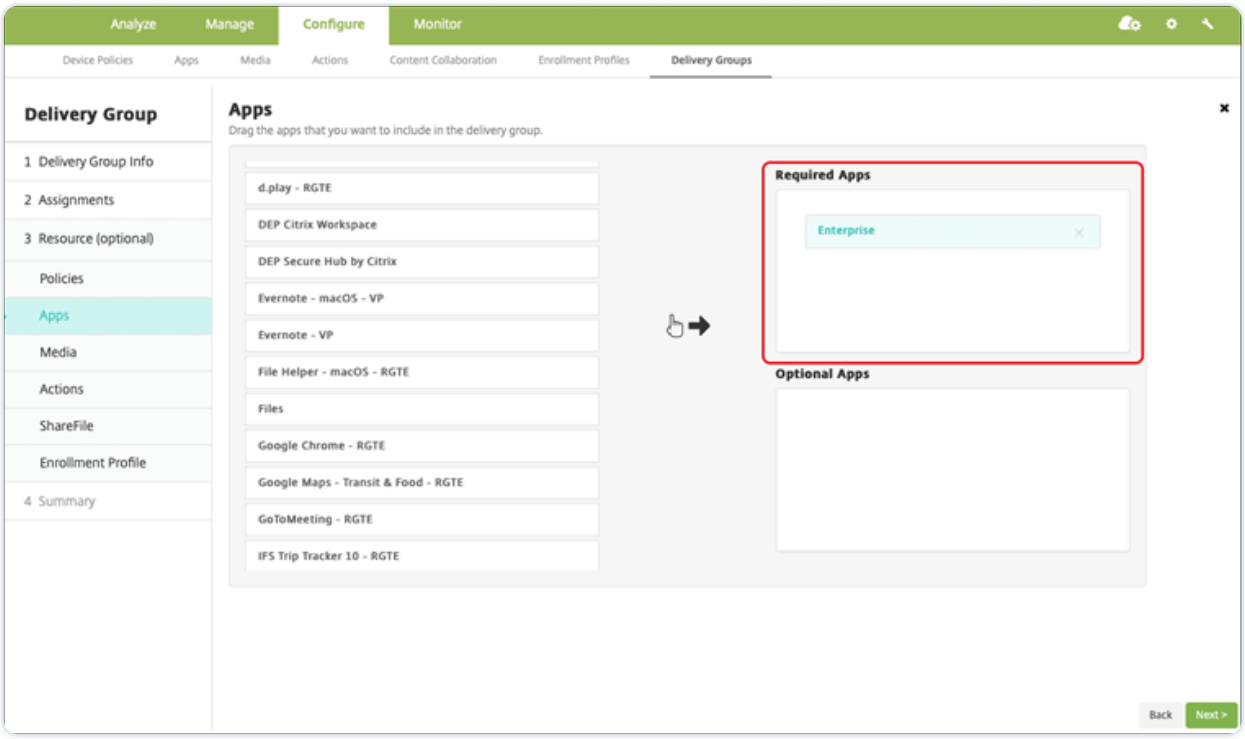
7. Configure as **Políticas MDX**. As políticas MDX variam por plataforma e incluem opções para áreas de política, incluindo autenticação, segurança do dispositivo e restrições de aplicativos. No console, cada uma das políticas possui uma dica de ferramenta que descreve a política. Para obter informações sobre as políticas de aplicativo disponíveis para cada tipo de plataforma de dispositivo, consulte:

   - Visão geral do SDK MAM
   - Políticas MDX em um relance

8. Configure as regras de implantação e a configuração da loja.
9. Atribua quaisquer grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte Implantar recursos.

Etapa 2: Configurar a implantação do aplicativo

1. navegar para **Configure > Delivery Groups** e selecione o grupo de entrega que você configurou. Clique em **Edit**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa **Aplicativos Necessários**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

Aplicativos empresariais

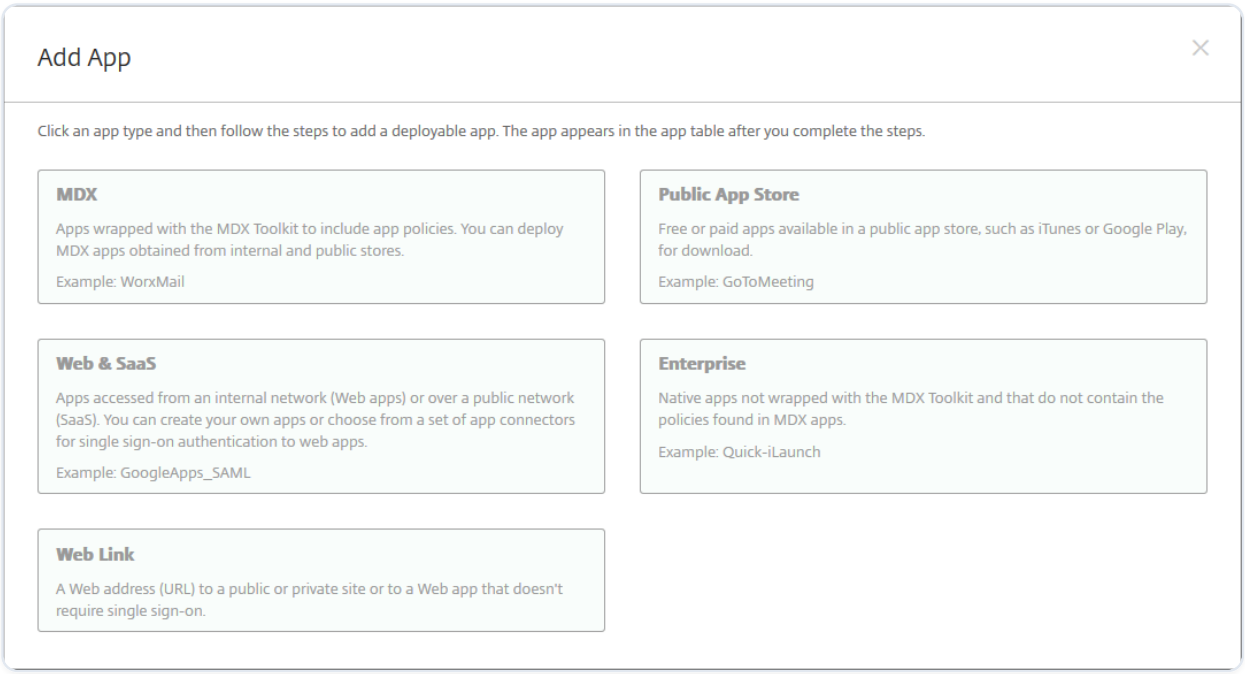
Aplicativos empresariais representam aplicativos privados que não são preparados com o SDK MAM ou o MDX Toolkit. Você desenvolve esses aplicativos por conta própria ou os obtém diretamente de outras fontes. Para adicionar um aplicativo empresarial, você precisa do arquivo APK associado ao aplicativo. Certifique-se de seguir as Melhores práticas para aplicativos privados do Google.

Etapa 1: Adicionar e configurar aplicativos

Adicione o aplicativo de uma das duas maneiras:

- Publique o aplicativo diretamente na Google Play Store gerenciada e adicione-o ao console do XenMobile como um aplicativo da loja gerenciada. Siga a documentação do Google sobre como Publicar aplicativos privados e, em seguida, siga as etapas na seção Aplicativos da loja de aplicativos gerenciados.
- Adicione o aplicativo ao console do XenMobile como um aplicativo empresarial. Siga as etapas abaixo:

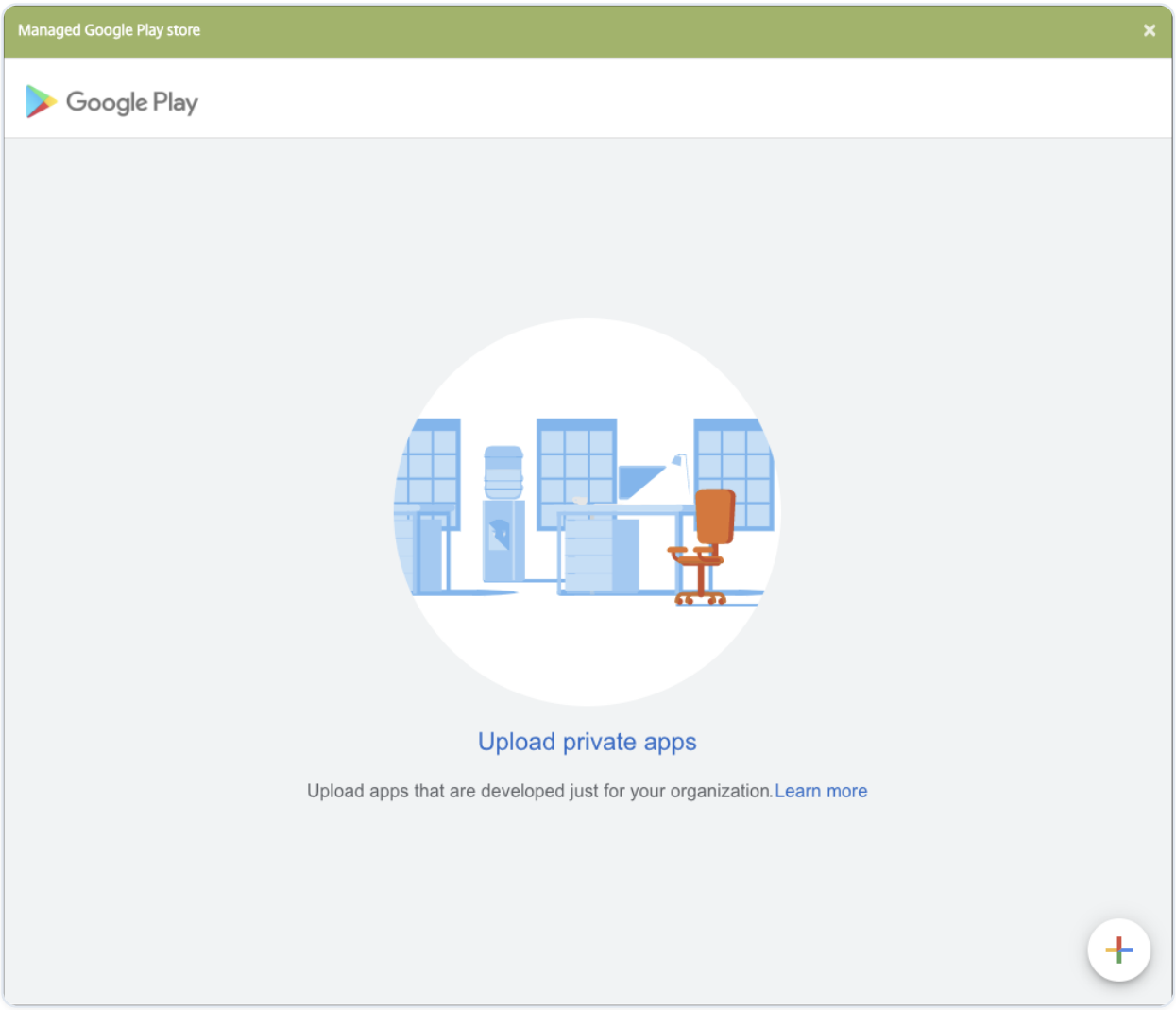
1. No console do XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



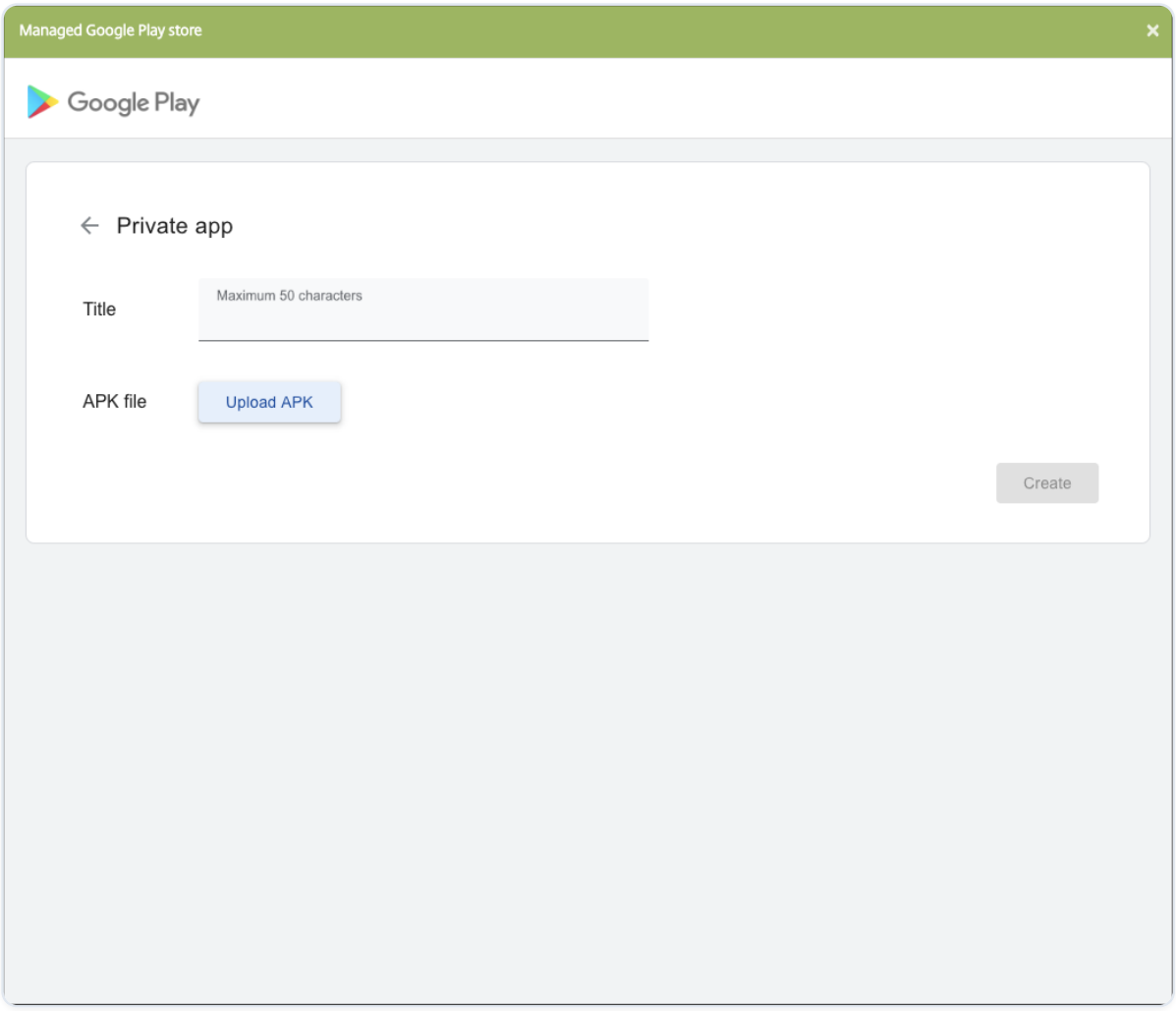
2. Clique em **Enterprise**. No painel **App Information**, digite as seguintes informações:

   - **Nome:** Digite um nome descritivo para o aplicativo. Este nome é listado em Nome do Aplicativo na tabela Aplicativos.
   - **Descrição:** Digite uma descrição opcional do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

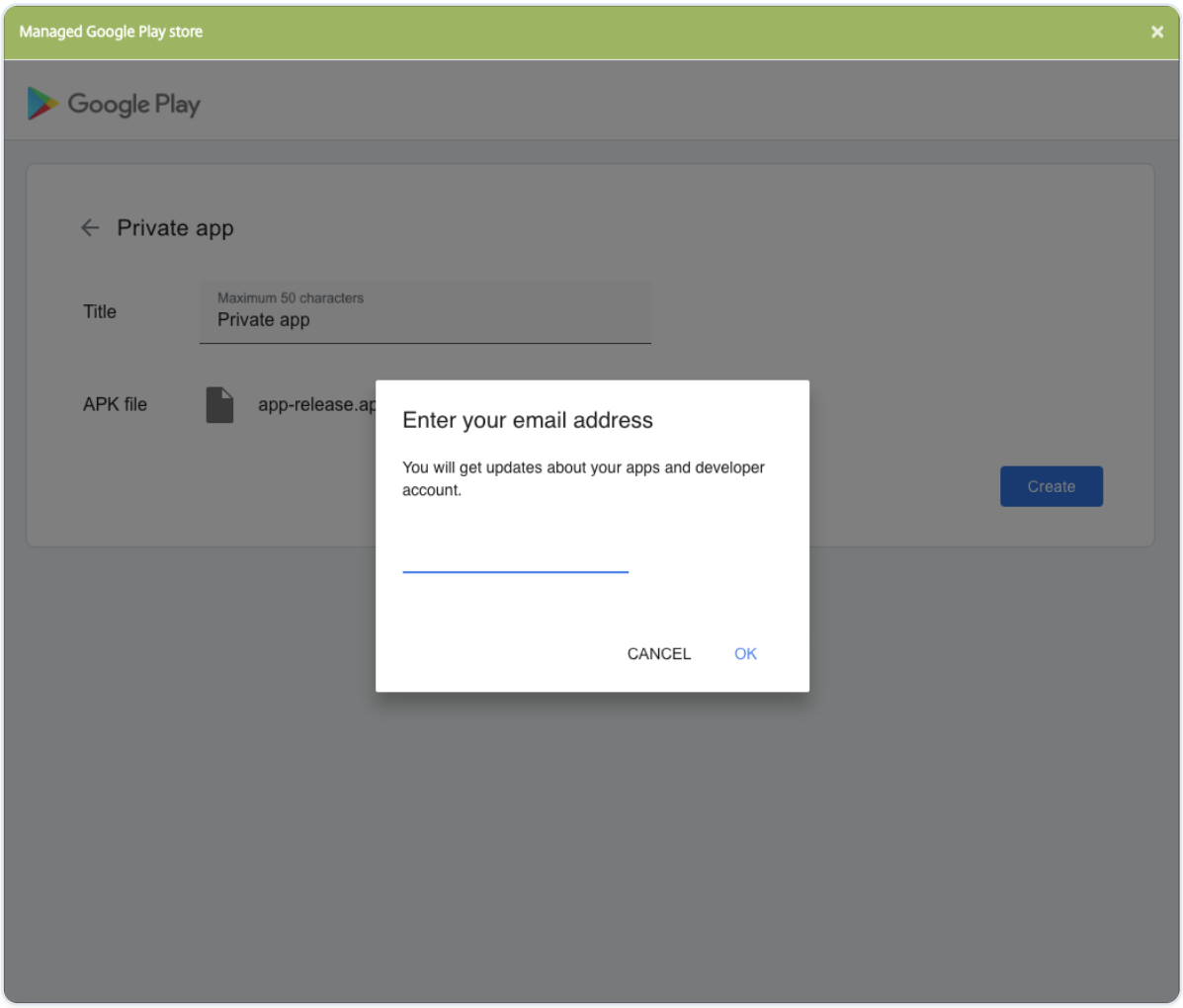
3. Selecione **Android Enterprise** como a plataforma.
4. O botão **Upload** abre a Google Play Store gerenciada. Você não precisa se registrar para uma conta de desenvolvedor para publicar um aplicativo privado. Clique no ícone **Mais** no canto inferior direito para continuar.



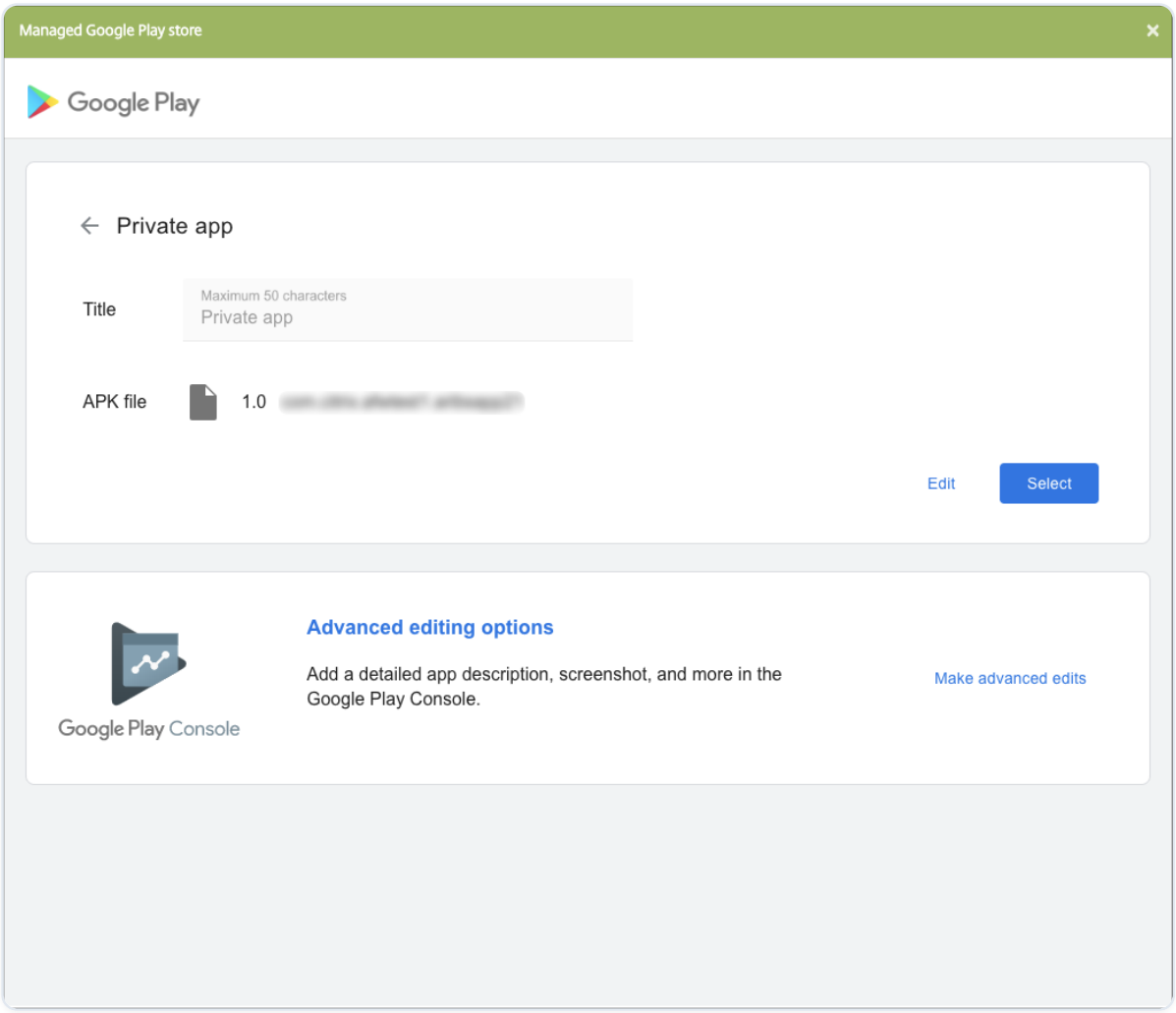
a. Digite o nome do seu aplicativo e carregue o arquivo .apk. Ao terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo privado seja publicado.



b. Insira um endereço de e-mail para receber atualizações sobre seus aplicativos.



c. Depois que seu aplicativo for publicado, clique no ícone do aplicativo privado. Se você quiser adicionar uma descrição do aplicativo, alterar o ícone do aplicativo e outras ações, clique em **Fazer edições avançadas**. Caso contrário, clique em **Selecionar** para abrir a página de informações do aplicativo.

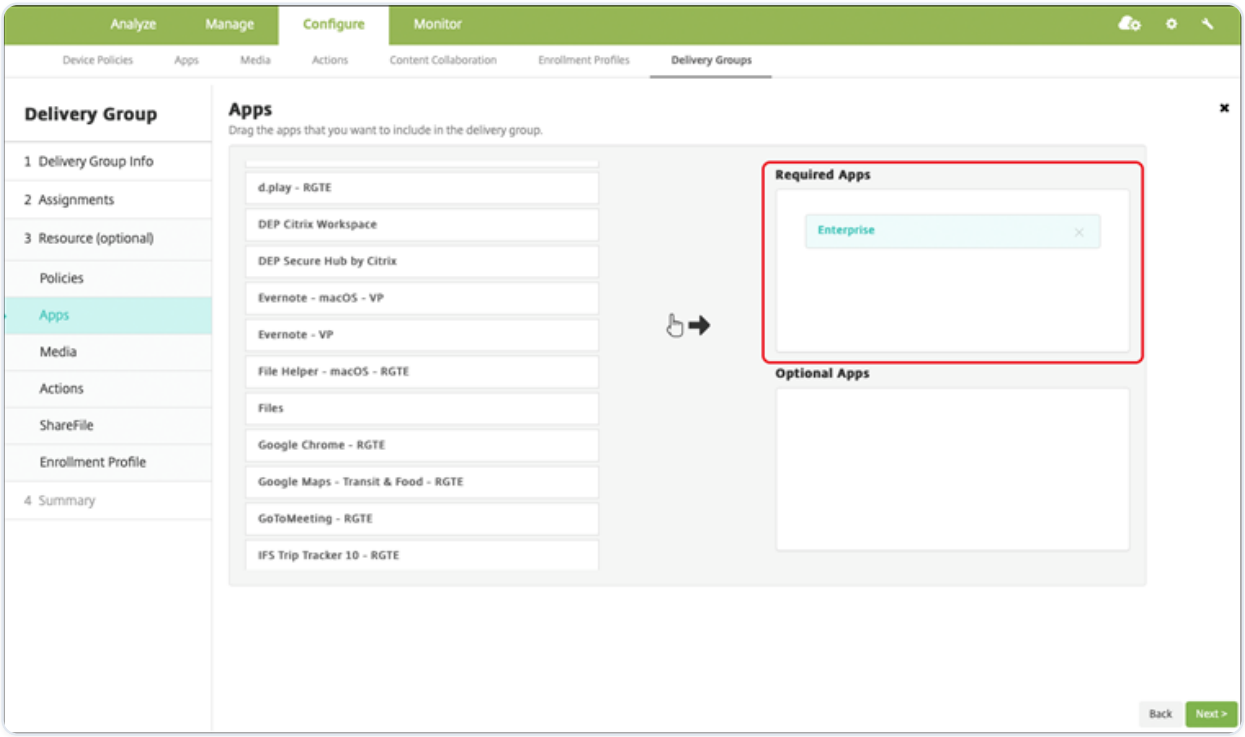


5. Clique em **Avançar**. A página de informações do aplicativo para a plataforma é exibida.
6. Configure as configurações para o tipo de plataforma, como:
    - **Nome do arquivo:** Opcionalmente, digite um novo nome para o aplicativo.
    - **Descrição do aplicativo:** Opcionalmente, digite uma nova descrição para o aplicativo.
    - **Versão do aplicativo:** Você não pode alterar este campo.
    - **ID do pacote:** Identificador exclusivo do seu aplicativo.
    - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
    - **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
    - **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
7. Configure as regras de implantação e a configuração da loja.

8. Atribua quaisquer grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte Implantar recursos.

Etapa 2: Configurar a implantação do aplicativo

1. navegar para **Configurar > Grupos de Entrega** e selecione o grupo de entrega que você configurou. Clique em **Editar**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa **Aplicativos Necessários**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

Aplicativos privados habilitados para MDX

Para adicionar aplicativos Android Enterprise como aplicativos empresariais habilitados para MDX:

1. Crie um aplicativo Android Enterprise privado e habilite o aplicativo para MDX.
2. Adicione o aplicativo ao console do XenMobile.
   - Hospede e publique o aplicativo na Google Play Store gerenciada.
   - Adicione o aplicativo ao console do XenMobile como um aplicativo Enterprise.
3. Adicione o arquivo MDX ao XenMobile.

Se você decidir hospedar e publicar aplicativos pela Google Play Store, não opte pela assinatura de certificado do Google. Assine o aplicativo com o mesmo certificado usado para habilitar o aplicativo para MDX. Para obter mais informações sobre a publicação de aplicativos, consulte a documentação do Google sobre Publicar seu aplicativo e Assinar seu aplicativo. O SDK MAM não empacota aplicativos, portanto, não requer um certificado diferente daquele usado para desenvolver o aplicativo.

Para obter mais informações sobre a publicação de aplicativos privados por meio do Google Play Console, consulte a documentação do Google sobre como Publicar aplicativos privados no Play Console.

Para publicar um aplicativo por meio do XenMobile, consulte as seções a seguir.

Preparar um aplicativo Android Enterprise privado

Ao criar um aplicativo Android Enterprise privado, certifique-se de seguir as Práticas recomendadas para aplicativos privados do Google.

Depois de criar um aplicativo Android Enterprise privado, integre o SDK MAM ao aplicativo ou empacote o aplicativo usando o MDX Toolkit. Em seguida, adicione os arquivos resultantes ao XenMobile.

Você pode atualizar o aplicativo carregando um arquivo .apk atualizado. As etapas a seguir abordam o empacotamento de aplicativos com o MDX Toolkit.

1. Crie seu aplicativo Android Enterprise privado e gere um arquivo .apk assinado.
2. O seguinte arquivo de exemplo contém todas as políticas conhecidas, algumas das quais podem não ser aplicáveis ao seu ambiente. Quaisquer configurações inutilizáveis são ignoradas. Crie um arquivo XML com os seguintes parâmetros:

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>
```

```
        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>

        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>

        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>

        <WifiOnly>false</WifiOnly>

        <RequireInternalNetwork>false</RequireInternalNetwork>

        <InternalWifiNetworks/>

        <AllowedWifiNetworks/>

        <UpgradeGracePeriod>168</UpgradeGracePeriod>

        <WipeDataOnAppLock>false</WipeDataOnAppLock>

        <ActivePollPeriod>60</ActivePollPeriod>

        <PublicFileAccessLimitsList/>

        <CutAndCopy>Unrestricted</CutAndCopy>

        <Paste>Unrestricted</Paste>

        <DocumentExchange>Unrestricted</DocumentExchange>

        <OpenInExclusionList/>
```

```
        <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

        <InboundDocumentExchangeWhitelist/>

        <connectionSecurityLevel>TLS</connectionSecurityLevel>

        <DisableCamera>false</DisableCamera>

        <DisableGallery>false</DisableGallery>

        <DisableMicrophone>false</DisableMicrophone>

        <DisableLocation>false</DisableLocation>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>
```

```
        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>

        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. Empacote o aplicativo usando o MDX Toolkit. Para obter informações sobre como usar o MDX Toolkit, consulte Empacotamento de aplicativos móveis Android.

   Defina o parâmetro **apptype** como **Premium**. Use o arquivo XML da etapa anterior no comando descrito a seguir.

   Se você souber a URL da loja para o aplicativo, defina o parâmetro **storeURL** como a URL da loja. Os usuários baixam o aplicativo da URL da loja depois que você o publica.

   Aqui está um exemplo de um comando do MDX Toolkit usado para empacotar um aplicativo chamado SampleAEapp:

```
```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
```
```

```
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0

 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>

```

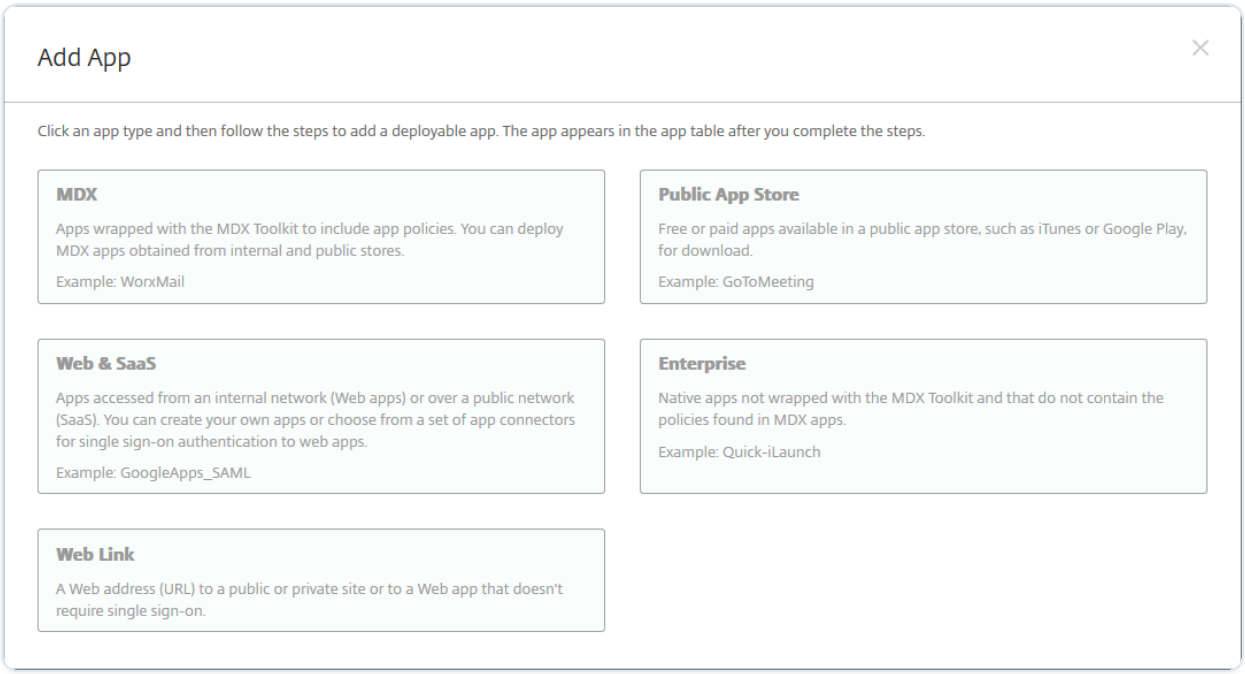
O empacotamento do aplicativo gera um arquivo .apk empacotado e um arquivo .mdx.

Adicionar o arquivo .apk empacotado

Adicione o aplicativo de uma das duas maneiras:

- Publique o aplicativo diretamente na Google Play Store gerenciada e adicione-o ao console do XenMobile como um aplicativo da loja gerenciada. Siga a documentação do Google sobre como Publicar aplicativos privados, e então siga as etapas na seção Aplicativos da loja de aplicativos gerenciados.
- Adicione o aplicativo ao console do XenMobile como um aplicativo empresarial. Siga as etapas abaixo:

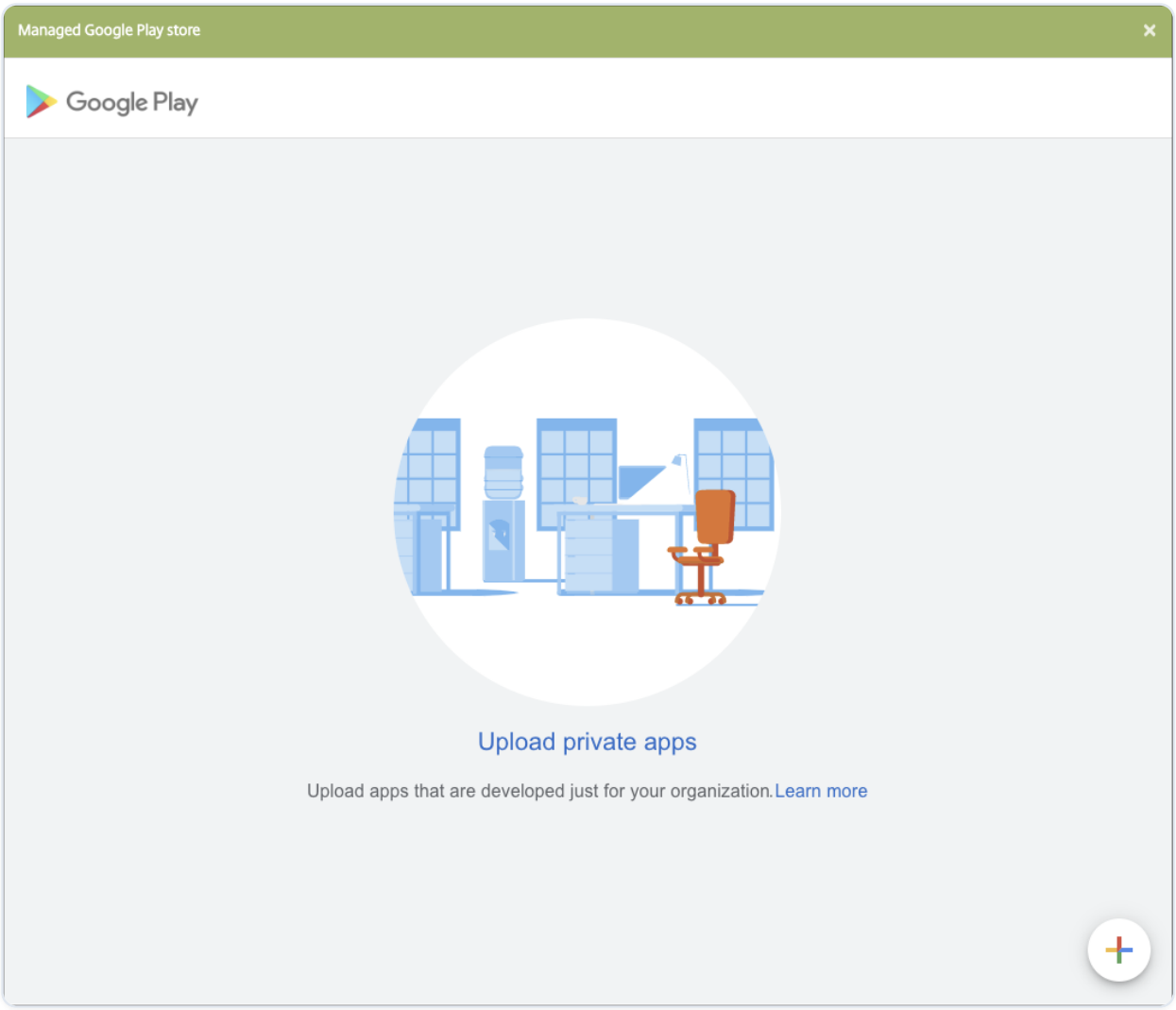
1. No console do XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é aberta.
2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



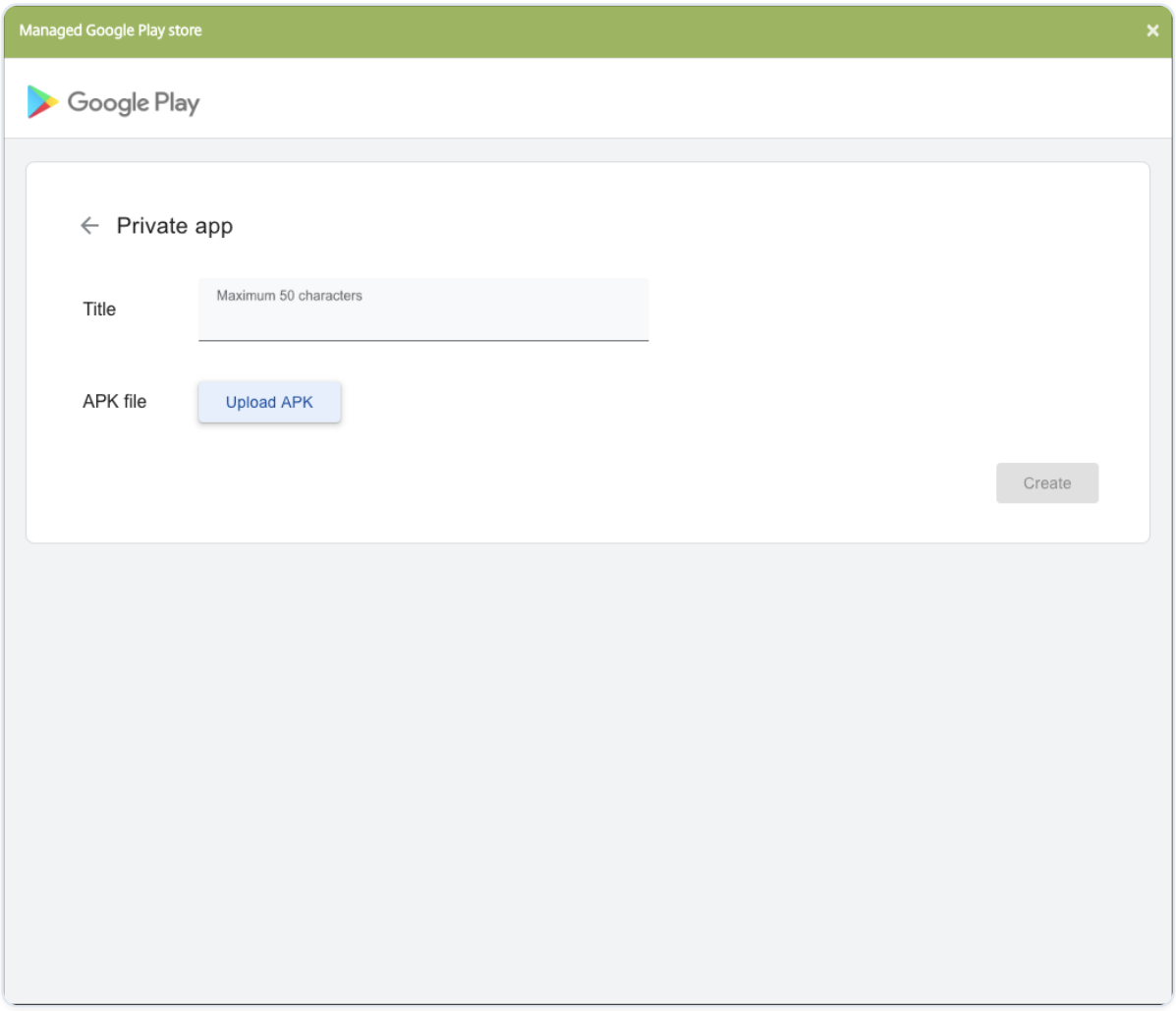
3. Clique em **Empresarial**. No painel **Informações do Aplicativo**, digite as seguintes informações:

   - **Nome:** Digite um nome descritivo para o aplicativo. Este nome é listado em Nome do Aplicativo na tabela Aplicativos.
   - **Descrição:** Digite uma descrição opcional do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

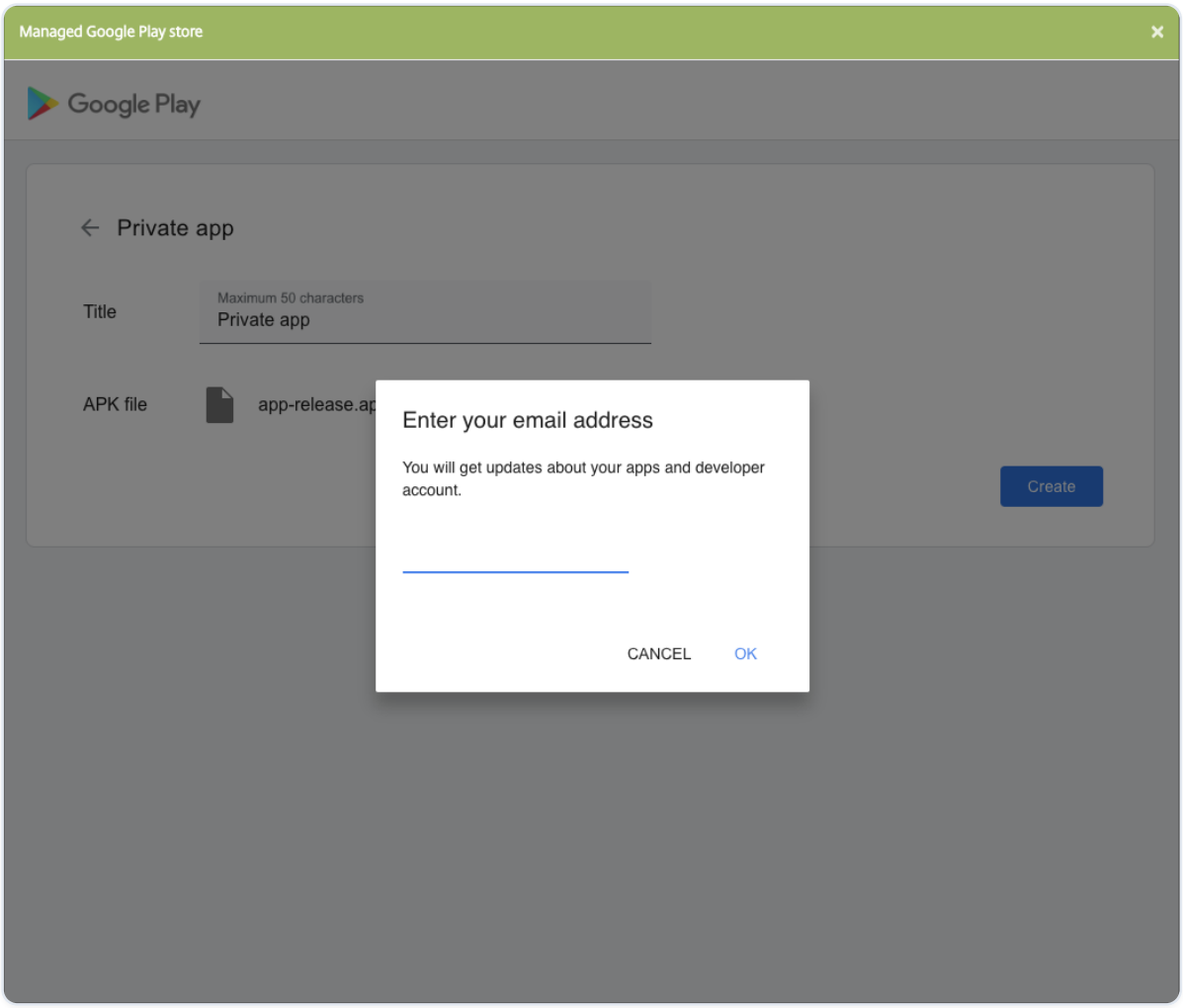
4. Selecione **Android Enterprise** como a plataforma.
5. O botão **Carregar** abre a Google Play Store gerenciada. Você não precisa se registrar para uma conta de desenvolvedor para publicar um aplicativo privado. Clique no ícone **Mais** no canto inferior direito para continuar.



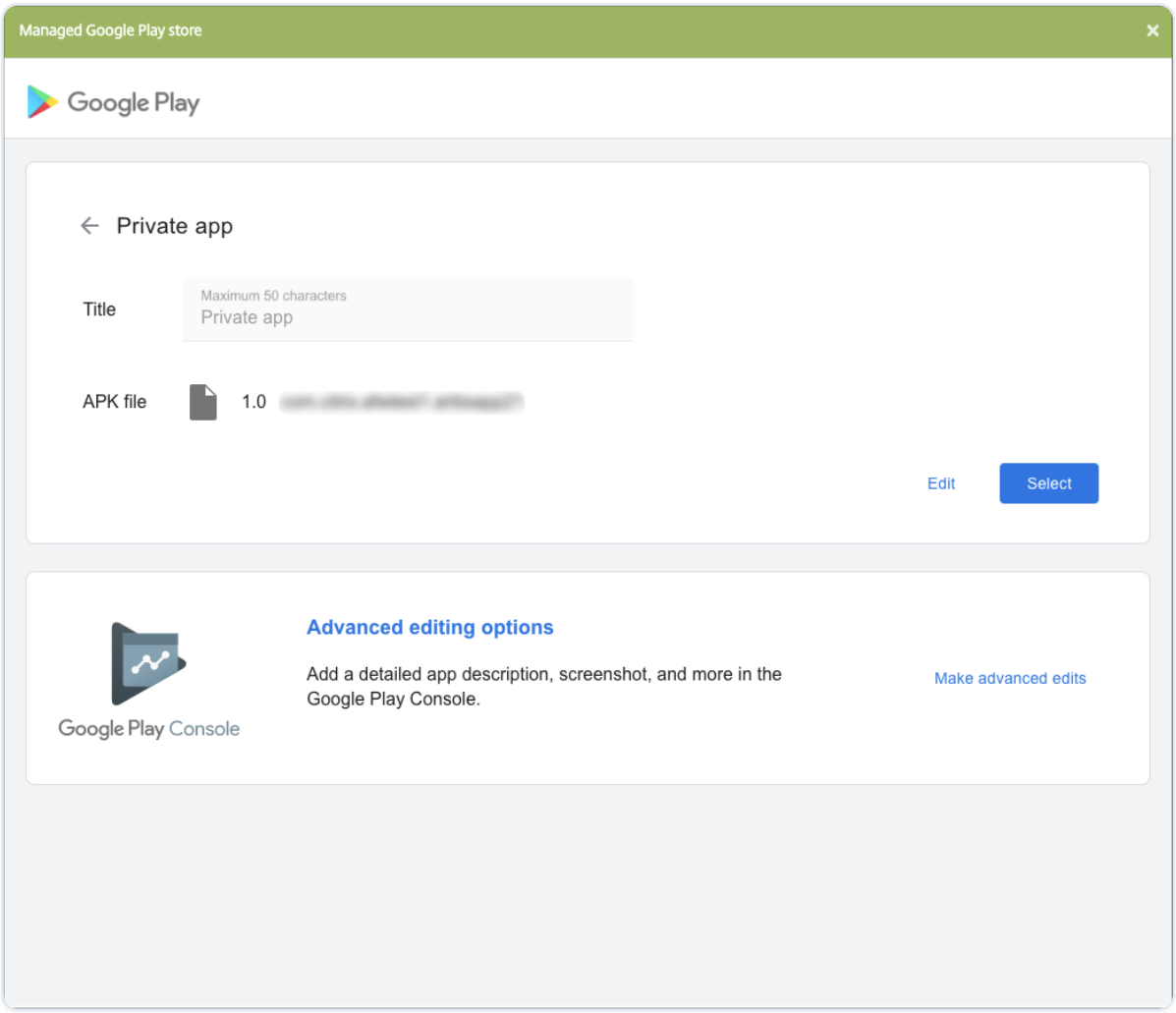
a. Digite o nome do seu aplicativo e carregue o arquivo .apk. Ao terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo privado seja publicado.



b. Insira um endereço de e-mail para receber atualizações sobre seus aplicativos.



c. Depois que seu aplicativo for publicado, clique no ícone de um aplicativo privado e clique em **Selecionar** para abrir a página de informações do aplicativo.



6. Clique em **Avançar**. A página de informações do aplicativo para a plataforma é exibida.
7. Configure as configurações para o tipo de plataforma, como:
    - **Nome do arquivo:** Opcionalmente, digite um novo nome para o aplicativo.
    - **Descrição do aplicativo:** Opcionalmente, digite uma nova descrição para o aplicativo.
    - **Versão do aplicativo:** Você não pode alterar este campo.
    - **ID do pacote:** Identificador exclusivo do seu aplicativo.
    - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
    - **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
    - **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
8. Configure as regras de implantação e a configuração da loja.

9. Na página **Aplicativo Corporativo do Android Enterprise**, clique em **Avançar**. A página **Aprovações** é exibida.

   Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não precisar de um fluxo de trabalho de aprovação, pode pular para a Etapa 13.

10. Clique em **Avançar**.
11. A página **Atribuição de Grupo de Entrega** é exibida. Nenhuma ação é necessária nesta página. Você configura os grupos de entrega e o agendamento de implantação para este aplicativo ao adicionar o arquivo .mdx. Clique em **Salvar**.

OPCIONAL: ADICIONAR OU ALTERAR O URL DA LOJA

Se você não sabia o URL da loja ao empacotar o aplicativo, adicione o URL da loja agora.

1. Visualize o aplicativo na Google Play Store gerenciada. Ao selecionar o aplicativo, o URL da loja aparece na barra de endereço do seu navegador. Copie o nome do pacote do aplicativo do formulário de URL. Por exemplo: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. O URL que você copia pode começar com `https://play.google.com/work/`. Certifique-se de alterar `work` para `store`.
2. Use o MDX Toolkit para adicionar o URL da loja ao arquivo .mdx:

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

Adicionar o arquivo .mdx

1. No console XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

   Tela de configuração de aplicativos(/en-us/xenmobile/server/media/configure-apps-add.png)

2. Clique em **MDX**. A página **Informações do Aplicativo MDX** é exibida. No painel **Informações do Aplicativo**, digite as seguintes informações:

- **Nome:** Digite um nome descritivo para o aplicativo. O nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
- **Descrição:** Digite uma descrição opcional do aplicativo.
- **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

3. Selecione **Android Enterprise** como a plataforma.
4. Clique em **Carregar** e navegar até o arquivo MDX. O Android Enterprise só oferece suporte a aplicativos empacotados com o MDX Toolkit.

   - A interface do usuário notifica você se o aplicativo anexado requer aprovação da Google Play Store gerenciada. Para aprovar o aplicativo sem sair do console XenMobile, clique em **Sim**.

     Adicionar um aplicativo MDX(/en-us/xenmobile/server/media/mdx-app-not-approved.png)

     Depois que a Google Play Store gerenciada for aberta, siga as instruções para aprovar e salvar o aplicativo.

     Aprovar um aplicativo MDX(/en-us/xenmobile/server/media/mdx-approve-app.png)

     Quando você adiciona o aplicativo com sucesso, a página **Detalhes do aplicativo** é exibida.

5. Configure estas configurações:

   - **Nome do arquivo:** Digite o nome do arquivo associado ao aplicativo.
   - **Descrição do Aplicativo:** Digite uma descrição para o aplicativo.
   - **Versão do aplicativo:** Opcionalmente, digite o número da versão do aplicativo.
   - **ID do Pacote:** Digite o ID do pacote para o aplicativo obtido na Google Play Store gerenciada.
   - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
   - **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
   - **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.

6. Configure as **Políticas MDX**. As políticas MDX variam de acordo com a plataforma e incluem opções para áreas de política, incluindo Autenticação, Segurança do Dispositivo e Restrições de Aplicativos. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política. Para obter informações sobre as políticas de aplicativo disponíveis para cada tipo de plataforma de dispositivo, consulte:

   - Visão geral do SDK MAM
   - Políticas de aplicativos de terceiros MDX em resumo

7. Configure as regras de implantação e a configuração da loja.

   A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

   A opção sempre ativa:

   - Não está disponível para clientes Android Enterprise que começaram a usar o Endpoint Management com a versão 10.18.19 ou posterior
   - Não é recomendada para clientes Android Enterprise que começaram a usar o Endpoint Management antes da versão 10.18.19

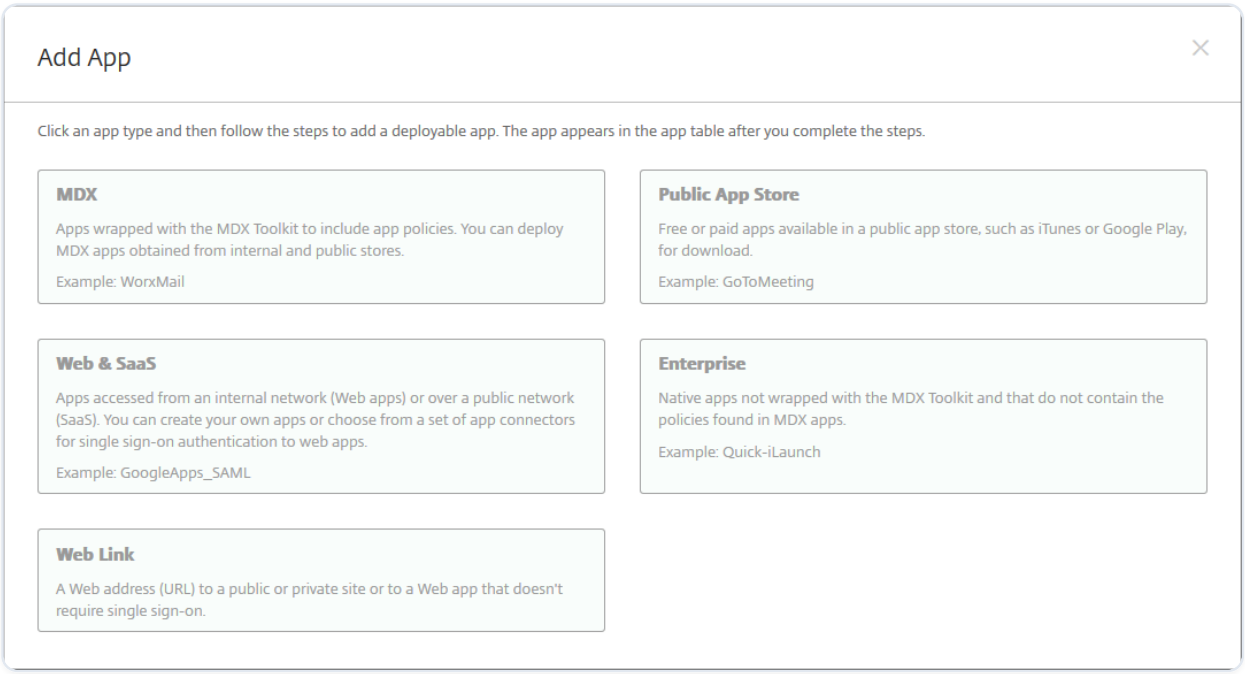
   O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você fizer se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.

8. Atribua quaisquer grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte Implantar recursos.

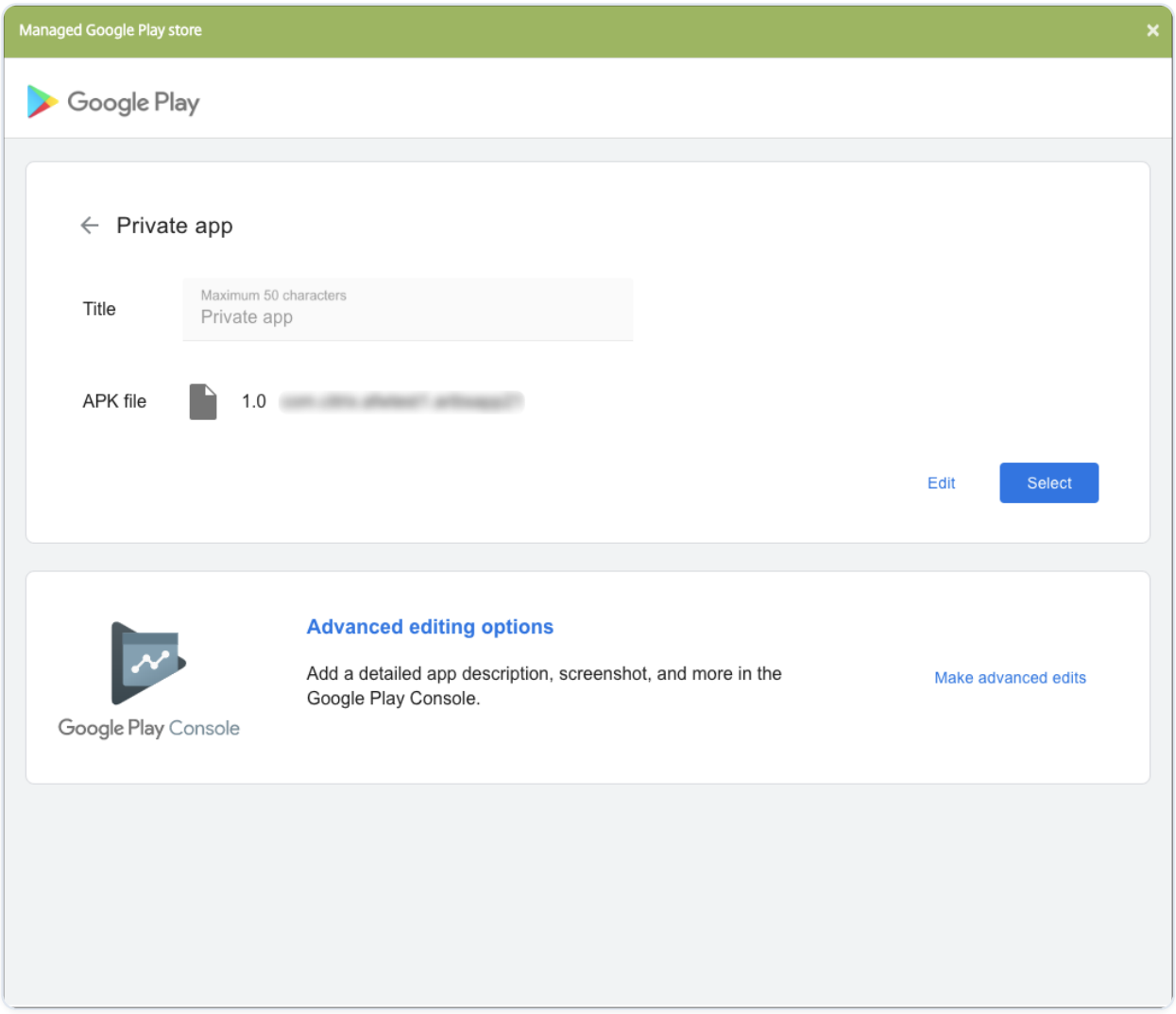
Atualizar o aplicativo

Para atualizar o aplicativo Android Enterprise, empacote e carregue um arquivo .apk atualizado:

1. Empacote o arquivo .apk para o aplicativo atualizado usando o MAM SDK ou o MDX Toolkit.
2. No console do XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é aberta.



3. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.
4. Clique em **Empresarial**. No painel **Informações do Aplicativo**, digite as seguintes informações:
    - **Nome:** Digite um nome descritivo para o aplicativo. Este nome é listado em Nome do Aplicativo na tabela Aplicativos.
    - **Descrição:** Digite uma descrição opcional do aplicativo.
    - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
5. Selecione **Android Enterprise** como a plataforma.
6. Clique em **Avançar**. A página **Aplicativo Empresarial Android Enterprise** é exibida.
7. Clique em **Carregar**.
8. Na página da Google Play Store gerenciada, selecione o aplicativo que você deseja atualizar.
9. Na página de informações do aplicativo, clique em **editar** ao lado do nome do arquivo .apk.



10. navegar para o novo arquivo .apk e faça o upload.
11. Na página da Google Play Store gerenciada, clique em **Salvar**.

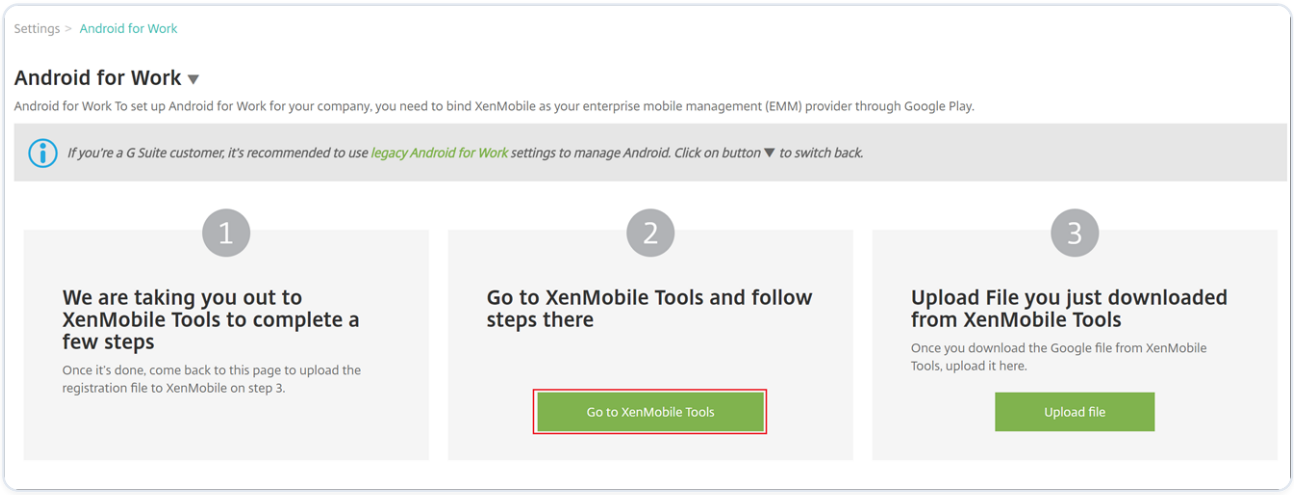
Android Enterprise Legado para clientes do Google Workspace (antigo G Suite)

Os clientes do Google Workspace (antigo G Suite) devem usar as configurações do Android Enterprise legado para configurar o Android Enterprise legado.

Requisitos para o Android Enterprise legado:

- Um domínio acessível publicamente
- Uma conta de administrador do Google
- Dispositivos com suporte a perfil gerenciado e que executam Android 5.0+ Lollipop
- Uma conta do Google com o Google Play instalado
- Um perfil de trabalho configurado no dispositivo

Para começar a configurar um Android Enterprise legado, clique em **Android Enterprise legado** na página **Android Enterprise** em Configurações do XenMobile®.



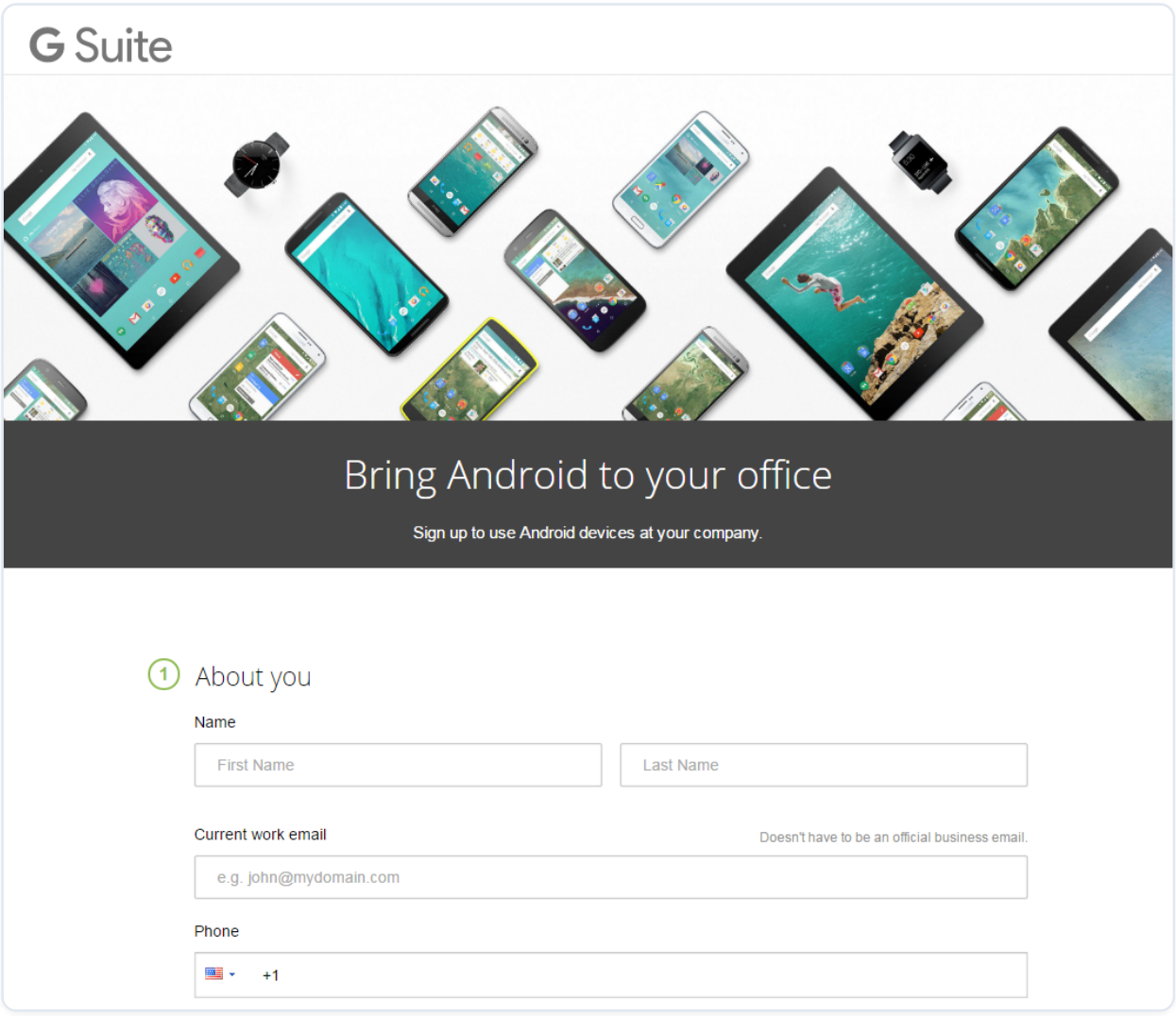
Criar uma conta do Android Enterprise

Antes de configurar uma conta do Android Enterprise, você deve verificar seu nome de domínio com o Google.

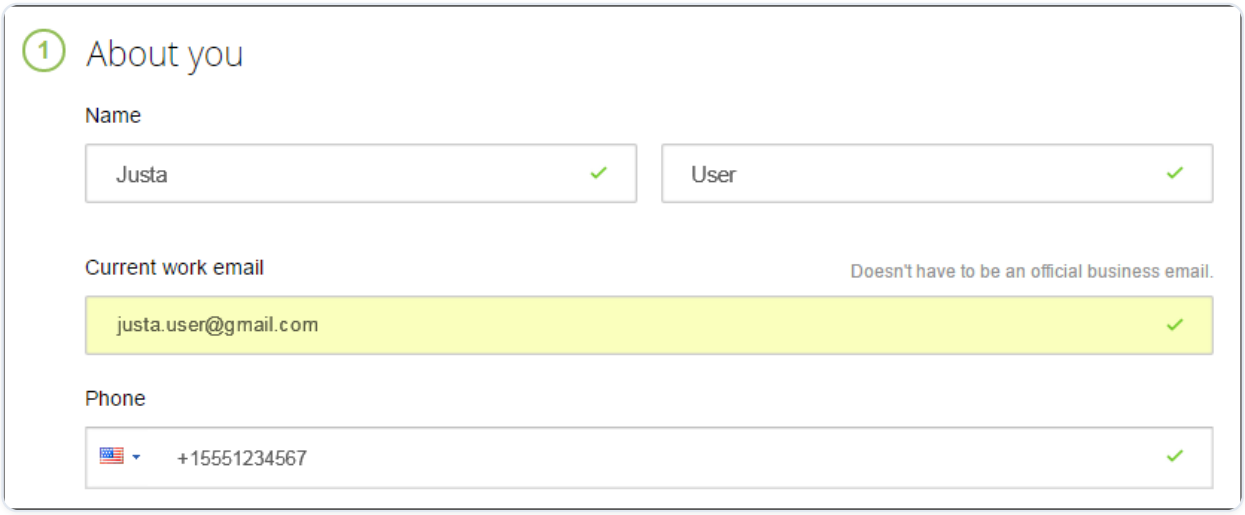
Se você já verificou seu nome de domínio com o Google, pode pular para esta etapa: Configurar uma conta de serviço do Android Enterprise e baixar um certificado do Android Enterprise.

1. navegar para `<https://gsuite.google.com/signup/basic/welcome>`.

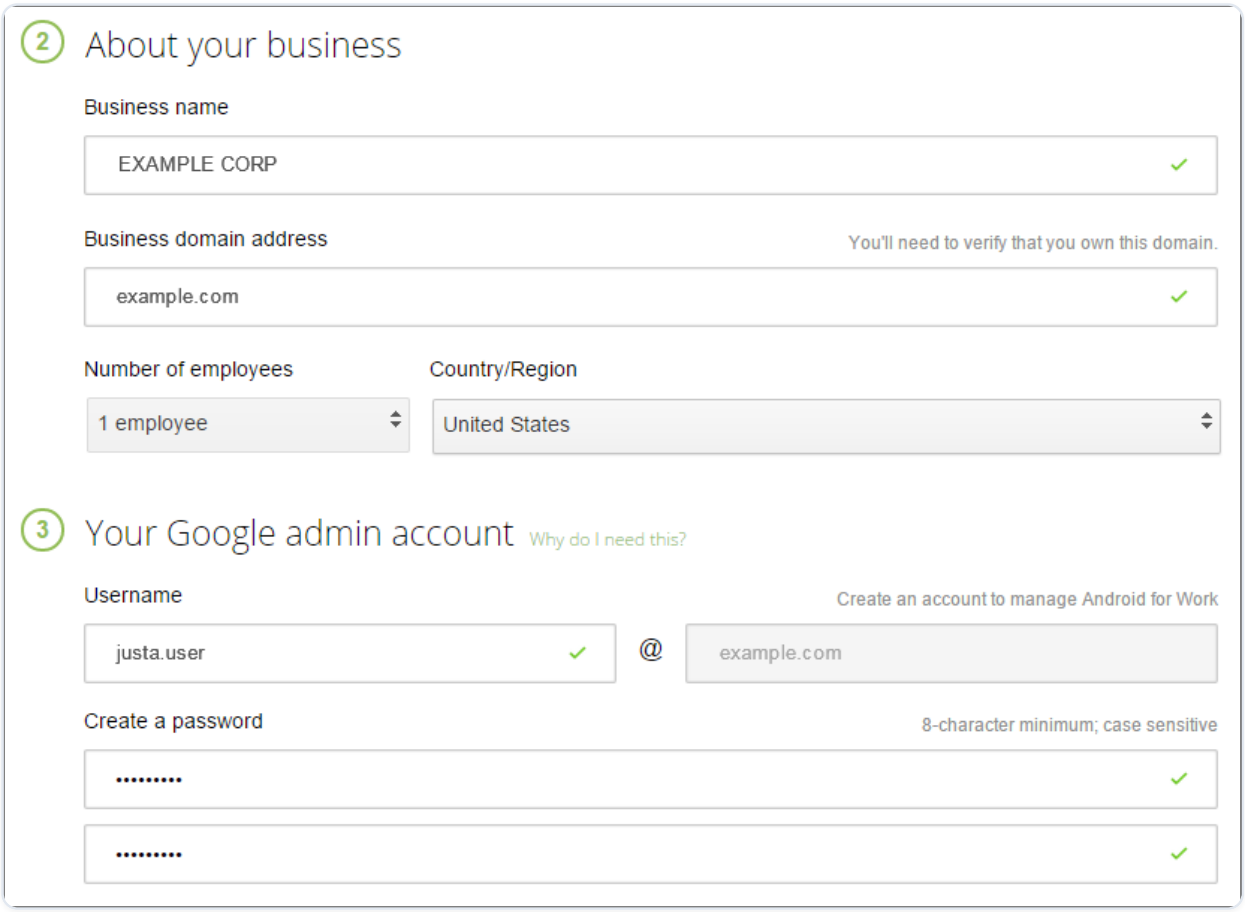
   A página a seguir é exibida, onde você digita as informações do seu administrador e da empresa.



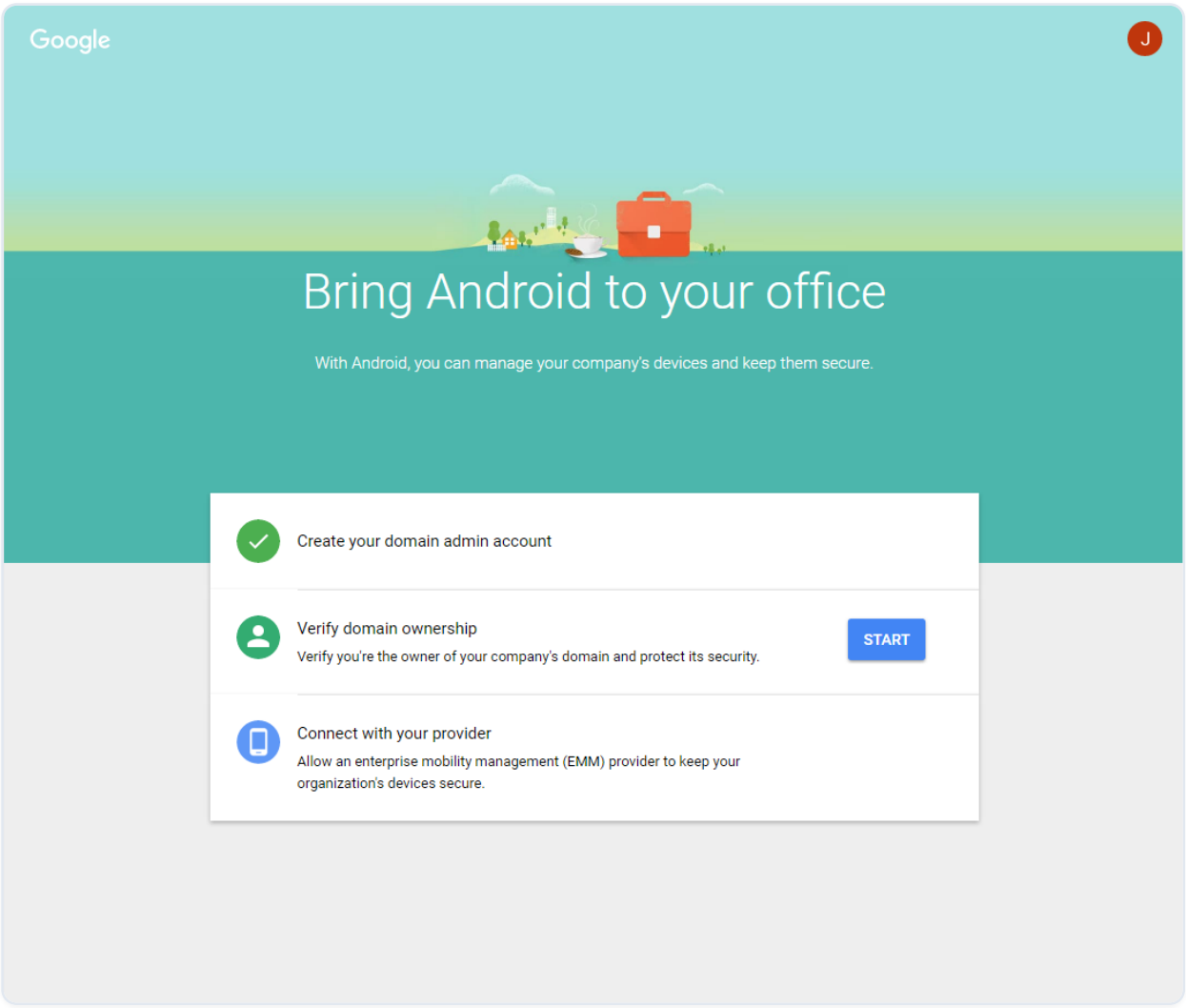
2. Digite suas informações de usuário administrador.



3. Digite as informações da sua empresa, além das informações da sua conta de administrador.



A primeira etapa do processo está concluída e você verá a seguinte página.



Verificar a propriedade do domínio

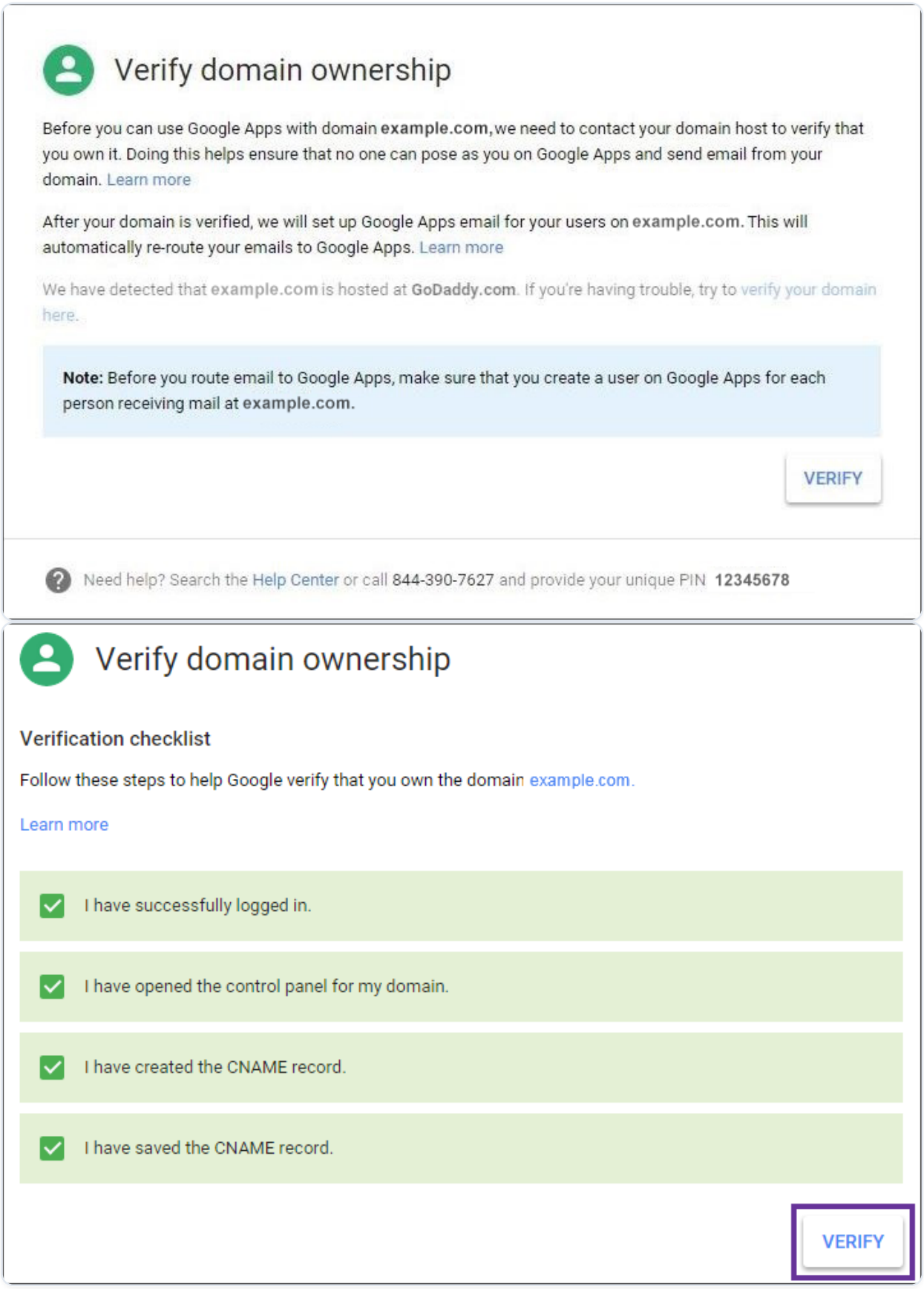
Permita que o Google verifique seu domínio de uma das seguintes maneiras:

- Adicione um registro TXT ou CNAME ao site do seu provedor de domínio.
- Carregue um arquivo HTML para o servidor web do seu domínio.
- Adicione uma tag `<meta>` à sua página inicial. O Google recomenda o primeiro método. Este artigo não aborda as etapas para verificar a propriedade do seu domínio, mas você pode encontrar as informações necessárias aqui: https://support.google.com/a/answer/6248925.

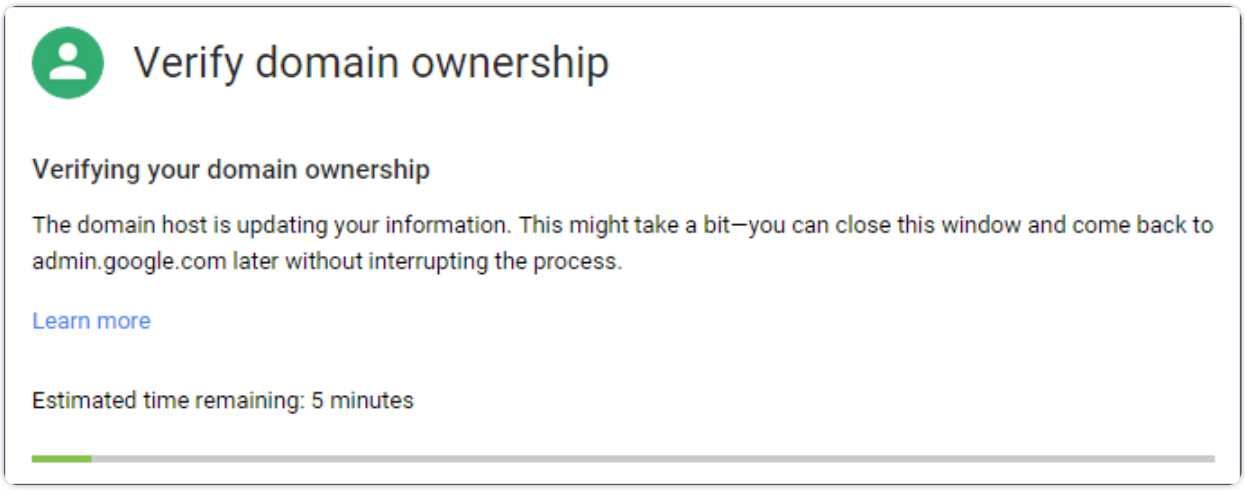
1. Clique em **Iniciar** para começar a verificação do seu domínio.

   A página **Verificar a propriedade do domínio** é exibida. Siga as instruções na página para verificar seu domínio.

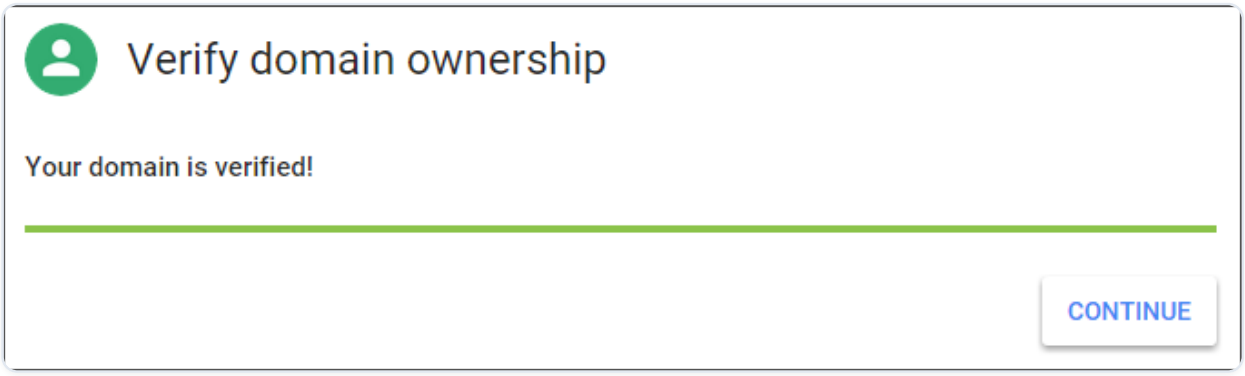
2. Clique em **Verificar**.



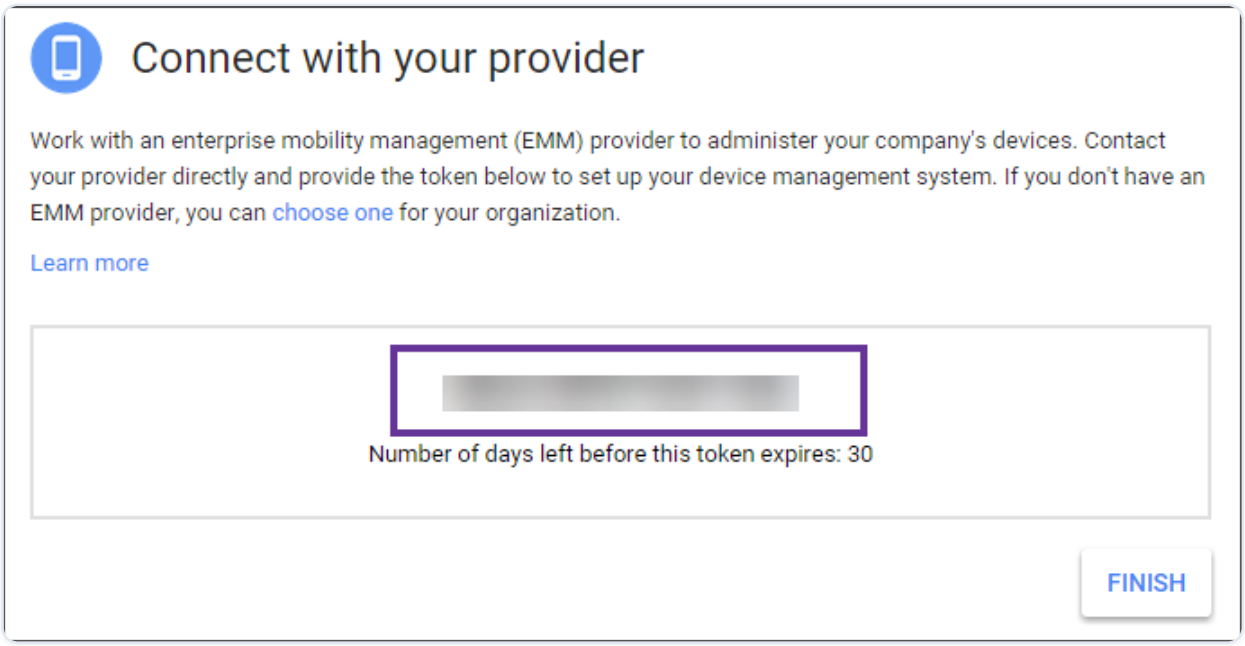
3. O Google verifica a propriedade do seu domínio.



4. Após a verificação bem-sucedida, a seguinte página é exibida. Clique em **Continuar**.



5. O Google cria um token de vinculação EMM que você fornece à Citrix® e usa ao configurar as configurações do Android Enterprise. Copie e salve o token; você precisará dele mais tarde no procedimento de configuração.



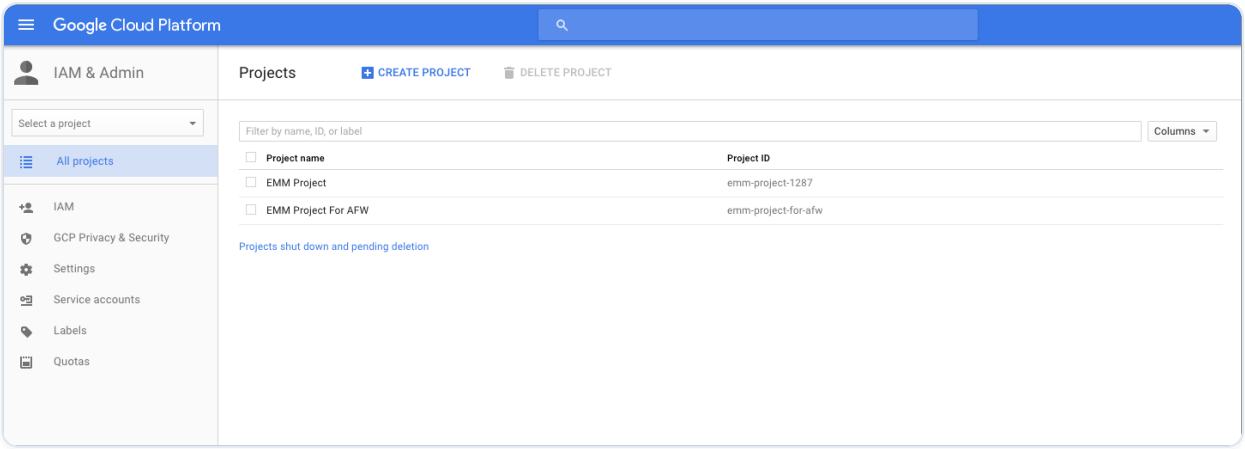
6. Clique em **Concluir** para finalizar a configuração do Android Enterprise. Uma página é exibida, indicando que você verificou seu domínio com sucesso.

Depois de criar uma conta de serviço do Android Enterprise, você pode fazer login no console de administração do Google para gerenciar suas configurações de gerenciamento de mobilidade.

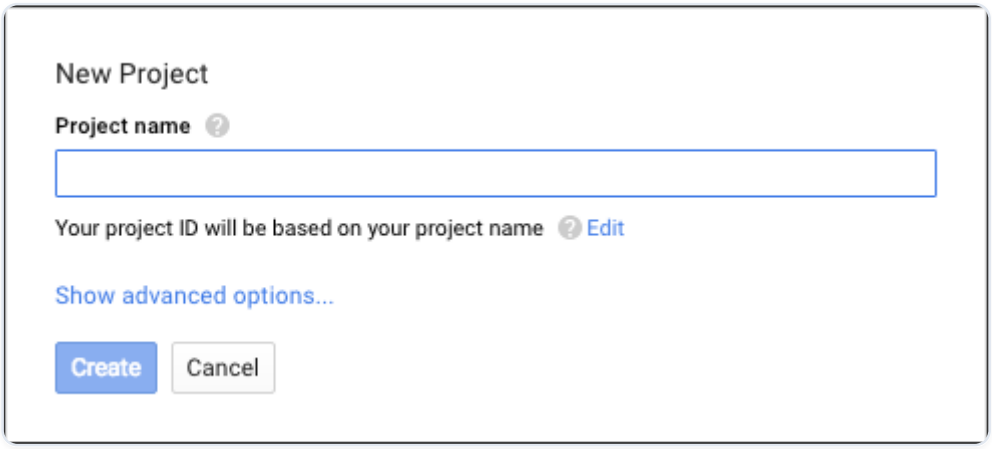
Configurar uma conta de serviço do Android Enterprise e baixar um certificado do Android Enterprise

Para permitir que o XenMobile entre em contato com os serviços do Google Play e do Diretório, você deve criar uma conta de serviço usando o portal do Google Project para desenvolvedores. Esta conta de serviço é usada para comunicação servidor a servidor entre o XenMobile e os serviços do Google para Android. Para obter mais informações sobre o protocolo de autenticação que está sendo usado, acesse `<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`.

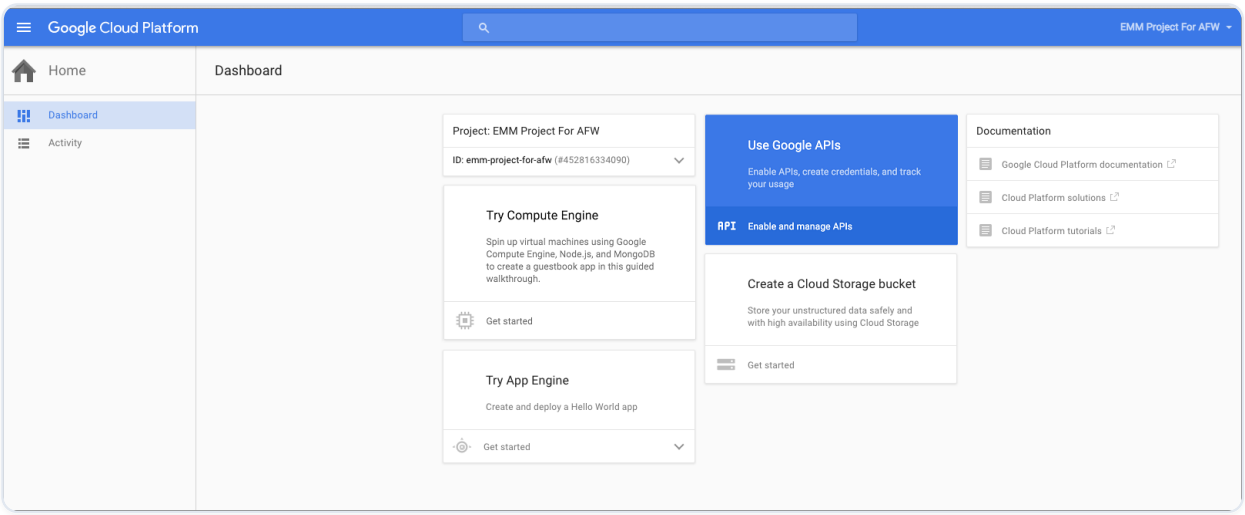
1. Em um navegador da web, acesse `<https://console.cloud.google.com/project>` e faça login com suas credenciais de administrador do Google
2. Na lista **Projetos**, clique em **Criar Projeto.**



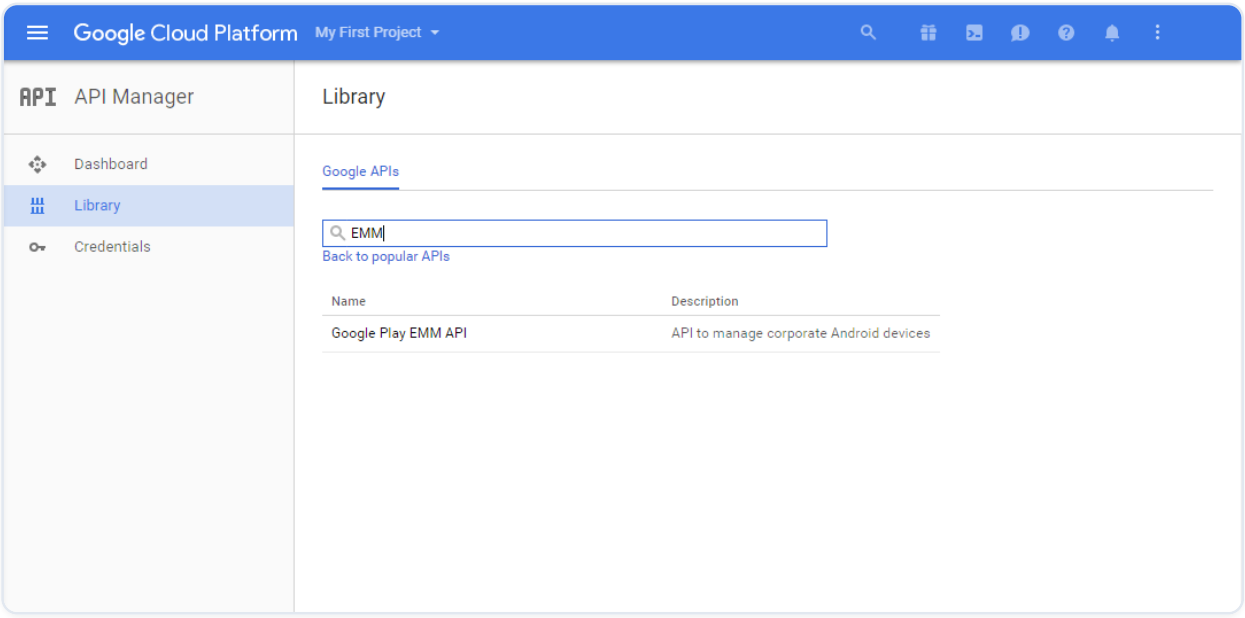
3. Em **Nome do projeto**, digite um nome para o projeto.



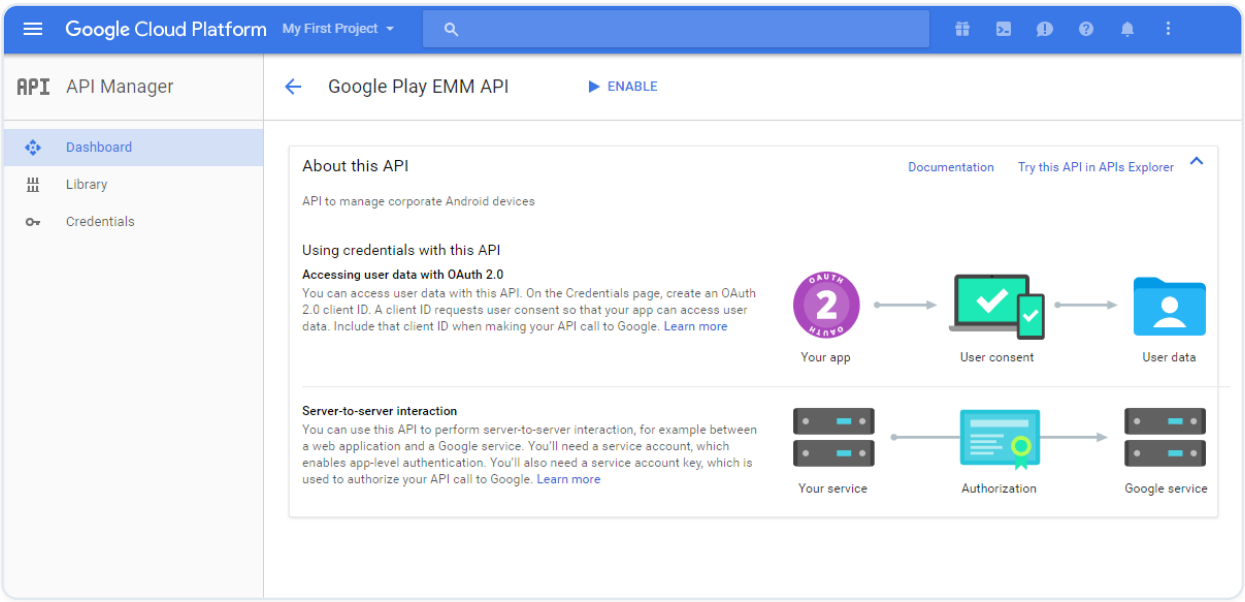
4. No Painel, clique em **Usar APIs do Google**.



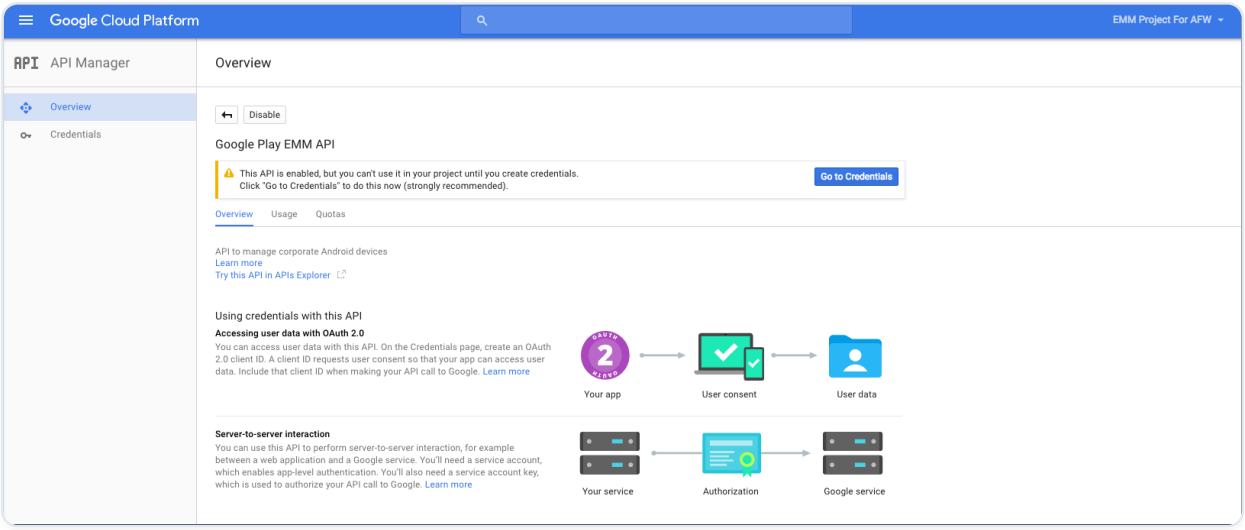
5. Clique em **Biblioteca**, em **Pesquisar**, digite **EMM** e, em seguida, clique no resultado da pesquisa.



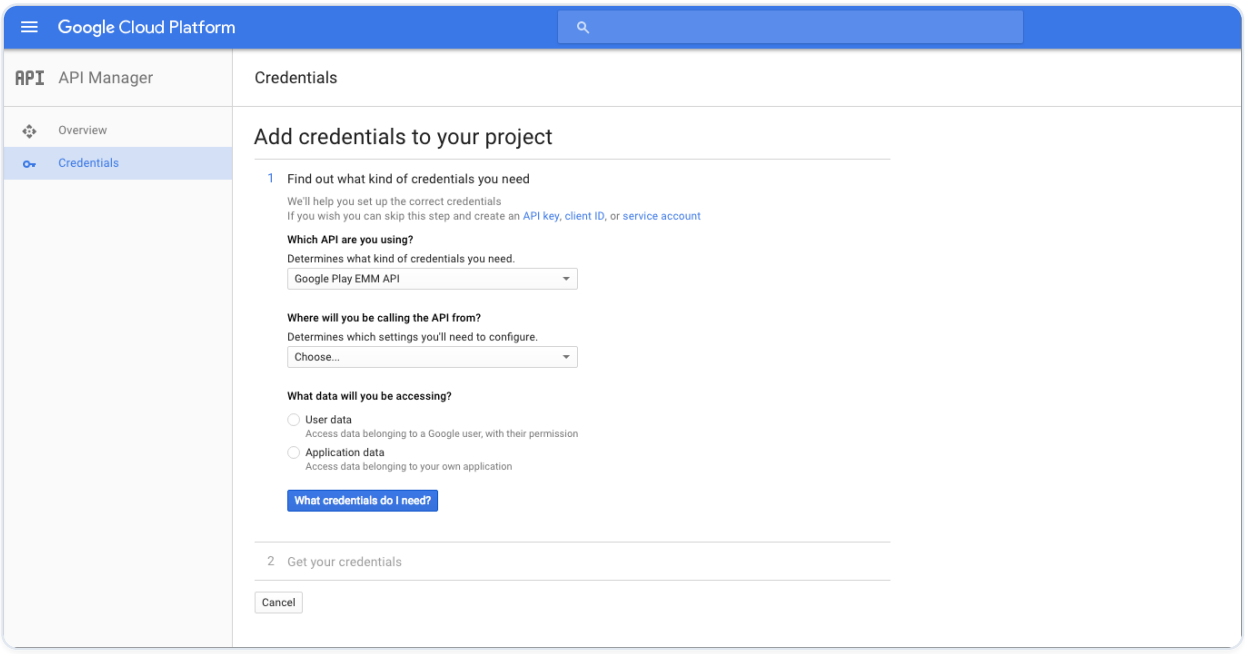
6. Na página **Visão geral**, clique em **Ativar**.



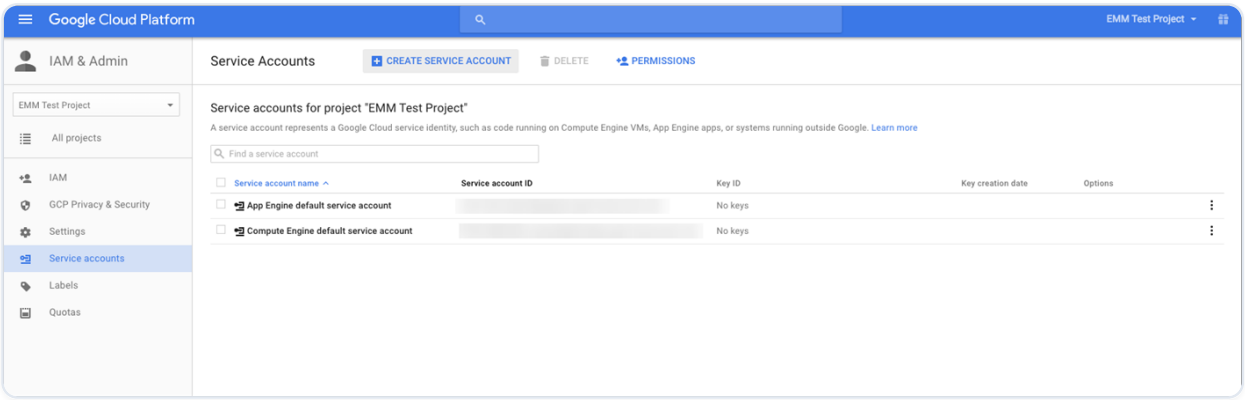
7. Ao lado de **API EMM do Google Play**, clique em **Ir para Credenciais**.



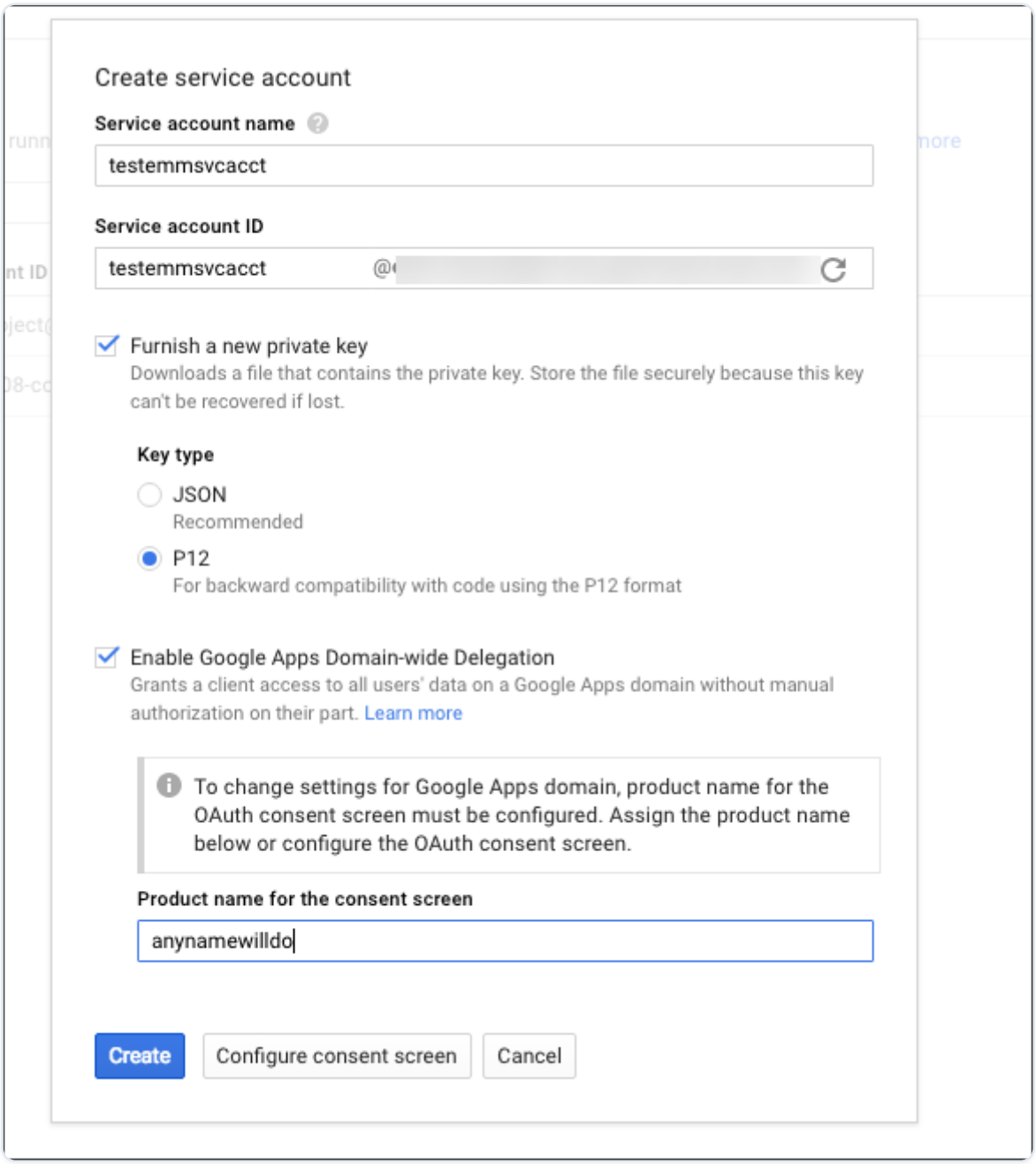
8. Na lista **Adicionar credenciais ao nosso projeto**, na etapa 1, clique em **conta de serviço**.



9. Na página **Contas de Serviço**, clique em **Criar Conta de Serviço**.

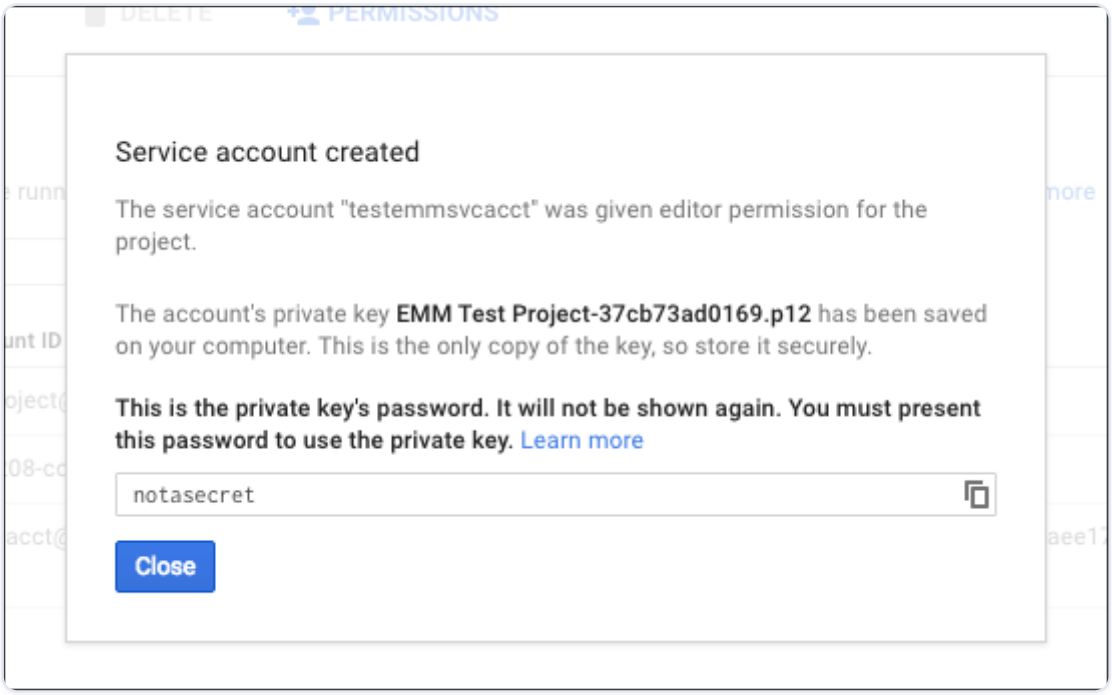


10. Em **Criar conta de serviço**, nomeie a conta e selecione a caixa de seleção **Fornecer uma nova chave privada**. Clique em **P12**, selecione a caixa de seleção **Ativar Delegação de todo o domínio do Google Apps** e, em seguida, clique em **Criar.**

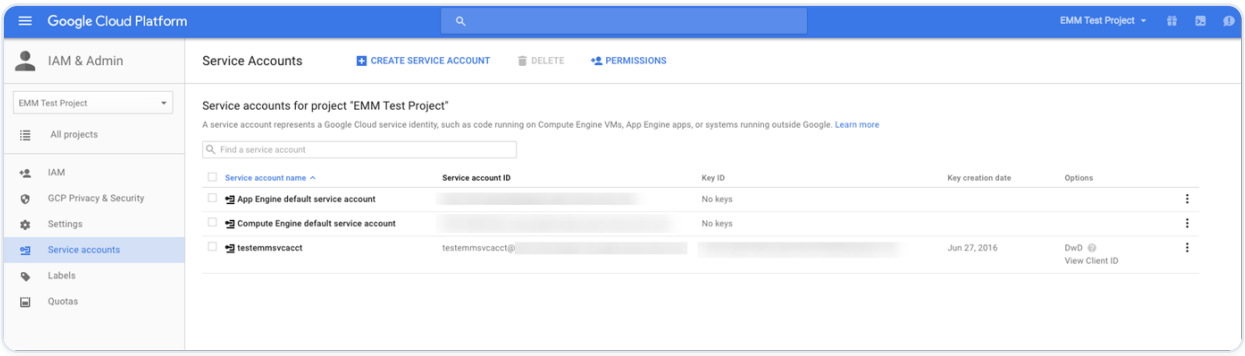


O certificado (arquivo P12) é baixado para o seu computador. Certifique-se de salvar o certificado em um local seguro.

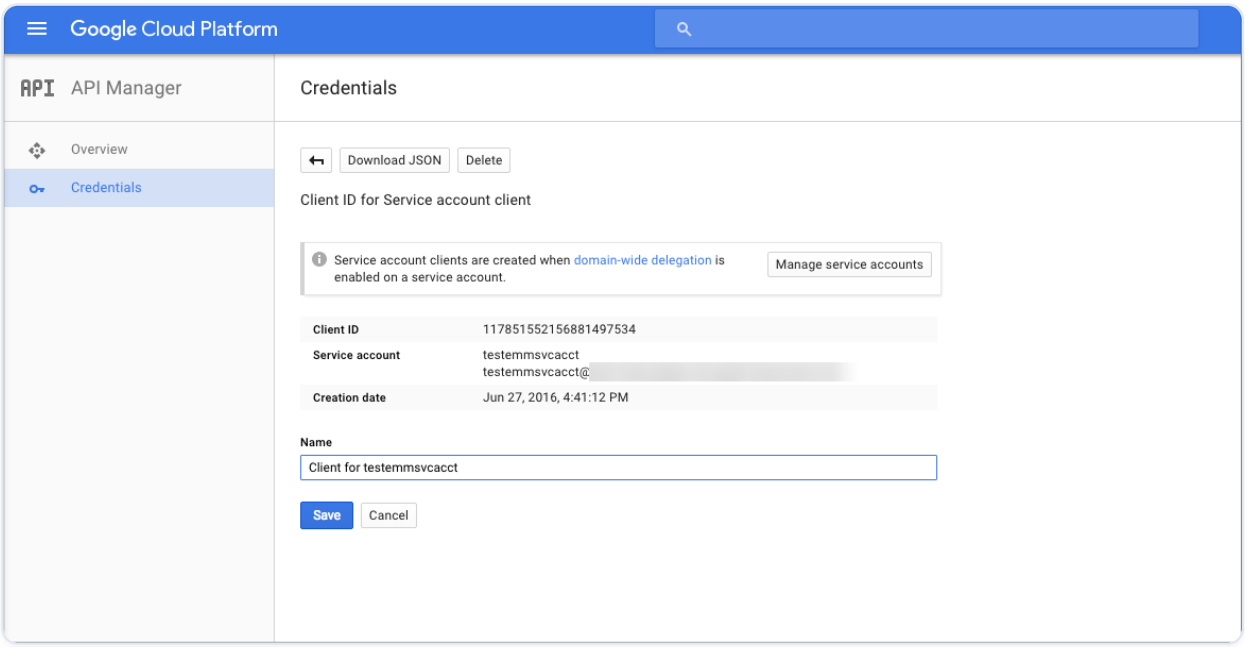
11. Na página de confirmação **Conta de serviço criada**, clique em **Fechar**.



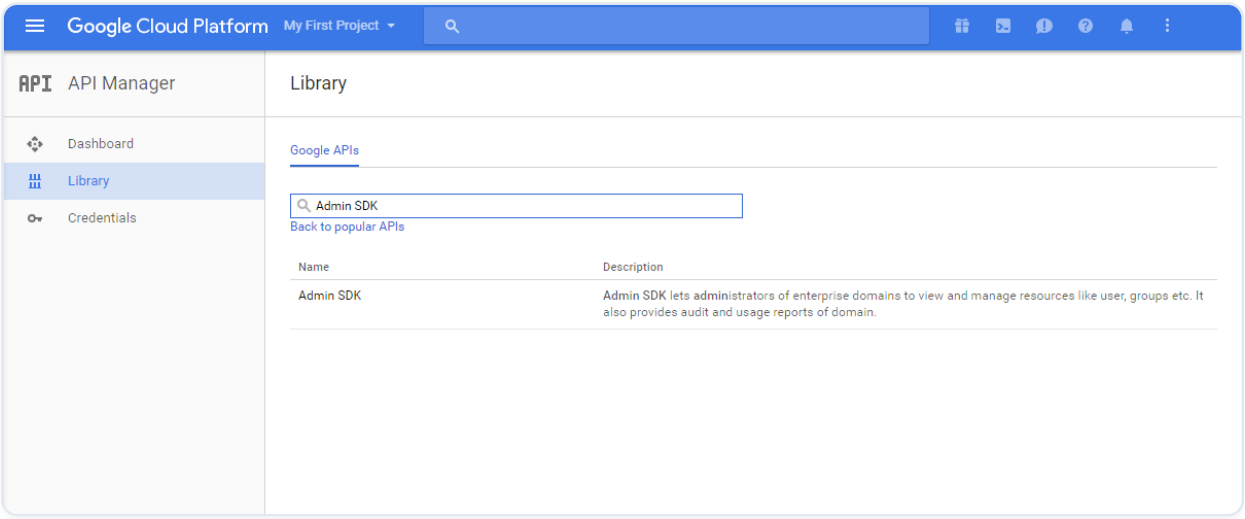
12. Em **Permissões**, clique em **Contas de serviço** e, em seguida, em **Opções** para sua conta de serviço, clique em **Visualizar ID do Cliente**.



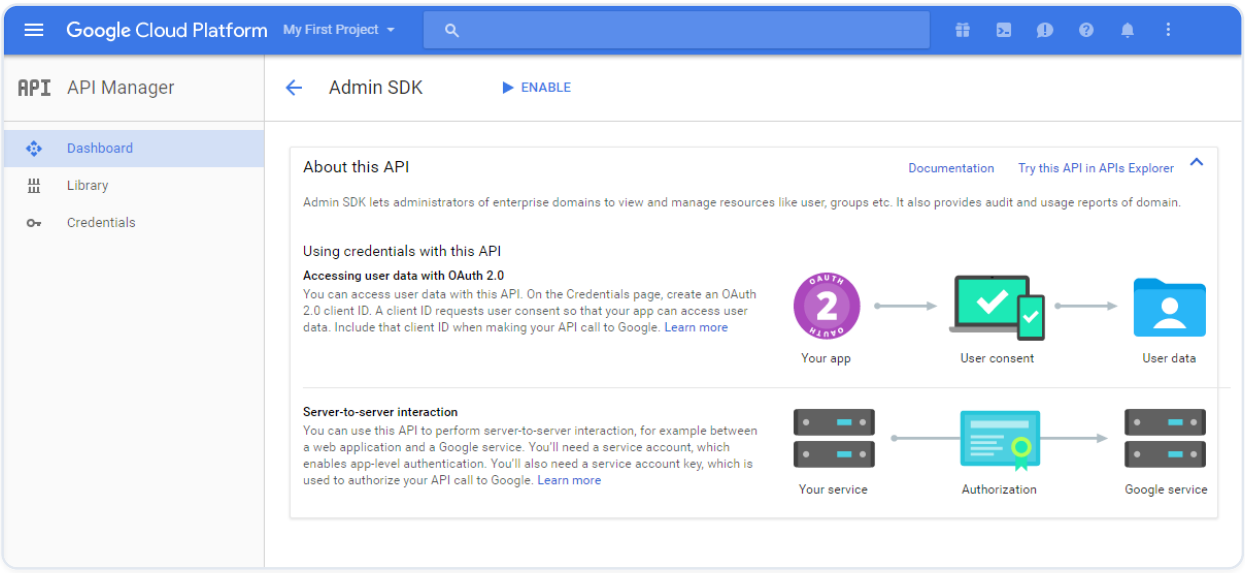
13. Os detalhes necessários para a autorização da conta no console de administração do Google são exibidos. Copie o **ID do Cliente** e o **ID da conta de serviço** para um local onde você possa recuperar as informações mais tarde. Você precisará dessas informações, juntamente com o nome de domínio, para enviar ao suporte da Citrix para permitir.



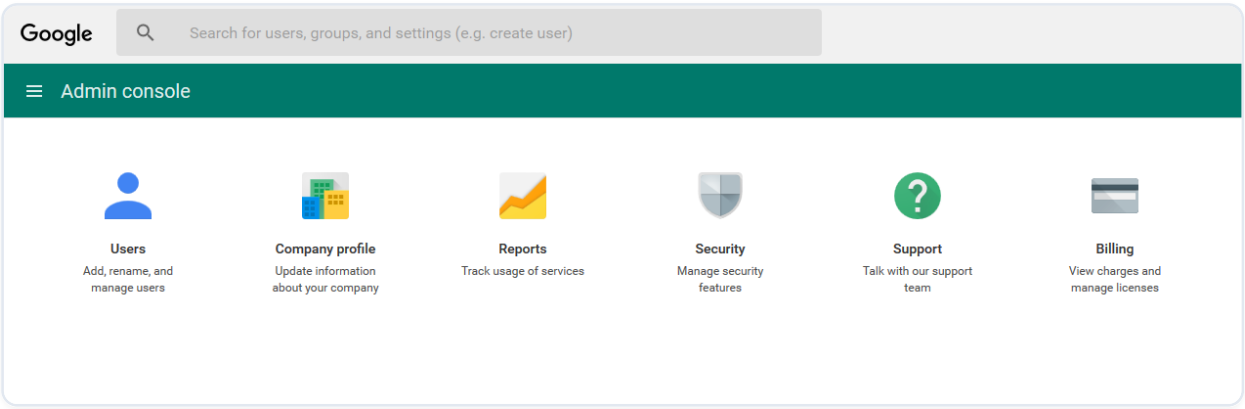
14. Na página **Biblioteca**, pesquise por **Admin SDK** e, em seguida, clique no resultado da pesquisa.



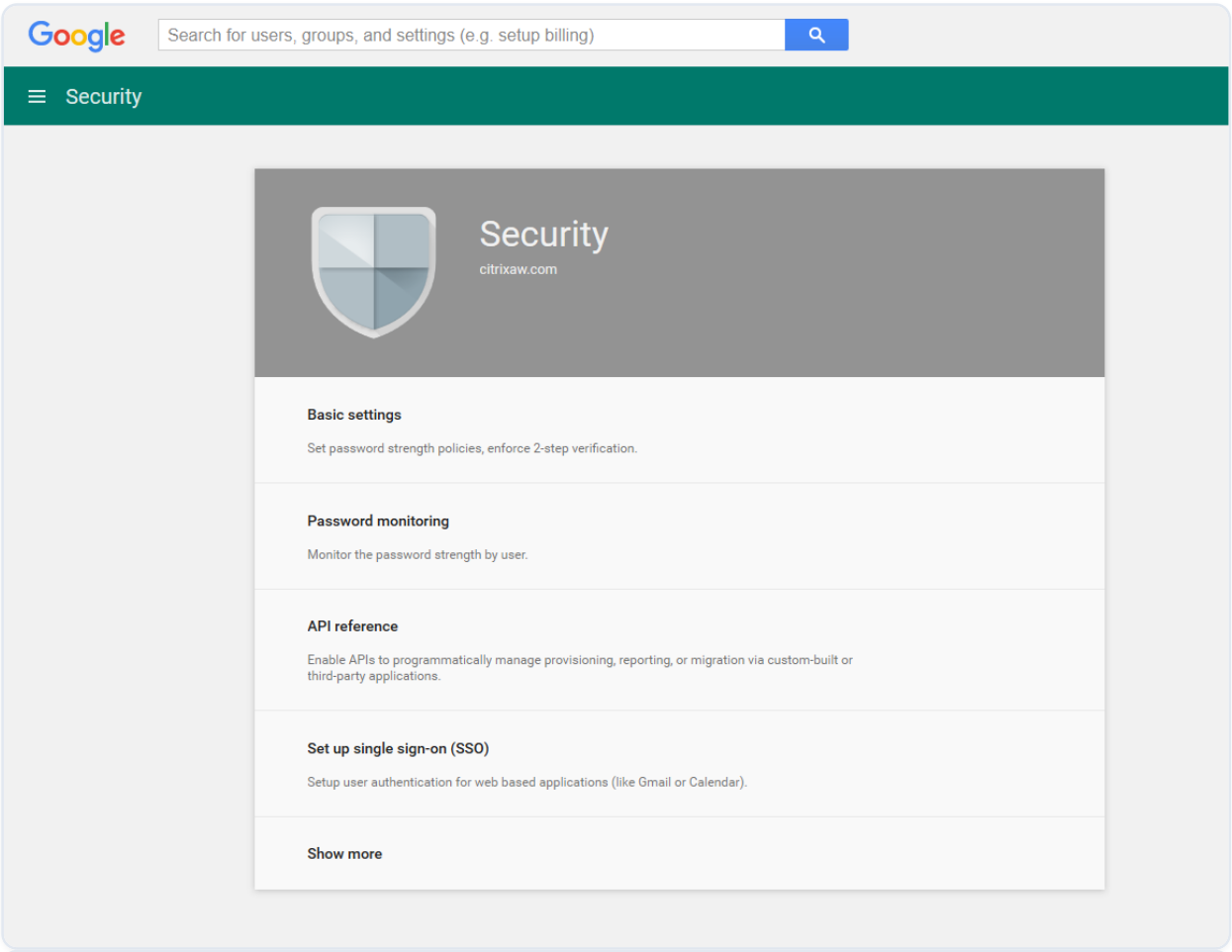
15. Na página **Visão geral**, clique em **Ativar**.

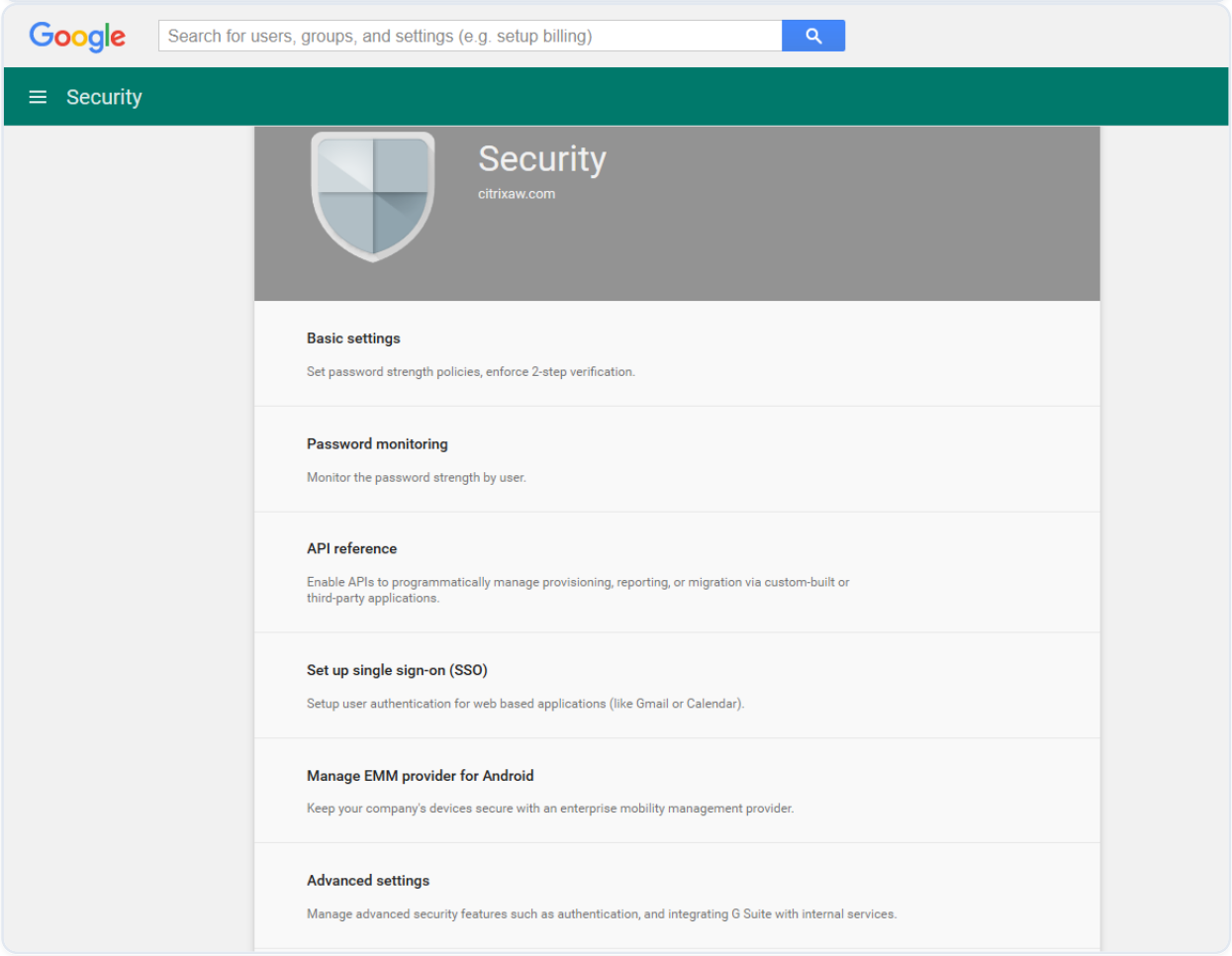


16. Abra o console de administração do Google para seu domínio e, em seguida, clique em **Segurança**.

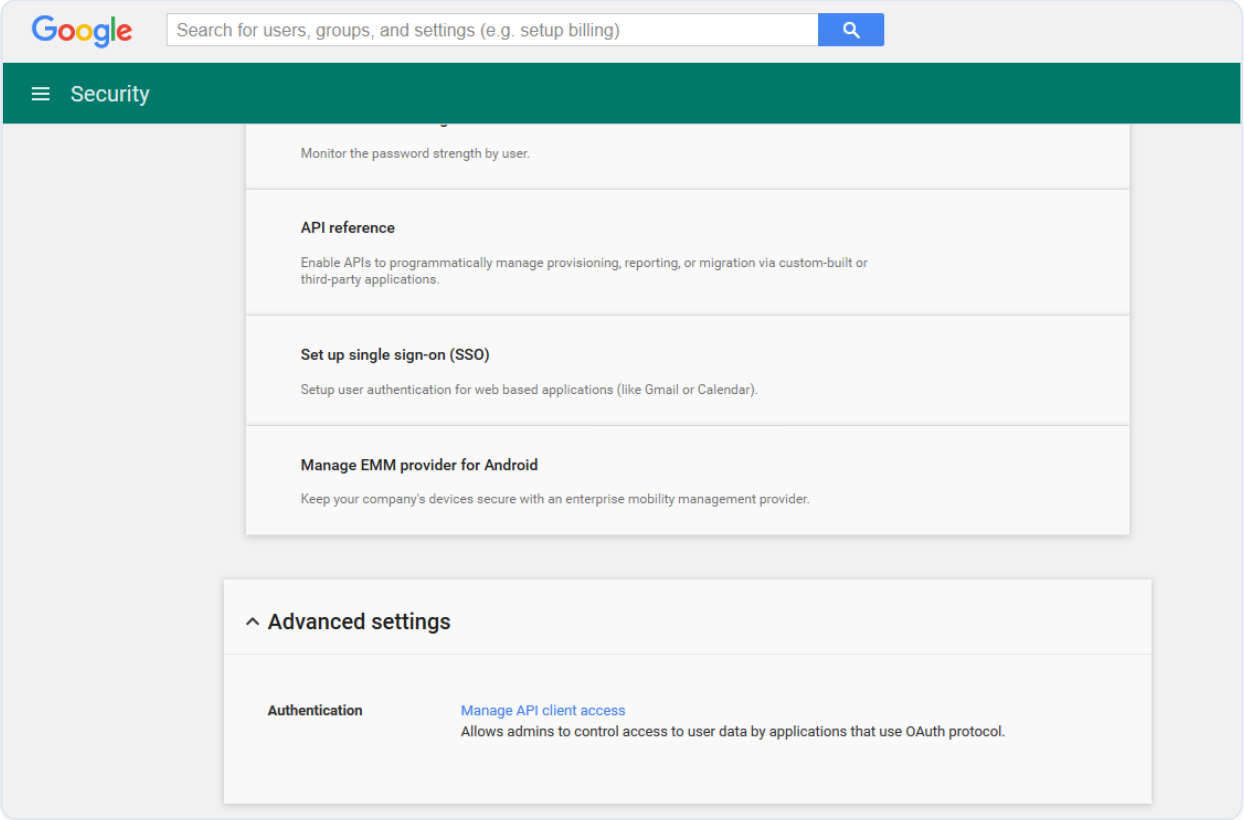


17. Na página **Configurações**, clique em **Mostrar mais** e, em seguida, clique em **Configurações avançadas**.

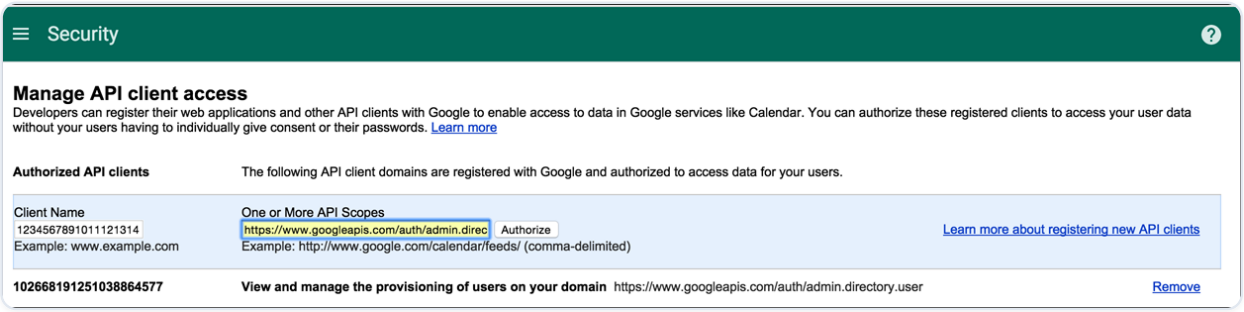

Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Show more


Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Manage EMM provider for Android
Keep your company's devices secure with an enterprise mobility management provider.
Advanced settings
Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. Clique em **Manage API client access**.



19. Em **Client Name**, digite o ID do cliente que você salvou anteriormente, em **One or More API Scopes**, digite `https://www.googleapis.com/auth/admin.directory.user` e clique em **Authorize**.



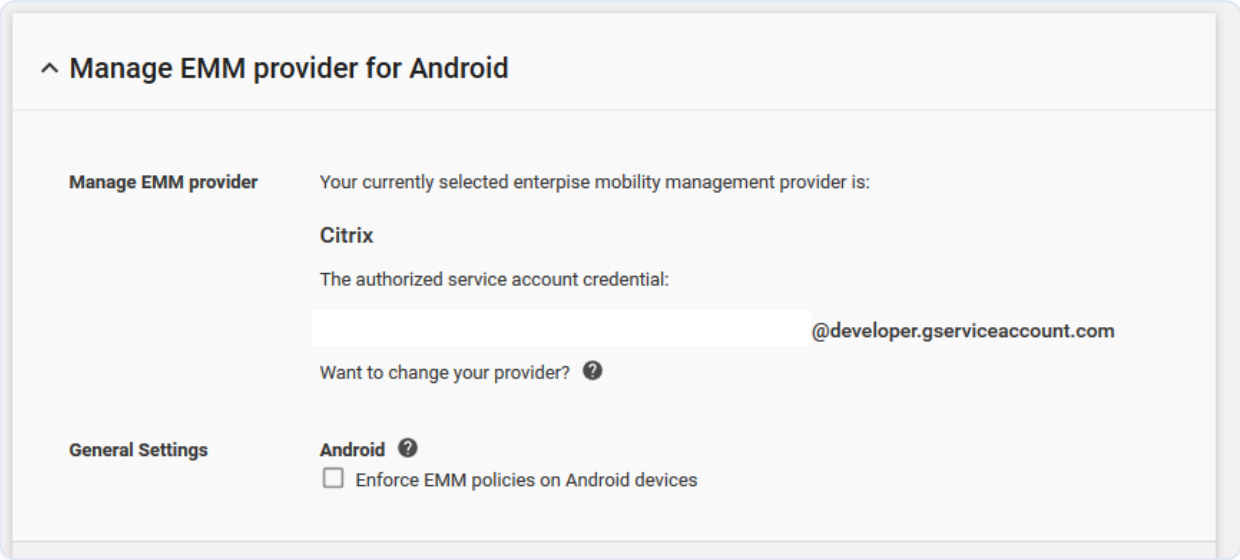
Vinculação ao EMM

Antes de usar o XenMobile para gerenciar seus dispositivos Android, você deve entrar em contato com o Suporte Técnico da Citrix e fornecer seu nome de domínio, conta de serviço e token de vinculação. A Citrix vincula o token ao XenMobile como seu provedor de gerenciamento de mobilidade empresarial (EMM). Para obter informações de contato do Suporte Técnico da Citrix, consulte Suporte Técnico da Citrix.

1. Para confirmar a vinculação, faça login no portal do Google Admin e clique em **Security**.
2. Clique em **Manage EMM provider for Android**.

Você verá que sua conta do Google Android Enterprise está vinculada à Citrix como seu provedor EMM.

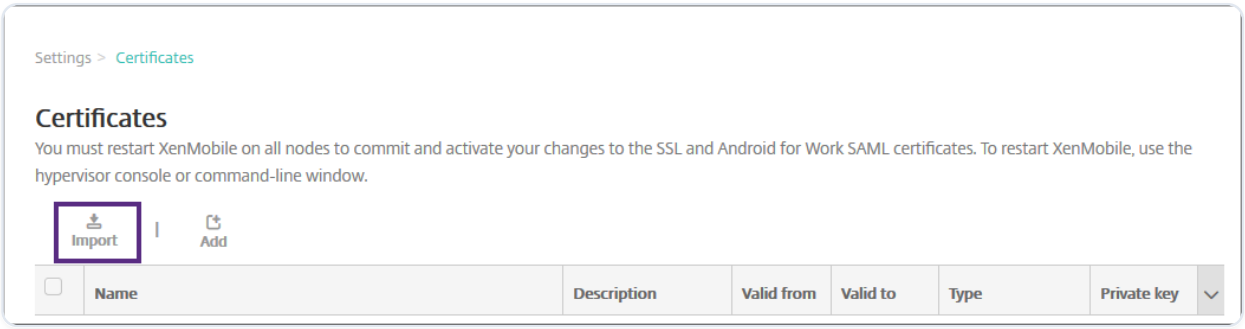
Depois de confirmar a vinculação do token, você pode começar a usar o console do XenMobile para gerenciar seus dispositivos Android. Importe o certificado P12 que você gerou na etapa 14. Configure as configurações do servidor Android Enterprise, ative o logon único (SSO) baseado em SAML e defina pelo menos uma política de dispositivo Android Enterprise.



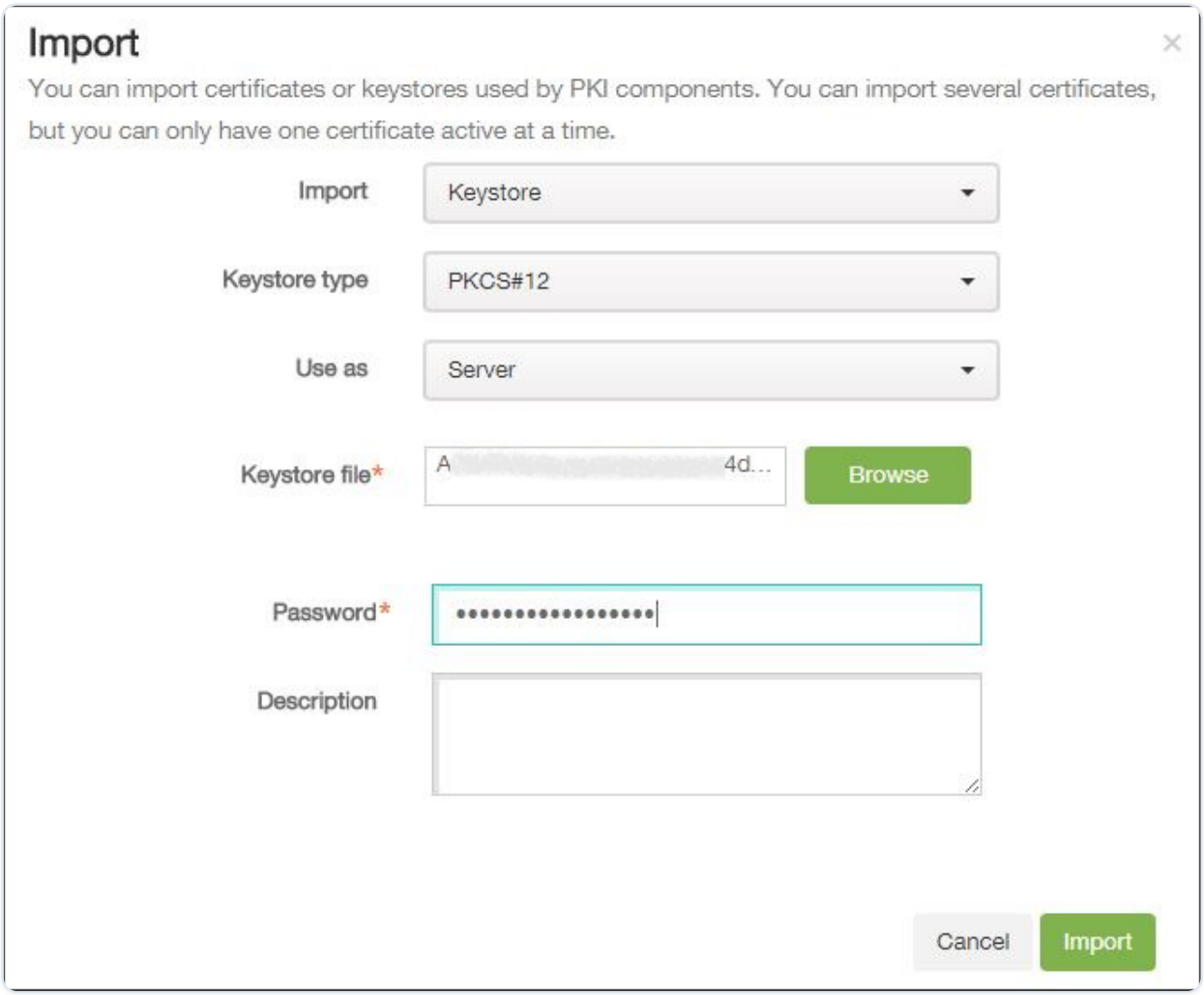
Importar o certificado P12

Siga estas etapas para importar seu certificado P12 do Android Enterprise:

1. Faça login no console do XenMobile.
2. Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e, em seguida, clique em **Certificados**. A página **Certificados** é exibida.



3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.



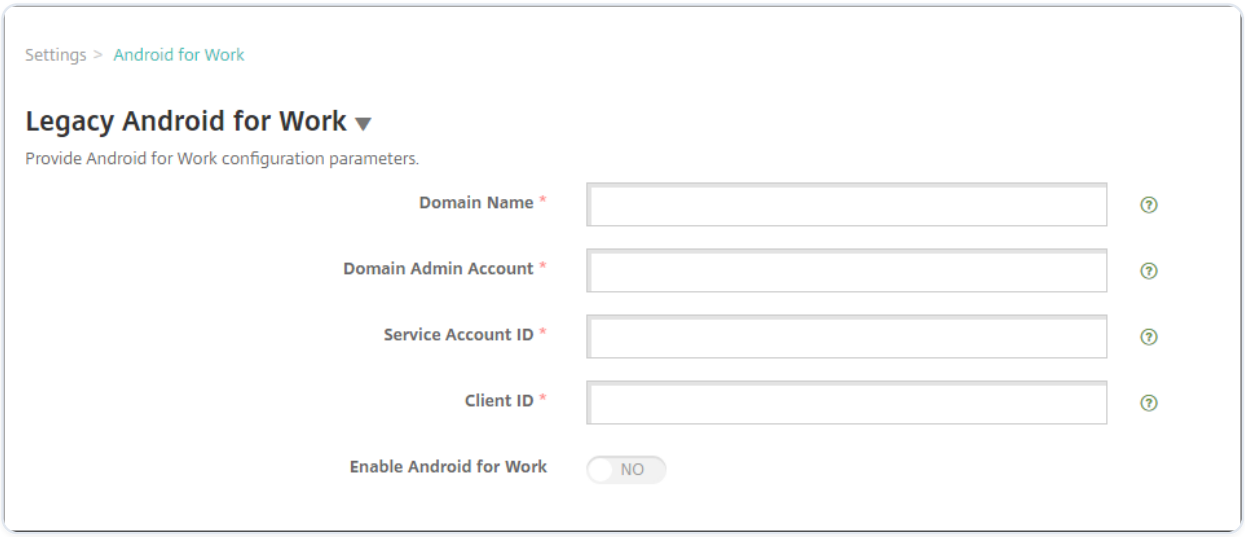
Configure as seguintes configurações:

- **Importar:** Na lista, clique em **Keystore**.
- **Tipo de Keystore:** Na lista, clique em **PKCS#12**.
- **Usar como:** Na lista, clique em **Servidor**.
- **Arquivo Keystore:** Clique em **Procurar** e navegar até o certificado P12.
- **Senha:** Digite a senha do keystore.
- **Descrição:** Opcionalmente, digite uma descrição do certificado.

4. Clique em **Importar**.

Configurar as definições do servidor Android Enterprise

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Android Enterprise**. A página **Android Enterprise** é exibida.

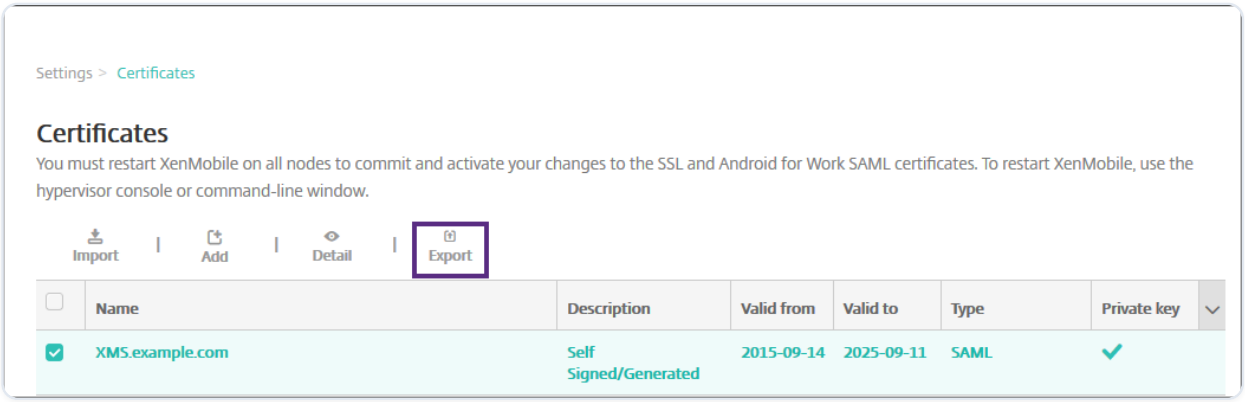


Configure as seguintes configurações e depois clique em **Salvar.**

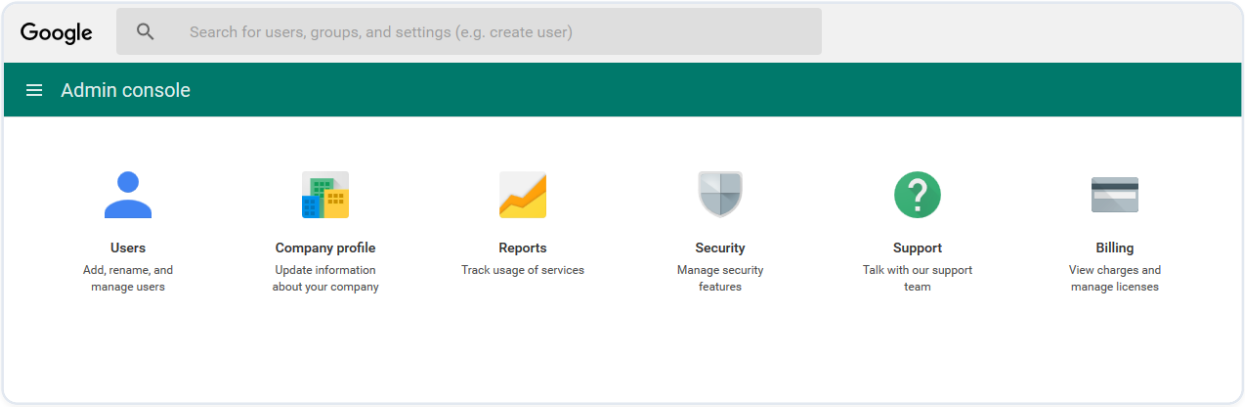
- **Nome de domínio:** Digite o nome de domínio do seu Android Enterprise; por exemplo, domain.com.
- **Conta de Administrador de Domínio:** Digite o nome de usuário do seu administrador de domínio; por exemplo, a conta de e-mail usada para o Google Developer Portal.
- **ID da Conta de Serviço:** Digite o ID da sua conta de serviço; por exemplo, o e-mail associado na Conta de Serviço do Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **ID do Cliente:** Digite o ID numérico do cliente da sua conta de serviço do Google.
- **Habilitar Android Enterprise:** Selecione para habilitar ou desabilitar o Android Enterprise.

Habilitar logon único baseado em SAML

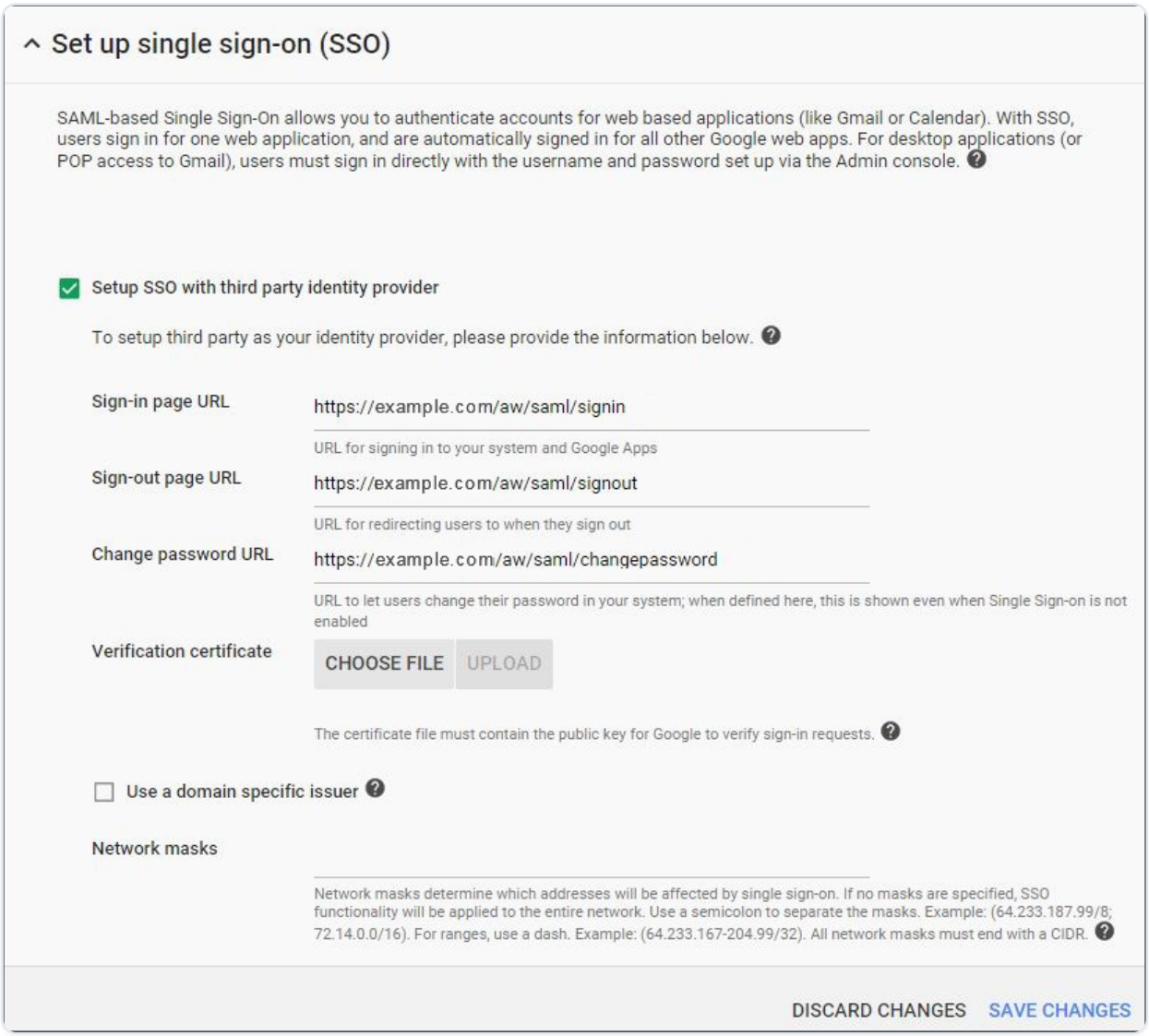
1. Faça logon no console do XenMobile.
2. Clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
3. Clique em **Certificados**. A página **Certificados** é exibida.



4. Na lista de certificados, clique no certificado SAML.
5. Clique em **Exportar** e salve o certificado no seu computador.
6. Faça login no portal do Google Admin usando suas credenciais de administrador do Android Enterprise. Para acessar o portal, consulte o portal do Google Admin.
7. Clique em **Segurança**.



8. Em **Segurança**, clique em **Configurar logon único (SSO)** e, em seguida, configure as seguintes configurações.

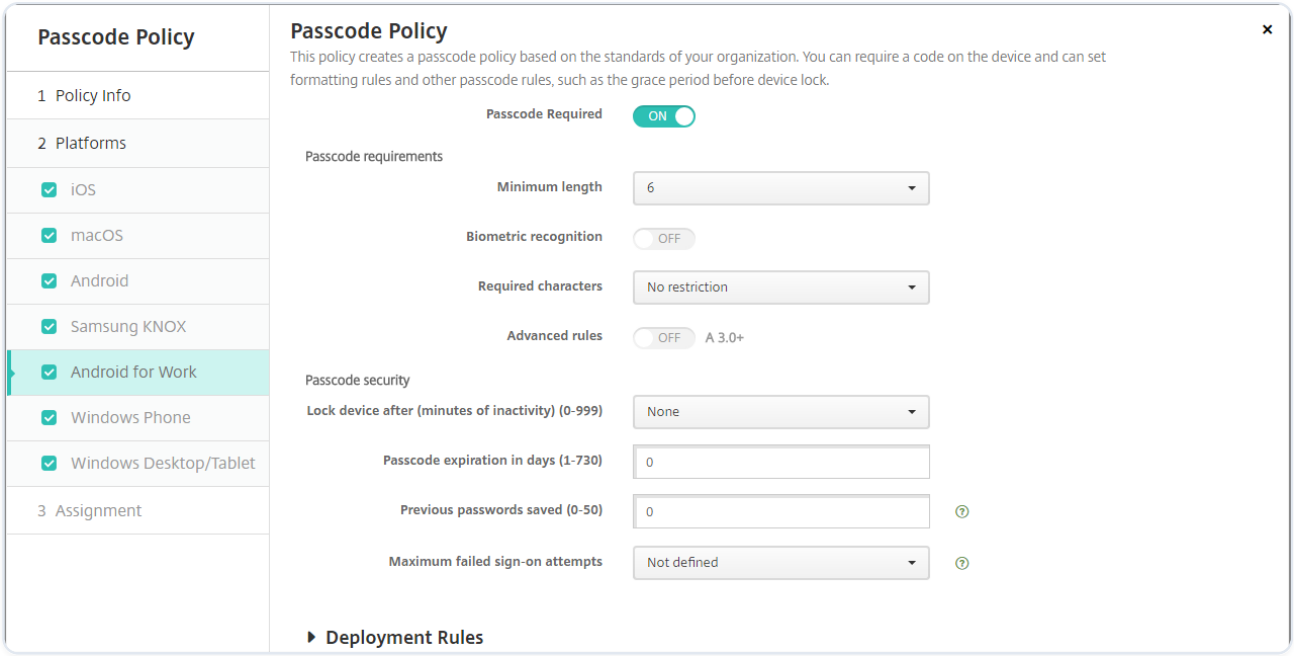


- **URL da página de login:** Digite o URL para usuários que fazem login no seu sistema e no Google Apps. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **URL da página de logout:** Digite o URL para o qual os usuários são redirecionados quando fazem logout. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **URL para alterar senha:** Digite o URL para permitir que os usuários alterem suas senhas em seu sistema. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Se este campo for definido, os usuários verão este prompt mesmo quando o SSO não estiver disponível.
- **Certificado de verificação:** Clique em **ESCOLHER ARQUIVO** e, em seguida, navegar até o certificado SAML exportado do XenMobile.

9. Clique em **SALVAR ALTERAÇÕES**.

Configurar uma política de dispositivo Android Enterprise

Configure uma política de senha para que os usuários precisem estabelecer uma senha em seus dispositivos quando se registrarem pela primeira vez.



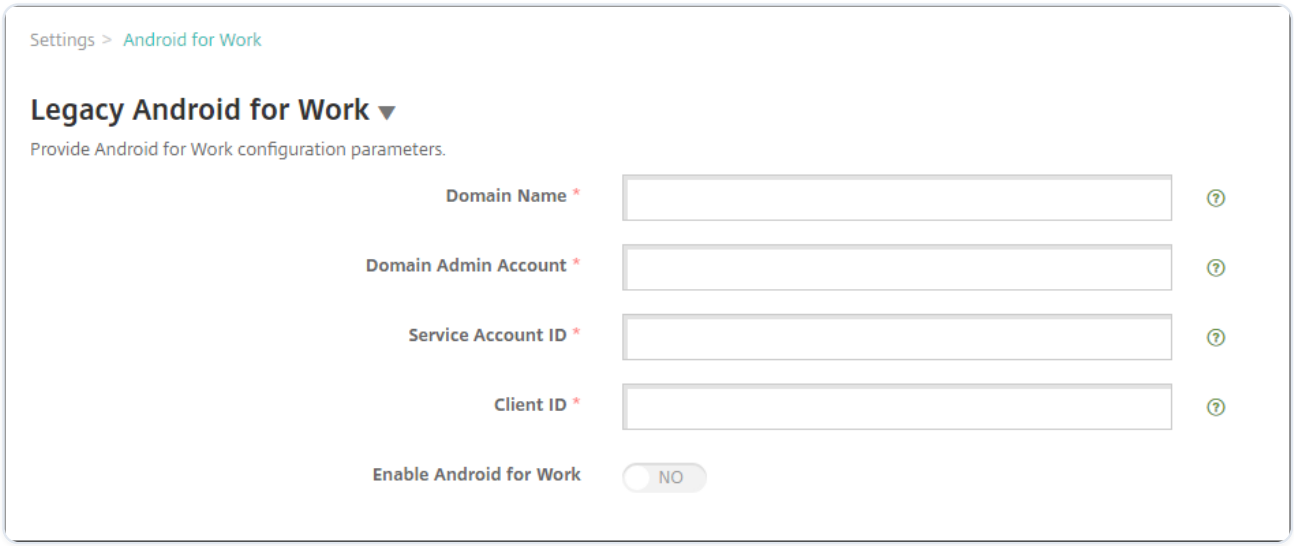
As etapas básicas para configurar qualquer política de dispositivo são as seguintes.

1. Faça login no console do XenMobile.
2. Clique em **Configurar** e, em seguida, clique em **Políticas de Dispositivo**.
3. Clique em **Adicionar** e, em seguida, na caixa de diálogo **Adicionar uma Nova Política**, selecione a política que deseja adicionar. Neste exemplo, você clica em **Senha**.
4. Conclua a página **Informações da Política**.
5. Clique em **Android Enterprise** e, em seguida, configure as definições para a política.
6. Atribua a política a um Grupo de Entrega.

Configurar as definições da conta do Android Enterprise

Antes de começar a gerenciar aplicativos e políticas Android em dispositivos, você deve configurar um domínio do Android Enterprise e informações da conta no XenMobile. Primeiro, conclua as tarefas de configuração do Android Enterprise no Google para configurar um administrador de domínio e obter um ID de conta de serviço e um token de vinculação.

1. No console web do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Android Enterprise**. A página de configuração do **Android Enterprise** é exibida.



1. Na página **Android Enterprise**, configure as seguintes definições:
   - **Nome de Domínio:** Digite seu nome de domínio.
   - **Conta de Administrador de Domínio:** Digite seu nome de usuário de administrador de domínio.
   - **ID da Conta de Serviço:** Digite seu ID da Conta de Serviço do Google.
   - **ID do Cliente::** Digite o ID do cliente da sua conta de serviço do Google.
   - **Habilitar Android Enterprise:** Selecione se deseja habilitar o Android Enterprise ou não.
2. Clique em **Salvar**.

Configurar o acesso de parceiro do Google Workspace para o XenMobile

Alguns recursos de gerenciamento de endpoint para Chrome usam APIs de parceiros do Google para se comunicar entre o XenMobile e seu domínio do Google Workspace. Por exemplo, o XenMobile requer as APIs para políticas de dispositivo que gerenciam recursos do Chrome, como o modo de navegação anônima e o modo de convidado.

Para habilitar as APIs de parceiro, você configura seu domínio do Google Workspace no console do XenMobile e, em seguida, configura sua conta do Google Workspace.

Configurar seu domínio do Google Workspace (anteriormente G Suite) no XenMobile

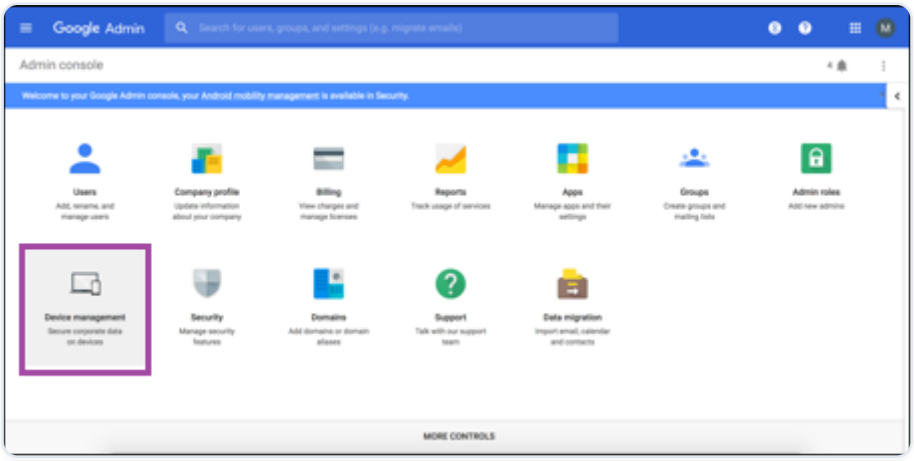
Para permitir que o XenMobile se comunique com as APIs em seu domínio do Google Workspace, vá para **Configurações > Configuração do Google Chrome** e configure as definições.

- **Domínio do G Suite:** O domínio do Google Workspace que hospeda as APIs necessárias pelo XenMobile.

- **Conta de administrador do G Suite:** A conta de administrador para o seu domínio do G Suite.
- **ID do cliente do G Suite:** O ID do cliente para Citrix. Use este valor para configurar o acesso de parceiro para o seu domínio do Google Workspace.
- **ID da empresa do G Suite:** O ID da empresa para sua conta, preenchido a partir de sua conta empresarial do Google.

Habilitar o acesso de parceiro para dispositivos e usuários em seu domínio do Google Workspace

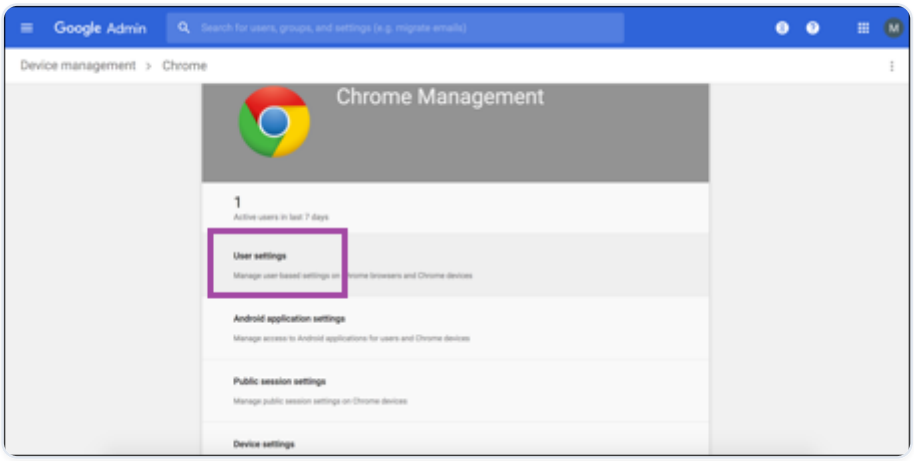
1. Faça login no console de administração do Google: `<https://admin.google.com>`
2. Clique em **Gerenciamento de Dispositivos**.



3. Clique em **Gerenciamento do Chrome**.



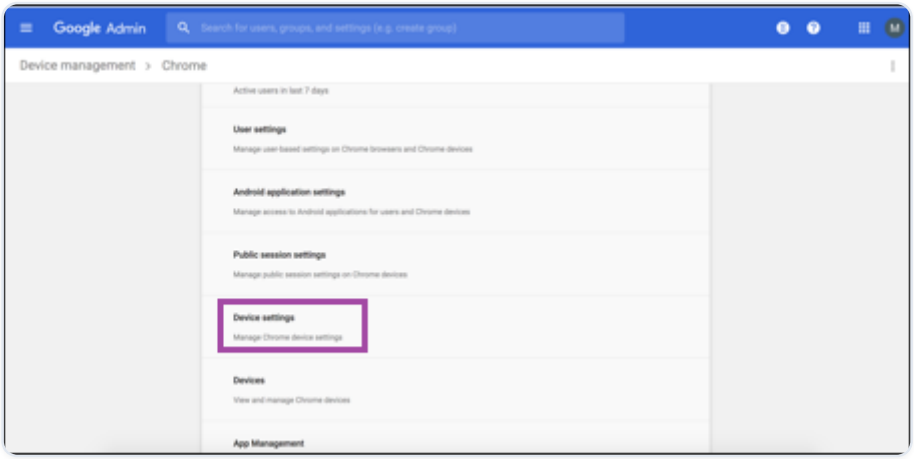
4. Clique em **Configurações do usuário**.



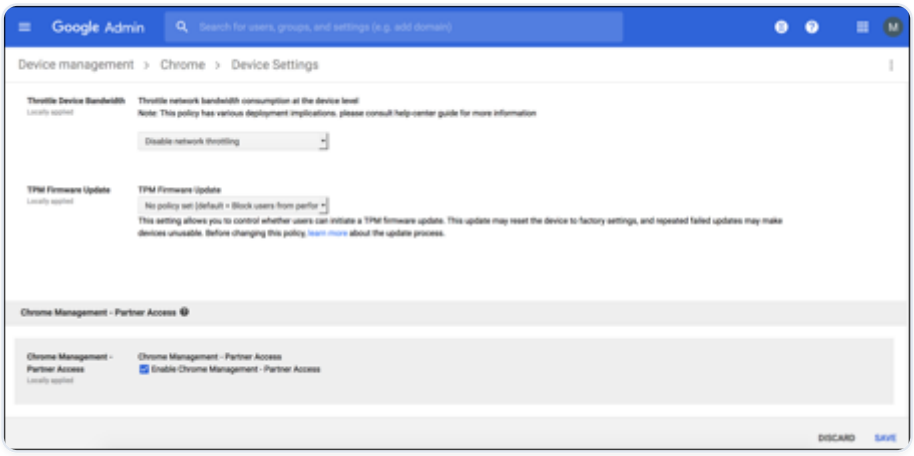
5. Pesquise por **Gerenciamento do Chrome - Acesso de Parceiro**.



6. Selecione a caixa de seleção **Ativar Gerenciamento do Chrome - Acesso de Parceiro**.
7. Concorde que você entende e deseja habilitar o acesso de parceiro. Clique em **Salvar**.
8. Na página de gerenciamento do Chrome, clique em **Configurações do dispositivo**.



9. Pesquise por **Gerenciamento do Chrome - Acesso de Parceiro**.



10. Selecione a caixa de seleção **Ativar Gerenciamento do Chrome - Acesso de Parceiro**.
11. Concorde que você entende e deseja habilitar o acesso de parceiro. Clique em **Salvar**.
12. Vá para a página **Segurança** e clique em **Configurações avançadas**.

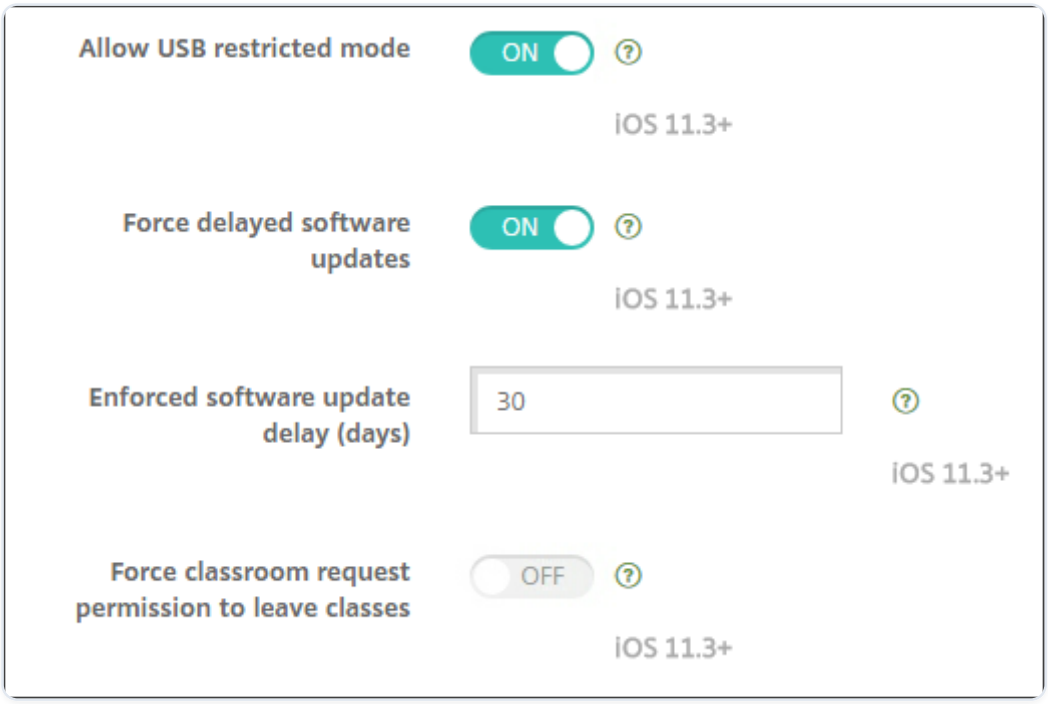


13. Clique em **Manage API client Access**.
14. No console do XenMobile, vá para **Settings > Google Chrome Configuration** e copie o valor de Google Workspace Client ID. Em seguida, retorne à página **Manage API client Access** e cole o valor copiado no campo **Client Name**.
15. Em **One or More API Scopes**, adicione a URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. Clique em **Authorize**.

A mensagem "Your settings have been saved" aparece.



Registrando dispositivos Android Enterprise

Se o processo de registro do seu dispositivo exigir que os usuários insiram um nome de usuário ou ID de usuário, o formato aceito depende de como o XenMobile Server está configurado para pesquisar usuários por Nome Principal de Usuário (UPN) ou nome de conta SAM.

Se o XenMobile Server estiver configurado para pesquisar usuários por UPN, os usuários devem inserir um UPN no formato:

- *username@domain*

Se o XenMobile Server estiver configurado para pesquisar usuários por SAM, os usuários devem inserir um SAM em um destes formatos:

- *username@domain*
- *domain\username*

Para determinar para qual tipo de nome de usuário seu XenMobile Server está configurado:

1. No console do XenMobile Server, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **LDAP** para visualizar a configuração da conexão LDAP.
3. Perto da parte inferior da página, visualize o campo **Pesquisa de usuário por**:

- Se estiver definido como **userPrincipalName**, o XenMobile Server está configurado para UPN.
- Se estiver definido como **sAMAccountName**, o XenMobile Server está configurado para SAM.

Desvinculando uma empresa Android Enterprise

Você pode desvincular uma empresa Android Enterprise usando o console do XenMobile Server e as Ferramentas XenMobile.

Ao executar esta tarefa, o XenMobile Server abre uma janela pop-up para as Ferramentas XenMobile. Antes de começar, certifique-se de que o XenMobile Server tenha permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desative o bloqueio de pop-ups e adicione o endereço do site XenMobile à lista de permissões de bloqueio de pop-ups.

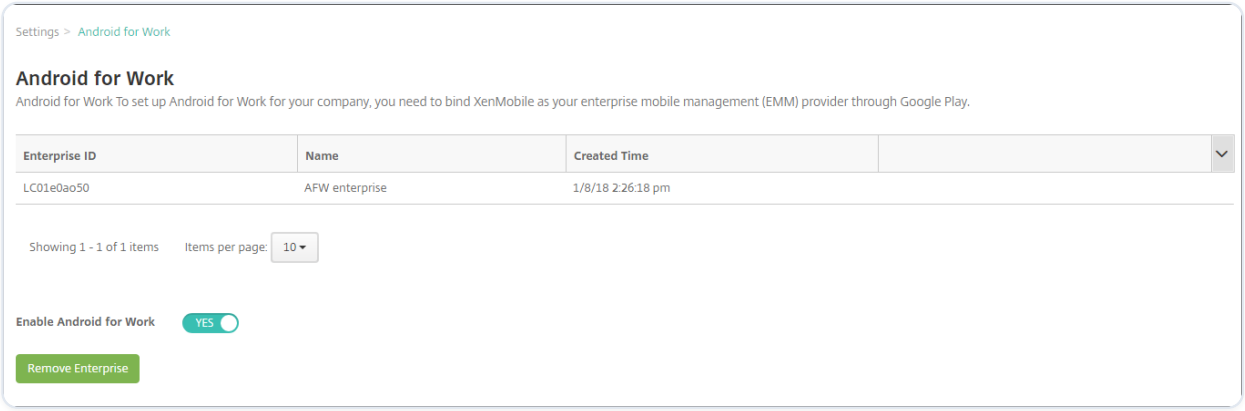
> **Aviso:**
>
> Depois que uma empresa é desvinculada, os aplicativos Android Enterprise em dispositivos já registrados por meio dela são redefinidos para seus estados padrão. Os dispositivos não serão mais gerenciados pelo Google. Registrá-los novamente em uma empresa Android Enterprise pode não restaurar a funcionalidade anterior sem configuração adicional.

> Depois que a empresa Android Enterprise é desvinculada:

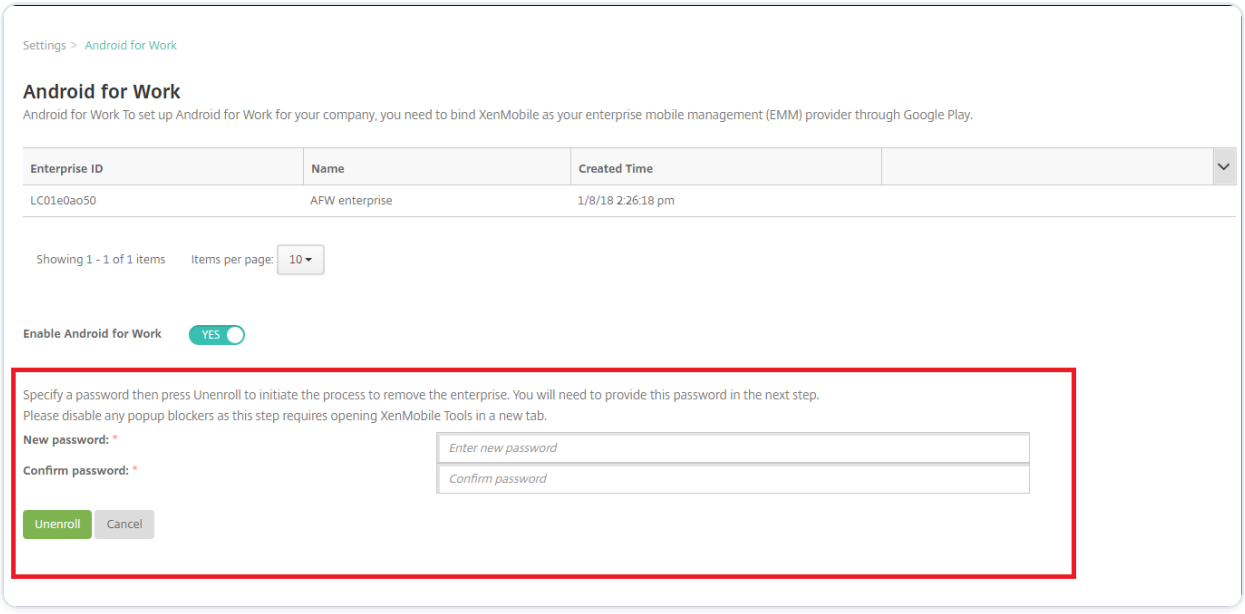
- Dispositivos e usuários registrados por meio da empresa têm os aplicativos Android Enterprise redefinidos para o estado padrão. As políticas de Permissões de Aplicativos Android Enterprise e Restrições de Aplicativos Android Enterprise aplicadas anteriormente não têm mais efeito.
- Os dispositivos registrados por meio da empresa são gerenciados pelo XenMobile, mas não são gerenciados do ponto de vista do Google. Nenhum novo aplicativo Android Enterprise pode ser adicionado. Nenhuma política de Permissões de Aplicativos Android Enterprise ou Restrições de Aplicativos Android Enterprise pode ser aplicada. Outras políticas, como Agendamento, Senha e Restrições, ainda podem ser aplicadas a esses dispositivos.
- Se você tentar registrar dispositivos no Android Enterprise, eles serão registrados como dispositivos Android, não como dispositivos Android Enterprise.

Para desvincular uma empresa do Android Enterprise:

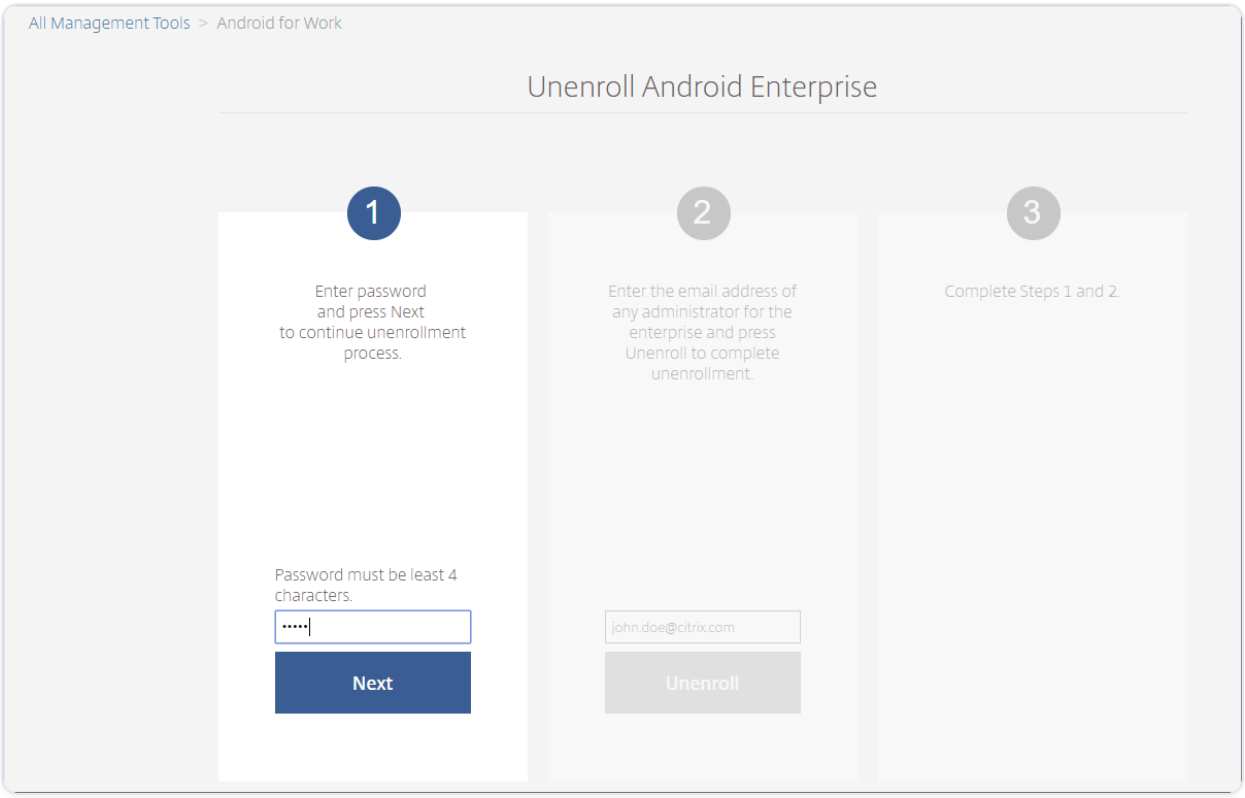
1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página Configurações é exibida.
2. Na página Configurações, clique em **Android Enterprise**.
3. Clique em **Remover Empresa**.



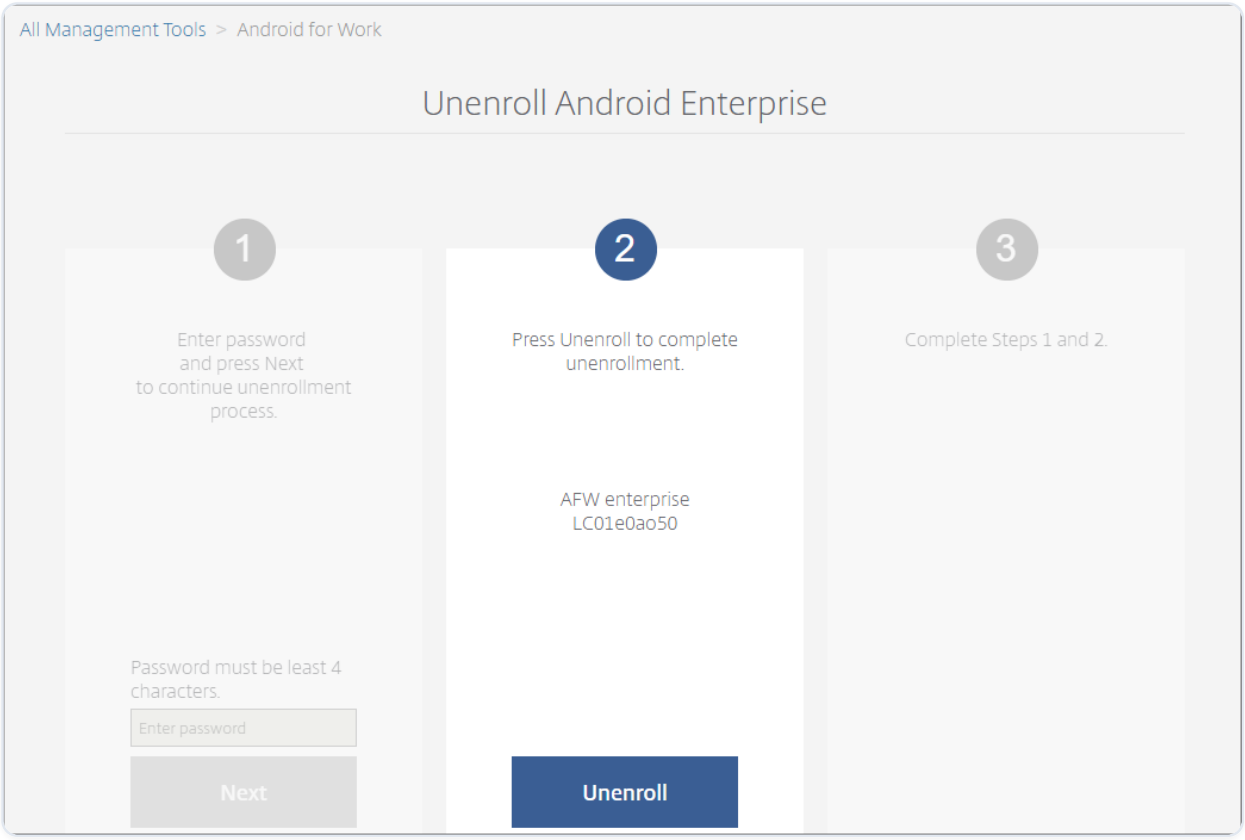
4. Especifique uma senha. Você precisará dessa senha para a próxima etapa para concluir a desvinculação. Em seguida, clique em **Desvincular**.



5. Quando a página Ferramentas do XenMobile for aberta, insira a senha que você criou na etapa anterior.



6. Clique em **Desvincular**.



Provisionamento de dispositivos totalmente gerenciados no Android Enterprise

Somente dispositivos de propriedade da empresa podem ser dispositivos totalmente gerenciados para o Android Enterprise. Em dispositivos totalmente gerenciados, o dispositivo inteiro, e não apenas o perfil de trabalho, é controlado pela empresa ou organização. Dispositivos totalmente gerenciados também são conhecidos como dispositivos gerenciados pelo trabalho.

O XenMobile oferece suporte a estes métodos de registro para dispositivos totalmente gerenciados:

- **afw#xenmobile:** Com este método de registro, o usuário insere os caracteres "afw#xenmobile" ao configurar o dispositivo. Este token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub.
- **Código QR:** O provisionamento por código QR é uma maneira fácil de provisionar uma frota distribuída de dispositivos que não suportam NFC, como tablets. O método de registro por código QR pode ser usado em dispositivos da frota que foram redefinidos para as configurações de fábrica. O método de registro por código QR configura e define dispositivos totalmente gerenciados ao escanear um código QR do assistente de configuração.
- **Toque NFC (Near Field Communication):** O método de registro por toque NFC pode ser usado em dispositivos da frota que foram redefinidos para as configurações de fábrica. Um toque NFC transfere dados entre dois dispositivos usando comunicação de campo próximo. Bluetooth, Wi-Fi e outros modos de comunicação são desativados em um dispositivo redefinido de fábrica. NFC é o único protocolo de comunicação que o dispositivo pode usar neste estado.

afw#xenmobile

O método de registro é usado após ligar um dispositivo novo ou redefinido de fábrica para a configuração inicial. Os usuários inserem "afw#xenmobile" quando solicitados a inserir uma conta Google. Esta ação baixa e instala o Secure Hub. Os usuários então seguem os prompts de configuração do Secure Hub para concluir o registro.

Este método de registro é recomendado para a maioria dos clientes porque a versão mais recente do Secure Hub é baixada da Google Play Store. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download a partir do XenMobile Server.

Pré-requisitos:

- Compatível com todos os dispositivos Android executando Android 5.0 e posterior.

Código QR

Para registrar um dispositivo no modo de dispositivo usando um código QR, você gera um código QR criando um JSON e convertendo o JSON em um código QR. As câmeras do dispositivo escaneiam o código QR para registrar o dispositivo.

Pré-requisitos:

- Compatível com todos os dispositivos Android executando Android 7.0 e superior.

CRIAR UM CÓDIGO QR A PARTIR DE UM JSON

Crie um JSON com os seguintes campos.

Estes campos são obrigatórios:

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valor: com.zenprise/com.zenprise.configuration.AdminFunction

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valor: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Chave: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valor: `https://path/to/securehub.apk`

> **Nota:**
>
> Se o Secure Hub for carregado no Citrix XenMobile Server como um aplicativo empresarial, ele poderá ser baixado de `https://<fqdn>:4443/*instanceName*/worxhome.apk`. O caminho para o APK do Secure Hub deve estar acessível pela conexão Wi-Fi à qual o dispositivo se conecta durante o provisionamento.

> Estes campos são opcionais:

- **android.app.extra.PROVISIONING_LOCALE:** Insira os códigos de idioma e país.

  Os códigos de idioma são códigos de idioma ISO de duas letras minúsculas (como en), conforme definido por ISO 639-1. Os códigos de país são códigos de país ISO de duas letras

maiúsculas (como US), conforme definido por ISO 3166-1. Por exemplo, insira en_US para inglês falado nos Estados Unidos.

- **android.app.extra.PROVISIONING_TIME_ZONE:** O fuso horário em que o dispositivo está sendo executado.

  Insira um nome Olson no formato área/localização. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir um, o fuso horário será preenchido automaticamente.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Tempo em milissegundos desde a Época.

  A época Unix (ou tempo Unix, tempo POSIX, ou timestamp Unix) é o número de segundos que se passaram desde January 1, 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (em ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Defina como **true** para pular a criptografia durante a criação do perfil. Defina como **false** para forçar a criptografia durante a criação do perfil.

Um JSON típico se parece com o seguinte:

Imagem de um JSON típico(/en-us/xenmobile/server/media/afw-qr-code-json.png)

Valide o JSON criado usando qualquer ferramenta de validação de JSON, como https://jsonlint.com. Converta essa string JSON em um código QR usando qualquer gerador de código QR online, como https://goqr.me.

Este código QR é escaneado por um dispositivo redefinido de fábrica para registrar o dispositivo no modo de dispositivo gerenciado pelo trabalho.

Para registrar o dispositivo

Para registrar um dispositivo como um dispositivo totalmente gerenciado, o dispositivo deve estar no estado de redefinição de fábrica.

1. Toque na tela seis vezes na tela de boas-vindas para iniciar o fluxo de registro por código QR.
2. Quando solicitado, conecte-se ao Wi-Fi. O local de download do Secure Hub no código QR (codificado no JSON) é acessível por esta rede Wi-Fi.

   Assim que o dispositivo se conecta com sucesso ao Wi-Fi, ele baixa um leitor de código QR do Google e inicia a câmera.
3. Aponte a câmera para o código QR para escanear o código.

O Android baixa o Secure Hub do local de download no código QR, valida a assinatura do certificado de assinatura, instala o Secure Hub e o define como proprietário do dispositivo.

Para mais informações, consulte este guia do Google para desenvolvedores Android EMM: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`.

Toque NFC

Para registrar um dispositivo como um dispositivo totalmente gerenciado usando toques NFC, são necessários dois dispositivos: Um que esteja redefinido para as configurações de fábrica e outro executando a Ferramenta de Provisionamento XenMobile.

Pré-requisitos:

- Compatível com todos os dispositivos Android executando Android 5.0, Android 5.1, Android 6.0 e superior.
- Uma versão 10.4 do XenMobile Server que esteja habilitada para Android Enterprise.
- Um dispositivo novo ou redefinido de fábrica, provisionado para Android Enterprise como um dispositivo totalmente gerenciado. Você pode encontrar as etapas para concluir este pré-requisito mais adiante neste artigo.
- Outro dispositivo com capacidade NFC, executando a Ferramenta de Provisionamento configurada. A Ferramenta de Provisionamento está disponível no Secure Hub 10.4 ou na página de downloads da Citrix.

Cada dispositivo pode ter apenas um perfil do Android Enterprise, gerenciado por um aplicativo de gerenciamento de mobilidade empresarial (EMM). No XenMobile, o Secure Hub é o aplicativo EMM. Apenas um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo EMM remove o primeiro aplicativo EMM.

DADOS TRANSFERIDOS ATRAVÉS DO TOQUE NFC

O provisionamento de um dispositivo redefinido de fábrica exige que você envie os seguintes dados por meio de um toque NFC para inicializar o Android Enterprise:

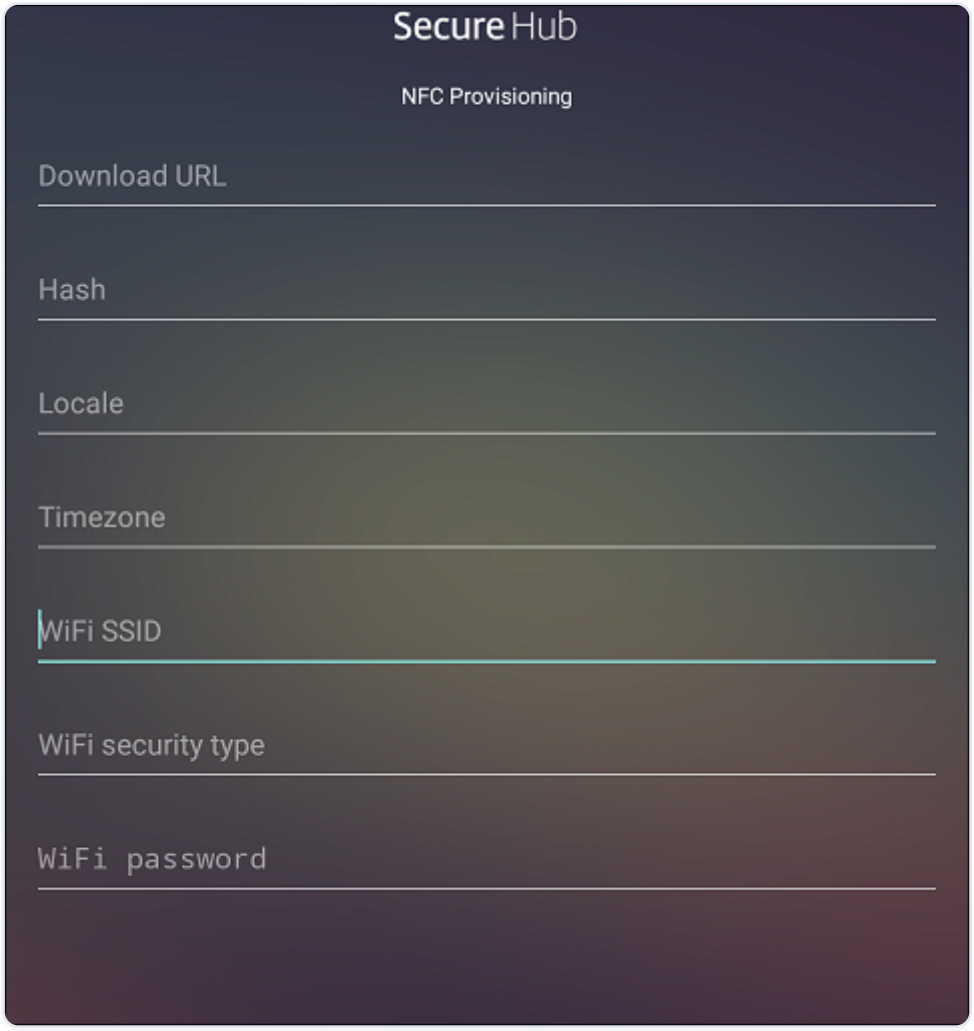
- Nome do pacote do aplicativo provedor de EMM que atua como proprietário do dispositivo (neste caso, Secure Hub).
- Localização na Intranet/Internet de onde o dispositivo pode baixar o aplicativo provedor de EMM.
- Hash SHA1 do aplicativo provedor de EMM para verificar se o download foi bem-sucedido.

- Detalhes da conexão Wi-Fi para que um dispositivo redefinido de fábrica possa se conectar e baixar o aplicativo provedor de EMM. Observação: o Android agora não oferece suporte a Wi-Fi 802.1x para esta etapa.
- Fuso horário para o dispositivo (opcional).
- Localização geográfica para o dispositivo (opcional).

Quando os dois dispositivos são tocados, os dados da Ferramenta de Provisionamento são enviados para o dispositivo redefinido de fábrica. Esses dados são então usados para baixar o Secure Hub com as configurações de administrador. Se você não inserir os valores de fuso horário e localização, o Android configurará automaticamente os valores no novo dispositivo.

CONFIGURANDO A FERRAMENTA DE PROVISIONAMENTO DO XENMOBILE

Antes de fazer um NFC bump, você deve configurar a Ferramenta de Provisionamento. Essa configuração é então transferida para o dispositivo redefinido de fábrica durante o NFC bump.



Você pode digitar dados nos campos obrigatórios ou preenchê-los por meio de um arquivo de texto. As etapas no próximo procedimento descrevem como configurar o arquivo de texto e contêm descrições para cada campo. O aplicativo não salva informações depois que você as

digita, então você pode querer criar um arquivo de texto para manter as informações para uso futuro.
Para configurar a Ferramenta de Provisionamento usando um arquivo de texto
Nomeie o arquivo nfcprovisioning.txt e coloque-o na pasta /sdcard/ no cartão SD do dispositivo. O aplicativo poderá então ler o arquivo de texto e preencher os valores.

O arquivo de texto deve ter os seguintes dados:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Esta linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo redefinido de fábrica se conecta ao Wi-Fi após o NFC bump, o dispositivo deve ter acesso a este local para download. A URL é uma URL regular, sem necessidade de formatação especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

Esta linha é o checksum do aplicativo do provedor EMM. Este checksum é usado para verificar se o download foi bem-sucedido. As etapas para obter o checksum são discutidas posteriormente neste artigo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esta linha é o SSID Wi-Fi conectado do dispositivo no qual a Ferramenta de Provisionamento está sendo executada.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Os valores suportados são WEP e WPA2. Se o Wi-Fi estiver desprotegido, este campo deve estar vazio.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Se o Wi-Fi não estiver protegido, este campo deve estar vazio.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO de duas letras minúsculas (como en) conforme definido por ISO 639-1. Os códigos de país são códigos de país ISO de duas letras maiúsculas (como US) conforme definido por ISO 3166-1. Por exemplo, digite en_US para inglês falado nos Estados Unidos. Se você não digitar nenhum código, o país e o idioma serão preenchidos automaticamente.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

O fuso horário em que o dispositivo está sendo executado. Digite um nome Olson no formato área/localização. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir um nome, o fuso horário será preenchido automaticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Esses dados não são necessários, pois o valor é codificado no aplicativo como Secure Hub. É mencionado aqui apenas para fins de conclusão.

Se houver um Wi-Fi protegido usando WPA2, um arquivo nfcprovisioning.txt preenchido pode ser semelhante ao seguinte:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name`

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2`

`android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

Se houver um Wi-Fi desprotegido, um arquivo nfcprovisioning.txt concluído pode ser parecido com o seguinte:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

PARA OBTER O CHECKSUM DO SECURE HUB

Para obter o checksum de qualquer aplicativo, adicione o aplicativo como um aplicativo empresarial.

1. No console do XenMobile, vá para **Configurar > Aplicativos** e clique em **Adicionar**.

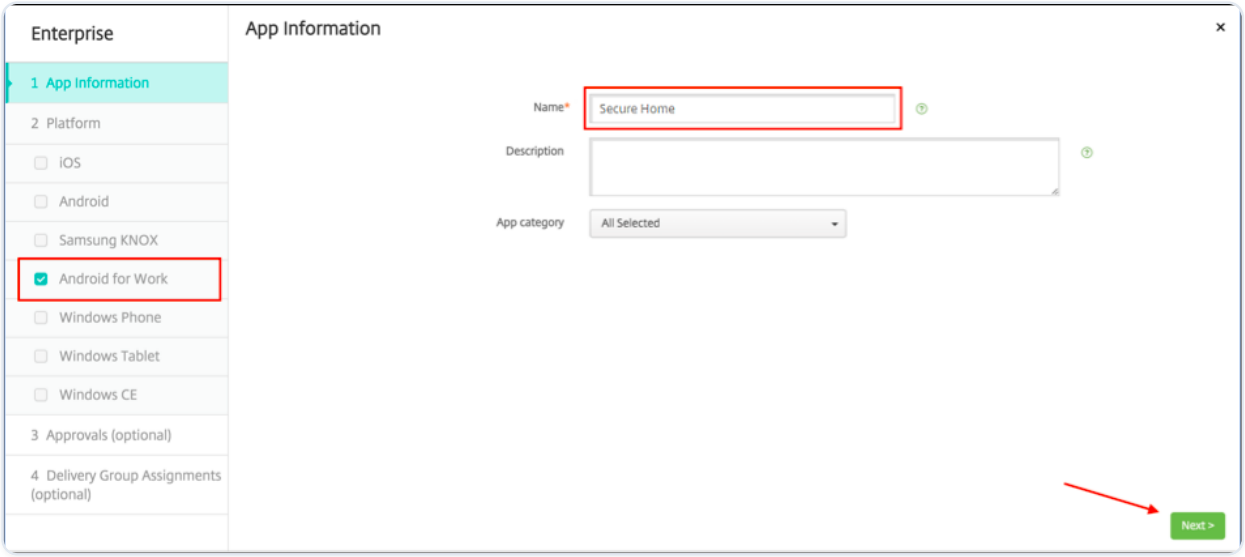
   A janela **Adicionar Aplicativos** é exibida.

2. Clique em **Empresarial**.

   A página **Informações do aplicativo** é exibida.

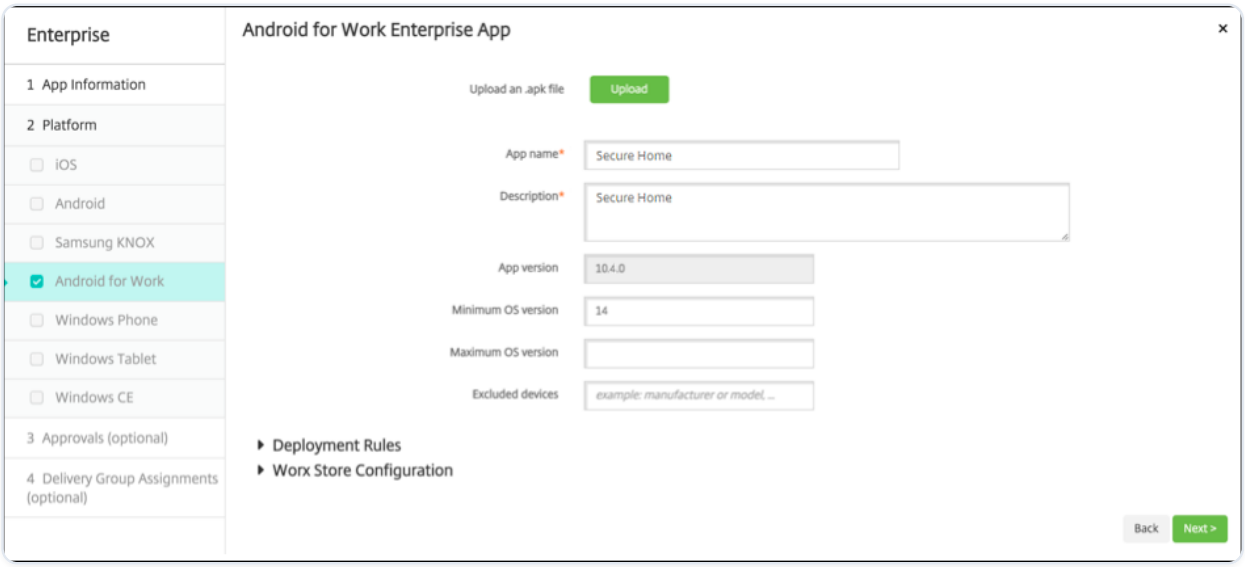
3. Selecione a seguinte configuração e clique em **Avançar**.

   A página **Aplicativo Empresarial do Android Enterprise** é exibida.



4. Forneça o caminho para o .apk e clique em **Avançar** para carregar o arquivo.

   Após a conclusão do upload, os detalhes do pacote carregado aparecem.



5. Clique em **Avançar** para abrir a página de download do arquivo JSON, que você usará para fazer upload para o Google Play. Para o Secure Hub, o upload para o Google Play não é necessário, mas você precisa do arquivo JSON para ler o valor SHA1 dele.

   Um arquivo JSON típico se parece com o seguinte:

6. Copie o **valor file_sha1_base64** e use-o no campo **Hash** na Ferramenta de Provisionamento.

   > **Nota:**
   >
   > O hash deve ser seguro para URL.

   - Converta quaisquer símbolos **+** em **-**
   - Converta quaisquer símbolos **/** em _
   - Substitua o **\\u003d** final por **=**

   Se você armazenar o hash no arquivo nfcprovisioning.txt no cartão SD do dispositivo, o aplicativo fará a conversão de segurança. No entanto, se você optar por digitar o hash manualmente, é sua responsabilidade garantir a segurança da URL.

BIBLIOTECAS USADAS

A Ferramenta de Provisionamento usa as seguintes bibliotecas em seu código-fonte:

- biblioteca v7 appcompat, biblioteca de suporte de design e biblioteca v7 Palette do Google sob licença Apache 2.0

  Para obter informações, consulte Guia de Recursos da Biblioteca de Suporte.

- Butter Knife de Jake Wharton sob licença Apache 2.0

Provisionar dispositivo de perfil de trabalho no Android Enterprise

Em dispositivos de perfil de trabalho no Android Enterprise, você separa com segurança as áreas corporativa e pessoal em um dispositivo. Por exemplo, dispositivos BYOD podem ser dispositivos de perfil de trabalho. A experiência de registro para dispositivos de perfil de trabalho é semelhante ao registro Android no XenMobile. Os usuários baixam o Secure Hub do Google Play e registram seus dispositivos.

Por padrão, as configurações de Depuração USB e Fontes Desconhecidas são desativadas em um dispositivo quando ele é registrado no Android Enterprise como um dispositivo de perfil de trabalho.

> **Dica:**
>
> Ao registrar dispositivos no Android Enterprise como dispositivos de perfil de trabalho, sempre vá ao Google Play. A partir daí, habilite o Secure Hub para aparecer no perfil pessoal do usuário.

Suporte a feedback de configurações gerenciadas (Pré-visualização Técnica)

> **Nota:**
>
> Os recursos em Pré-visualização Técnica estão disponíveis para uso em ambientes de não produção ou produção limitada, e para dar aos clientes a oportunidade de compartilhar feedback. A Citrix® não aceita casos de suporte para recursos em pré-visualização técnica, mas agradece o feedback para melhorá-los. Você pode fornecer feedback sobre este recurso clicando em **Envie-nos seu feedback**. A Citrix pode agir com base no feedback, dependendo de sua gravidade, criticidade e importância.

O recurso de feedback de configuração gerenciada permite que os administradores obtenham feedback sobre os estados de aplicativos de dispositivos Android que são configurados com políticas de configuração gerenciada. Este feedback pode ser usado para monitorar a eficácia e o status dessas políticas.

Pré-requisitos

1. `App Support`: O aplicativo deve suportar políticas de configuração gerenciada.
2. `Keyed App States`: O aplicativo também deve suportar estados de aplicativo com chave. Para obter informações detalhadas sobre como o feedback do aplicativo funciona, consulte Enviar feedback do aplicativo para EMMs.

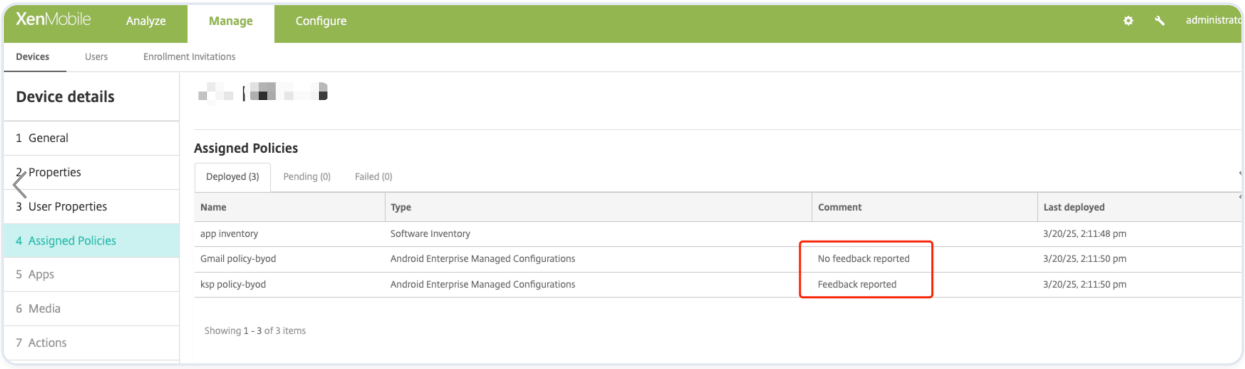
Procedimento para gerenciar e utilizar o feedback de configuração

1. Habilite a Propriedade do Servidor `afw.app_managed_configurations.feedback` para o XenMobile Server especificado.

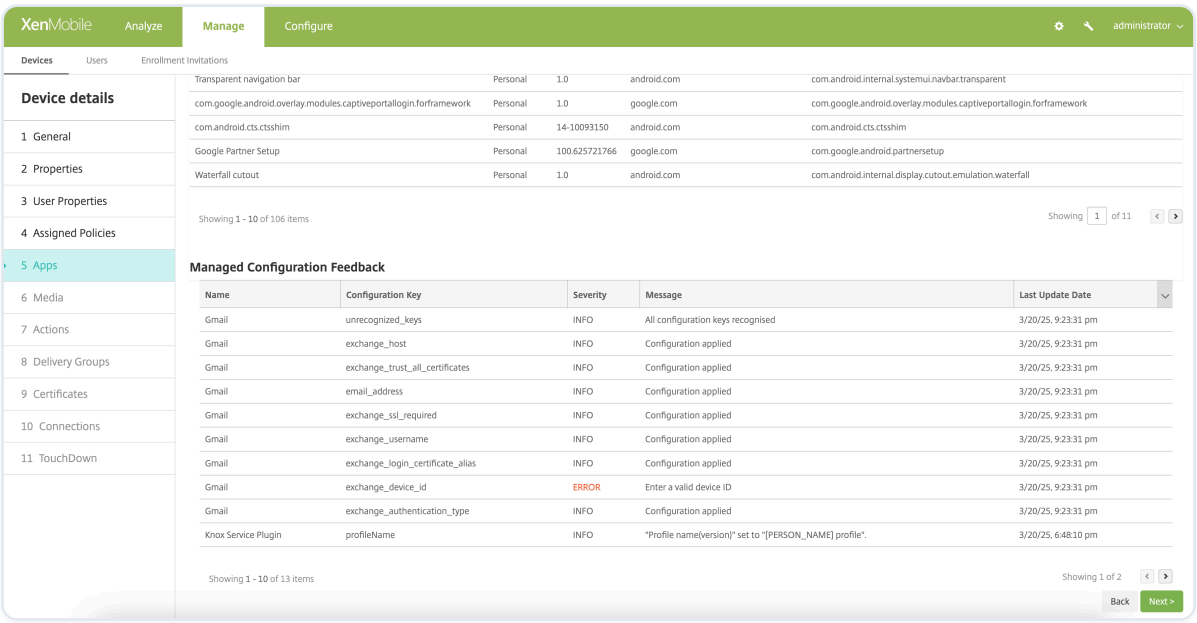
2. Verifique a política de configuração gerenciada.

   - Confirme se o dispositivo Android está registrado e se a política de configuração gerenciada foi aplicada com sucesso.
   - navegar até **Detalhes do dispositivo** e clique em **Políticas Atribuídas**. Os comentários relacionados à política de configuração gerenciada são exibidos.

     - **Feedback relatado**: Indica que o feedback está disponível para este aplicativo relacionado à política.
     - **Nenhum feedback relatado**: Indica que nenhum feedback foi relatado para este aplicativo relacionado à política.

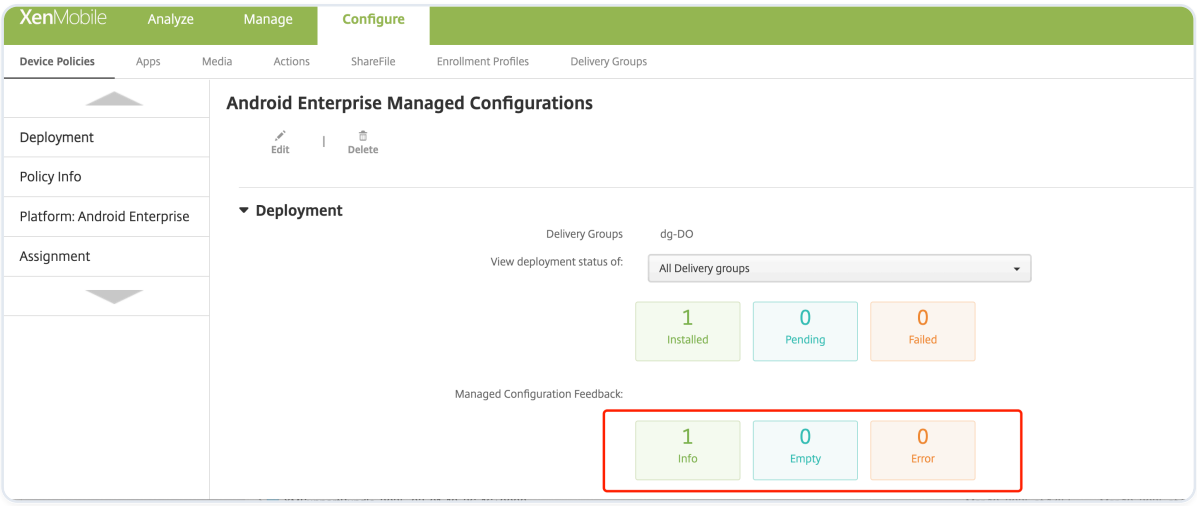


   - navegar para **Detalhes do dispositivo** e clique em **Aplicativos**. O feedback detalhado é exibido na tabela **Feedback de Configuração Gerenciada**, contendo todos os dados dos aplicativos.

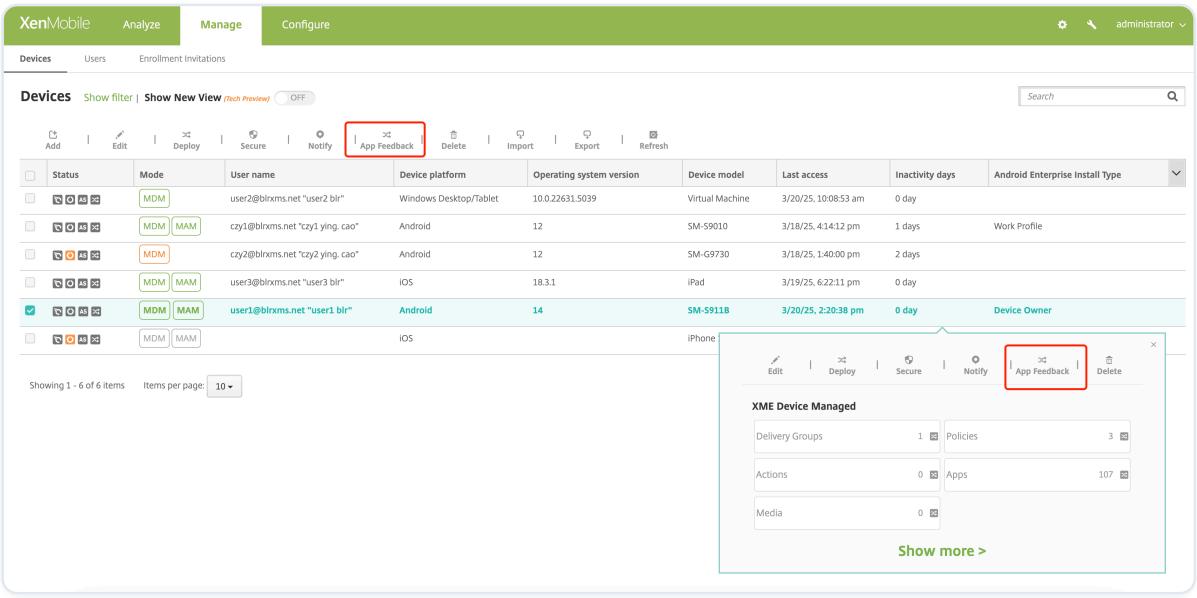


   - Para uma única política de configuração gerenciada, você pode verificar os detalhes do feedback para todos os dispositivos atribuídos:

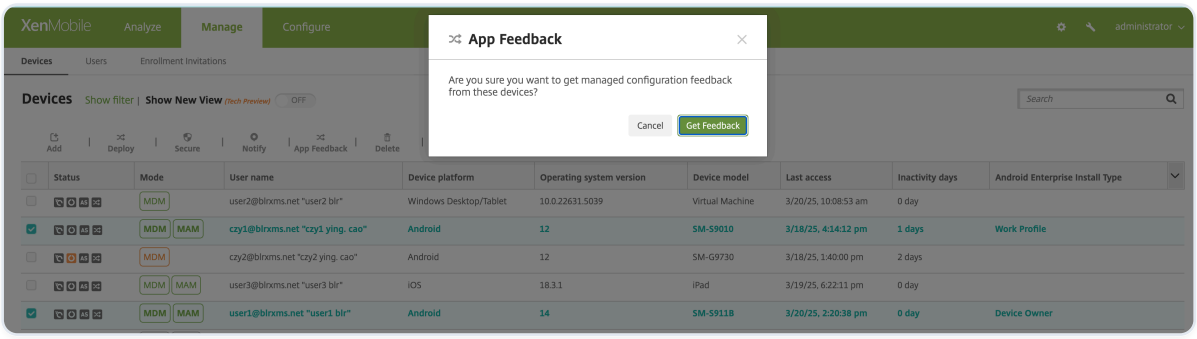
- **Informações**: Todos os dispositivos com dados de feedback relatados que não contêm erros.
- **Erro**: Todos os dispositivos com dados de feedback relatados que contêm erros.
- **Vazio**: Todos os dispositivos sem dados de feedback relatados.



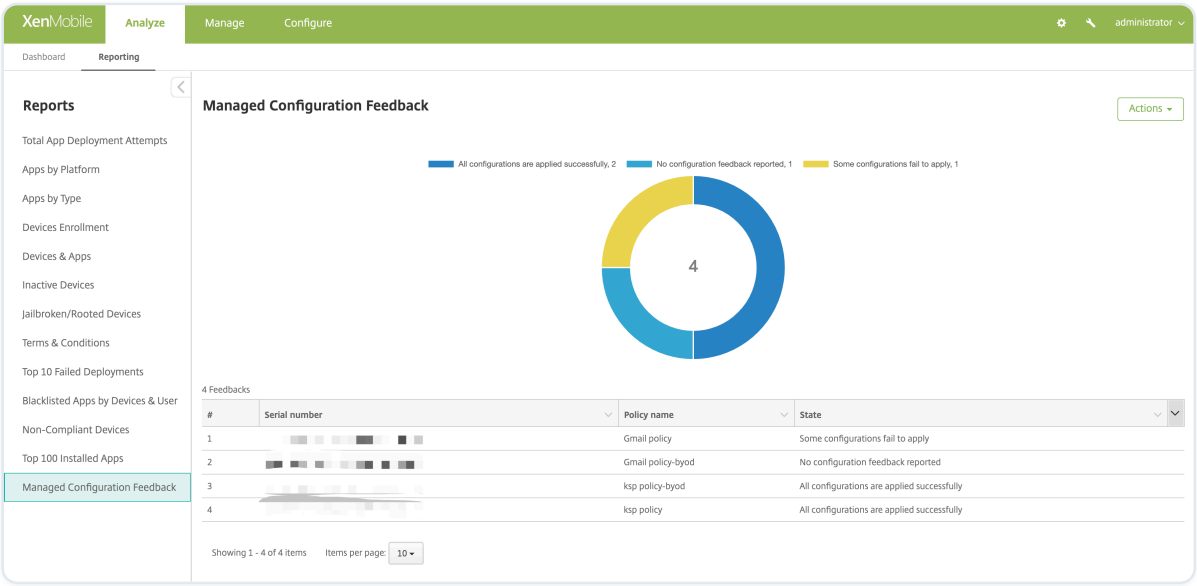
- Para obter o feedback manualmente, clique em **Gerenciar** e selecione a caixa de seleção para localizar os dispositivos correspondentes. Por exemplo, você pode selecionar as caixas de seleção correspondentes e clicar em **Feedback do aplicativo**.



- Clique em **Obter Feedback** para obter o feedback de configuração gerenciada dos dispositivos selecionados.



- No relatório de Feedback de Configuração Gerenciada, selecione **Analisar** e clique em **Relatórios** para obter um feedback geral. Você pode ver os relatórios de todos os dispositivos, gerenciar políticas de configuração e as falhas de configuração relacionadas.



3. Duas propriedades de servidor foram introduzidas para ajustar o agendamento do feedback. Modifique o valor no console usando as propriedades do servidor e controle quando os dados de feedback são salvos no banco de dados.

   a. Tamanho do Lote para Atualizar o Banco de Dados de Feedback de Configuração Gerenciada do Android Enterprise:

      - chave: `android.managed.configuration.feedback.db.update.batch.size`
      - Você pode definir o tamanho do lote de relatórios a serem armazenados no banco de dados; somente os dados armazenados no banco de dados poderão ser exibidos na interface do usuário. O valor padrão é 100 e o valor máximo é 1000.

   b. Intervalo de Tempo de Atualização do Banco de Dados de Feedback de Configuração Gerenciada do Android Enterprise:

      - chave: `android.managed.configuration.feedback.db.update.time.interval`

- Você pode especificar por quanto tempo os relatórios são armazenados no banco de dados, mesmo que o tamanho não atinja o limite do lote. O valor padrão é de seis horas.

Solução de problemas

Por padrão, os relatórios de feedback são recuperados durante cada check-in do dispositivo (quando o Secure Hub se conecta ao servidor). No entanto, você pode buscar manualmente o relatório para dispositivos específicos usando o botão Feedback do Aplicativo.

iOS

Para gerenciar dispositivos iOS no XenMobile Server, você configura um certificado do Apple Push Notification service (APNs) da Apple. Para obter informações, consulte Certificados APNs.

Os perfis de registro determinam se os dispositivos iOS se registram em MDM+MAM, com a opção de os usuários optarem por não usar o MDM. O XenMobile Server oferece suporte aos seguintes tipos de autenticação para dispositivos iOS em MDM+MAM. Para obter informações, consulte os artigos em Certificados e autenticação.

- Domínio
- Domínio mais token de segurança
- Certificado de cliente
- Certificado de cliente mais domínio

> **Requisitos para certificados confiáveis no iOS 13:**

> A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, `<https://support.apple.com/pt-br/HT210176>`. Para obter ajuda com o gerenciamento de certificados, consulte Carregando certificados no XenMobile Server.

> Para sistemas operacionais compatíveis, consulte Sistemas operacionais de dispositivos compatíveis.

Compatibilidade com iOS 14

O XenMobile® Server e os aplicativos móveis Citrix® são compatíveis com o iOS 14, mas atualmente não oferecem suporte aos novos recursos do iOS 14.

Para dispositivos iOS supervisionados, você pode atrasar as atualizações de software por até 90 dias. Na política de dispositivo Restrições para iOS, use estas configurações:

- **Forçar atualizações de software atrasadas**
- **Atraso forçado na atualização de software**

Consulte configurações do iOS. Essas configurações não estão disponíveis para dispositivos no modo de registro de usuário ou no modo não supervisionado (MDM completo).

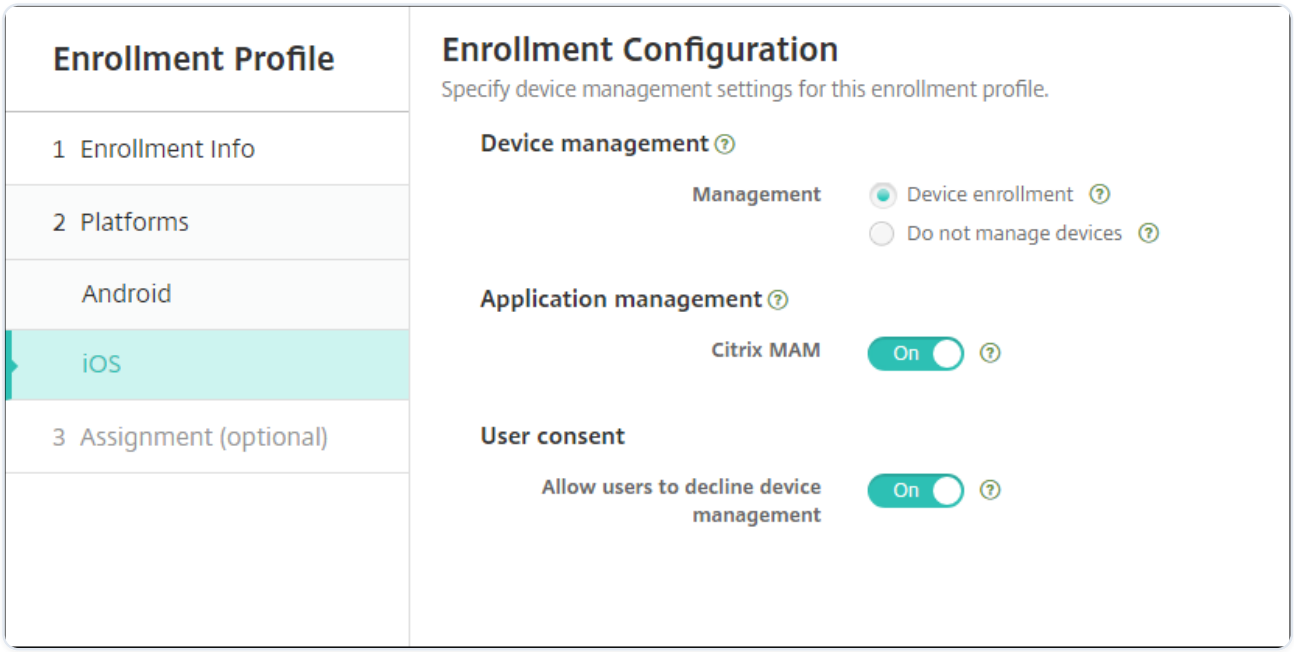
Nomes de host da Apple que devem permanecer abertos

Alguns nomes de host da Apple devem permanecer abertos para garantir o funcionamento adequado do iOS, macOS e da Apple App Store. O bloqueio desses nomes de host pode afetar a instalação, atualização e o funcionamento adequado do seguinte: iOS, aplicativos iOS, operação de MDM e registro de dispositivos e aplicativos. Para obter mais informações, consulte `<https://support.apple.com/pt-br/HT201999>`.

Métodos de registro suportados

Você especifica como gerenciar dispositivos iOS em perfis de registro. Você pode escolher o registro de dispositivo ou nenhum registro MDM.

Para configurar as definições de registro para dispositivos iOS, vá para **Configurar > Perfis de Registro > iOS**.



A tabela a seguir lista quais métodos de registro o XenMobile Server suporta para dispositivos iOS:

MÉTODO	SUPORTADO
Programa de Implantação da Apple	Sim
Apple School Manager	Sim
Apple Configurator	Sim
Registro manual	Sim
Convites de registro	Sim

A Apple tem programas de registro de dispositivos para contas empresariais e educacionais. Para contas empresariais, você se registra no Apple Deployment Program para usar o Apple Deployment Program para registro e gerenciamento de dispositivos no XenMobile Server. Esse programa é para dispositivos iOS e macOS. Consulte Implantar dispositivos através do Apple Deployment Program.

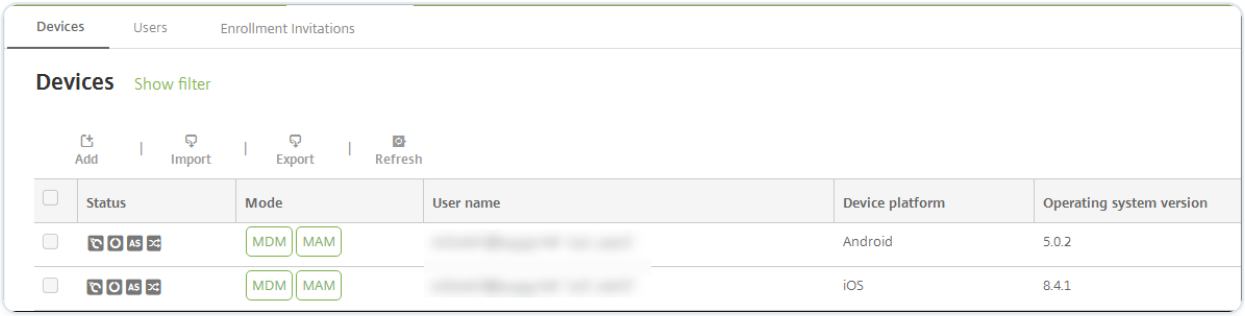
Para contas educacionais, você cria uma conta do Apple School Manager. O Apple School Manager unifica o Programa de Implantação e a compra em volume. O Apple School Manager é um tipo de Programa de Implantação Apple para Educação. Consulte Integrar com recursos do Apple Education.

Você pode usar o Apple Deployment Program para registrar em massa dispositivos iOS e macOS. Você pode comprar esses dispositivos diretamente da Apple, de um Revendedor Autorizado Apple participante ou de uma operadora. Se você comprar dispositivos iOS diretamente da Apple, poderá usar o Apple Configurator para registrar esses dispositivos. Consulte Registro em massa de dispositivos Apple.

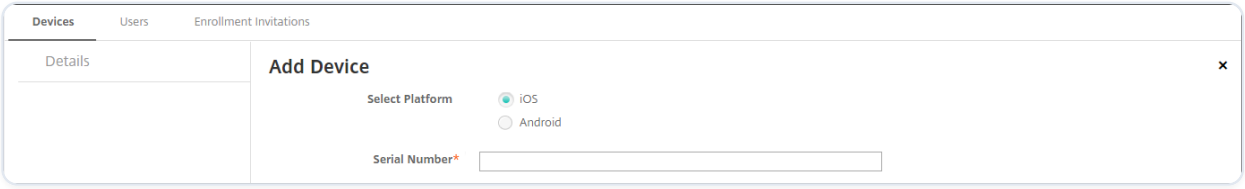
Adicionar um dispositivo iOS manualmente

Se você quiser adicionar um dispositivo iOS manualmente, por exemplo, para fins de teste, siga estas etapas.

1. No console do XenMobile Server, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



2. Clique em **Adicionar**. A página **Adicionar Dispositivo** é exibida.



3. Configure estas configurações:

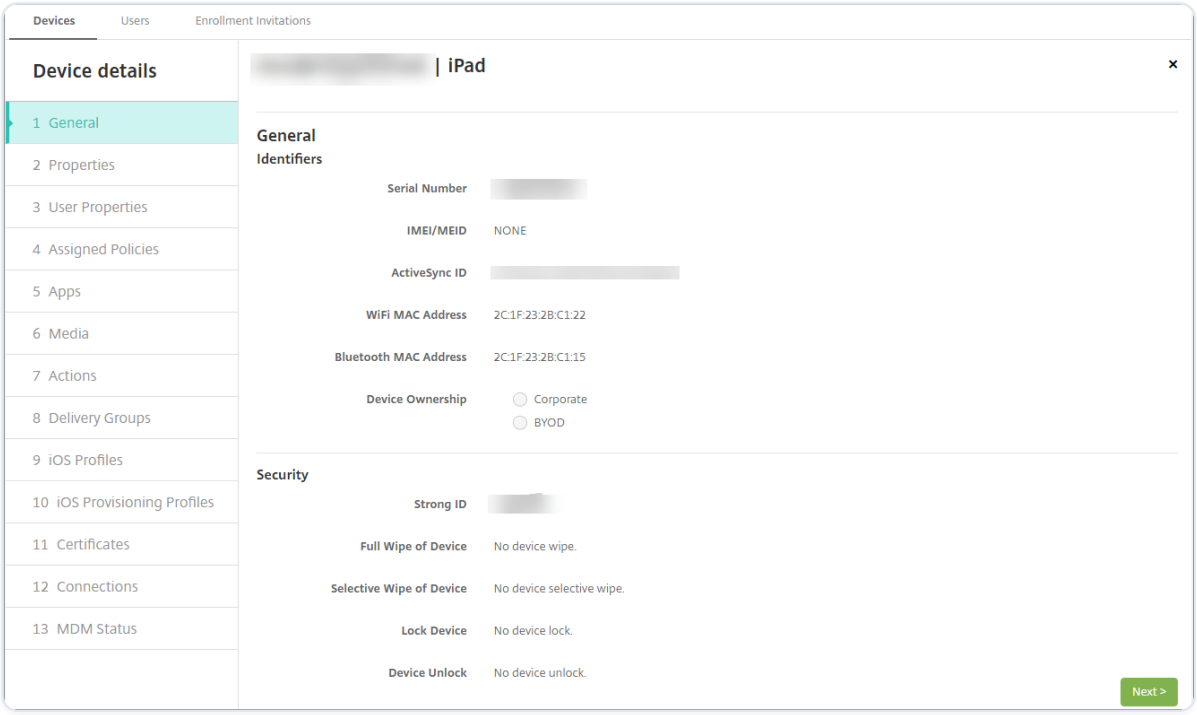
   - **Selecionar plataforma:** Clique em **iOS**.
   - **Número de Série:** Digite o número de série do dispositivo.

4. Clique em **Adicionar**. A tabela **Dispositivos** é exibida com o dispositivo adicionado na parte inferior da lista. Para visualizar e confirmar os detalhes do dispositivo: Escolha o dispositivo que você adicionou e, no menu que aparece, clique em **Editar**.

> **Observação:**

> Quando você seleciona a caixa de seleção ao lado de um dispositivo, o menu de opções aparece acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de opções aparece no lado direito da listagem.

- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
  - Um ou mais grupos locais.
  - Usuários locais atribuídos a grupos locais.
  - Grupos de entrega estão associados a grupos locais.
- Se estiver usando o Active Directory:
  - Grupos de entrega estão associados a grupos do Active Directory.



5. A página **Geral** lista os **Identificadores** do dispositivo, como o número de série e outras informações para o tipo de plataforma. Para **Propriedade do Dispositivo**, selecione **Corporativo** ou **BYOD**.

   A página **Geral** também lista as propriedades de **Segurança** do dispositivo, como ID Forte, Bloquear Dispositivo, Ignorar Bloqueio de Ativação e outras informações para o tipo de plataforma. O campo **Limpeza Completa do Dispositivo** inclui o código PIN do usuário. O usuário deve inserir esse código após a limpeza do dispositivo. Se o usuário esquecer o código, você pode consultá-lo aqui.

6. A página **Propriedades** lista as propriedades do dispositivo que o XenMobile Server deve provisionar. Esta lista mostra todas as propriedades do dispositivo incluídas no arquivo de provisionamento usado para adicionar o dispositivo. Para adicionar uma propriedade, clique em **Adicionar** e selecione uma propriedade da lista. Para valores válidos para cada propriedade, consulte o PDF Nomes e valores das propriedades do dispositivo.

   Quando você adiciona uma propriedade, ela aparece inicialmente na categoria onde você a adicionou. Depois de clicar em **Avançar** e retornar à página **Propriedades**, a propriedade aparece na lista apropriada.

   Para excluir uma propriedade, passe o mouse sobre o item e clique no **X** no lado direito. O XenMobile Server exclui o item imediatamente.

7. As seções restantes de **Detalhes do Dispositivo** contêm informações de resumo para o dispositivo.

   - **Propriedades do Usuário:** Exibe funções RBAC, associações de grupo, contas de compra por volume e propriedades para o usuário. Você pode desativar uma conta de compra por volume a partir desta página.
   - **Políticas Atribuídas:** Exibe o número de políticas atribuídas, incluindo o número de políticas implantadas, pendentes e com falha. Fornece o nome da política, tipo e informações da última implantação para cada política.
   - **Aplicativos:** Exibe, para o último inventário, o número de implantações de aplicativos instaladas, pendentes e com falha. Fornece o nome do aplicativo, identificador, tipo e outras informações. Para uma descrição das chaves de inventário do iOS e macOS, como **HasUpdateAvailable**, consulte Protocolo de Gerenciamento de Dispositivos Móveis (MDM).
   - **Mídia:** Exibe, para o último inventário, o número de implantações de mídia implantadas, pendentes e com falha.
   - **Ações:** Exibe o número de ações implantadas, pendentes e com falha. Fornece o nome da ação e a hora da última implantação.
   - **Grupos de Entrega:** Exibe o número de grupos de entrega bem-sucedidos, pendentes e com falha. Para cada implantação, fornece o nome do grupo de entrega e a hora da implantação. Selecione um grupo de entrega para visualizar informações mais detalhadas, incluindo status, ação e canal ou usuário.
   - **Perfis iOS:** Exibe o último inventário de perfis iOS, incluindo nome, tipo, organização e descrição.

- **Perfis de Provisionamento iOS:** Exibe informações de perfil de provisionamento de distribuição empresarial, como UUID, data de expiração e status gerenciado.
- **Certificados:** Exibe, para certificados válidos, expirados ou revogados, informações como tipo, provedor, emissor, número de série e o número de dias restantes antes da expiração.
- **Conexões:** Exibe o status da primeira conexão e o status da última conexão. Fornece para cada conexão, o nome de usuário, a hora da penúltima (próxima à última) autenticação e a hora da última autenticação.
- **Status MDM:** Exibe informações como o status MDM, a hora do último push e a hora da última resposta do dispositivo.

Configurar políticas de dispositivo iOS

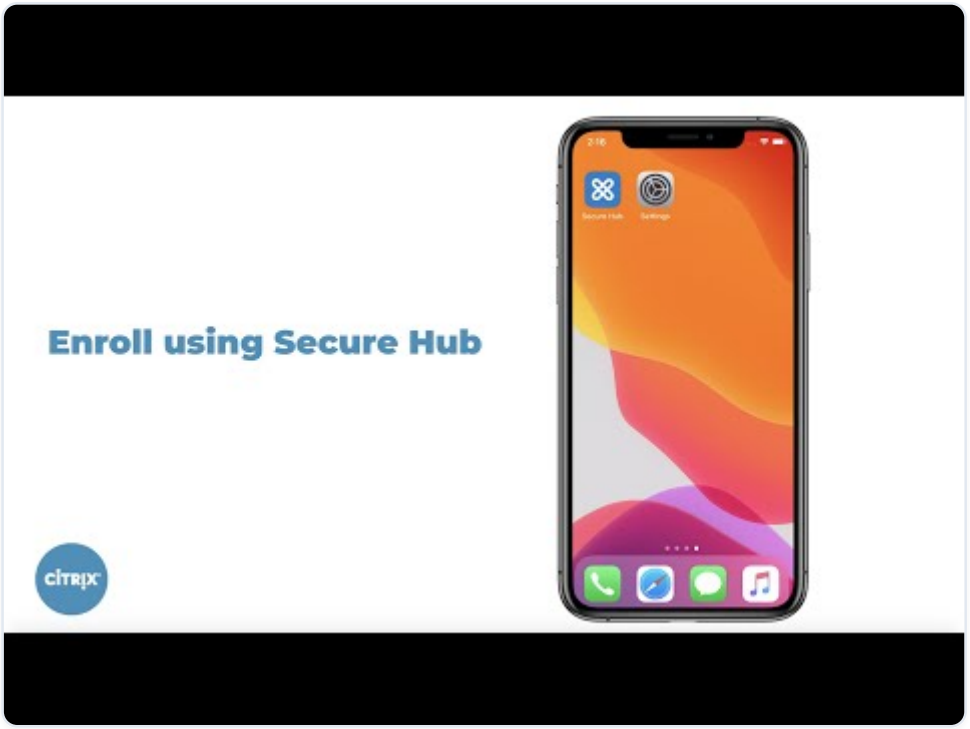
Use estas políticas para configurar como o XenMobile Server interage com dispositivos que executam iOS. Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos iOS.

Espelhamento AirPlay	AirPrint	APN
Acesso a Aplicativos	Atributos de Aplicativos	Configuração de Aplicativos
Inventário de Aplicativos	Bloqueio de Aplicativos	Uso de Rede de Aplicativos
Desinstalação de Aplicativos	Notificações de Aplicativos	Calendário (CalDAV)
Celular	Contatos (CardDAV)	Controle de Atualização do SO
Credenciais	Nome do Dispositivo	Configuração de Educação
Exchange	Fonte	Layout da Tela Inicial
Importar Perfil iOS e macOS	LDAP	Localização
E-mail	Domínios Gerenciados	Opções de MDM
Informações da Organização	Código de Acesso	Ponto de Acesso Pessoal
Remoção de Perfil	Perfil de Provisionamento	Remoção de Perfil de Provisionamento
Proxy	Restrições	Roaming

SCEP	iPad Compartilhado - Número Máximo de Usuários Residentes	iPad Compartilhado - Período de Carência do Bloqueio por Código de Acesso
Conta SSO	Loja	Calendários Assinados
Termos e Condições	VPN	Papel de Parede
Filtro de Conteúdo Web	Webclip	Wi-Fi

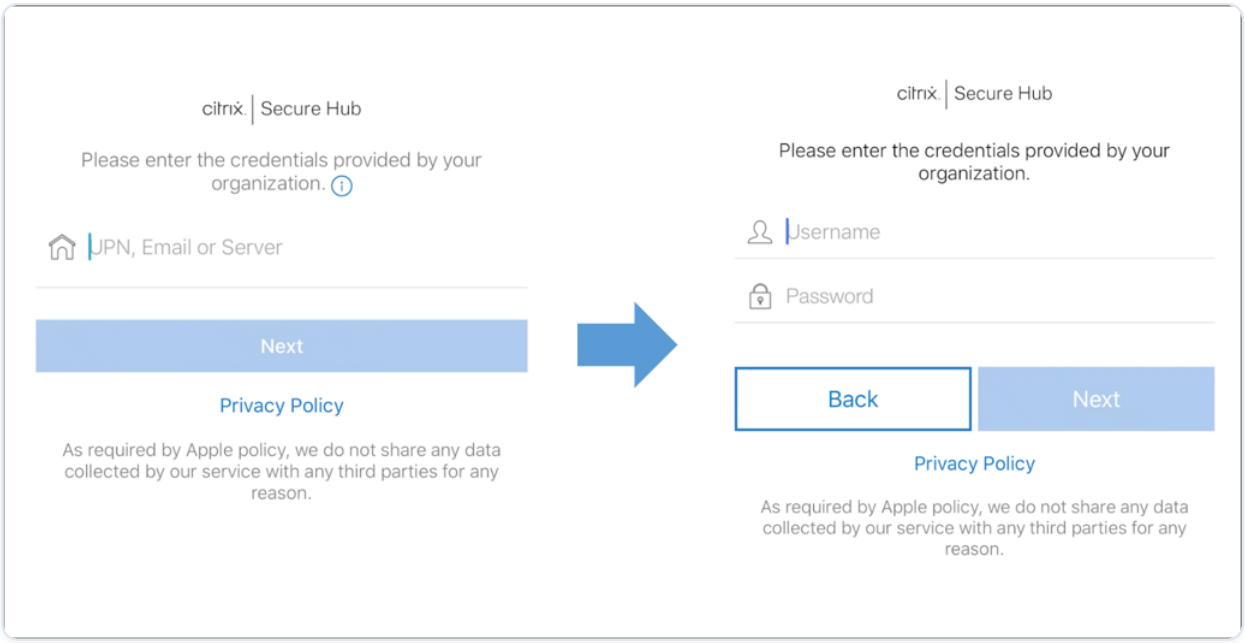
Registrar dispositivos iOS

Esta seção mostra como os usuários registram dispositivos iOS (12.2 ou posterior) no XenMobile Server. Para obter mais informações sobre o registro de iOS, abra o seguinte vídeo:

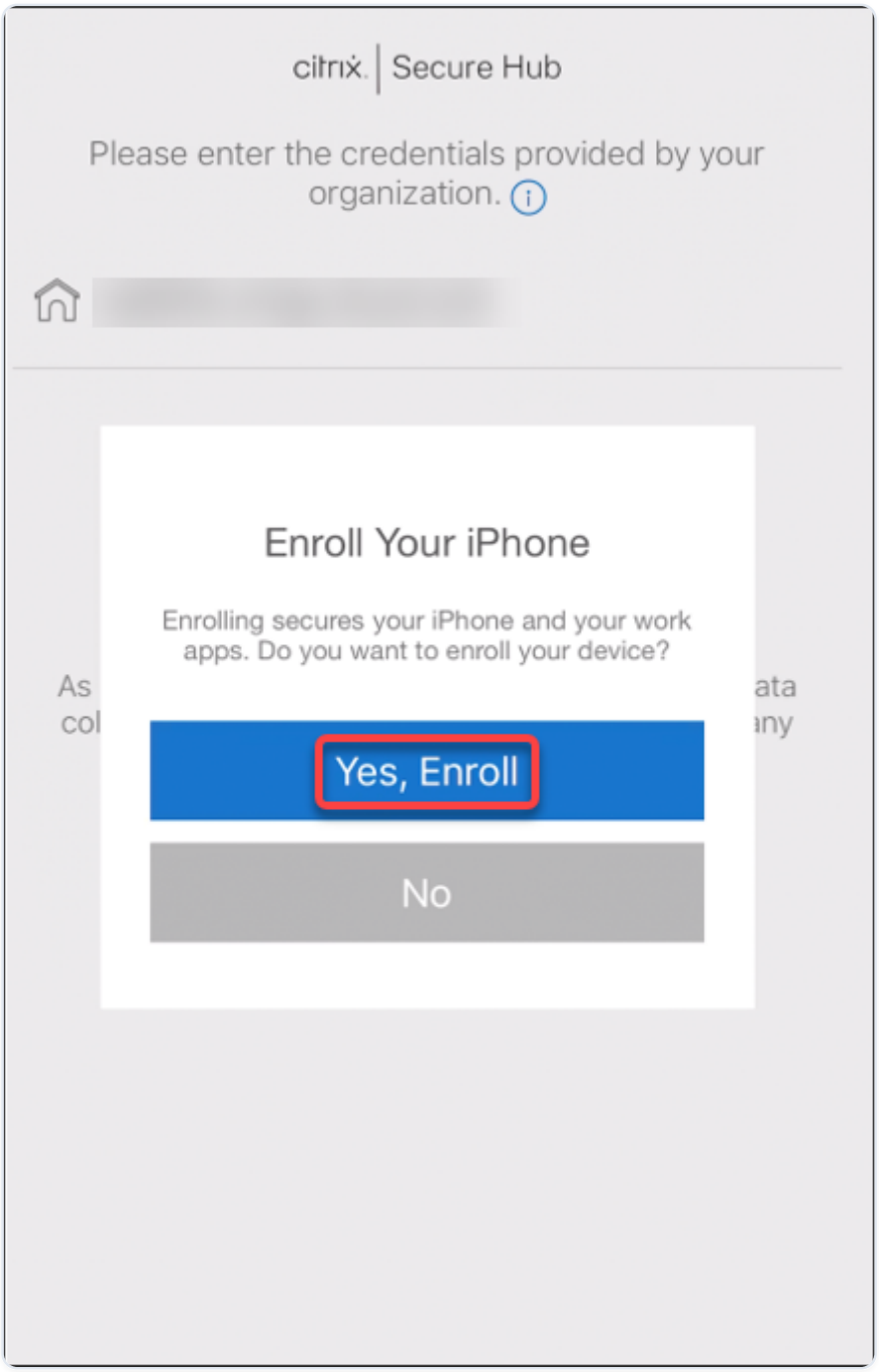


1. Vá para a App Store no seu dispositivo iOS, baixe o aplicativo Citrix Secure Hub™ e, em seguida, toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, toque em **Avançar** e, em seguida, toque em **Instalar**.
3. Após a instalação do Secure Hub, toque em **Abrir**.

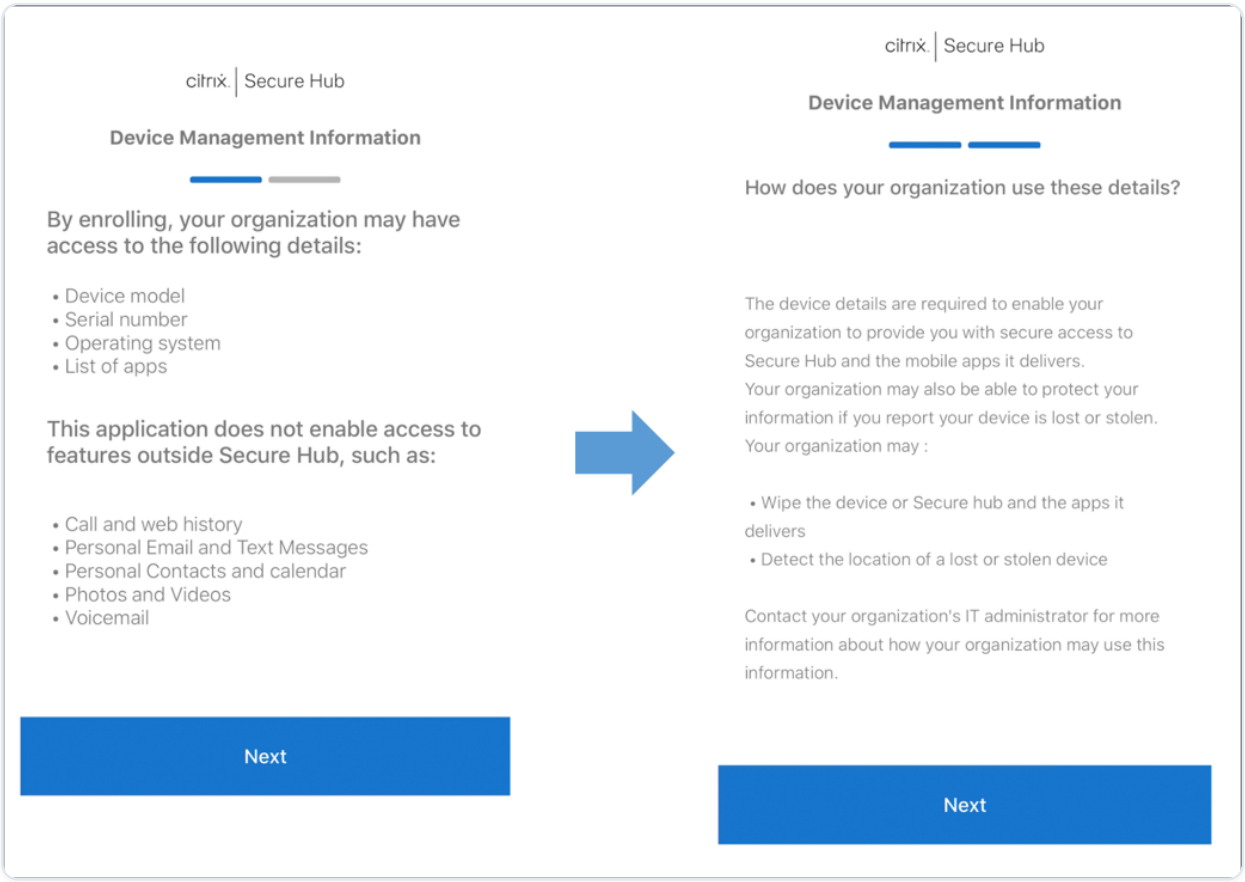
4. Insira suas credenciais corporativas, como o nome do servidor XenMobile Server, Nome Principal de Usuário (UPN) ou endereço de e-mail. Em seguida, clique em **Avançar**.



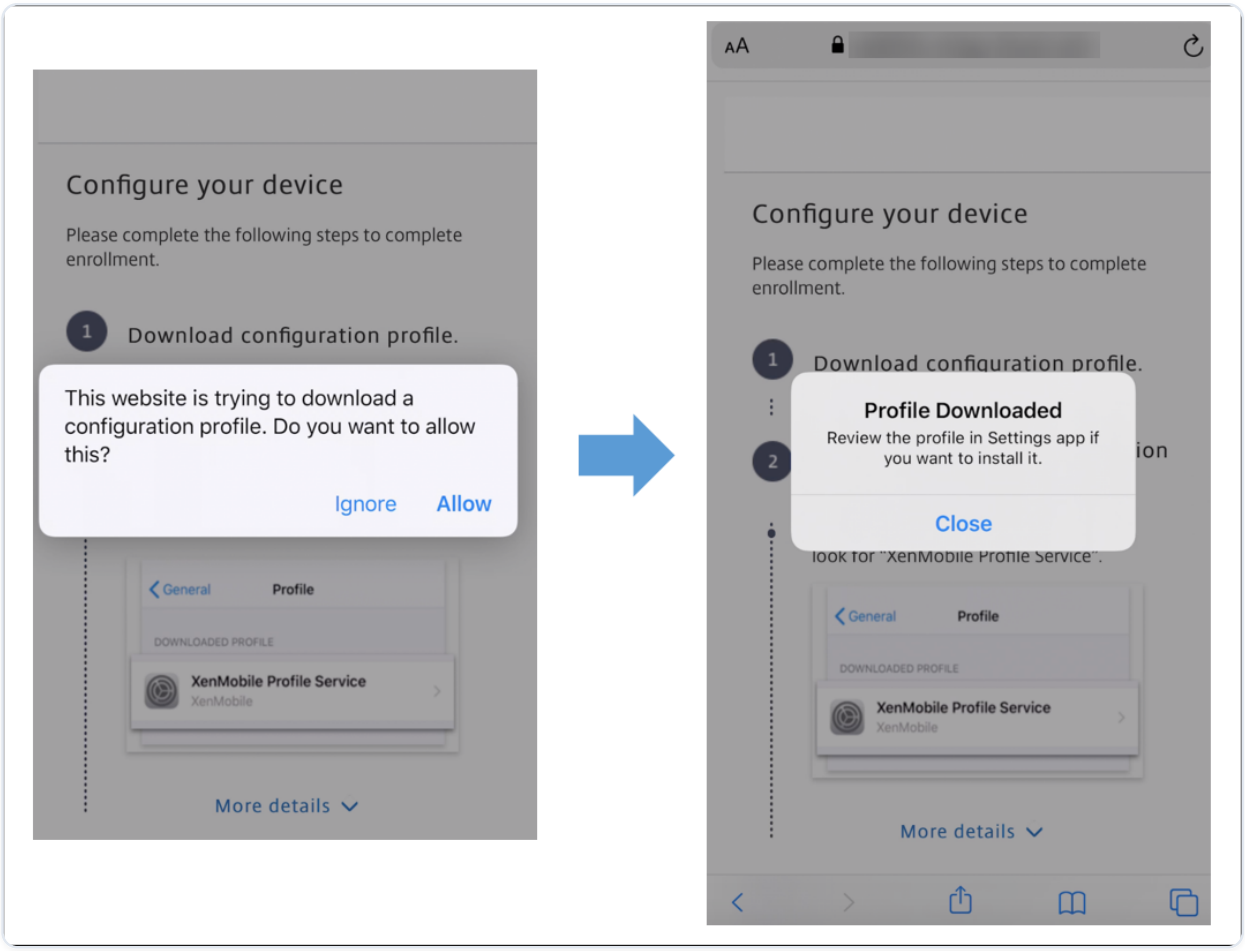
5. Toque em **Sim, Registrar** para registrar seu dispositivo iOS.



6. Uma lista dos dados que o XenMobile Server coleta é exibida. Clique em **Avançar**. Uma explicação de como uma organização usa esses dados é exibida. Clique em **Avançar**.



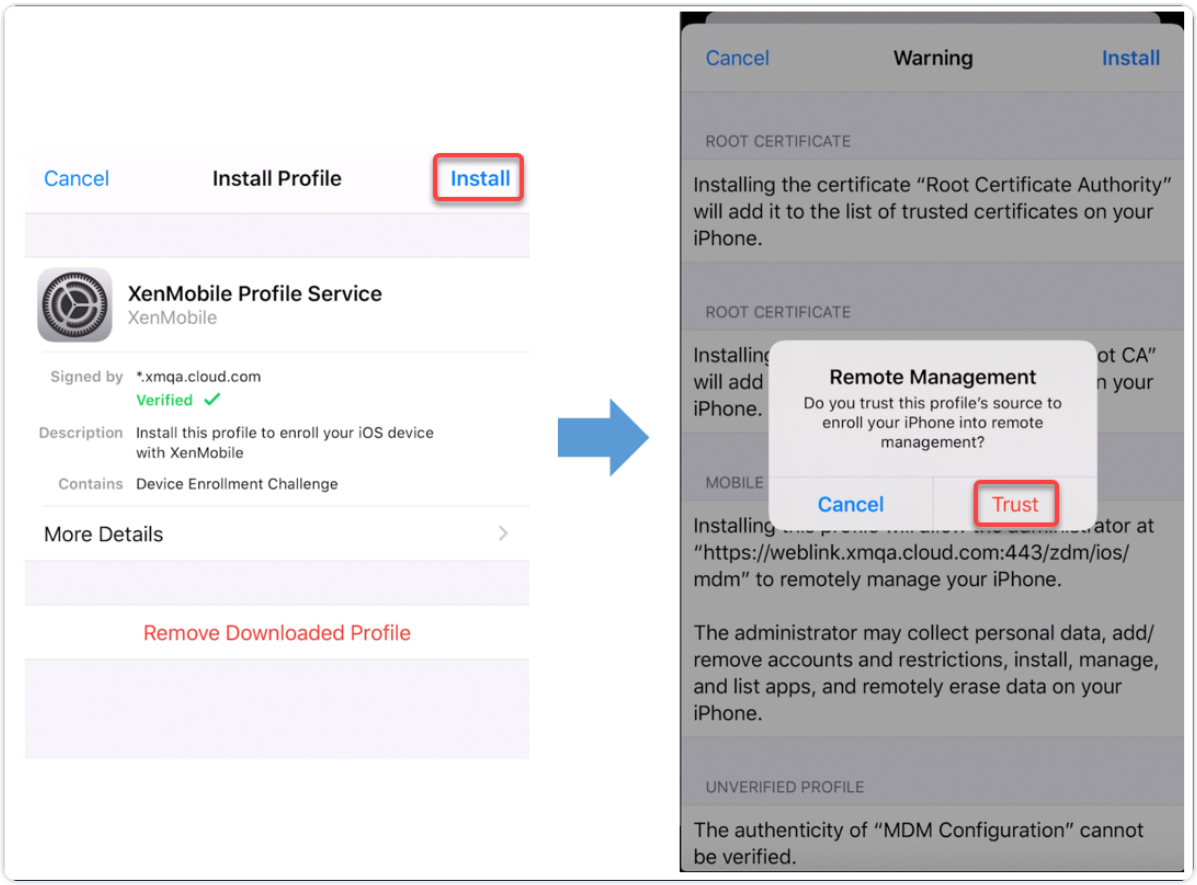
7. Depois de digitar suas credenciais, toque em **Permitir** quando solicitado, para baixar o perfil de configuração. Após baixar o perfil de configuração, toque em **Fechar**.



8. Nas configurações do seu dispositivo, instale o certificado iOS e adicione o dispositivo à lista de confiança.

    - Vá para **Ajustes > Geral > Perfil > Serviço de Perfil XenMobile** e toque em **Instalar** para adicionar o perfil.

- Na janela de notificação, toque em **Confiar** para registrar seu dispositivo no gerenciamento remoto.



9. Assim que o registro for bem-sucedido, abra o Secure Hub. Se você estiver se registrando no MDM+MAM: Após a validação de suas credenciais, crie e confirme seu PIN Citrix quando solicitado.
10. Após a conclusão do fluxo de trabalho, o dispositivo é registrado. Você pode então acessar a loja de aplicativos para visualizar os aplicativos que pode instalar em seu dispositivo iOS.

Ações de segurança

O iOS oferece suporte às seguintes ações de segurança. Para uma descrição de cada ação de segurança, consulte Ações de segurança.

Bypass de Bloqueio de Ativação	Bloqueio de App	Limpeza de App
Bloqueio de Ativação ASM	Renovação de Certificado	Limpar Restrições
Ativar/Desativar Modo Perdido	Ativar/Desativar Rastreamento	Limpeza Completa

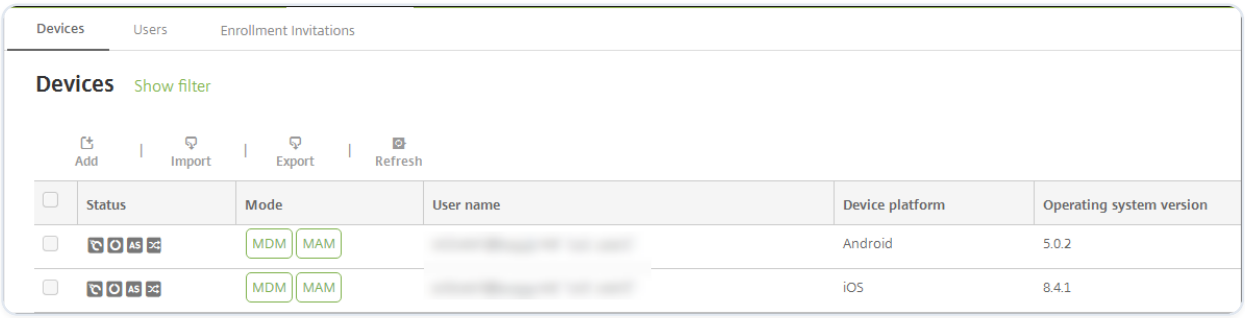
Localizar	Bloquear	Tocar
Solicitar/Parar Espelhamento AirPlay	Reiniciar/Desligar	Revogar/Autorizar
Limpeza Seletiva	Desbloquear	

Bloquear dispositivos iOS

Você pode bloquear um dispositivo iOS perdido com uma mensagem e um número de telefone que são exibidos na tela de bloqueio do dispositivo.

Para exibir uma mensagem e um número de telefone em um dispositivo bloqueado, defina a política Código de acesso como **true** no console do XenMobile Server. Alternativamente, os usuários podem habilitar o código de acesso no dispositivo manualmente.

1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



2. Selecione o dispositivo iOS que você deseja bloquear.

   Selecione a caixa de seleção ao lado de um dispositivo para exibir o menu de opções acima da lista de dispositivos. Clique em qualquer outro lugar na lista para exibir o menu de opções no lado direito da listagem.

   O menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

   O menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. No menu de opções, clique em **Proteger**. A caixa de diálogo **Ações de Segurança** é exibida.

   A caixa de diálogo Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de Segurança** é exibida.

A confirmação das Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. Opcionalmente, digite uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo.

   O iOS anexa as palavras “iPad Perdido” ao que você digita no campo **Mensagem**.

   Se você deixar o campo **Mensagem** vazio e fornecer um número de telefone, a Apple exibe a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

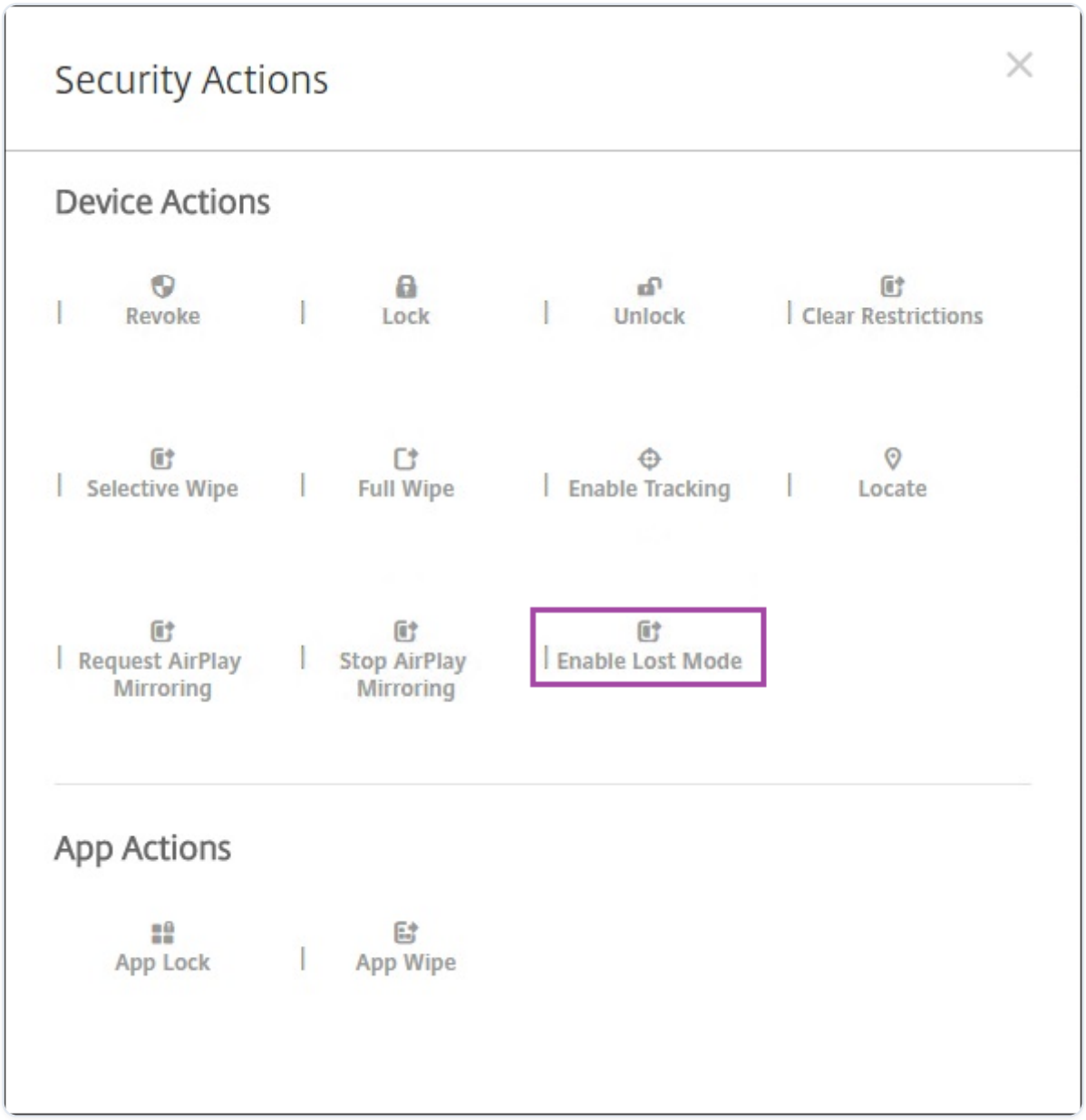
6. Clique em **Bloquear Dispositivo**.

Colocar dispositivos iOS no Modo Perdido

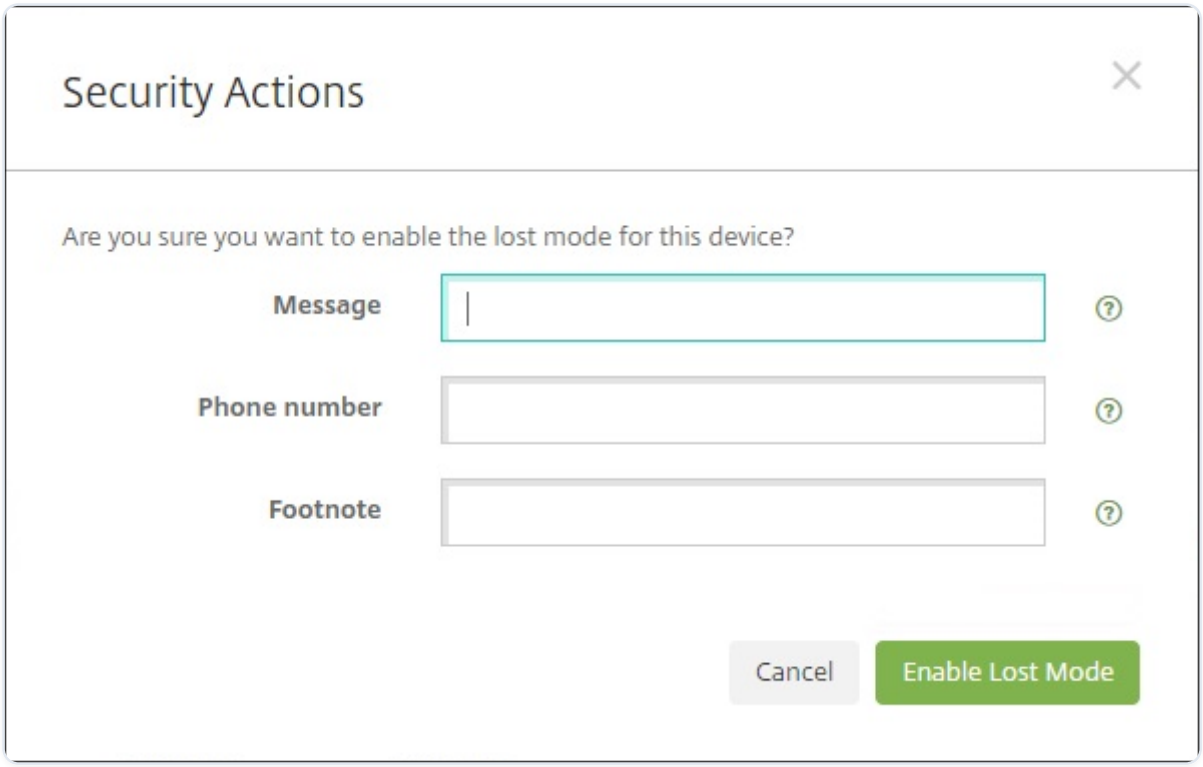
A propriedade de dispositivo Modo Perdido do XenMobile Server coloca um dispositivo iOS no Modo Perdido. Ao contrário do Modo Perdido Gerenciado pela Apple, o Modo Perdido do XenMobile Server não exige que um usuário realize nenhuma das seguintes ações para permitir a localização de seu dispositivo: Configurar a definição **Buscar Meu iPhone/iPad** ou habilitar os Serviços de Localização para o Citrix Secure Hub.

No Modo Perdido do XenMobile Server, somente o XenMobile Server pode desbloquear o dispositivo. (Em contraste, se você usar o recurso de bloqueio de dispositivo do XenMobile Server, os usuários podem desbloquear o dispositivo diretamente usando um código PIN que você fornece.

Para habilitar ou desabilitar o modo perdido: Vá para **Gerenciar > Dispositivos**, escolha um dispositivo iOS supervisionado e então clique em **Proteger**. Em seguida, clique em **Habilitar Modo Perdido** ou **Desabilitar Modo Perdido**.

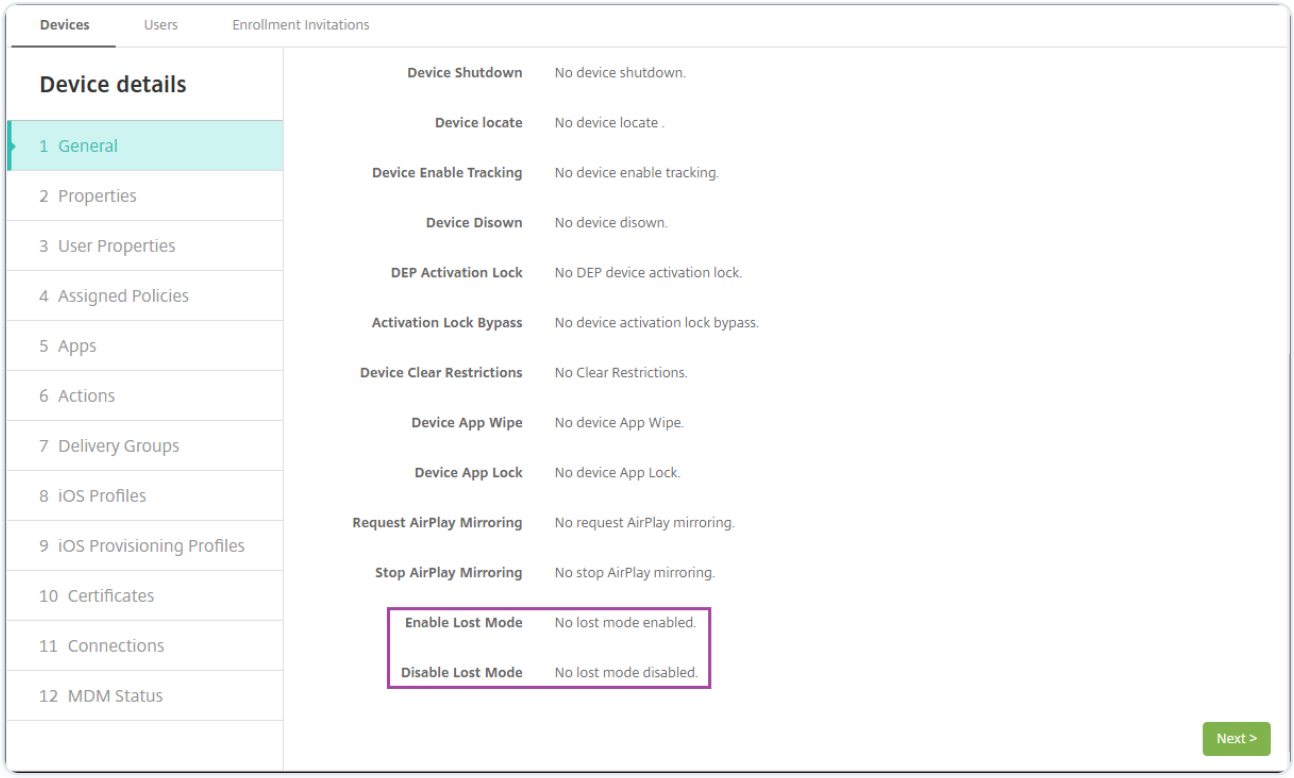


Se você clicar em **Habilitar Modo Perdido**, digite as informações para aparecer no dispositivo quando ele estiver no modo perdido.

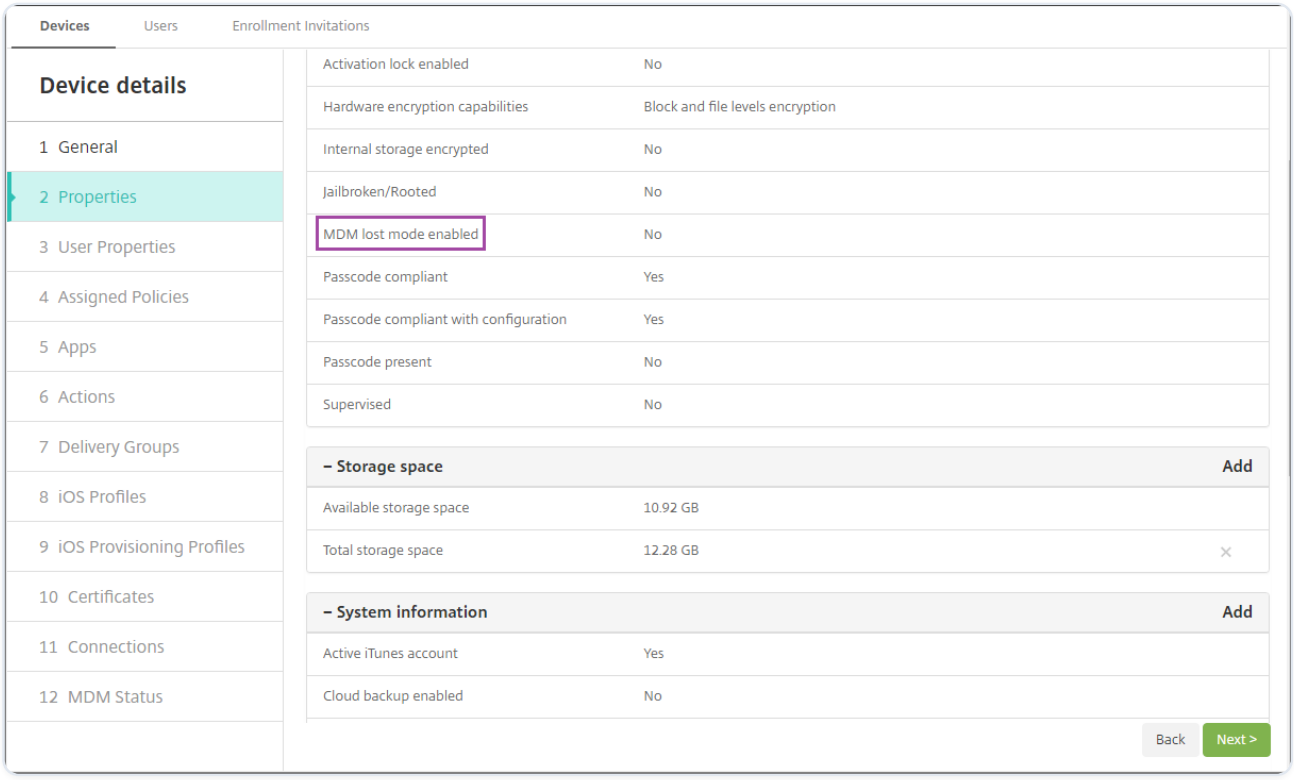


Use qualquer um dos seguintes métodos para verificar o status do Modo Perdido:

- Na janela **Ações de Segurança**, verifique se o botão está definido como **Desabilitar Modo Perdido**.
- Em **Gerenciar > Dispositivos**, na guia **Geral** em **Segurança**, veja a última ação de Habilitar Modo Perdido ou Desabilitar Modo Perdido.



- Em **Gerenciar > Dispositivos**, na guia **Propriedades**, verifique se o valor da configuração **Modo perdido MDM habilitado** está correto.



Se você habilitar o Modo Perdido do XenMobile Server em um dispositivo iOS, o console do XenMobile Server também muda da seguinte forma:

- Em **Configurar > Ações**, a lista de **Ações** não inclui estas ações automatizadas: **Revogar o dispositivo**, **Limpar seletivamente o dispositivo** e **Limpar completamente o dispositivo**.
- Em **Gerenciar > Dispositivos**, a lista de **Ações de Segurança** não inclui mais as ações de dispositivo **Revogar** e **Limpeza Seletiva**. Você ainda pode usar uma ação de segurança para realizar uma ação de **Limpeza Completa**, conforme necessário.

O iOS anexa as palavras "iPad Perdido" ao que você digita na **Mensagem** na tela **Ações de Segurança**.

Se você deixar a **Mensagem** vazia e fornecer um número de telefone, a Apple exibe a mensagem "Ligar para o proprietário" na tela de bloqueio do dispositivo.

Ignorar um bloqueio de ativação do iOS

O Bloqueio de Ativação é um recurso do Buscar Meu iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação exige o ID Apple e a senha do usuário antes que qualquer pessoa possa realizar estas ações: Desativar o Buscar Meu iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos que sua

organização possui, ignorar um Bloqueio de Ativação é necessário para, por exemplo, redefinir ou realocar dispositivos.

Para habilitar o Bloqueio de Ativação, você configura e implanta a política de dispositivo Opções de MDM do XenMobile Server. Você pode então gerenciar um dispositivo a partir do console do XenMobile Server sem as credenciais Apple do usuário. Para ignorar o requisito de credencial Apple de um Bloqueio de Ativação, emita a ação de segurança Ignorar Bloqueio de Ativação a partir do console do XenMobile Server.

Por exemplo, se o usuário devolver um telefone perdido ou para configurar o dispositivo antes ou depois de uma Limpeza Completa: Quando o telefone solicitar a credencial da conta da App Store da Apple, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação a partir do console do XenMobile Server.

Requisitos do dispositivo para ignorar o bloqueio de ativação

- Supervisionado via Apple Configurator ou Apple Deployment Program
- Configurado com uma conta iCloud
- Buscar Meu iPhone/iPad ativado
- Registrado no XenMobile Server
- Política de dispositivo Opções de MDM, com bloqueio de ativação habilitado, implantada nos dispositivos

Para ignorar um bloqueio de ativação antes de emitir uma Limpeza Completa de um dispositivo:

1. Vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Proteger** e, em seguida, clique em **Ignorar Bloqueio de Ativação**.
2. Apague o dispositivo. A tela de bloqueio de ativação não aparece durante a configuração do dispositivo.

Para ignorar um bloqueio de ativação após emitir uma Limpeza Completa de um dispositivo:

1. Redefina ou apague o dispositivo. A tela de bloqueio de ativação aparece durante a configuração do dispositivo.
2. Vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Proteger** e, em seguida, clique em **Ignorar Bloqueio de Ativação**.
3. Toque no botão Voltar no dispositivo. A tela inicial aparece.

Tenha em mente o seguinte:

- Aconselhe seus usuários a não desativar o Buscar Meu iPhone/iPad. Não faça uma limpeza completa a partir do dispositivo. Em qualquer um desses casos, o usuário é solicitado a inserir a senha da conta do iCloud. Após a validação da conta, o usuário não verá uma tela Ativar iPhone/iPad após apagar todo o conteúdo e configurações.
- Para um dispositivo com um código de desvio de Bloqueio de Ativação gerado e com o Bloqueio de Ativação ativado: Se você não conseguir ignorar a página Ativar iPhone/iPad após uma Limpeza Completa, não há necessidade de excluir o dispositivo do XenMobile Server. Você ou o usuário podem entrar em contato com o suporte da Apple para desbloquear o dispositivo diretamente.
- Durante um inventário de hardware, o XenMobile Server consulta um dispositivo para obter um código de desvio de Bloqueio de Ativação. Se um código de desvio estiver disponível, o dispositivo o envia para o XenMobile Server. Em seguida, para remover o código de desvio do dispositivo, envie a ação de segurança Desvio de Bloqueio de Ativação do console do XenMobile Server. Nesse ponto, o XenMobile Server e a Apple têm o código de desvio necessário para desbloquear o dispositivo.
- A ação de segurança Desvio de Bloqueio de Ativação depende da disponibilidade de um serviço da Apple. Se a ação não funcionar, você pode desbloquear um dispositivo da seguinte forma. No dispositivo, insira manualmente as credenciais da conta do iCloud. Ou, deixe o campo de nome de usuário vazio e digite o código de desvio no campo de senha. Para procurar o código de desvio, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Propriedades**. O **código de desvio de Bloqueio de Ativação** está em **Informações de segurança**.

macOS

Para gerenciar dispositivos macOS no XenMobile, você configura um certificado do Serviço de Notificação por Push da Apple (APNs) da Apple. Para obter informações, consulte Certificados APNs.

O XenMobile® registra dispositivos macOS no MDM. O XenMobile oferece suporte aos seguintes tipos de autenticação de registro para dispositivos macOS no MDM.

- Domínio
- Domínio mais senha de uso único
- URL de convite mais senha de uso único

> **Requisitos para certificados confiáveis no macOS 15:**

> A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, `<https://support.apple.com/pt-br/HT210176>`. Para obter ajuda com o gerenciamento de certificados, consulte Carregar certificados no XenMobile.

> Um fluxo de trabalho geral para iniciar o gerenciamento de dispositivos macOS é o seguinte:

1. Configurar políticas de dispositivos macOS.
2. Registrar dispositivos macOS.
3. Configure ações de segurança de dispositivos e aplicativos. Consulte Ações de segurança.

Para sistemas operacionais compatíveis, consulte Sistemas operacionais de dispositivos compatíveis.

Nomes de host da Apple que devem permanecer abertos

Alguns nomes de host da Apple devem permanecer abertos para garantir o funcionamento adequado do iOS, macOS e da Apple App Store. O bloqueio desses nomes de host pode afetar a instalação, atualização e o funcionamento adequado do seguinte: iOS, aplicativos iOS, operação MDM e registro de dispositivos e aplicativos. Para obter mais informações, consulte `<https://support.apple.com/pt-br/HT201999>`.

Métodos de registro compatíveis

A tabela a seguir lista os métodos de registro que o XenMobile oferece suporte para dispositivos macOS:

MÉTODO	COMPATÍVEL
Apple Deployment Program	Sim
Apple School Manager	Sim
Apple Configurator	Não
Registro manual	Sim
Convites de registro	Sim

A Apple tem programas de registro de dispositivos para contas empresariais e educacionais. Para contas empresariais, você se registra no Apple Deployment Program para usar o Apple Deployment Program para registro e gerenciamento de dispositivos no XenMobile. Esse programa é para dispositivos iOS e macOS. Consulte Implantar dispositivos por meio do Apple Deployment Program.

Para contas educacionais, você cria uma conta do Apple School Manager. O Apple School Manager unifica o Programa de Implantação e a compra em volume. O Apple School Manager é um tipo de Programa de Implantação Educacional da Apple. Consulte Integrar com recursos do Apple Education.

Você pode usar o Programa de Implantação da Apple para registrar em massa dispositivos iOS e macOS. Você pode adquirir esses dispositivos diretamente da Apple, de um Revendedor Autorizado Apple participante ou de uma operadora.

Configurar políticas de dispositivo macOS

Use estas políticas para configurar como o XenMobile interage com dispositivos que executam macOS. Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos macOS.

Espelhamento AirPlay	Inventário de Aplicativos	Calendário (CalDAV)
Contatos (CardDAV)	Controle de Atualização do SO	Credenciais

Firewall	Fonte	Importar perfil iOS e macOS
LDAP	E-mail	Senha
Remoção de perfil	Restrições	SCEP
VPN	Clipe da Web	Wi-Fi

Registrar dispositivos macOS

O XenMobile oferece dois métodos para registrar dispositivos que executam macOS. Ambos os métodos permitem que os usuários de macOS se registrem sem fio, diretamente de seus dispositivos.

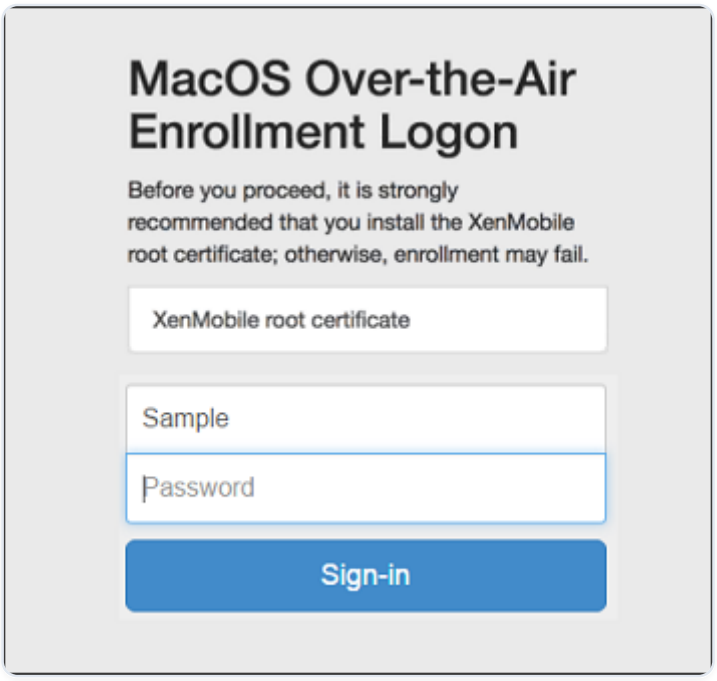
- **Enviar aos usuários um convite de registro:** Este método de registro permite definir qualquer um dos seguintes modos de segurança de registro para dispositivos macOS:
  - Nome de usuário + senha
  - Nome de usuário + PIN
  - Autenticação de dois fatores

  Quando o usuário segue as instruções no convite de registro, uma tela de logon com o nome de usuário preenchido é exibida.
- **Enviar aos usuários um link de registro:** Este método de registro para dispositivos macOS envia aos usuários um link de registro, que eles podem abrir nos navegadores Safari ou Chrome. Um usuário então se registra fornecendo seu nome de usuário e senha.

  Para evitar o uso de um link de registro para dispositivos macOS, defina a propriedade do servidor **Enable macOS OTAE** como **false**. Como resultado, os usuários de macOS podem se registrar apenas usando um convite de registro.

Enviar um convite de registro para usuários de macOS

1. Adicione um convite para o registro de usuário macOS. Consulte Criar um convite de registro.
2. Depois que os usuários recebem o convite e clicam no link, a seguinte tela aparece no navegador Safari. O XenMobile preenche o nome de usuário. Se você escolheu **Dois Fatores** para o modo de segurança de registro, outro campo aparece.



3. Os usuários instalam os certificados conforme necessário. Se os usuários veem o prompt para instalar certificados depende de você ter configurado o seguinte para macOS: Um certificado

SSL publicamente confiável e um certificado de assinatura digital publicamente confiável. Para obter informações sobre certificados, consulte Certificados e autenticação.

4. Os usuários fornecem as credenciais solicitadas.

   As políticas do dispositivo Mac são instaladas. Agora você pode começar a gerenciar dispositivos macOS com o XenMobile da mesma forma que gerencia dispositivos móveis.

Enviar um link de instalação para usuários de macOS

1. Envie o link de registro `https://serverFQDN:8443/instanceName/macos/otae`, que os usuários podem abrir nos navegadores Safari ou Chrome.

   - **serverFQDN** é o nome de domínio totalmente qualificado (FQDN) do servidor que executa o XenMobile.
   - A porta **8443** é a porta segura padrão. Se você configurou uma porta diferente, use essa porta em vez de 8443.
   - O **instanceName**, frequentemente exibido como `zdm`, é o nome especificado durante a instalação do servidor.

   Para obter mais informações sobre o envio de links de instalação, consulte Enviar um convite de inscrição.

2. Os usuários instalam os certificados conforme necessário. Se você configurou um certificado SSL publicamente confiável e um certificado de assinatura digital para iOS e macOS, os usuários verão o prompt para instalar os certificados. Para obter informações sobre certificados, consulte Certificados e autenticação.
3. Os usuários fazem login em seus Macs.

   As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar dispositivos macOS com o XenMobile da mesma forma que gerencia dispositivos móveis.

Ações de segurança

O macOS oferece suporte às seguintes ações de segurança. Para obter uma descrição de cada ação de segurança, consulte Ações de segurança.

Revogar	Bloquear	Limpeza Seletiva
Limpeza Completa	Renovação de certificado	

Bloquear dispositivos macOS

Você pode bloquear remotamente um dispositivo macOS perdido. O XenMobile bloqueia o dispositivo. Em seguida, ele gera um código PIN e o define no dispositivo. Para acessar o dispositivo, o usuário digita o código PIN. Use **Cancelar Bloqueio** para remover o bloqueio do console do XenMobile.

Você pode usar a política de dispositivo Código de acesso para configurar mais definições associadas ao código PIN. Para obter mais informações, consulte Configurações do macOS.

1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

   A página Dispositivo(/en-us/xenmobile/server/media/manage-devices-macos.png)

2. Selecione o dispositivo macOS que você deseja bloquear.

   Selecione a caixa de seleção ao lado de um dispositivo para exibir o menu de opções acima da lista de dispositivos. Você também pode clicar em qualquer outro lugar em um item listado para exibir o menu de opções no lado direito da lista.

   O menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos.png)

   O menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos-2.png)

3. No menu de opções, clique em **Proteger**. A caixa de diálogo **Ações de Segurança** é exibida.

   A caixa de diálogo Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-secure-lock-macos.png)

4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de Segurança** é exibida.

   A confirmação de Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm-macos.png)

5. Clique em **Bloquear Dispositivo**.

> **Importante:**
>
> Você também pode especificar uma senha em vez de usar o código que o XenMobile gera. A ação de bloqueio falha se o código especificado não atender aos requisitos de código do dispositivo ou do perfil de trabalho existente.

Registro em massa de dispositivos Apple

Você pode registrar um grande número de dispositivos iOS, iPadOS e macOS no XenMobile® de duas maneiras.

- Use o Programa de Implantação da Apple para registrar os dispositivos iOS, iPadOS e macOS que você compra diretamente da Apple, de um Revendedor Autorizado Apple participante ou de uma operadora. Esse suporte inclui iPads Compartilhados. O XenMobile oferece suporte ao Programa de Implantação da Apple para o Apple Business Manager (ABM) e o Apple School Manager (ASM) para Educação. Este artigo descreve como integrar vários dispositivos com sua conta ABM. Para obter informações sobre como se registrar no ABM e conectar sua conta ABM ao XenMobile, consulte Implantar dispositivos por meio do Programa de Implantação da Apple. Para obter informações sobre contas do Apple School Manager, consulte Integrar com recursos do Apple Education.

  Para o registro de dispositivos macOS, o XenMobile exige que os dispositivos executem o macOS 10.10 ou posterior.
- Você também pode usar o Apple Configurator 2 para registrar dispositivos iOS, independentemente de tê-los comprado diretamente da Apple ou não.

Com o ABM:

- Você não precisa tocar ou preparar os dispositivos. Em vez disso, você envia números de série de dispositivos ou números de pedidos de compra por meio do ABM para configurar e registrar os dispositivos.
- Depois que o XenMobile registra os dispositivos, você pode entregá-los aos usuários, que podem começar a usá-los imediatamente. Ao configurar dispositivos com o ABM, você pode eliminar algumas das etapas do Assistente de Configuração que os usuários talvez precisem concluir ao iniciar seus dispositivos pela primeira vez.
- Para obter mais informações sobre como configurar o ABM, consulte a documentação disponível em Apple Business Manager.

Com o Apple Configurator 2:

- Você conecta dispositivos iOS a um computador Apple executando macOS 10.7.2 ou posterior e o aplicativo Apple Configurator 2. Você prepara os dispositivos iOS e configura políticas por meio do Apple Configurator 2.

- Depois de provisionar os dispositivos com as políticas necessárias, na primeira vez que os dispositivos se conectarem ao XenMobile, eles receberão políticas do XenMobile. Você pode então começar a gerenciar os dispositivos.
- Para obter mais informações sobre como usar o Apple Configurator 2, consulte a Ajuda do Apple Configurator.

Pré-requisitos

Abra as portas necessárias para a conectividade entre o XenMobile e a Apple. Para obter mais informações, consulte Requisitos de porta.

Integre sua conta do Apple Business Manager com o XenMobile

Se você não tiver uma conta ABM configurada com o XenMobile, conclua as seguintes etapas em Implantar dispositivos por meio do Programa de Implantação da Apple.

- Inscreva-se no Apple Business Manager.
- Conecte sua conta do Apple Business Manager ao XenMobile.
- Peça dispositivos habilitados para o Programa de Implantação.
- Gerencie dispositivos habilitados para o Programa de Implantação.

Defina um servidor padrão para registro em massa

Para atribuir grandes pedidos de dispositivos iOS, iPadOS e macOS a um servidor MDM, você pode definir o XenMobile como o servidor padrão.

1. Faça login no Apple Business Manager usando uma conta de administrador ou de gerente de registro de dispositivo.
2. Na barra lateral, clique em **Configurações > Configurações de Gerenciamento de Dispositivos**.
3. Escolha um servidor MDM existente. Em **Atribuição de Dispositivo Padrão**, clique em **Alterar**. Selecione o servidor XenMobile padrão para cada tipo de dispositivo. Clique em **Concluído**.

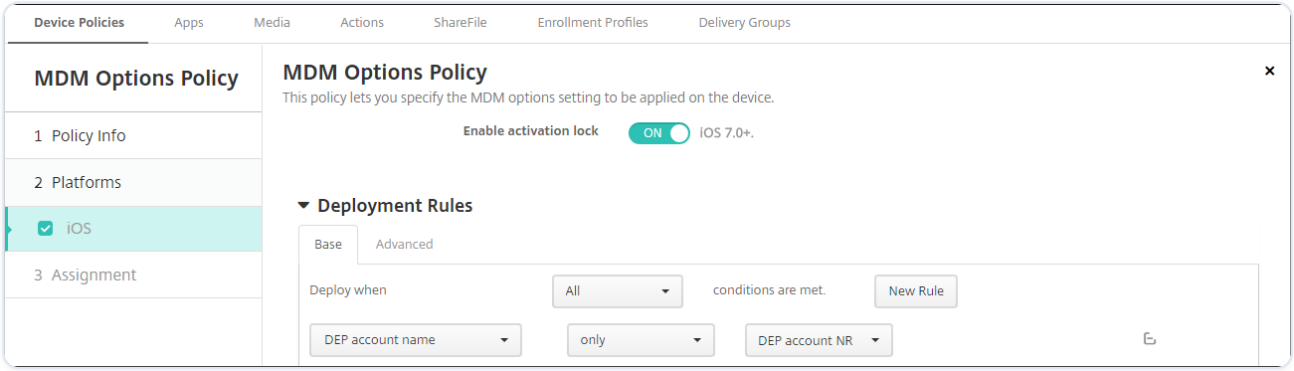
Configure regras de implantação de políticas de dispositivo e aplicativos para contas ABM

Você pode associar contas ABM a diferentes políticas de dispositivo e aplicativos usando a seção **Regras de Implantação** em **Configurar > Políticas de Dispositivo** e **Configurar > Aplicativos**. Você pode especificar que uma política ou aplicativo:

- É implantado apenas para uma conta ABM específica.
- É implantado para todas as contas ABM, exceto a selecionada.

A lista de contas ABM inclui apenas as contas com status ativado ou desativado. Se a conta ABM estiver desativada, o dispositivo ABM não pertence a esta conta. Assim, o XenMobile não implanta o aplicativo ou a política no dispositivo.

No exemplo a seguir, uma política de dispositivo é implantada apenas para dispositivos com o nome de conta ABM "ABM Account NR".



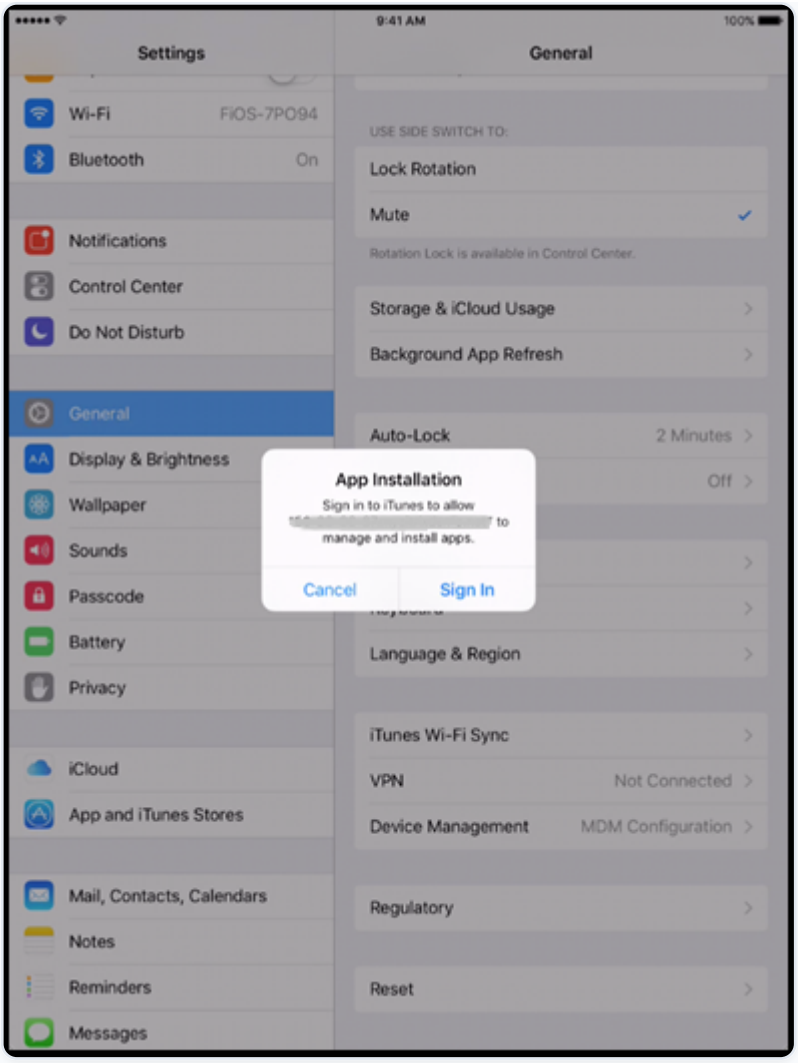
Experiência do usuário ao registrar um dispositivo habilitado para o Programa de Implantação da Apple

Quando os usuários registram um dispositivo habilitado para o Programa de Implantação da Apple, a experiência deles é a seguinte.

1. Os usuários iniciam seu dispositivo habilitado para o Programa de Implantação da Apple.
2. O XenMobile entrega a configuração do Programa de Implantação da Apple que você configurou no console do XenMobile para o dispositivo habilitado para o Programa de Implantação da Apple.
3. Os usuários configuram as configurações iniciais em seu dispositivo.
4. O dispositivo inicia automaticamente o processo de registro de dispositivo do XenMobile.
5. Os usuários continuam a configurar as outras configurações iniciais em seu dispositivo.
6. Na tela inicial, os usuários podem ser solicitados a fazer login na Apple App Store para que possam baixar o Citrix Secure Hub.

> **Nota:**

> Esta etapa é opcional se você configurar o XenMobile para implantar o aplicativo Secure Hub usando a atribuição de aplicativo de compra por volume baseada em dispositivo. Neste caso, você não precisa criar uma conta da Apple App Store ou usar uma conta existente.



7. Os usuários abrem o Secure Hub e digitam suas credenciais. Se exigido pela política, os usuários podem ser solicitados a criar e verificar um PIN do Citrix.

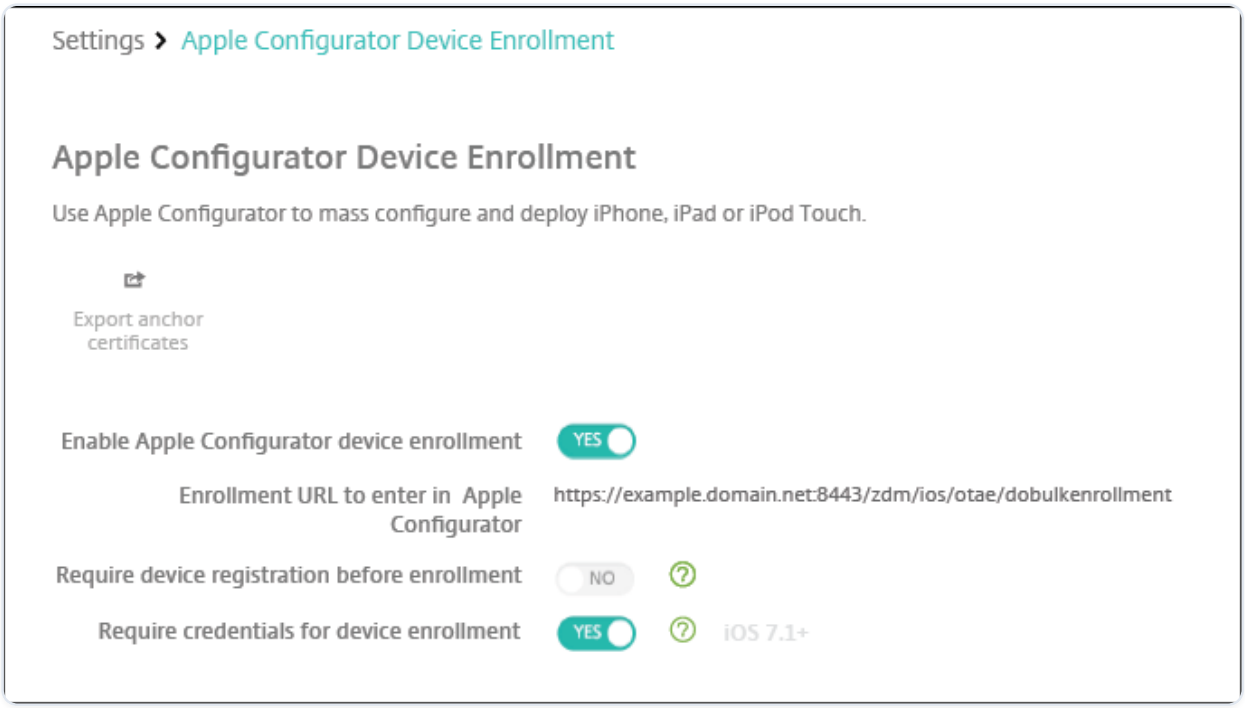
   O XenMobile implanta quaisquer aplicativos restantes necessários no dispositivo.

Para configurar as definições do Apple Configurator 2

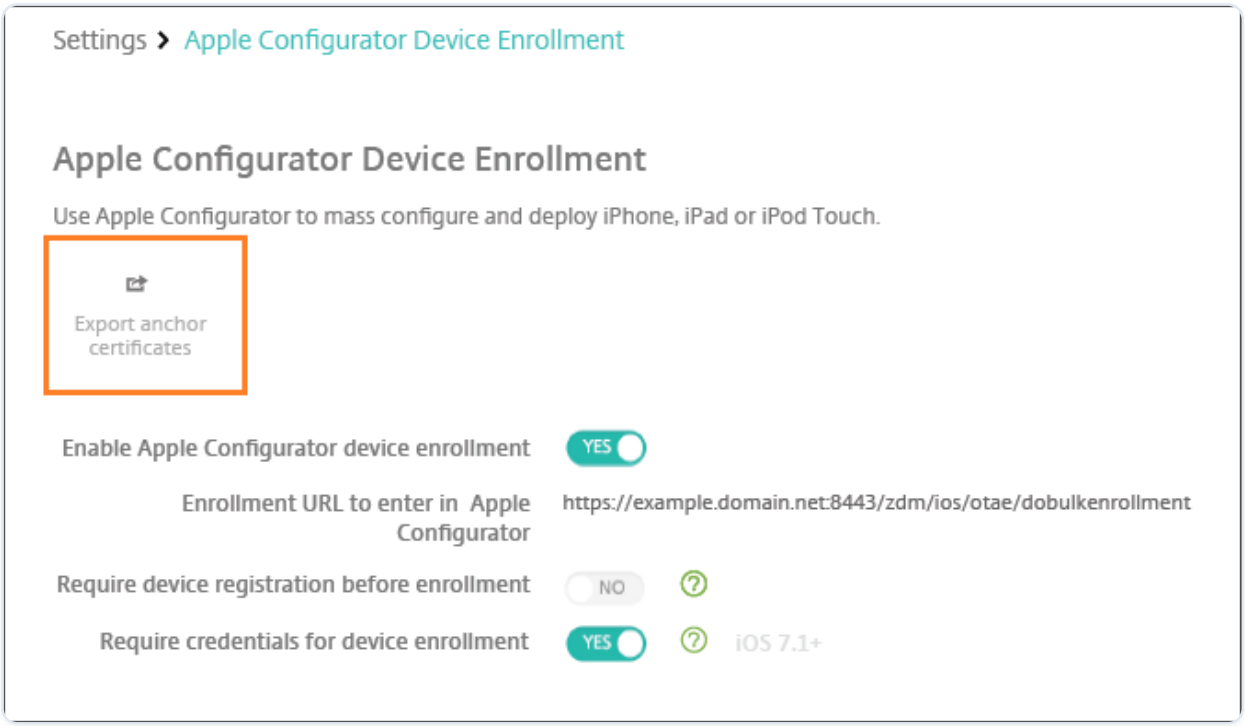
Você pode configurar e implantar dispositivos iPhone e iPad em massa usando o Apple Configurator 2 em vez do Apple Business Manager.

Etapa 1: Configurar as definições no XenMobile

1. No console do XenMobile, vá para **Configurações > Registro de Dispositivo do Apple Configurator**.



2. Defina **Habilitar registro de dispositivo do Apple Configurator** como **Sim**.
3. A **URL de registro para inserir no Apple Configurator** é um campo somente leitura. Essa configuração fornece a URL para o XenMobile Server que se comunica com a Apple. Copie e cole esta URL ao configurar as definições no Apple Configurator 2. A URL de registro é o nome de domínio totalmente qualificado (FQDN) do XenMobile Server, como `mdm.server.url.com`, ou o endereço IP.
4. Para evitar que dispositivos desconhecidos se registrem, defina **Exigir registro do dispositivo antes do registro** como **Sim**. Observação: Se esta configuração for **Sim**, você deve adicionar os dispositivos configurados em **Gerenciar > Dispositivos** no XenMobile manualmente ou por meio de um arquivo CSV antes do registro.
5. Para exigir que os usuários de dispositivos iOS insiram suas credenciais ao se registrar, defina **Exigir credenciais para registro de dispositivo** como **Sim**. O padrão é não exigir credenciais para o registro.
6. Observação: Se o XenMobile Server estiver usando um certificado SSL confiável, pule esta etapa. Clique em **Exportar certificados âncora** e salve o arquivo certchain.pem no chaveiro do macOS (login ou Sistema).



Etapa 2: Configurar as definições no Apple Configurator 2

1. Instale o Apple Configurator 2 da App Store.
2. Use um cabo Dock Connector para USB para conectar dispositivos ao Mac executando o Apple Configurator 2. Você pode configurar até 30 dispositivos conectados simultaneamente. Se você não tiver um Dock Connector, use um ou mais hubs USB 2.0 de alta velocidade alimentados para conectar os dispositivos.
3. Inicie o Apple Configurator 2. O configurador mostra todos os dispositivos que você pode preparar para supervisão.
4. Para preparar um dispositivo para supervisão:

   - Selecione **Supervisionar dispositivos** se você pretende manter o controle do dispositivo reaplicando uma configuração regularmente. Clique em **Avançar**.

     > **Importante:**
     >
     > Colocar um dispositivo no modo Supervisionado instala a versão selecionada do iOS no dispositivo, apagando completamente todos os dados de usuário ou aplicativos armazenados anteriormente.

   - No iOS, clique em **Mais recente** para a versão mais recente do iOS que você deseja instalar.

5. Em **Registrar no Servidor MDM**, escolha um servidor MDM. Para adicionar um novo servidor, clique em **Avançar**
6. Em **Definir um servidor MDM**, forneça um nome para o servidor e cole o URL do servidor MDM do console do XenMobile.
7. Em **Atribuir à organização**, escolha uma organização para supervisionar o dispositivo.

   Para obter mais informações sobre como preparar dispositivos com o Apple Configurator 2, consulte a página de ajuda do Apple Configurator, Preparar dispositivos.
8. À medida que cada dispositivo é preparado, ligue-o para iniciar o Assistente de Configuração do iOS, que prepara o dispositivo para o primeiro uso.

Para atribuir dispositivos do Apple Configurator 2 ao Apple Business Manager

Você pode associar dispositivos iPhone e iPad do Apple Configurator 2 à sua conta do Apple Business Manager. Ao adicionar dispositivos, eles aparecem na seção **Dispositivos**. Esses dispositivos não incluem mais as configurações de registro atribuídas através do Apple Configurator 2. Para obter mais informações, consulte Atribuir dispositivos adicionados do Apple Configurator 2 ao Apple Business Manager.

Renovar ou atualizar certificados ao usar o Programa de Implantação da Apple

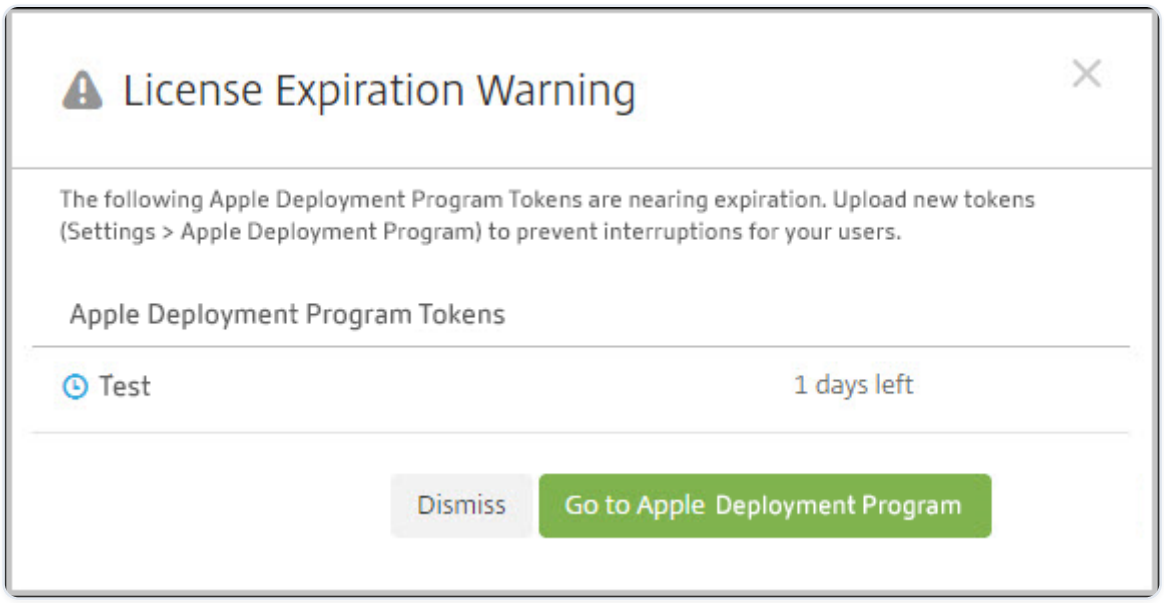
Quando o certificado SSL (Secure Sockets Layer) do XenMobile é renovado, você carrega um novo certificado no console do XenMobile em **Configurações > Certificados**. Na caixa de diálogo **Importar**, em **Usar como**, clique em **Ouvinte SSL** para que o certificado seja usado para SSL. Após reiniciar o servidor, o XenMobile usa o novo certificado SSL. Para obter mais informações sobre certificados no XenMobile, consulte Carregar Certificados no XenMobile.

Não é necessário restabelecer a relação de confiança entre o Programa de Implantação da Apple e o XenMobile ao renovar ou atualizar o certificado SSL. Você pode, no entanto, reconfigurar suas configurações do **Programa de Implantação da Apple** a qualquer momento, seguindo as etapas anteriores neste artigo.

Para obter mais informações sobre o Programa de Implantação da Apple, consulte a documentação da Apple.

Renove sua conexão entre o Programa de Implantação da Apple e o XenMobile

O XenMobile exibe um Aviso de Expiração de Licença quando o token do servidor de Registro Automatizado de Dispositivos expira.



Substitua o token do Apple School Manager/Apple Business Manager.

Etapa 1: Baixe uma chave pública do seu servidor XenMobile

1. No console do XenMobile, vá para **Configurações > Programa de Implantação da Apple** para baixar uma nova chave pública.

Etapa 2: Crie e baixe um arquivo de token de servidor da sua conta Apple

1. Faça login no Apple Business Manager para baixar o token.
2. Abra **Configurações** e selecione o servidor do qual você precisa de um token. Clique em **Editar**.
3. Em **Configurações do Servidor MDM**, carregue a nova chave pública que você baixou do XenMobile e salve as alterações.
4. Clique em **Baixar Token** para baixar o novo token.

Etapa 3: Carregue um arquivo de token de servidor no XenMobile

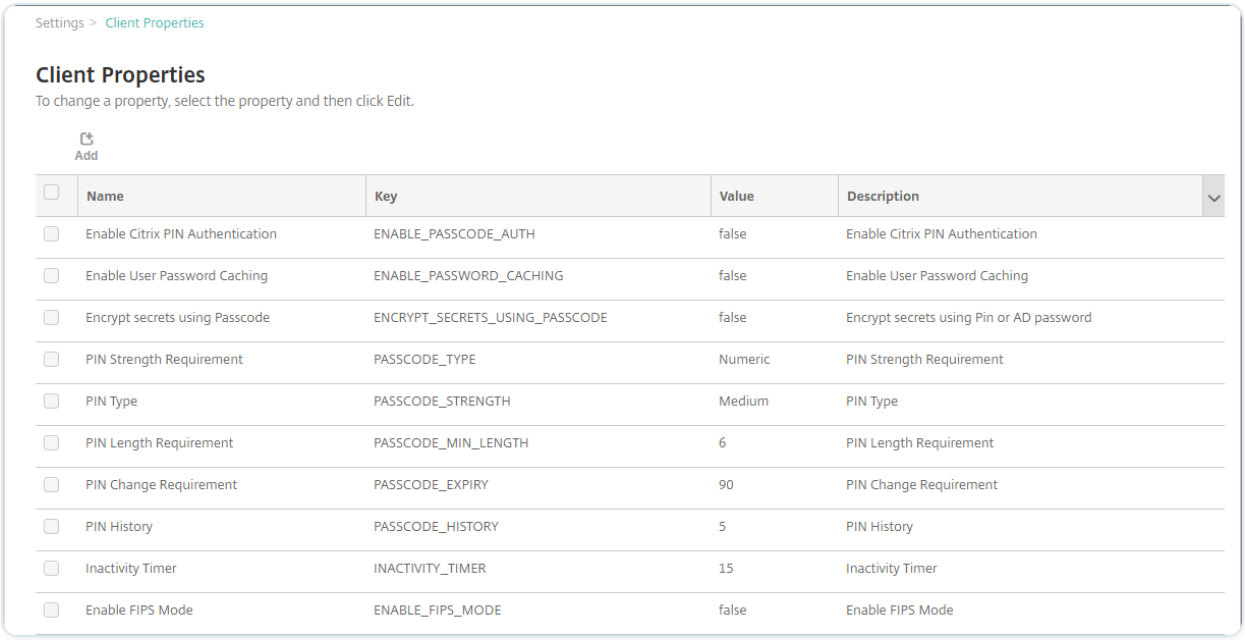
1. No Citrix XenMobile, vá para **Configurações > Programa de Implantação da Apple**.
2. Selecione a conta do Programa de Implantação, clique em **Editar** e carregue seu arquivo de token de servidor.
3. Clique em **Avançar** e salve as alterações.

Propriedades do cliente

As propriedades do cliente contêm informações que são fornecidas diretamente ao Secure Hub nos dispositivos do usuário. Você pode usar essas propriedades para configurar definições avançadas, como o PIN do Citrix. Você obtém as propriedades do cliente do suporte Citrix.

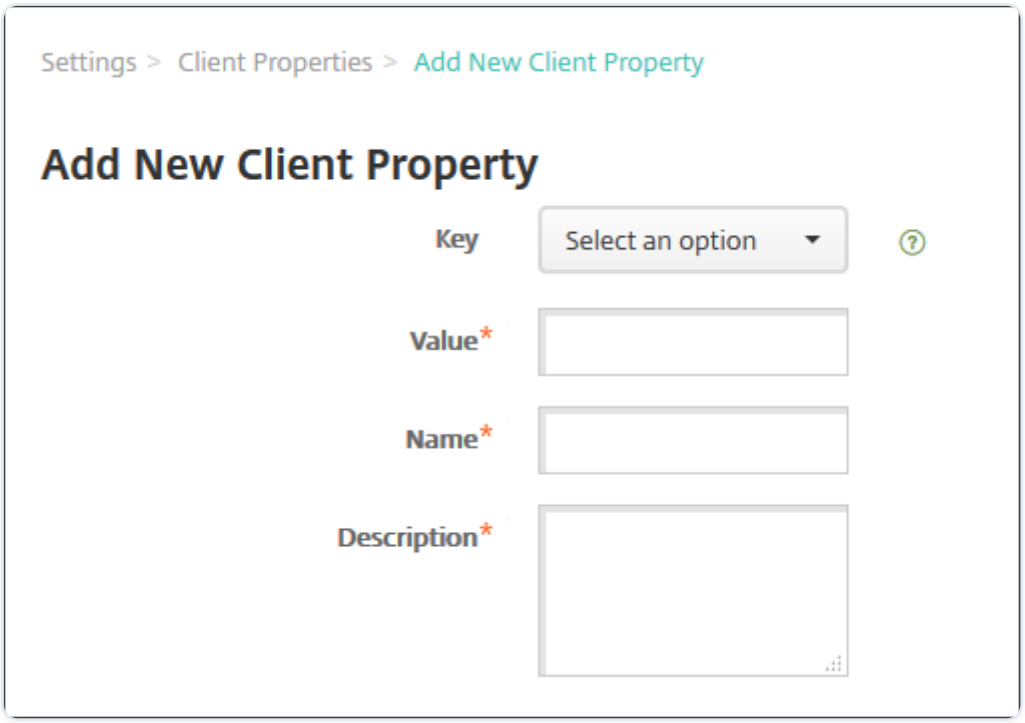
As propriedades do cliente estão sujeitas a alterações a cada lançamento do Secure Hub e, ocasionalmente, para aplicativos cliente. Para obter detalhes sobre as propriedades do cliente mais comumente configuradas, consulte Referência de propriedades do cliente, mais adiante neste artigo.

1. No console do XenMobile®, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Cliente**, clique em **Propriedades do Cliente**. A página **Propriedades do Cliente** é exibida. Você pode adicionar, editar e excluir propriedades do cliente nesta página.



Para adicionar uma propriedade do cliente

1. Clique em **Adicionar**. A página **Adicionar Nova Propriedade do Cliente** é exibida.



2. Configure estas definições:

   - **Chave:** Na lista, clique na chave de propriedade que você deseja adicionar. Importante: Entre em contato com o Suporte Citrix antes de atualizar as configurações. Você pode solicitar uma chave especial.
   - **Valor:** O valor da propriedade selecionada.
   - **Nome:** Um nome para a propriedade.
   - **Descrição:** Uma descrição da propriedade.

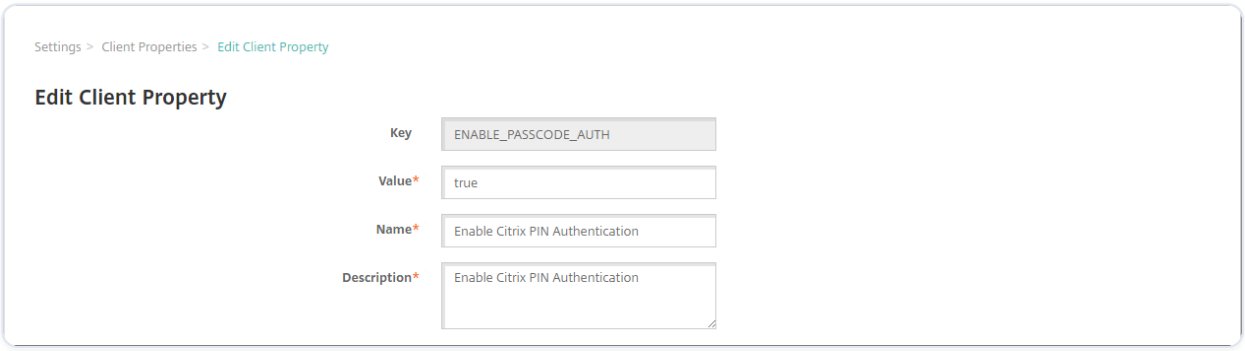
3. Clique em **Salvar**.

Para editar uma propriedade de cliente

1. Na tabela **Propriedades do Cliente**, selecione a propriedade do cliente que você deseja editar.

   Quando você seleciona a caixa de seleção ao lado de uma propriedade de cliente, o menu de opções aparece acima da lista de propriedades do cliente. Quando você clica em qualquer outro lugar da lista, o menu de opções aparece no lado direito da listagem.

2. Clique em **Editar**. A página **Editar Propriedade do Cliente** é exibida.



3. Altere as seguintes informações conforme apropriado:

   - **Chave:** Você não pode alterar este campo.
   - **Valor:** O valor da propriedade.
   - **Nome:** O nome da propriedade.
   - **Descrição:** A descrição da propriedade.

4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir uma propriedade de cliente

1. Na tabela **Propriedades do Cliente**, selecione a propriedade do cliente que você deseja excluir.

   Você pode selecionar mais de uma propriedade para excluir selecionando a caixa de seleção ao lado de cada propriedade.

2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Referência de propriedade do cliente

As propriedades de cliente predefinidas do XenMobile e suas configurações padrão são as seguintes:

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Nome de exibição: Período de autodestruição do contêiner MDX
  - A autodestruição impede o acesso ao Secure Hub e aos aplicativos gerenciados, após um número especificado de dias de inatividade. Após o limite de tempo, os aplicativos não são mais utilizáveis. A limpeza dos dados inclui a exclusão dos dados do aplicativo para cada aplicativo instalado, incluindo o cache do aplicativo e os dados do usuário.

O tempo de inatividade é quando o servidor não recebe uma solicitação de autenticação para validar o usuário por um período específico. Por exemplo, se esta propriedade for de 30 dias e o usuário não usar o aplicativo por mais de 30 dias, a política entrará em vigor.

Esta política de segurança global se aplica às plataformas iOS e Android e é um aprimoramento das políticas existentes de bloqueio e limpeza de aplicativos.

- Para configurar esta política global, vá para **Configurações > Propriedades do Cliente** e adicione a chave personalizada **CONTAINER_SELF_DESTRUCT_PERIOD**.
- Valor: Número de dias

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - Nome de exibição: Enviar logs do dispositivo para o suporte de TI
  - Esta propriedade habilita ou desabilita a capacidade de enviar logs para o suporte de TI.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **DISABLE_LOGGING**
  - Nome de exibição: Desabilitar Registro em Log
  - Use esta propriedade para impedir que os usuários coletem e carreguem logs de seus dispositivos. Esta propriedade desabilita o registro em log para o Secure Hub e para todos os aplicativos MDX instalados. Os usuários não podem enviar logs para nenhum aplicativo da página de Suporte. Embora a caixa de diálogo de composição de e-mail apareça, os logs não são anexados. Uma mensagem indica que o registro em log está desabilitado. Essa configuração também impede que você atualize as configurações de log no console do XenMobile para o Secure Hub e aplicativos MDX.

    Quando esta propriedade é definida como **true**, o Secure Hub define **Bloquear logs de aplicativo** como **true**. Como resultado, os aplicativos MDX param de registrar logs quando a nova política é aplicada.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false** (o registro em log não está desabilitado)
- **ENABLE_CRASH_REPORTING**
  - Nome de exibição: Habilitar Relatório de Falhas
  - Se **true**, a Citrix coleta relatórios de falhas e diagnósticos para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se **false**, nenhum dado é coletado.

- Valores possíveis: **true** ou **false**
- Valor padrão: **true**

- **ENABLE_CREDENTIAL_STORE**
  - Nome de exibição: Habilitar Armazenamento de Credenciais
  - Habilitar o armazenamento de credenciais significa que os usuários Android ou iOS inserem sua senha uma única vez ao acessar aplicativos de produtividade móvel. Você pode usar o armazenamento de credenciais, independentemente de habilitar ou não o PIN da Citrix. Se você não habilitar o PIN da Citrix, os usuários inserem sua senha do Active Directory. O XenMobile oferece suporte ao uso de senhas do Active Directory com o armazenamento de credenciais apenas para o Secure Hub e aplicativos de loja pública. Se você usar senhas do Active Directory com o armazenamento de credenciais, o XenMobile não oferece suporte à autenticação PKI.
  - O registro automático no Secure Mail exige que você defina esta propriedade como **true**.
  - Para configurar esta política de cliente personalizada, vá para **Configurações > Propriedades do Cliente**, adicione a chave personalizada **ENABLE_CREDENTIAL_STORE** e defina o **Valor** como **true**.

- **ENABLE_FIPS_MODE**
  - Nome de exibição: Habilitar Modo FIPS
  - Esta propriedade habilita ou desabilita o modo FIPS em dispositivos móveis. Depois de alterar o valor, o Secure Hub passa o novo valor para o dispositivo quando o Secure Hub realiza a próxima autenticação online.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**

- **ENABLE_PASSCODE_AUTH**
  - Nome de exibição: Habilitar Autenticação por PIN Citrix
  - Esta propriedade permite ativar a funcionalidade de PIN Citrix. Com o PIN ou código de acesso Citrix, os usuários são solicitados a definir um PIN para usar em vez de sua senha do Active Directory. Essa configuração é habilitada automaticamente quando ENABLE_PASSWORD_CACHING está habilitado ou quando o XenMobile está usando autenticação por certificado.

Para autenticação offline, o PIN Citrix é validado localmente e os usuários têm permissão para acessar o aplicativo ou conteúdo solicitado. Para autenticação online, o PIN ou código de acesso Citrix desbloqueia a senha ou certificado do Active Directory, que é então enviado para realizar a autenticação com o XenMobile.

Se ENABLE_PASSCODE_AUTH for true e ENABLE_PASSWORD_CACHING for false, a autenticação online sempre solicitará a senha porque o Secure Hub não a salva.

- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_PASSWORD_CACHING**
  - Nome de exibição: Habilitar Cache de Senha do Usuário
  - Esta propriedade permite que as senhas do Active Directory sejam armazenadas em cache localmente no dispositivo móvel. Ao definir esta propriedade como **true**, você também deve definir a propriedade **ENABLE_PASSCODE_AUTH** como **true**. Com o cache de senha do usuário habilitado, o XenMobile solicita que os usuários definam um PIN ou código de acesso Citrix.
  - Valores possíveis: **verdadeiro** ou **falso**
  - Valor padrão: **falso**
- **ENABLE_TOUCH_ID_AUTH**
  - Nome de exibição: Habilitar Autenticação Touch ID
  - Para dispositivos que suportam autenticação Touch ID, esta propriedade habilita ou desabilita a autenticação Touch ID no dispositivo. Requisitos:

    Os dispositivos do usuário devem ter o PIN Citrix ou LDAP habilitado. Se a autenticação LDAP estiver desativada (por exemplo, porque apenas a autenticação baseada em certificado é usada), os usuários devem definir um PIN Citrix. Nesse caso, o XenMobile exige o PIN Citrix mesmo que a propriedade do cliente **ENABLE_PASSCODE_AUTH** seja **falsa**.

    Defina **ENABLE_PASSCODE_AUTH** como **falso** para que, quando os usuários iniciarem um aplicativo, eles precisem responder a um prompt para usar o Touch ID.
  - Valores possíveis: **verdadeiro** ou **falso**
  - Valor padrão: **falso**
- **ENABLE_WORXHOME_CEIP**

- Nome de exibição: Habilitar CEIP do Worx Home
- Esta propriedade ativa o Programa de Melhoria da Experiência do Cliente. Esse recurso envia dados anônimos de configuração e uso para a Citrix periodicamente. Os dados ajudam a Citrix a melhorar a qualidade, a confiabilidade e o desempenho do XenMobile.
- Valor: **verdadeiro** ou **falso**
- Valor padrão: **falso**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Nome de exibição: Criptografar segredos usando Senha
  - Esta propriedade armazena dados confidenciais no dispositivo em um cofre secreto, em vez de em um armazenamento nativo baseado em plataforma, como o chaveiro do iOS. Esta propriedade permite uma criptografia forte de artefatos-chave e adiciona entropia do usuário. Entropia do usuário é um código PIN aleatório gerado pelo usuário que somente o usuário conhece.

    A Citrix recomenda que você habilite esta propriedade para ajudar a fornecer maior segurança nos dispositivos dos usuários. Como resultado, os usuários experimentam mais solicitações de autenticação para o PIN do Citrix.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**

- **INACTIVITY_TIMER**
  - Nome de exibição: Temporizador de Inatividade
  - Esta propriedade define por quanto tempo os usuários podem deixar seus dispositivos inativos e, em seguida, acessar um aplicativo sem uma solicitação de PIN ou senha do Citrix. Para habilitar esta configuração para um aplicativo MDX, defina a configuração de Senha do Aplicativo como Ativada. Se a configuração de Senha do Aplicativo estiver definida como Desativada, os usuários serão redirecionados para o Secure Hub para fazer uma autenticação completa. Quando você altera esta configuração, o valor entra em vigor na próxima vez que os usuários forem solicitados a autenticar.

    No iOS, o Temporizador de Inatividade também governa o acesso ao Secure Hub para aplicativos MDX e não-MDX.
  - Valores possíveis: Qualquer número inteiro positivo
  - Valor padrão: **15** (minutos)

- **ON_FAILURE_USE_EMAIL**
  - Nome de exibição: Em caso de falha, usar e-mail para enviar logs do dispositivo para o suporte de TI
  - Esta propriedade habilita ou desabilita a capacidade de usar e-mail para enviar logs do dispositivo para a TI.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **true**
- **PASSCODE_EXPIRY**
  - Nome de exibição: Requisito de Alteração de PIN
  - Esta propriedade define por quanto tempo o PIN ou senha do Citrix é válido, após o qual o usuário é forçado a alterar seu PIN ou senha do Citrix. Ao alterar esta configuração, o novo valor é definido somente quando o PIN ou senha do Citrix atual expira.
  - Valores possíveis: **1** a **99** recomendado. Para eliminar redefinições de PIN, defina o valor para um número alto (por exemplo, 100.000.000.000). Se você definiu originalmente o período de expiração entre 1 e 99 dias e depois alterou para o número grande durante esse período: os PINs ainda expiram no final do período inicial, mas nunca mais depois disso.
  - Valor padrão: **90** (dias)
- **PASSCODE_HISTORY**
  - Nome de exibição: Histórico de PIN
  - Esta propriedade define o número de PINs ou senhas do Citrix usados anteriormente que os usuários não podem reutilizar ao alterar seu PIN ou senha do Citrix. Ao alterar esta configuração, o novo valor é definido na próxima vez que os usuários redefinirem seu PIN ou senha do Citrix.
  - Valores possíveis: **1** a **99**
  - Valor padrão: **5**
- **PASSCODE_MAX_ATTEMPTS**
  - Nome de exibição: Tentativas de PIN
  - Esta propriedade define quantas tentativas incorretas de PIN ou senha do Citrix os usuários podem fazer antes de serem solicitados a uma autenticação completa. Depois

que os usuários realizam uma autenticação completa com sucesso, eles são solicitados a criar um PIN ou senha do Citrix.

- Valores possíveis: Qualquer número inteiro positivo
- Valor padrão: **15**

- **PASSCODE_MIN_LENGTH**
  - Nome de exibição: Requisito de Comprimento do PIN
  - Esta propriedade define o comprimento mínimo dos PINs Citrix.
  - Valores possíveis: **4** a **10**
  - Valor padrão: **6**
- **PASSCODE_STRENGTH**
  - Nome de exibição: Requisito de Força do PIN
  - Esta propriedade define a força de um PIN ou senha Citrix. Ao alterar esta configuração, os usuários são solicitados a criar um PIN ou senha Citrix na próxima vez que forem solicitados a autenticar.
  - Valores possíveis: **Baixo**, **Médio**, **Alto** ou **Forte**
  - Valor padrão: **Médio**
  - As regras de senha para cada configuração de força, com base na configuração PASSCODE_TYPE, são as seguintes:

Regras para senhas numéricas:

FORÇA DA SENHA	REGRAS PARA O TIPO DE SENHA NUMÉRICA	PERMITIDO	NÃO PERMITIDO
Baixo	Todos os números, qualquer sequência permitida	444444, 123456, 654321	
Médio (configuração padrão)	Todos os números não podem ser iguais ou consecutivos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321

FORÇA DA SENHA	REGRAS PARA O TIPO DE SENHA NUMÉRICA	PERMITIDO	NÃO PERMITIDO
Alto	Números adjacentes não podem ser iguais.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Forte	Não use o mesmo número mais de duas vezes. Não use três ou mais números consecutivos em sequência. Não use três ou mais números consecutivos em ordem inversa.	102983, 085085, 824673, 132312	132132, 131313, 902030

Regras para senhas alfanuméricas:

FORÇA DA SENHA	REGRAS PARA O TIPO DE SENHA ALFANUMÉRICA	PERMITIDO	NÃO PERMITIDO
Baixa	Deve conter pelo menos um número e uma letra	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, Abcdef
Média (configuração padrão)	Além das regras para senhas de força Baixa, letras e todos os números não podem ser os mesmos. As letras não podem ser consecutivas e os números não podem ser consecutivos.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, ou aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, ou cba123

FORÇA DA SENHA	REGRAS PARA O TIPO DE SENHA ALFANUMÉRICA	PERMITIDO	NÃO PERMITIDO
Alto	Inclua pelo menos uma letra maiúscula e uma letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Forte	Inclua pelo menos um número, um símbolo especial, uma letra maiúscula e uma letra minúscula.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - Nome de exibição: Tipo de PIN
  - Esta propriedade define se os usuários podem definir um PIN numérico do Citrix ou uma senha alfanumérica. Ao selecionar **Numérico**, os usuários podem usar apenas números (PIN do Citrix). Ao selecionar **Alfanumérico**, os usuários podem usar uma combinação de letras e números (senha).

    Se você alterar esta configuração, os usuários deverão definir um novo PIN ou senha do Citrix na próxima vez que forem solicitados a autenticar.
  - Valores possíveis: **Numérico** ou **Alfanumérico**
  - Valor padrão: **Numérico**
- **REFRESHINTERVAL**
  - Nome de exibição: REFRESHINTERVAL
  - Por padrão, o XenMobile faz ping no Auto Discovery Server (ADS) para certificados fixados a cada 3 dias. Para alterar o intervalo de atualização, vá para **Configurações > Propriedades do Cliente**, adicione a chave personalizada **REFRESHINTERVAL** e defina o **Valor** para o número de horas.
  - Valor padrão: **72** horas (3 dias)
- **SEND_LDAP_ATTRIBUTES**

- Para implantações somente MAM de dispositivos Android, iOS ou macOS: Você pode configurar o XenMobile para que os usuários que se inscrevem no Secure Hub com credenciais de e-mail sejam automaticamente inscritos no Secure Mail. Como resultado, os usuários não fornecem informações extras nem precisam de etapas adicionais para se inscrever no Secure Mail.
- Para configurar esta política de cliente global, vá para **Configurações > Propriedades do Cliente**, adicione a chave personalizada **SEND_LDAP_ATTRIBUTES** e defina o **Valor** da seguinte forma.
- Valor: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
- Os valores dos atributos são especificados como macros, semelhante às políticas MDM.
- Aqui está uma resposta de serviço de conta de exemplo para esta propriedade:

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
  name="SEND_LDAP_ATTRIBUTES"/>
  ```

- Para esta propriedade, o XenMobile trata os caracteres de vírgula como terminadores de string. Portanto, se um valor de atributo incluir uma vírgula, preceda-o com uma barra invertida. A barra invertida impede que o cliente interprete a vírgula incorporada como o fim do valor do atributo. Represente os caracteres de barra invertida com `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Quando esta propriedade não está definida ou está definida como **false**, os usuários podem acessar o menu de recursos ocultos tocando com três dedos em seus dispositivos. O menu de recursos ocultos permitia que os usuários redefinissem os dados do aplicativo. Definir esta propriedade como **true** desabilita o acesso dos usuários ao menu de recursos ocultos.
  - Para configurar esta política de cliente global, vá para **Configurações > Propriedades do Cliente**, adicione a chave personalizada **HIDE_THREE_FINGER_TAP_MENU** e defina o **Valor**.
- **TUNNEL_EXCLUDE_DOMAINS**
  - Nome de exibição: Domínios a Excluir do Túnel
  - Por padrão, o MDX exclui do tunelamento de micro VPN alguns endpoints de serviço que os SDKs e aplicativos do XenMobile usam para vários recursos. Por exemplo, esses endpoints incluem serviços que não exigem roteamento através de redes corporativas,

como Google Analytics, serviços Citrix Cloud™ e serviços Active Directory. Use esta propriedade de cliente para substituir a lista padrão de domínios excluídos.

- Para configurar esta política de cliente global, vá para **Configurações > Propriedades do Cliente**, adicione a chave personalizada **TUNNEL_EXCLUDE_DOMAINS** e defina o **Valor**.
- Valor: Para substituir a lista padrão pelos domínios que você deseja excluir do tunelamento, digite uma lista de sufixos de domínio separados por vírgulas. Para incluir todos os domínios no tunelamento, digite **none**. O padrão é:

  `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

As propriedades de cliente personalizadas para o XenMobile Server são as seguintes:

- **ENABLE_MAM_NFACTOR_SSO**
  - Esta propriedade permite habilitar ou desabilitar o SSO nFactor do MAM durante o registro ou login do MAM para o Secure Hub ao usar a política de autenticação avançada no NetScaler® Gateway. Se o valor for definido como **true**, então o SSO nFactor do MAM é habilitado durante o registro ou login do MAM para o Secure Hub.
  - Para configurar esta propriedade, vá para **Configurações > Propriedades do Cliente** e clique em **Adicionar**. Selecione **Chave Personalizada** no menu suspenso **Chave** e atualize as seguintes informações conforme apropriado:
    - Chave - ENABLE_MAM_NFACTOR_SSO
    - Valor - true ou false
    - Nome - ENABLE_MAM_NFACTOR_SSO
    - Descrição - Adicione a descrição relevante
- **MICROSOFT_CERTIFICATE_STRONG_MAPPING**
  - Esta propriedade controla se os certificados de cliente existentes são renovados para suportar o recurso de mapeamento forte de certificado, anexando o Identificador de Segurança (SID) ao Nome Alternativo do Assunto (SAN) ao usar o Secure Mail com uma Infraestrutura de Chave Pública (PKI) da Microsoft. Se o valor for definido como **true**, então os certificados de cliente existentes serão renovados para incluir o SAN SID.
  - Esta propriedade se aplica apenas ao Microsoft PKI.

- Para configurar esta propriedade, vá para **Settings > Client Properties** e clique em **Add**. Selecione **Custom Key** no menu suspenso **Key** e atualize as seguintes informações conforme apropriado:
  - Chave - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - Valor - true ou false
  - Nome - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - Descrição - Renovar certificados de cliente para incluir SAN SID

Implantar dispositivos através do Programa de Implantação da Apple

A Apple possui programas de registro de dispositivos para contas empresariais e educacionais. Para contas empresariais, você se registra no Programa de Implantação da Apple para usar o Apple Business Manager (ABM) ou o Apple School Manager (ASM) para registro e gerenciamento de dispositivos no XenMobile. Esse programa é para dispositivos iOS, iPadOS e macOS.

O Programa de Implantação da Apple está disponível para organizações e não para indivíduos. Você deve fornecer um número considerável de detalhes e informações corporativas para criar uma conta do Programa de Implantação da Apple. Portanto, pode levar tempo para solicitar e receber aprovação para as contas.

Para contas educacionais, você cria uma conta do Apple School Manager. O ASM unifica o Programa de Implantação da Apple e a compra por volume da Apple. Para criar uma conta do Apple School Manager, acesse o site da Apple School.

Registrar-se no Programa de Implantação da Apple

Para se registrar no Apple Business Manager, acesse business.apple.com. Clique em **Registrar agora** para solicitar uma nova conta. A melhor prática é usar um endereço de e-mail da sua organização, como `deployment@company.com`. O processo de registro pode levar alguns dias. Depois de receber suas credenciais de logon, siga as etapas fornecidas no Apple Business Manager para criar uma conta.

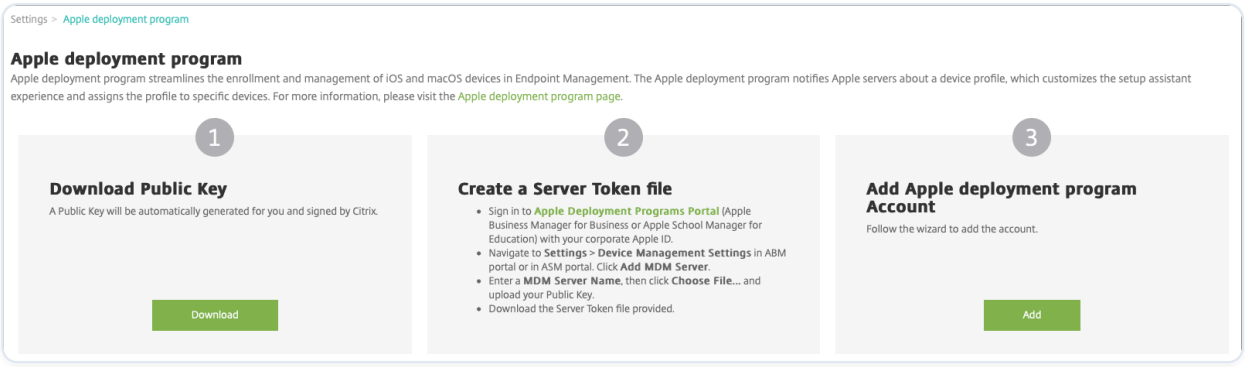
> **Observação:**
>
> Para contas educacionais, consulte Integrar com recursos do Apple Education.

Conecte sua conta do Apple Business Manager com o XenMobile

Para conectar sua conta do Apple Business Manager com sua implantação do XenMobile, insira as informações no console do XenMobile e no Apple Business Manager. Siga estas etapas:

Etapa 1: Baixe uma chave pública do seu XenMobile Server

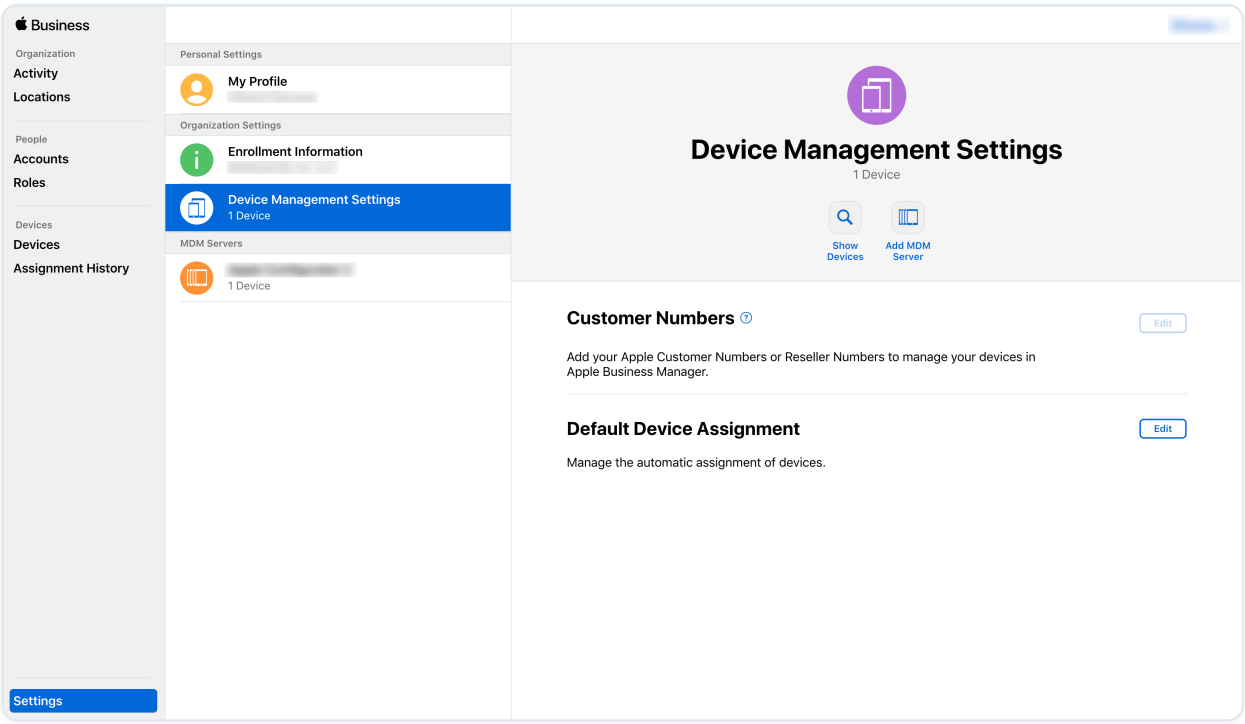
1. No console do XenMobile, vá para **Configurações > Programa de Implantação da Apple**.



2. Em **Baixar Chave Pública**, clique em **Baixar**.

Etapa 2: Crie e baixe um arquivo de token de servidor da sua conta Apple

1. Faça login no Apple Business Manager usando uma conta de administrador ou de gerente de registro de dispositivo.
2. Na parte inferior da barra lateral, clique em **Settings** e depois em **Device Management Settings > Add MDM Server**.



3. Na configuração **MDM Server Name**, digite um nome para o XenMobile Server. O nome do servidor que você digita é para sua referência. Não é a URL ou o nome do servidor.
4. Em **Upload Public Key**, clique em **Choose File**. Carregue a chave pública que você baixou do XenMobile e salve as alterações.
5. Clique em **Download Token** para baixar o arquivo de token do servidor para o seu computador.

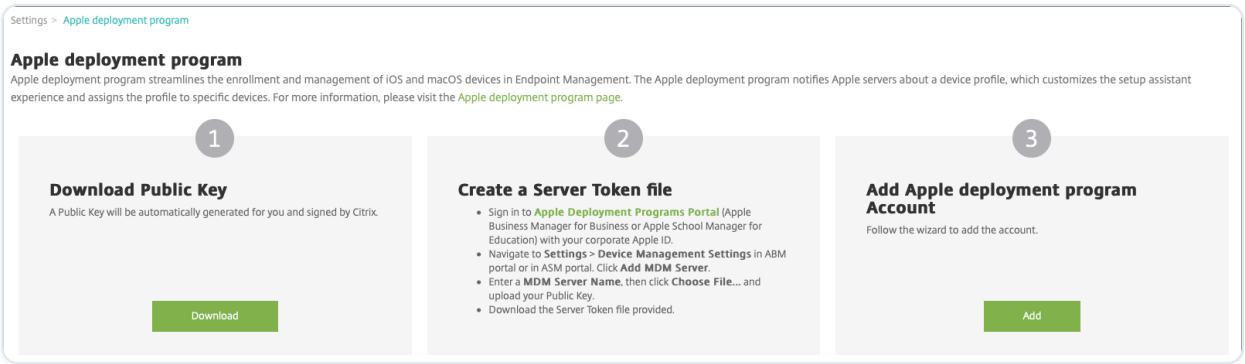
   Você deve carregar o arquivo de token do servidor ao adicionar a conta ABM ao XenMobile. Suas informações de token ABM aparecem no console do XenMobile depois que você importa o arquivo de token.
6. Em **Default Device Assignment**, clique em **Change**. Escolha como deseja atribuir dispositivos e forneça as informações solicitadas. Para obter informações, consulte o Guia do Usuário ABM.

Etapa 3: Adicionar uma conta ABM ao XenMobile

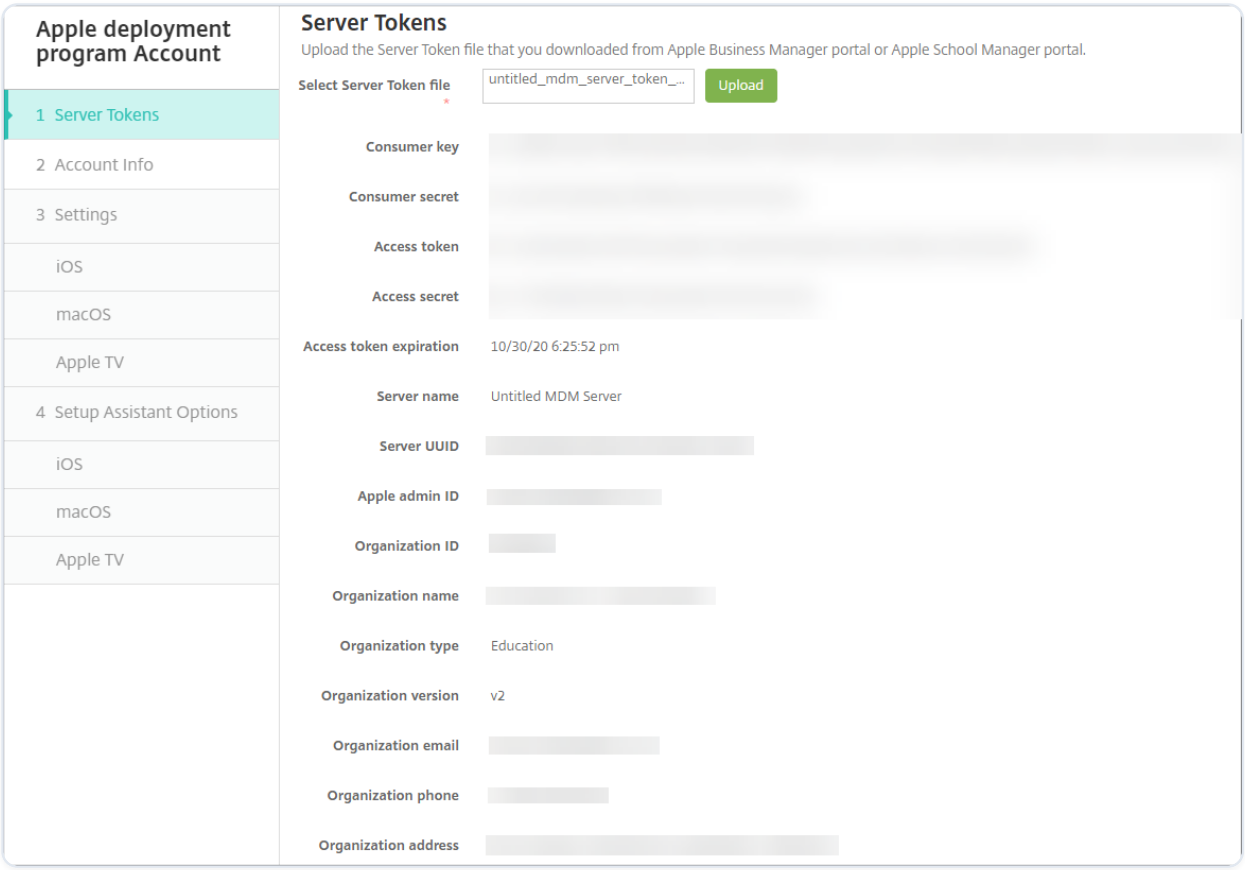
Você pode adicionar várias contas ABM ao XenMobile. Esse recurso permite que você use diferentes configurações de registro e opções de assistente de configuração por país, departamento e assim por diante. Em seguida, você associa as contas ABM a diferentes políticas de dispositivo.

Por exemplo, você pode centralizar todas as suas contas ABM de diferentes países no mesmo XenMobile Server, para importar e supervisionar todos os dispositivos ABM. Ao personalizar as configurações de registro e as opções do assistente de configuração por departamento, hierarquia organizacional ou outra estrutura, as políticas fornecem a funcionalidade apropriada em toda a sua organização, e os usuários recebem a assistência adequada.

1. No console do XenMobile, vá para **Settings > Apple Deployment Program** e, em **Add Apple Deployment Program Account**, clique em **Add**.

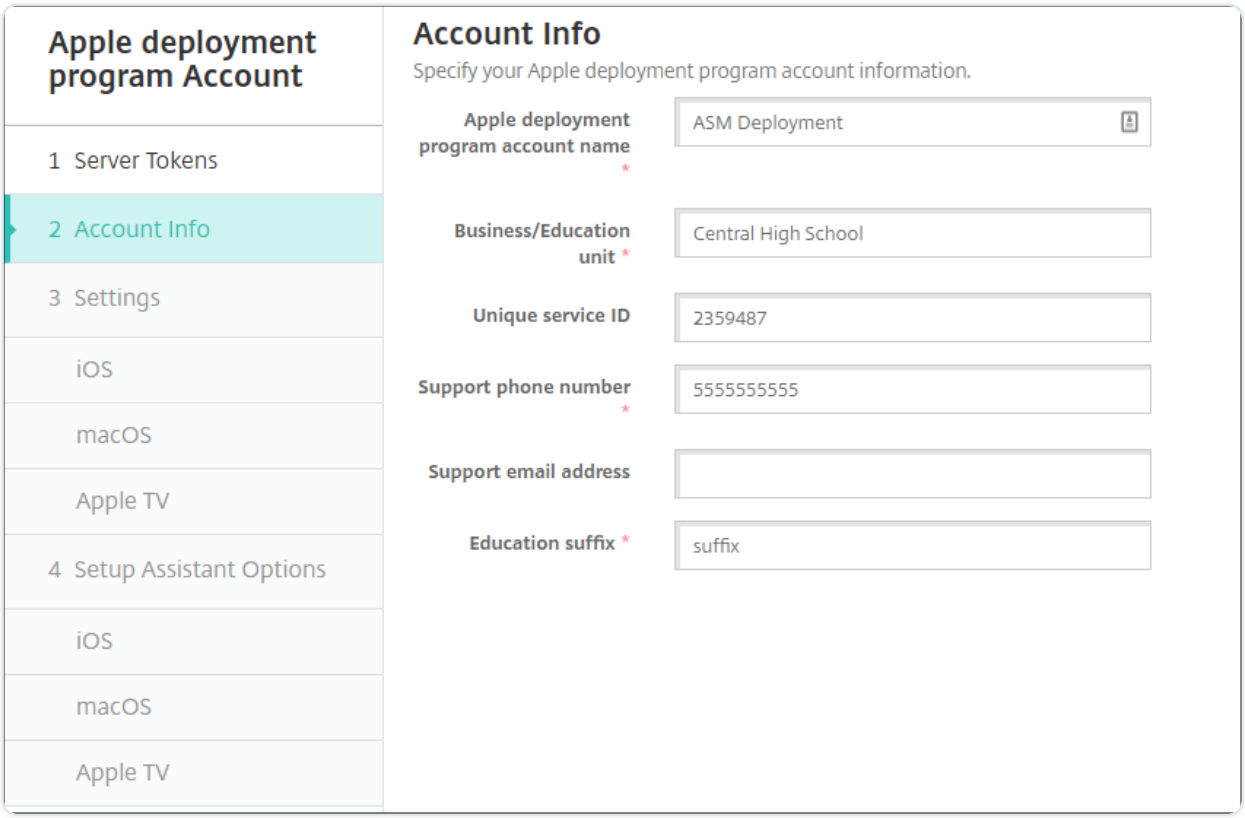


2. Na página **Server Tokens**, especifique seu arquivo de token do servidor e clique em **Upload**.



As informações do token do seu servidor aparecem.

3. Na página **Informações da Conta**, especifique estas configurações:

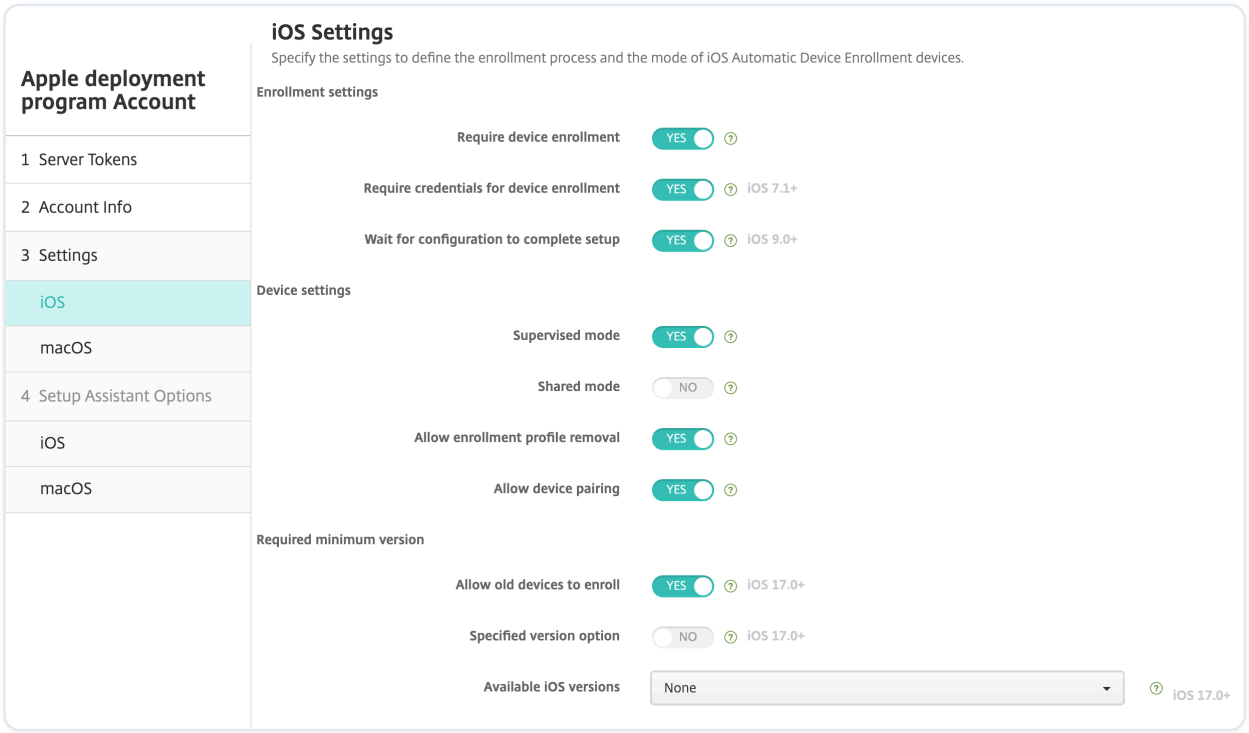


- **Nome da conta do Programa de Implantação da Apple:** Um nome exclusivo para esta conta do Programa de Implantação da Apple. Use nomes que reflitam como você organiza

as contas do Programa de Implantação da Apple, como por país ou hierarquia organizacional.

- **Unidade de Negócios/Educação:** A unidade de negócios ou departamento ao qual o dispositivo está atribuído. Este campo é obrigatório.
- **ID de serviço exclusivo:** Um ID exclusivo opcional para ajudar a identificar ainda mais a conta.
- **Número de telefone de suporte:** Um número de telefone de suporte para o qual os usuários ligam para obter ajuda durante a configuração. Este campo é obrigatório.
- **Endereço de e-mail de suporte:** Um endereço de e-mail de suporte opcional disponível para os usuários finais.
- **Sufixo de Educação**: Para contas ASM. Digite o sufixo atribuído aos dispositivos registrados por meio desta conta.

4. Em **Configurações do iOS**, especifique estas configurações:



Configurações de registro

- **Exigir registro do dispositivo:** Se deve exigir que os usuários registrem seus dispositivos. O padrão é **Sim**.
- **Exigir credenciais para registro do dispositivo:** Se deve exigir que os usuários insiram suas credenciais durante a configuração do ABM. A Citrix® recomenda que você exija que

todos os usuários insiram suas credenciais durante o registro do dispositivo, permitindo assim que apenas usuários autorizados registrem dispositivos. O padrão é **Sim**.

Quando você habilita o ABM antes da primeira configuração e não seleciona esta opção, o XenMobile cria os componentes do ABM. Esta criação inclui componentes como usuário ABM, Secure Hub, inventário de software e grupo de implantação ABM. Se você selecionar esta opção, o XenMobile não cria os componentes. Como resultado, se você desmarcar esta opção posteriormente, os usuários que não inseriram suas credenciais não poderão se registrar no ABM porque esses componentes ABM não existem. Para adicionar componentes ABM, nesse caso, desative a conta ABM e ative-a novamente.

- **Aguardar a conclusão da configuração:** Se é necessário que os dispositivos dos usuários permaneçam no modo Assistente de Configuração até que todos os recursos MDM sejam implantados no dispositivo. Essa configuração está disponível para dispositivos no modo supervisionado. O padrão é **Não**.
- A documentação da Apple afirma que os seguintes comandos podem não funcionar enquanto um dispositivo estiver no modo Assistente de Configuração:
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Configurações do dispositivo

- **Modo supervisionado:** Deve ser definido como **Sim** se você estiver usando o Apple Configurator para gerenciar dispositivos registrados no ABM ou quando **Aguardar a conclusão da configuração** estiver ativado. O padrão é **Sim**. Para obter detalhes sobre como colocar um dispositivo iOS no modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.
- **Permitir remoção do perfil de registro:** Se permite que os dispositivos usem um perfil que você pode remover remotamente. O padrão é **Não**.
- **Permitir emparelhamento de dispositivos:** Para dispositivos registrados via ABM, se você pode gerenciá-los através do Apple Music e do Apple Configurator. O padrão é **Não**.

Versão mínima necessária

- **Permitir que dispositivos antigos se registrem**: Se ativado, os dispositivos podem se registrar mesmo que não possam ser atualizados para a versão mínima exigida atual. O padrão é Ativado. Esta opção está disponível apenas no iOS 17.0 e posterior.
- **Opção de versão especificada**: Se permite que o administrador insira a versão especificada manualmente. O padrão é **Desativado**. Esta opção está disponível apenas no iOS 17.0 e posterior.
- **Versões iOS disponíveis**: Você pode escolher as versões iOS disponíveis na lista. Se o dispositivo tiver uma versão iOS inferior à versão atual, ele iniciará o processo de atualização no dispositivo. Se a versão expirar no futuro, será usada uma versão mínima da lista de versões disponíveis. O padrão é **Nenhum**, não terá efeito quando definido como **Nenhum**. Esta opção está disponível apenas no iOS 17.0 e posterior.
- **Versão especificada**: Se o dispositivo tiver uma versão iOS inferior à versão atual, ele iniciará o processo de atualização no dispositivo. Se a versão expirar no futuro, será usada uma versão mínima da lista de versões disponíveis. Certifique-se de inserir o número da versão correto para evitar erros inesperados.

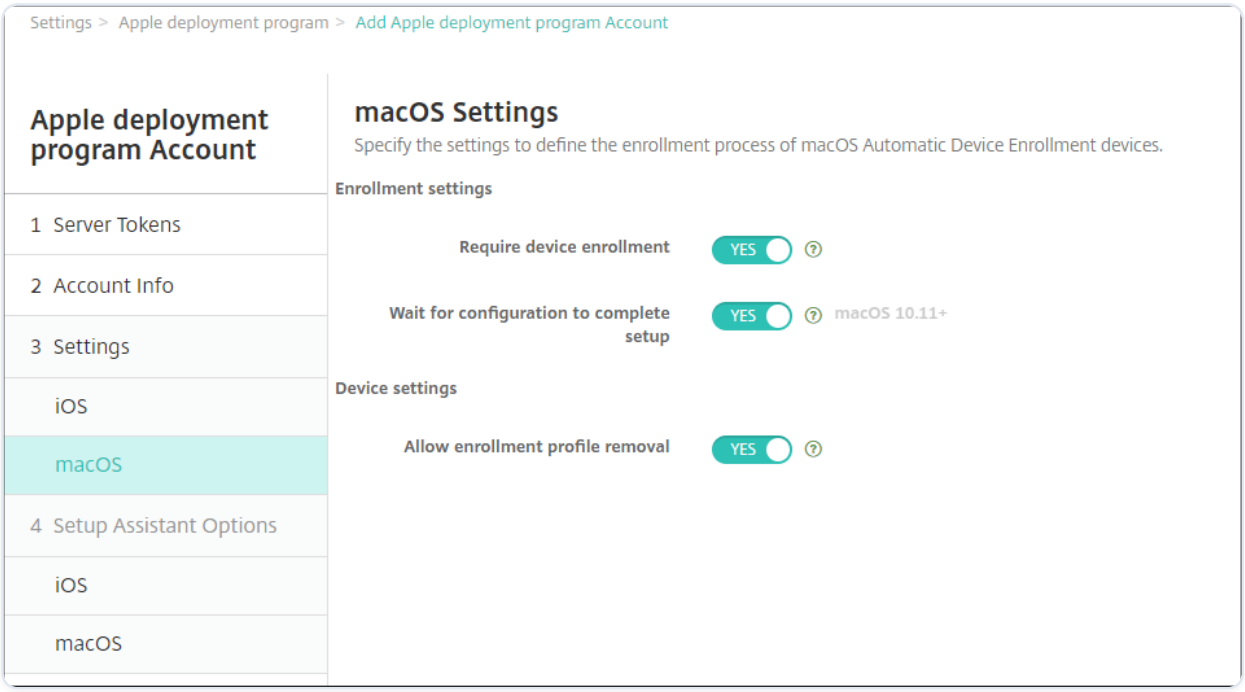
Identidades de Supervisão

Se você usar a ferramenta GroundControl, poderá adicionar um certificado para fazer o seguinte:

- Ignorar restrições de emparelhamento para evitar o prompt "Confiar neste host".
- Escalonar ações de dispositivo gerenciado via USB para realizar atividades como instalação de perfil sem interação do usuário. Isso permite que o GroundControl ative o modo de aplicativo único e o bloqueio do dispositivo para checkout.
- Restaurar um backup para dispositivos ABM.

Para obter mais informações sobre o GroundControl, consulte o site do GroundControl.

5. Em **Configurações do macOS**, especifique estas configurações:



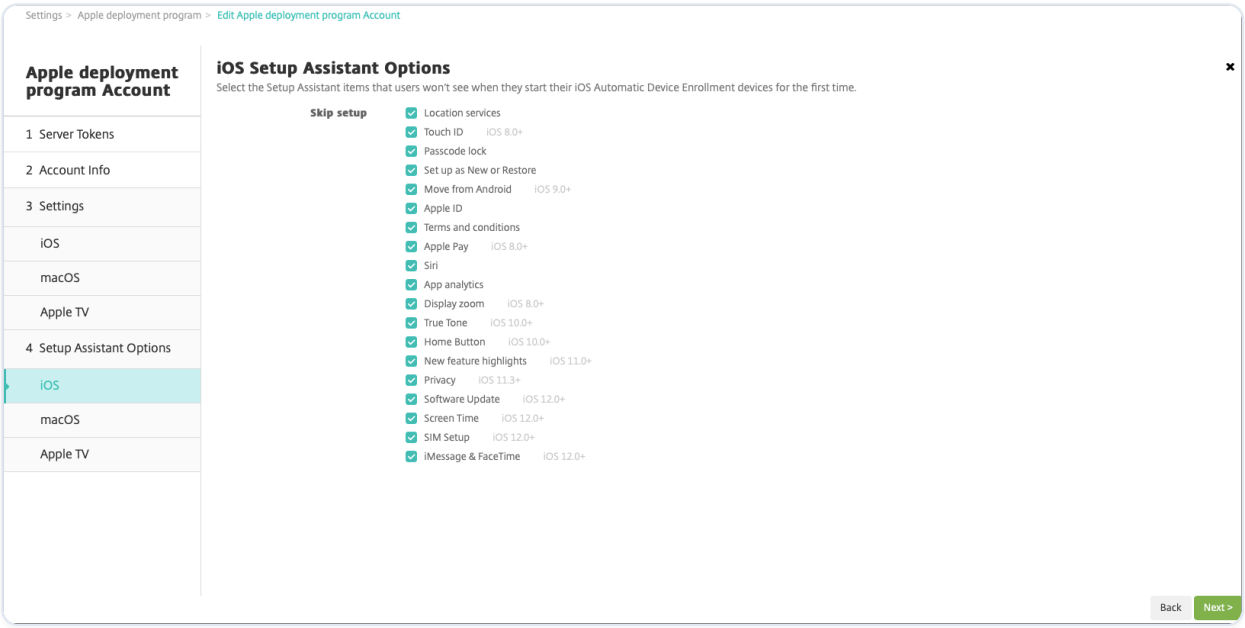
Configurações de registro

- **Exigir registro do dispositivo:** Se deve exigir que os usuários registrem seus dispositivos. O padrão é **Sim**.
- **Aguardar a conclusão da configuração:** Se **Sim**, o dispositivo macOS não continua no assistente de configuração até que a senha do recurso MDM seja implantada no dispositivo. Essa implantação ocorre antes da criação da conta local. Essa configuração está disponível para dispositivos macOS 10.11 e superiores. O padrão é **Não**.

Configurações do dispositivo

- **Permitir remoção do perfil de registro:** Se deve permitir que os dispositivos usem um perfil que você pode remover remotamente. O padrão é **Não**.

6. Em **Opções do Assistente de Configuração do iOS**, selecione as etapas que o Assistente de Configuração do iOS ignora quando os usuários iniciam seus dispositivos pela primeira vez. Quando uma tela é ignorada, o recurso relacionado usa as configurações padrão. Os usuários podem configurar os recursos ignorados após a conclusão da configuração, a menos que você restrinja completamente o acesso a esses recursos. Para obter mais informações sobre como restringir o acesso a recursos, consulte Política de dispositivo de restrições. O padrão para todos os itens é desmarcado. As descrições a seguir explicam o que ocorre quando uma configuração é selecionada.

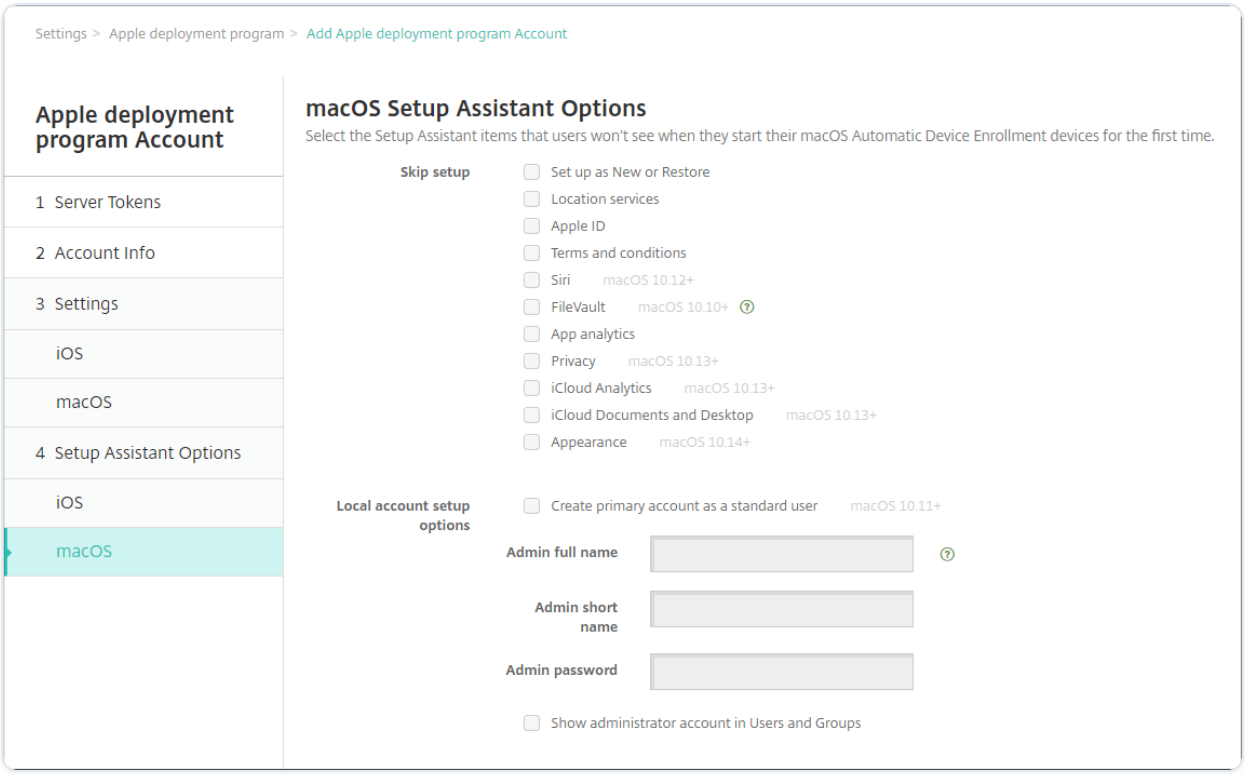


- **Serviços de localização:** Impede que os usuários configurem o serviço de localização no dispositivo.
- **Touch ID:** Impede que os usuários configurem o Touch ID ou o Face ID em dispositivos iOS. Obsoleto no iOS 15.
- **Bloqueio por código:** Impede que os usuários configurem um código para o dispositivo. Se nenhum código existir, os usuários não poderão usar o Touch ID ou o Apple Pay.
- **Configurar como novo ou restaurar:** Impede que os usuários configurem o dispositivo como novo ou a partir de um backup do iCloud ou da Apple App Store.
- **Migrar do Android:** Impede que os usuários transfiram dados de um dispositivo Android para um dispositivo iOS. Esta opção está disponível apenas quando **Configurar como novo ou restaurar** é selecionado (ou seja, a etapa é ignorada).
- **Apple ID:** Impede que os usuários configurem uma conta de ID Apple Gerenciado para o dispositivo.
- **Termos e condições:** Impede que os usuários leiam e aceitem os termos e condições de uso do dispositivo.
- **Apple Pay:** Impede que os usuários configurem o Apple Pay. Se esta configuração for desmarcada, os usuários devem configurar o Touch ID e o Apple ID. Certifique-se de que essas configurações estejam desmarcadas.
- **Siri:** Impede que o usuário configure a Siri.
- **Análise de aplicativos:** Impede que os usuários configurem se desejam compartilhar dados de falhas e estatísticas de uso com a Apple.

- **Zoom da tela:** Impede que os usuários configurem a resolução da tela (padrão ou ampliada) em dispositivos iOS. Obsoleto no iOS 17.
- **True Tone:** Impede que os usuários configurem sensores de quatro canais para ajustar dinamicamente o balanço de branco da tela.
- **Botão Início:** Impede que os usuários configurem o estilo de feedback do botão Início. Obsoleto no iOS 15.
- **Destaques de novos recursos:** Impede que os usuários vejam telas que exibem informações sobre novos recursos do software Apple.
- **Privacidade:** Impede que os usuários vejam o painel de dados e privacidade. Para iOS 11.3 e posterior.
- **Atualização de software:** Impede que os usuários atualizem o iOS para a versão mais recente. Para iOS 12.0 e posterior.
- **Tempo de Uso:** Impede que os usuários ativem o Tempo de Uso. Para iOS 12.0 e posterior.
- **Configuração do SIM:** Impede que os usuários configurem um plano de celular. Para iOS 12.0 e posterior.
- **iMessage e FaceTime:** Impede que os usuários ativem o iMessage e o FaceTime. Para iOS 12.0 e posterior.
- **Aparência:** Impede que os usuários selecionem o modo de aparência. Para iOS 13.0 e posterior.
- **Boas-vindas:** Impede que o usuário veja a tela **Começar**. Para iOS 13.0 e posterior.
- **Restauração concluída:** Impede que os usuários vejam se uma restauração é concluída durante a configuração. Para iOS 14.0 e posterior.
- **Atualização concluída:** Impede que os usuários vejam se uma atualização de software é concluída durante a configuração. Para iOS 14.0 e posterior.
- **Botão de Ação:** Impede que os usuários vejam o painel de configuração do Botão de Ação. Para iOS 17.0 e posterior.
- **Modo de Bloqueio:** Impede que os usuários vejam o painel do Modo de Bloqueio se uma Conta Apple estiver configurada. Para iOS 17.1 e posterior.
- **Inteligência:** Impede que os usuários vejam o painel de Inteligência. Para iOS 18.0 e posterior.
- **Botão da Câmera:** Impede que os usuários vejam o painel do Botão da Câmera. Para iOS 18.0 e posterior.

A conta ABM aparece em **Ajustes > Programa de Implantação da Apple**.

7. Em **Opções do Assistente de Configuração do macOS**, selecione as etapas que o Assistente de Configuração do macOS ignora quando os usuários iniciam seus dispositivos pela primeira vez. Quando uma tela é ignorada, o recurso relacionado usa as configurações padrão. Os usuários podem configurar os recursos ignorados após a conclusão da configuração, a menos que você restrinja completamente o acesso a esses recursos. Para obter mais informações sobre como restringir o acesso a recursos, consulte Política de dispositivo de restrições. O padrão para todos os itens é desmarcado. As descrições a seguir explicam o que ocorre quando uma configuração é selecionada.



- **Configurar como novo ou restaurar:** Impede que os usuários configurem o dispositivo como novo ou a partir de um backup do Time Machine ou façam uma migração do sistema.
- **Serviços de localização:** Impede que os usuários configurem o serviço de localização no dispositivo. Para macOS 10.11 e posterior.
- **ID Apple:** Impede que os usuários configurem uma conta de ID Apple Gerenciado para o dispositivo.
- **Termos e condições:** Impede que os usuários leiam e aceitem os termos e condições de uso do dispositivo.
- **Siri:** Impede que o usuário configure a Siri. Para macOS 10.12 e posterior.

- **FileVault:** Use o FileVault para criptografar o disco de inicialização. O XenMobile aplica a configuração do FileVault somente se o sistema tiver uma única conta de usuário local e essa conta estiver conectada ao iCloud.

  Você pode usar o recurso de Criptografia de Disco FileVault do macOS para proteger o volume do sistema criptografando seu conteúdo (https://support.apple.com/pt-br/HT204837). Se você executar o assistente de configuração em um Mac portátil de modelo recente que não tenha o FileVault ativado, poderá ser solicitado a ativar esse recurso. O prompt aparece em sistemas novos e em sistemas atualizados para OS X 10.10 ou 10.11, mas somente se o sistema tiver uma única conta de administrador local e essa conta estiver conectada ao iCloud.
- **Análise de aplicativos:** Impede que os usuários configurem se desejam compartilhar dados de falhas e estatísticas de uso com a Apple.
- **Privacidade:** Impede que os usuários vejam o painel Dados e privacidade. Para macOS 10.13 e posterior.
- **Análise do iCloud:** Impede que os usuários escolham se desejam enviar dados de diagnóstico do iCloud para a Apple. Para macOS 10.13 e posterior.
- **Documentos e Mesa do iCloud:** Impede que os usuários configurem a Mesa e os Documentos do iCloud. Para macOS 10.13 e posterior.
- **Aparência:** Impede que os usuários selecionem o modo de aparência. Para macOS 10.14 e posterior.
- **Acessibilidade:** Impede que o usuário ouça o Voice Over automaticamente. Disponível apenas se o dispositivo estiver conectado ao Ethernet. Para macOS 11 e posterior.
- **Biométrico:** Impede o usuário de configurar o Touch ID e o Face ID. Para macOS 10.12.4 e posterior.
- **True Tone:** Impede os usuários de configurar sensores de quatro canais para ajustar dinamicamente o balanço de branco da tela. Para macOS 10.13.6 e posterior.
- **Apple Pay:** Impede os usuários de configurar o Apple Pay. Se esta configuração for desmarcada, os usuários devem configurar o Touch ID e o Apple ID. Certifique-se de que as configurações de **Apple ID** e **Biométrico** estejam desmarcadas. Para macOS 10.12.4 e posterior.
- **Tempo de Uso:** Impede os usuários de habilitar o Tempo de Uso. Para macOS 10.15 e posterior.

- **Opções de configuração de conta local:** Especifique as configurações para criar uma conta de administrador no dispositivo. Os usuários fazem login em seu dispositivo macOS com essas informações. O XenMobile cria a conta, usando as informações especificadas.
    - **Criar conta principal como usuário padrão:** Em vez de conceder a este usuário privilégios de administrador no dispositivo, o XenMobile cria o usuário com permissões padrão. Como o macOS exige uma conta de administrador, o XenMobile cria uma conta de administrador primeiro, depois cria uma nova conta padrão e a define como principal.
    - **Nome completo do administrador:** Digite o nome que o sistema exibe para a conta de administrador.
    - **Nome abreviado do administrador:** Digite o nome que o dispositivo exibe para a pasta pessoal e no shell.
    - **Senha do administrador:** Digite uma senha segura para a conta de administrador.
    - **Mostrar conta de administrador em Usuários e Grupos:** Se desmarcada, a conta de administrador não aparece em **Usuários e Grupos** nas configurações do macOS. Se você criar a conta principal como um usuário padrão, habilite esta configuração para ocultar a conta de administrador que o XenMobile cria primeiro.

Solicitar dispositivos habilitados para o Programa de Implantação

Você pode solicitar dispositivos habilitados para o Programa de Implantação diretamente da Apple ou de revendedores ou operadoras autorizados habilitados para o Programa de Implantação. Para solicitar da Apple, forneça seu ID de Cliente Apple no Portal do Programa de Implantação da Apple. Seu ID de Cliente permite que a Apple associe seus dispositivos comprados à sua conta do Programa de Implantação da Apple.

Para fazer o pedido ao seu revendedor ou operadora, entre em contato com seu revendedor ou operadora Apple para verificar se eles participam do Programa de Implementação da Apple. Solicite o ID do Programa de Implementação da Apple do revendedor ao comprar dispositivos. A Apple exige essa informação ao adicionar seu revendedor do Programa de Implementação da Apple à sua conta do programa. Após adicionar o ID do Programa de Implementação da Apple para o revendedor, você receberá um ID de cliente do programa. Forneça o ID de cliente do programa ao revendedor, que o utilizará para enviar informações sobre suas compras de dispositivos à Apple. Para obter mais informações, consulte este site de Registro de Dispositivos da Apple.

Gerenciar dispositivos habilitados para o Programa de Implantação

Após o envio do seu pedido, você pode associar dispositivos iOS, iPadOS e macOS ao seu XenMobile Server.

1. Faça login no Apple Business Manager usando uma conta de administrador ou de gerente de registro de dispositivo.
2. Na barra lateral, clique em **Dispositivos**. Os dispositivos que você comprou diretamente da Apple aparecem automaticamente. Para atribuir dispositivos do Apple Configurator 2 ao Apple Business Manager, consulte o Guia do Usuário do Apple Business Manager.
3. Na lista, selecione um dispositivo ou o número total de dispositivos e clique em **Editar Gerenciamento de Dispositivos**. Você tem duas opções:

    - Para atribuir um dispositivo a um servidor MDM, em **Atribuir ao Servidor**, escolha o nome do seu XenMobile Server. Clique em **Continuar**.

      Para atribuir novos dispositivos ao Apple Business Manager em massa, defina um XenMobile Server padrão para implantação. Para obter mais informações, consulte Definir um servidor padrão para registro em massa.
    - Para desatribuir um dispositivo do XenMobile Server, escolha **Desatribuir**.

Seus dispositivos do Programa de Implantação da Apple agora estão associados ao XenMobile Server selecionado.

Se você enviar um dispositivo iOS, iPadOS ou macOS para manutenção, precisará remover o dispositivo do Apple Business Manager. Ao receber o dispositivo de volta após a manutenção, você deve reatribuir o dispositivo ao XenMobile Server. Ao substituir o dispositivo, você pode atribuir um novo dispositivo ao XenMobile Server usando um número de pedido.

Para revisar o histórico de dispositivos atribuídos:

1. Faça login no Apple Business Manager usando uma conta de administrador ou de gerente de registro de dispositivo.
2. Na barra lateral, clique em **Histórico de Atribuições**. Em seguida, escolha uma atribuição para ver mais informações.
3. Clique em **Baixar** para baixar um arquivo CSV com os números de série de todos os dispositivos atribuídos e não atribuídos.

Você pode remover dispositivos iOS, iPadOS e macOS do Apple Business Manager se o dispositivo tiver sido vendido, roubado ou não puder ser reparado.

1. Faça login no Apple Business Manager usando uma conta de administrador ou de gerente de registro de dispositivo.
2. Na barra lateral, clique em **Dispositivos** e procure um dispositivo.
3. Selecione um dispositivo e clique em **Liberar Dispositivo**. Na caixa de diálogo, confirme suas alterações para remover o dispositivo do programa. Para adicionar dispositivos iOS e iPadOS novamente, use o Apple Configurator 2. Você não pode adicionar dispositivos macOS novamente com o Apple Configurator 2.

Registrar dispositivos

Para gerenciar dispositivos de usuário remotamente e com segurança, você registra os dispositivos de usuário no XenMobile. O software cliente do XenMobile é instalado no dispositivo do usuário e a identidade do usuário é autenticada. Em seguida, o XenMobile e o perfil do usuário são instalados. Depois, no console do XenMobile, você pode realizar tarefas de gerenciamento de dispositivos. Você pode aplicar políticas, implantar aplicativos, enviar dados para o dispositivo e bloquear, limpar e localizar dispositivos perdidos ou roubados.

O registro do Azure Active Directory é compatível com dispositivos iOS, Android, Windows 10 e Windows 11. Para obter mais informações sobre como configurar o Azure como seu provedor de identidade (IdP), consulte Integração do XenMobile com o Azure Active Directory como IdP.

> **Nota:**
>
> Antes de registrar usuários de dispositivos iOS, você deve solicitar um certificado APNs. Para obter detalhes, consulte Certificados e autenticação.

> Para atualizar as opções de configuração para usuários e dispositivos, vá para a página **Gerenciar > Convites de Registro**. Para obter detalhes, consulte Enviar um convite de registro neste artigo.

Dispositivos Android

> **Nota:**
>
> Para obter informações sobre como registrar dispositivos Android Enterprise, consulte Android Enterprise.

1. Vá para a Google Play Store no seu dispositivo Android, baixe o aplicativo Citrix Secure Hub™ e, em seguida, toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, clique em **Avançar** e, em seguida, clique em **Instalar**.
3. Após a instalação do Secure Hub, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome do seu XenMobile Server, Nome Principal do Usuário (UPN) ou endereço de e-mail. Em seguida, clique em **Avançar**.
5. Na tela **Ativar administrador do dispositivo**, toque em **Ativar**.
6. Insira sua senha corporativa e, em seguida, toque em **Entrar**.
7. Dependendo de como o XenMobile está configurado, pode ser solicitado que você crie um PIN Citrix. Você pode usar o PIN para fazer login no Secure Hub e em outros aplicativos habilitados para XenMobile, como Secure Mail e Citrix Files. Você insere seu PIN Citrix duas vezes. Na tela **Criar PIN Citrix**, insira um PIN.
8. Reinsira o PIN. O Secure Hub é aberto. Você pode então acessar a Loja XenMobile para visualizar os aplicativos que pode instalar em seu dispositivo Android.
9. Se você configurou o XenMobile para enviar aplicativos para dispositivos automaticamente após o registro, os usuários são solicitados a instalar os aplicativos. Além disso, as políticas que você configura no XenMobile são implantadas no dispositivo. Toque em **Instalar** para instalar o aplicativo.

Para cancelar o registro e registrar novamente um dispositivo Android

Os usuários podem cancelar o registro de dentro do Secure Hub. Quando os usuários cancelam o registro usando o procedimento a seguir, o dispositivo ainda aparece no inventário de dispositivos no console do XenMobile. No entanto, você não pode realizar ações no dispositivo. Você não pode rastrear o dispositivo e não pode monitorar a conformidade do dispositivo.

1. Toque para abrir o aplicativo Secure Hub.
2. Dependendo se você tem um telefone ou um tablet, faça o seguinte:

   Em um telefone:

   - Deslize da esquerda da tela para abrir um painel de configurações.
   - Toque em **Preferências**, toque em **Contas** e, em seguida, toque em **Excluir Conta**.

   Em um tablet:

   - Toque na seta ao lado do seu endereço de e-mail no canto superior direito.

- Toque em **Preferências**, toque em **Contas** e, em seguida, toque em **Excluir Conta**.

3. Toque em **Registrar Novamente**. Uma mensagem aparece para confirmar que você deseja registrar novamente seu dispositivo.
4. Toque em **OK**.

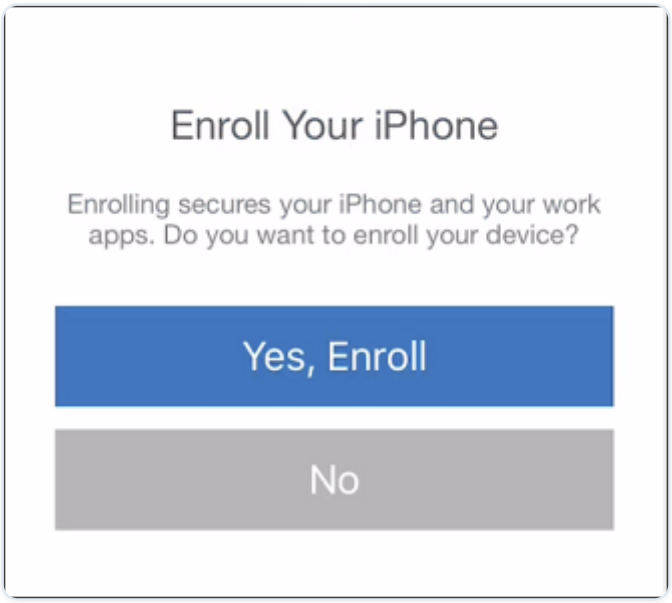
   Seu dispositivo não está registrado.
5. Siga as instruções na tela para registrar novamente seu dispositivo.

Registrar dispositivos iOS

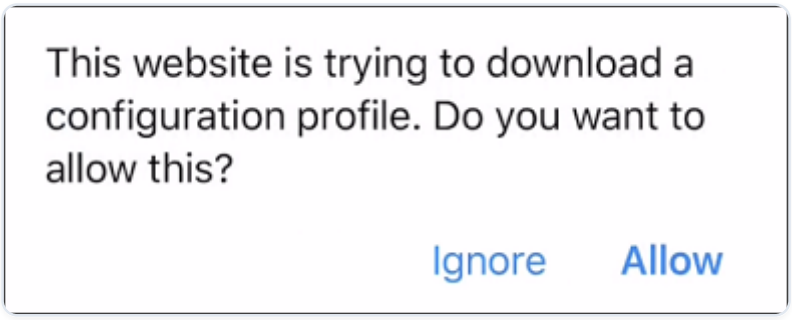
Esta seção mostra como os usuários registram dispositivos iOS (12.2 ou posterior) no XenMobile Server. Para obter mais informações sobre o registro de iOS, abra o seguinte vídeo:



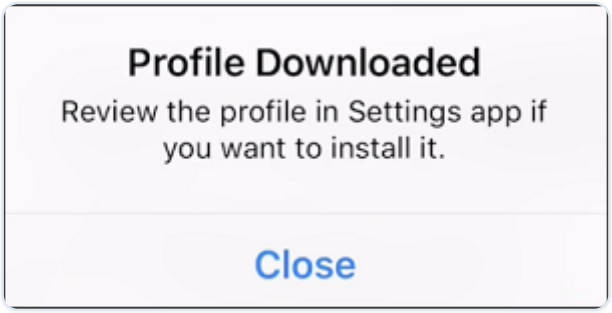
1. Vá para a App Store no seu dispositivo iOS, baixe o aplicativo Citrix Secure Hub e, em seguida, toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, toque em **Avançar** e, em seguida, toque em **Instalar**.
3. Após a instalação do Secure Hub, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome do seu XenMobile Server, Nome Principal de Usuário (UPN) ou endereço de e-mail. Em seguida, clique em **Avançar**.
5. Toque em **Sim, Registrar** para registrar seu dispositivo iOS.



6. Depois de digitar suas credenciais, toque em **Permitir** quando solicitado, para baixar o perfil de configuração.

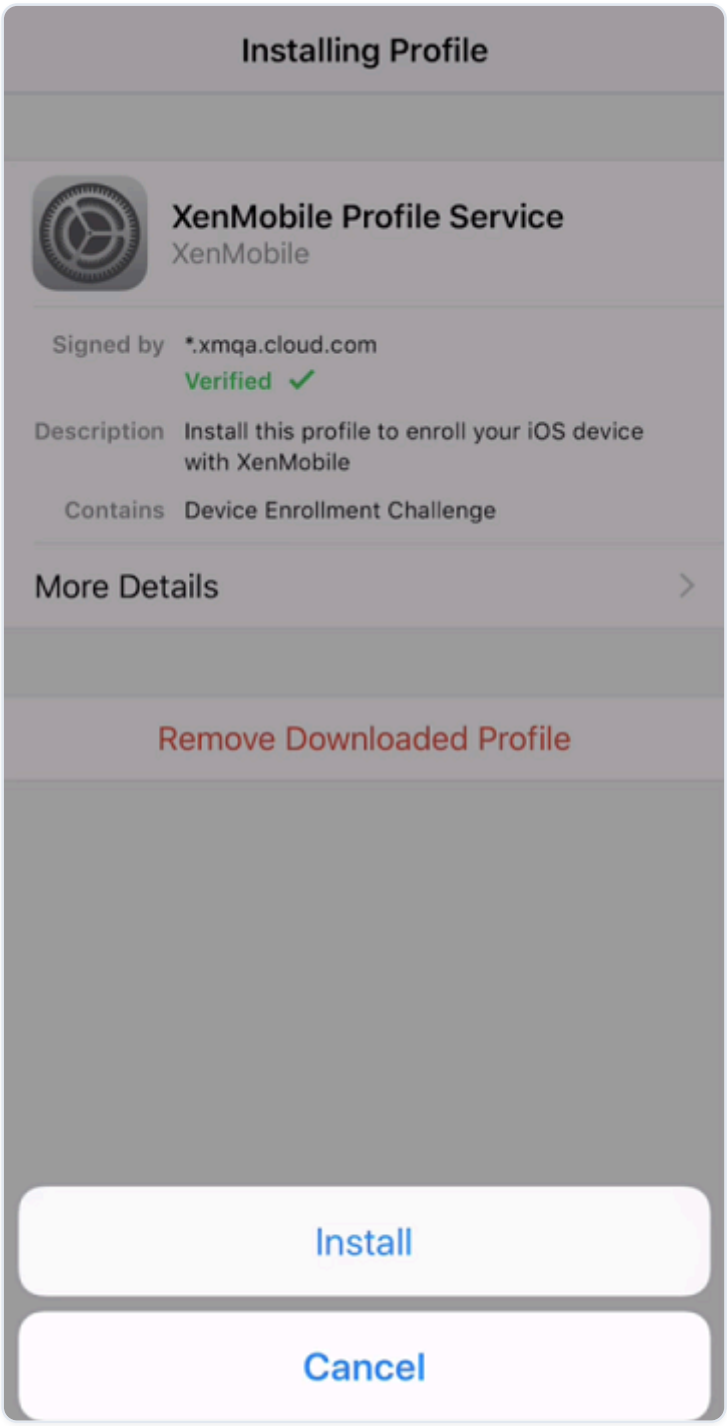


7. Depois de baixar o perfil de configuração, toque em **Fechar**.

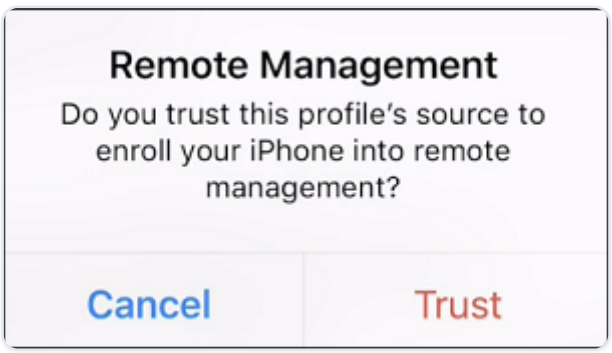


8. Nas configurações do seu dispositivo, instale o certificado iOS e adicione o dispositivo à lista confiável.

    - Vá para **Ajustes > Geral > Perfil > XenMobile Profile Service** e toque em **Instalar** para adicionar o perfil.



- Na janela de notificação, toque em **Confiar** para registrar seu dispositivo no gerenciamento remoto.



9. Faça login no Secure Hub. Se você estiver se registrando no MDM+MAM: Após a validação de suas credenciais, crie e confirme seu PIN Citrix quando solicitado.
10. Após a conclusão do fluxo de trabalho, o dispositivo é registrado. Você pode então acessar a loja de aplicativos para visualizar os aplicativos que pode instalar em seu dispositivo iOS.

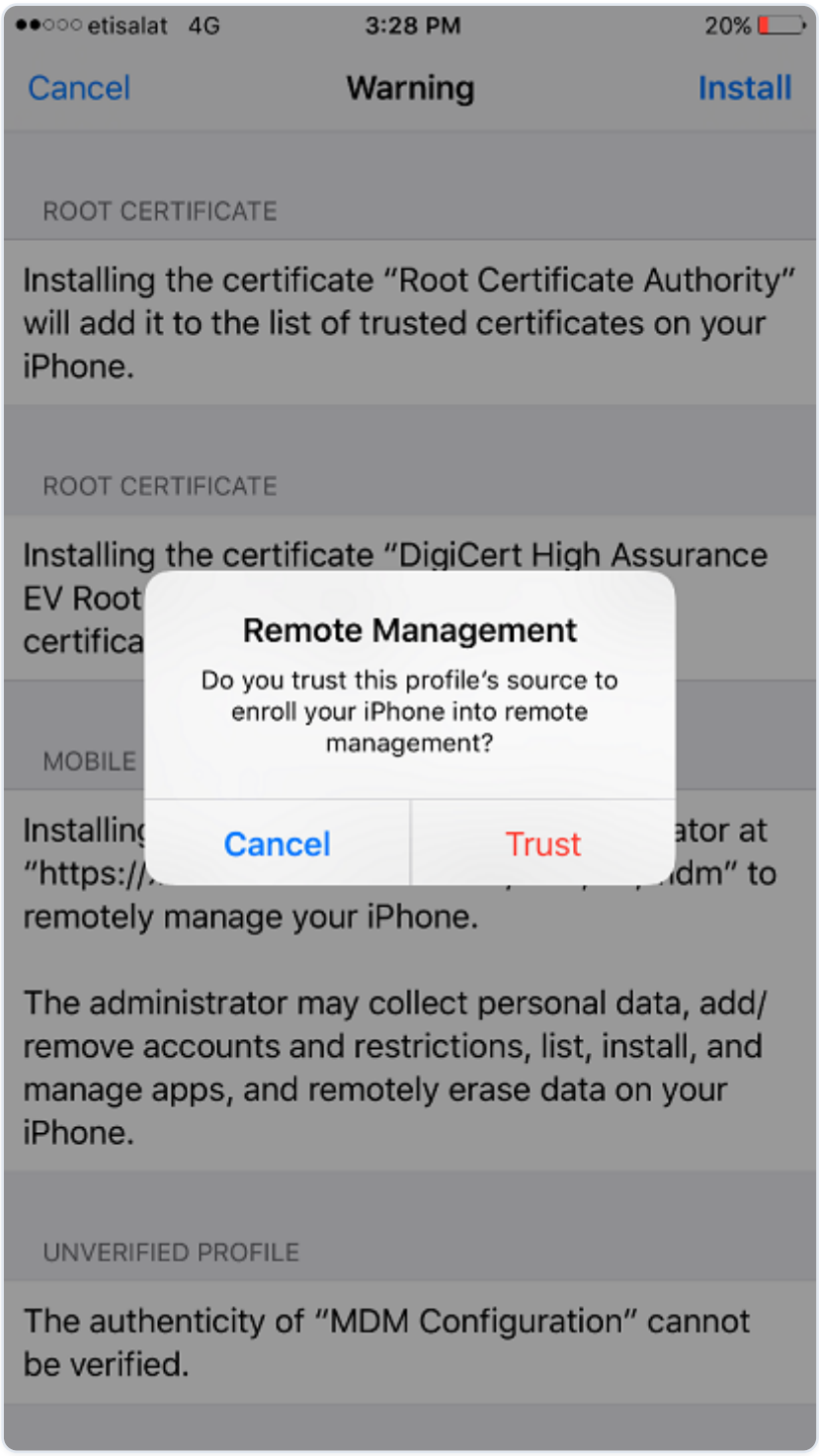
Dispositivos iOS

1. Baixe o aplicativo Secure Hub na Apple iTunes App Store no dispositivo e, em seguida, instale o aplicativo no dispositivo.
2. Na tela inicial do dispositivo iOS, toque no aplicativo Secure Hub.
3. Quando o aplicativo Secure Hub abrir, insira o endereço do servidor fornecido pelo seu suporte técnico.

   As telas apresentadas podem diferir desses exemplos, dependendo de como o XenMobile está configurado.
4. Quando solicitado, insira seu nome de usuário e senha ou PIN. Clique em **Avançar**.
5. Quando solicitado a registrar, clique em **Sim, Registrar** e, em seguida, insira suas credenciais quando solicitado.
6. Toque em **Instalar** para instalar os Serviços de Perfil Citrix.



7. Toque em **Confiar**.



8. Toque em **Abrir** e, em seguida, insira suas credenciais.

Dispositivos macOS

O XenMobile oferece dois métodos para registrar dispositivos que executam macOS. Ambos os métodos permitem que os usuários de macOS se registrem sem fio, diretamente de seus dispositivos.

- **Enviar aos usuários um convite de registro:** Este método de registro permite definir qualquer um dos seguintes modos de segurança de registro para dispositivos macOS:

- Nome de usuário + senha
- Nome de usuário + PIN
- Dois Fatores

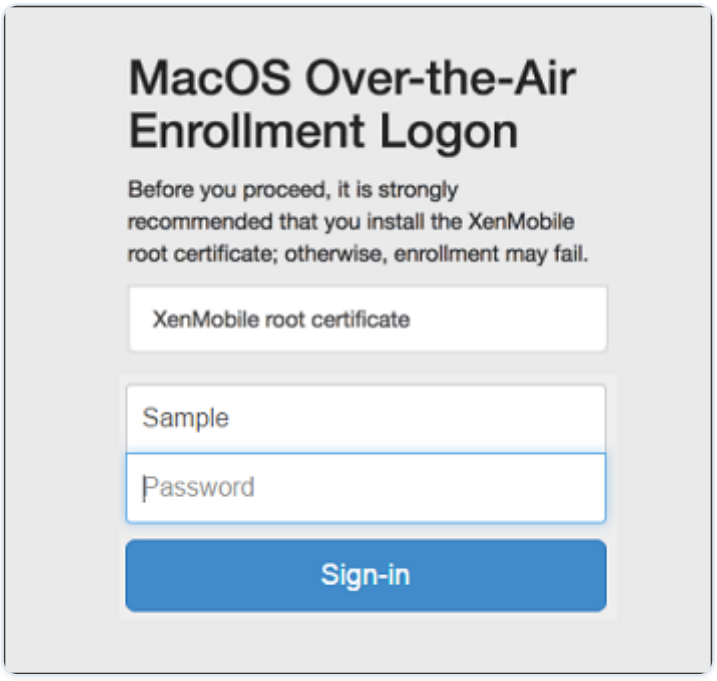
Quando o usuário segue as instruções no convite de registro, uma tela de logon com o nome de usuário preenchido é exibida.

- **Enviar aos usuários um link de instalação:** Este método de registro para dispositivos macOS envia aos usuários um link de registro, que eles podem abrir nos navegadores Safari ou Chrome. Um usuário então se registra inserindo seu nome de usuário e senha.

  Para evitar o uso de um link de registro para dispositivos macOS, defina a propriedade do servidor **Enable macOS OTAE** como **false**. Como resultado, os usuários de macOS podem se registrar apenas usando um convite de registro.

Enviar aos usuários um convite de registro

1. Opcionalmente, configure políticas de dispositivo macOS no console do XenMobile. Para obter mais informações sobre políticas de dispositivo, consulte Políticas de Dispositivo.
2. Adicione um convite para o registro de usuário do macOS. Para obter mais informações, consulte Enviar um convite de registro neste artigo.
3. Depois que os usuários recebem o convite e clicam no link, a seguinte tela aparece no navegador Safari. O XenMobile preenche o nome de usuário. Se você escolheu **Dois Fatores** para o modo de segurança de registro, outro campo aparece.



4. Os usuários instalam os certificados conforme necessário. Se os usuários veem o prompt para instalar certificados depende se você configurou o seguinte para macOS: Um certificado SSL publicamente confiável e um certificado de assinatura digital publicamente confiável. Para obter mais informações sobre certificados, consulte Certificados e autenticação.
5. Os usuários fornecem as credenciais solicitadas.

   As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar Macs com o XenMobile da mesma forma que gerencia dispositivos móveis.

Enviar um link de instalação aos usuários

1. Opcionalmente, configure políticas de dispositivo macOS no console do XenMobile. Para obter mais informações sobre políticas de dispositivo, consulte Políticas de Dispositivo.
2. Envie o link de registro `https://serverFQDN:8443/instanceName/macos/otae`, que os usuários podem abrir nos navegadores Safari ou Chrome.

   - **serverFQDN** é o nome de domínio totalmente qualificado (FQDN) do servidor que executa o XenMobile.
   - A porta **8443** é a porta segura padrão. Se você configurou uma porta diferente, use essa porta em vez de 8443.
   - O **instanceName**, frequentemente exibido como zdm, é o nome especificado durante a instalação do servidor.

   Para obter mais informações sobre como enviar links de instalação, consulte Para enviar um link de instalação.
3. Os usuários instalam os certificados conforme necessário. Se você configurou um certificado SSL publicamente confiável e um certificado de assinatura digital para iOS e macOS, os usuários veem o prompt para instalar os certificados. Para obter mais informações sobre certificados, consulte Certificados e autenticação.
4. Os usuários fazem logon em seus Macs.

   As políticas do dispositivo Mac são instaladas. Agora você pode começar a gerenciar Macs com o XenMobile da mesma forma que gerencia dispositivos móveis.

Dispositivos Windows

Dispositivos Windows 10 e Windows 11 são registrados no Azure como um meio federado de autenticação do Active Directory. Você pode unir dispositivos Windows 10 e Windows 11 ao Microsoft Azure AD de qualquer uma das seguintes maneiras:

- Registrar no MDM como parte da junção ao Azure AD (Azure AD Join) pronta para uso na primeira vez que o dispositivo é ligado.
- Registrar no MDM como parte da junção ao Azure AD (Azure AD Join) na página Configurações do Windows depois que o dispositivo for configurado.

Você pode registrar dispositivos no XenMobile que estejam executando os seguintes sistemas operacionais Windows:

- Windows 10
- Windows 11

Os usuários podem se registrar diretamente por meio de seus dispositivos.

> **Nota:**
>
> Para Windows 10 RS2 Phone e Tablet, durante o novo registro, o usuário não é solicitado a informar a URL do Servidor. Para contornar esse problema, reinicie o dispositivo. Ou, na tela de endereço de e-mail, toque no X ao lado de **Conectando a um serviço** para ir para a página da URL do Servidor. Este é um problema de terceiros.

> Você deve configurar o AutoDiscovery e o serviço de descoberta do Windows para o registro de usuários para habilitar o gerenciamento de dispositivos Windows compatíveis.

Antes que os usuários de dispositivos Windows possam se registrar usando o Azure, você deve configurar as configurações do servidor Microsoft Azure no XenMobile. Para obter detalhes, consulte Configurações do servidor Microsoft Azure Active Directory.

Para registrar dispositivos Windows com autodescoberta

Para habilitar o gerenciamento de dispositivos Windows, a Citrix recomenda que você configure o Serviço AutoDiscovery e o serviço de descoberta do Windows. Para obter detalhes, consulte Serviço AutoDiscovery do XenMobile.

1. No dispositivo, verifique e instale todas as atualizações do Windows disponíveis.
2. No menu de charms, toque em **Configurações** e depois toque em **Contas > Acessar trabalho ou escola > Conectar ao trabalho ou escola**.
3. Para Windows 10 e Windows 11: Insira seu endereço de e-mail corporativo e toque em **Continuar**. Para Windows 8.1: Toque em **Ativar gerenciamento de dispositivo**. Para se

registrar como um usuário local, insira um endereço de e-mail inexistente com o nome de domínio correto (por exemplo, `foo@mydomain.com`). Isso permite que você ignore uma limitação conhecida da Microsoft onde o registro é feito pelo Gerenciamento de Dispositivo integrado no Windows; na caixa de diálogo **Conectando a um serviço**, insira o nome de usuário e a senha associados ao usuário local. O dispositivo encontra automaticamente um XenMobile Server e inicia o processo de registro.

4. Insira sua senha. Use a senha associada a uma conta que faz parte de um grupo de usuários no XenMobile.
5. Para Windows 10 e Windows 11: Na caixa de diálogo **Termos de uso**, indique que você concorda em ter seu dispositivo gerenciado e toque em **Aceitar**. Para Windows 8.1: Na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda em ter seu dispositivo gerenciado e toque em **Ativar**.

Para registrar dispositivos Windows sem autodescoberta

É possível registrar dispositivos Windows sem AutoDiscovery. A Citrix, no entanto, recomenda que você configure o AutoDiscovery. O registro sem AutoDiscovery resulta em uma chamada para a porta 80 antes de se conectar à URL desejada, portanto, não é considerado uma prática recomendada para implantação em produção. A Citrix recomenda que você use este processo apenas em ambientes de teste e implantações de prova de conceito.

1. No dispositivo, verifique e instale todas as atualizações do Windows disponíveis.
2. Para Windows 10 e Windows 11: No menu de charms, toque em **Configurações** e depois toque em **Contas > Acessar trabalho ou escola > Conectar ao trabalho ou escola**. Para Windows 8.1: Toque em **Configurações do PC > Rede > Local de trabalho**.
3. Insira seu endereço de e-mail corporativo.
4. Para Windows 10 e Windows 11: Se o AutoDiscovery não estiver configurado, uma opção aparecerá onde você pode inserir os detalhes do servidor, conforme descrito na etapa 5. Para Windows 8.1: Se **Detectar endereço do servidor automaticamente** estiver definido como **ativado**, toque para desativar a opção **desativado**.
5. Para Windows 10 e Windows 11, no campo **Inserir endereço do servidor**, digite o endereço: `https://serverfqdn:8443/serverInstance/wpe`.

   Se uma porta diferente de 8443 for usada para conexões SSL não autenticadas, use esse número de porta no lugar de 8443 neste endereço.

   Para Windows 8.1: Digite o endereço do servidor no seguinte formato: `https://serverfqdn:8443/serverInstance/Discovery.svc`.

Se uma porta diferente de 8443 for usada para conexões SSL não autenticadas, use esse número de porta no lugar de 8443 neste endereço.

6. Digite sua senha.
7. Para Windows 10 e Windows 11: Na caixa de diálogo **Termos de uso**, indique que você concorda em ter seu dispositivo gerenciado e, em seguida, toque em **Aceitar**. Para Windows 8.1: Na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda em ter seu dispositivo gerenciado e, em seguida, toque em **Ativar**.

Enviar um convite de registro

No console do XenMobile, você pode enviar um convite de registro para usuários com dispositivos iOS, macOS, Android Enterprise e Android herdado. Você também pode enviar um link de instalação para usuários com dispositivos iOS, Android Enterprise ou Android herdado.

Os convites de registro são enviados da seguinte forma:

- Se o convite de registro for para um usuário local ou do Active Directory: O usuário recebe o convite por SMS no número de telefone e nome da operadora que você especificar.
- Se o convite de registro for para um grupo: Os usuários recebem convites por SMS. Se os usuários do Active Directory tiverem um endereço de e-mail e número de telefone celular no Active Directory, eles receberão o convite. Os usuários locais recebem o convite no e-mail e número de telefone especificados nas propriedades do usuário.

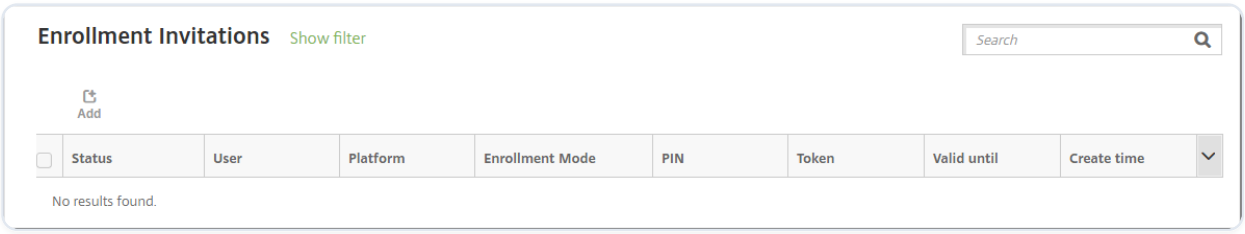
Depois que os usuários se registram, seus dispositivos aparecem como gerenciados em **Gerenciar > Dispositivos**. O status da URL do convite é mostrado como **Resgatado**.

Pré-requisitos

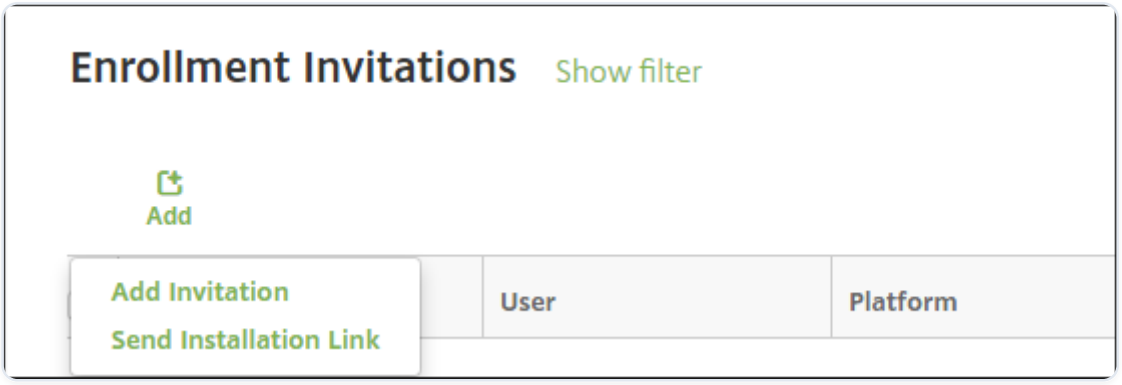
- XenMobile Server configurado no modo Enterprise (XME) ou MDM
- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
  - Um ou mais grupos locais.
  - Usuários locais atribuídos a grupos locais.
  - Grupos de entrega estão associados a grupos locais.
- Se estiver usando o Active Directory:
  - Os grupos de entrega estão associados aos grupos do Active Directory.

Criar um convite de inscrição

1. No console do XenMobile, clique em **Gerenciar > Convites de Inscrição**. A página **Convites de Inscrição** é exibida.



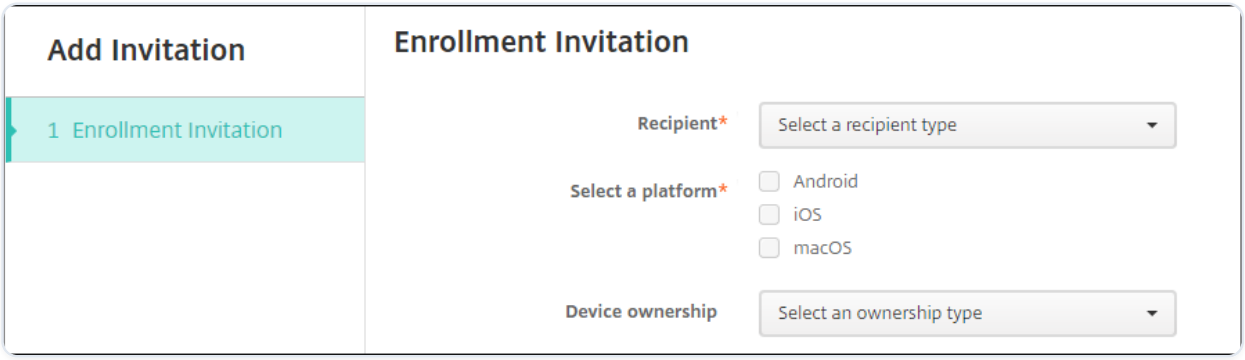
2. Clique em **Adicionar**. Um menu de opções de inscrição é exibido.



   - Para enviar um convite de inscrição para um usuário ou grupo, clique em **Adicionar Convite**.
   - Para enviar um link de instalação de inscrição para uma lista de destinatários via SMTP ou SMS, clique em **Enviar Link de Instalação**.

   O envio de convites de inscrição e links de instalação é descrito após estas etapas.

3. Clique em **Adicionar Convite**. A tela **Convite de Inscrição** é exibida.



4. Configure estas configurações:

   - **Destinatário:** Escolha **Grupo** ou **Usuário**.

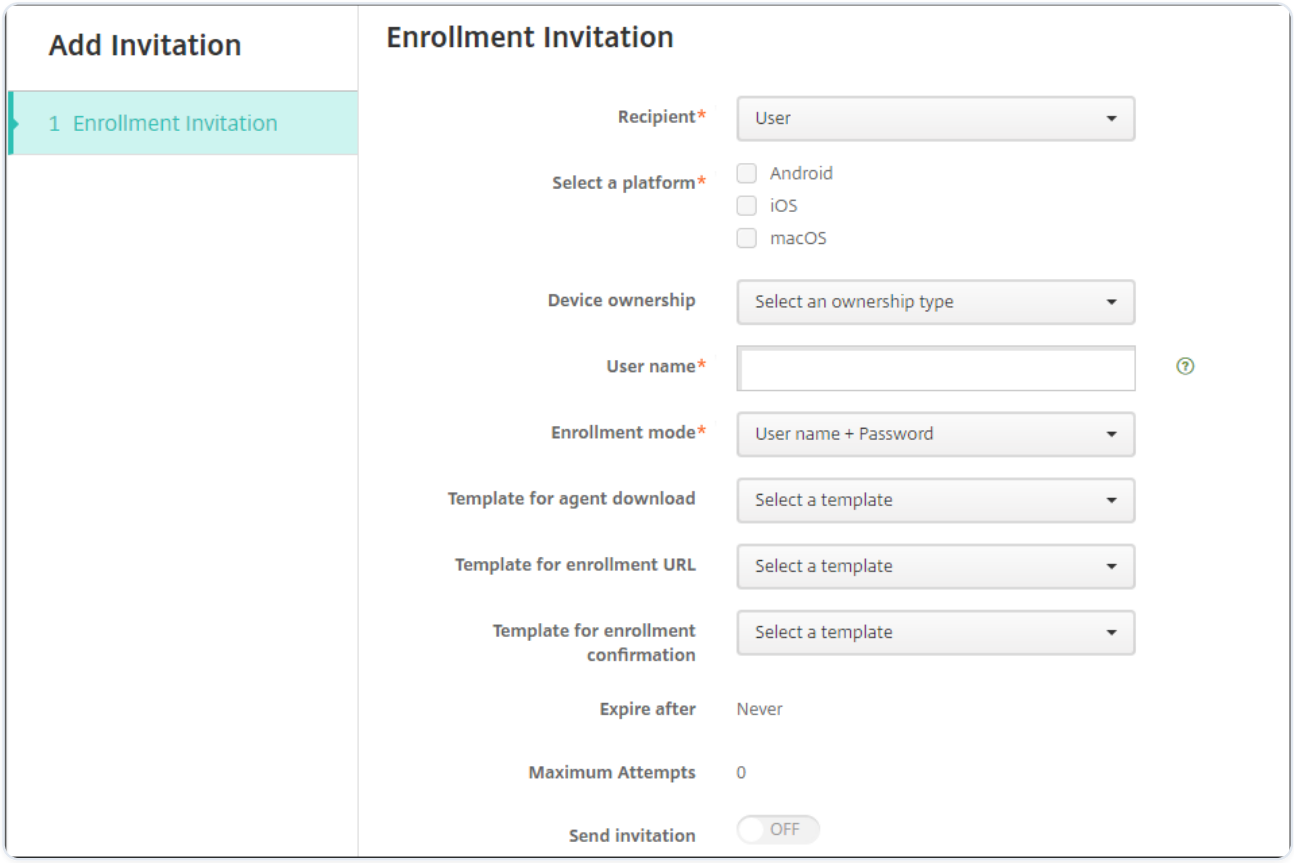
- **Selecionar uma plataforma:** Se **Destinatário** for **Grupo**, todas as plataformas são selecionadas. Você pode alterar a seleção da plataforma. Se **Destinatário** for **Usuário**, nenhuma plataforma é selecionada. Selecione uma plataforma.

  Para criar um convite de inscrição para dispositivos Android Enterprise, selecione **Android > Android Enterprise**.

- **Propriedade do dispositivo:** Selecione **Corporativo** ou **Funcionário**.

As configurações para usuários ou grupos aparecem, conforme descrito nas seções a seguir.

Para enviar um convite de inscrição a um usuário



1. Configure estas configurações de **Usuário**:

   - **Nome de usuário:** Digite um nome de usuário. O usuário deve existir no XenMobile Server como um usuário local ou como um usuário no Active Directory. Se o usuário for local, certifique-se de que a propriedade de e-mail do usuário esteja definida para que você possa enviar notificações a esse usuário. Se o usuário estiver no Active Directory, certifique-se de que o LDAP esteja configurado.
   - **Informações do dispositivo:** Esta configuração não aparece se você selecionar várias plataformas ou se selecionar apenas macOS. Escolha **Número de série**, **UDID** ou **IMEI**.

Depois de escolher uma opção, um campo aparece onde você pode digitar o valor correspondente para o dispositivo.

- **Número de telefone:** Esta configuração não aparece se você selecionar várias plataformas ou se selecionar apenas macOS. Opcionalmente, digite o número de telefone do usuário.
- **Operadora:** Esta configuração não aparece se você selecionar várias plataformas ou se selecionar apenas macOS. Escolha uma operadora para associar ao número de telefone do usuário.
- **Modo de inscrição:** Escolha o modo de segurança de inscrição para os usuários. O padrão é **Nome de usuário + Senha**. Algumas das opções a seguir não estão disponíveis para todas as plataformas:
  - Nome de usuário + Senha
  - Alta Segurança
  - URL de Convite
  - URL de Convite + PIN
  - URL de Convite + Senha
  - Dois Fatores
  - Nome de usuário + PIN

Para enviar convites de inscrição, você só pode usar os modos de segurança de inscrição **URL de Convite**, **URL de Convite + PIN** ou **URL de Convite + Senha**. Para dispositivos que se inscrevem com **Nome de usuário + Senha**, **Dois Fatores** ou **Nome de usuário + PIN**, os usuários devem inserir manualmente suas credenciais no Secure Hub.

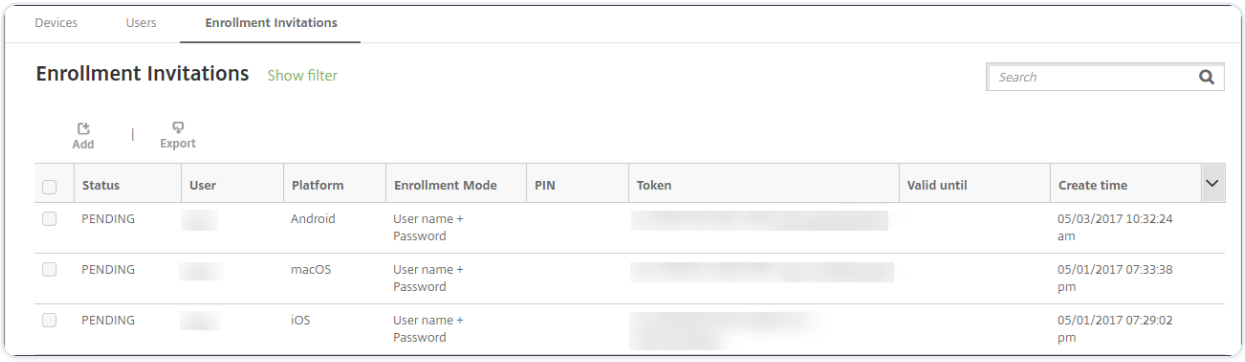
Um PIN para inscrição também é chamado de PIN de uso único. Esses PINs são válidos apenas quando o usuário se inscreve.

> **Nota:**
>
> Quando você seleciona qualquer modo de segurança de inscrição que inclua um PIN, o campo **Modelo para PIN de inscrição** aparece, onde você clica em **PIN de inscrição**.

- **Modelo para download do agente:** Escolha o modelo de link de download chamado **Link de download**. Esse modelo é para todas as plataformas suportadas.

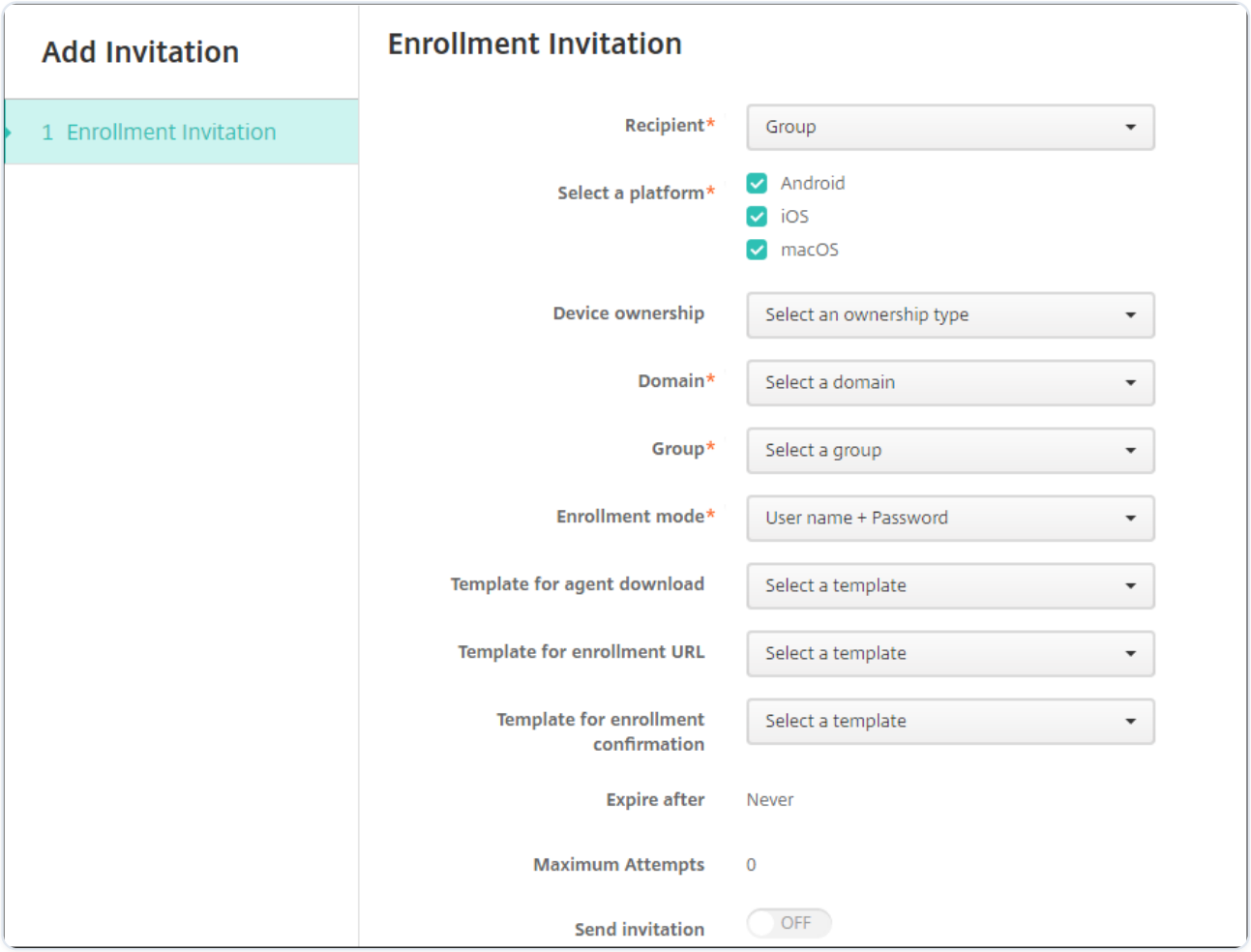
- **Modelo para URL de inscrição:** Escolha **Convite de Inscrição**.
- **Modelo para confirmação de inscrição:** Escolha **Confirmação de Inscrição**.
- **Expirar após:** Este campo é definido quando você configura o Modo de Inscrição e indica quando a inscrição expira. Para obter mais informações sobre como configurar modos de segurança de inscrição, consulte Configurar modos de segurança de inscrição.
- **Tentativas Máximas:** Este campo é definido quando você configura o **Modo de Inscrição** e indica o número máximo de vezes que o processo de inscrição ocorre. Para obter mais informações sobre como configurar modos de segurança de inscrição, consulte Configurar modos de segurança de inscrição.
- **Enviar convite:** Selecione **ATIVADO** para enviar o convite imediatamente. Selecione **DESATIVADO** para adicionar o convite à tabela na página **Convites de Inscrição**, mas não enviá-lo.

2. Clique em **Salvar e Enviar** se você ativou **Enviar convite**. Caso contrário, clique em **Salvar**. O convite aparece na tabela na página **Convites de Inscrição**.



Para enviar um convite de inscrição a um grupo

A figura a seguir mostra as configurações para configurar um convite de inscrição para um grupo.



1. Configure estas configurações:

   - **Domínio:** Escolha o domínio do grupo para receber o convite.
   - **Grupo:** Escolha o grupo para receber o convite.
   - **Modo de inscrição:** Escolha como você deseja que os usuários do grupo se inscrevam. O padrão é **Nome de usuário + Senha**. Algumas das opções a seguir não estão disponíveis para todas as plataformas:

     - Nome de usuário + Senha
     - Alta Segurança
     - URL de Convite
     - URL de Convite + PIN
     - URL de Convite + Senha
     - Dois Fatores
     - Nome de usuário + PIN

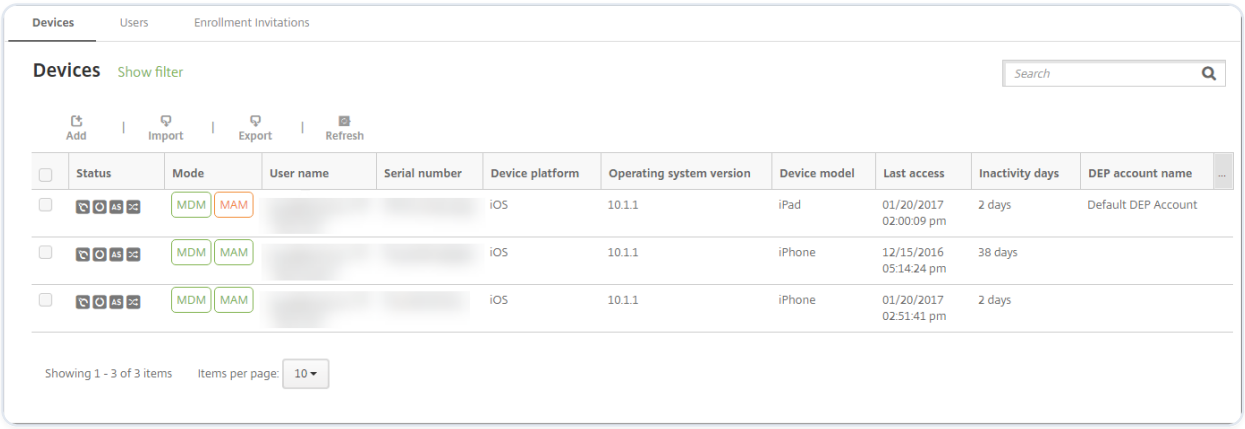
Para enviar convites de inscrição, você só pode usar os modos de segurança de inscrição **URL de Convite**, **URL de Convite + PIN** ou **URL de Convite + Senha**. Para dispositivos que se inscrevem com **Nome de usuário + Senha**, **Dois Fatores** ou **Nome de usuário + PIN**, os usuários devem inserir manualmente suas credenciais no Secure Hub.

Apenas os modos de segurança de inscrição que são válidos para cada uma das plataformas selecionadas aparecem.

> **Nota:**
>
> Quando você seleciona qualquer modo de segurança de inscrição que inclua um PIN, o campo **Modelo para PIN de inscrição** aparece onde você clica em **PIN de inscrição**.

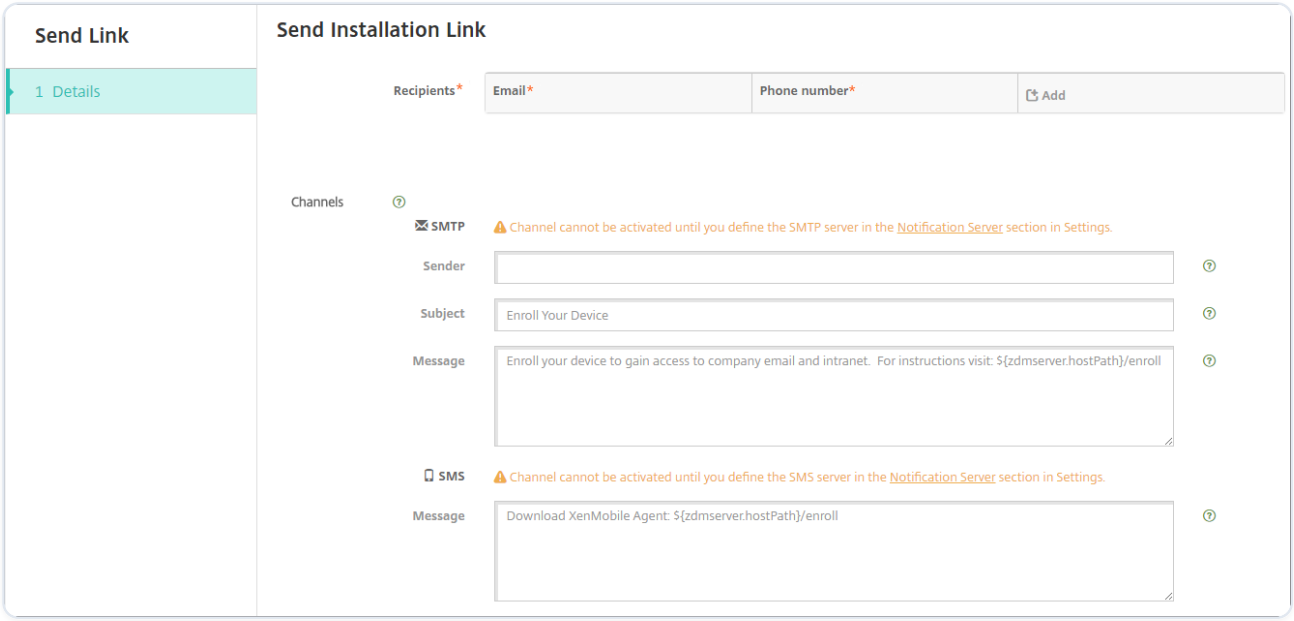
- **Modelo para download do agente:** Escolha o modelo de link de download chamado **Link de download:**. Esse modelo é para todas as plataformas suportadas.
- **Modelo para URL de inscrição:** Escolha **Convite de Inscrição**.
- **Modelo para confirmação de inscrição:** Escolha **Confirmação de Inscrição**.
- **Expirar após:** Este campo é definido quando você configura o Modo de Inscrição e indica quando a inscrição expira. Para obter mais informações sobre como configurar os modos de segurança de inscrição, consulte Configurar modos de segurança de inscrição.
- **Tentativas Máximas:** Este campo é definido quando você configura o Modo de Inscrição e indica o número máximo de vezes que o processo de inscrição ocorre. Para obter mais informações sobre como configurar os modos de segurança de inscrição, consulte Configurar modos de segurança de inscrição.
- **Enviar convite:** Selecione **ATIVADO** para enviar o convite imediatamente. Selecione **DESATIVADO** para adicionar o convite à tabela na página **Convites de Inscrição**, mas sem enviá-lo.

2. Clique em **Salvar e Enviar** se você ativou **Enviar convite**. Caso contrário, clique em **Salvar**. O convite aparece na tabela na página **Convite de Inscrição**.



Para enviar um link de instalação

Antes de poder enviar um link de instalação de inscrição, você deve configurar os canais (SMTP ou SMS) no servidor de notificação a partir da página **Configurações**. Para obter detalhes, consulte Notificações.



1. Configure estas configurações e, em seguida, clique em **Salvar**.

   - **Destinatário:** Para cada destinatário que você deseja adicionar, clique em **Adicionar** e, em seguida, faça o seguinte:

     - **Email:** Digite o endereço de email do destinatário. Este campo é obrigatório.
     - **Número de telefone:** Digite o número de telefone do destinatário. Este campo é obrigatório.

> **Observação:**

> Para excluir um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone da lixeira no lado direito. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou clique em **Cancelar** para manter a listagem.

> Para editar um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta no lado direito. Atualize a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.

- **Canais:** Selecione um canal para usar para enviar o link de instalação de inscrição. Você pode enviar notificações por **SMTP** ou **SMS**. Esses canais não podem ser ativados até que você configure as configurações do servidor na página **Configurações** em **Servidor de Notificações**. Para obter detalhes, consulte Notificações.
- **SMTP:** Configure estas configurações opcionais. Se você não digitar nada nesses campos, os valores padrão especificados no modelo de notificação configurado para a plataforma selecionada serão usados:
  - **Remetente:** Digite um remetente opcional.
  - **Assunto:** Digite um assunto opcional para a mensagem. Por exemplo, "Inscreva seu dispositivo."
  - **Mensagem:** Digite uma mensagem opcional a ser enviada ao destinatário. Por exemplo, "Inscreva seu dispositivo para obter acesso a aplicativos e e-mail organizacionais."
- **SMS:** Configure esta configuração. Se você não digitar nada neste campo, o valor padrão especificado no modelo de notificação configurado para a plataforma selecionada será usado:
  - **Mensagem:** Digite uma mensagem a ser enviada aos destinatários. Este campo é obrigatório para notificações baseadas em SMS.

> **Observação:** Na América do Norte, mensagens SMS que excedem 160 caracteres são entregues em várias mensagens.

2. Clique em **Enviar**.

> **Nota:**
>
> Se seu ambiente usa sAMAccountName: Depois que os usuários recebem o convite e clicam no link, eles devem editar o nome de usuário para concluir a autenticação. O nome de usuário aparece no formato `sAMAccountName@domainname.com`. Os usuários devem remover a parte @domainname.com.

Modos de segurança de registro por plataforma

A tabela a seguir exibe os modos de segurança que você pode usar para registrar dispositivos de usuário. Na tabela, **Sim** indica quais plataformas de dispositivo suportam modos específicos de registro e gerenciamento com diferentes perfis de registro.

MODO DE SEGURANÇA DE REGISTRO MDM	MODO DE SEGURANÇA DE REGISTRO MAM NO CITRIX GATEWAY	MODOS DE GERENCIAMENTO	SUPORTE A DIFERENTES PERFIS DE REGISTRO	ANDROID (LEGADO)	ANDROID ENTERPRISE	IOS (MODO DE REGISTRO DE USUÁRIO)	IOS	MACOS	WINDOWS
Azure AD e Okta como provedores de identidade via Citrix	Certificado de cliente	MDM+MAM ou MDM	Sim	Sim	Sim	Sim	Sim	Não	Não

MODO DE SEGURANÇA DE REGISTRO MDM	MODO DE SEGURANÇA DE REGISTRO MAM NO CITRIX GATEWAY	MODOS DE GERENCIAMENTO	SUPORTE A DIFERENTES PERFIS DE REGISTRO	ANDROID (LEGADO)	ANDROID ENTERPRISE	IOS (MODO DE REGISTRO DE USUÁRIO)	IOS	MAC OS	WINDOWS
Cloud™									
Nome de usuário + Senha	LDAP, LDAP + certificado de cliente e somente certificado de cliente	MDM+MAM, MDM ou MAM (o modo somente MAM não oferece suporte a certificados de cliente no Citrix Gateway)	Sim	Sim	Sim	Sim	Sim	Sim	Sim

MODO DE SEGURANÇA DE REGISTRO MDM	MODO DE SEGURANÇA DE REGISTRO MAM NO CITRIX GATEWAY	MODOS DE GERENCIAMENTO	SUPORTE A DIFERENTES PERFIS DE REGISTRO	ANDROID (LEGADO)	ANDROID ENTERPRISE	IOS (MODO DE REGISTRO DE USUÁRIO)	IOS	MACOS	WINDOWS
URL de convite	Certificado de cliente	MDM+MAM ou MDM	Sim	Sim	Sim	Não	Sim	Não	Não
URL de convite + PIN	Certificado de cliente	MDM+MAM ou MDM	Sim	Sim	Sim	Não	Sim	Não	Não
URL de convite + Senha	LDAP, LDAP + certificado de cliente e somente certificado de	MDM+MAM ou MDM	Sim	Sim	Sim	Não	Sim	Não	Não

MODO DE SEGURANÇA DE REGISTRO MDM	MODO DE SEGURANÇA DE REGISTRO MAM NO CITRIX GATEWAY	MODOS DE GERENCIAMENTO	SUPORTE A DIFERENTES PERFIS DE REGISTRO	ANDROID (LEGADO)	ANDROID ENTERPRISE	IOS (MODO DE REGISTRO DE USUÁRIO)	IOS	MACOS	WINDOWS
	client e								
Autenticação de dois fatores (nome de usuário + senha + PIN)	LDAP, LDAP + certificado de client e e somente certificado de client e	MDM +MAM ou MDM	Sim	Sim	Sim	Não	Sim	Sim	Não
Nome de usuário + PIN	Certificado de client e	MDM +MAM ou MDM	Sim	Sim	Sim	Não	Sim	Sim	Não

O seguinte descreve como os modos de segurança de registro se comportam em dispositivos iOS, Android e Android Enterprise:

- **Nome de usuário + Senha** (padrão)
  - Envia ao usuário uma única notificação que contém um URL de registro. Quando o usuário clica no URL, o Secure Hub é aberto. O usuário então digita um nome de usuário e senha para registrar o dispositivo no XenMobile.
- **URL de convite**
  - Envia ao usuário uma única notificação que contém um URL de registro. Quando o usuário clica no URL, o Secure Hub é aberto. O nome do XenMobile Server e o botão **Sim, Registrar** aparecem. O usuário toca em **Sim, Registrar** para registrar o dispositivo no XenMobile.
- **URL de convite + PIN**
  - Envia ao usuário os seguintes e-mails:
    - Um e-mail com um URL de registro, que permite ao usuário registrar o dispositivo no XenMobile através do Secure Hub.
    - Um e-mail com um PIN de uso único que o usuário deve digitar ao registrar o dispositivo, juntamente com a senha do Active Directory (ou local) do usuário.
  - Com este modo, o usuário se registra apenas usando o URL de registro na notificação. Se o usuário perder o convite de notificação, ele não poderá se registrar. No entanto, você pode enviar outro convite.
- **URL de Convite + Senha**
  - Envia ao usuário uma única notificação que contém um URL de registro. Quando o usuário clica no URL, o Secure Hub é aberto. O nome do XenMobile Server aparece, juntamente com um campo que permite ao usuário digitar uma senha.
- **Dois Fatores**
  - Envia ao usuário uma única notificação que contém um URL de registro e um PIN de uso único. Quando o usuário clica no URL, o Secure Hub é aberto. O nome do XenMobile Server aparece, juntamente com dois campos que permitem ao usuário digitar uma senha e o número PIN.
- **Nome de usuário + PIN**

    - Envia ao usuário os seguintes e-mails:
        - Um e-mail com um URL de registro, que permite ao usuário baixar e instalar o Secure Hub. Depois que o Secure Hub é aberto, o usuário é solicitado a digitar um nome de usuário e senha para registrar o dispositivo no XenMobile.
        - Um e-mail com um PIN de uso único que o usuário deve digitar ao registrar o dispositivo, juntamente com a senha do Active Directory (ou local) do usuário.
    - Se o usuário perder o convite de notificação, ele não poderá se registrar. No entanto, você pode enviar outro convite.

A seguir, é descrito como os modos de segurança de registro se comportam em dispositivos macOS:

- **Nome de usuário + Senha**
    - Envia ao usuário uma única notificação que contém um URL de inscrição. Quando o usuário clica no URL, o navegador Safari é aberto. Uma página de login aparece, solicitando que o usuário digite um nome de usuário e senha para inscrever o dispositivo no XenMobile.
- **Dois Fatores**
    - Envia ao usuário uma única notificação que contém um URL de inscrição e um PIN de uso único. Quando o usuário clica no URL, o navegador Safari é aberto. Uma página de login aparece, exibindo dois campos que permitem ao usuário digitar uma senha e o número PIN.
- **Nome de usuário + PIN**
    - Envia ao usuário os seguintes e-mails:
        - Um e-mail com um URL de inscrição. Quando o usuário clica no URL, o navegador Safari é aberto. Uma página de login aparece, solicitando que o usuário digite um nome de usuário e senha para inscrever o dispositivo no XenMobile.
        - Um e-mail com um PIN de uso único que o usuário deve digitar ao inscrever o dispositivo, juntamente com a senha do Active Directory (ou local) do usuário.
    - Se o usuário perder o convite de notificação, ele não poderá se inscrever. No entanto, você pode enviar outro convite.

Você não pode enviar convites de inscrição para dispositivos Windows. Os usuários do Windows se inscrevem diretamente por meio de seus dispositivos.

Firebase Cloud Messaging

> **Nota:**
>
> O Firebase Cloud Messaging (FCM) era anteriormente conhecido como Google Cloud Messaging (GCM). Alguns rótulos e mensagens do console do XenMobile® usam a terminologia GCM.

> A Citrix® recomenda que você use o Firebase Cloud Messaging (FCM) para controlar como e quando os dispositivos Android se conectam ao XenMobile. O XenMobile, quando configurado para FCM, envia notificações de conexão para dispositivos Android que estão habilitados para FCM. Qualquer ação de segurança ou comando de implantação aciona uma notificação push para solicitar que o usuário se reconecte ao XenMobile Server.

Depois de concluir as etapas de configuração neste artigo e um dispositivo fazer check-in, o dispositivo se registra no serviço FCM no XenMobile Server. Essa conexão permite comunicação quase em tempo real do seu Serviço XenMobile para o seu dispositivo usando FCM. O registro FCM funciona para novas inscrições de dispositivos e dispositivos previamente inscritos.

Quando o XenMobile precisa iniciar uma conexão com o dispositivo, ele se conecta ao serviço FCM. Então, o serviço FCM notifica o dispositivo para se conectar. Esse tipo de conexão é semelhante ao que a Apple usa para seu Serviço de Notificação Push.

Pré-requisitos

- Cliente Secure Hub mais recente
- Credenciais da conta de desenvolvedor do Google
- Serviços do Google Play instalados em dispositivos Android habilitados para FCM

Portas de firewall

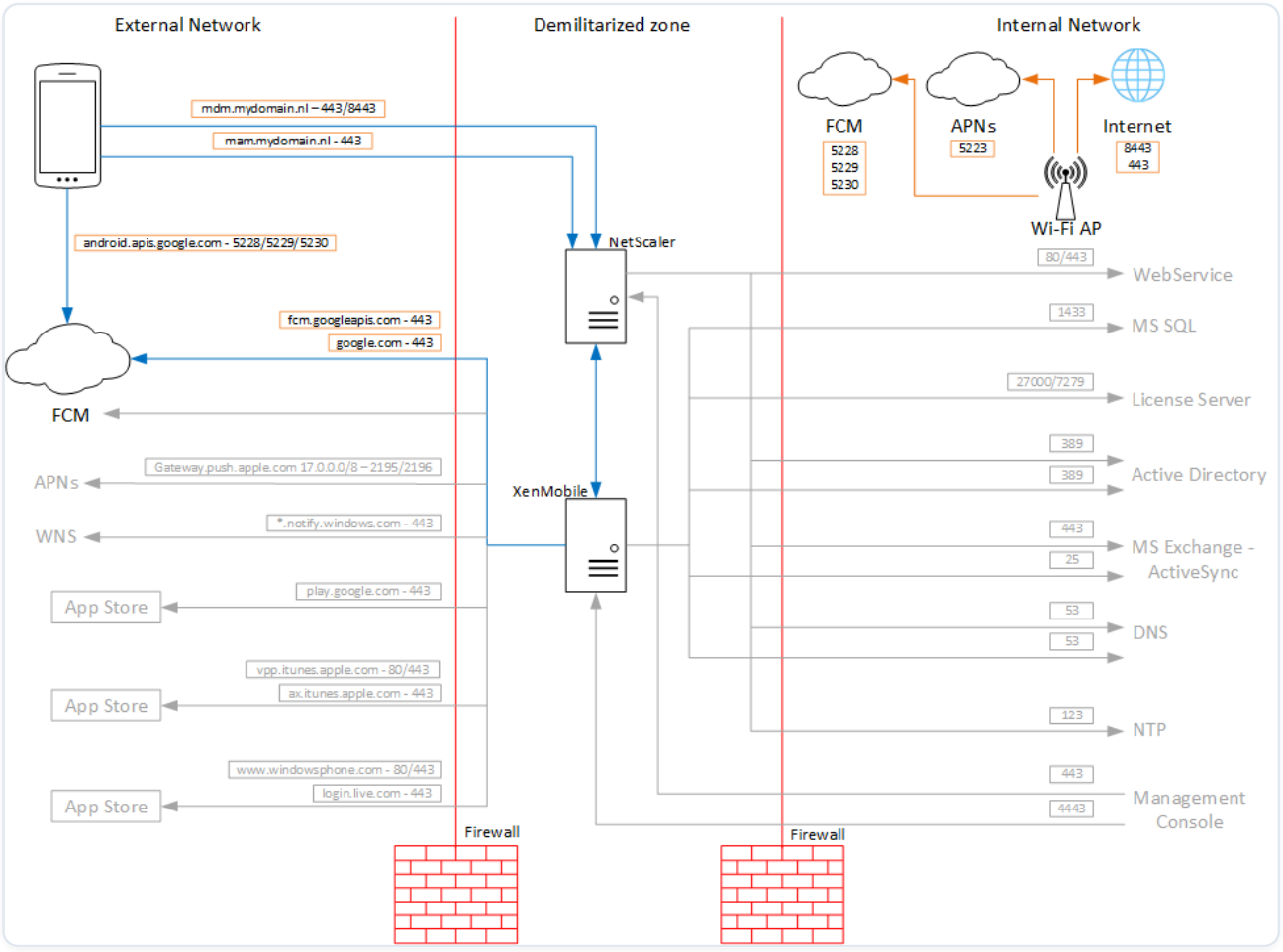
- Abra a porta 443 no XenMobile para `fcm.googleapis.com` e `Google.com`.
- Abra a comunicação de Internet de saída para Wi-Fi do dispositivo nas portas 5228, 5229 e 5230.

- Para permitir conexões de saída, o FCM recomenda permitir as portas 5228 a 5230 sem restrições de IP. No entanto, se você precisar de restrições de IP, o FCM recomenda permitir todos os endereços IP nos blocos IPv4 e IPv6. Esses blocos estão listados no Google ASN de 15169. Atualize essa lista mensalmente. Para obter mais informações sobre as portas FCM, consulte a documentação do Google sobre portas FCM.

Para obter mais informações, consulte Requisitos de porta.

Arquitetura

Este diagrama mostra o fluxo de comunicação para FCM na rede externa e interna.

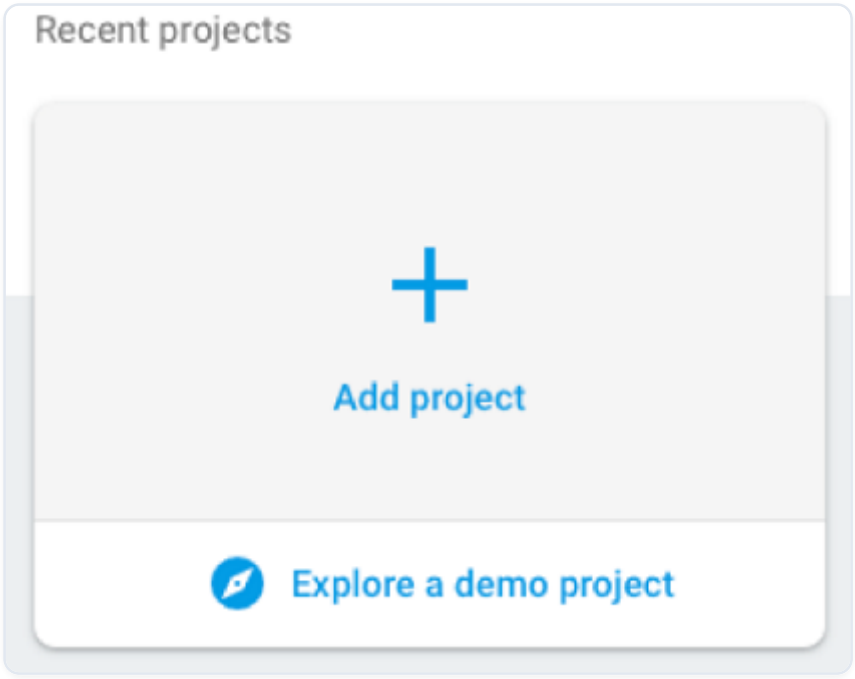


Para configurar sua conta Google para FCM

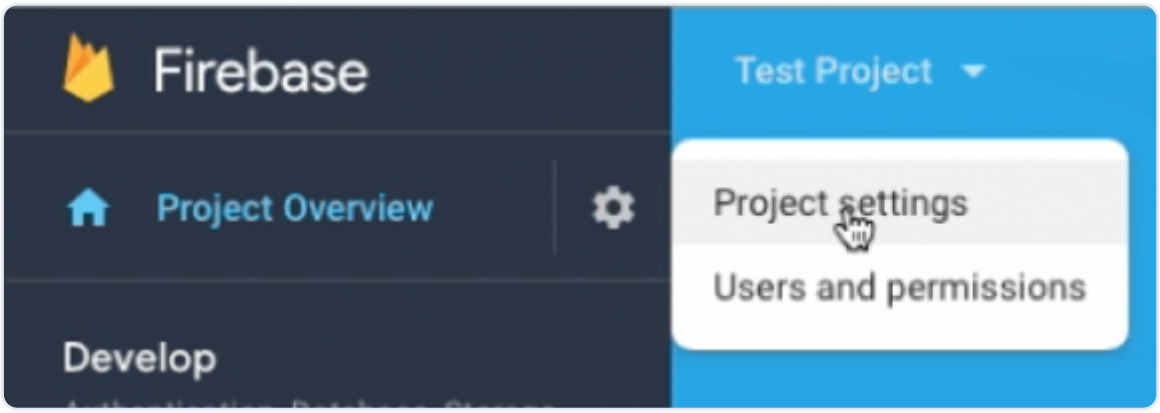
1. Faça login no seguinte URL usando suas credenciais de conta de desenvolvedor do Google:

   `<https://console.firebase.google.com/>`

2. Clique em **Adicionar projeto**.



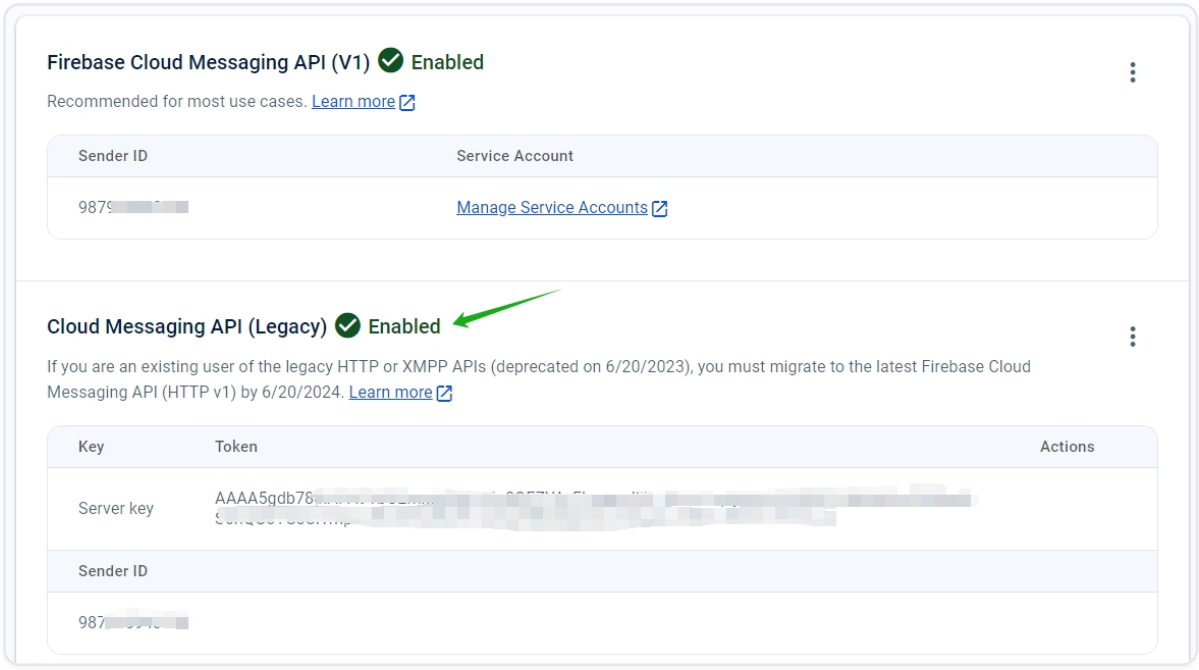
3. Depois de criar o projeto, clique em **Configurações do projeto**.



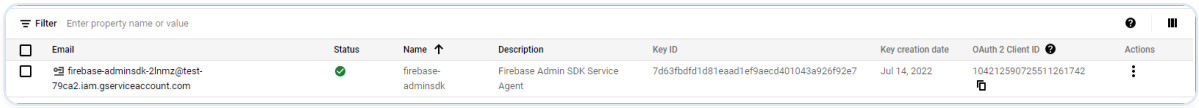
> **Nota:**
>
> O Google vai descontinuar as APIs legadas do FCM para HTTP, que são atualmente usadas em nossa implementação do FCM. O prazo de migração é em June 21, 2024. Precisamos migrar o FCM da API legada do FCM para a API HTTP v1. Para mais informações, consulte Migrar das APIs legadas do FCM para HTTP v1.

4. Clique na guia **Cloud Messaging**. Verifique se a API do Firebase Cloud Messaging está ativada e clique em **Gerenciar contas de serviço**.

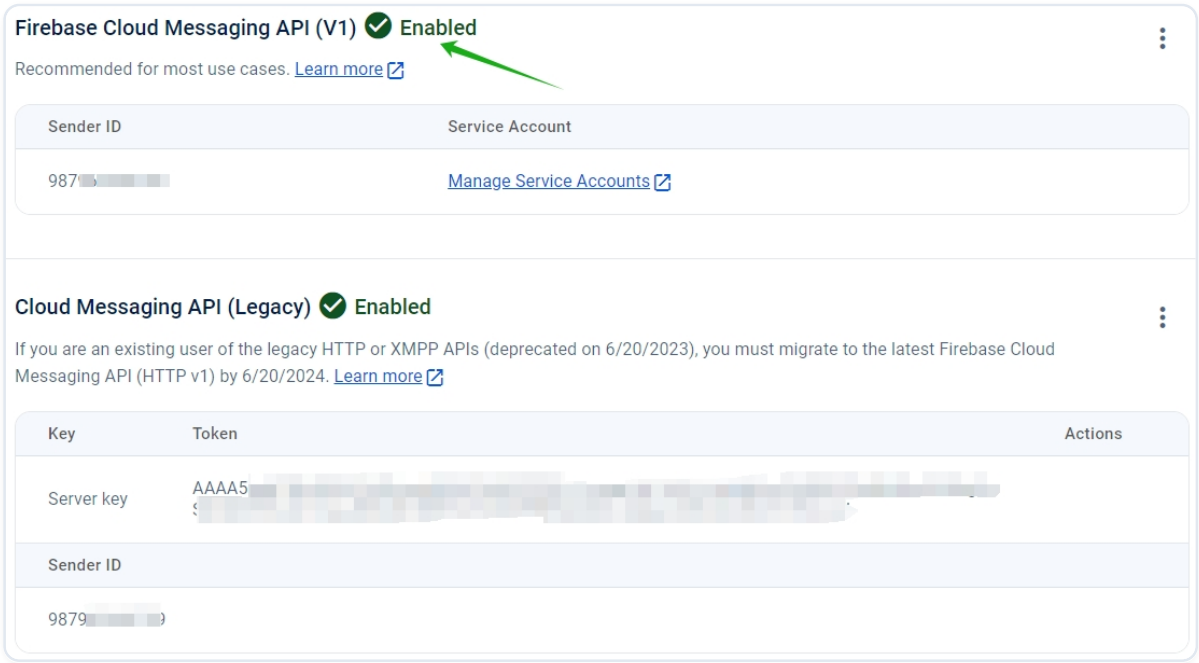
   a. Antes da migração, você poderia usar a API legada, certifique-se de que a API do Cloud Messaging (Legada) esteja ativada. Copie os valores dos campos **Chave** e **ID do Remetente**.



Se você não tiver uma chave listada, clique nas reticências em **Ações** para adicionar uma chave.

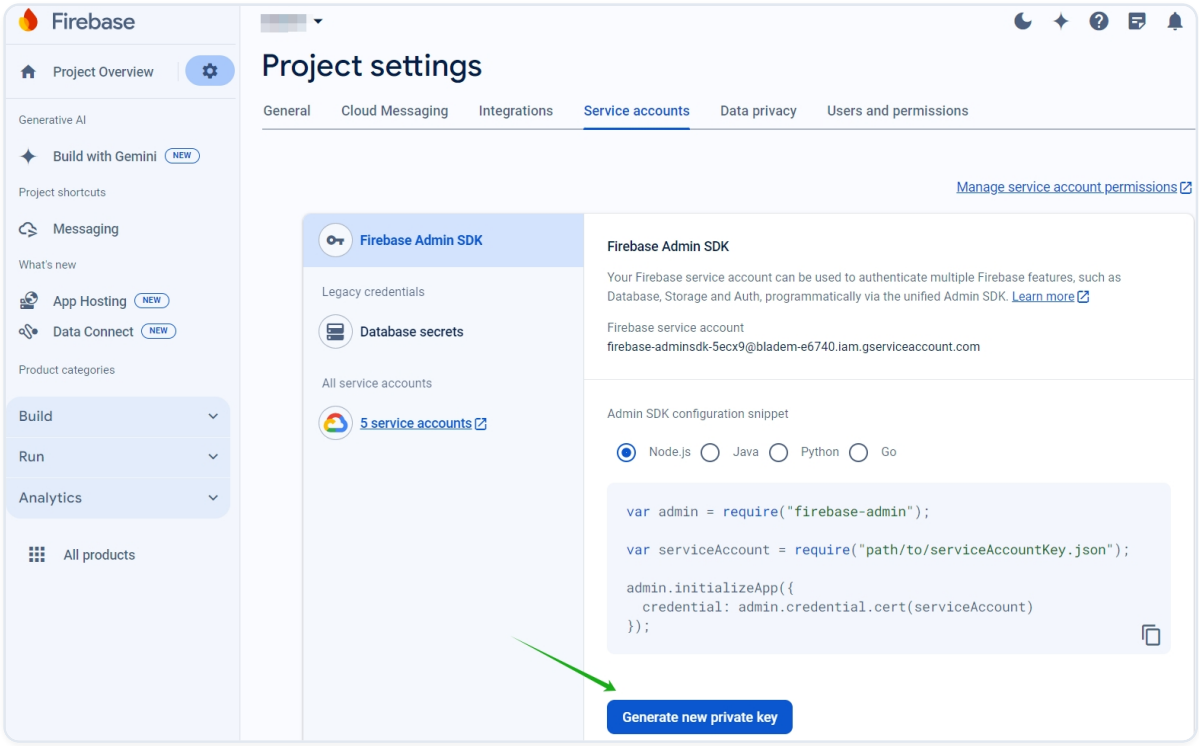


b. Após a migração, a API legada é descontinuada pelo Google. Você precisa habilitar a API do Firebase Cloud Messaging (V1). Para obter mais informações, consulte Migrar de APIs FCM legadas para HTTP v1.



Baixe o arquivo JSON da conta de serviço em **Contas de serviço** em **Configurações do projeto**. Consulte a seção Fornecer credenciais manualmente para gerar um arquivo de

chave privada para sua conta de serviço. Clique em **Gerar nova chave privada** para baixar o arquivo JSON da chave da conta de serviço.



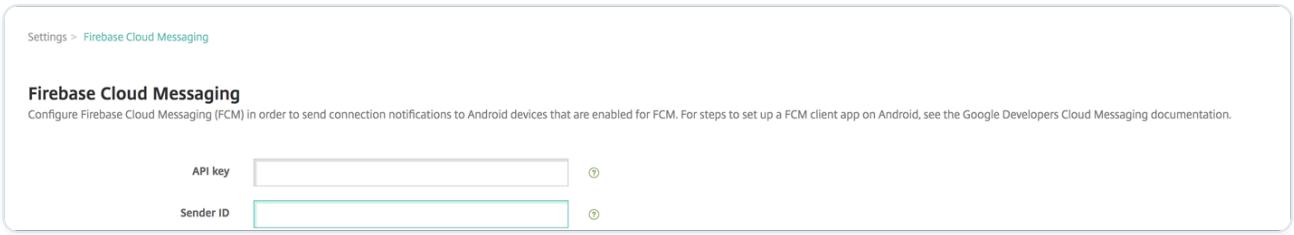
Para obter as etapas para configurar um aplicativo cliente FCM no Android, consulte este artigo do Google Developers Cloud Messaging: `<https://firebase.google.com/docs/cloud-messaging/android/client>`.

Para configurar o XenMobile para FCM

No console do XenMobile, vá para **Configurações > Firebase Cloud Messaging**.

Para API do Cloud Messaging (Legado)

1. Insira a **Chave** do Firebase Cloud Messaging da última etapa da configuração do Firebase Cloud Messaging no campo **Chave da API**.
2. Insira o valor do **ID do Remetente** do procedimento anterior.

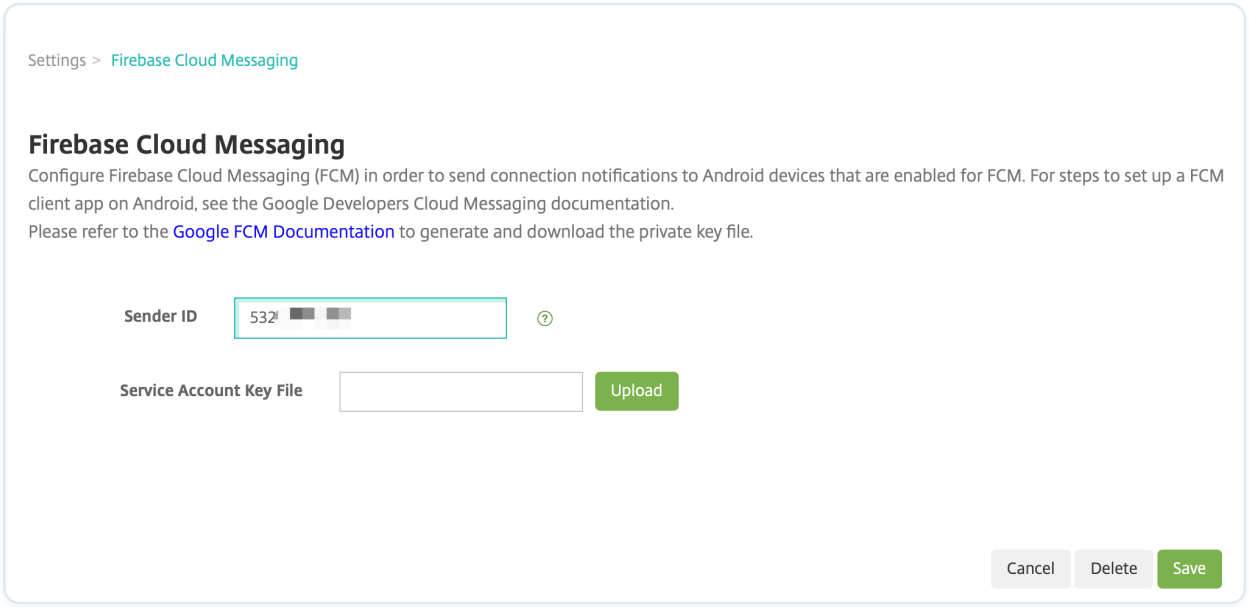


Para API do Firebase Cloud Messaging (V1)

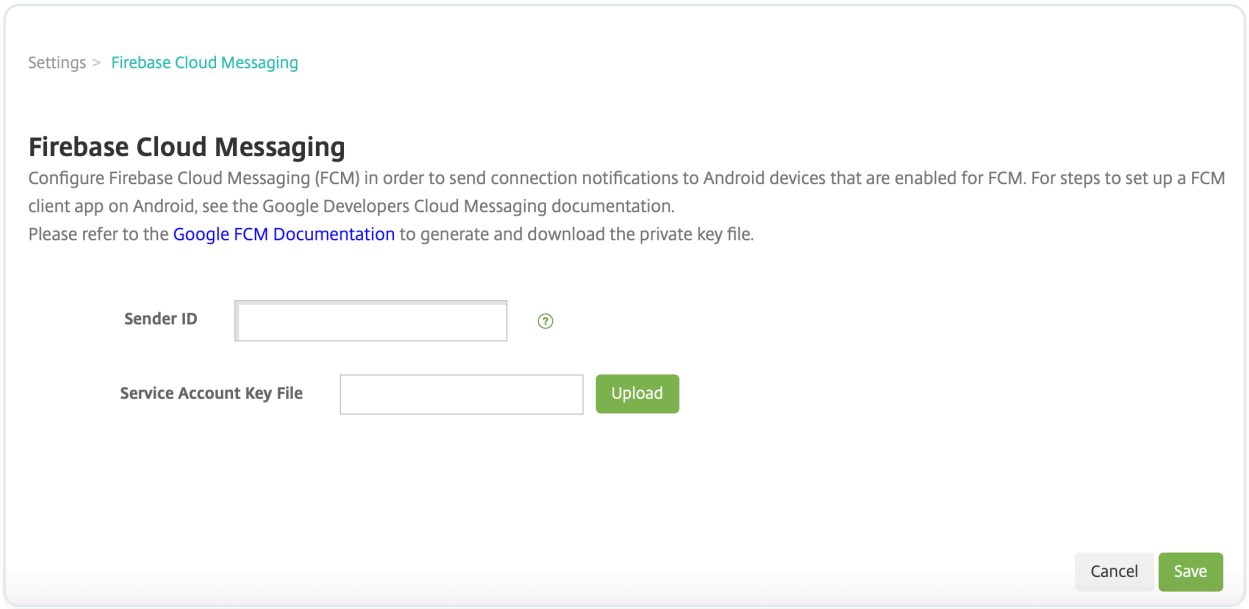
Observações:

- Para habilitar a API V1 do FCM para o XenMobile Server versão 10.15 Rolling Patch 7 e posterior, consulte o artigo da Central de Conhecimento CTX677031.
- Se você for um novo usuário do FCM, pule a etapa 1 e prossiga a partir da etapa 2.

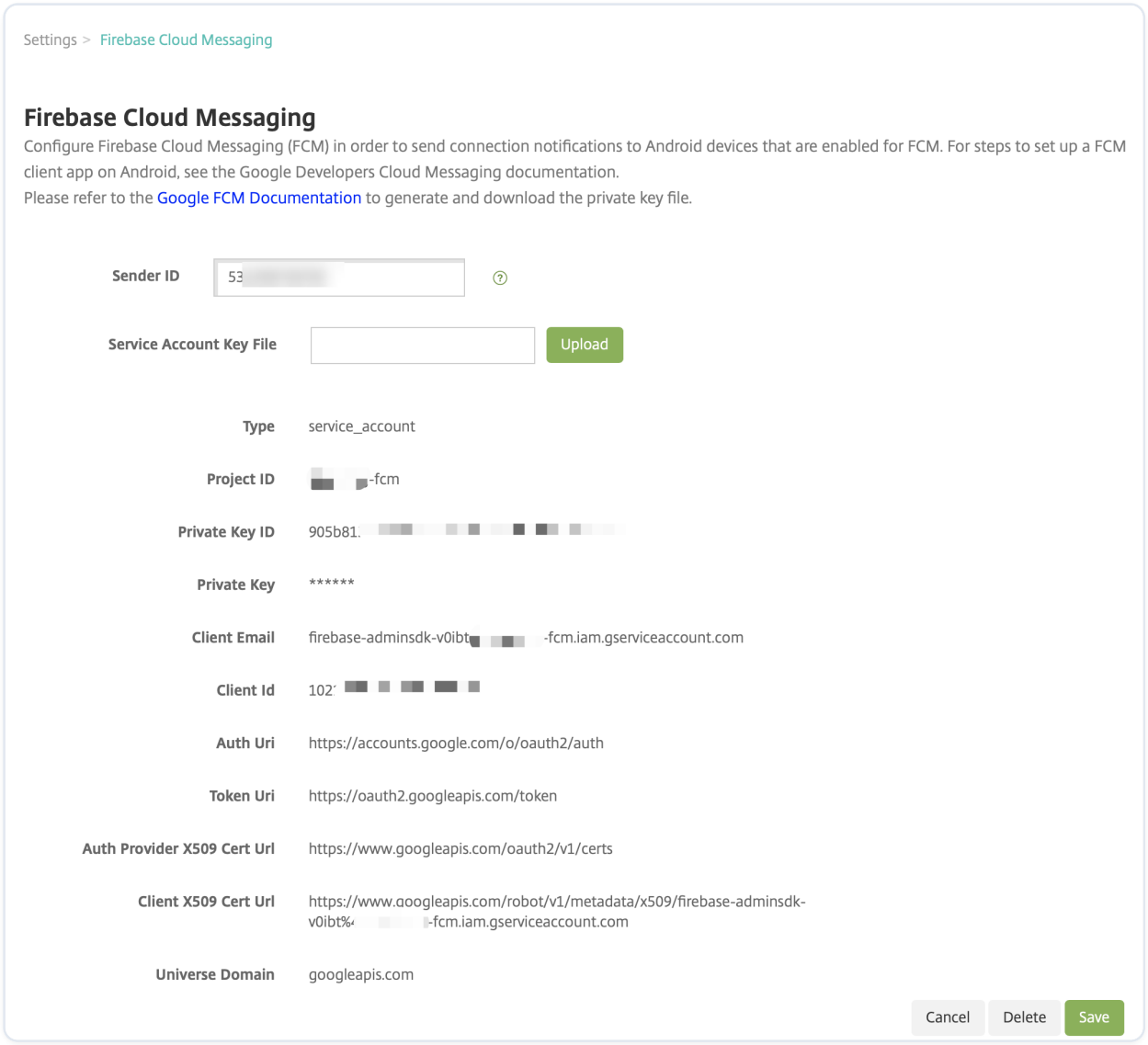
1. Se você já estiver usando o FCM, notará que o ID do Remetente é preenchido automaticamente com seu projeto FCM atual e uma nova opção para carregar o **Arquivo de Chave da Conta de Serviço**.



2. Se você for um novo usuário do FCM, insira o **ID do Remetente** e carregue o **Arquivo de Chave da Conta de Serviço** do procedimento anterior.



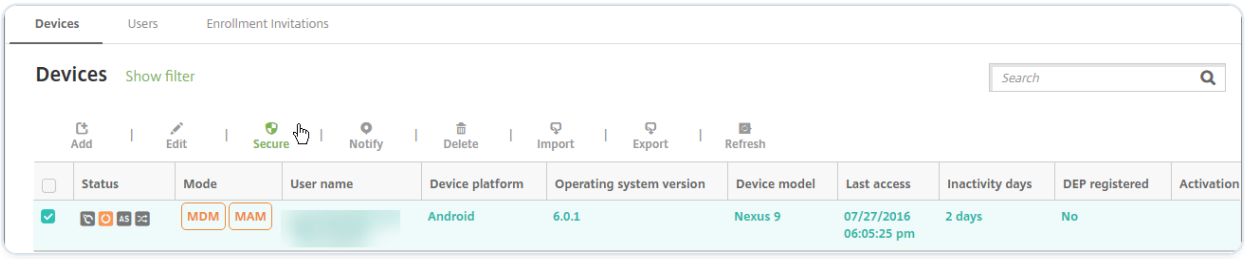
3. O arquivo carregado será analisado e os campos correspondentes serão gerados automaticamente.



4. Verifique as informações e clique em **Salvar**.

Para testar sua configuração

1. Registre um dispositivo Android.
2. Deixe o dispositivo ocioso por algum tempo, para que ele se desconecte do XenMobile.
3. Faça login no console do XenMobile, clique em **Gerenciar**, selecione o dispositivo Android e, em seguida, clique em **Proteger**.



4. Em **Ações do Dispositivo**, clique em **Limpeza Seletiva**.



Em uma configuração bem-sucedida, a limpeza seletiva ocorre no dispositivo.

Integrar com recursos do Apple Education

Você pode usar o XenMobile® como sua solução de gerenciamento de dispositivos móveis (MDM) em um ambiente que usa o Apple Education. O suporte do XenMobile inclui o Apple School Manager (ASM) e o aplicativo Classroom para iPad. A política de dispositivo de Configuração de Educação do XenMobile configura dispositivos de instrutores e alunos para uso com o Apple Education.

Você fornece iPads pré-configurados e supervisionados para instrutores e alunos. Essa configuração inclui o registro do ASM no XenMobile, uma conta de ID Apple Gerenciado configurada com uma nova senha e aplicativos e iBooks de compra por volume necessários.

Aqui estão os destaques do suporte do XenMobile para os recursos do Apple Education.

Apple School Manager

O ASM é um serviço que permite configurar, implantar e gerenciar dispositivos iOS (iPadOS) e laptops macOS usados em instituições de ensino. O ASM inclui um portal baseado na web que permite aos administradores de TI:

- Atribuir dispositivos do Programa de Implantação da Apple a diferentes servidores MDM.
- Comprar licenças de compra por volume para aplicativos e iBooks
- Criar **IDs Apple Gerenciados** em massa. Esses IDs Apple personalizados fornecem acesso a serviços da Apple, como armazenamento de documentos no iCloud Drive e inscrição em cursos da App Store da Apple.

Você pode adicionar várias contas ASM ao XenMobile. Por exemplo, esse recurso permite usar diferentes configurações de registro e opções do Assistente de Configuração por unidade ou departamento de Educação. Em seguida, você associa as contas ASM a diferentes políticas de dispositivo.

Depois de adicionar uma conta ASM ao console do XenMobile, o XenMobile recupera informações de classe e lista de alunos. Durante a configuração do dispositivo, o XenMobile:

- Registra os dispositivos.
- Instala os recursos configurados para implantação, como políticas de dispositivo (Configuração de Educação, layout da tela inicial e assim por diante).
- Também instala aplicativos e iBooks comprados por meio de compra por volume.

Em seguida, você fornece os dispositivos pré-configurados para instrutores e alunos. Se um dispositivo for perdido ou roubado, você pode usar o recurso Modo Perdido do MDM para bloquear e localizar dispositivos.

Aplicativo Classroom para iPad

O aplicativo Classroom para iPad permite que os instrutores se conectem e gerenciem os dispositivos dos alunos. Você pode visualizar as telas dos dispositivos, abrir aplicativos em iPads e compartilhar e abrir links da web.

O Classroom é gratuito na App Store. Você carrega o aplicativo para o console do XenMobile. Em seguida, você usa a política de dispositivo de Configuração de Educação para configurar o aplicativo Classroom, que você implanta nos dispositivos dos instrutores.

Para obter mais informações sobre os recursos do Apple Education, consulte o site Apple Education e o Guia de Implantação do Apple Education no mesmo site.

Pré-requisitos

- Citrix Gateway
- Perfil de registro configurado para MDM+MAM.

- Apple iPad de terceira geração (versão mínima) ou iPad Mini, com iOS 9.3 (versão mínima)

Nota:

O XenMobile não valida contas de usuário ASM em relação ao LDAP ou Active Directory. No entanto, você pode conectar o XenMobile ao LDAP ou Active Directory para o gerenciamento de usuários e dispositivos não relacionados a instrutores ou alunos ASM. Por exemplo, você pode usar o Active Directory para fornecer Secure Mail e Secure Web a outros membros ASM, como administradores de TI e gerentes.

Como os instrutores e alunos ASM são usuários locais, não há necessidade de implantar o Citrix Secure Hub™ em seus dispositivos.

O registro MAM que inclui autenticação do Citrix Gateway não oferece suporte a usuários locais (apenas usuários do Active Directory). Assim, o XenMobile implanta apenas aplicativos de compra por volume e iBooks necessários nos dispositivos de instrutores e alunos.

Configurar o Apple School Manager e o XenMobile

Depois de comprar iPads da Apple ou de revendedores autorizados Apple ou operadoras: Siga o fluxo de trabalho nesta seção para configurar sua conta e dispositivos ASM. Este fluxo de trabalho inclui etapas que você realiza no portal ASM e no console do XenMobile.

Siga estas instruções para configurar sua integração para quaisquer iPads que você use em um modelo Um-para-Um (um iPad por aluno) ou para iPads de instrutor (não compartilhados). Para configurar iPads Compartilhados, consulte Configurar iPads Compartilhados.

Passo 1: Crie sua conta do Apple School Manager e conclua o Assistente de Configuração

Se você planeja fazer upgrade do Programa de Implantação da Apple, consulte o artigo de Suporte da Apple, Atualize sua instituição para o ASM. Para criar sua conta ASM, acesse `<https://school.apple.com/>` e siga as instruções para se inscrever. Na primeira vez que você fizer login no ASM, o Assistente de Configuração será aberto.

- Para obter informações sobre os pré-requisitos do ASM, o Assistente de Configuração e as tarefas de gerenciamento, consulte o Guia do Usuário do Apple School Manager.

- Ao configurar um ASM, use um nome de domínio que seja diferente do nome de domínio do Active Directory. Por exemplo, prefixe o nome de domínio do ASM com algo como `appleid`.
- Quando você conecta o ASM aos seus dados de lista, o ASM cria IDs Apple Gerenciados para instrutores e alunos. Seus dados de lista incluem instrutores, alunos e turmas. Para obter informações sobre como adicionar dados de lista ao ASM, consulte o Guia do Usuário do ASM, mencionado anteriormente.
- Você pode personalizar o formato do ID Apple Gerenciado para sua instituição, conforme descrito no Guia do Usuário do ASM, mencionado anteriormente.

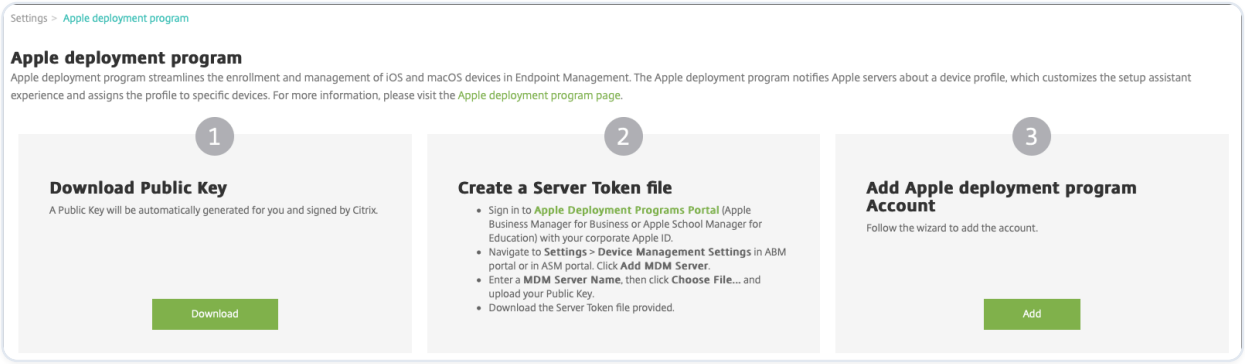
> **Importante:**
>
> Não altere os IDs Apple Gerenciados depois de importar as informações do ASM para o XenMobile.

- Se você comprou dispositivos por meio de revendedores ou operadoras, vincule esses dispositivos ao ASM. Para obter informações, consulte o Guia do Usuário do ASM, mencionado anteriormente.

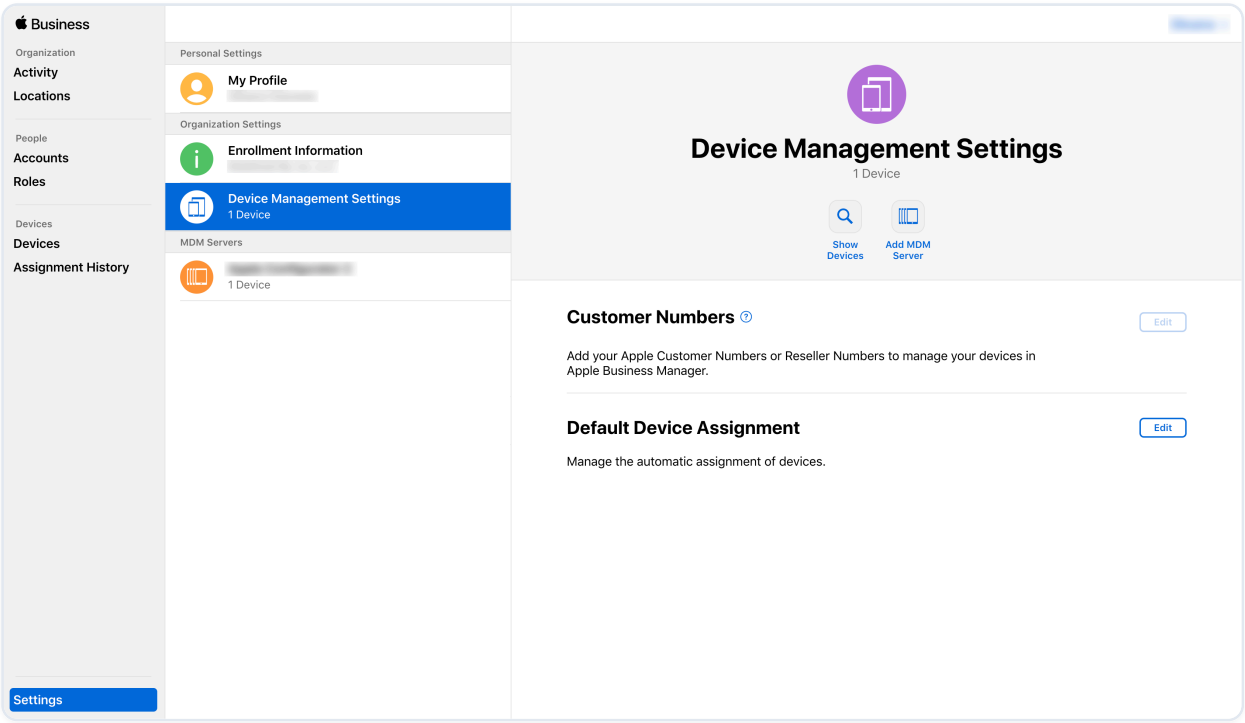
Passo 2: Configure o XenMobile como o Servidor MDM para o Apple School Manager e configure as atribuições de dispositivo

O portal ASM inclui uma guia **Servidores MDM**. Você precisa do arquivo de chave pública do XenMobile para concluir essa configuração.

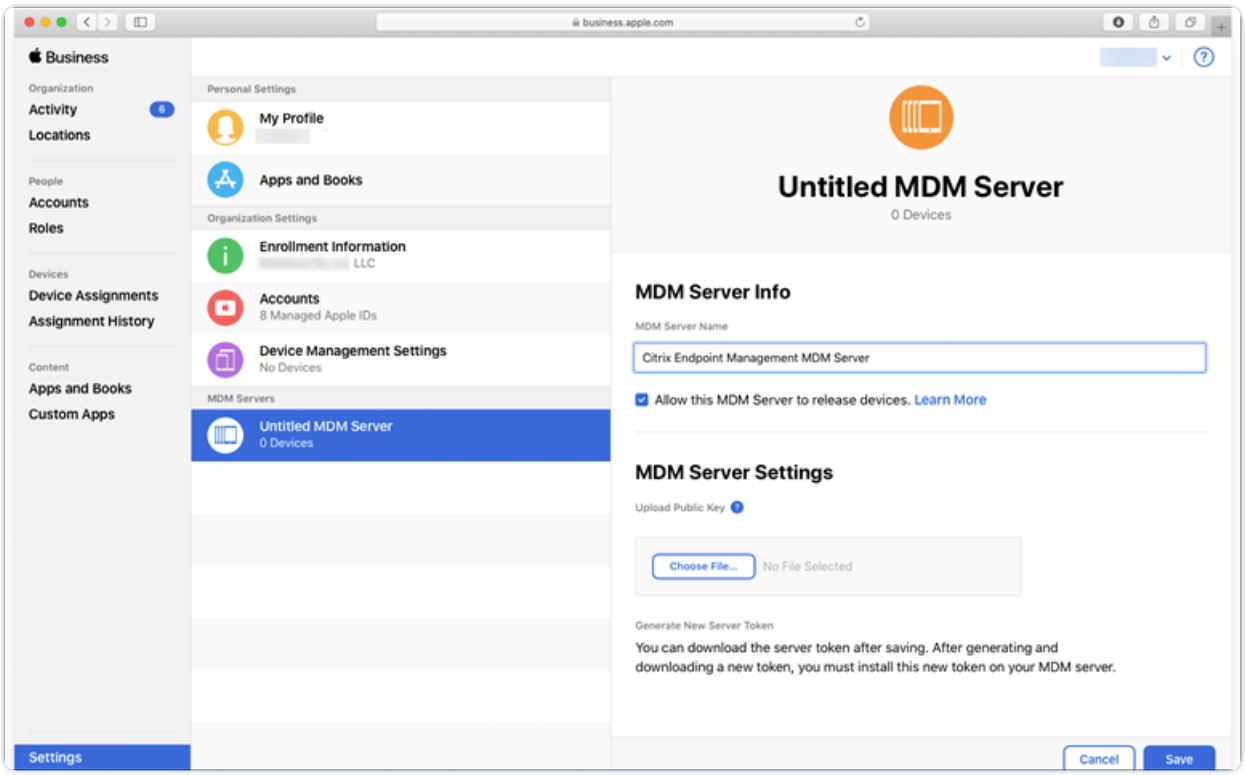
1. Baixe a chave pública do seu XenMobile para o seu computador local: No console do XenMobile, vá para **Configurações > Programa de Implantação da Apple**.



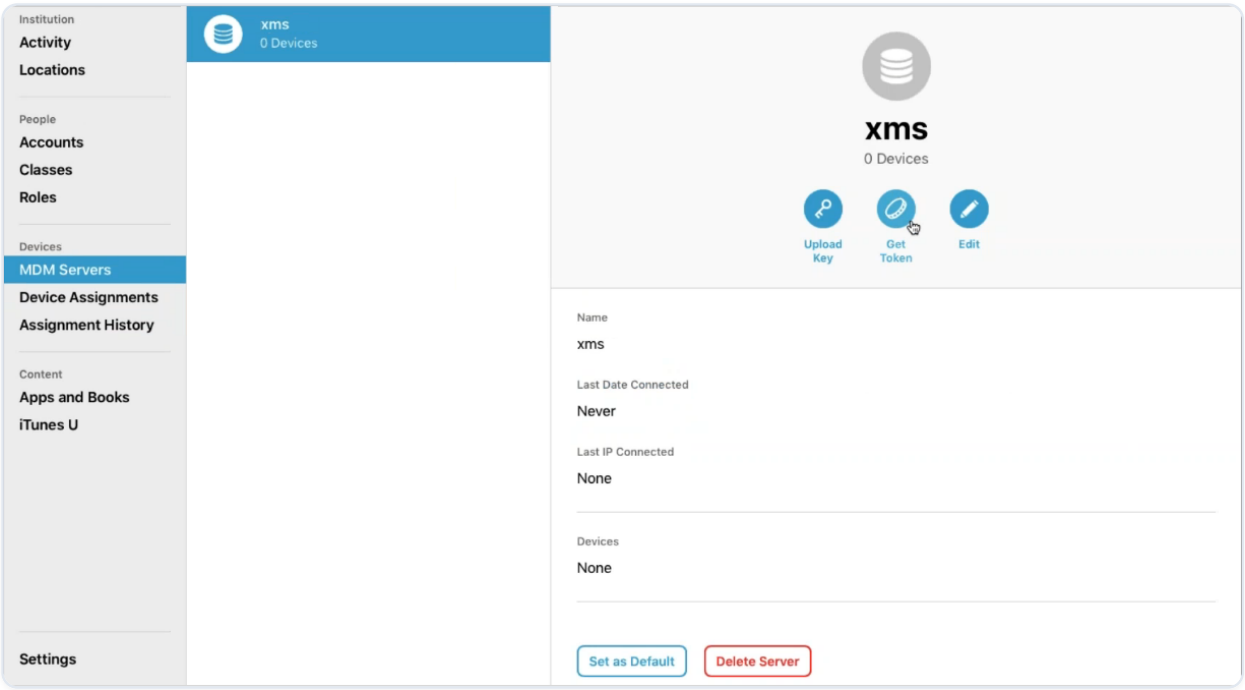
2. Em **Baixar Chave Pública**, clique em **Baixar** e salve o arquivo PEM.
3. No portal **Apple School Manager**, clique em **Configurações**, depois em **Configurações de Gerenciamento de Dispositivos**. Clique em **Adicionar Servidor MDM**.



4. Digite um nome para o XenMobile. O nome do servidor que você digita é para sua referência e não é a URL ou o nome do servidor. Em **Carregar Chave Pública**, clique em **Escolher Arquivo**.



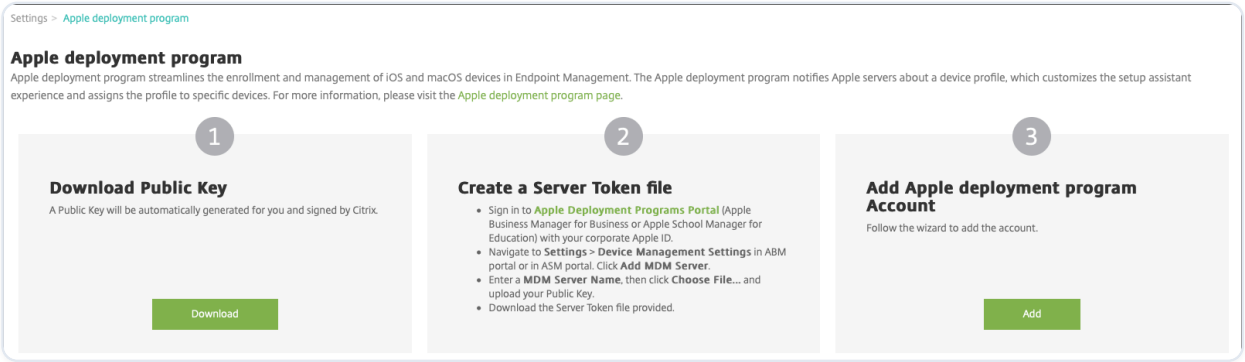
5. Carregue a chave pública que você baixou do XenMobile e, em seguida, clique em **Salvar**.
6. Gerar um token de servidor: Clique em **Baixar Token** para baixar o arquivo de token do servidor para o seu computador.



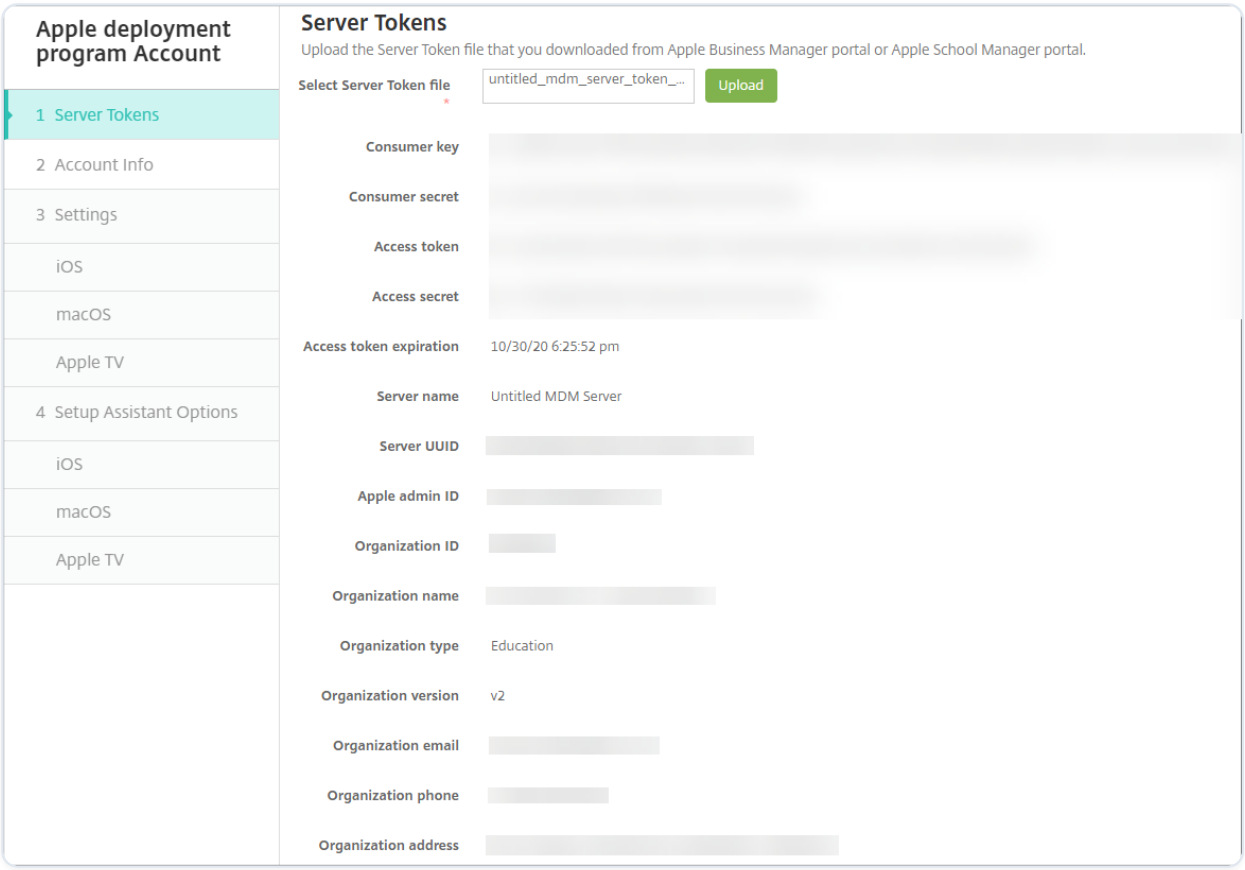
7. Em **Atribuição Padrão de Dispositivo**, clique em **Alterar**. Escolha como você deseja atribuir dispositivos e, em seguida, forneça as informações solicitadas. Para obter informações, consulte o Guia do Usuário do ASM.

Etapa 3: Adicionar a conta do Apple School Manager ao XenMobile

1. No console do XenMobile, vá para **Configurações > Programa de Implantação da Apple** e em **Adicionar Conta do Programa de Implantação da Apple**, clique em **Adicionar**.



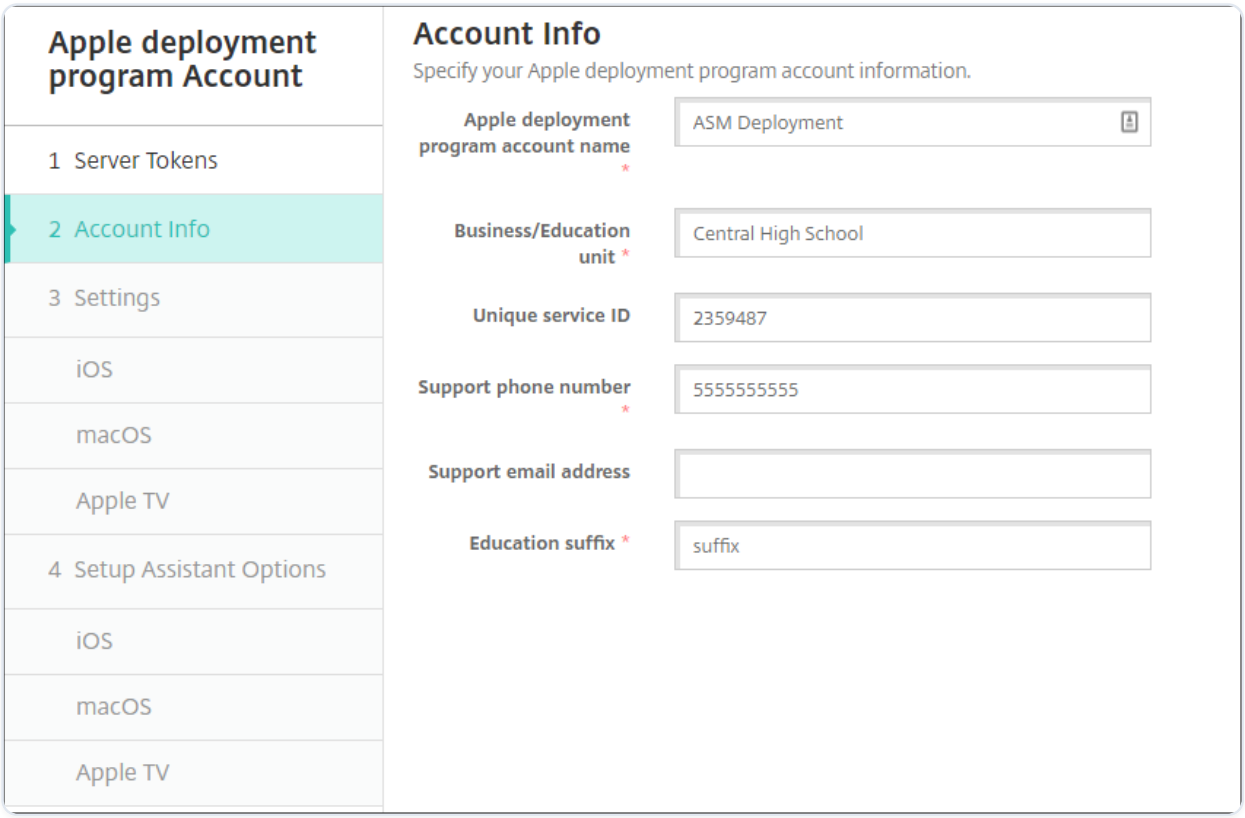
2. Na página **Tokens do Servidor**, clique em **Carregar** e escolha o arquivo de token do servidor (um arquivo P7M) que você baixou do portal ASM. As informações do token aparecem.



Observações:

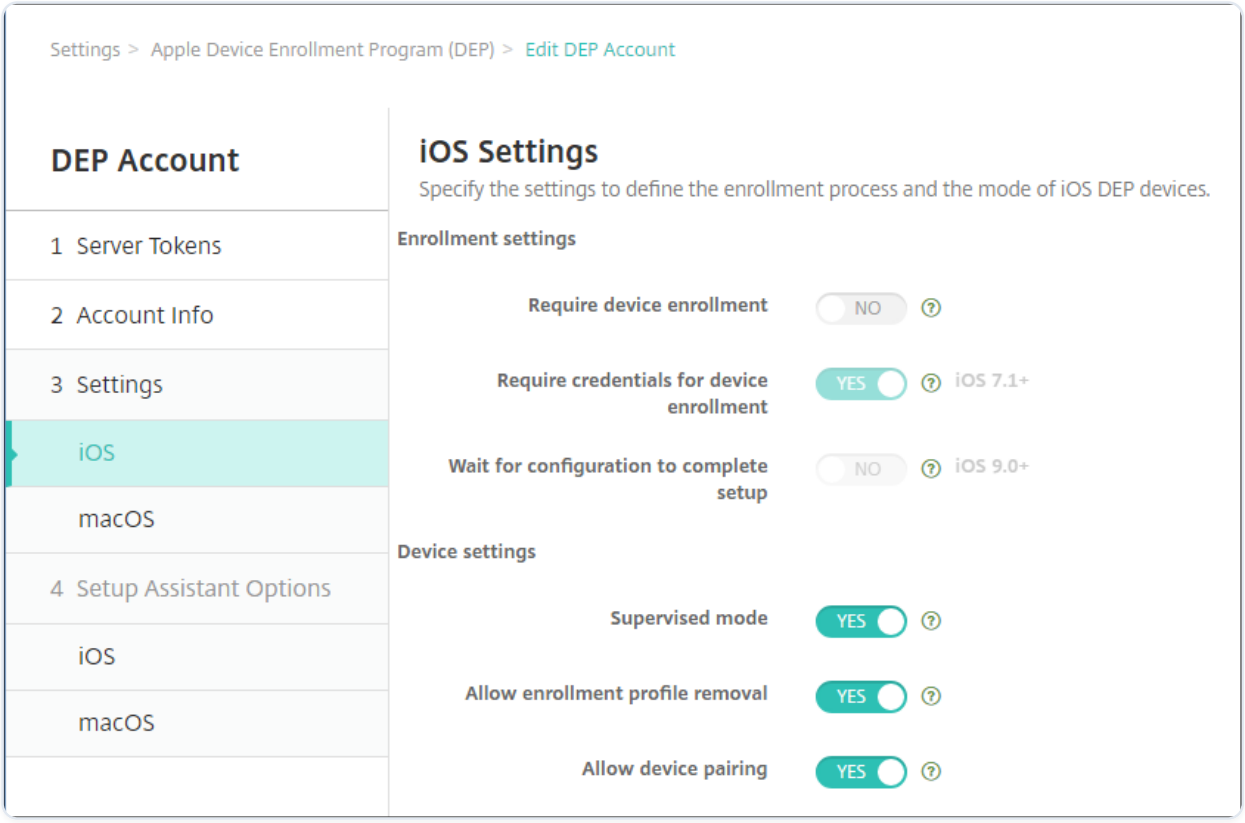
- **ID da Organização** é o seu ID de cliente para o Programa de Implantação da Apple.
- As contas ASM têm um **Tipo de organização** de **Educação** e uma **Versão da organização** de **v2**.

3. Na página **Informações da Conta**, especifique as seguintes configurações.



- **Nome da conta do Programa de Implantação da Apple:** Um nome exclusivo para esta conta do Programa de Implantação da Apple. Use nomes que reflitam como você organiza as contas do Programa de Implantação da Apple, como por país ou hierarquia organizacional.
- **Unidade de Negócios/Educação:** A unidade ou departamento de Educação para atribuição de dispositivos. Este campo é obrigatório.
- **ID de serviço exclusivo:** Um ID exclusivo opcional para ajudar a identificar ainda mais a conta.
- **Número de telefone de suporte:** Um número de telefone de suporte para o qual os usuários podem ligar para obter ajuda durante a configuração. Este campo é obrigatório.
- **Endereço de e-mail de suporte:** Um endereço de e-mail de suporte opcional disponível para os usuários finais.
- **Sufixo de Educação:** Sinaliza as turmas para uma determinada conta do Programa de Implantação ASM. (O sufixo de compra por volume sinaliza aplicativos e iBooks para uma determinada conta de compra por volume.) A recomendação é usar o mesmo sufixo para ambas as contas, Programa de Implantação ASM e compra por volume ASM.

4. Clique em **Avançar**. Em **Configurações do iOS**, especifique as seguintes configurações.

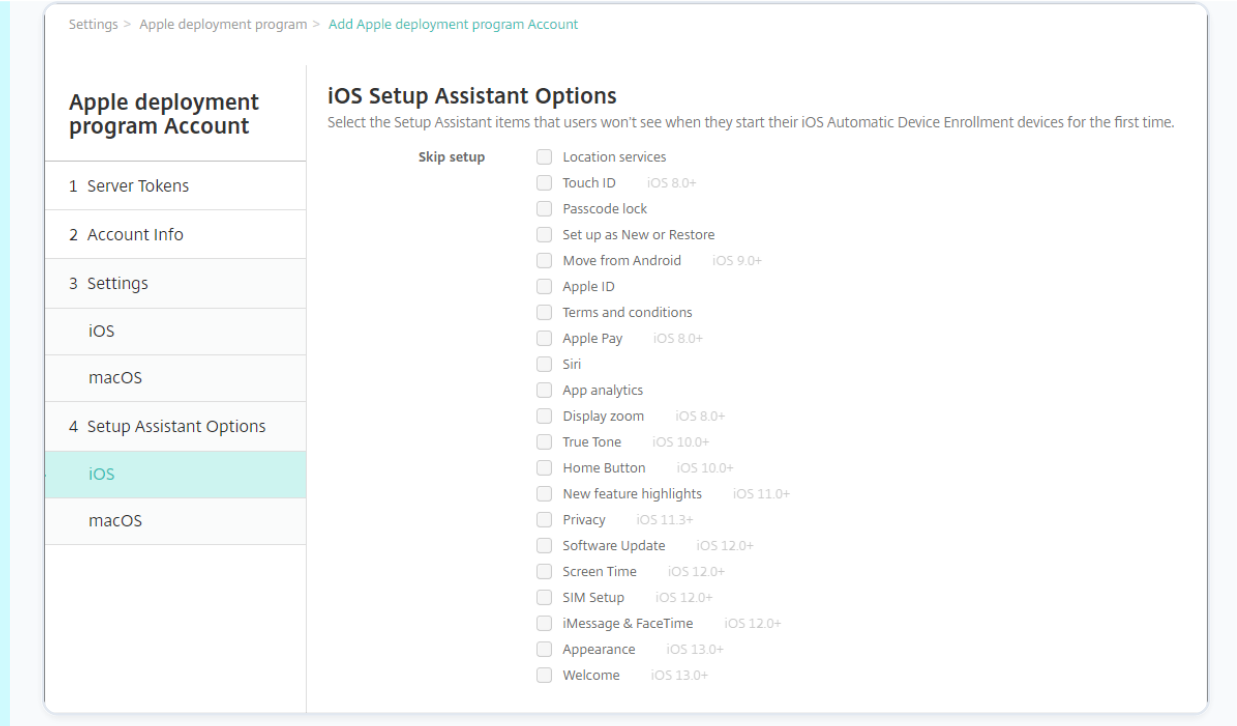


- **Configurações de registro**
  - **Exigir registro de dispositivo:** Exija que os usuários registrem seus dispositivos. Altere esta configuração para **Não**.
  - **Exigir credenciais para registro de dispositivo:** Exija que os usuários insiram suas credenciais durante a configuração do Programa de Implantação da Apple. Para a integração do ASM com o XenMobile, esta configuração é **Sim** por padrão e não pode ser alterada. O Programa de Implantação da Apple exige credenciais para o registro de dispositivos.
  - **Aguardar a conclusão da configuração:** Se os dispositivos do usuário devem permanecer no modo Assistente de Configuração até que todos os recursos MDM sejam implantados no dispositivo. Para a integração do ASM com o XenMobile, esta configuração é **Não** por padrão. De acordo com a documentação da Apple, os seguintes comandos podem não funcionar enquanto um dispositivo estiver no modo Assistente de Configuração:
    - InviteToProgram
    - InstalarAplicativo
    - InstalarMídia
    - AplicarCódigoDeResgate

- **Configurações do dispositivo**
  - **Modo supervisionado:** Coloque os dispositivos iOS em modo supervisionado. Não altere o padrão **Sim**. Para obter detalhes sobre como colocar um dispositivo iOS em modo supervisionado, consulte Para colocar um dispositivo iOS em modo supervisionado usando o Apple Configurator.
  - **Modo compartilhado:** Habilite o modo compartilhado em iPads. Dispositivos que não atendem aos requisitos mínimos não podem compartilhar.
  - **Permitir remoção do perfil de registro:** Para integração com o ASM, permita que o usuário remova o perfil de registro do dispositivo. Altere esta configuração para **Sim**.
  - **Permitir emparelhamento de dispositivos:** Para integração com o ASM, permita o emparelhamento de dispositivos para que você possa gerenciá-los através da Apple App Store e do Apple Configurator. Altere esta configuração para **Sim**.

5. Em **Opções do Assistente de Configuração do iOS**, selecione as etapas do Assistente de Configuração do iOS a serem ignoradas quando os usuários iniciarem seus dispositivos pela primeira vez. Por padrão, o Assistente de Configuração inclui todas as etapas. Considere que a remoção de etapas do Assistente de Configuração simplifica a experiência do usuário.

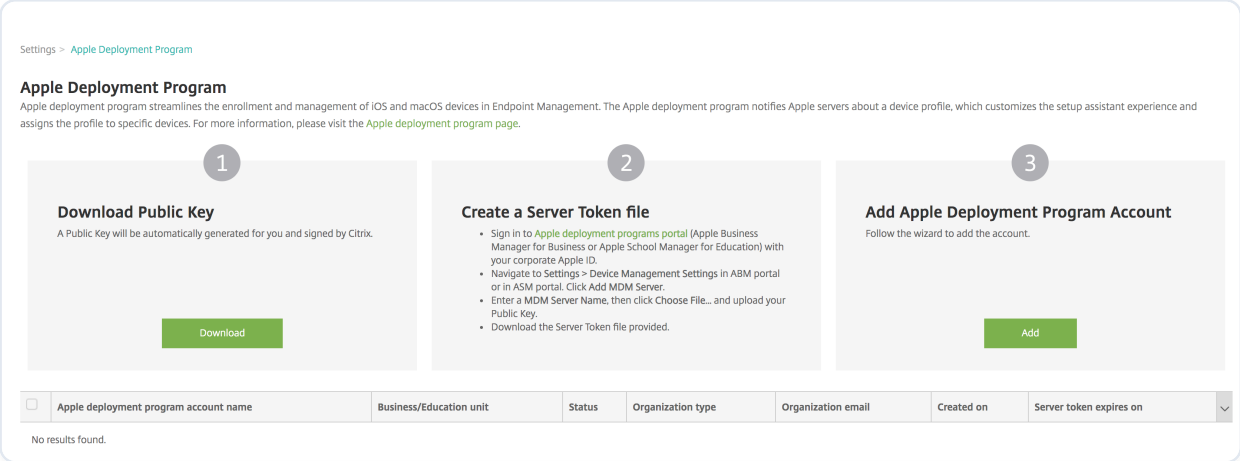
> **Importante:**
>
> A Citrix recomenda fortemente que você inclua as etapas de **ID Apple** e **Termos e Condições**. Essas etapas permitem que instrutores e alunos forneçam suas novas senhas de ID Apple Gerenciado e aceitem os termos e condições exigidos.



- **Serviços de localização:** Configure o serviço de localização no dispositivo.
- **Touch ID:** Configure o Touch ID em dispositivos iOS.
- **Bloqueio por código:** Crie um código para o dispositivo.
- **Configurar como Novo ou Restaurar:** Configure o dispositivo como novo ou a partir de um backup do iCloud ou da Apple App Store.
- **Mover do Android:** Habilite a transferência de dados de um dispositivo Android para um dispositivo iOS. Esta opção está disponível apenas quando **Configurar como Novo ou Restaurar** é selecionado (ou seja, a etapa é ignorada).
- **Apple ID:** Configure uma conta Apple ID para o dispositivo. A Citrix recomenda que você selecione a caixa de seleção para incluir esta etapa.
- **Termos e condições:** Exija que os usuários aceitem os termos e condições para o uso do dispositivo. A Citrix recomenda que você selecione a caixa de seleção para incluir esta etapa.
- **Apple Pay:** Configure o Apple Pay em dispositivos iOS.
- **Siri:** Usar ou não usar a Siri no dispositivo.
- **Análise de aplicativos:** Configure se deseja compartilhar dados de falhas e estatísticas de uso com a Apple.
- **Zoom da tela:** Configure a resolução da tela (padrão ou ampliada) em dispositivos iOS.
- **True Tone:** Configure a Tela True Tone em dispositivos iOS.
- **Botão Início:** Configure a sensibilidade da tela do Botão Início.

- **Destaques de novos recursos:** Configure as telas informativas de integração, Acessar o Dock de Qualquer Lugar e Alternar Entre Aplicativos Recentes em dispositivos iOS 11.0 (versão mínima).
- **Privacidade:** Impede que os usuários vejam o painel de dados e privacidade durante a configuração de dispositivos do Programa de Implantação da Apple. Para iOS 11.3 e posterior.
- **SoftwareUpdate:** Impede que o usuário veja a tela de atualização de software obrigatória durante a configuração dos dispositivos do Programa de Implantação da Apple. Para iOS 12.0 e posterior.
- **Tempo de Uso:** Impede que o usuário veja a tela de Tempo de Uso durante a configuração dos dispositivos do Programa de Implantação da Apple. Para iOS 12.0 e posterior.
- **Configuração do SIM:** Impede que o usuário veja a tela Adicionar Plano Celular durante a configuração dos dispositivos do Programa de Implantação da Apple. Para iOS 12.0 e posterior.
- **iMessage & FaceTime:** Impede que o usuário veja a tela do iMessage e FaceTime durante a configuração dos dispositivos do Programa de Implantação da Apple. Para iOS 12.0 e posterior.

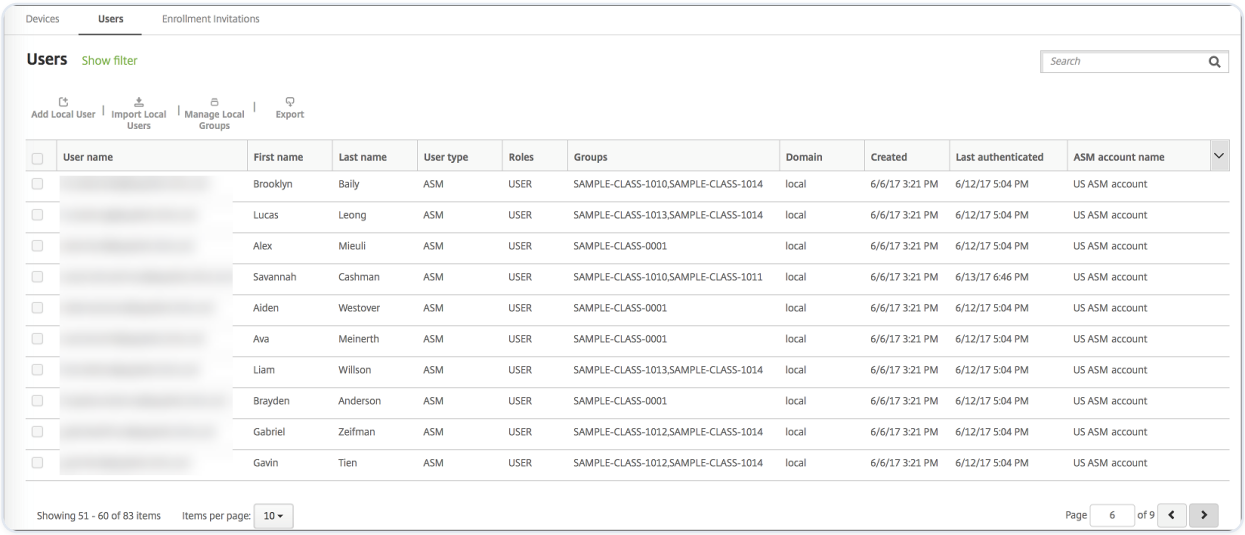
6. A conta aparece em **Configurações > Programa de Implantação da Apple**. Para testar a conectividade entre o XenMobile e sua conta ASM, selecione a conta e clique em **Testar Conectividade**.



Uma mensagem de status é exibida.



Após alguns minutos, as contas de usuário do ASM aparecem na página **Gerenciar > Usuários**. O XenMobile cria contas de usuário locais com base no ID Apple Gerenciado importado para cada usuário. No exemplo a seguir, o prefixo do nome de domínio dos IDs Apple personalizados para contas de usuário é `appleid`.

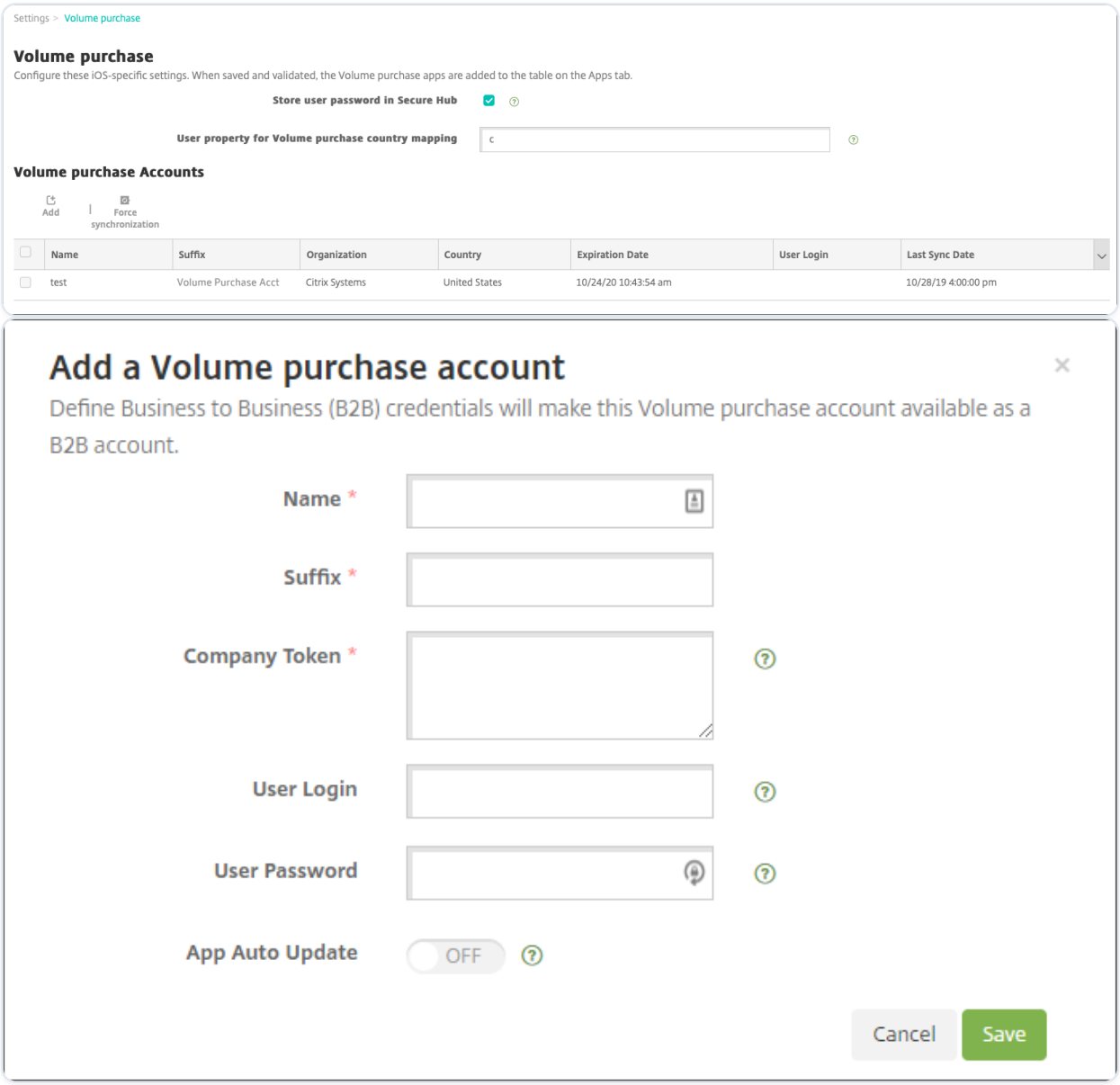


Para encontrar todos os usuários de uma determinada conta ASM, digite o nome da conta no filtro de pesquisa de usuário.

Etapa 4: Configurar uma conta de compra por volume de Educação para o Apple School Manager

Nesta seção, você aponta o XenMobile para a conta de compra por volume que você usa para adquirir licenças de compra por volume para aplicativos e iBooks.

1. Para configurar uma conta de compra por volume de Educação para o ASM, siga as instruções em Compra por Volume da Apple. A tela Adicionar uma conta de compra por volume exige que você forneça um Token da Empresa. Baixe seu token diretamente da sua conta de compra por volume de Educação e cole-o na tela **Adicionar uma conta de compra por volume**.



2. Aguarde alguns minutos para que as licenças de compra por volume sejam importadas para o XenMobile.

Etapa 5: Adicionar senhas para usuários do Apple School Manager

Depois de adicionar uma conta ASM, o XenMobile importa classes e usuários do ASM. O XenMobile trata as classes como grupos locais e usa o termo "grupo" no console. Se uma classe tiver um nome de grupo no ASM, o XenMobile atribui o nome do grupo à classe. Caso contrário, o XenMobile usa o ID do sistema de origem para o nome do grupo. O XenMobile não usa o nome do curso para o nome da classe porque os nomes dos cursos no ASM não são exclusivos.

O XenMobile usa os Managed Apple IDs para criar usuários locais com o tipo de usuário **ASM**. Os usuários são locais porque o ASM cria as credenciais independentemente de todas as fontes de dados externas. Como resultado, o XenMobile não usa um servidor de diretório para autenticar esses novos usuários.

O ASM não envia senhas temporárias de usuário para o XenMobile. Você pode importá-las de um arquivo CSV ou adicioná-las manualmente. Para importar senhas temporárias de usuário:

1. Obtenha o arquivo CSV gerado pelo ASM ao criar as senhas temporárias do Managed Apple ID.
2. Edite o arquivo CSV, substituindo as senhas temporárias por novas senhas que os usuários fornecem para se inscrever no XenMobile. Não há restrição quanto ao tipo de senha para essa finalidade.

   O formato de uma entrada no arquivo CSV é o seguinte: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   Onde:

   Usuário: `user@appleid.citrix.com`

   Primeiro nome: `Firstname`

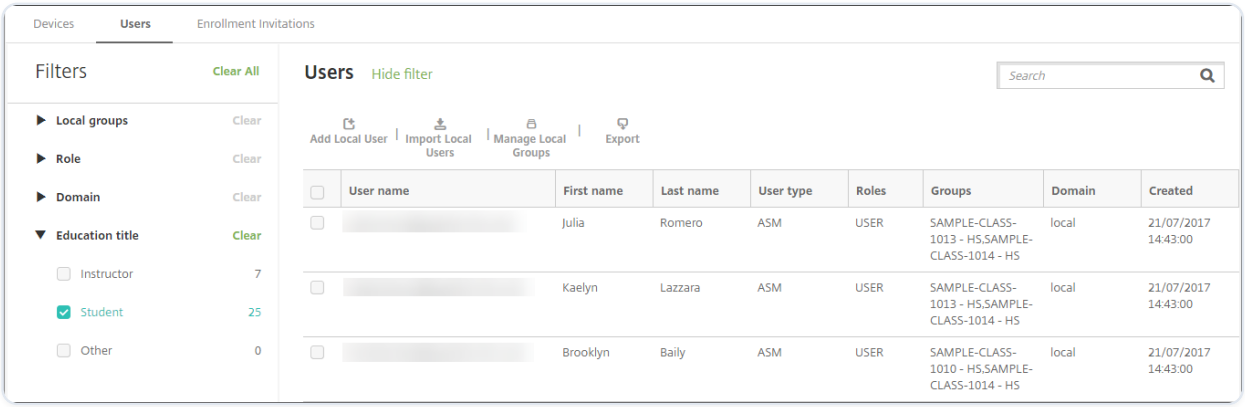
   Nome do meio: `Middle`

   Sobrenome: `Lastname`

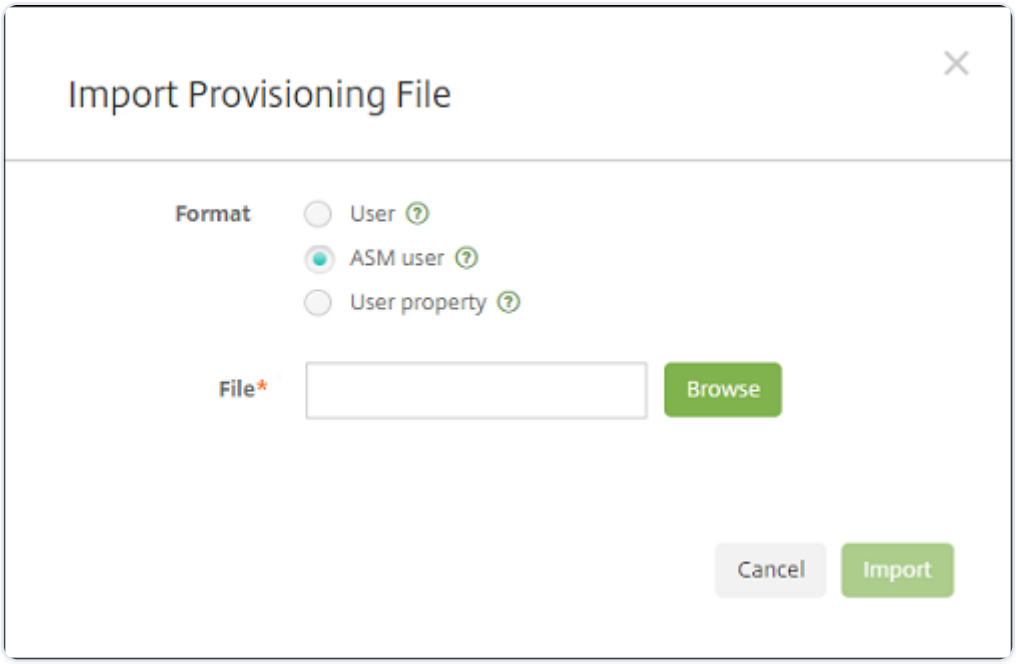
   Senha: `Password123!`!
3. No console do XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.

   A amostra de tela **Gerenciar > Usuários** a seguir mostra uma lista de usuários importados do ASM. Na lista **Usuários**:

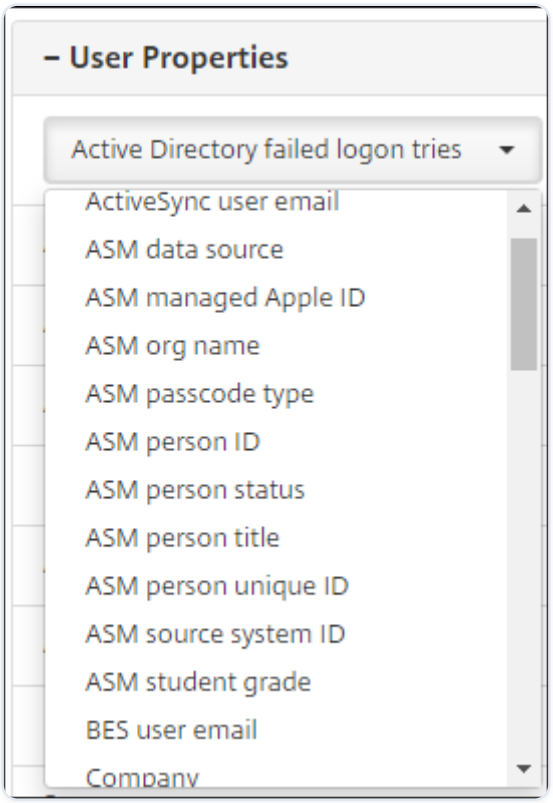
   - **Nome de usuário** mostra o Apple ID gerenciado.
   - Tipo de usuário é **ASM**, para indicar que a conta se originou do ASM.
   - **Grupos** mostram as turmas.



4. Clique em **Importar Usuários Locais**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.
5. Para Formato, escolha **usuário ASM**, navegar até o arquivo CSV que você preparou na etapa 2 e, em seguida, clique em **Importar**.



6. Para visualizar as propriedades de um usuário local, selecione o usuário e, em seguida, clique em **Editar**.



Além das propriedades de nome, estas propriedades ASM estão disponíveis:

- **Fonte de dados ASM:** A fonte de dados da turma, como **CSV** ou **SFTP**.
- **ID Apple gerenciado ASM:** Um ID Apple gerenciado pode incluir o nome da sua instituição e `appleid`. Por exemplo, o ID pode se assemelhar a `johnappleseed@appleid.myschool.edu`. O XenMobile requer um ID Apple gerenciado para autenticação.
- **Nome da organização ASM:** O nome que você deu à conta no XenMobile.
- **Tipo de senha ASM:** Política de senha da pessoa: **complexa** (uma senha não estudantil de oito ou mais números e letras), **quatro** (dígitos) ou **seis** (dígitos).
- **ID exclusivo da pessoa ASM:** Identificador para o usuário.
- **Status da pessoa ASM:** Especifica se o ID Apple gerenciado está **Ativo** ou **Inativo**. Este status se torna ativo depois que o usuário fornece sua nova senha para a conta do ID Apple gerenciado.
- **Título da pessoa ASM:** Instrutor, Aluno ou Outro.
- **ID exclusivo da pessoa ASM:** Identificador exclusivo para o usuário.
- **ID do sistema de origem ASM:** Identificador para a origem do sistema.
- **Nota do aluno ASM:** Informações sobre a nota do aluno (não usadas por instrutores).

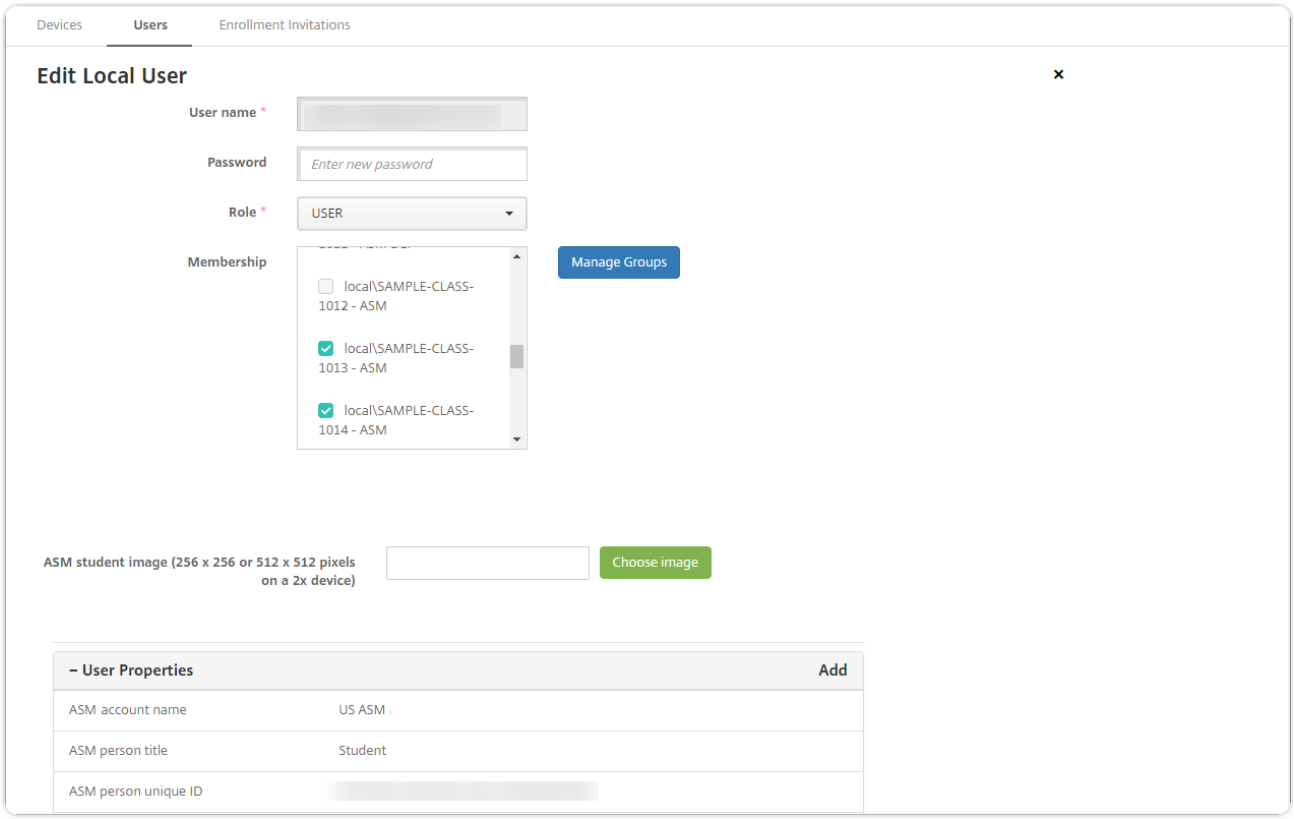
Etapa 6: Opcionalmente, adicione fotos de alunos

Você pode adicionar uma foto de cada aluno. Se os instrutores usarem o aplicativo Apple Classroom, as fotos aparecerão neste aplicativo.

Recomendado para fotos:

- Resolução: 256 x 256 pixels (512 x 512 pixels em um dispositivo 2x)
- Formato: JPEG, PNG ou TIFF

Para adicionar uma foto, vá para **Gerenciar > Usuários**, selecione um usuário, clique em **Editar** e, em seguida, clique em **Escolher imagem**.



Etapa 7: Planejar e adicionar recursos e grupos de entrega ao XenMobile

Um grupo de entrega especifica os recursos a serem implantados para categorias de usuários. Por exemplo, você pode criar um grupo de entrega para instrutores e alunos. Alternativamente, você pode criar vários grupos de entrega para personalizar os aplicativos, mídias e políticas enviados a vários instrutores ou alunos. Você pode criar um ou mais grupos de entrega por turma. Você também pode criar um ou mais grupos de entrega para gerentes (outros funcionários em sua instituição de ensino).

Os recursos que você implanta em dispositivos de usuário incluem políticas de dispositivo, aplicativos de compra por volume e iBooks.

- Políticas de dispositivo:

  Se os instrutores usarem o aplicativo Classroom, a política de dispositivo de Configuração de Educação será necessária. Certifique-se de revisar outras políticas de dispositivo para determinar como você deseja configurar e restringir os iPads de instrutores e alunos.

- Aplicativos de compra por volume:

  O XenMobile exige que você implante aplicativos de compra por volume como aplicativos obrigatórios para usuários de educação. O XenMobile não oferece suporte à implantação de tais aplicativos de compra por volume como opcionais.

Se você usar o aplicativo Apple Classroom, implante-o apenas em dispositivos de instrutores.

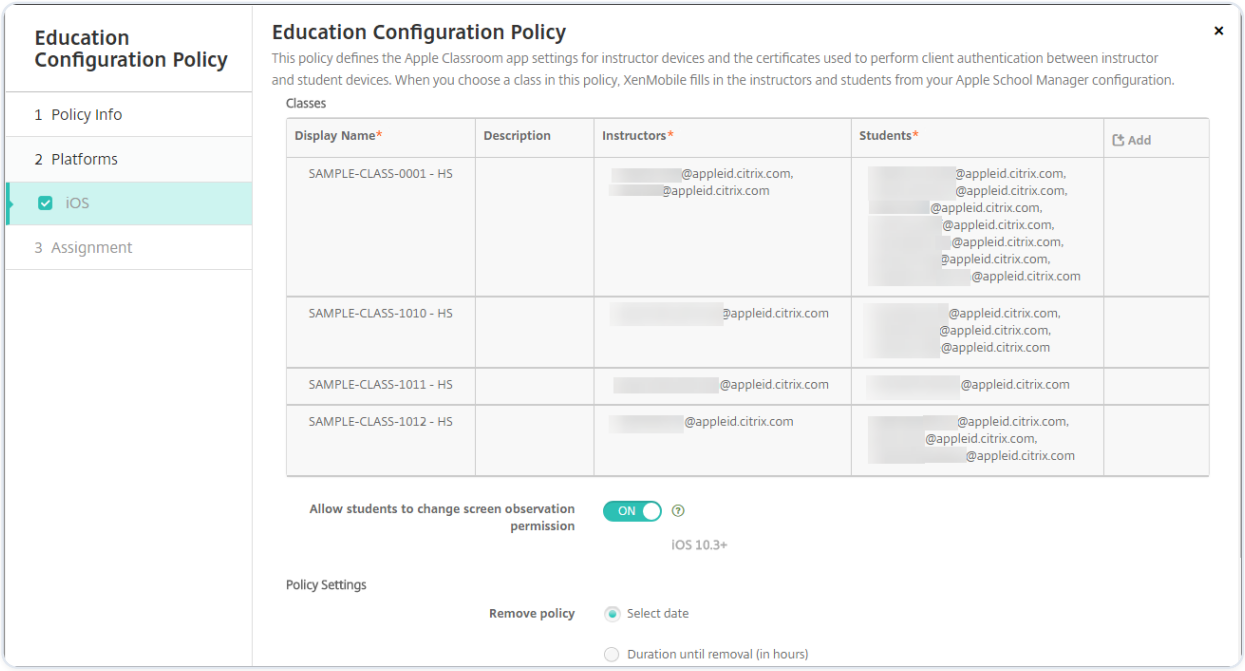
Implante quaisquer outros aplicativos que você deseja fornecer a instrutores ou alunos. Esta solução não usa o aplicativo Citrix Secure Hub, portanto, não há necessidade de implantá-lo para instrutores ou alunos.

- iBooks de compra por volume:

  Depois que o XenMobile se conectar à sua conta ASM, seus iBooks comprados aparecerão no console do XenMobile em **Configurar > Mídia**. Os iBooks listados nessa página estão disponíveis para serem adicionados a grupos de entrega. O XenMobile oferece suporte à adição de iBooks apenas como mídia obrigatória.

Depois de planejar os recursos e grupos de entrega para instrutores e alunos, você pode criar esses itens no console do XenMobile.

1. Crie quaisquer políticas de dispositivo que você deseja implantar em dispositivos de instrutores ou alunos. Para obter informações sobre a política de dispositivo de Configuração de Educação, consulte Política de dispositivo de Configuração de Educação.



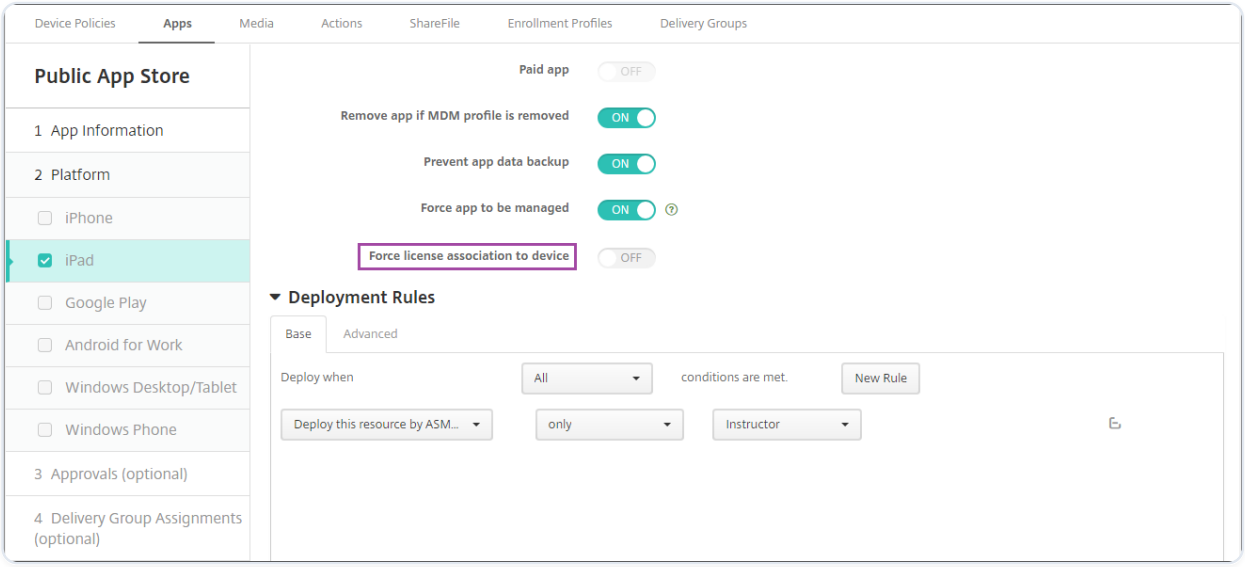
   Para obter informações sobre políticas de dispositivo, consulte Políticas de dispositivo e os artigos de política individuais.

2. Configure aplicativos (**Configurar > Aplicativos**) e iBooks (**Configurar > Mídia**):

   - Por padrão, o XenMobile atribui aplicativos e iBooks no nível do usuário. Durante a primeira implantação, instrutores e alunos recebem um prompt para se registrar no ASM. Após aceitar o convite, os usuários recebem seus aplicativos e iBooks do ASM na próxima

implantação (dentro de seis horas). A Citrix recomenda que você force a implantação de aplicativos e iBooks para novos usuários do ASM. Para fazer isso, selecione o grupo de entrega e clique em **Implantar**.

Você pode optar por atribuir aplicativos (mas não iBooks) no nível do dispositivo. Para fazer isso, altere a configuração **Forçar associação de licença ao dispositivo** para **Ativado**. Ao atribuir aplicativos no nível do dispositivo, os usuários não recebem um convite para participar da compra por volume da Apple.

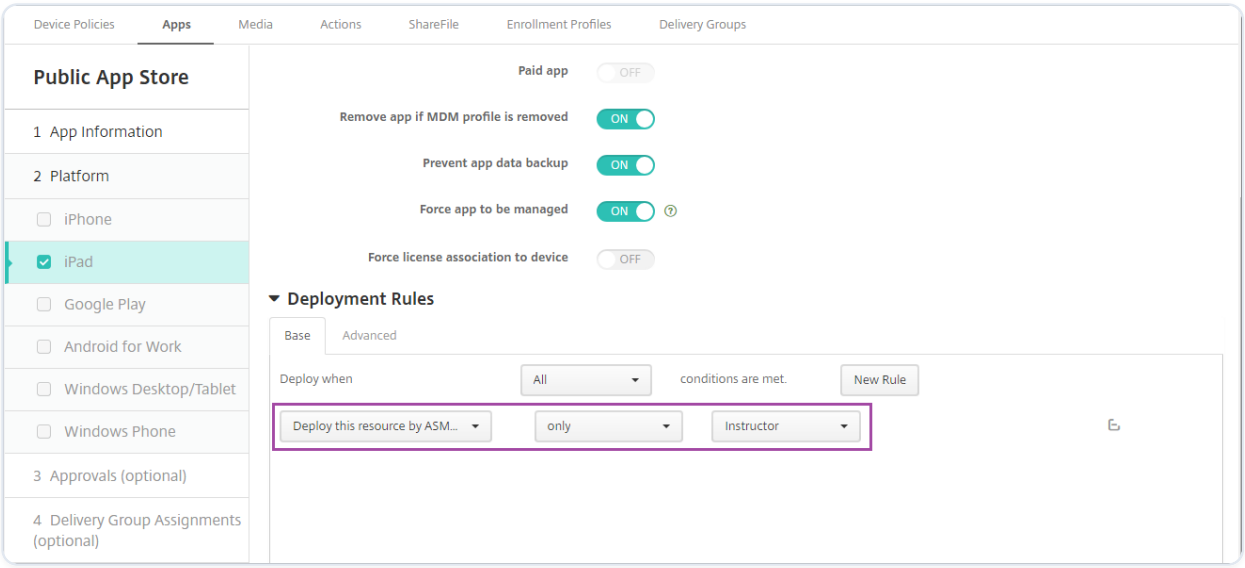


- Para implantar um aplicativo apenas para instrutores, selecione um grupo de entrega que inclua apenas instrutores ou use a seguinte regra de implantação:

```
Deploy this resource by ASM device type

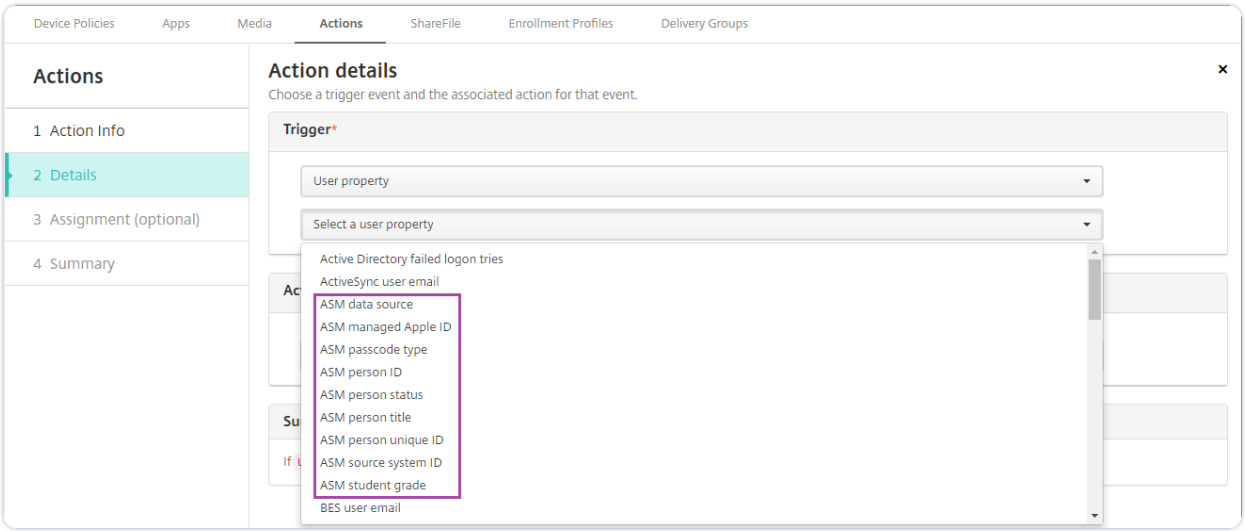
only

Instructor
```



- Para obter ajuda com a adição de aplicativos de compra por volume, consulte Adicionar um aplicativo da App Store pública.

3. Opcional. Crie ações com base nas propriedades do usuário do ASM. Por exemplo, você pode criar uma ação para enviar uma notificação para dispositivos de alunos quando um novo aplicativo for instalado. Alternativamente, você pode criar uma ação que uma propriedade de usuário aciona, conforme mostrado no exemplo a seguir.



Para criar uma ação, vá para **Configurar > Ações**. Para obter informações sobre como configurar ações, consulte Ações automatizadas.

4. Em **Configurar > Grupos de Entrega**, crie grupos de entrega para instrutores e para alunos. Escolha as turmas que foram importadas do ASM. Além disso, crie uma regra de implantação para instrutores e alunos.

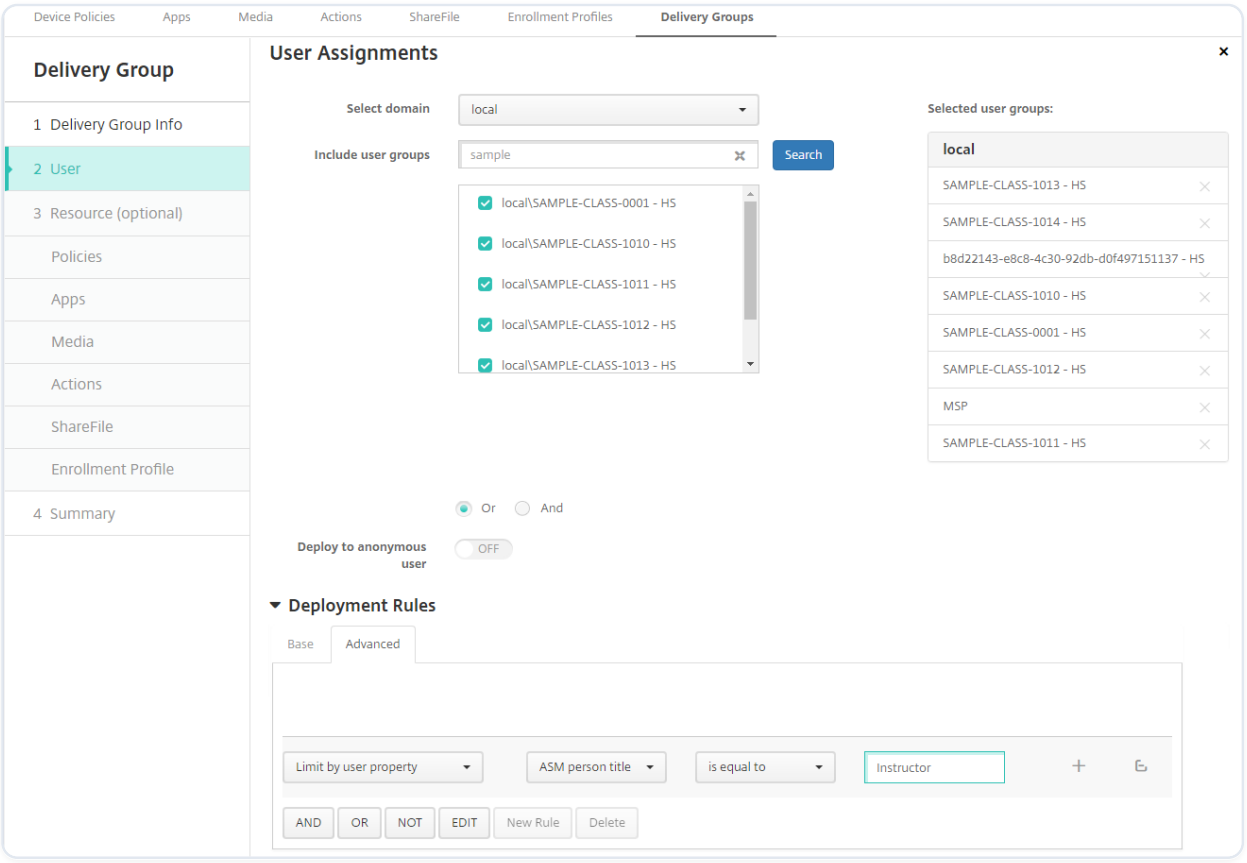
   Por exemplo, as seguintes atribuições de usuário são para instrutores. A regra de implantação é:

```
Limit by user property

ASM person title

is equal to

Instructor
```



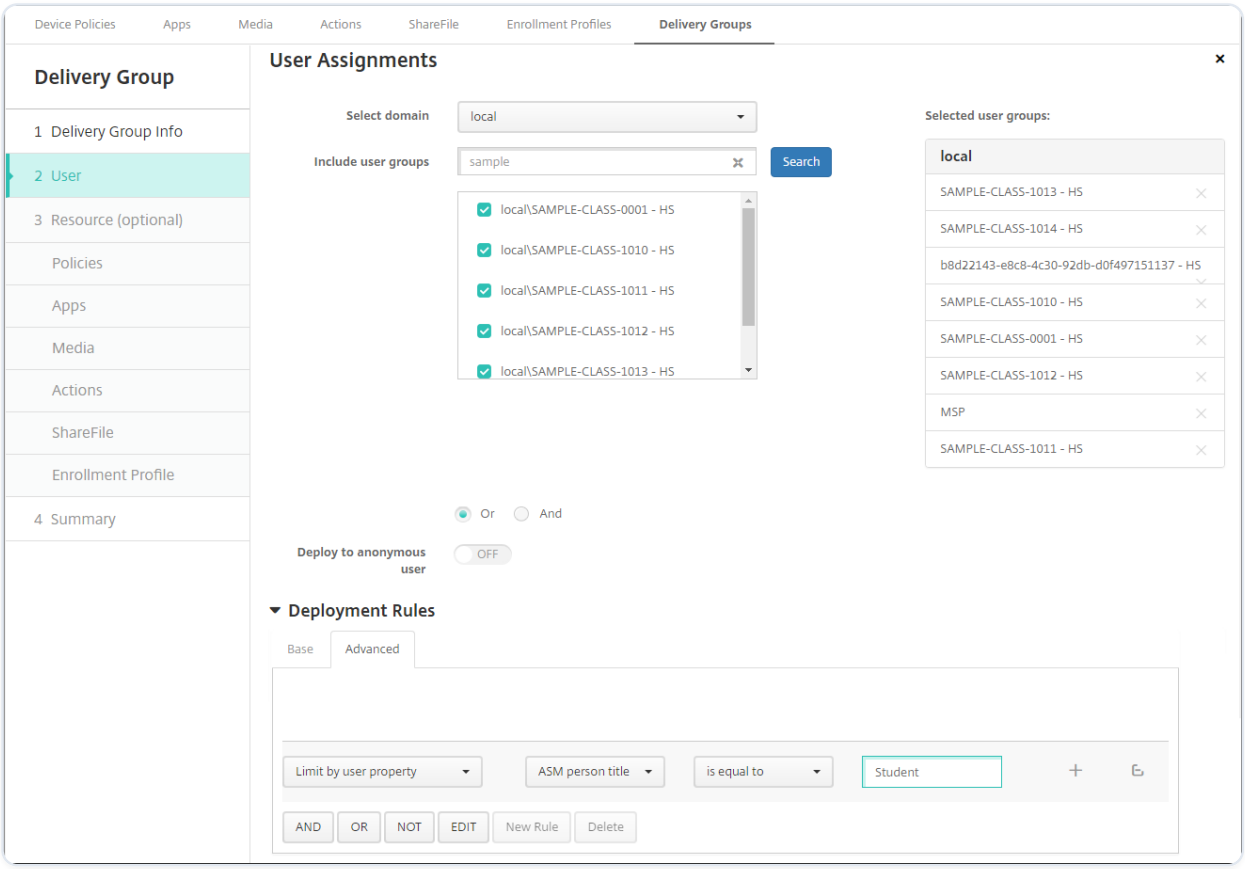
As seguintes atribuições de usuário são para alunos. A regra de implantação é:

```
Limit by user property

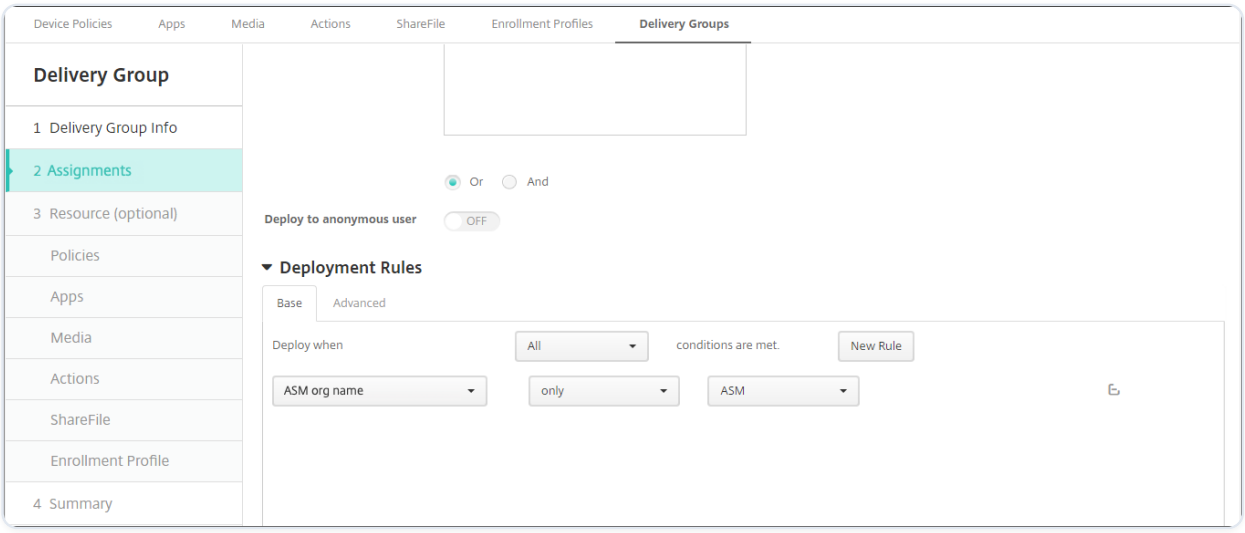
ASM person title

is equal to

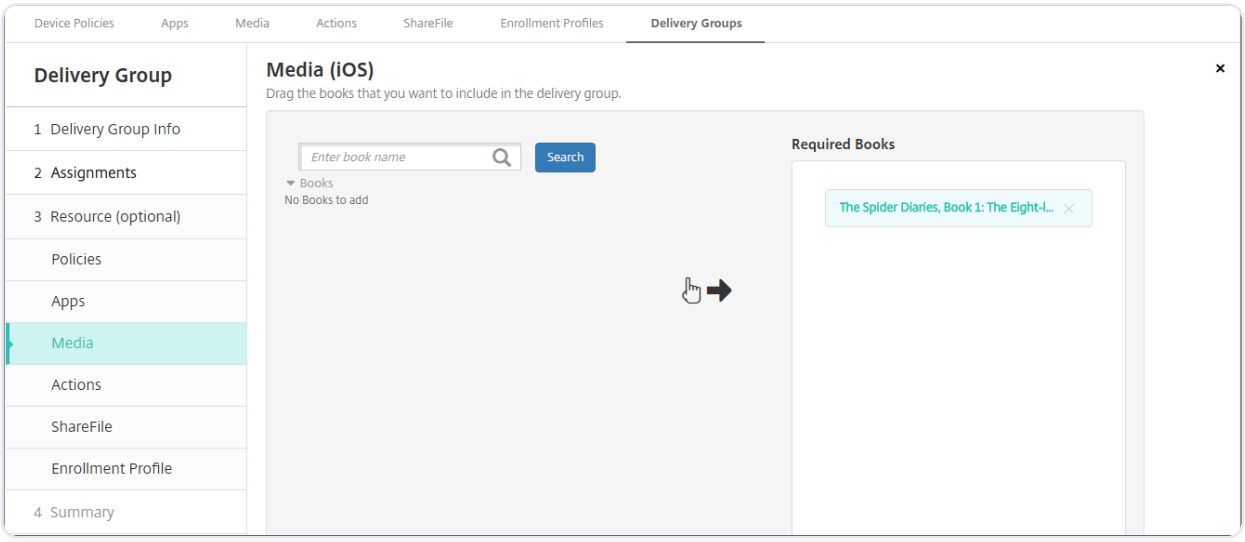
Student
```



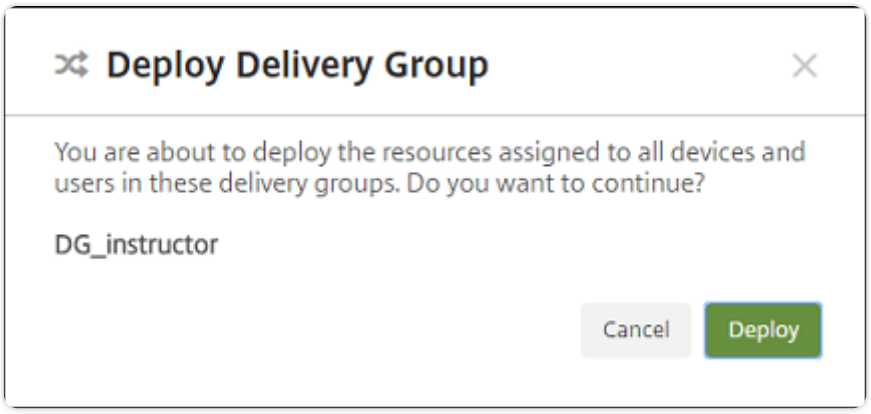
Você também pode filtrar um grupo de entrega usando uma regra de implantação baseada no nome da organização ASM.



5. Atribua os recursos aos grupos de entrega. O exemplo a seguir mostra um iBook contido em um grupo de entrega.



O exemplo a seguir mostra a caixa de diálogo de confirmação que aparece quando você seleciona um grupo de entrega e clica em **Implantar**.



Para obter mais informações, consulte "Para editar um grupo de entrega" e "Para implantar em grupos de entrega" em Implantar recursos.

Etapa 8: Testar os registros de dispositivos de instrutores e alunos

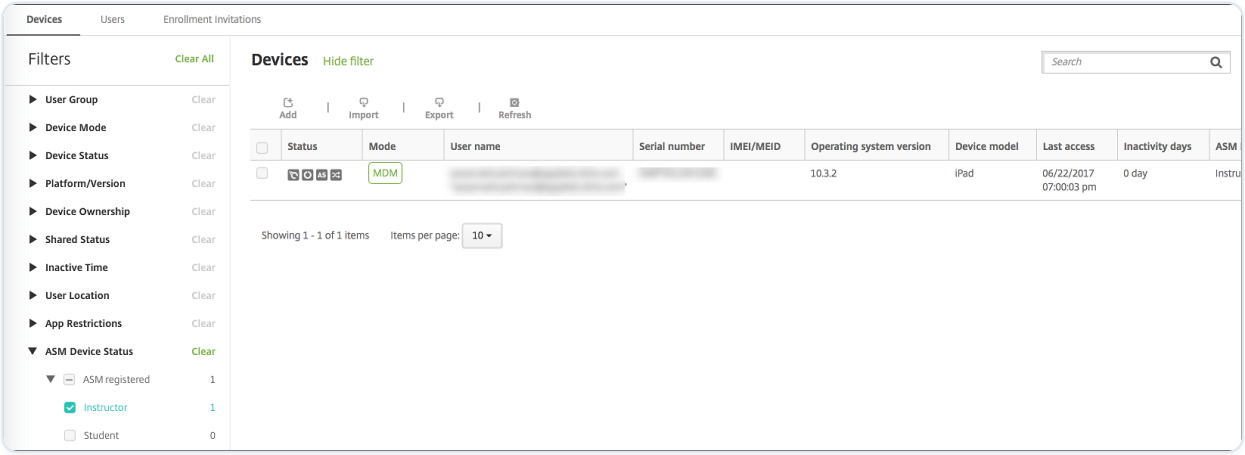
Você pode registrar dispositivos por meio de um dos seguintes métodos:

- Um administrador escolar pode registrar dispositivos de instrutores e alunos usando a senha de usuário que você pode definir no console do XenMobile. Como resultado, você pode fornecer aos usuários dispositivos que já estão configurados com aplicativos e mídias.
- Quando os usuários recebem os dispositivos, eles se registram usando a senha de usuário que você lhes fornece. Após a conclusão do registro, o XenMobile envia políticas de dispositivo, aplicativos e mídias para os dispositivos.

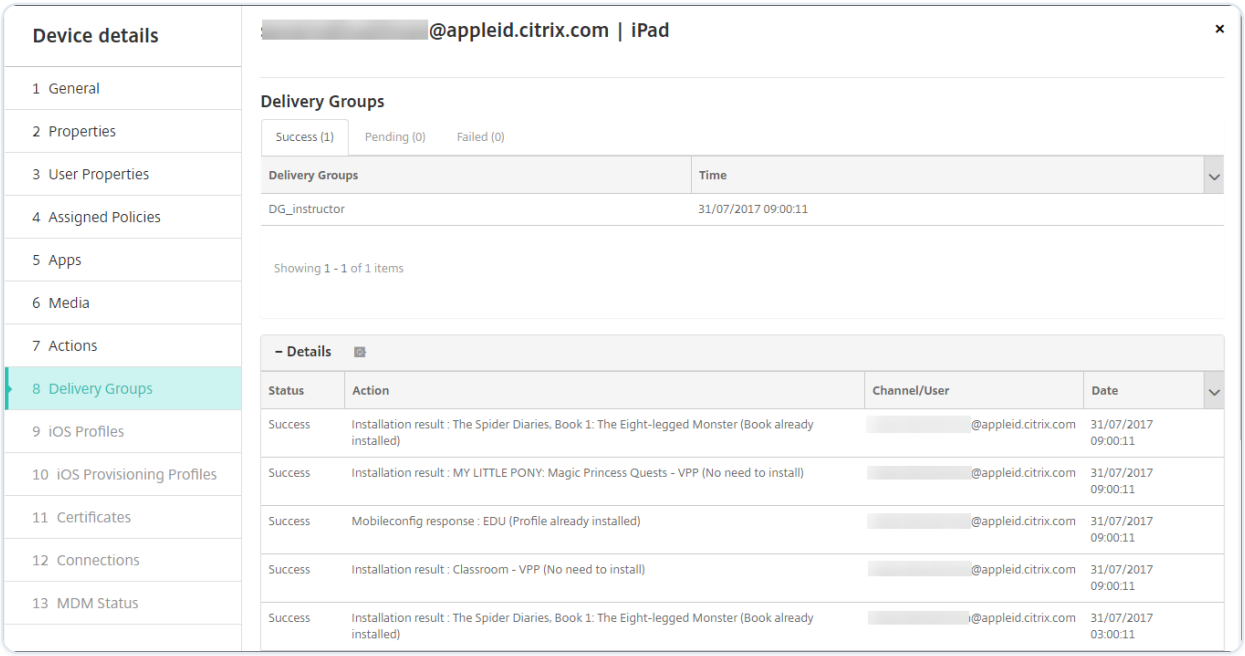
Para testar o registro, use dispositivos do Programa de Implantação da Apple que estejam vinculados ao ASM.

1. Se os dispositivos não estiverem vinculados ao ASM, apague o conteúdo e as configurações do dispositivo fazendo uma redefinição completa.
2. Registre um dispositivo ASM com um instrutor. Em seguida, registre um dispositivo ASM com um aluno.
3. Na página **Gerenciar > Dispositivos**, verifique se ambos os dispositivos ASM estão registrados apenas no MDM.

   Você pode filtrar a página **Dispositivos** pelo status do dispositivo ASM: **ASM registrado**, **ASM compartilhado**, **Instrutor** e **Aluno**.



4. Para verificar se os recursos MDM foram implantados corretamente para cada dispositivo: Selecione o dispositivo, clique em **Editar** e verifique as várias páginas.



Passo 9: Distribuir dispositivos

A Apple recomenda que você organize um evento para que possa distribuir os dispositivos a instrutores e alunos.

Se você não distribuir dispositivos pré-registrados, forneça também o seguinte a esses usuários:

- Senhas do XenMobile para registro
- Senhas temporárias do ASM para Managed Apple IDs.

A experiência do usuário pela primeira vez é a seguinte.

1. Na primeira vez que um usuário inicia seu dispositivo após uma redefinição de fábrica, o XenMobile o solicita na tela de registro para registrar seu dispositivo.
2. O usuário fornece seu Managed Apple ID e a senha do XenMobile usados para autenticar no XenMobile.
3. Na etapa de configuração do Apple ID, o dispositivo solicita ao usuário que forneça seu Managed Apple ID e a senha temporária do ASM. Esses itens autenticar o usuário nos serviços da Apple.
4. O dispositivo solicita ao usuário que crie uma senha para seu Managed Apple ID, usada para proteger seus dados no iCloud.
5. Ao final do Assistente de Configuração, o XenMobile começa a instalar as políticas, aplicativos e mídias no dispositivo. Para aplicativos e iBooks atribuídos no nível do usuário, o assistente solicita que instrutores e alunos se registrem para compra por volume. Após aceitar o convite, os usuários recebem seus aplicativos e iBooks de compra por volume na próxima implantação (dentro de seis horas).

Gerenciar dados de instrutores, alunos e turmas

Ao gerenciar dados de instrutores, alunos e turmas, observe o seguinte:

- Não altere os Managed Apple IDs depois de importar as informações do ASM para o XenMobile. O XenMobile também usa identificadores de usuário do ASM para identificar usuários.
- Se você adicionar ou alterar dados de turma no ASM depois de criar uma ou mais políticas de dispositivo de Configuração de Educação: Edite as políticas e, em seguida, reimplemente-as.
- Se o instrutor de uma turma mudar depois que você implantar a política de dispositivo de Configuração de Educação: Revise a política para garantir que ela seja atualizada no console do XenMobile e, em seguida, reimplemente a política.

- Se você atualizar as propriedades do usuário no portal ASM, o XenMobile também atualizará essas propriedades no console. No entanto, o XenMobile não recebe a propriedade de título de pessoa do ASM (Instrutor, Aluno ou Outro) da mesma forma que recebe outras propriedades. Assim, se você alterar o título de pessoa do ASM no ASM, conclua as seguintes etapas para refletir essa alteração no XenMobile.

Para gerenciar os dados:

1. No portal ASM, atualize a nota do aluno e limpe a nota do instrutor.
2. Se você alterou uma conta de aluno para uma conta de instrutor, remova o usuário da lista de alunos da turma. Em seguida, adicione o usuário à lista de instrutores na mesma turma ou em outra.

   Se você alterou uma conta de instrutor para uma conta de aluno, remova o usuário da turma. Em seguida, adicione o usuário à lista de alunos na mesma turma ou em outra. Suas atualizações aparecem no console do XenMobile durante a próxima sincronização (a cada cinco minutos por padrão) ou busca (a cada 24 horas por padrão).
3. Edite a política de dispositivo de Configuração de Educação para aplicar a alteração e reimplemente-a.

   - Se você excluir um usuário do portal ASM, o XenMobile também excluirá esse usuário do console do XenMobile após uma busca.

     Você pode reduzir o intervalo entre as duas linhas de base alterando este valor de propriedade do servidor: **bulk.enrollment.fetchRosterInfoDelay** (o padrão é **1440** minutos).
   - Depois de implantar os recursos: Se um aluno entrar em uma turma, crie um grupo de entrega apenas com esse aluno e implante os recursos para o aluno.
   - Se um aluno ou instrutor perder sua senha temporária, peça para ele entrar em contato com o administrador do ASM. O administrador pode fornecer a senha temporária ou gerar uma nova.

Gerenciar um dispositivo perdido ou roubado que está inscrito no Programa de Implantação da Apple do Apple School Manager

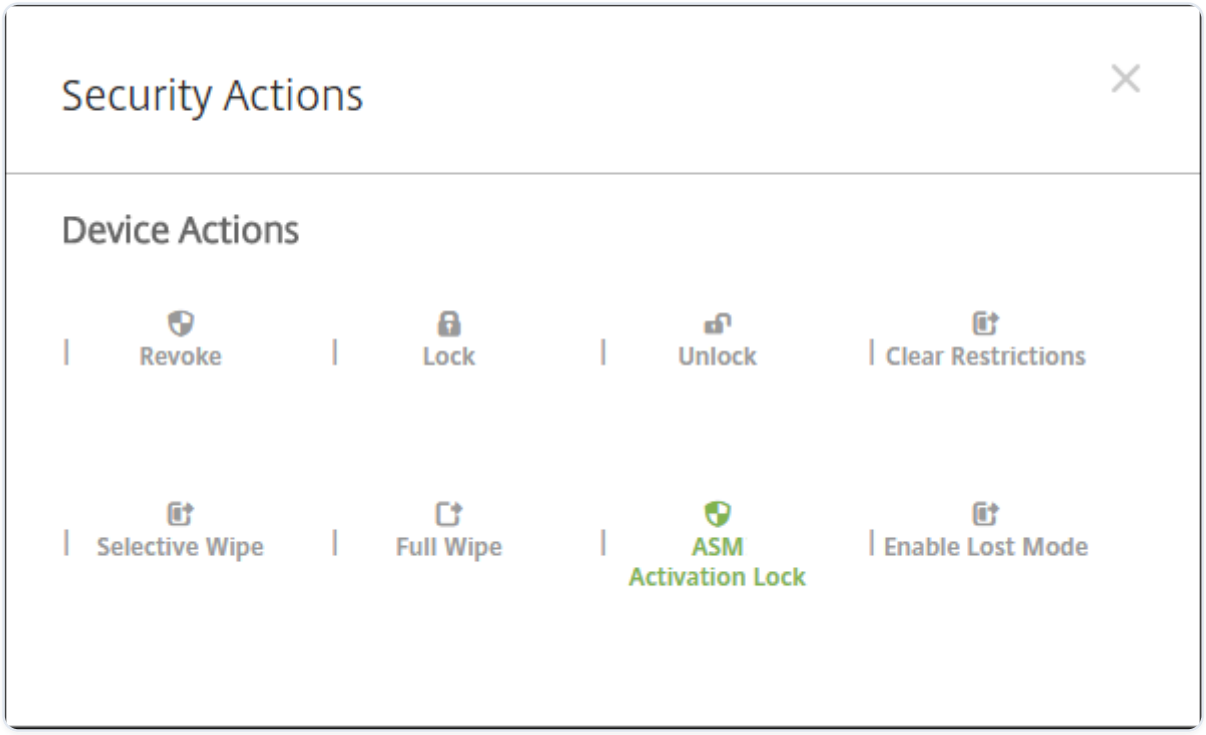
O serviço Buscar iPhone/iPad da Apple inclui um recurso de Bloqueio de Ativação. O Bloqueio de Ativação impede que usuários não autorizados usem ou revendam um dispositivo perdido ou roubado que esteja inscrito no Programa de Implantação da Apple.

O XenMobile inclui uma ação de segurança **Bloqueio de Ativação ASM** que permite enviar um código de bloqueio para um dispositivo inscrito no Programa de Implantação da Apple do ASM.

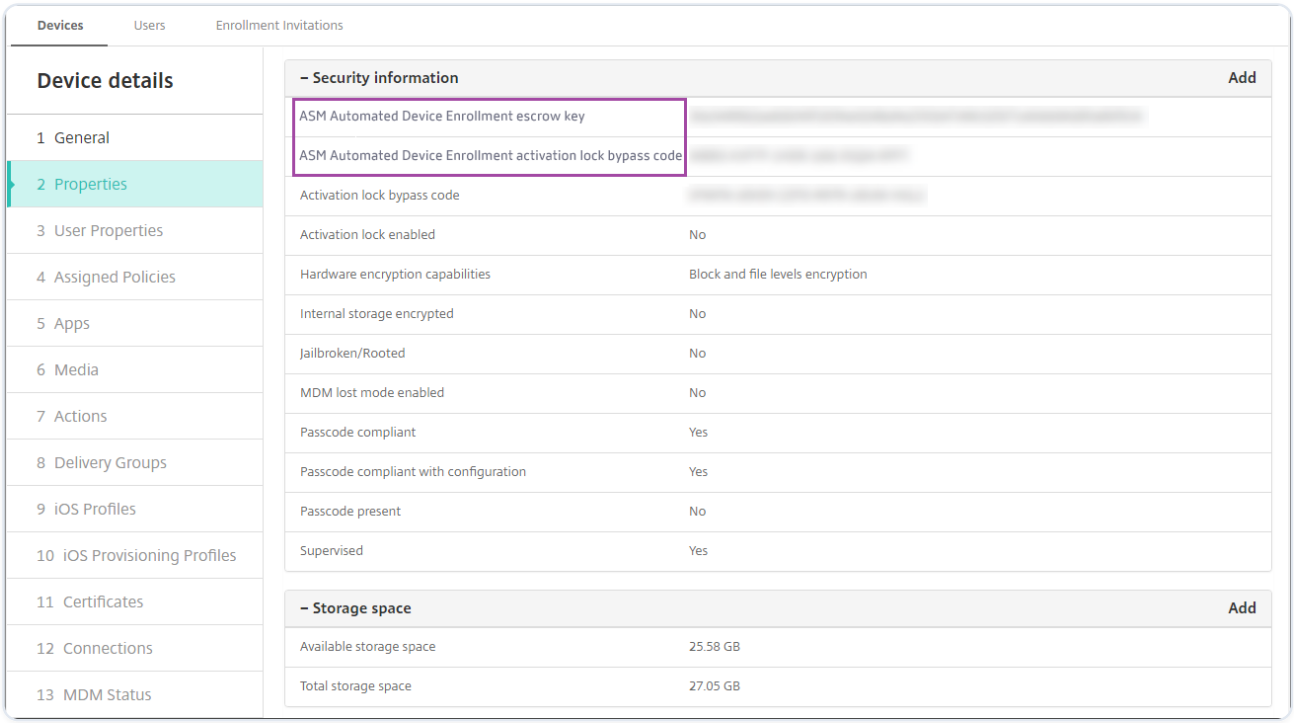
Ao usar a ação de segurança **Bloqueio de Ativação ASM**, o XenMobile pode localizar dispositivos sem exigir que os usuários ativem o serviço Buscar iPhone/iPad. Quando um dispositivo ASM é redefinido ou totalmente apagado, o usuário fornece seu ID Apple Gerenciado e senha para desbloquear o dispositivo.

Para liberar o bloqueio do console, clique na ação de segurança **Ignorar Bloqueio de Ativação**. Para obter informações sobre como ignorar um bloqueio de ativação, consulte Ignorar um bloqueio de ativação do iOS. O usuário também pode deixar o login em branco e digitar o **código de ignorar bloqueio de ativação ASM** como senha. Essa informação está disponível em **Detalhes do Dispositivo**, na guia **Propriedades**.

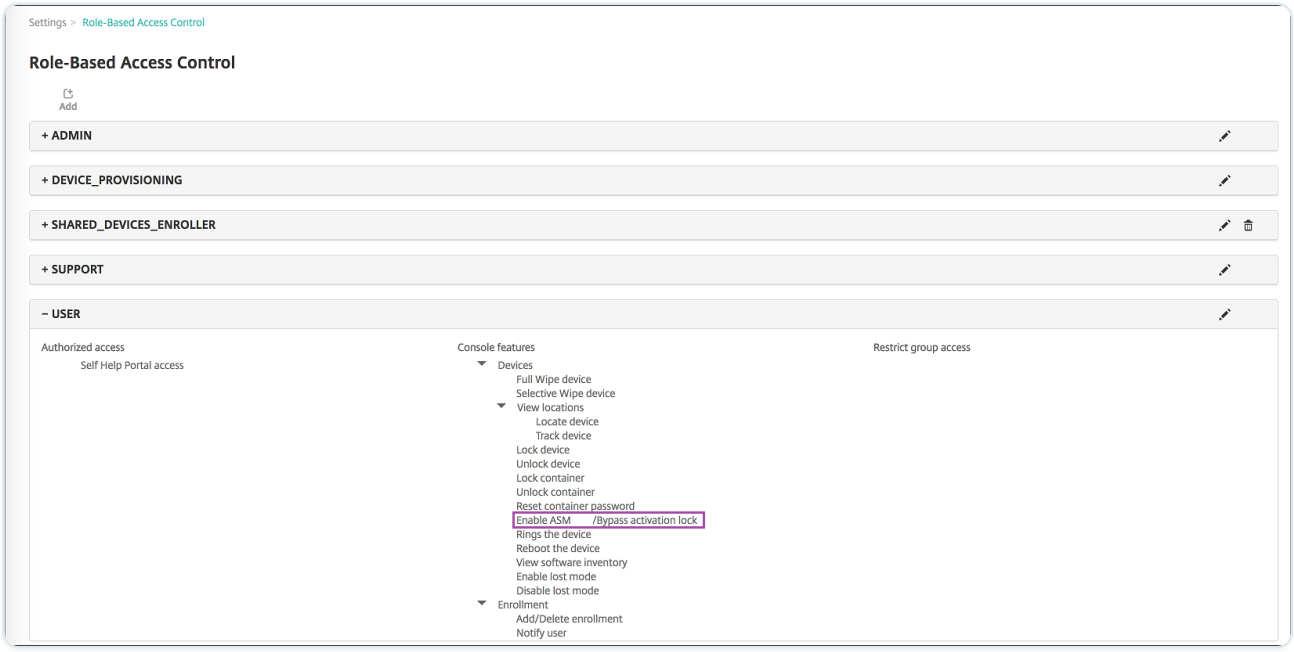
Para definir o bloqueio de ativação, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e, em seguida, clique em **Bloqueio de Ativação ASM**.



As propriedades **Chave de custódia ASM** e **código de ignorar bloqueio de ativação ASM** aparecem em **Detalhes do dispositivo**.



A permissão RBAC para um Bloqueio de Ativação ASM é **Dispositivos > Habilitar bloqueio de ativação de ignorar ASM**.



iPads Compartilhados

O recurso de iPad compartilhado permite que vários usuários utilizem um iPad. As experiências do usuário podem ser personalizadas, mesmo que os dispositivos sejam compartilhados. Você pode usar iPads compartilhados para educação ou negócios. O Apple School Manager (ASM) oferece suporte às funções de instrutor e aluno, além das funções que o Apple Business Manager (ABM) oferece.

Pré-requisitos

- Apple School Manager ou Apple Business Manager
- XenMobile® Server
- Qualquer iPad Pro, iPad de quinta geração, iPad Air 2 ou posterior e iPad mini 4 ou posterior
- Pelo menos 32 GB de armazenamento
- Supervisionado

Configurar iPads Compartilhados

Vários alunos em uma sala de aula podem compartilhar um iPad para diferentes disciplinas ensinadas por um ou vários instrutores.

Você ou os instrutores registram os iPads Compartilhados e, em seguida, implantam políticas de dispositivo, aplicativos e mídia nos dispositivos. Depois disso, os alunos fornecem suas credenciais de ID Apple gerenciado para fazer login em um iPad Compartilhado. Se você implantou anteriormente uma política de Configuração de Educação para os alunos, eles não farão mais login como um "Outro Usuário" em dispositivos compartilhados.

O XenMobile usa dois canais de comunicação para iPads Compartilhados: O canal do sistema para o proprietário do dispositivo (instrutor) e o canal do usuário para o usuário residente atual (aluno). O XenMobile usa esses canais para enviar os comandos MDM apropriados para os recursos suportados pela Apple.

Os recursos que são implantados pelo canal do sistema são:

- Políticas de dispositivo: Configuração de Educação, Número Máximo de Usuários Residentes e Período de Carência de Bloqueio por Senha
- Aplicativos de compra por volume baseados em dispositivo

  A Apple não oferece suporte a aplicativos corporativos ou aplicativos de compra por volume baseados no usuário em iPads Compartilhados. Os aplicativos instalados em um iPad Compartilhado são globais para o dispositivo e não por usuário.
- iBooks de compra por volume baseados no usuário

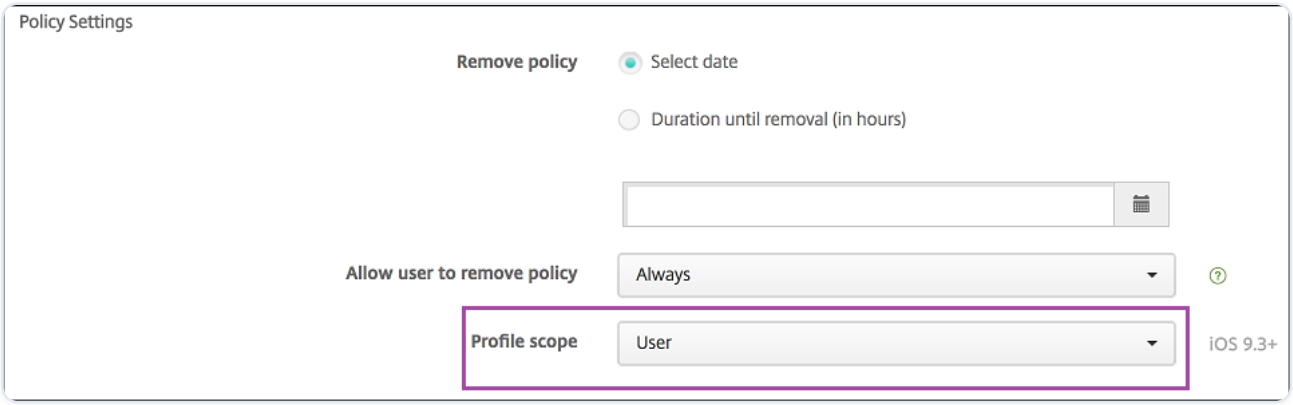
  A Apple oferece suporte à atribuição de iBooks de compra por volume baseados no usuário em iPads Compartilhados.

Os recursos que são implantados pelo canal do usuário são:

- Políticas de dispositivo: Notificações de Aplicativos, Layout da Tela Inicial, Restrições e Webclip

  O XenMobile oferece suporte apenas a essas políticas de dispositivo pelo canal do usuário.

Ao configurar políticas de dispositivo, você especifica o canal de implantação na configuração da política **Escopo do perfil**.



Para remover políticas de dispositivo que você implantou pelo canal do usuário, certifique-se de escolher um **Escopo de implantação** de **Usuário** para a política de Remoção de Perfil.

Fluxo de trabalho geral

Normalmente, você fornece iPads Compartilhados pré-configurados e supervisionados aos instrutores. Os instrutores então distribuem os dispositivos aos alunos. Se você não distribuir iPads Compartilhados pré-registrados aos instrutores: Certifique-se de fornecer aos instrutores as senhas do XenMobile Server para que eles possam registrar seus dispositivos.

O fluxo de trabalho geral para configurar e registrar iPads Compartilhados é o seguinte:

1. Use o console do XenMobile Server para adicionar contas ASM ou ABM (**Configurações** > **Programa de Implantação da Apple**) com o **Modo compartilhado** ativado. Para obter mais informações, consulte Gerenciar contas ASM ou ABM para iPads Compartilhados.
2. Conforme descrito nesta seção, adicione as políticas de dispositivo, aplicativos e mídias necessários ao XenMobile. Atribua esses recursos a grupos de entrega.
3. Peça aos instrutores para fazerem um reset de fábrica nos iPads Compartilhados. A tela de Gerenciamento Remoto para registro aparece.
4. Os instrutores registram os iPads Compartilhados.

   O XenMobile implanta recursos configurados em cada iPad Compartilhado registrado. Após uma reinicialização automática, os instrutores podem compartilhar os dispositivos com os alunos. Uma página de login aparece no iPad.

5. Um aluno escolhe a turma e, em seguida, insere seu ID Apple Gerenciado e a senha temporária do ASM ou ABM.

   O iPad Compartilhado autentica-se com o ASM ou ABM e solicita que o aluno crie uma senha do ASM ou ABM. Para o próximo login no iPad Compartilhado, o aluno deve inserir a nova senha.
6. Outro aluno que está compartilhando o iPad pode então fazer login repetindo a etapa anterior.

Gerenciar contas do Apple School Manager ou Apple Business Manager para iPads Compartilhados

Se você já usa o XenMobile com o Apple Education: Você tem uma conta ASM ou ABM existente configurada no XenMobile para dispositivos que não são compartilhados, como os dispositivos usados por instrutores. Você pode usar o mesmo ASM ou ABM e o mesmo XenMobile Server para dispositivos compartilhados e não compartilhados.

O XenMobile oferece suporte a estes cenários de implantação:

- Um grupo de iPads Compartilhados por turma

  Nesse cenário, você atribui os iPads Compartilhados a uma turma de alunos. Os iPads permanecem na sala de aula. Instrutores que ensinam diferentes matérias nessa turma usam o mesmo conjunto de iPads.
- Um grupo de iPads Compartilhados por instrutor

  Nesse cenário, você atribui os iPads Compartilhados a um instrutor, que usa esses iPads para as várias turmas que ele leciona.

Organizar iPads Compartilhados em grupos de dispositivos

O ASM ou ABM permite organizar dispositivos em grupos criando vários servidores MDM. Ao atribuir os iPads Compartilhados a um servidor MDM, crie um grupo de dispositivos para cada grupo de iPads Compartilhados, por turma ou por instrutor:

- Grupo 1 de iPads Compartilhados > Servidor MDM do Grupo de Dispositivos 1
- Grupo 2 de iPads Compartilhados > Servidor MDM do Grupo de Dispositivos 2
- Grupo N de iPads Compartilhados > Servidor MDM do Grupo de Dispositivos N

Adicionar contas ASM ou ABM para cada grupo de dispositivos

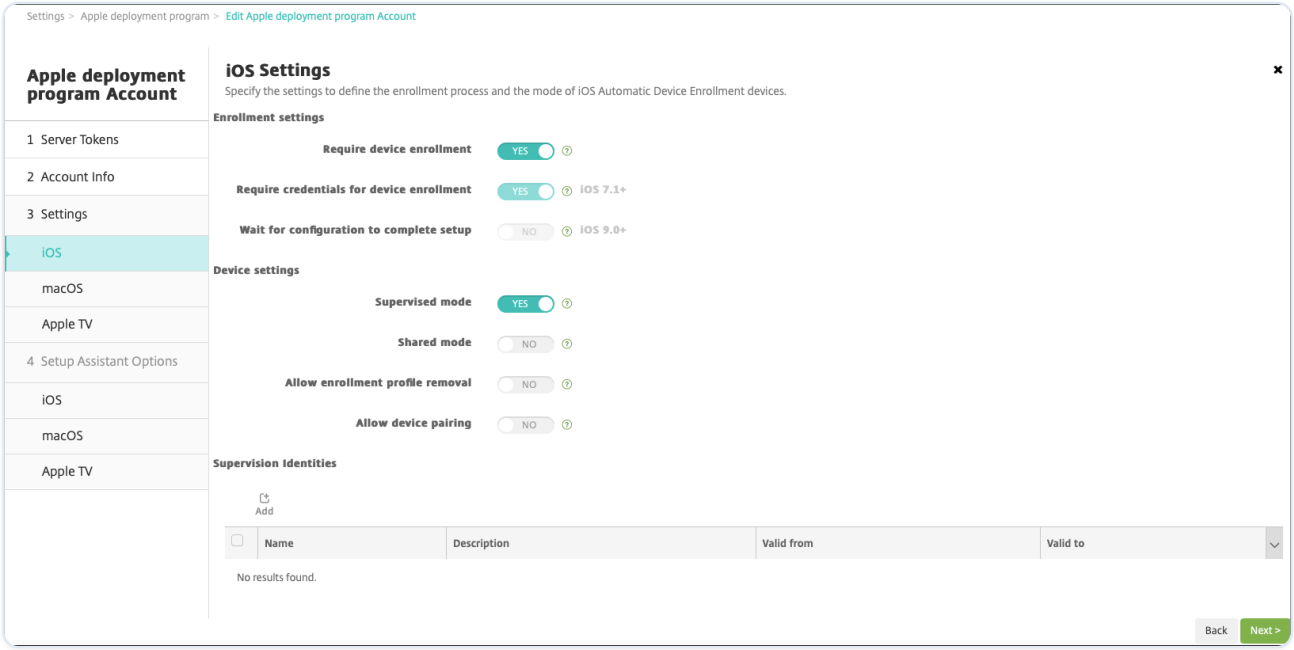
Ao criar múltiplas contas ASM ou ABM no console do XenMobile Server, você importa automaticamente grupos de iPads Compartilhados (um para cada turma ou instrutor):

- Servidor MDM do Grupo de Dispositivos 1 > conta do Grupo de Dispositivos 1
- Servidor MDM do Grupo de Dispositivos 2 > conta do Grupo de Dispositivos 2
- Servidor MDM do Grupo de Dispositivos N > conta do Grupo de Dispositivos N

Os requisitos específicos para iPads Compartilhados são os seguintes:

- Uma conta ASM ou ABM para cada grupo de dispositivos com estas configurações habilitadas:
  - **Exigir registro de dispositivo**
  - **Modo supervisionado**
  - **Modo compartilhado**
- Para uma determinada organização educacional, certifique-se de usar o mesmo **sufixo de Educação** para todas as contas ASM ou ABM.

Para adicionar uma conta, vá para **Configurações** > **Programa de Implantação da Apple**.



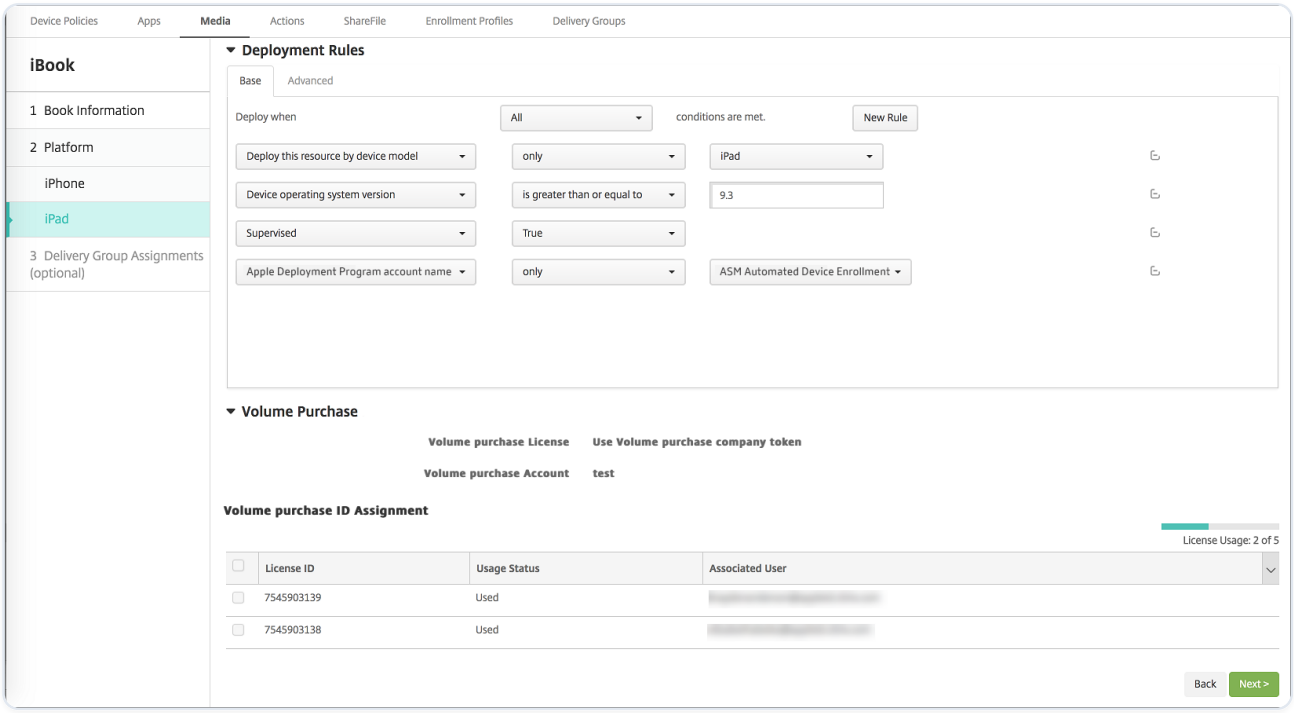
Apps para iPads Compartilhados

Os iPads Compartilhados suportam a atribuição de aplicativos de compra por volume baseados em dispositivo. Antes de implantar um aplicativo em um iPad Compartilhado, o XenMobile envia uma solicitação ao servidor de compra por volume da Apple para atribuir licenças de compra por

volume aos dispositivos. Para verificar as atribuições de compra por volume, vá para **Configurar** > **Aplicativos** > **iPad** e expanda **Compra por Volume**.

Mídia para iPads Compartilhados

Os iPads Compartilhados suportam a atribuição de iBooks de compra por volume baseados em usuário. Antes de implantar iBooks em um iPad Compartilhado, o XenMobile envia uma solicitação ao servidor de compra por volume da Apple para atribuir licenças de compra por volume aos alunos. Para verificar as atribuições de compra por volume, vá para **Configurar** > **Mídia** > **iPad** e expanda **Compra por Volume**.



Regras de implantação para iPads Compartilhados

Para a implantação de iPads Compartilhados, as regras no nível do grupo de entrega não se aplicam porque se relacionam a propriedades do usuário. Para filtrar as políticas, aplicativos e mídias para cada grupo de dispositivos: Adicione uma regra de implantação para os recursos com base no nome da conta. Por exemplo:

- Para a conta do Grupo de Dispositivos 1, defina esta regra de implantação:

```
Apple Deployment Program account name

Only
```

```
Device Group 1 account
```

- Para a conta do Grupo de Dispositivos 2, defina esta regra de implantação:

```
Apple Deployment Program account name

Only

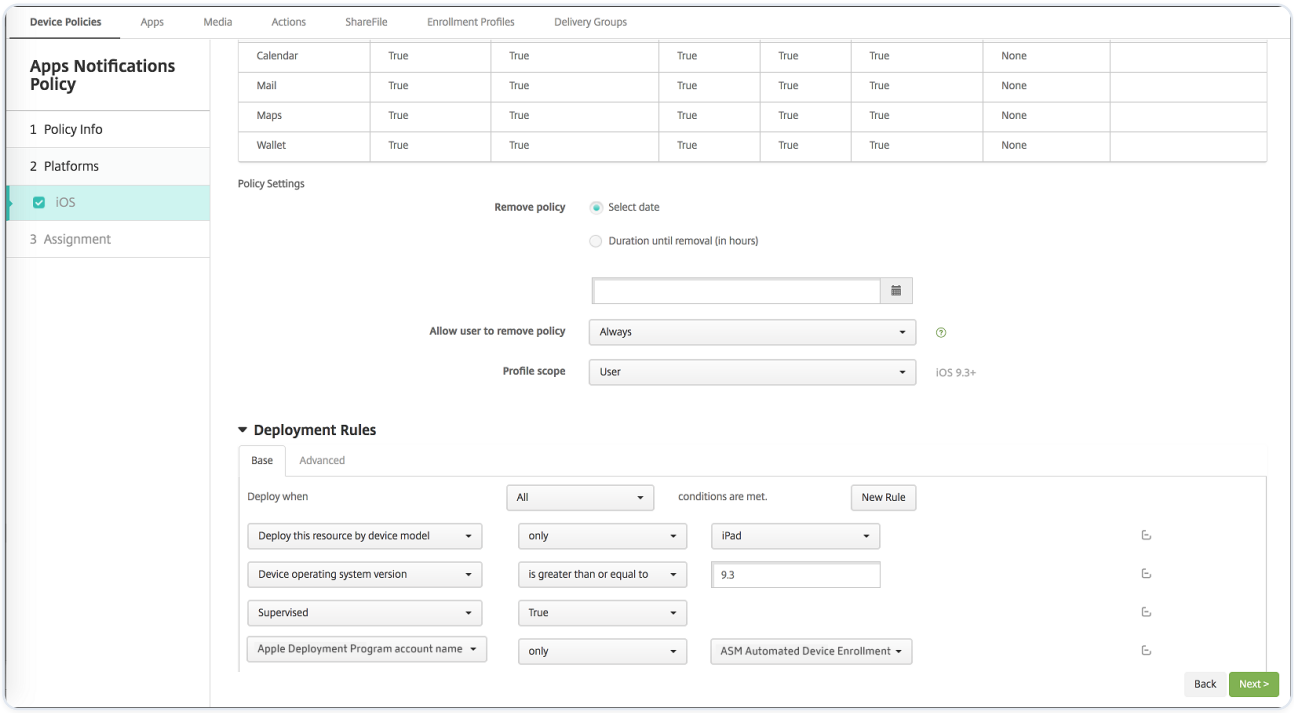
Device Group 2 account
```

- Para a conta do Grupo de Dispositivos N, defina esta regra de implantação:

```
Apple Deployment Program account name

Only

Device Group N account
```



Para implantar o aplicativo Apple Classroom apenas para instrutores (usando iPads não compartilhados), filtre os recursos por status compartilhado ASM ou ABM com estas regras de implantação:

```
Deploy this resource regarding ASM or ABM shared mode

only

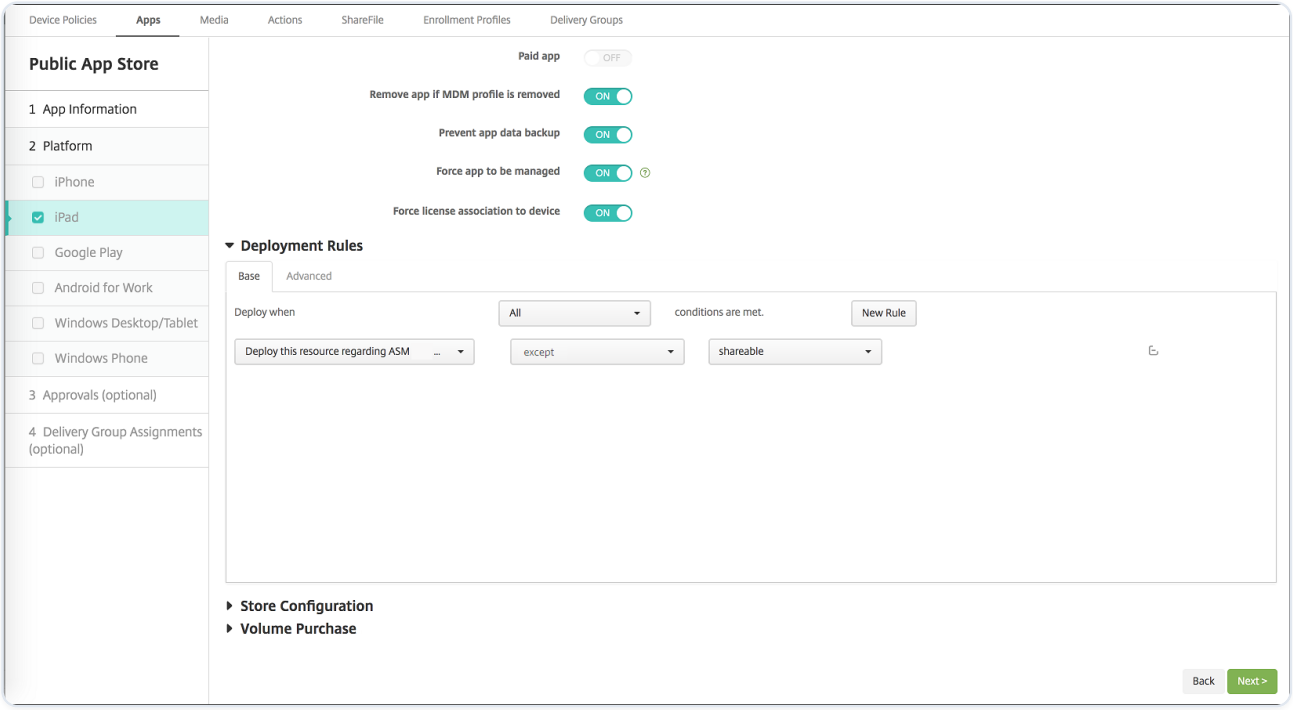
unshared
```

Ou:

```
Deploy this resource regarding ASM or ABM shared mode

except

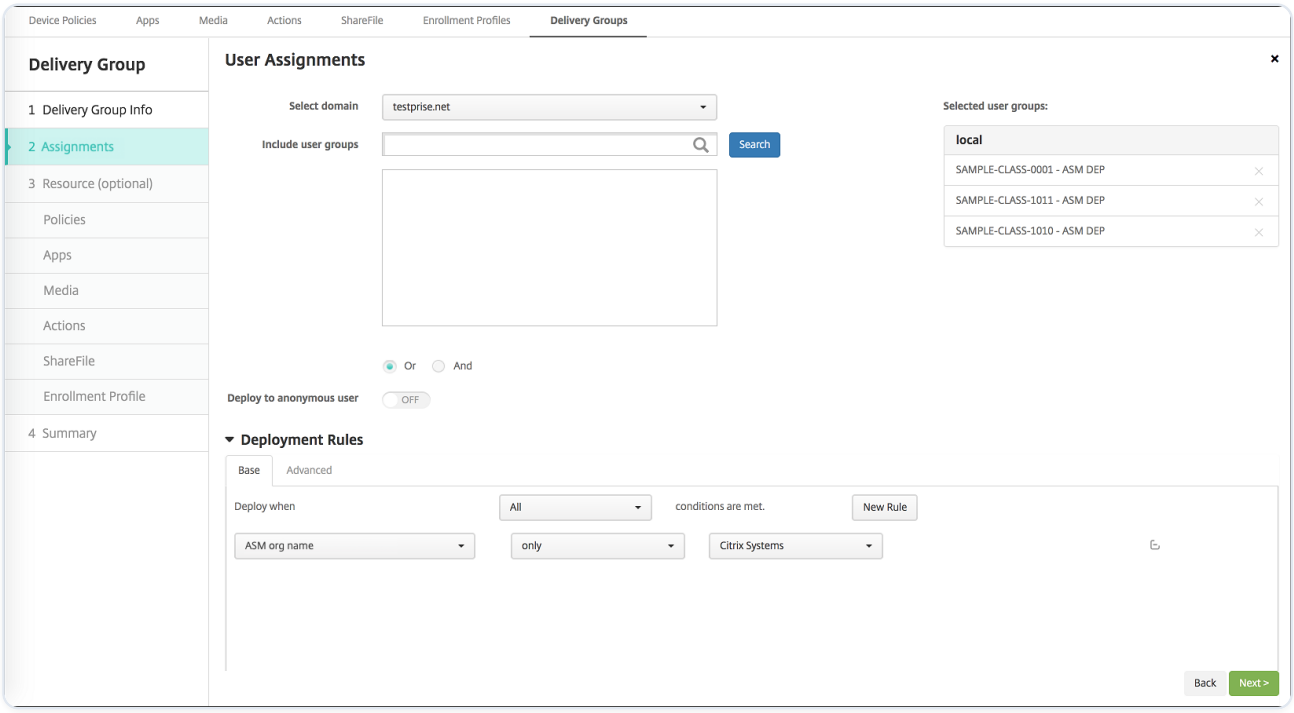
shareable
```



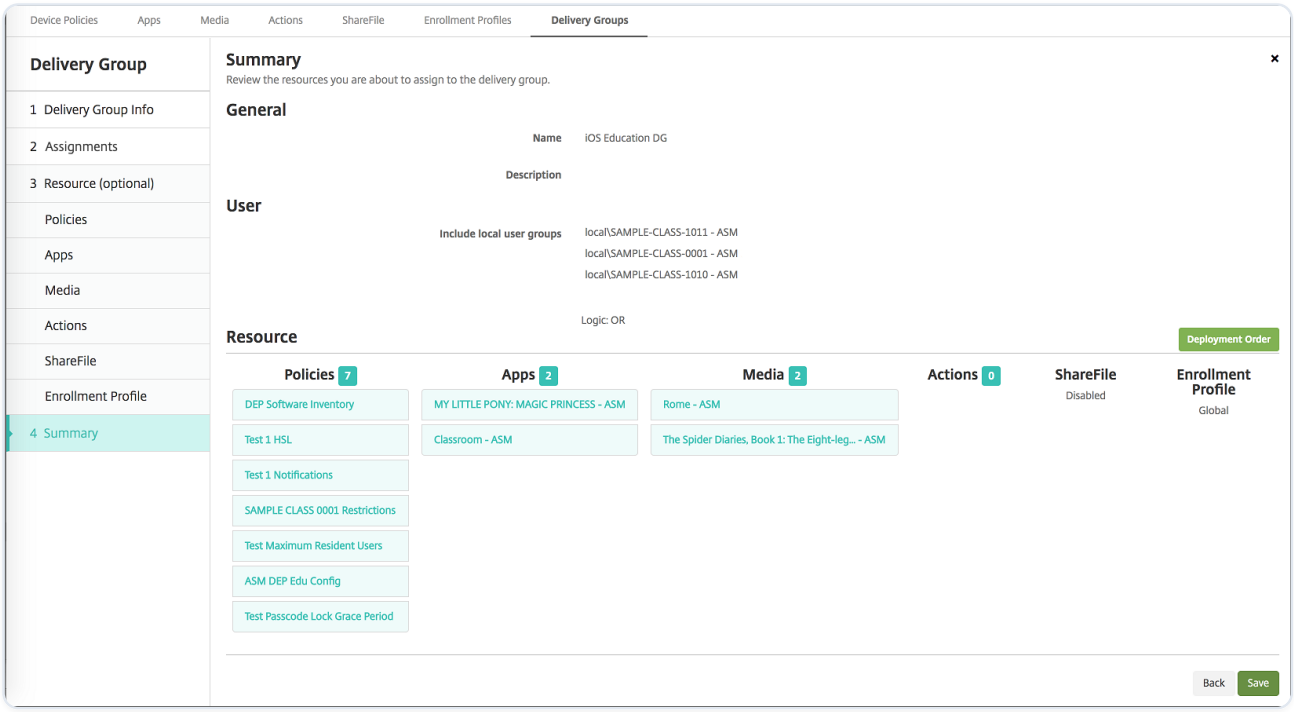
Grupos de entrega para iPads Compartilhados

Para o grupo de dispositivos de cada instrutor:

- Configure um grupo de entrega. Para o instrutor, atribua todas as turmas que a política de Configuração de Educação define.



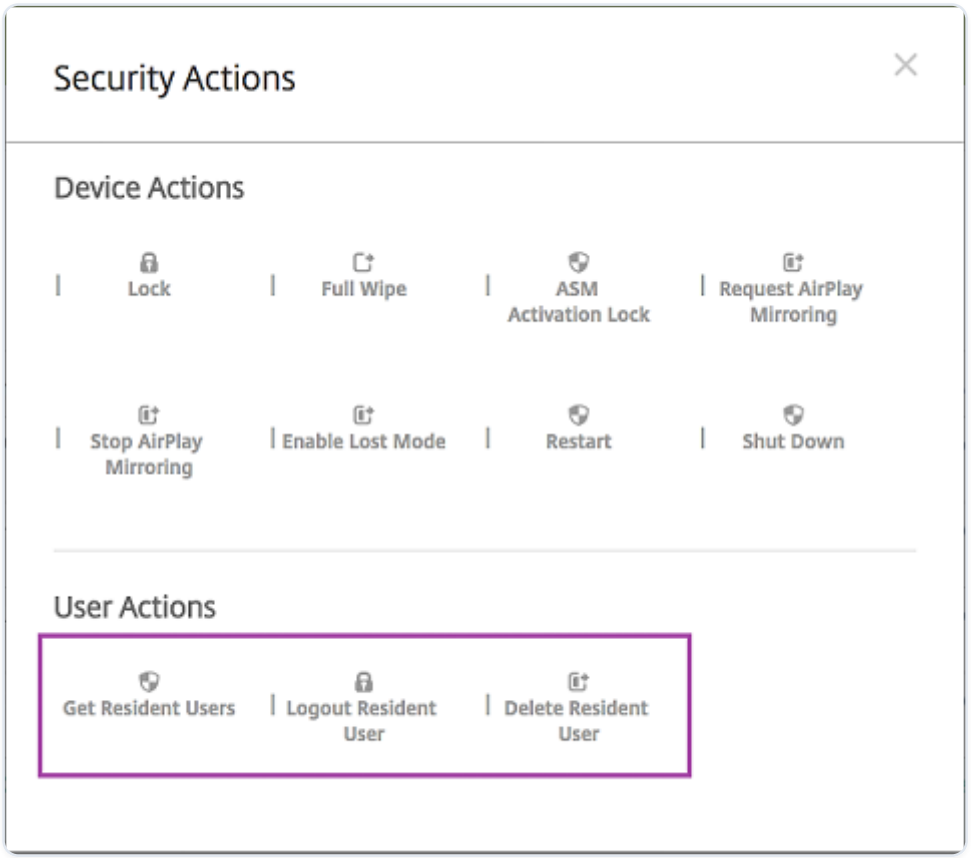
- Esse grupo de entrega deve incluir estes recursos MDM:
  - Políticas de dispositivo:
    - Configuração de Educação
    - Notificações de Aplicativos
    - Layout da Tela Inicial
    - Restrições
    - Número Máximo de Usuários Residentes
    - Período de Carência do Bloqueio por Senha
  - Aplicativos de compra por volume obrigatórios
  - iBooks de compra por volume obrigatórios



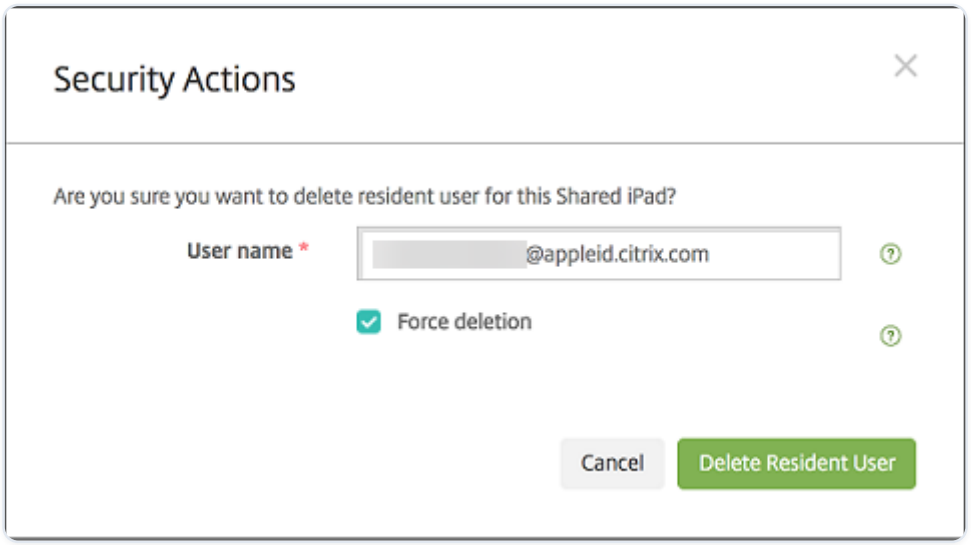
Ações de segurança para iPads Compartilhados

Além das ações de segurança existentes, você pode usar estas ações de segurança para iPads Compartilhados:

- **Obter Usuários Residentes:** Lista os usuários que têm contas ativas no dispositivo atual. Esta ação força uma sincronização entre o dispositivo e o console XenMobile.
- **Fazer Logout do Usuário Residente:** Força o logout do usuário atual.
- **Excluir Usuário Residente:** Exclui a sessão atual para um usuário específico. O usuário pode fazer login novamente.
- **Excluir Todos os Usuários:** Exclui todos os usuários do dispositivo.



Depois de clicar em **Excluir Usuário Residente**, você pode especificar o nome de usuário.



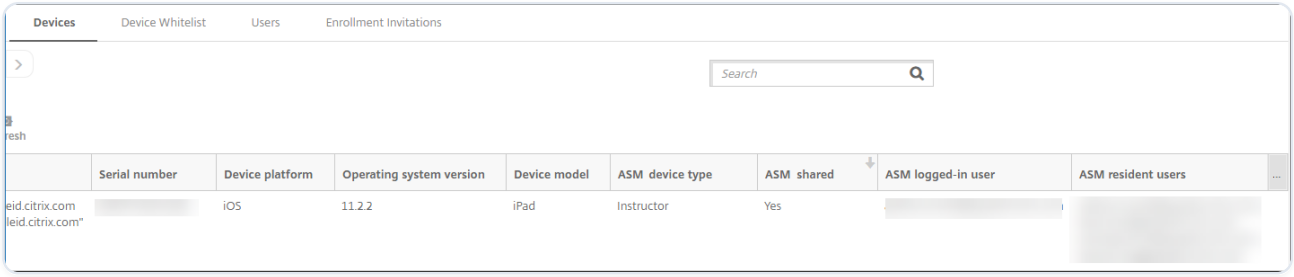
Os resultados das ações de segurança aparecem nas páginas **Gerenciar** > **Dispositivos** > **Geral** e **Gerenciar** > **Dispositivos** > **Grupos de Entrega**.

Obter informações sobre iPads Compartilhados

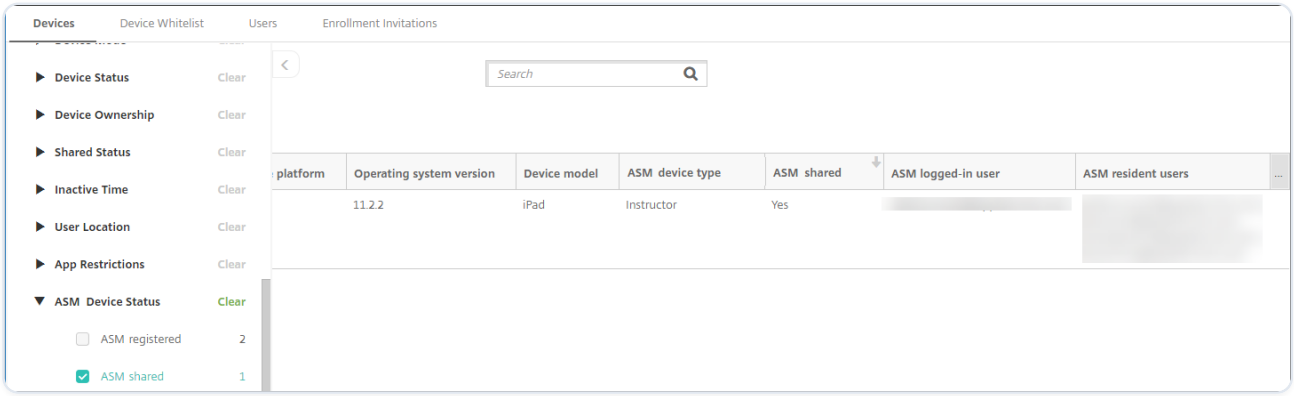
Encontre informações específicas sobre iPads Compartilhados na página **Gerenciar** > **Dispositivos**:

- Pesquisar:

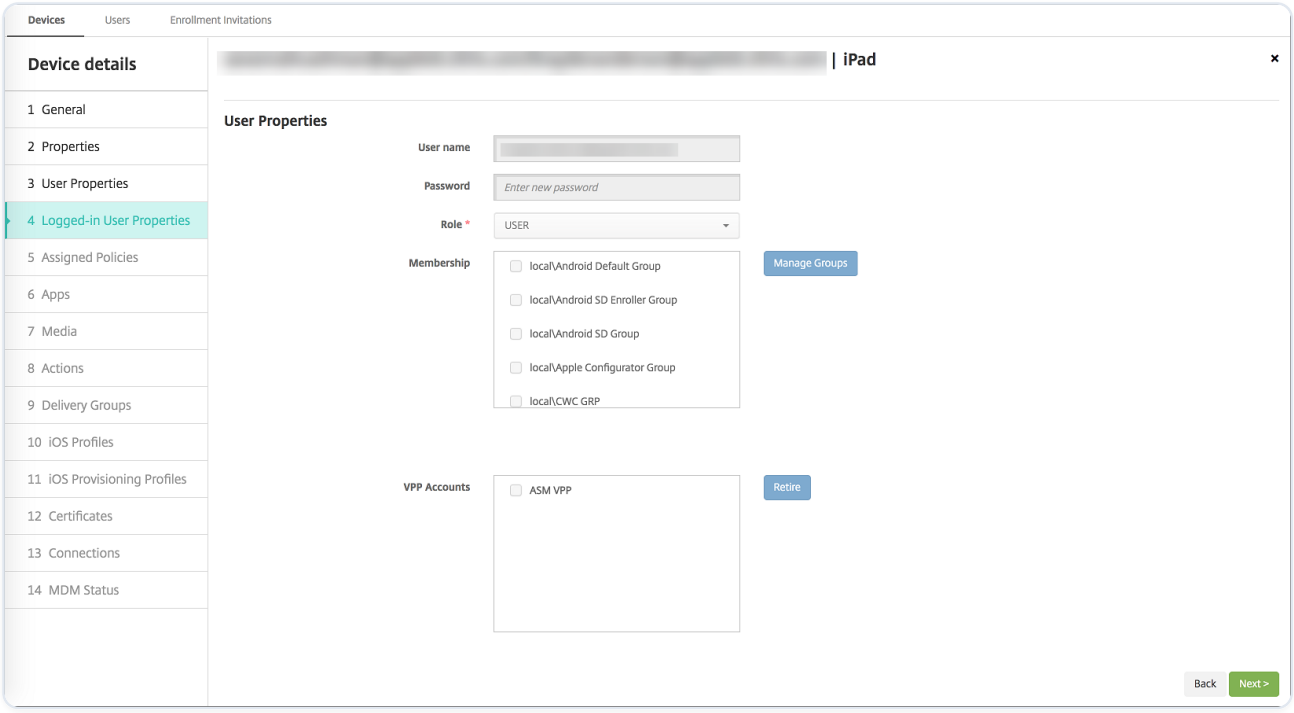
- Se um dispositivo é compartilhado (**compartilhado por ASM ou ABM**)
- Quem está logado no dispositivo compartilhado (**usuário logado por ASM ou ABM**)
- Todos os usuários atribuídos ao dispositivo compartilhado (**usuários residentes por ASM ou ABM**)

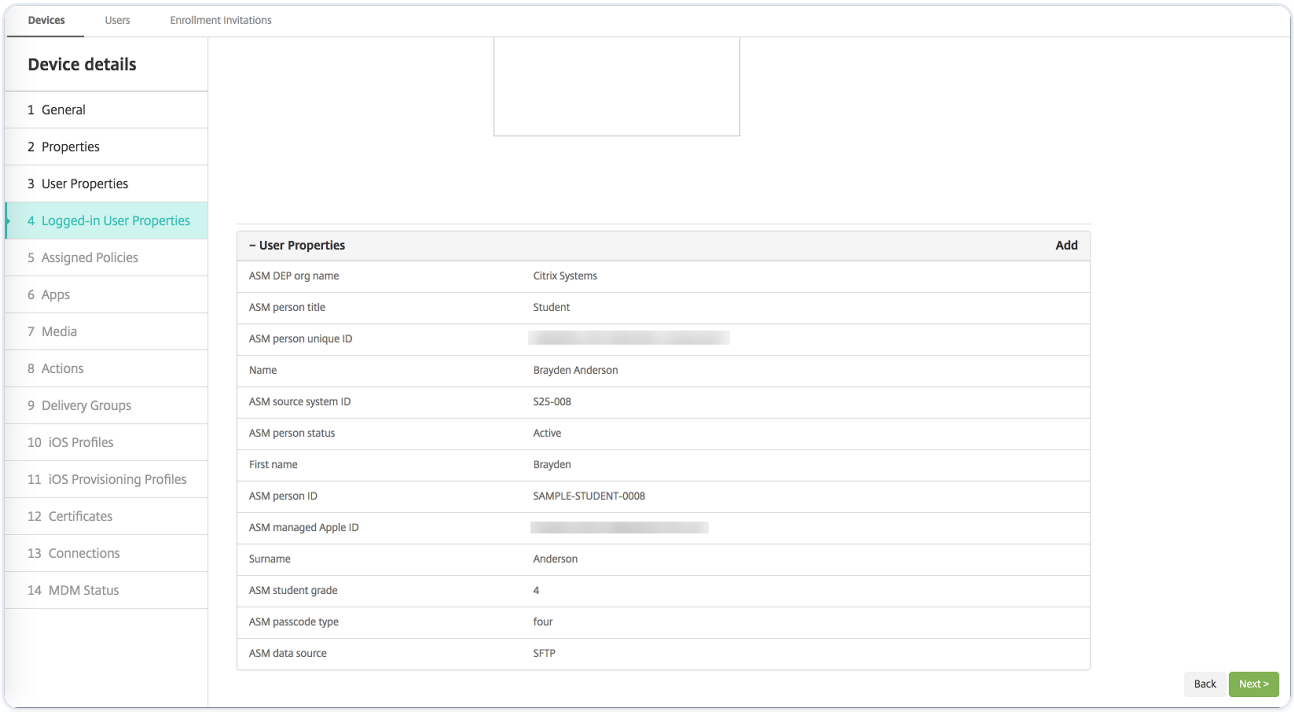


- Filtre a lista de dispositivos por seu **Status do Dispositivo ASM ou ABM:**

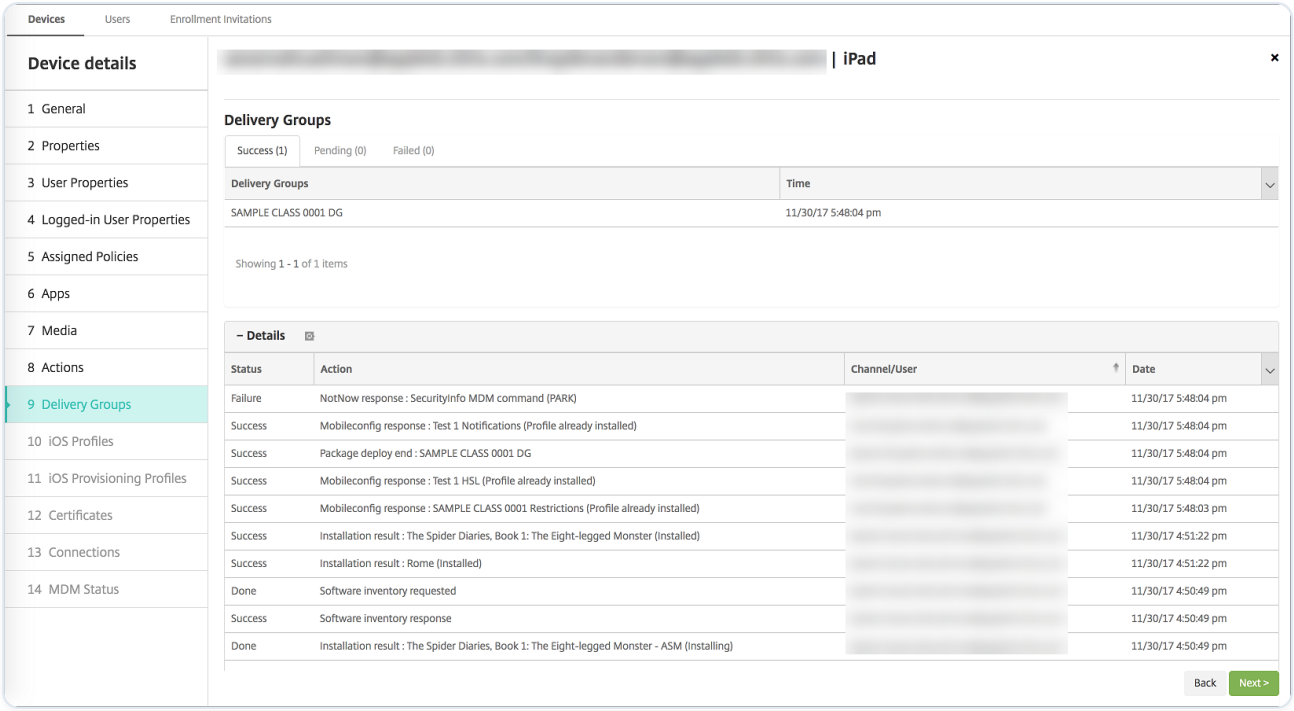


- Visualize detalhes sobre o usuário conectado a um iPad Compartilhado, na página **Gerenciar** > **Dispositivos** > **Propriedades do Usuário Conectado**.



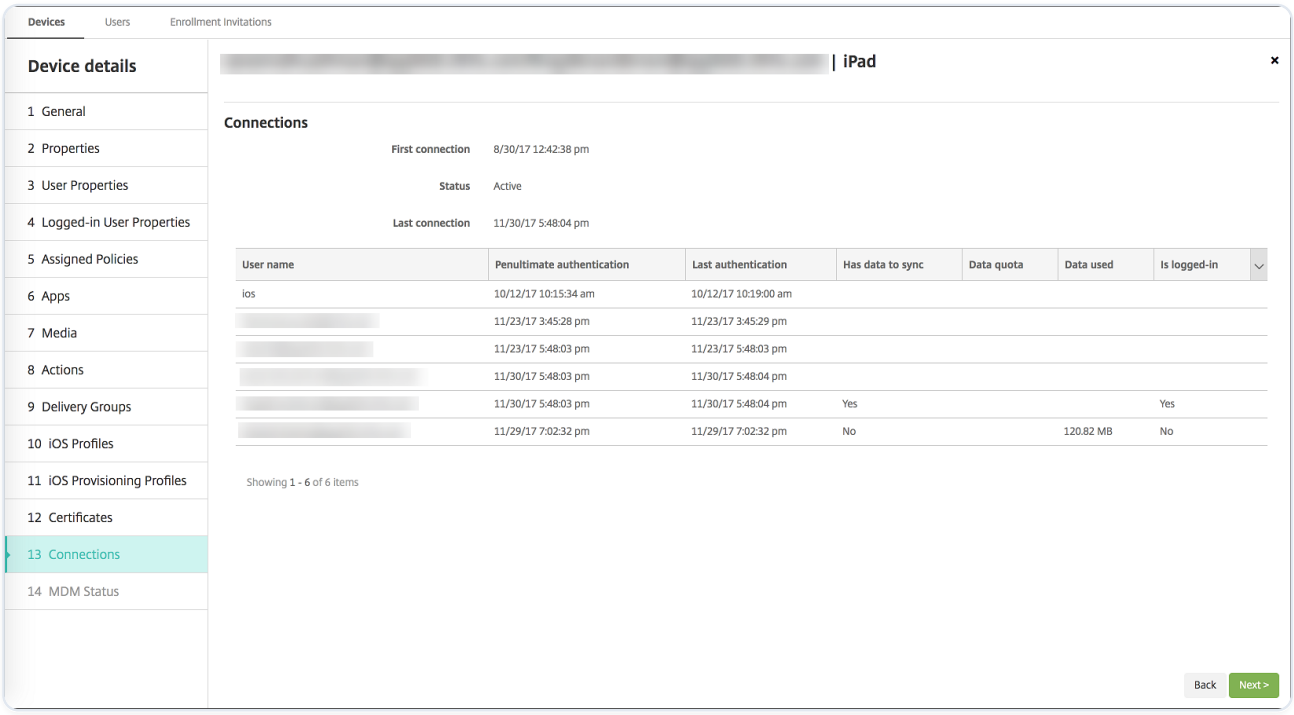


- Veja o canal usado para implantar recursos para instrutores e usuários em um grupo de entrega na página **Gerenciar** > **Dispositivos** > **Grupos de Entrega**. A coluna **Canal/Usuário** mostra o tipo (**Sistema** ou **Usuário**) e o destinatário (instrutor ou aluno).

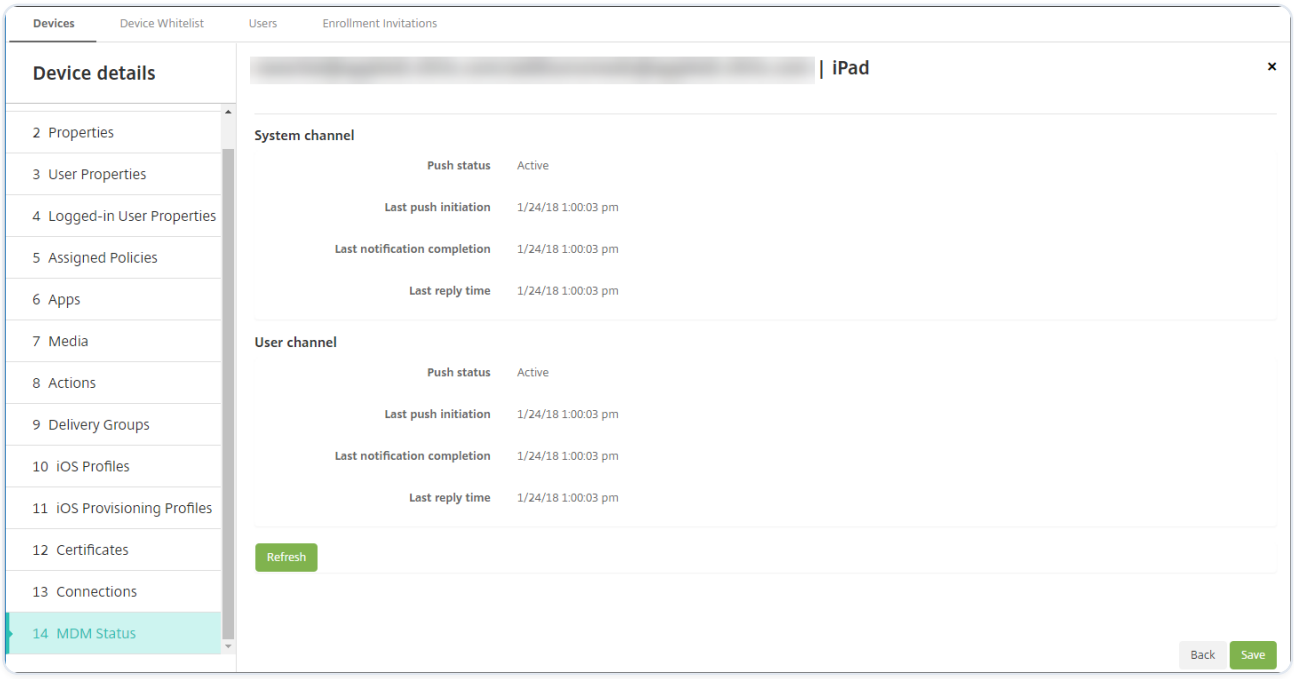


- Obtenha informações sobre usuários residentes:
  - **Tem dados para sincronizar:** Se o usuário tem dados a serem sincronizados com a nuvem.

- **Cotas de dados:** A cota de dados definida para o usuário em bytes. Uma cota pode não aparecer se as cotas de usuário estiverem temporariamente desativadas ou não forem aplicadas para o usuário.
- **Dados usados:** A quantidade de dados usada pelo usuário em bytes. Um valor pode não aparecer se ocorrer um erro enquanto o sistema coleta as informações.
- **Está conectado:** Se o usuário está conectado ao dispositivo.



- Visualize o status de push para ambos os canais.



Distribuir aplicativos Apple

O XenMobile gerencia aplicativos implantados em dispositivos. Você pode organizar e implantar os seguintes tipos de aplicativos iOS/iPadOS e macOS.

- **App Store Pública (somente iOS/iPadOS):** Esses aplicativos incluem aplicativos gratuitos ou pagos disponíveis em uma loja de aplicativos pública, como a Apple App Store ou o Google Play. Por exemplo, GoToMeeting.
- **Empresarial (iOS/iPadOS/macOS):** Aplicativos nativos que não são habilitados para MDX e não possuem as políticas associadas aos aplicativos MDX.
- **MDX (somente iOS/iPadOS):** Aplicativos preparados com o SDK MAM ou empacotados com o MDX Toolkit. Esses aplicativos incluem políticas MDX. Você obtém aplicativos MDX de fontes internas e lojas públicas.
- **Compra por volume (iOS/iPadOS/macOS):** Aplicativos com licenças gerenciadas por meio do programa de compra por volume da Apple.
- **Aplicativos personalizados do iOS (somente iOS/iPadOS):** Aplicativos proprietários business-to-business desenvolvidos internamente ou por terceiros.

Para obter mais informações sobre os diferentes tipos de aplicativos, consulte Adicionar aplicativos.

Algumas implantações exigem uma conta do Apple Business Management (ABM) ou Apple School Management (ASM). Consulte as seções a seguir para obter mais informações.

Para cada tipo de aplicativo e método de distribuição, a Citrix recomenda um conjunto de práticas de configuração. Para obter informações sobre a distribuição de aplicativos para outras plataformas, consulte Adicionar aplicativos. As seções a seguir fornecem informações mais detalhadas para a configuração de aplicativos iOS.

Etapas gerais para a distribuição de aplicativos

CENÁRIO	ETAPA 1: VINCULAR CONTAS	ETAPA 2: ADICIONAR E CONFIGURAR APLICATIVOS	ETAPA 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLANTAR APLICATIVOS
Aplicativos da loja de aplicativos pública(#public-app-	Não aplicável	**Em XenMobile®: Configurar > Aplicativos**,	**Em XenMobile:** Configure e implante

CENÁRIO	ETAPA 1: VINCULAR CONTAS	ETAPA 2: ADICIONAR E CONFIGURAR APLICATIVOS	ETAPA 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLANTAR APLICATIVOS
store-apps), incluindo aplicativos de mobilidade Citrix®		adicione aplicativos da **Loja de Aplicativos Pública** para iPhone ou iPad. Configure os aplicativos e atribua-os a grupos de entrega.	aplicativos usando grupos de entrega.
Aplicativos da loja de aplicativos pública entregues com compra por volume da Apple(#public-app-store-apps-delivered-with-apple-volume-purchase), incluindo aplicativos de mobilidade Citrix	Inscreva-se em um programa de implantação da Apple. **Em XenMobile:** Vá para **Configurações > Compra por volume** para adicionar sua conta de compra por volume.	**No ABM ou ASM:** Compre e adicione aplicativos de Aplicativos e Livros. **Em XenMobile:** Vá para **Configurar > Aplicativos**, configure os aplicativos e atribua-os a grupos de entrega.	**Em XenMobile:** Configure e implante aplicativos usando grupos de entrega.
Aplicativos empresariais(#enterprise-apps)	Não aplicável	**Em XenMobile:** Vá para **Configurar > Aplicativos**. Clique em **Adicionar** e depois em **Empresarial**. Carregue o arquivo IPA. Configure os aplicativos e atribua-os a grupos de entrega.	**Em XenMobile:** Configure e implante aplicativos usando grupos de entrega.
Aplicativos MDX(#mdx-apps)	Não aplicável	**Em XenMobile:** Vá para **Configurar > Aplicativos**. Clique em **Adicionar** e	**No XenMobile:** Configure e implante

CENÁRIO	ETAPA 1: VINCULAR CONTAS	ETAPA 2: ADICIONAR E CONFIGURAR APLICATIVOS	ETAPA 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLANTAR APLICATIVOS
		depois em **MDX**. Certifique-se de selecionar **iPad/ iPhone** para a plataforma. Carregue o arquivo MDX. Configure os aplicativos e atribua-os a grupos de entrega.	aplicativos usando grupos de entrega.
Aplicativos MDX distribuídos usando compra por volume da Apple	Inscreva-se em um programa de implantação da Apple. **No XenMobile:** Vá para **Configurações > Compra por volume** para adicionar sua conta de compra por volume.	**No ABM:** Compre e adicione aplicativos MDX de Aplicativos e Livros. Vincule o aplicativo à sua conta ABM. **No XenMobile:** Vá para **Configurar > Aplicativos**, configure os aplicativos e atribua-os a grupos de entrega.	**No XenMobile:** Configure e implante aplicativos usando grupos de entrega.
Aplicativos personalizados	Inscreva-se em um programa de implantação da Apple. **No XenMobile:** Vá para **Configurações > Compra por volume** para adicionar sua conta de compra por volume.	**No ABM:** Adicione seu aplicativo à App Store como um aplicativo privado. Vincule o aplicativo à sua conta ABM. **No XenMobile:** Vá para **Configurar > Aplicativos**, configure os aplicativos e atribua-	**No XenMobile:** Configure e implante aplicativos usando grupos de entrega.

CENÁRIO	ETAPA 1: VINCULAR CONTAS	ETAPA 2: ADICIONAR E CONFIGURAR APLICATIVOS	ETAPA 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLANTAR APLICATIVOS
		os a grupos de entrega.	
Aplicativos personalizados habilitados para MDX	Inscreva-se em um programa de implantação da Apple. **No XenMobile:** Vá para **Configurações > Compra por volume** para adicionar sua conta de compra por volume.	**No ABM:** Adicione seu aplicativo à App Store como um aplicativo privado. Vincule o aplicativo à sua conta ABM. **No XenMobile:** Vá para **Configurar > Aplicativos** e carregue o arquivo MDX. Configure os aplicativos e atribua-os a grupos de entrega.	**No XenMobile:** Configure e implante aplicativos usando grupos de entrega.

Aplicativos da loja de aplicativos públicos

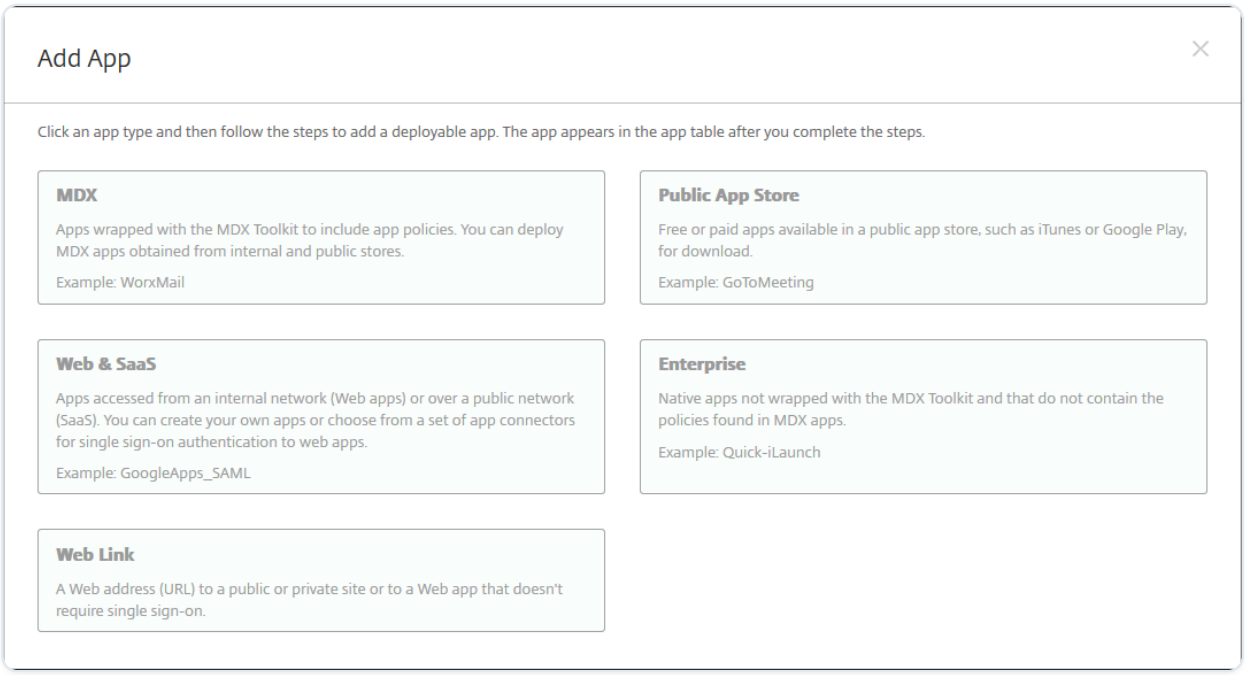
Você pode adicionar aplicativos gratuitos e pagos disponíveis na App Store ao XenMobile.

DISPONIBILIDADE DO RECURSO	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Não
Disponível em	iOS/iPadOS

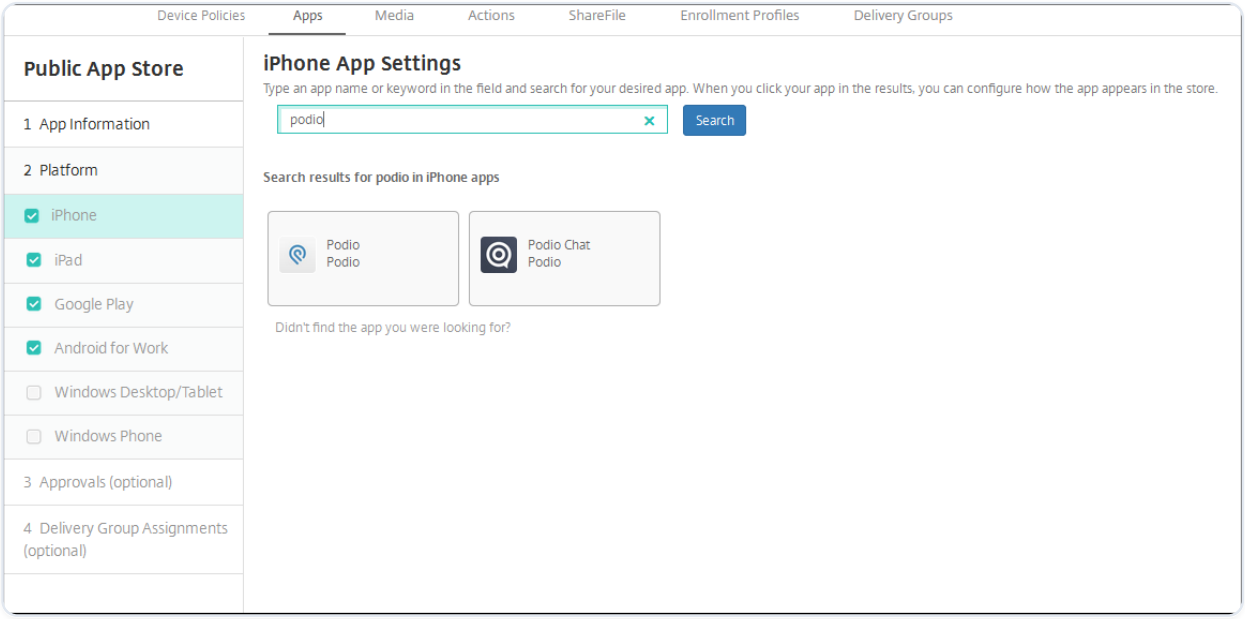
Etapa 1: Adicionar e configurar aplicativos

1. No console do XenMobile, navegar para **Configurar > Aplicativos**. Clique em **Adicionar**.

2. Clique em **Loja de Aplicativos Pública**.



3. Selecione **iPhone** ou **iPad** para as plataformas
4. Digite o nome do aplicativo na caixa de pesquisa e clique em **Pesquisar**.

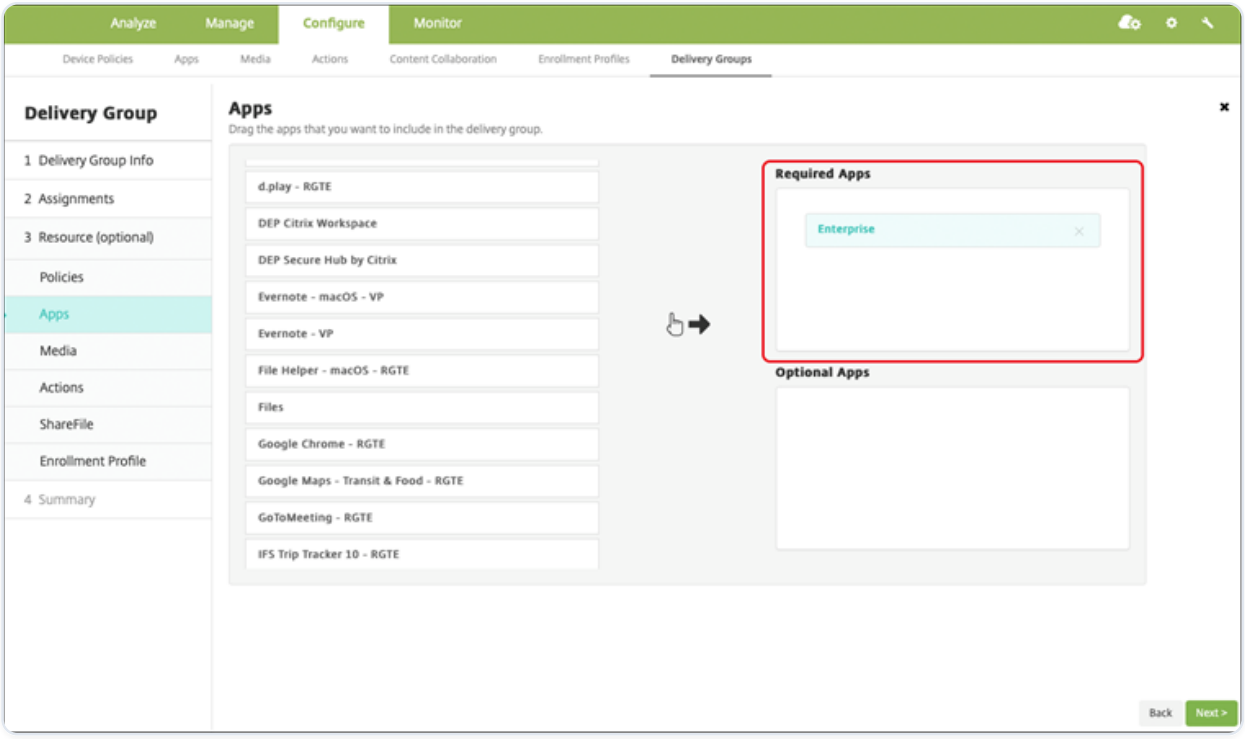


5. Os aplicativos que correspondem aos critérios de pesquisa aparecem. Clique no aplicativo desejado.
6. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configurar > Aplicativos**.
2. Selecione o aplicativo que deseja configurar e clique em **Editar**.
3. A Citrix recomenda habilitar o recurso **Forçar o gerenciamento do aplicativo**.

4. Atribua quaisquer grupos de entrega e clique em **Salvar**.
5. navegar para **Configurar > Grupos de Entrega > Aplicativos**.
6. Marque os aplicativos desejados como **Obrigatório**.



7. navegar de volta para **Configurar > Grupos de Entrega**.
8. Selecione o grupo de entrega e clique em **Implantar**.

9. Os usuários recebem uma solicitação para instalar o aplicativo, e o aplicativo é instalado em segundo plano após a aceitação.



Aplicativos da loja pública entregues com compra por volume da Apple

Você pode gerenciar licenças de aplicativos iOS/iPadOS por meio do programa de compra por volume da Apple. Siga estas etapas para adicionar aplicativos de compra por volume ao XenMobile.

DISPONIBILIDADE DE RECURSOS	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS/macOS

Etapa 1: Vincular contas

1. Configure e inscreva-se no Apple Business Manager (ABM) ou Apple School Manager (ASM). Para obter mais informações sobre esses programas, consulte a documentação da Apple.
2. Vincule sua conta ABM/ASM ao XenMobile. Para obter mais informações sobre como vincular contas de compra por volume, consulte Compra por Volume da Apple.

3. Ao adicionar sua conta de compra por volume, ative **Atualização Automática de Aplicativos**. Essa configuração garante que os aplicativos nos dispositivos dos usuários sejam atualizados automaticamente quando uma atualização aparecer na loja da Apple.

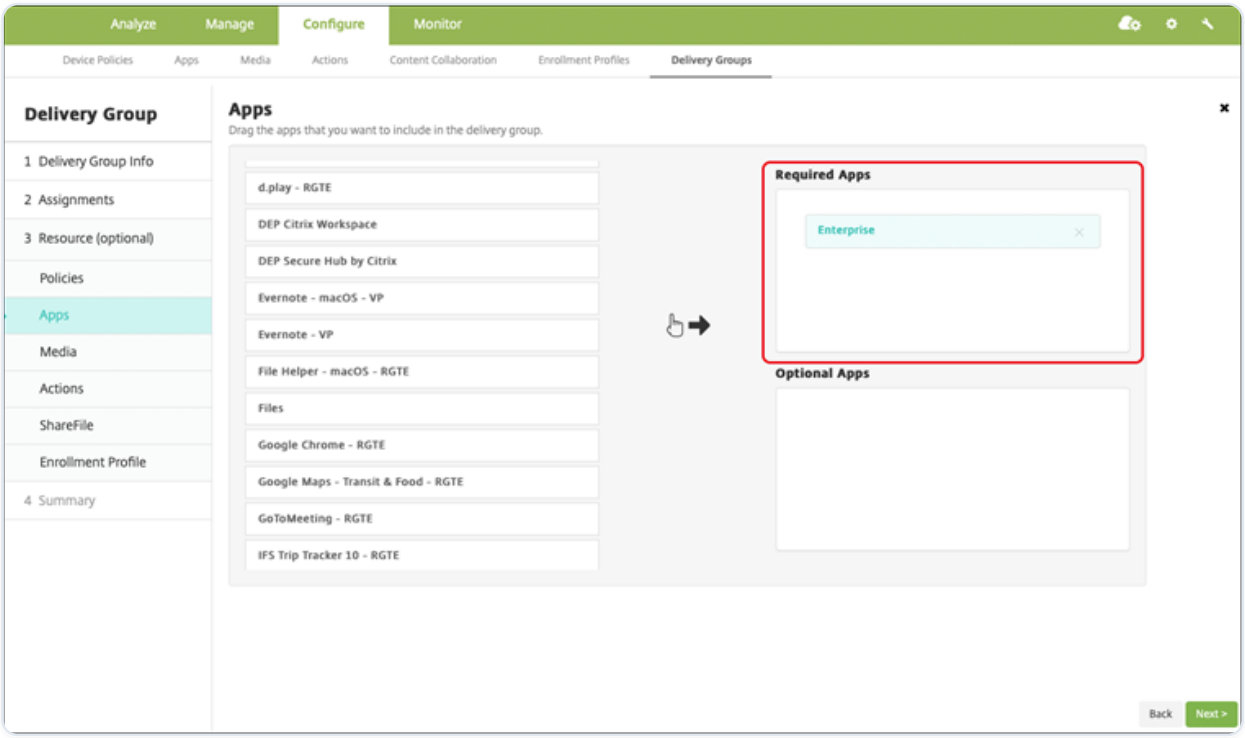
Etapa 2: Obtenha aplicativos e licenças da Apple

Adicione aplicativos à sua conta ABM/ASM. Você pode adicionar compras da Apple App Store ou Apple Books (somente para iOS/iPadOS). Lembre-se de que você deve comprar todos os aplicativos, mesmo que sejam gratuitos.

Para obter informações sobre como disponibilizar aplicativos para sua empresa, consulte a documentação da Apple.

Etapa 3: Configurar implantação de aplicativo

1. No console do XenMobile, navegar para **Configurar > Aplicativos**.
2. Selecione o aplicativo de compra por volume que você deseja configurar e clique em **Editar**.
3. Selecione as plataformas: **iPhone**, **iPad** ou **macOS**.
4. A Citrix recomenda habilitar o recurso **Forçar gerenciamento do aplicativo** (somente iOS/iPadOS).
5. Atribua quaisquer grupos de entrega e clique em **Salvar**.
6. navegar até **Configurar > Grupos de Entrega > Aplicativos**.
7. Marque os aplicativos desejados como **Obrigatório**.



8. navegar de volta para **Configurar > Grupos de Entrega**.

9. Selecione o grupo de entrega e clique em **Implantar**.
10. Os usuários recebem uma solicitação para instalar o aplicativo, e o aplicativo é instalado em segundo plano após a aceitação.



Aplicativos empresariais

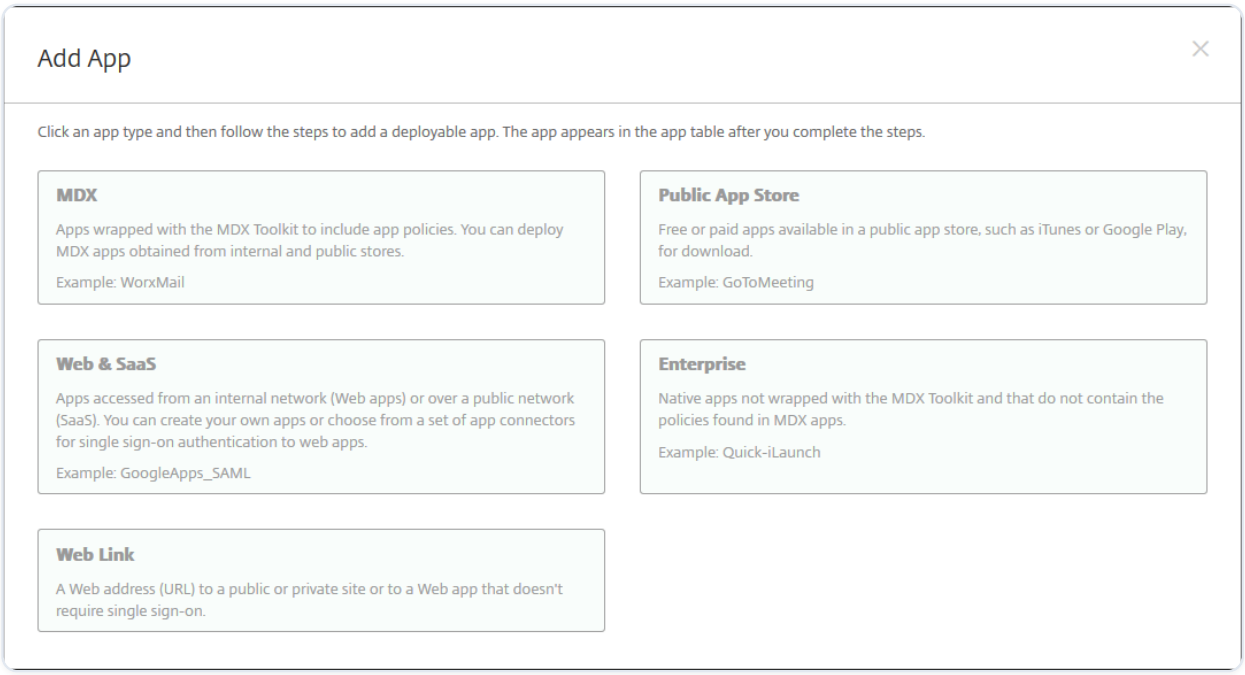
Você também pode adicionar aplicativos nativos que não possuem políticas MDX associadas a eles. Siga estas etapas para adicionar aplicativos que não existem na App Store.

DISPONIBILIDADE DO RECURSO	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
SO	iOS/iPadOS/macOS

Etapa 1: Adicionar e configurar aplicativos

1. No console do XenMobile, navegar até **Configurar > Aplicativos**. Clique em **Adicionar**.

2. Clique em **Empresarial**.



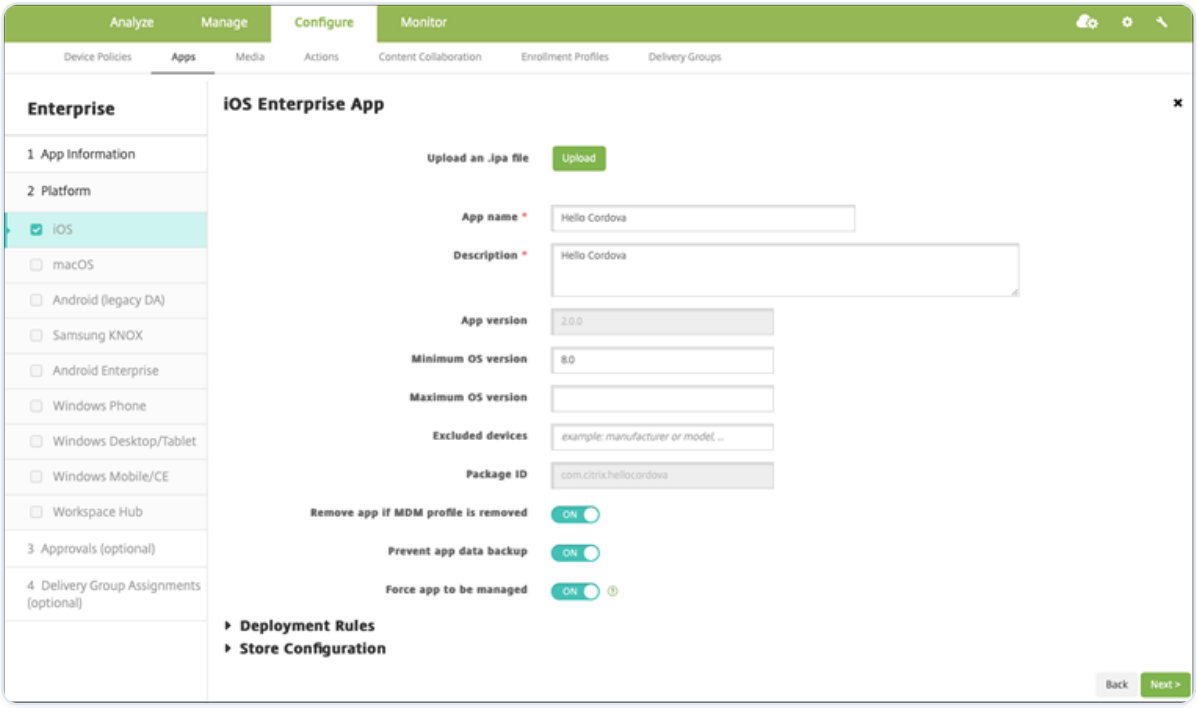
3. Na página **Informações do aplicativo**, configure o seguinte:

   - **Nome:** Digite um nome descritivo para o aplicativo. O nome aparece em Nome do aplicativo na tabela Aplicativos.
   - **Descrição:** Digite uma descrição opcional do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo.

4. Clique em **Avançar**. A página **Plataformas de aplicativo** é exibida.
5. Selecione as plataformas: **iPhone**, **iPad** ou **macOS**.
6. Carregue o arquivo IPA (iOS/iPadOS) ou carregue o arquivo PKG (macOS)
7. Clique em **Avançar**. A página **Detalhes do aplicativo** é exibida.
8. Configure estas configurações:

   - **Nome do arquivo:** Opcionalmente, digite um novo nome para o aplicativo.
   - **Descrição do aplicativo:** Opcionalmente, digite uma nova descrição para o aplicativo.
   - **Versão do aplicativo:** Você não pode alterar este campo.
   - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
   - **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.

- **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
- **Remover aplicativo se o perfil MDM for removido:** Selecione se deseja remover o aplicativo de um dispositivo quando o perfil MDM for removido. O padrão é ATIVADO. (Somente iOS/iPadOS)
- **Impedir backup de dados do aplicativo:** Selecione se deseja impedir que o aplicativo faça backup de dados. O padrão é ATIVADO. (Somente iOS/iPadOS)
- **Forçar gerenciamento do aplicativo:** Se você instalar um aplicativo não gerenciado, selecione **ATIVADO** se quiser que os usuários em dispositivos não supervisionados vejam um prompt para permitir o gerenciamento do aplicativo. Se eles aceitarem o prompt, o aplicativo será gerenciado. (Somente iOS/iPadOS)

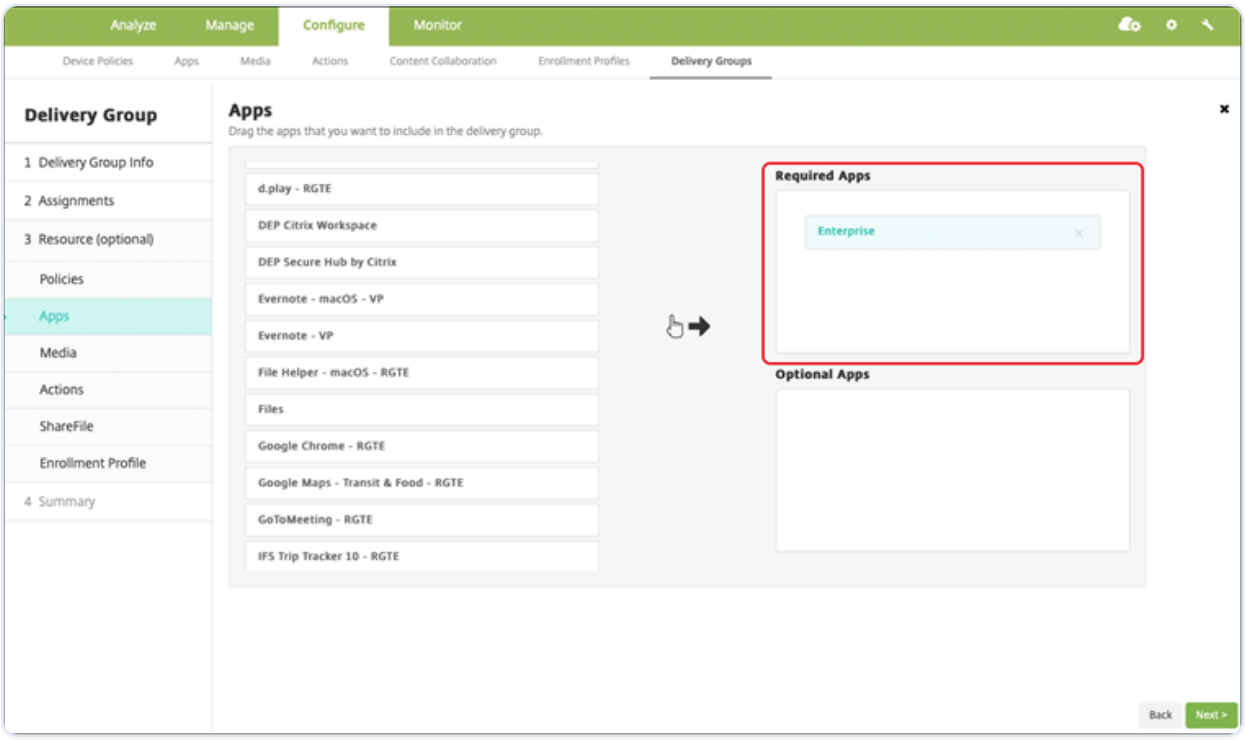


9. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configurar > Grupos de Entrega**. Selecione o grupo de entrega a ser configurado e clique na página **Aplicativos**.

2. Marque os aplicativos desejados como **Obrigatórios**.



3. navegar para **Configurar > Grupos de Entrega**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo, e o aplicativo é instalado em segundo plano depois que eles aceitam.



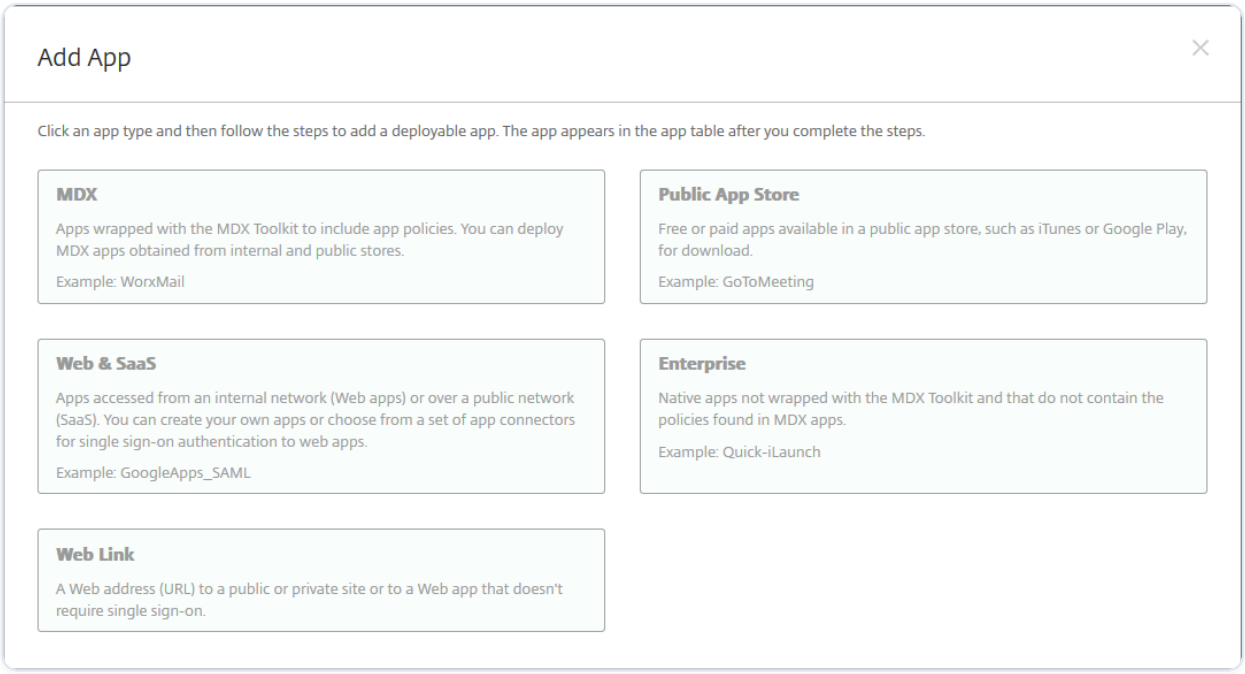
Aplicativos MDX

Para usar as políticas MDX e os recursos de segurança, adicione aplicativos que tenham o MAM SDK ativado ou que sejam empacotados em MDX. Você pode implantar aplicativos MDX usando compra por volume ou sem ela.

DISPONIBILIDADE DO RECURSO	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

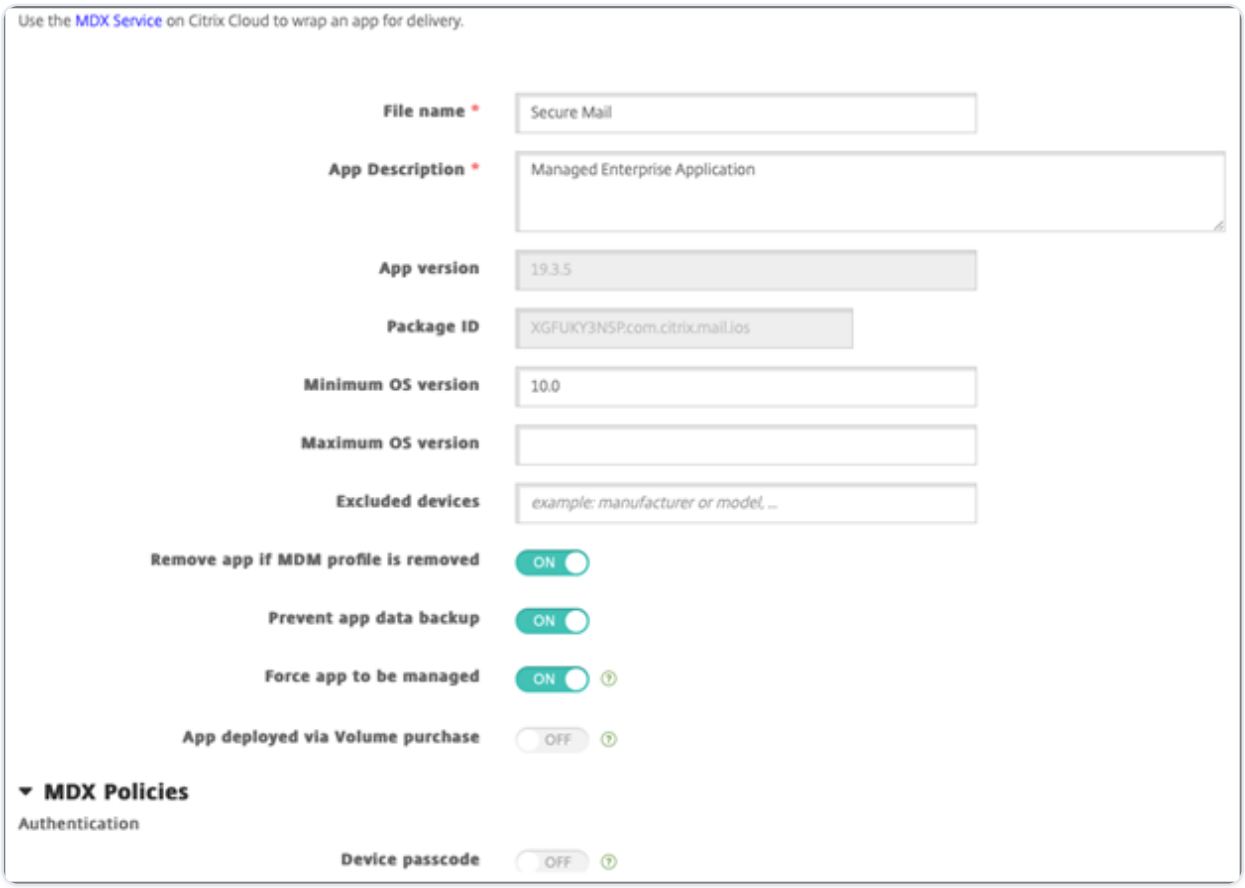
Etapa 1: Adicionar e configurar aplicativos

1. No console do XenMobile, navegar para **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **MDX**.

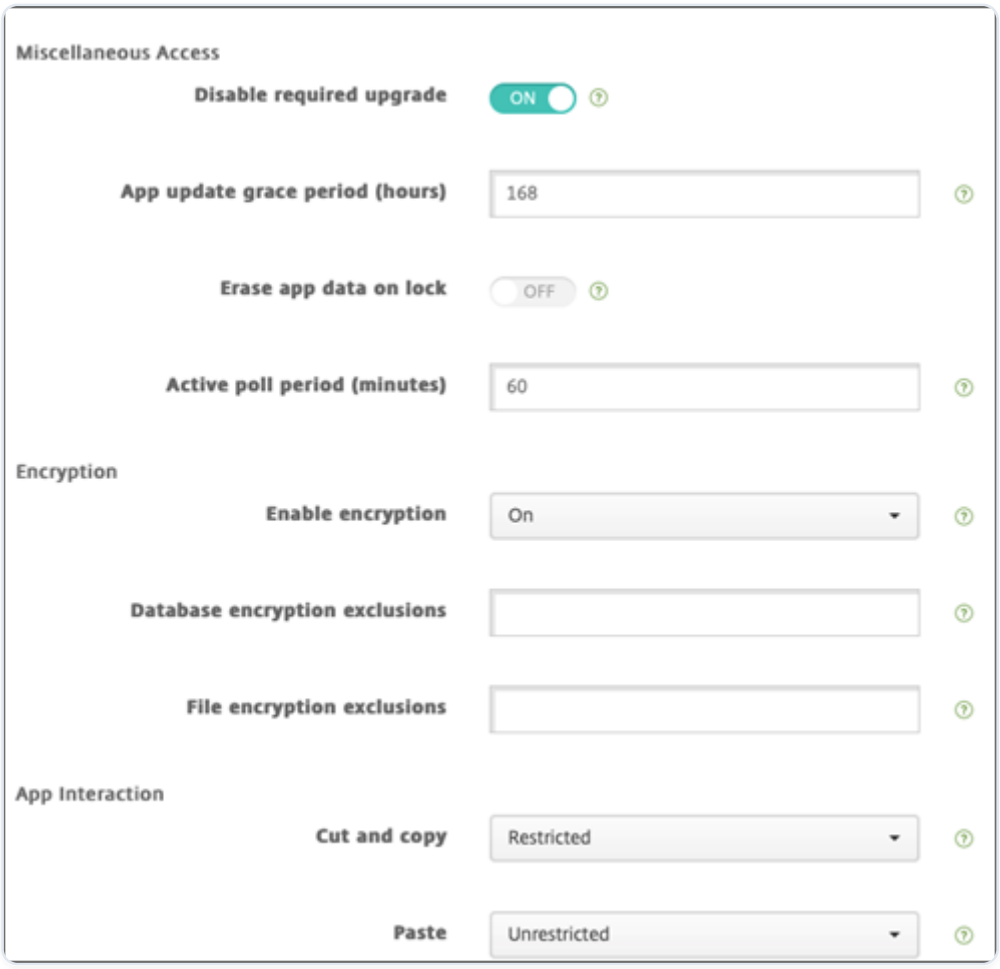


3. Selecione **iPhone** ou **iPad** para as plataformas.
4. Carregue o arquivo MDX.
5. Configure os detalhes do aplicativo. Defina **Aplicativo implantado via compra por volume** como **Desativado**. A Citrix também recomenda habilitar o recurso **Forçar gerenciamento do**

aplicativo.


Use the MDX Service on Citrix Cloud to wrap an app for delivery.
File name *
Secure Mail
App Description *
Managed Enterprise Application
App version
19.3.5
Package ID
XGFUKY3N5P.com.citrix.mail.ios
Minimum OS version
10.0
Maximum OS version
Excluded devices
example: manufacturer or model, ...
Remove app if MDM profile is removed
ON
Prevent app data backup
ON
Force app to be managed
ON
App deployed via Volume purchase
OFF
MDX Policies
Authentication
Device passcode
OFF

6. Configure as políticas MDX. Defina **Desabilitar atualização obrigatória** como **Ativado**.

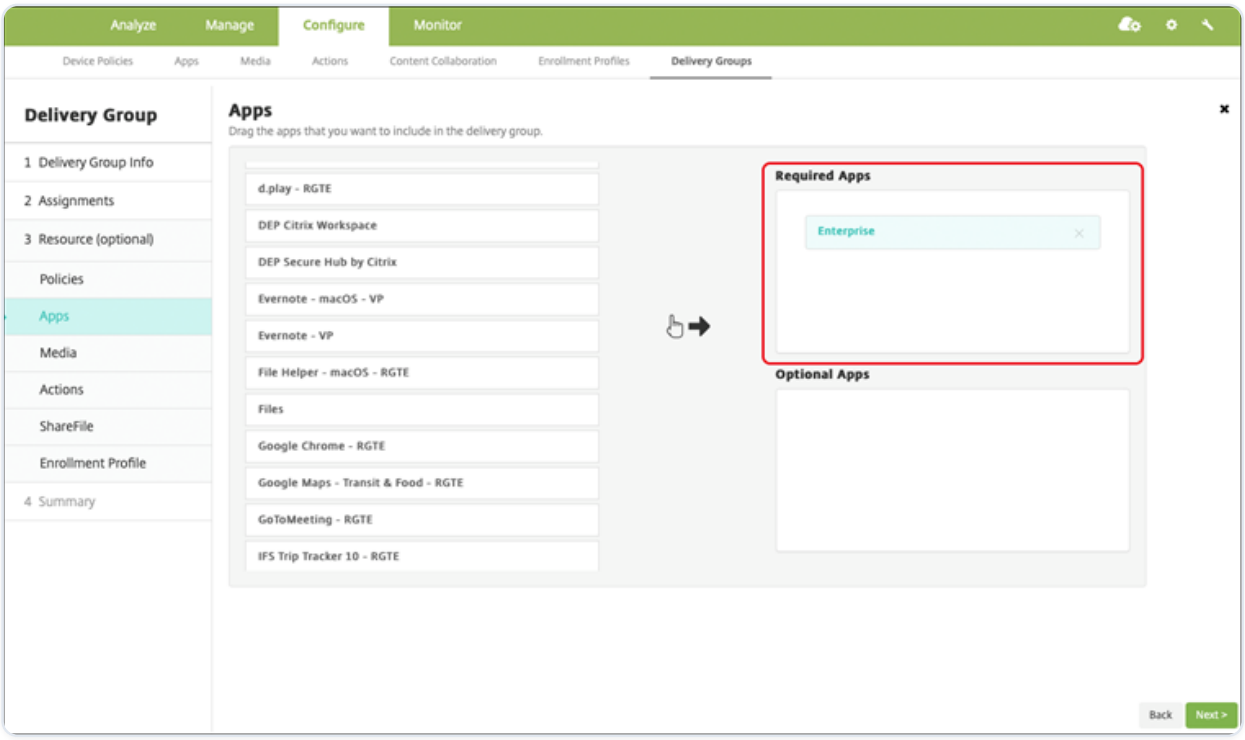


7. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configure > Delivery Groups > Apps**.

2. Marque os aplicativos desejados como **Obrigatório**.



3. navegar para **Configure > Delivery Groups**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo, e o aplicativo é instalado em segundo plano após a aceitação.



Aplicativos MDX distribuídos usando compra por volume da Apple

Para usar as políticas MDX e os recursos de segurança, adicione aplicativos que tenham o MAM SDK ativado ou que sejam empacotados em MDX. Para implantar aplicativos usando compra por volume, os aplicativos devem existir na loja de aplicativos.

DISPONIBILIDADE DO RECURSO	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

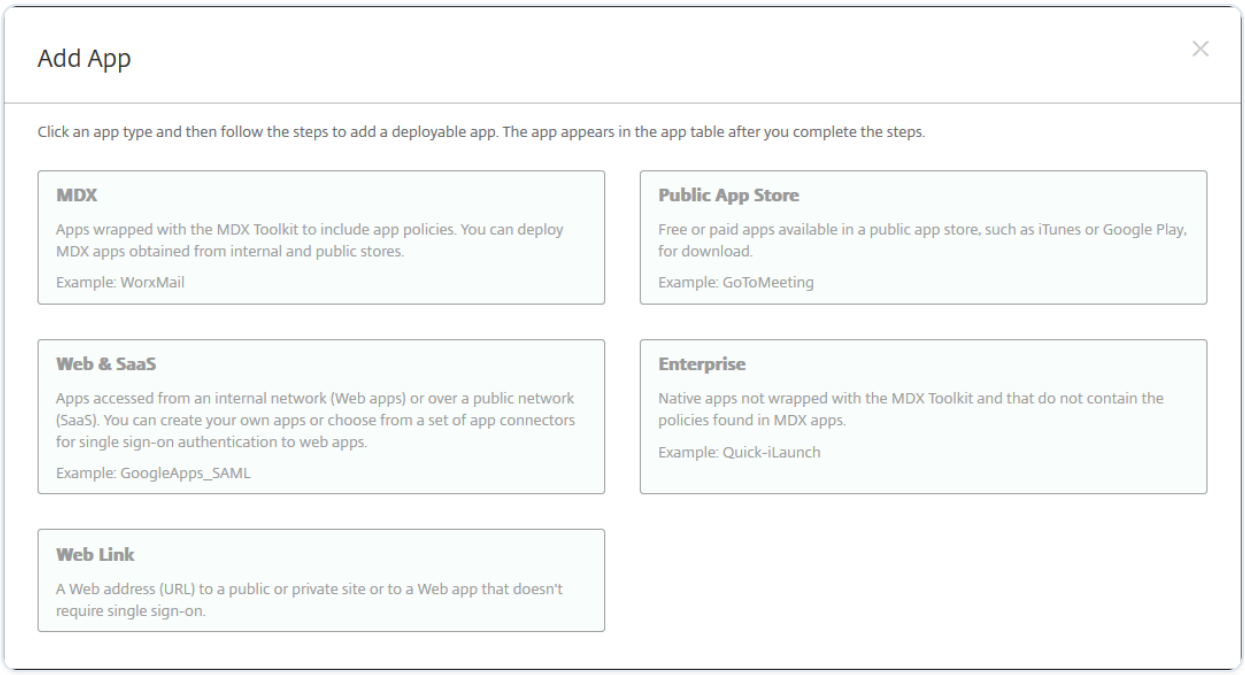
Etapa 1: Vincular contas

1. Configure e inscreva-se no Apple Business Manager (ABM) ou Apple School Manager (ASM). Para obter mais informações sobre esses programas, consulte a documentação da Apple.
2. Vincule sua conta ABM/ASM ao XenMobile. Para obter mais informações sobre como vincular contas de compra por volume, consulte Apple Volume Purchase.
3. Ao adicionar sua conta de compra por volume, ative **App Auto Update**. Essa configuração garante que os aplicativos nos dispositivos dos usuários sejam atualizados automaticamente quando uma atualização aparecer na Apple Store.

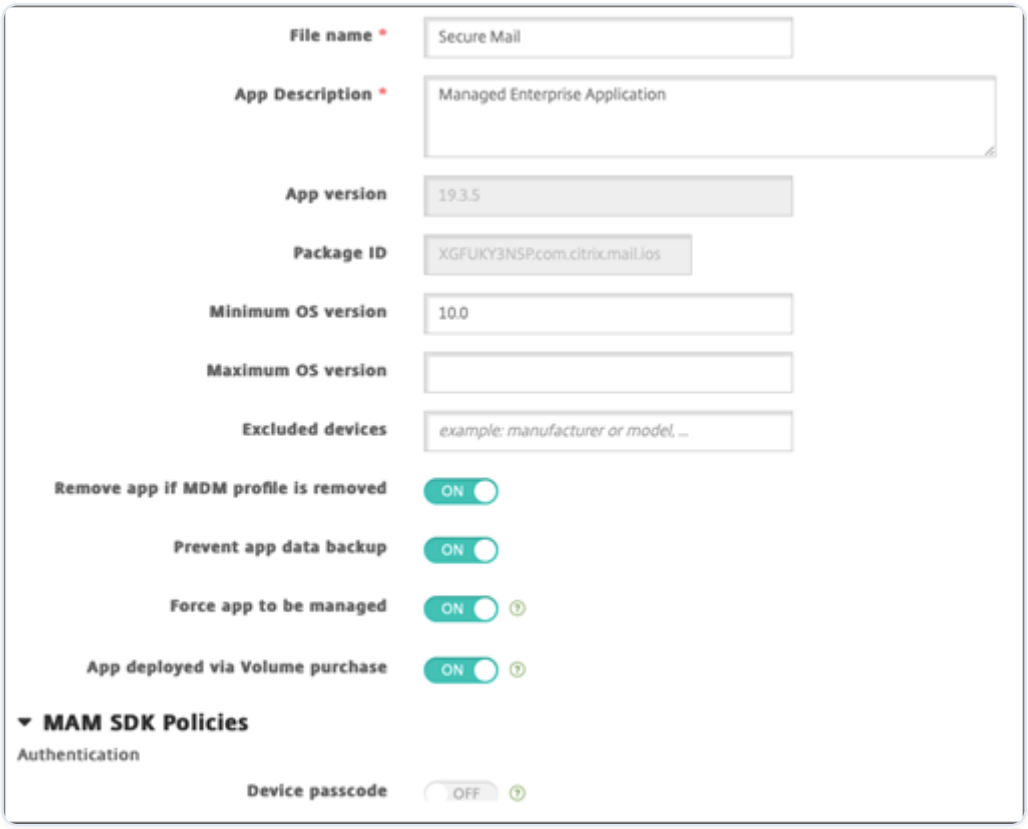
Etapa 2: Adicionar e configurar aplicativos

1. No console do XenMobile, navegar para **Configure > Apps**. Clique em **Add**.

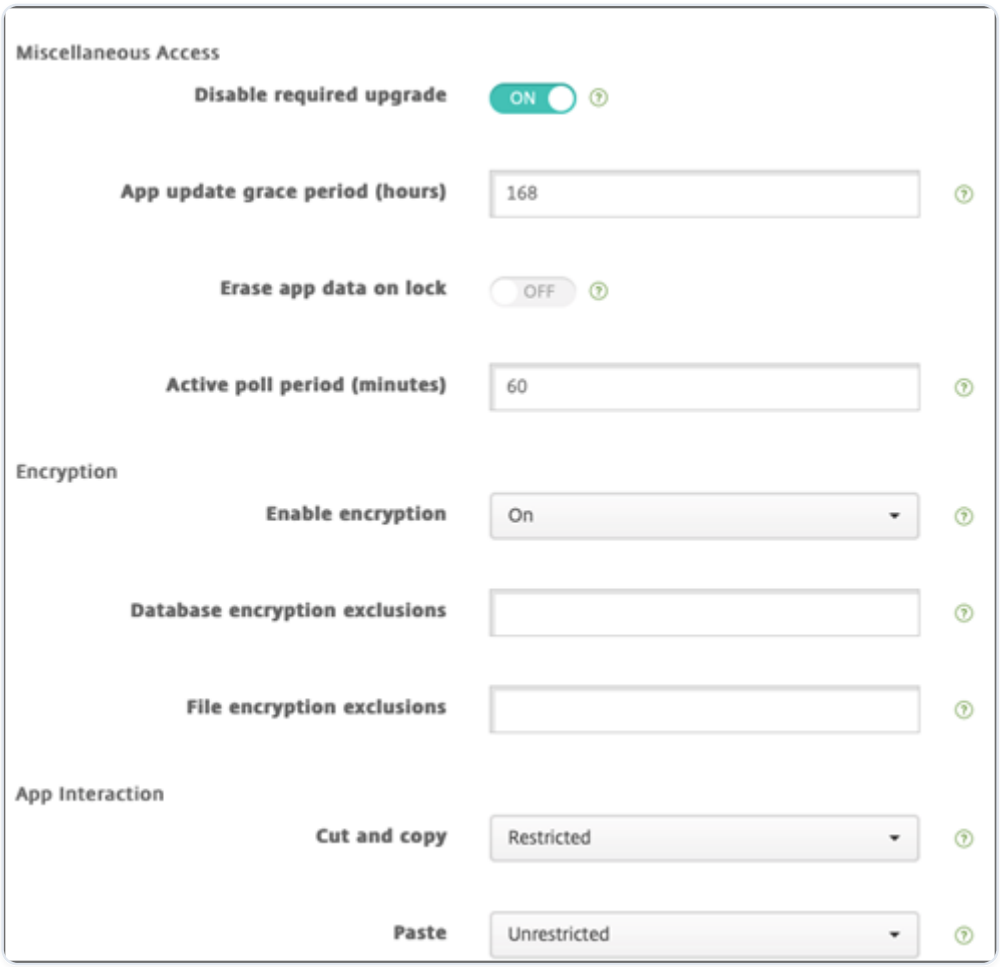
2. Clique em **MDX**.



3. Selecione **iPhone** ou **iPad** para as plataformas.
4. Carregue o arquivo MDX.
5. Configure os detalhes do aplicativo. Defina **App deployed via Volume purchase** como **On**. A Citrix também recomenda habilitar o recurso **Force app to be managed**.



6. Configure as políticas MDX. Defina **Disable required upgrade** como **On**.



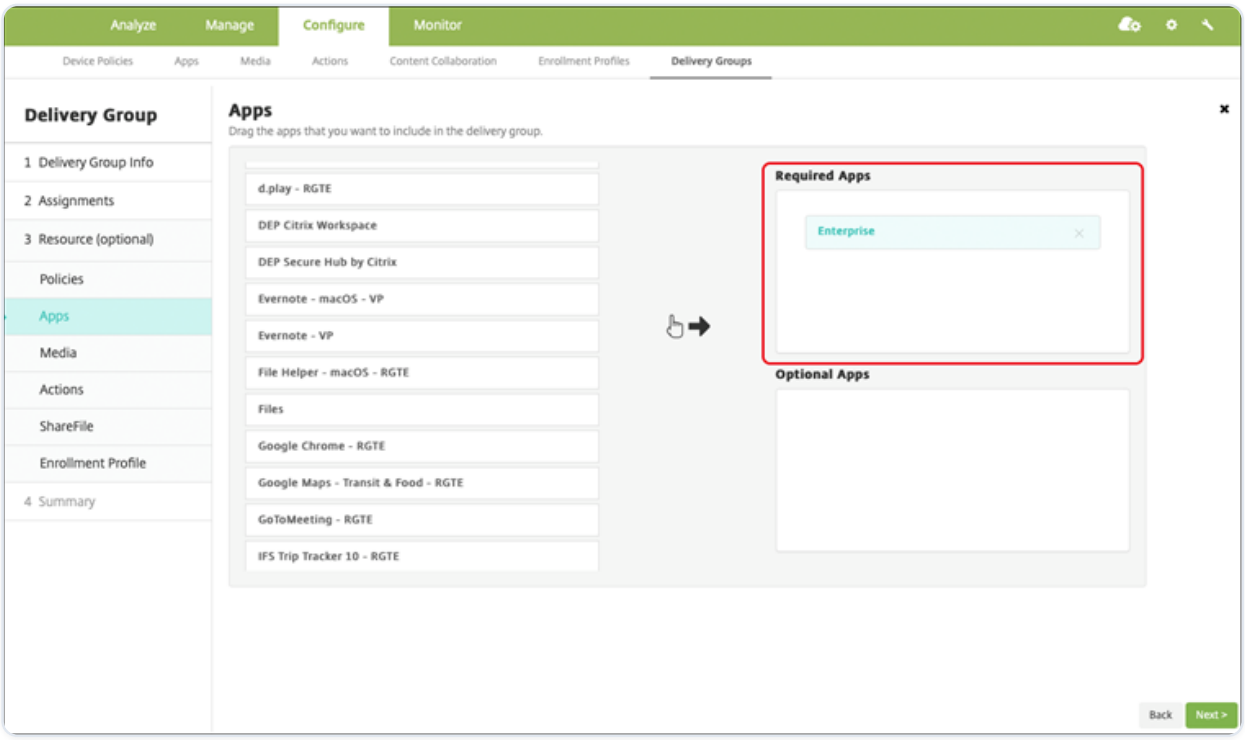
7. Atribua um grupo de entrega ao aplicativo para cada plataforma e clique em **Save**.

Essa configuração resulta em duas entradas listadas para este aplicativo na lista de aplicativos. Ao selecionar um aplicativo para configurar, selecione o aplicativo com **Type MDX**.

Etapa 3: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configure > Delivery Groups > Apps**.

2. Marque os aplicativos de compra por volume desejados como **Obrigatório**.



3. navegar para **Configurar > Grupos de Entrega**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo, e o aplicativo é instalado em segundo plano após a aceitação.



Aplicativos personalizados

Aplicativos personalizados são aplicativos proprietários business-to-business. Você pode usar o XenMobile e a compra por volume da Apple para distribuir aplicativos proprietários de forma privada e segura. Você pode distribuir os aplicativos para parceiros, clientes, franqueados e funcionários internos específicos.

DISPONIBILIDADE DE RECURSOS	
Requer supervisão do dispositivo	Não
Disponível para modo de registro de usuário	Sim
Disponível em	iOS/iPadOS

Requisitos para aplicativos personalizados

- Conta do Apple Business Manager ou Apple School Manager
- Conta de compra por volume da Apple (requer dispositivos com iOS 7 ou posterior)
- Registre dispositivos no XenMobile, usando um dos seguintes modos de registro da Apple:
  - Registro Automatizado de Dispositivo
  - Registro de dispositivo
  - Registro de usuário

Etapa 1: Vincular contas

Para implantar aplicativos personalizados usando compra por volume, vincule sua conta de compra por volume ao XenMobile.

1. Configure e registre-se no Apple Business Manager (ABM). Para obter mais informações sobre esses programas, consulte a documentação da Apple.
2. Vincule sua conta ABM ao XenMobile. Para obter mais informações sobre como vincular contas de compra por volume, consulte Compra por Volume da Apple.
3. Ao adicionar sua conta de compra por volume, habilite **Atualização Automática de Aplicativos**. Essa configuração garante que os aplicativos nos dispositivos dos usuários sejam atualizados automaticamente quando uma atualização aparecer na loja da Apple.

Etapa 2: Configurar aplicativos no ABM

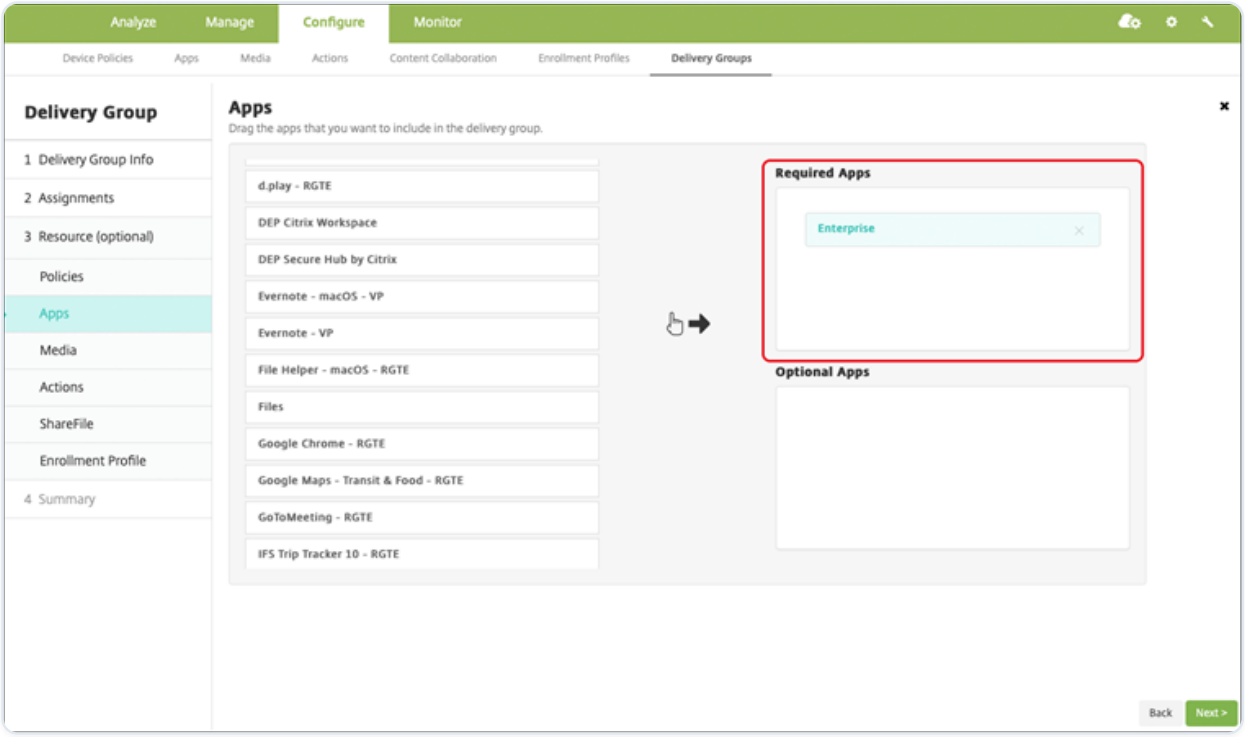
Adicione aplicativos em sua conta ABM. Você pode carregar e distribuir seus próprios aplicativos personalizados ou comprar licenças para aplicativos personalizados de outras organizações. Para obter mais informações sobre como adicionar e habilitar aplicativos personalizados no ABM, consulte a documentação da Apple.

Etapa 3: Adicionar e configurar aplicativos no XenMobile

1. No console do XenMobile, navegar para **Configurar > Aplicativos**. Os aplicativos de compra por volume aparecem na lista de aplicativos.
2. Selecione o aplicativo que você deseja configurar. Clique em **Editar**.
3. Selecione as plataformas: **iPhone**, **iPad** ou **macOS**.
4. Escolha os grupos de entrega para os quais você deseja que o aplicativo seja distribuído. Clique em **Salvar**.

Etapa 4: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configure > Delivery Groups > Apps**.
2. Marque os aplicativos que você deseja que sejam distribuídos como **Obrigatório**.



3. navegar de volta para **Configure > Delivery Groups**.
4. Selecione o grupo de entrega que você deseja implantar e clique em **Implantar**.

5. Os usuários recebem uma solicitação para implantar aplicativos. Os aplicativos são instalados em segundo plano depois que os usuários os aceitam.



Aplicativos personalizados habilitados para MDX

Para usar as políticas MDX e os recursos de segurança, adicione aplicativos personalizados que são habilitados para MAM SDK ou empacotados em MDX.

DISPONIBILIDADE DE RECURSOS	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

Etapa 1: Vincular contas

Para implantar aplicativos personalizados usando compra por volume, vincule sua conta de compra por volume ao XenMobile.

1. Configure e inscreva-se no Apple Business Manager (ABM). Para obter mais informações sobre esses programas, consulte a documentação da Apple.

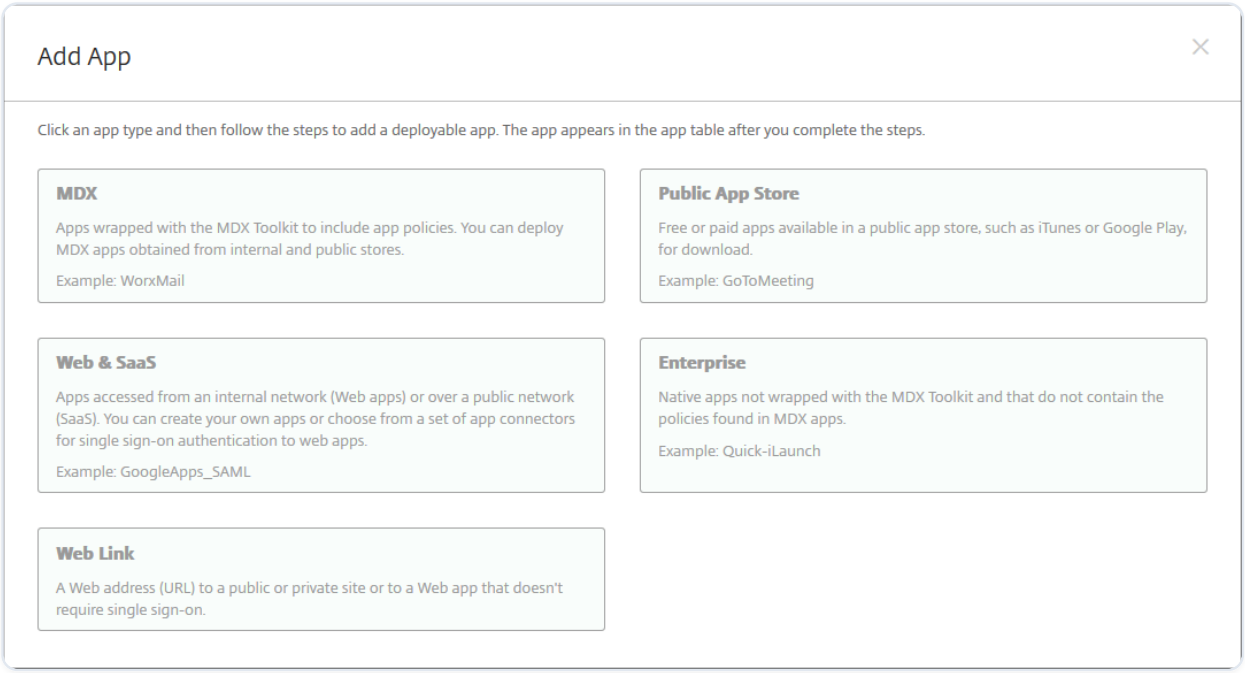
2. Vincule sua conta ABM ao XenMobile. Para obter mais informações sobre como vincular contas de compra por volume, consulte Compra por Volume da Apple.
3. Ao adicionar sua conta de compra por volume, ative **Atualização Automática de Aplicativos**. Essa configuração garante que os aplicativos nos dispositivos dos usuários sejam atualizados automaticamente quando uma atualização aparecer na loja da Apple.

Etapa 2: Configurar aplicativos no ABM

Adicione aplicativos em sua conta ABM. Você pode carregar e distribuir seus próprios aplicativos personalizados ou comprar licenças para aplicativos personalizados de outras organizações. Para obter mais informações sobre como adicionar e habilitar aplicativos personalizados no ABM, consulte a documentação da Apple.

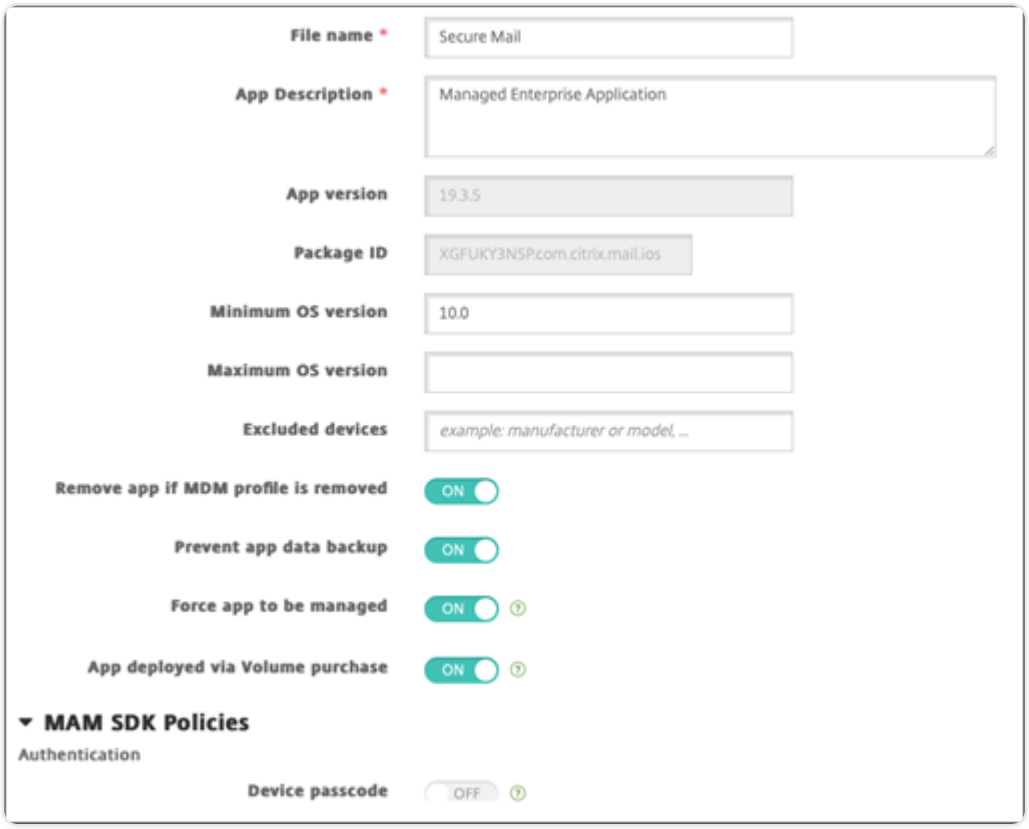
Etapa 3: Adicionar e configurar aplicativos no XenMobile

1. No console do XenMobile, navegar para **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **MDX**.

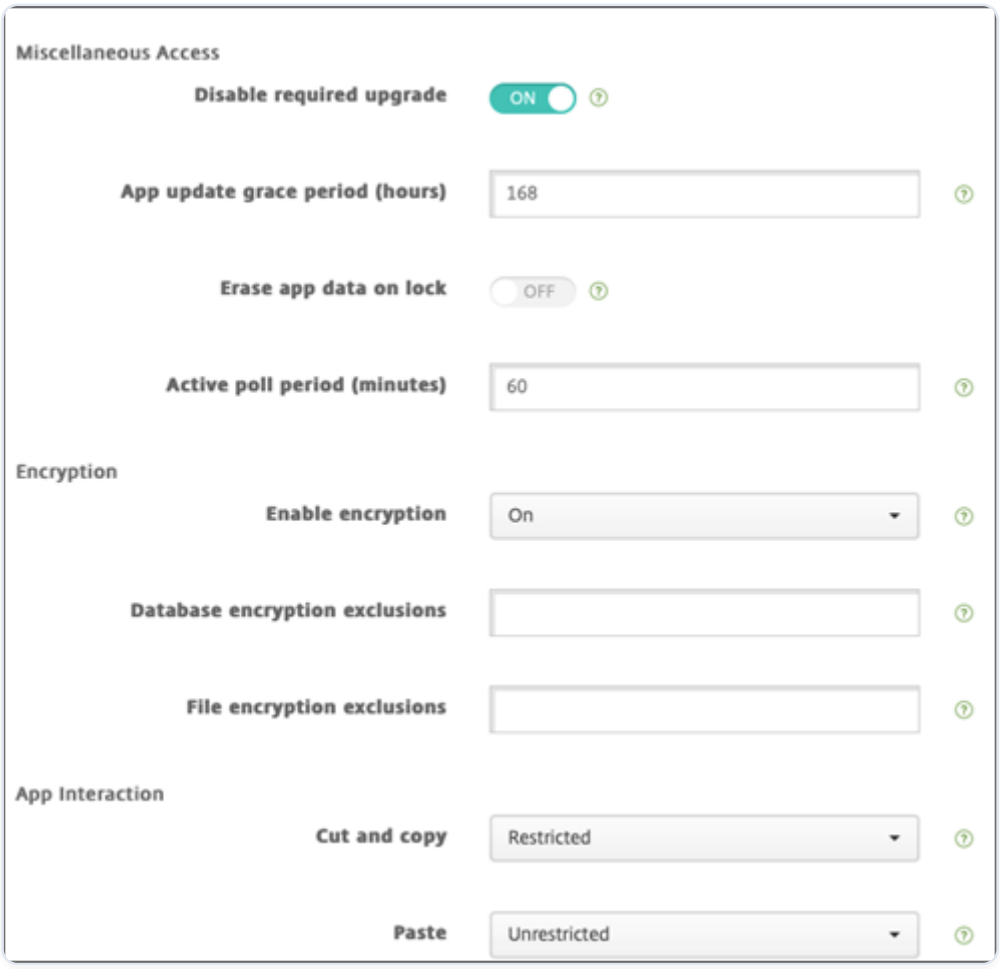


3. Selecione as plataformas **iPhone** ou **iPad**.
4. Carregue o arquivo MDX para o aplicativo que você deseja adicionar.

5. Configure os detalhes do aplicativo. Defina **Aplicativo implantado via compra por volume** como **Ativado**. A Citrix também recomenda habilitar o recurso **Forçar gerenciamento do aplicativo**.



6. Configure as políticas MDX. Defina **Desabilitar atualização obrigatória** como **Ativado**.



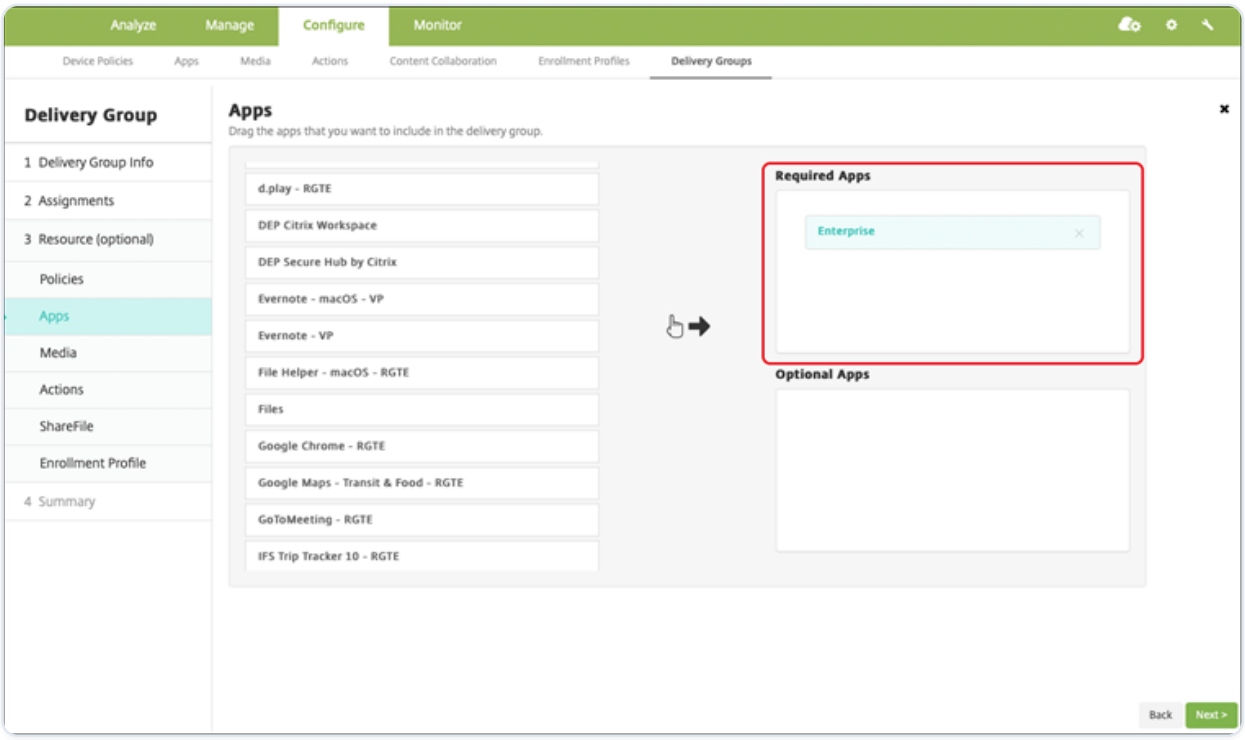
7. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Essa configuração resulta em duas entradas listadas para este aplicativo na lista de aplicativos. Ao selecionar um aplicativo para configurar, selecione o aplicativo com **Tipo MDX**.

Etapa 4: Configurar a implantação do aplicativo

1. No console do XenMobile, navegar para **Configurar > Aplicativos**. Os aplicativos de compra por volume aparecem na lista de aplicativos.
2. Selecione o aplicativo que você deseja configurar. Clique em **Editar**.
3. Escolha os grupos de entrega para os quais você deseja que o aplicativo seja distribuído em cada plataforma. Clique em **Salvar**.
4. navegar de volta para **Configurar > Grupos de Entrega > Aplicativos**.

5. Marque os aplicativos que você deseja que sejam distribuídos como **Obrigatório**.



6. navegar de volta para **Configurar > Grupos de Entrega**.
7. Selecione o grupo de entrega que você deseja implantar e clique em **Implantar**.
8. Os usuários recebem uma solicitação para implantar aplicativos. Os aplicativos são instalados em segundo plano após a aceitação.

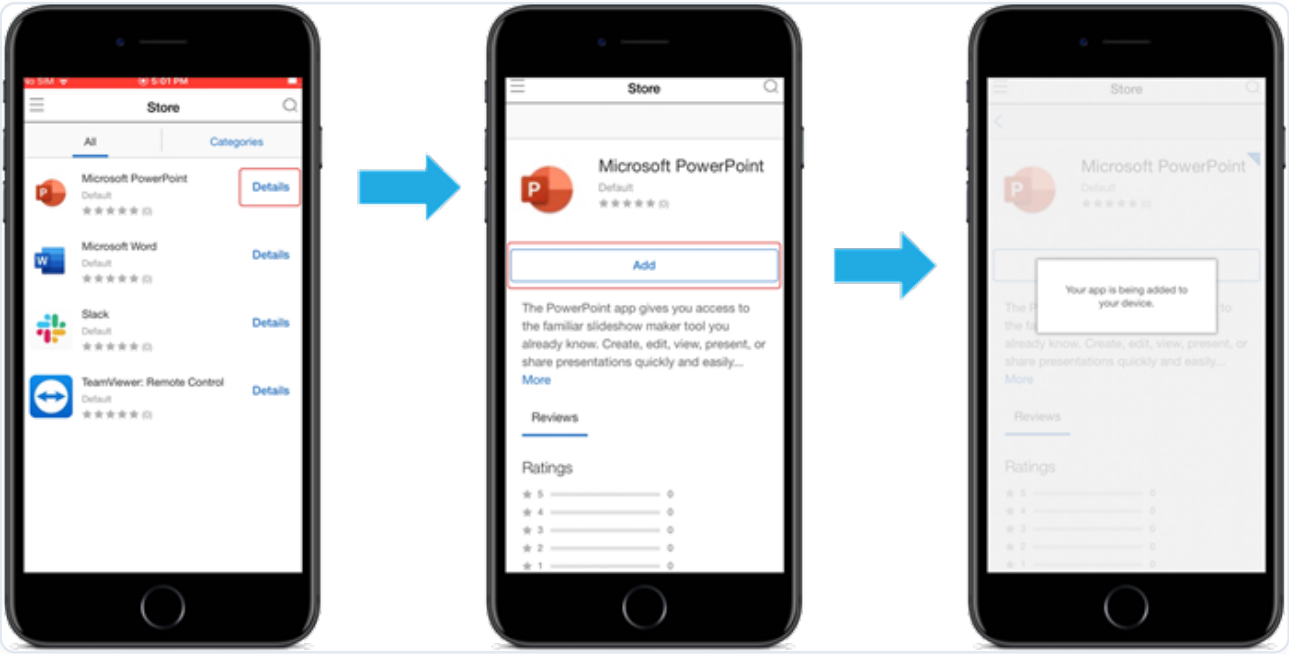


Aplicativos opcionais (somente iOS/iPadOS)

A Citrix recomenda implantar aplicativos como **Obrigatório**. Aplicativos obrigatórios são instalados silenciosamente nos dispositivos dos usuários, minimizando a interação. Ter esse recurso ativado também permite que os aplicativos sejam atualizados automaticamente.

Aplicativos opcionais permitem que os usuários escolham quais aplicativos instalar, mas os usuários devem iniciar a instalação manualmente através do Secure Hub.

Para instalar aplicativos opcionais, os usuários devem iniciar o Secure Hub, ir para **Loja**, selecionar **Detalhes** para o aplicativo desejado e clicar em **Adicionar**.



Controle de Acesso à Rede

Você pode usar a solução de Controle de Acesso à Rede (NAC) para estender a avaliação de segurança de dispositivos XenMobile® para dispositivos Android e Apple. A solução NAC usa a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação. Depois de configurar seu dispositivo NAC, as políticas de dispositivo e os filtros NAC que você configura no XenMobile são aplicados.

Usar o XenMobile com uma solução NAC adiciona QoS e um controle mais granular sobre os dispositivos internos à sua rede. Para um resumo das vantagens de integrar o NAC com o XenMobile, consulte Controle de acesso.

A Citrix® oferece suporte a estas soluções para integração com o XenMobile:

- Citrix Gateway

- Cisco Identity Services Engine (ISE)
- ForeScout

A Citrix® não garante a integração para outras soluções NAC.

Com um dispositivo NAC em sua rede:

- O XenMobile oferece suporte ao NAC como um recurso de segurança de endpoint para dispositivos iOS, Android Enterprise e Android.
- Você pode habilitar filtros no XenMobile para definir dispositivos como compatíveis ou não compatíveis para NAC, com base em regras ou propriedades. Por exemplo:
  - Se um dispositivo gerenciado no XenMobile não atender aos critérios especificados, o XenMobile marca o dispositivo como não compatível. Um dispositivo NAC bloqueia dispositivos não compatíveis em sua rede.
  - Se um dispositivo gerenciado no XenMobile tiver aplicativos não compatíveis instalados, um filtro NAC pode bloquear a conexão VPN. Como resultado, um dispositivo de usuário não compatível não pode acessar aplicativos ou sites através da VPN.
  - Se você usa o Citrix Gateway para NAC, você pode habilitar o tunelamento dividido para evitar que o plug-in do Citrix Gateway envie tráfego de rede desnecessário para o Citrix Gateway. Para obter mais informações sobre tunelamento dividido, consulte Configurando o Tunelamento Dividido.

Filtros de conformidade NAC suportados

O XenMobile Server suporta os seguintes filtros de conformidade NAC:

Dispositivos Anônimos: Verifica se um dispositivo está no modo anônimo. Essa verificação está disponível se o XenMobile não conseguir reautenticar o usuário quando um dispositivo tentar se reconectar.

Atestado Samsung Knox com falha: Verifica se um dispositivo falhou em uma consulta ao servidor de atestado Samsung Knox.

Aplicativos Proibidos: Verifica se um dispositivo possui aplicativos proibidos, conforme definido em uma política de dispositivo de Acesso a Aplicativos. Para obter informações sobre essa política, consulte Políticas de dispositivo de acesso a aplicativos.

Dispositivos Inativos: Verifica se um dispositivo está inativo conforme definido pela configuração **Limite de Dias de Inatividade do Dispositivo** em **Propriedades do Servidor**. Para obter detalhes, consulte Propriedades do servidor.

Aplicativos Obrigatórios Ausentes: Verifica se um dispositivo está faltando algum aplicativo obrigatório, conforme definido em uma política de Acesso a Aplicativos.

Aplicativos Não Sugeridos: Verifica se um dispositivo possui aplicativos não sugeridos, conforme definido em uma política de Acesso a Aplicativos.

Senha Não Conforme: Verifica se a senha do usuário está em conformidade. Em dispositivos iOS e Android, o XenMobile pode determinar se a senha atualmente no dispositivo está em conformidade com a política de senha enviada ao dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de senha para o dispositivo. Antes que o usuário defina a senha, a senha pode não estar em conformidade.

Dispositivos Fora de Conformidade: Verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Fora de Conformidade. Normalmente, ações automatizadas ou terceiros usando APIs do XenMobile alteram essa propriedade do dispositivo.

Status Revogado: Verifica se o certificado do dispositivo foi revogado. Um dispositivo revogado não pode se registrar novamente até ser autorizado novamente.

Dispositivos Android com Root e iOS com Jailbreak: Verifica se um dispositivo Android ou iOS tem jailbreak.

Dispositivos Não Gerenciados: Verifica se um dispositivo ainda está em um estado gerenciado sob o controle do XenMobile. Por exemplo, um dispositivo registrado no MAM ou um dispositivo não registrado não é gerenciado.

> **Observação:**
>
> O filtro Implícito Conforme/Não Conforme define o valor padrão apenas em dispositivos que o XenMobile está gerenciando. Por exemplo, quaisquer dispositivos que tenham um aplicativo bloqueado instalado ou não estejam registrados, são marcados como Não Conformes. O dispositivo NAC bloqueia esses dispositivos da sua rede.

Visão geral da configuração

Recomendamos que você configure os componentes do NAC na ordem listada.

1. Configure as políticas de dispositivo para oferecer suporte ao NAC:

Para dispositivos iOS: Consulte Configurar a política de dispositivo VPN para oferecer suporte ao NAC.

Para dispositivos Android Enterprise: Consulte Criar uma configuração gerenciada do Android Enterprise para Citrix SSO.

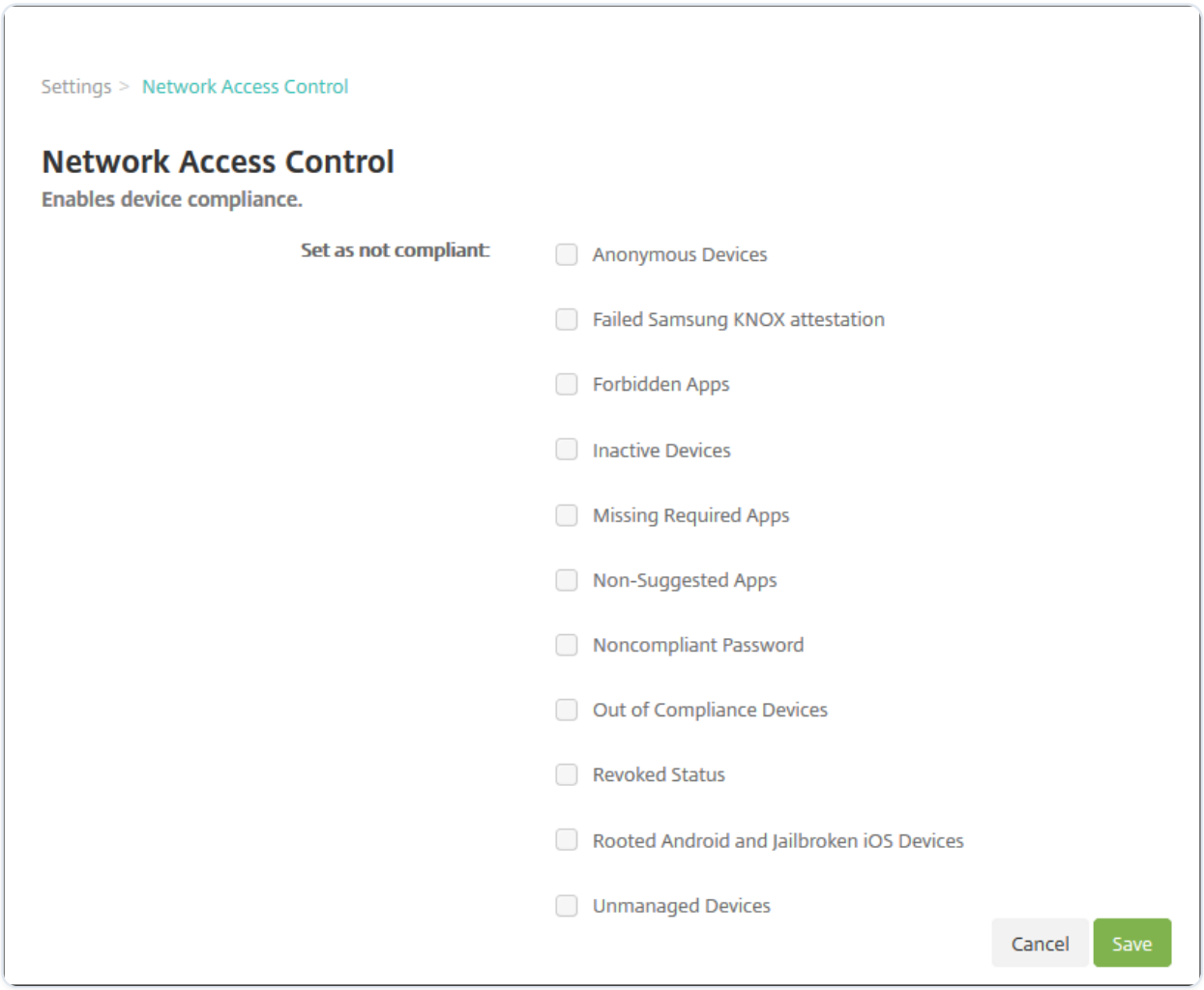
Para dispositivos Android: Consulte Configurar o protocolo Citrix SSO para Android.

2. Habilitar filtros NAC no XenMobile.
3. Configure uma solução NAC:
   - Citrix Gateway, detalhado em Atualizar políticas do Citrix Gateway para oferecer suporte ao NAC.

     Requer que você instale o Citrix SSO nos dispositivos. Consulte Clientes do Citrix Gateway.
   - Cisco ISE: Consulte a documentação da Cisco.
   - ForeScout: Consulte a documentação da ForeScout.

Habilitar filtros NAC no XenMobile

1. No console do XenMobile, vá para **Configurações > Controle de Acesso à Rede**.



2. Selecione as caixas de seleção para os filtros **Definir como não compatível** que você deseja habilitar.
3. Clique em **Salvar**.

Atualizar políticas do Citrix Gateway para oferecer suporte a NAC

Você deve configurar políticas de autenticação e sessões VPN avançadas (não clássicas) no seu servidor virtual VPN.

Estas etapas atualizam um Citrix Gateway com uma destas características:

- Está integrado com um ambiente de servidor XenMobile.
- Ou, está configurado para VPN, não faz parte do ambiente de servidor XenMobile e pode acessar o XenMobile.

No seu servidor virtual VPN, em uma janela de console, faça o seguinte. Os endereços IP nos comandos e exemplos são fictícios.

1. Se você estiver usando políticas clássicas no seu servidor virtual VPN, remova e desvincule todas as políticas clássicas. Para verificar, digite:

   `show vpn vserver <VPN_VServer>`

   Remova qualquer resultado que contenha a palavra **Classic**. Por exemplo: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Para remover a política, digite:

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`

2. Crie a política de sessão avançada correspondente digitando o seguinte.

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   Por exemplo: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Vincule a política ao seu servidor virtual VPN digitando o seguinte.

   `bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100`

4. Crie um servidor virtual de autenticação digitando o seguinte.

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   Por exemplo: `add authentication vserver authvs SSL 0.0.0.0` No exemplo, `0.0.0.0` significa que o servidor virtual de autenticação não está voltado para o público.

5. Vincule um certificado SSL ao servidor virtual digitando o seguinte.

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   Por exemplo: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associe um perfil de autenticação ao servidor virtual de autenticação a partir do servidor virtual VPN. Primeiro, crie o perfil de autenticação digitando o seguinte.

   `add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

   Por exemplo:

   `add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. Associe o perfil de autenticação ao servidor virtual VPN digitando o seguinte.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   Por exemplo:

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. Verifique a conexão do Citrix Gateway com um dispositivo digitando o seguinte.

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   Por exemplo, esta consulta verifica a conectividade obtendo o status de conformidade para o primeiro dispositivo (`deviceid_1`) registrado no ambiente:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   Um resultado bem-sucedido é semelhante ao exemplo a seguir.

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. Quando a etapa anterior for bem-sucedida, crie a ação de autenticação da web para o XenMobile. Primeiro, crie uma expressão de política para extrair o ID do dispositivo do plug-in VPN do iOS. Digite o seguinte.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envie a solicitação para o XenMobile digitando o seguinte. Neste exemplo, o IP do XenMobile Server é `10.207.87.82` e o FQDN é `example.em.server.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host: example.em.server.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " +
    ```

`xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"`

A saída bem-sucedida para o NAC do XenMobile é `HTTP status 200 OK`. O cabeçalho `X-Citrix-Device-State` deve ter o valor de `Compliant`.

11. Crie uma política de autenticação para associar a ação digitando o seguinte.

    `add authentication Policy <policy name> -rule <rule> -action <web authentication action>`

    Por exemplo: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. Converta a política LDAP existente em uma política avançada digitando o seguinte.

    `add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>`

    Por exemplo: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Adicione um rótulo de política ao qual associar a política LDAP digitando o seguinte.

    `add authentication policylabel <policy_label_name>`

    Por exemplo: `add authentication policylabel ldap_pol_label`

14. Associe a política LDAP ao rótulo da política digitando o seguinte.

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. Conecte um dispositivo compatível para fazer um teste NAC para confirmar a autenticação LDAP bem-sucedida. Digite o seguinte.

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. Adicione a interface do usuário para associar ao servidor virtual de autenticação. Digite o seguinte comando para recuperar o ID do dispositivo.

    `add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. Vincule o servidor virtual de autenticação digitando o seguinte.

    ```
    bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
    ```

18. Crie uma política de autenticação avançada LDAP para habilitar a conexão do Secure Hub. Digite o seguinte.

    ```
    add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP
    ```

    ```
    bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110 -gotoPriorityExpression NEXT
    ```

Samsung Knox

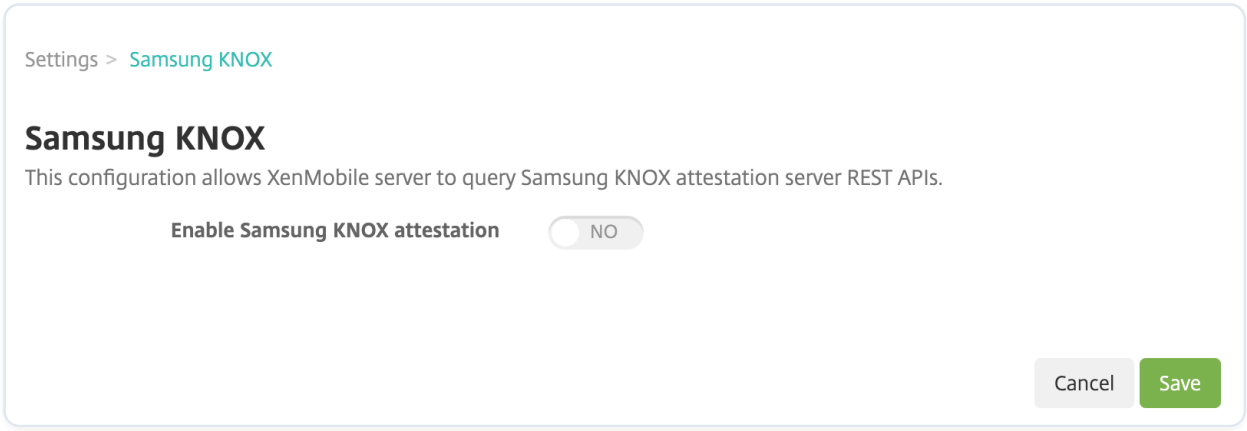
A Samsung oferece várias soluções compatíveis com o XenMobile® Server.

- O XenMobile oferece suporte e estende as políticas do Samsung Knox em dispositivos Samsung compatíveis.
- O plug-in do Knox Service (KSP) é um aplicativo que oferece suporte a um subconjunto de recursos do Knox Platform for Enterprise (KPE). Para obter informações da Samsung sobre o KPE, consulte Configurar o Knox Platform for Enterprise e Visão geral.

Você pode configurar o XenMobile para consultar as APIs REST do servidor de atestado do Samsung Knox.

O Samsung Knox usa recursos de segurança de hardware que fornecem vários níveis de proteção para o sistema operacional e aplicativos. Um nível dessa segurança está na plataforma, por meio de atestado. Um servidor de atestado fornece verificação do software do sistema central do dispositivo móvel (por exemplo, os carregadores de inicialização e o kernel). A verificação ocorre em tempo de execução com base nos dados coletados durante a inicialização confiável.

1. No console web do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Plataformas**, clique em **Samsung KNOX**. A página **Samsung KNOX** é exibida.



3. Em **Habilitar atestado do Samsung KNOX**, selecione se deseja habilitar o atestado do Samsung Knox. O padrão é **NÃO**.
4. Clique em **Salvar**.

Nota:

Você pode usar o Samsung Knox Mobile Enrollment para registrar vários dispositivos Samsung Knox no XenMobile (ou em qualquer gerenciador de dispositivos móveis) sem configurar manualmente cada dispositivo. Para obter informações, consulte Registro em massa do Samsung Knox.

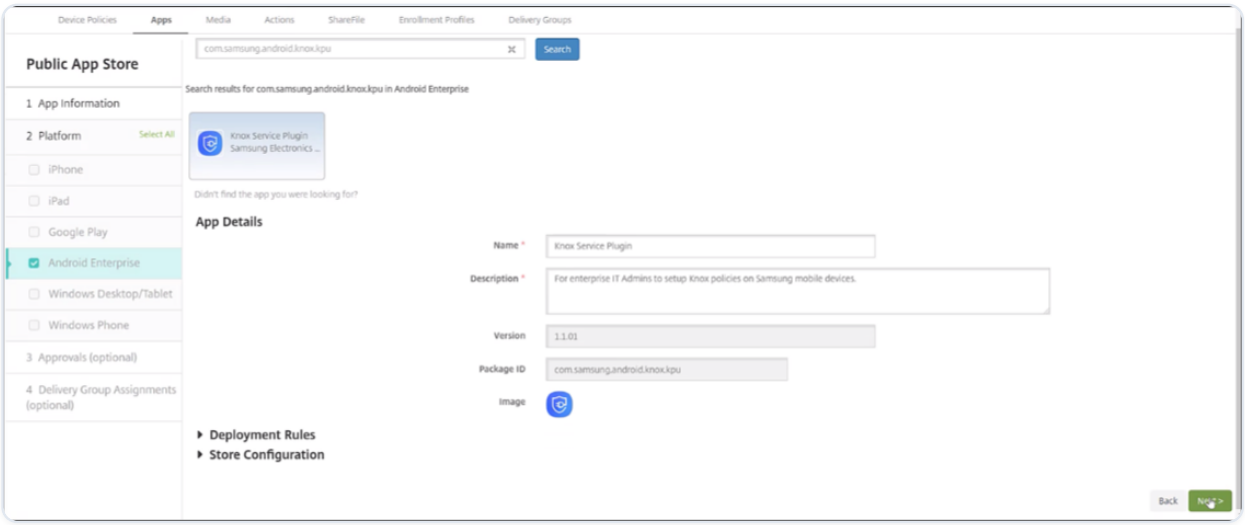
Adicionar o aplicativo plug-in do serviço Knox

Se você planeja usar o Android Enterprise com o Knox, adicione o plug-in do serviço Knox (KSP) ao XenMobile. O aplicativo KSP usa o AndroidOEMConfig para oferecer suporte a recursos como políticas de segurança, configuração flexível de VPN e controles de autenticação biométrica. O AndroidOEMConfig permite que OEMs e gerentes de mobilidade de endpoint (EMM) ofereçam suporte a APIs OEM personalizadas. Essas APIs cobrem casos de uso não suportados pelo Android Enterprise.

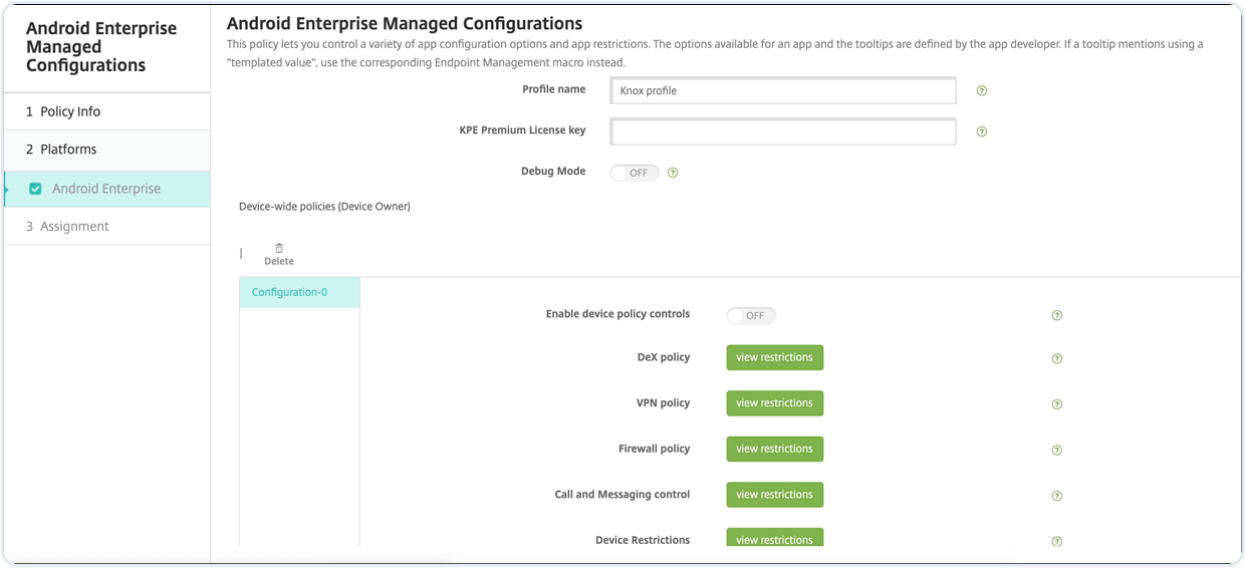
Para mais informações sobre KSP, consulte o Guia do Plug-in do Serviço Knox.

1. Faça login na sua conta Google e navegar para `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`. Aprove o aplicativo Knox Service Plug-in.
2. Faça login no seu console XenMobile e adicione o plug-in do serviço Knox como um aplicativo da loja de aplicativos pública. Para mais informações sobre como adicionar aplicativos da loja

de aplicativos pública, consulte Adicionar um aplicativo da loja de aplicativos pública.

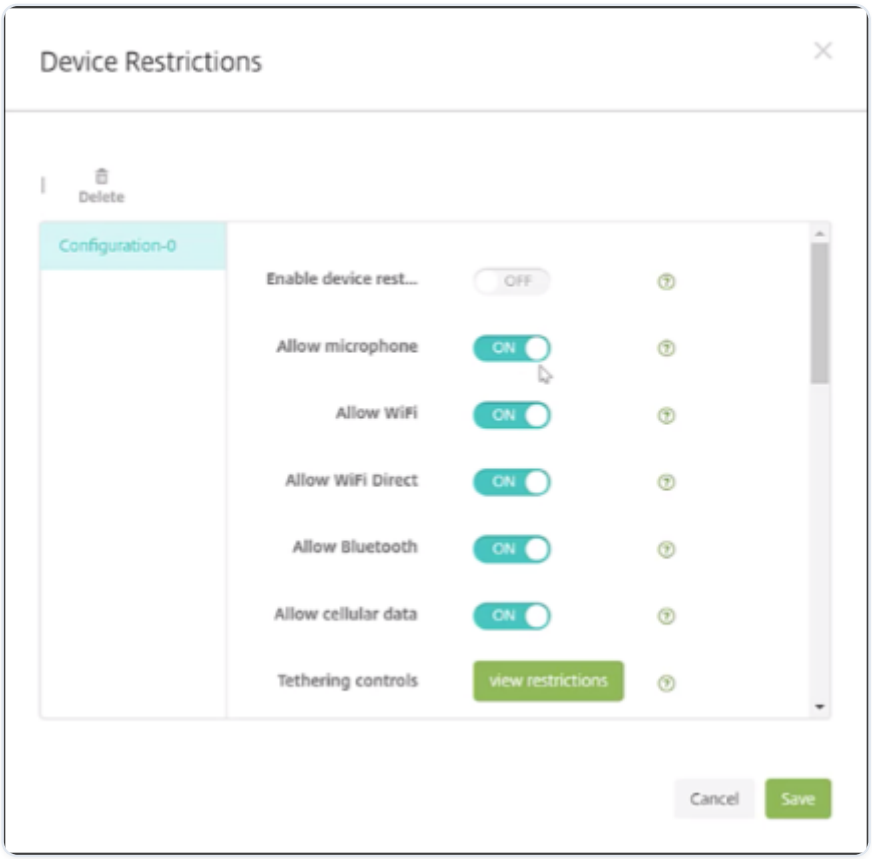


3. No seu console XenMobile, navegar para **Configurar > Políticas de dispositivo**. Clique em **Adicionar**.
4. Clique em **Configurações Gerenciadas**. Na caixa de diálogo que aparece, selecione **Knox Service Plugin** no menu. Para mais informações sobre a política de configuração gerenciada, consulte Política de configurações gerenciadas.
5. Digite um nome para a política e continue para a página da plataforma.



6. Na página da plataforma, digite um **Nome do perfil** para o seu perfil Knox e insira a **chave de licença KPE Premium** da Samsung. As políticas que aparecem abaixo desses campos vêm da sua implantação Knox. Para mais informações sobre as políticas Knox, consulte o Guia do

Plug-in de Administração do Serviço Knox referenciado anteriormente nesta seção.



7. Clique em **Avançar** e configure as regras de implantação para a política.
8. Clique em **Salvar**.

Registro em massa do Samsung Knox

Para registrar vários dispositivos Samsung Knox no XenMobile® (ou em qualquer gerenciador de dispositivos móveis) sem configurar manualmente cada dispositivo, use o Registro Móvel Knox. O registro ocorre no primeiro uso ou após uma redefinição de fábrica. Os administradores também podem passar nomes de usuário e senhas diretamente para o dispositivo, para que os usuários não precisem inserir nenhuma informação no momento do registro.

> **Nota:**
>
> A configuração para o Registro Móvel Knox não está relacionada ao contêiner Knox do XenMobile. Para obter mais informações sobre o Registro Móvel Knox, consulte o Guia do Administrador do Registro Móvel Knox.

Pré-requisitos para o Registro Móvel Knox

- O XenMobile deve estar configurado (incluindo licenças e certificados) e em execução.
- Arquivo APK do Secure Hub. Você carrega o arquivo ao configurar o Registro Móvel Knox.
- Para obter uma lista de requisitos do KME, consulte a Introdução ao Registro Móvel Knox.
- Licença do Samsung Knox Platform for Enterprise (PKE) que é necessária para aplicar políticas de dispositivo. Forneça a chave de licença na política de dispositivo do XenMobile, Knox Platform for Enterprise.

Para baixar o arquivo APK do Secure Hub

Vá para a Google Play Store para baixar o arquivo Citrix Secure Hub™ para Android.

Configurar exceções de firewall

Para acessar o Registro Móvel Knox, configure as seguintes exceções de firewall. Algumas dessas exceções de firewall são necessárias para todos os dispositivos e algumas são específicas para a região geográfica do dispositivo.

REGIÃO DO DISPOSITIVO	URL	PORTA	DESTINO
Todos	`https://gslb.secb2b.com`	443	Balanceador de carga global para iniciação do Knox Mobile Enrollment
Todos	`https://gslb.secb2b.com`	80	Balanceador de carga global para iniciação do Knox Mobile Enrollment em alguns dispositivos legados limitados
Todos	`umc-cdn.secb2b.com`	443	Servidores de atualização do agente Samsung
Todos	`bulkenrollment.s3.amazonaws.com`	80	EULAs do cliente do Knox Mobile Enrollment

XENMOBILE® SERVER

REGIÃO DO DISPOSITIVO	URL	PORTA	DESTINO
Todos	`eula.secb2b.com`	443	EULAs do cliente do Knox Mobile Enrollment
Todos	`us-be-api-mssl.samsungknox.com`	443	Servidores Samsung para verificação de IMEI
Estados Unidos	`https://us-segd-api.secb2b.com`	443	Samsung Enterprise Gateway para a região dos EUA
Europa	`https://eu-segd-api.secb2b.com`	443	Samsung Enterprise Gateway para a região europeia
China	`https://china-segd-api.secb2b.com`	443	Samsung Enterprise Gateway para a região da China

Nota:

Você pode encontrar uma lista completa de exceções de firewall no Guia do Administrador do Knox Mobile Enrollment.

Obtendo acesso ao Knox Mobile Enrollment

Siga a documentação da Samsung para obter acesso ao Knox Mobile Enrollment em Começar com o KME.

Configurando o Knox Mobile Enrollment

Depois de obter acesso ao Knox Mobile Enrollment, faça login no portal Knox.

O processo de registro segue estas etapas gerais.

1. Crie um perfil MDM com as informações e configurações do seu console MDM.

O perfil MDM indica aos seus dispositivos como se conectar ao seu MDM.

2. Adicione os dispositivos ao seu perfil MDM.

   Você pode fazer upload de um arquivo CSV com informações do dispositivo ou instalar e usar o aplicativo de implantação Knox do Google Play.

3. A Samsung o alerta quando a propriedade do dispositivo é verificada.
4. Forneça aos usuários credenciais MDM. Instrua-os a se conectar à Internet usando Wi-Fi e a aceitar o prompt para registrar seu dispositivo.

Para criar um perfil MDM

Siga as etapas descritas na documentação da Samsung sobre Configuração de Perfil.

Ao encontrar os seguintes campos ou etapas, configure-os conforme descrito:

- **Escolha seu MDM:** Selecione **Citrix®** no menu. Somente para perfis de proprietário de dispositivo.
- **APK do Agente MDM:** Somente para perfis de proprietário de dispositivo. Digite o URL de download do APK do Secure Hub: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

  O arquivo APK pode permanecer em qualquer servidor que o dispositivo possa acessar durante o registro. Durante o registro, um dispositivo:

  - Baixa o Secure Hub do URL de download do APK
  - Instala o Secure Hub
  - Em seguida, abre o Secure Hub com os dados JSON personalizados descritos a seguir.

  A capitalização do nome do arquivo .apk deve corresponder à URL que você insere. Por exemplo, se o nome do arquivo estiver todo em minúsculas, ele também deve estar todo em minúsculas na URL.
- **URI do Servidor MDM:** Não especifique um URI do servidor MDM. O XenMobile não usa o protocolo MDM da Samsung.
- **Dados JSON Personalizados:** O Secure Hub precisa do endereço do XenMobile Server, além do nome de usuário e senha para o registro. Você pode fornecer esses dados em JSON para que o Secure Hub não solicite aos usuários. O Secure Hub solicita aos usuários o endereço do servidor, nome de usuário ou senha somente se o campo for omitido do JSON.

  O formato para dados JSON personalizados é:

`{"serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}`

Neste exemplo, típico para registro em massa, o Secure Hub não solicita aos usuários o endereço do servidor ou suas credenciais durante o registro:

`{"serverURL":"https://example.com/zdm", "xm_username":"userN", "xm_password":"password1234"}` `{"serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2", "xm_password":"password7890"}`

Neste exemplo, típico para dispositivos baseados em quiosque, o Secure Hub solicita aos usuários suas credenciais:

`{"serverURL":"https://example.com/zdm"}`

Você também pode inserir o JSON personalizado para registro zero-touch para Android Enterprise.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

    {


"serverURL":"URL","xm_username":"username","xm_password":"password"

    }

}
```

Quando um dispositivo inicia o registro, ele baixa o Secure Hub da URL fornecida, instala o Secure Hub e o abre.

Configuração adicional

Consulte as seguintes páginas da documentação da Samsung para obter mais informações sobre a configuração:

- Configuração do dispositivo: Adicione dispositivos em massa.
- Aplicativo de Implantação Samsung Knox: Registre dispositivos via Bluetooth, NFC ou registro Wi-Fi Direct.

- Knox Mobile Enrollment: Explore a documentação da Samsung para obter mais informações sobre o Samsung Knox.

Para registrar dispositivos que executam uma API Knox anterior à versão 2.4

Em dispositivos que possuem a API Knox anterior à versão 2.4, o registro em massa não é iniciado durante a configuração inicial do dispositivo. Em vez disso, os usuários devem iniciar o registro. Para fazer isso, os usuários acessam um site da Samsung para baixar o novo cliente de Registro Móvel e iniciar o registro.

O cliente de registro baixado usa o mesmo perfil MDM e APKs configurados no portal de registro em massa do Knox para dispositivos Knox 2.4/2.4.1.

Os usuários geralmente seguem estas etapas:

1. Ligue o dispositivo e conecte-se ao Wi-Fi. Se o Registro Móvel não iniciar ou o Wi-Fi não estiver disponível, faça o seguinte:
    a. Vá para Samsung Knox Mobile Enrollment.
    b. Toque no botão **Avançar** para registrar dispositivos com dados móveis.
2. Quando o prompt **Registrar com Knox** aparecer, toque em **Continuar**.
3. Leia os EULAs (se disponíveis). Toque em **Avançar**.
4. Se solicitado, insira o **ID de Usuário** e a **Senha** fornecidos pelo administrador de TI.

Neste ponto, as credenciais do usuário são validadas e o dispositivo é registrado no ambiente de TI corporativo da sua organização.

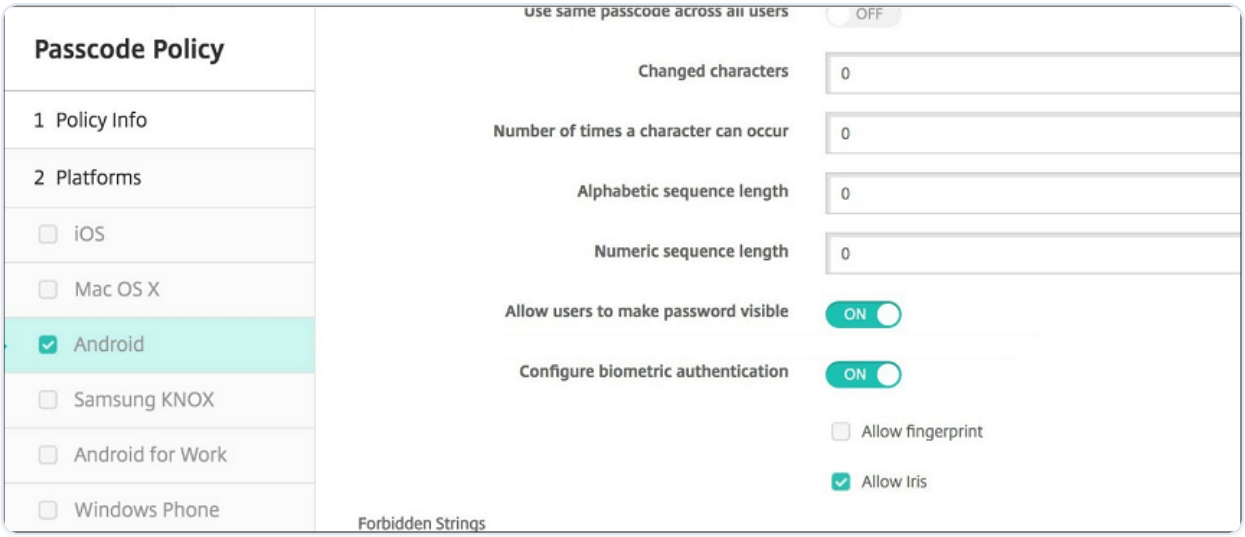
Ativar e desativar a autenticação biométrica para dispositivos Samsung

O XenMobile oferece suporte à autenticação por impressão digital e leitura de íris, também conhecida como autenticação biométrica. Você pode ativar e desativar a autenticação biométrica para dispositivos Samsung sem exigir nenhuma ação dos usuários. Se você desativar a autenticação biométrica no XenMobile, os usuários e aplicativos de terceiros não poderão ativar o recurso.

1. No console do XenMobile, clique em **Configurar** > **Políticas de Dispositivo**. A página **Políticas de Dispositivo** é exibida.
2. Clique em **Adicionar**. A página **Adicionar Nova Política** é exibida.
3. Clique em **Senha**. A página **Informações da Política de Senha** é exibida.
4. No painel **Informações da Política**, insira as seguintes informações:

- **Nome da Política:** Digite um nome descritivo para a política.
- **Descrição:** Opcionalmente, digite uma descrição da política.

5. Clique em **Avançar**. A página **Plataformas** é exibida.
6. Em **Plataformas**, selecione **Android** ou **Samsung Knox**.
7. Defina **Configurar autenticação biométrica** como **ATIVADO**.
8. Se você selecionou **Android**, em **Samsung SAFE**, selecione **Permitir impressão digital**, **Permitir íris** ou ambos.



Ações de segurança

Você realiza ações de segurança de dispositivo e aplicativo na página **Gerenciar** > **Dispositivos**. As ações de dispositivo incluem revogar, bloquear, desbloquear e limpar. As ações de segurança de aplicativo incluem bloqueio de aplicativo e limpeza de aplicativo.

- **Bypass de Bloqueio de Ativação:** Remove o Bloqueio de Ativação de dispositivos iOS supervisionados antes da ativação do dispositivo. Este comando não exige o ID Apple pessoal ou a senha de um usuário.
- **Bloqueio de aplicativo:** Nega o acesso a todos os aplicativos em um dispositivo. No Android, após um bloqueio de aplicativo, os usuários não podem fazer login no XenMobile. No iOS, os usuários podem fazer login, mas não podem acessar nenhum aplicativo.
- **Limpeza de aplicativo:** Remove a conta de usuário do Secure Hub e cancela o registro do dispositivo. Os usuários não podem se registrar novamente até que você execute a ação **Desfazer limpeza de aplicativo**.
- **Bloqueio de Ativação do Programa de Implantação ASM:** Cria um código de bypass de Bloqueio de Ativação para dispositivos iOS registrados no DEP do Apple School Manager.

- **Limpar restrições:** Em dispositivos iOS supervisionados, este comando permite que o XenMobile limpe a senha de restrições e as configurações de restrições configuradas pelo usuário.
- **Ativar/desativar Modo Perdido:** Coloca um dispositivo iOS supervisionado no Modo Perdido e envia ao dispositivo uma mensagem, número de telefone e nota de rodapé para exibir. A segunda vez que você envia este comando tira o dispositivo do Modo Perdido.
- **Ativar rastreamento:** Em dispositivos Android ou iOS, este comando permite que o XenMobile consulte a localização de dispositivos específicos em uma frequência que você definir. Para visualizar as coordenadas e a localização do dispositivo em um mapa, vá para **Gerenciar > Dispositivos**, selecione um dispositivo e clique em **Editar**. As informações do dispositivo estão na guia **Geral** em **Segurança**. Use **Ativar rastreamento** para rastrear o dispositivo continuamente. O Secure Hub relata a localização periodicamente quando o dispositivo está em execução.
- **Limpeza completa:** Apaga imediatamente todos os dados e aplicativos de um dispositivo, incluindo os de quaisquer cartões de memória.
    - Para dispositivos Android, esta solicitação também pode incluir a opção de limpar cartões de memória.
    - Para dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE), você pode fazer uma limpeza completa depois que uma limpeza seletiva remover o perfil de trabalho.
    - Para dispositivos iOS e macOS, a limpeza ocorre imediatamente, mesmo que o dispositivo esteja bloqueado.
        - Para dispositivos iOS 11 (versão mínima): Ao confirmar a limpeza completa, você pode optar por preservar o plano de dados celulares no dispositivo.
        - Para dispositivos iOS 11.3 (versão mínima): Ao confirmar a limpeza completa, você impede que dispositivos iOS façam a configuração por proximidade. Ao configurar um novo dispositivo iOS, os usuários normalmente podem usar um dispositivo iOS já configurado para configurar o seu próprio. Você pode bloquear a configuração por proximidade em dispositivos gerenciados pelo XenMobile Server e que foram limpos.
        - Para dispositivos iOS 17 (versão mínima): Ao confirmar a limpeza completa, o dispositivo apaga automaticamente todos os dados do usuário, conecta-se à rede Wi-Fi especificada e se reinscreve no servidor MDM usando o perfil de inscrição fornecido.
    - Se o usuário do dispositivo desligar o dispositivo antes que o conteúdo do cartão de memória seja excluído, o usuário ainda poderá ter acesso aos dados do dispositivo.

- Você pode cancelar a solicitação de limpeza até que a solicitação seja enviada ao dispositivo.

- **Localizar:** Localiza um dispositivo e relata a localização do dispositivo, incluindo um mapa, na página **Gerenciar > Dispositivos**, em **Detalhes do dispositivo > Geral**. Localizar é uma ação única. Use **Localizar** para exibir a localização atual do dispositivo no momento em que você executa a ação. Para rastrear continuamente o dispositivo por um período, use **Habilitar rastreamento**.
  - Ao aplicar esta ação a dispositivos Android (exceto Android Enterprise) ou a dispositivos Android Enterprise (de propriedade corporativa ou BYOD), esteja ciente do seguinte comportamento:
    - **Localizar** exige que o usuário conceda permissão de localização durante a inscrição. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante a inscrição, o XenMobile solicitará novamente a permissão de localização ao enviar o comando **Localizar**.
  - Ao aplicar este recurso a dispositivos iOS ou Android Enterprise, esteja ciente das seguintes limitações:
    - Para dispositivos Android Enterprise, esta solicitação falha, a menos que a política de dispositivo de localização tenha definido o modo de localização para o dispositivo como **Alta Precisão** ou **Economia de Bateria**.
    - Para dispositivos iOS, este comando só é bem-sucedido se os dispositivos estiverem no Modo Perdido do MDM.
- **Bloquear:** Bloqueia um dispositivo remotamente. Esta ação é útil quando você perde um dispositivo e não sabe se ele foi roubado. O XenMobile então gera um código PIN e o define no dispositivo. Para acessar o dispositivo, o usuário digita o código PIN. Use **Cancelar Bloqueio** para remover o bloqueio do console do XenMobile.
- **Bloquear e Redefinir Senha:** Bloqueia um dispositivo remotamente e redefine a senha.
  - Não suportado para dispositivos inscritos no Android Enterprise no modo de perfil de trabalho que estejam executando versões do Android anteriores ao Android 8.0.
  - Em dispositivos inscritos no Android Enterprise no modo de perfil de trabalho que estejam executando Android 8.0 ou superior:
    - A senha enviada bloqueia o perfil de trabalho. O dispositivo não é bloqueado.

    - Se nenhuma senha for enviada, ou a senha enviada não atender aos requisitos de senha, e nenhuma senha já estiver definida no perfil de trabalho: O dispositivo é bloqueado.
    - Se nenhuma senha for enviada, ou a senha enviada não atender aos requisitos de senha, mas uma senha já estiver definida no perfil de trabalho: O perfil de trabalho é bloqueado, mas o dispositivo não é bloqueado.

- **Notificar (Tocar):** Reproduz um som em dispositivos Android.
- **Reiniciar:** Reinicia dispositivos Windows 10 e Windows 11. Para tablets e PCs Windows, a mensagem "O sistema será reiniciado em breve" aparece e, em seguida, a reinicialização ocorre em cinco minutos.
- **Solicitar/Parar Espelhamento AirPlay:** Inicia e para o espelhamento AirPlay em dispositivos iOS supervisionados.
- **Reiniciar/Desligar:** Reinicia ou desliga imediatamente dispositivos iOS supervisionados.
- **Revogar:** Impede que um dispositivo se conecte a.
- **Revogar/Autorizar (iOS, macOS):** Executa as mesmas ações que uma Limpeza Seletiva. Após a revogação, você pode reautorizar o dispositivo para reenrolá-lo.
- **Tocar:** Se o dispositivo estiver no Modo Perdido, Tocar reproduz um som em um dispositivo iOS supervisionado. O som é reproduzido até que você remova o dispositivo do Modo Perdido ou o usuário desative o som.
- **Limpeza seletiva:** Apaga todos os dados e aplicativos corporativos de um dispositivo, deixando os dados e aplicativos pessoais no lugar. Após uma limpeza seletiva, um usuário pode reenrolar o dispositivo.

    - A limpeza seletiva de um dispositivo Android não desconecta o dispositivo do Device Manager e da rede corporativa. Para impedir que o dispositivo acesse o Device Manager, você também deve revogar os certificados do dispositivo.
    - A limpeza seletiva de um dispositivo Android também revoga o dispositivo. Você pode reenrolar o dispositivo somente após reautorizá-lo ou excluí-lo do console.
    - Para dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE), você pode realizar uma limpeza completa após uma limpeza seletiva remover o perfil de trabalho. Ou, você pode reenrolar o dispositivo com o mesmo nome de usuário. O reenrolamento do dispositivo recria o perfil de trabalho.
    - Se a API Samsung Knox estiver ativada, a limpeza seletiva do dispositivo também remove o contêiner Samsung Knox.

- Para dispositivos iOS e macOS, este comando remove qualquer perfil instalado via MDM.
- Uma limpeza seletiva em um dispositivo Windows também remove o conteúdo da pasta de perfil para qualquer usuário atualmente conectado. Uma limpeza seletiva não remove nenhum clipe da web que você entrega aos usuários por meio de uma configuração. Para remover clipes da web, os usuários devem desenrolar manualmente seus dispositivos. Você não pode reenrolar um dispositivo limpo seletivamente.

- **Desbloquear:** Limpa a senha enviada ao dispositivo quando ele foi bloqueado. Este comando não desbloqueia o dispositivo.

Em **Gerenciar > Dispositivos**, a página **Detalhes do dispositivo** também lista as propriedades de segurança do dispositivo. Essas propriedades incluem ID Forte, Bloquear Dispositivo, Ignorar Bloqueio de Ativação e outras informações para o tipo de plataforma. O campo **Limpeza Completa do Dispositivo** inclui o código PIN do usuário. O usuário deve inserir esse código depois que o dispositivo for limpo. Se o usuário esquecer o código, você pode consultá-lo aqui.

Ações de segurança para dispositivos Android

AÇÃO DE SEGURANÇA	ANDROID (EXCETO PARA DISPOSITIVOS ANDROID ENTERPRISE)	ANDROID ENTERPRISE (BYOD)	ANDROID ENTERPRISE (DE PROPRIEDADE DA EMPRESA)
Bloqueio de app	Sim	Não	Não
Limpeza de app	Sim	Não	Não
Limpeza Completa	Sim	Não	Sim
Localizar	Sim: Para dispositivos com Android 6.0 ou superior, Localizar exige que o usuário conceda permissão de Localização durante o registro. O usuário pode optar por não conceder a permissão de Localização. Se o	Sim: Para dispositivos com Android 6.0 ou superior, Localizar exige que o usuário conceda permissão de Localização durante o registro. O usuário pode optar por não conceder a permissão de Localização. Se o	Sim: Para dispositivos com Android 6.0 ou superior, Localizar exige que o usuário conceda permissão de Localização durante o registro. O usuário pode optar por não conceder a permissão de Localização. Se o

AÇÃO DE SEGURANÇA	ANDROID (EXCETO PARA DISPOSITIVOS ANDROID ENTERPRISE)	ANDROID ENTERPRISE (BYOD)	ANDROID ENTERPRISE (DE PROPRIEDADE DA EMPRESA)
	usuário não conceder a permissão durante o registro, o XenMobile solicitará novamente a permissão de localização ao enviar o comando Localizar.	usuário não conceder a permissão durante o registro, o XenMobile solicitará novamente a permissão de localização ao enviar o comando Localizar.	usuário não conceder a permissão durante o registro, o XenMobile solicitará novamente a permissão de localização ao enviar o comando Localizar.
Bloquear	Sim	Sim	Sim
Bloquear e Redefinir Senha	Sim	Não	Sim
Notificar (Tocar)	Sim	Sim	Sim
Revogar	Sim	Sim	Sim
Limpeza Seletiva	Sim	Sim	Não

Ações de segurança para dispositivos iOS e macOS

AÇÃO DE SEGURANÇA	IOS	MACOS
Bypass de Bloqueio de Ativação	Sim	Não
Bloquear App	Sim	Não
Apagar App	Sim	Não
Bloqueio de Ativação do Programa de Implantação ASM	Sim	Não
Limpar Restrições	Sim	Não

AÇÃO DE SEGURANÇA	IOS	MACOS
Ativar/Desativar Modo Perdido	Sim	Não
Ativar/Desativar Rastreamento	Sim	Não
Limpeza Completa	Sim	Sim
Localizar	Sim	Não
Bloquear	Sim	Sim
Tocar	Sim	Sim
Solicitar/Parar Espelhamento AirPlay	Sim	Não
Reiniciar/Desligar	Sim	Não
Revogar/Autorizar	Sim	Sim
Limpeza Seletiva	Sim	Sim
Desbloquear	Sim	Não

Ações de segurança para dispositivos Windows

AÇÃO DE SEGURANÇA	TABLET WINDOWS 10
Localizar	Sim
Bloquear	Sim
Bloquear e Redefinir Senha	Não
Reiniciar	Sim
Revogar	Sim
Tocar	Não

AÇÃO DE SEGURANÇA	TABLET WINDOWS 10
Limpeza Seletiva	Sim
Limpar	Sim

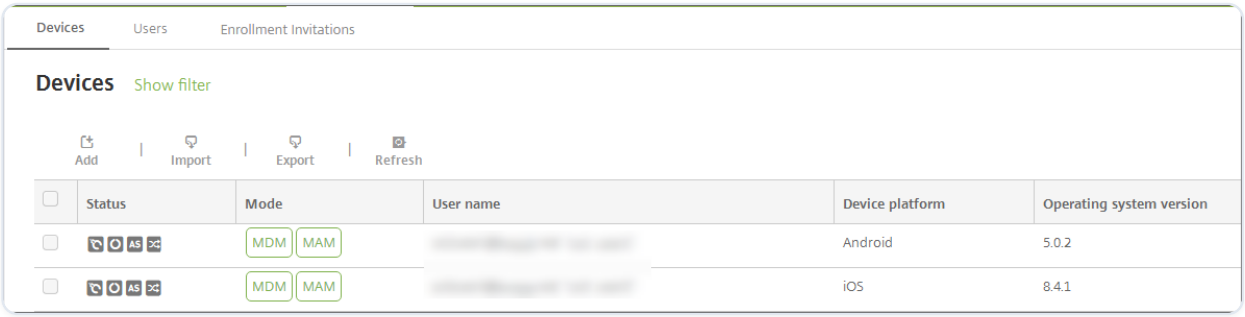
O restante deste artigo fornece os passos para realizar várias ações de segurança. Você também pode automatizar algumas ações. Para mais informações, consulte Ações automatizadas.

Bloquear dispositivos iOS

Você pode bloquear um dispositivo iOS perdido com a exibição de uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo. Este recurso é compatível com dispositivos que executam iOS 7 e superior.

Para exibir uma mensagem e um número de telefone em um dispositivo bloqueado, defina a política Código de acesso como **true** no console do XenMobile. Alternativamente, os usuários podem ativar o código de acesso no dispositivo manualmente.

1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



2. Selecione o dispositivo iOS que você deseja bloquear.

   Quando você seleciona a caixa de seleção ao lado de um dispositivo, o menu de opções é exibido acima da lista de dispositivos. Quando você clica em qualquer outro lugar na lista, o menu de opções aparece no lado direito da listagem.

   Imagem do menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

   Imagem do menu de opções(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. No menu de opções, clique em **Proteger**. A caixa de diálogo **Ações de Segurança** é exibida.

Imagem da caixa de diálogo Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de Segurança** é exibida.

   Imagem da confirmação de Ações de Segurança(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. Opcionalmente, digite uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo.

   Para iPads com iOS 7 e posterior: o iOS anexa as palavras “iPad Perdido” ao que você digita no campo **Mensagem**.

   Para iPhones com iOS 7 e posterior: se você deixar o campo **Mensagem** vazio e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

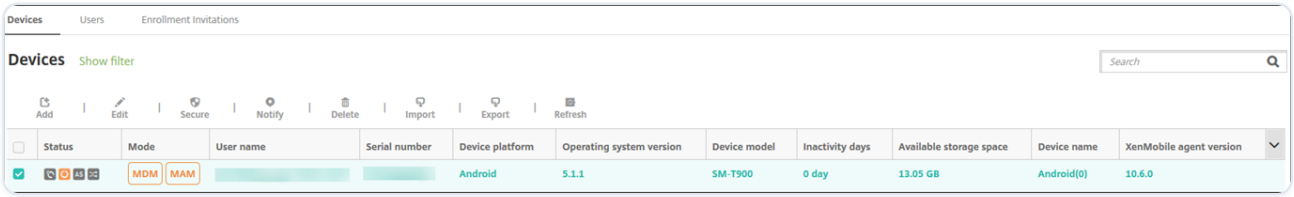
6. Clique em **Bloquear Dispositivo**.

Remover um dispositivo do console XenMobile

> **Importante:**

> Quando você remove um dispositivo do console XenMobile, os aplicativos e dados gerenciados permanecem no dispositivo. Para remover aplicativos e dados gerenciados do dispositivo, consulte "Excluir um dispositivo" mais adiante neste artigo.

> Para remover um dispositivo do console XenMobile, vá para **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Excluir**.



Limpar seletivamente um dispositivo

1. Vá para **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Proteger**.
2. Em **Ações de Segurança**, clique em **Limpeza seletiva**.

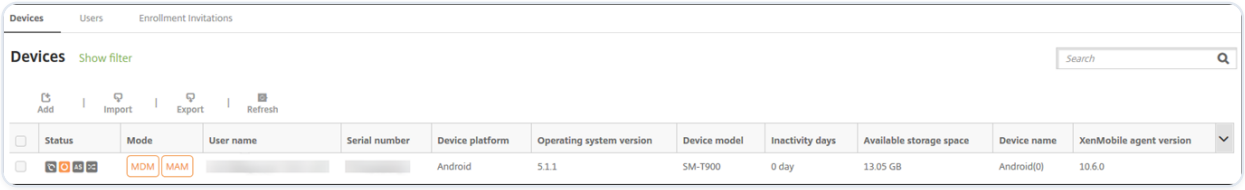
3. Apenas para dispositivos Android, desconecte o dispositivo da rede corporativa: Após a limpeza do dispositivo, em **Ações de Segurança**, clique em **Revogar**.

   Para retirar uma solicitação de limpeza seletiva antes que a limpeza ocorra, em **Ações de Segurança**, clique em **Cancelar limpeza seletiva**.

Excluir um dispositivo

Este procedimento remove aplicativos e dados gerenciados do dispositivo e exclui o dispositivo da lista de Dispositivos no console XenMobile. Você pode usar a API REST Pública do Endpoint Management para excluir dispositivos em massa.

1. Vá para **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Proteger**.
2. Clique em **Limpeza Seletiva**. Quando solicitado, clique em **Executar Limpeza Seletiva**.
3. Para verificar se o comando de limpeza foi bem-sucedido, atualize **Gerenciar > Dispositivos**. Na coluna **Modo**, a cor âmbar para MDM e MAM indica que o comando de limpeza foi bem-sucedido.



4. Em **Gerenciar > Dispositivos**, selecione o dispositivo e clique em **Excluir**. Quando solicitado, clique em **Excluir** novamente.

Bloquear, desbloquear, limpar ou desfazer limpeza de aplicativos

1. Vá para **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Proteger**.
2. Em **Ações de Segurança**, clique na ação do aplicativo.

   Você também pode usar a caixa **Ações de Segurança** para verificar o status do dispositivo de um usuário cuja conta está desativada ou foi excluída do Active Directory. A presença das ações Desbloquear Aplicativo ou Deslimpar Aplicativo indica aplicativos que estão bloqueados ou limpos.

Limpeza e deslimpeza de aplicativos

1. Vá para **Gerenciar > Dispositivos**. Selecione um dispositivo.

2. Limpeza de app

    - Clique em **Proteger > Limpeza de Aplicativo**. Uma caixa de diálogo com a seguinte mensagem aparece: **Tem certeza de que deseja limpar os aplicativos deste dispositivo?** Clique em **Limpeza de Aplicativo**.

3. Deslimpeza de aplicativo

    - Clique em **Proteger > Deslimpeza de Aplicativo**. Uma caixa de diálogo com a seguinte mensagem aparece: **Tem certeza de que deseja deslimpar os aplicativos deste dispositivo?** Clique em **Deslimpeza de Aplicativo do Dispositivo**.

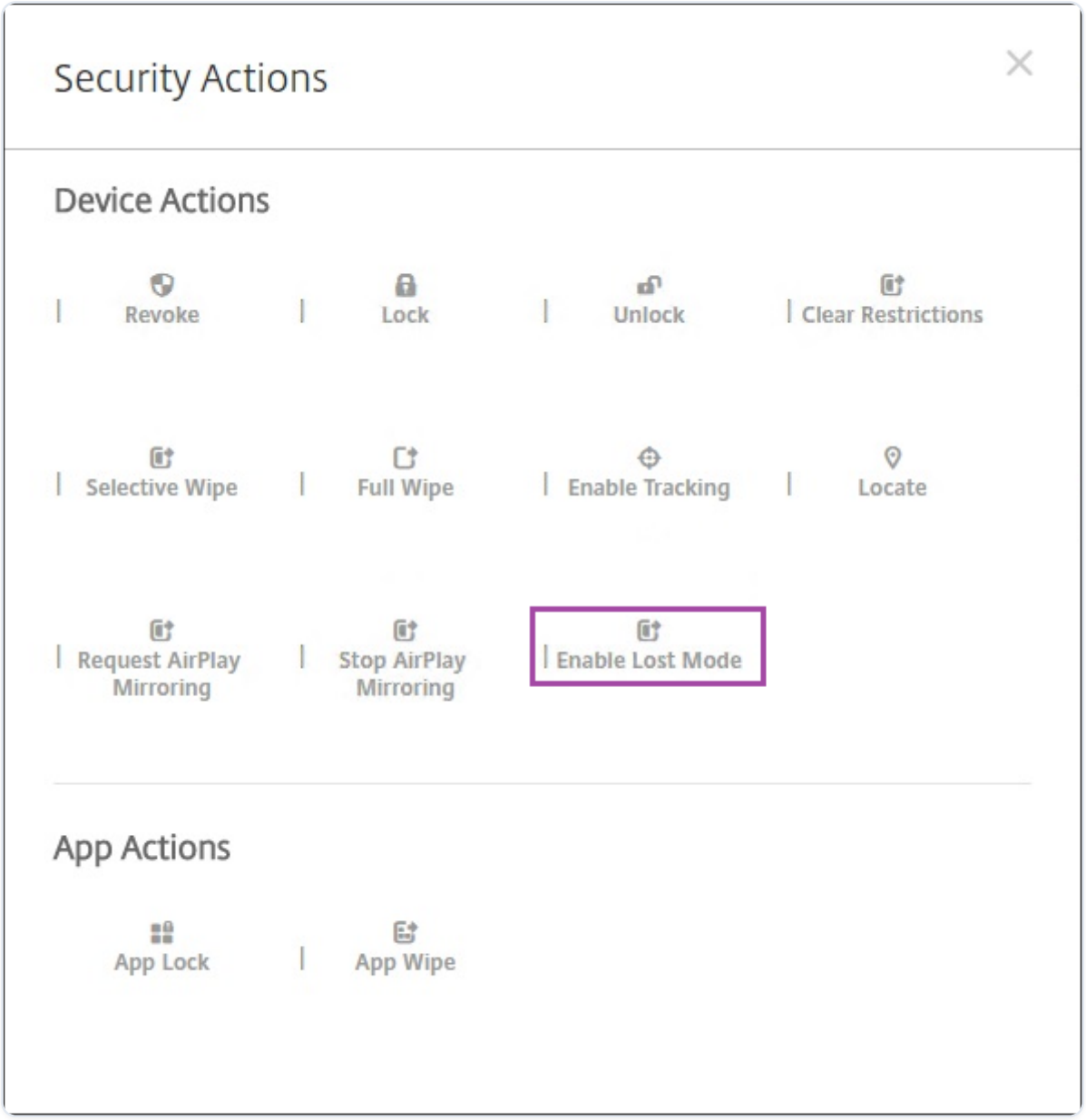
4. Abra o Secure Hub no dispositivo e clique em **Loja**.
5. Inicie o Secure Hub.

Colocar dispositivos iOS no Modo Perdido

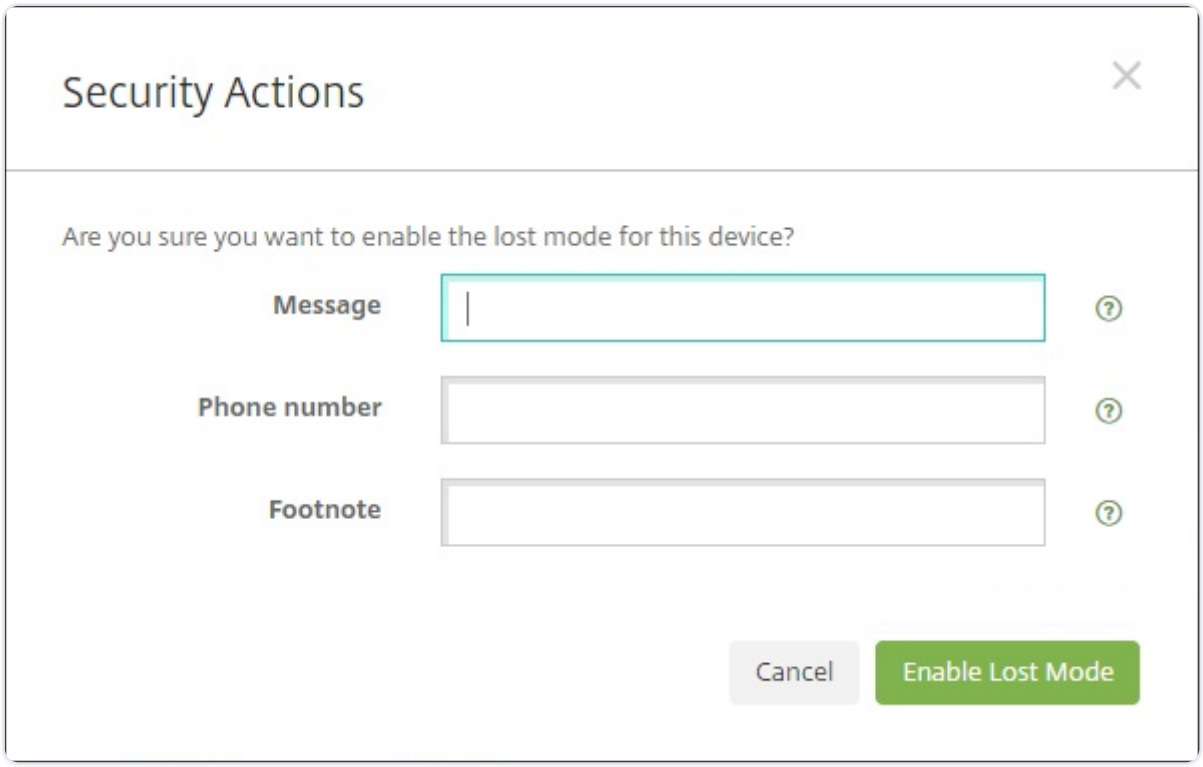
A propriedade de dispositivo Modo Perdido do XenMobile coloca um dispositivo iOS no Modo Perdido. Ao contrário do Modo Perdido Gerenciado da Apple, o Modo Perdido do XenMobile não exige que um usuário execute nenhuma das seguintes ações para permitir a localização de seu dispositivo: Configurar a definição **Buscar Meu iPhone/iPad** ou ativar os Serviços de Localização para o Citrix Secure Hub.

No Modo Perdido do XenMobile, apenas o pode desbloquear o dispositivo. (Em contraste, se você usar o recurso de bloqueio de dispositivo do XenMobile, os usuários podem desbloquear o dispositivo diretamente usando um código PIN que você fornece.

Para ativar ou desativar o modo perdido: Vá para **Gerenciar > Dispositivos**, escolha um dispositivo iOS supervisionado e clique em **Proteger**. Em seguida, clique em **Ativar Modo Perdido** ou **Desativar Modo Perdido**.

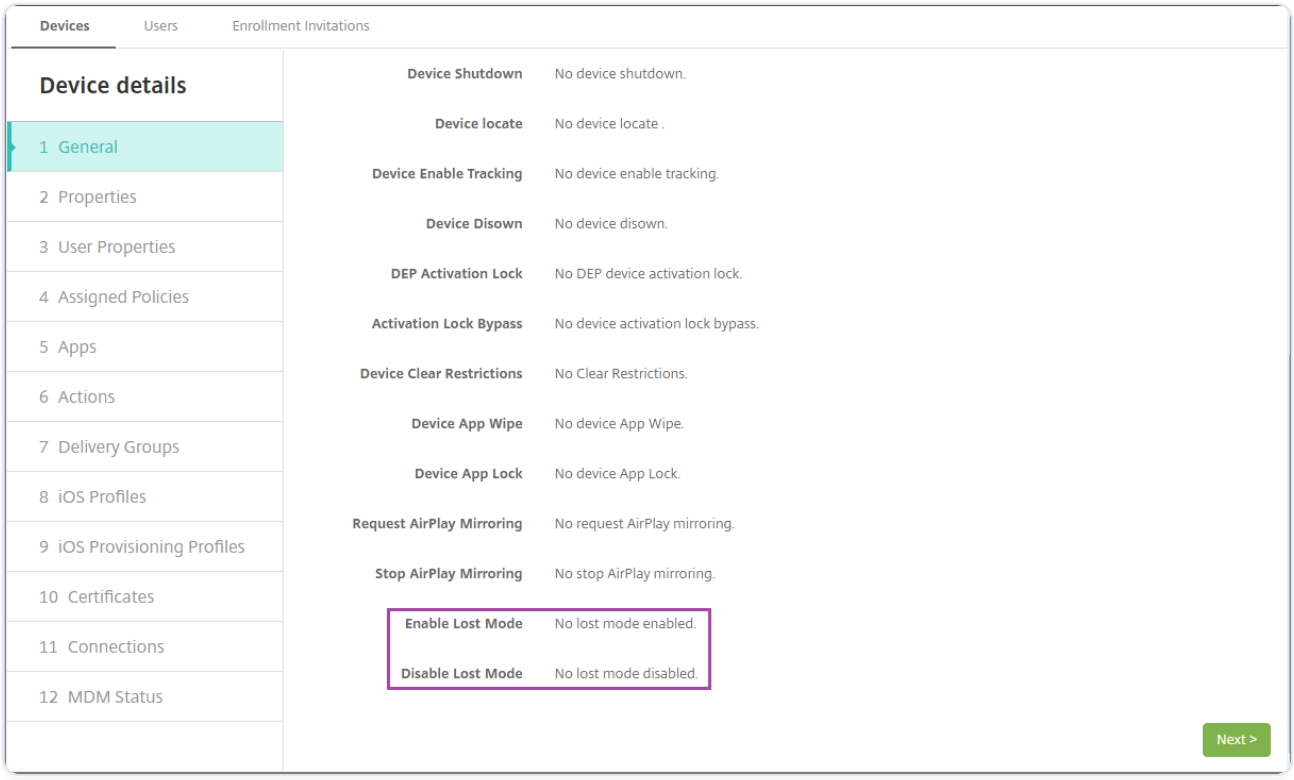


Se você clicar em **Ativar Modo Perdido**, digite as informações que aparecerão no dispositivo quando ele estiver no modo perdido.

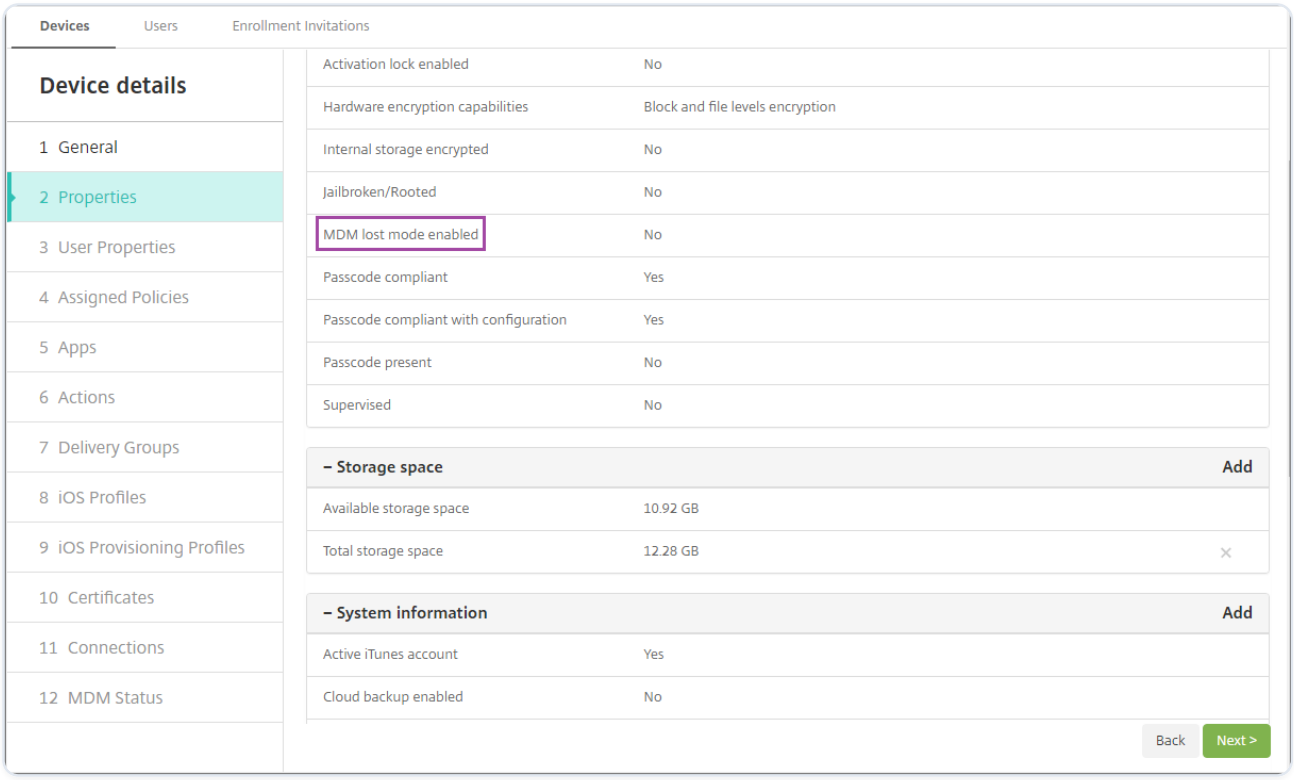


Use qualquer um dos seguintes métodos para verificar o status do Modo Perdido:

- Na janela **Ações de Segurança**, verifique se o botão é **Desativar Modo Perdido**.
- Em **Gerenciar > Dispositivos**, na guia **Geral** em **Segurança**, veja a última ação Ativar Modo Perdido ou Desativar Modo Perdido.



- Em **Gerenciar > Dispositivos**, na guia **Propriedades**, verifique se o valor da configuração **MDM lost mode enabled** está correto.



Se você ativar o Modo Perdido do XenMobile em um dispositivo iOS, o console do XenMobile também mudará da seguinte forma:

- Em **Configurar > Ações**, a lista **Ações** não inclui estas ações automatizadas: **Revogar o dispositivo**, **Limpar seletivamente o dispositivo** e **Limpar completamente o dispositivo**.
- Em **Gerenciar > Dispositivos**, a lista **Ações de Segurança** não inclui mais as ações de dispositivo **Revogar** e **Limpeza Seletiva**. Você ainda pode usar uma ação de segurança para realizar uma ação de **Limpeza Completa**, conforme necessário.

Para iPads com iOS 7 e posterior: o iOS anexa as palavras "iPad Perdido" ao que você digita na **Mensagem** na tela **Ações de Segurança**.

Para iPhones com iOS 7 e posterior: Se você deixar a **Mensagem** vazia e fornecer um número de telefone, a Apple exibirá a mensagem "Ligar para o proprietário" na tela de bloqueio do dispositivo.

Ignorar um bloqueio de ativação do iOS

O Bloqueio de Ativação é um recurso do Find My iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação exige o ID Apple e a senha do usuário antes que alguém possa desativar o Find My iPhone/iPad, apagar o dispositivo ou reativá-lo. Para os dispositivos que sua organização possui, ignorar um Bloqueio de Ativação é necessário para, por exemplo, redefinir ou realocar dispositivos.

Para habilitar o Bloqueio de Ativação, você configura e implanta a política de dispositivo Opções de MDM do XenMobile. Você pode então gerenciar um dispositivo a partir do console do XenMobile sem as credenciais da Apple do usuário. Para ignorar a exigência de credenciais da Apple de um Bloqueio de Ativação, emita a ação de segurança Ignorar Bloqueio de Ativação a partir do console do XenMobile.

Por exemplo, se o usuário devolver um telefone perdido ou para configurar o dispositivo antes ou depois de uma Limpeza Completa: Quando o telefone solicitar a credencial da conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação a partir do console do XenMobile.

Requisitos do dispositivo para ignorar o bloqueio de ativação

- iOS 7.1 (versão mínima)
- Supervisionado via Apple Configurator ou Apple DEP
- Configurado com uma conta do iCloud
- Find My iPhone/iPad habilitado
- Registrado no XenMobile
- A política de dispositivo Opções de MDM, com bloqueio de ativação habilitado, é implantada nos dispositivos

Para ignorar um bloqueio de ativação antes de emitir uma Limpeza Completa de um dispositivo:

1. Vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Proteger** e, em seguida, clique em **Ignorar Bloqueio de Ativação**.
2. Apague o dispositivo. A tela de bloqueio de ativação não aparece durante a configuração do dispositivo.

Para ignorar um bloqueio de ativação depois de emitir uma Limpeza Completa de um dispositivo:

1. Redefina ou apague o dispositivo. A tela de bloqueio de ativação aparece durante a configuração do dispositivo.
2. Vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Proteger** e, em seguida, clique em **Ignorar Bloqueio de Ativação**.
3. Toque no botão Voltar no dispositivo. A tela inicial é exibida.

Tenha em mente o seguinte:

- Aconselhe seus usuários a não desativar o Buscar Meu iPhone/iPad. Não faça uma limpeza completa a partir do dispositivo. Em qualquer um desses casos, o usuário é solicitado a inserir a senha da conta do iCloud. Após a validação da conta, o usuário não verá uma tela Ativar iPhone/iPad após apagar todo o conteúdo e configurações.
- Para um dispositivo com um código de ignorar Bloqueio de Ativação gerado e com o Bloqueio de Ativação ativado: Se você não conseguir ignorar a página Ativar iPhone/iPad após uma Limpeza Completa, não há necessidade de excluir o dispositivo do XenMobile. Você ou o usuário podem entrar em contato com o suporte da Apple para desbloquear o dispositivo diretamente.
- Durante um inventário de hardware, o XenMobile consulta um dispositivo para obter um código de ignorar Bloqueio de Ativação. Se um código de ignorar estiver disponível, o dispositivo o envia para o XenMobile. Em seguida, para remover o código de ignorar do dispositivo, envie a ação de segurança Ignorar Bloqueio de Ativação do console do XenMobile. Nesse ponto, e a Apple têm o código de ignorar necessário para desbloquear o dispositivo.
- A ação de segurança Ignorar Bloqueio de Ativação depende da disponibilidade de um serviço da Apple. Se a ação não funcionar, você pode desbloquear um dispositivo da seguinte forma. No dispositivo, insira manualmente as credenciais da conta do iCloud. Ou, deixe o campo de nome de usuário vazio e digite o código de ignorar no campo de senha. Para procurar o código de ignorar, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Propriedades**. O **código de ignorar Bloqueio de Ativação** está em **Informações de segurança**.

Serviço AutoDiscovery do XenMobile®

O serviço AutoDiscovery simplifica o processo de registro para usuários por meio da descoberta de URL baseada em e-mail. O serviço AutoDiscovery também oferece recursos como verificação de registro, fixação de certificado (certificate pinning) e outros benefícios para clientes do Citrix Workspace™. O serviço, hospedado no Citrix Cloud™, é uma parte importante de muitas implantações do XenMobile.

Com o serviço AutoDiscovery, os usuários:

- Podem usar suas credenciais de rede corporativa para registrar seus dispositivos.
- Não precisam inserir detalhes sobre o endereço do XenMobile Server.
- Inserem seu nome de usuário no formato de nome principal de usuário (UPN). Por exemplo, `user@mycompany.com`.

Recomendamos que você use o serviço AutoDiscovery para ambientes de alta segurança. O serviço AutoDiscovery oferece suporte à fixação de certificado de chave pública (public key certificate pinning), que impede ataques man-in-the-middle. A fixação de certificado garante que o certificado assinado pela sua empresa seja usado quando os clientes Citrix se comunicam com o XenMobile. Para configurar a fixação de certificado para seus sites XenMobile, entre em contato com o Suporte Citrix. Para obter informações sobre fixação de certificado, consulte Fixação de certificado.

Para acessar o serviço AutoDiscovery, navegar para `<https://adsui.cloud.com>` (comercial) ou `<https://adsui.cem.cloud.us>` (governamental).

Pré-requisitos

- O novo serviço AutoDiscovery no Citrix Cloud requer a versão mais recente do Secure Hub:
  - Para iOS, Secure Hub versão 21.6.0 ou posterior
  - Para Android, Secure Hub versão 21.8.5 ou posterior

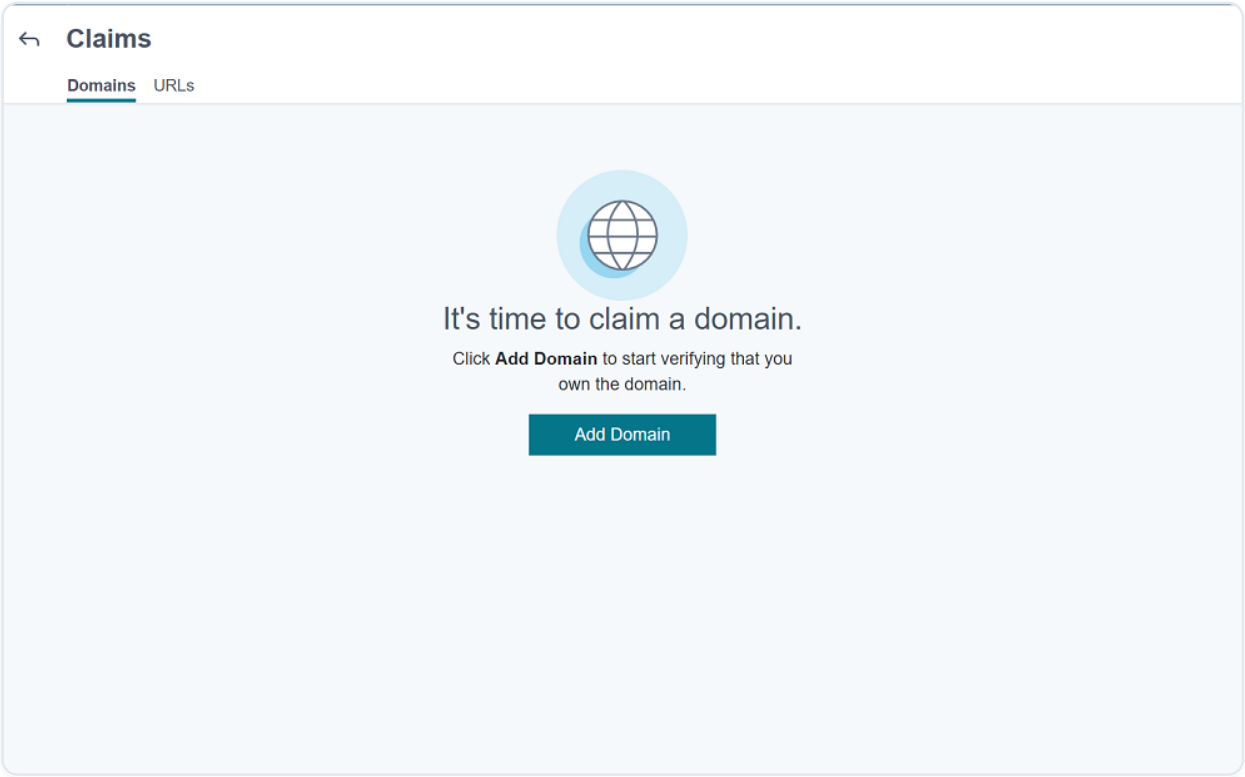
  Dispositivos executando versões anteriores do Secure Hub podem sofrer interrupções no serviço.
- Para acessar o novo serviço AutoDiscovery, você deve ter uma conta de administrador do Citrix Cloud com acesso total. O serviço AutoDiscovery não oferece suporte a contas de administrador com acesso personalizado. Se você não tiver uma conta, consulte Inscrever-se no Citrix Cloud.

  A Citrix migrou todos os registros AutoDiscovery existentes para o Citrix Cloud sem interrupção no serviço. Os registros migrados não aparecem automaticamente no novo console. Você deve reivindicar domínios no novo serviço AutoDiscovery para comprovar a propriedade. Para obter mais informações, consulte CTX312339.
- Antes de começar a usar o serviço AutoDiscovery para suas implantações do Endpoint Management, verifique e reivindique seu domínio. Você pode reivindicar até 10 domínios. A reivindicação associa o domínio verificado ao serviço AutoDiscovery. Para reivindicar mais de 10 domínios, abra um tíquete SRE ou entre em contato com o Suporte Técnico da Citrix.
- Use a configuração de Porta MAM em vez do FQDN do Citrix Gateway para direcionar o tráfego MAM para seu data center. Se você inserir um nome de domínio totalmente qualificado junto com a porta do seu Citrix Gateway, o dispositivo cliente usará a configuração da opção **Porta MAM**.

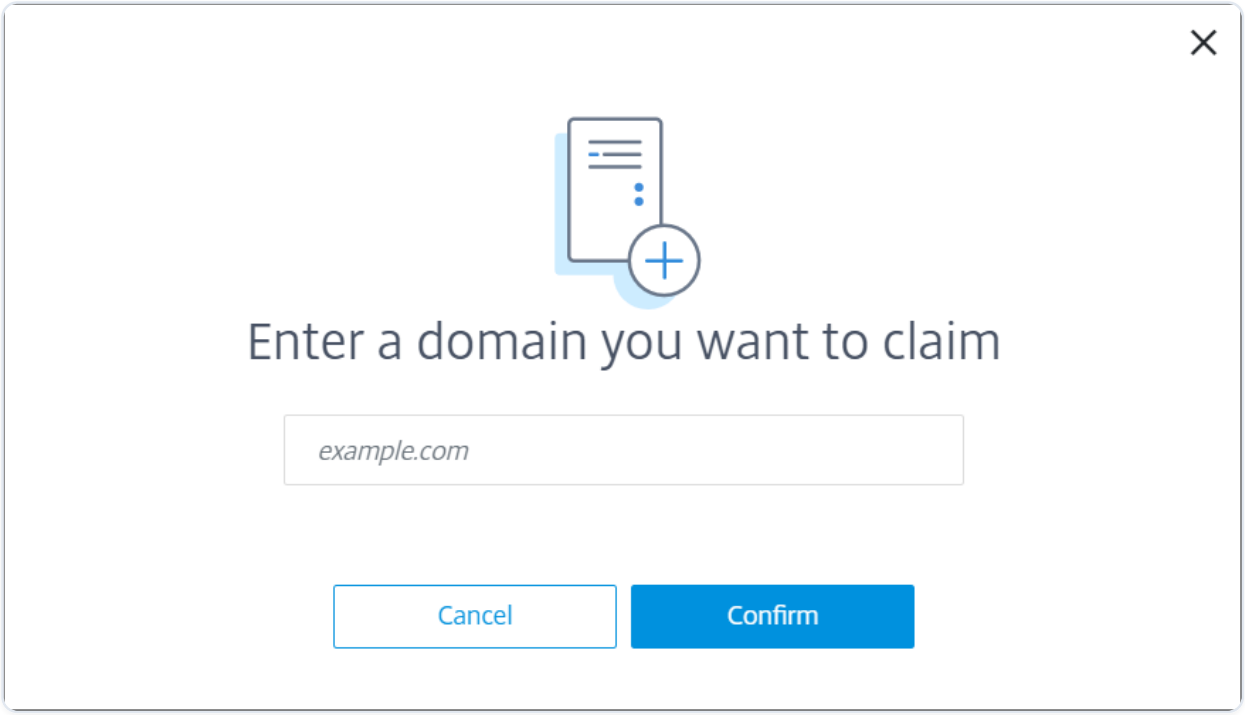
- Se um bloqueador de anúncios impedir a abertura do site, certifique-se de desativar o bloqueador de anúncios para todo o site.

Reivindicar um domínio

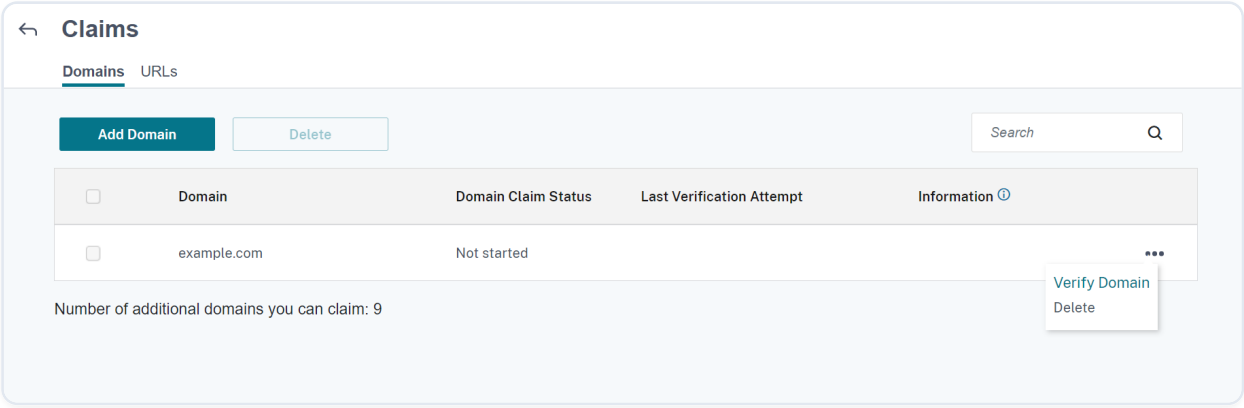
1. Na guia **Reivindicações > Domínios**, clique em **Adicionar Domínio**.



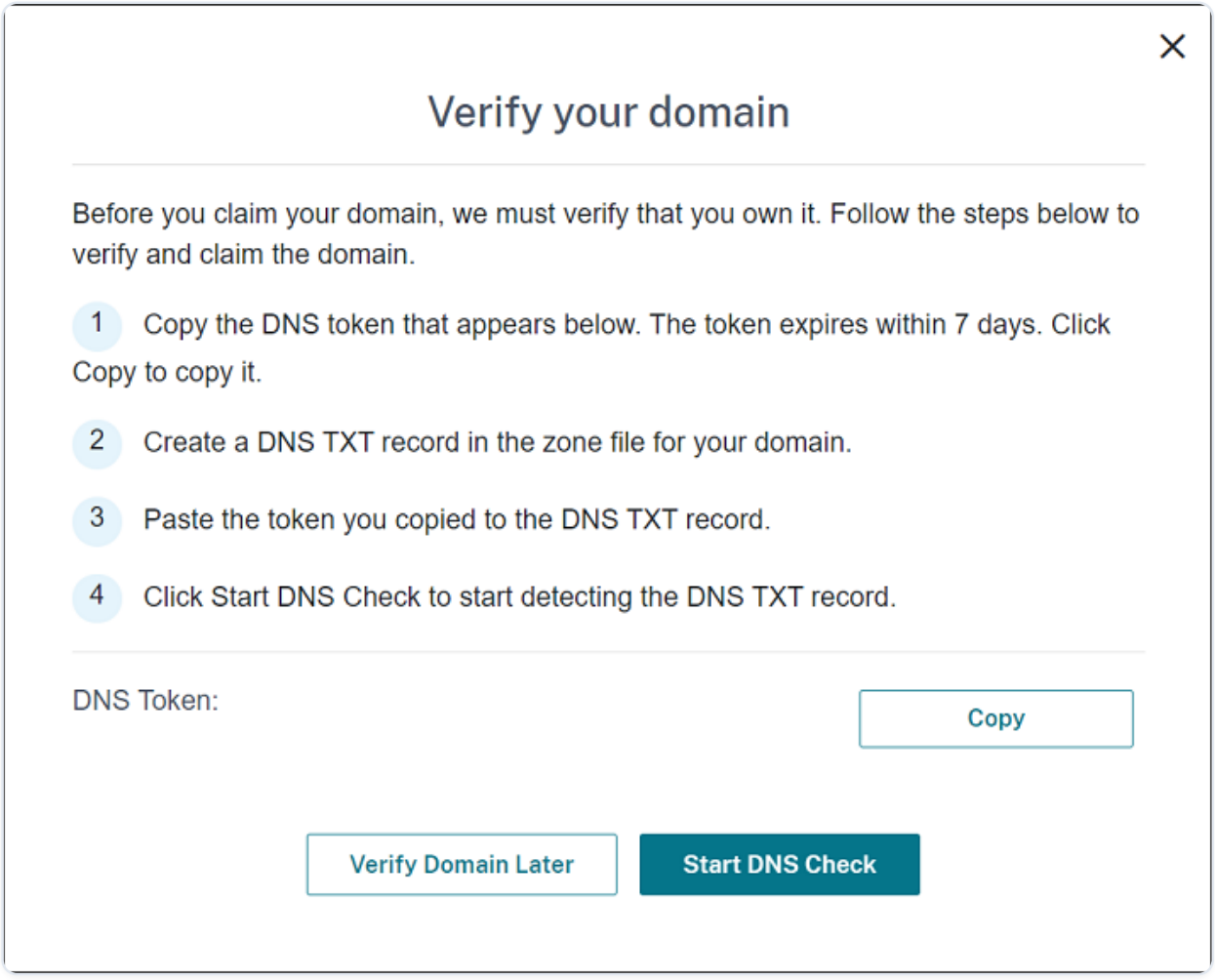
2. Na caixa de diálogo que aparece, insira o nome de domínio do seu ambiente XenMobile e clique em **Confirmar**. Seu domínio aparece em **Reivindicações > Domínios**.



3. No domínio que você adicionou, clique no menu de reticências e selecione **Verificar Domínio** para iniciar o processo de verificação. A página **Verificar seu domínio** é exibida.



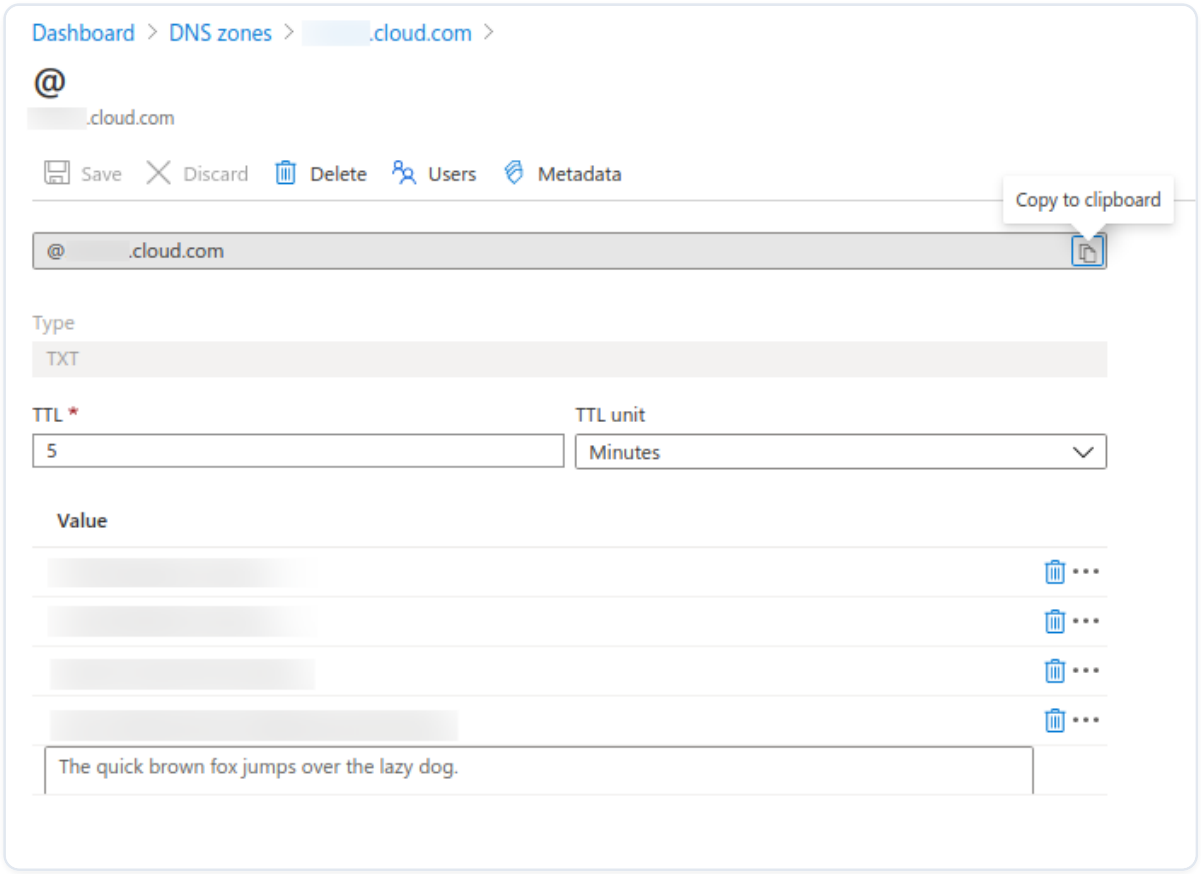
4. Na página **Verificar seu domínio**, siga as instruções para verificar se você é o proprietário do domínio.



   a. Clique em **Copiar** para copiar o token DNS para a área de transferência.

   b. Crie um registro DNS TXT no arquivo de zona do seu domínio. Para fazer isso, acesse o portal do seu provedor de hospedagem de domínio e adicione o token DNS que você copiou.

A captura de tela a seguir mostra um portal de provedor de hospedagem de domínio. Seu portal pode parecer diferente.



c. No Citrix Cloud, na página **Verificar seu domínio**, clique em **Iniciar Verificação de DNS** para começar a detectar seu registro DNS TXT. Se você quiser verificar o domínio mais tarde, clique em **Verificar Domínio Mais Tarde**.

O processo de verificação geralmente leva cerca de uma hora. No entanto, pode levar até dois dias para retornar uma resposta. Não há problema em sair e fazer login novamente durante a verificação de status.

Após a conclusão da configuração, o status do seu domínio muda de **Pendente** para **Verificado**.

5. Depois de reivindicar seu domínio, forneça informações sobre o serviço AutoDiscovery. Clique no menu de reticências no domínio que você adicionou e, em seguida, clique em **Adicionar Informações de Gerenciamento de Endpoint**. A página **Informações do Serviço AutoDiscovery** é exibida.
6. Insira as seguintes informações e, em seguida, clique em **Salvar**.

- **FQDN do Servidor de Gerenciamento de Endpoint:** Insira o nome de domínio totalmente qualificado do XenMobile Server. Por exemplo: `example.xm.cloud.com`. Essa configuração é usada para tráfego de controle MDM e MAM.
- **FQDN do Citrix Gateway:** Insira o nome de domínio totalmente qualificado do Citrix Gateway, no formato FQDN ou FQDN:porta. Por exemplo: `example.com`. Essa configuração é usada para direcionar o tráfego MAM para o seu data center. Para implantações somente MDM, deixe este campo em branco.

  > **Observação:**
  >
  > A Citrix recomenda que você use a configuração **Porta MAM** em vez de **FQDN do Citrix Gateway** para controlar o tráfego MAM. Se você inserir um nome de domínio totalmente qualificado junto com a porta do seu Citrix Gateway, o dispositivo cliente usará a configuração da **Porta MAM**.

- **Nome da Instância:** Insira o nome da instância do XenMobile Server que você configurou anteriormente. Se você não tiver certeza sobre o nome da sua instância, deixe o valor padrão **zdm**.
- **Porta MDM:** Insira a porta usada para tráfego de controle MDM e registro MDM. Para serviços baseados em nuvem, o padrão é 443.
- **Porta MAM:** Insira a porta usada para tráfego de controle MAM, registro MAM, registro iOS e enumeração de aplicativos. Para serviços baseados em nuvem, o padrão é 8443.

Solicitar AutoDiscovery para dispositivos Windows

Se você planeja registrar dispositivos Windows, faça o seguinte:

1. Entre em contato com o Suporte Citrix e crie uma solicitação de suporte para habilitar o AutoDiscovery do Windows.
2. Obtenha um certificado SSL assinado publicamente e não curinga para `enterpriseenrollment.mycompany.com`. A parte `mycompany.com` é o domínio que possui as contas que os usuários usam para se registrar. Anexe o certificado SSL no formato .pfx e sua senha à solicitação de suporte criada na etapa anterior.

   Para usar mais de um domínio para registrar dispositivos Windows, você também pode usar um certificado multidomínio com a seguinte estrutura:

- Um SubjectDN com um CN que especifica o domínio principal que ele atende (por exemplo, enterpriseenrollment.mycompany1.com).
- Os SANs apropriados para os domínios restantes (por exemplo, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com e assim por diante).

3. Crie um registro de nome canônico (CNAME) em seu DNS e mapeie o endereço do seu certificado SSL (enterpriseenrollment.mycompany.com) para autodisc.xm.cloud.com.

   Quando um usuário de dispositivo Windows se registra usando um UPN, o servidor de registro Citrix:

   - Fornece os detalhes do seu XenMobile Server.
   - Instrui o dispositivo a solicitar um certificado válido do XenMobile.

Neste ponto, você pode registrar todos os dispositivos suportados. Vá para a próxima seção para se preparar para entregar recursos aos dispositivos.

Políticas de dispositivo

Você pode configurar como o XenMobile® interage com seus dispositivos criando políticas. Embora muitas políticas sejam comuns a todos os dispositivos, cada dispositivo possui um conjunto de políticas específicas para seu sistema operacional. Como resultado, você pode encontrar diferenças entre plataformas e até mesmo entre diferentes fabricantes de dispositivos Android.

Para uma descrição resumida de cada política de dispositivo, consulte Resumos de políticas de dispositivo neste artigo.

> **Nota:**

> Se seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):

> Ao configurar políticas de dispositivo XenMobile para dispositivos Windows 10 e Windows 11, tenha em mente as seguintes regras. Se uma política em um ou mais dispositivos registrados entrar em conflito, a política alinhada com o GPO terá precedência.

> Para ver quais políticas o contêiner do Android Enterprise oferece suporte, consulte Android Enterprise.

Pré-requisitos

- Crie quaisquer grupos de entrega que você planeja usar.
- Instale quaisquer certificados de CA necessários.

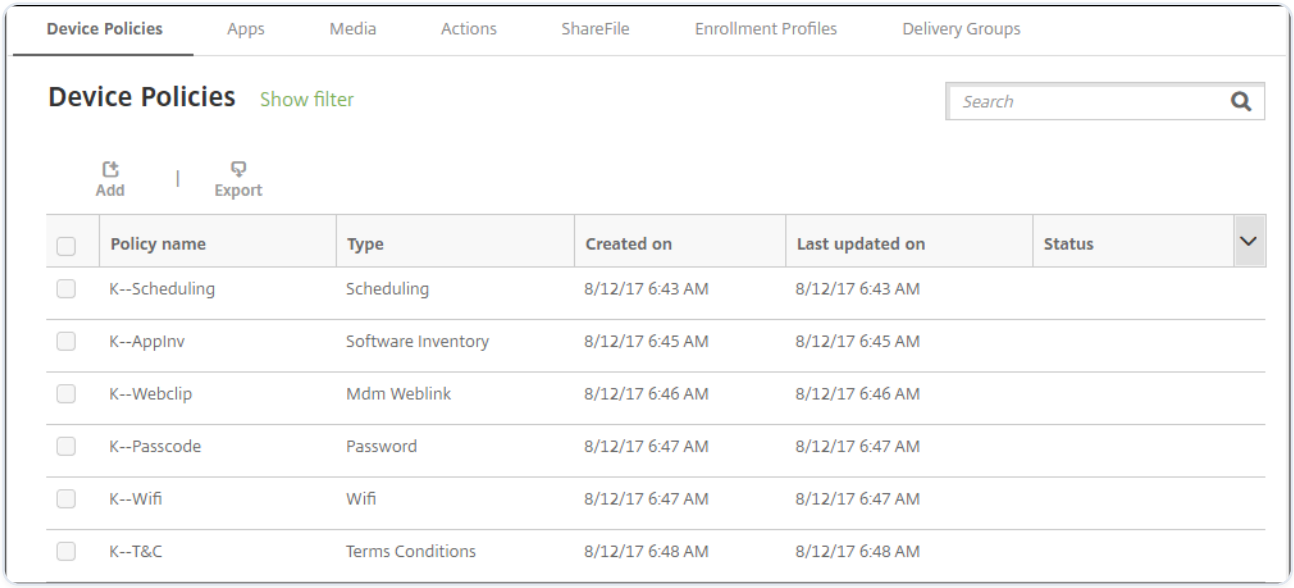
Adicionar uma política de dispositivo

As etapas básicas para criar uma política de dispositivo são as seguintes:

1. Nomeie e descreva a política.
2. Configure a política para uma ou mais plataformas.

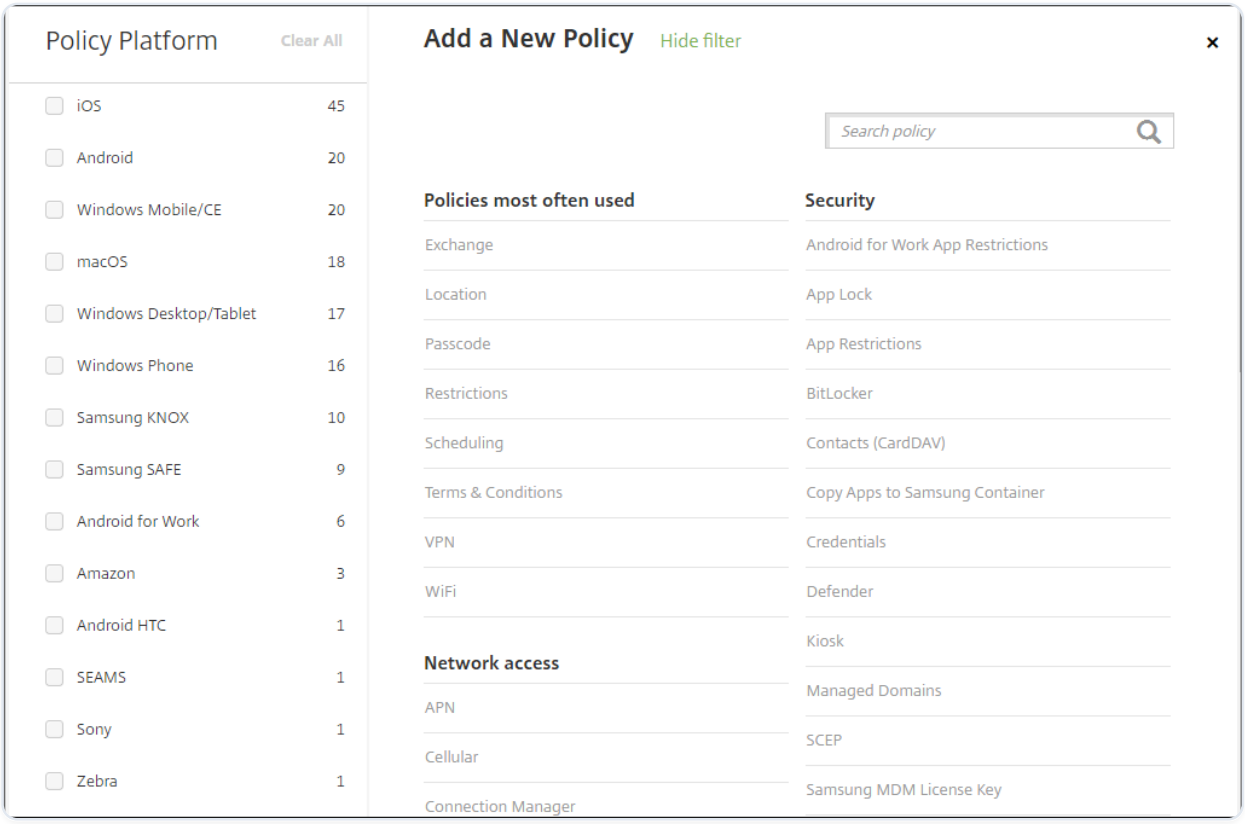
3. Crie regras de implantação (opcional).
4. Atribua a política a grupos de entrega.
5. Configure o agendamento de implantação (opcional).

Para criar e gerenciar políticas de dispositivo, vá para **Configurar > Políticas de Dispositivo**.

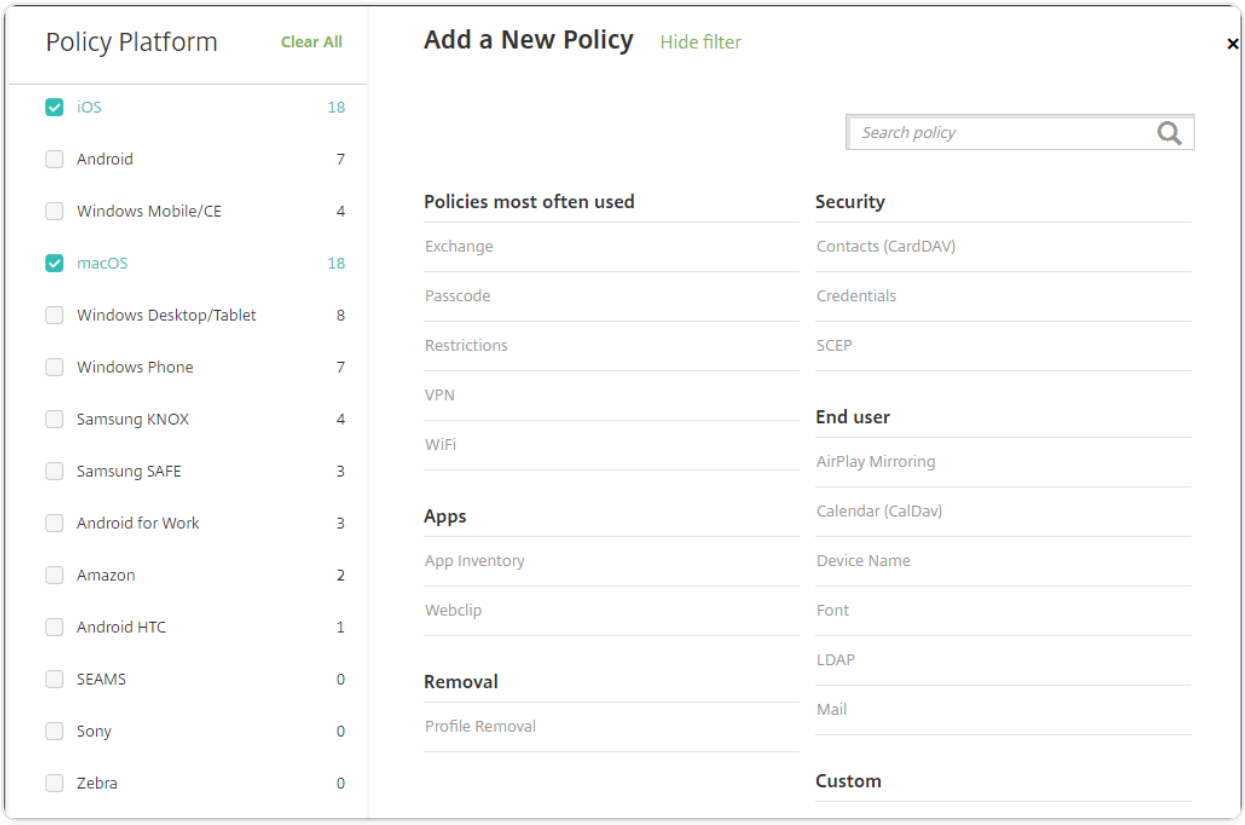


Para adicionar uma política:

1. Na página **Políticas de Dispositivo**, clique em **Adicionar**. A página **Adicionar Nova Política** é exibida.



2. Clique em uma ou mais plataformas para visualizar uma lista das políticas de dispositivo para as plataformas selecionadas. Clique em um nome de política para continuar adicionando a política.



   Você também pode digitar o nome da política na caixa de pesquisa. Conforme você digita, possíveis correspondências aparecem. Se sua política estiver na lista, clique nela. Apenas a política selecionada permanece nos resultados. Clique nela para abrir a página **Informações da Política** para essa política.

3. Selecione as plataformas que você deseja incluir na política. As páginas de configuração para as plataformas selecionadas aparecem na Etapa 5.

4. Preencha a página **Informações da Política** e clique em **Avançar**. A página **Informações da Política** coleta informações, como o nome da política, para ajudar você a identificar e rastrear suas políticas. Esta página é semelhante para todas as políticas.

5. Preencha as páginas da plataforma. As páginas da plataforma aparecem para cada plataforma que você selecionou na Etapa 3. Essas páginas são diferentes para cada política. Uma política pode diferir entre plataformas. Nem todas as políticas se aplicam a todas as plataformas.

   Algumas páginas incluem tabelas de itens. Para excluir um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone da lixeira no lado direito. Na caixa de diálogo de confirmação, clique em **Excluir**.

Para editar um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta no lado direito.

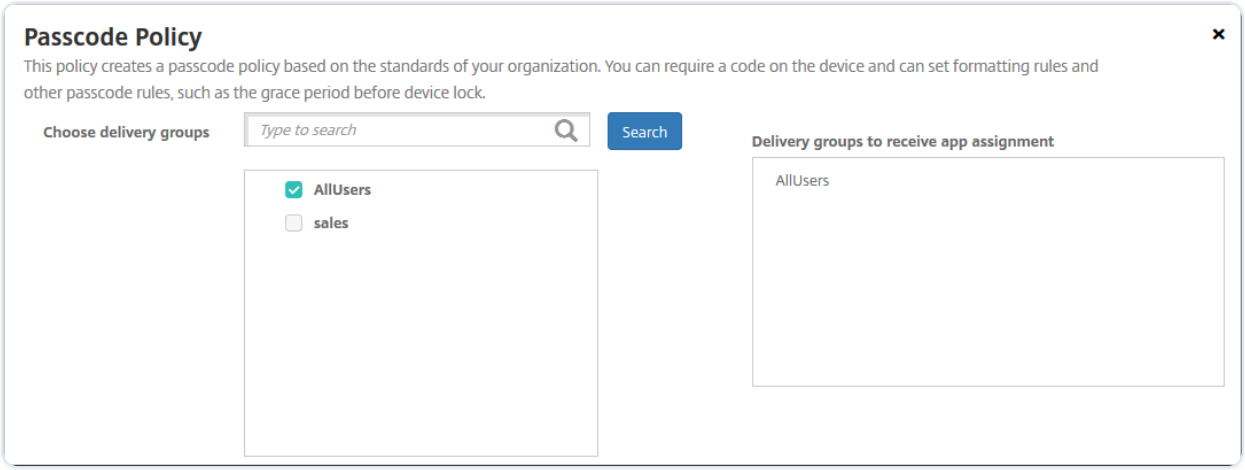
Para configurar regras de implantação, atribuições e agendamento

Para obter mais informações sobre como configurar regras de implantação, consulte Implantar recursos.

1. Em uma página de plataforma, expanda **Regras de Implantação** e configure as seguintes configurações. A guia **Base** aparece por padrão.
    - Nas listas, clique nas opções para determinar quando a política deve ser implantada. Você pode optar por implantar a política quando todas as condições forem atendidas ou quando qualquer condição for atendida. A opção padrão é definida como **Todas**.
    - Clique em **Nova Regra** para definir as condições.
    - Nas listas, clique nas condições, como **Propriedade do dispositivo** e **BYOD**.
    - Clique em **Nova Regra** novamente se quiser adicionar mais condições. Você pode adicionar quantas condições desejar.
2. Clique na guia **Avançado** para combinar as regras com opções booleanas. As condições que você escolheu na guia **Base** aparecem.
3. Você pode usar uma lógica booleana mais avançada para combinar, editar ou adicionar regras.
    - Clique em **E**, **OU** ou **NÃO**.
    - Nas listas, escolha as condições que você deseja adicionar à regra. Em seguida, clique no sinal de Mais (**+**) no lado direito para adicionar a condição à regra.

      A qualquer momento, você pode clicar para selecionar uma condição e, em seguida, clicar em **EDITAR** para alterar a condição ou em **Excluir** para remover a condição.
    - Clique em **Nova Regra** para adicionar outra condição.
4. Clique em **Avançar** para ir para a próxima página da plataforma ou, quando todas as páginas da plataforma estiverem concluídas, para a página **Atribuições**.
5. Na página **Atribuições**, selecione os grupos de entrega aos quais você deseja aplicar a política. Se você clicar em um grupo de entrega, o grupo aparecerá na caixa **Grupos de entrega para receber atribuição de aplicativo**.

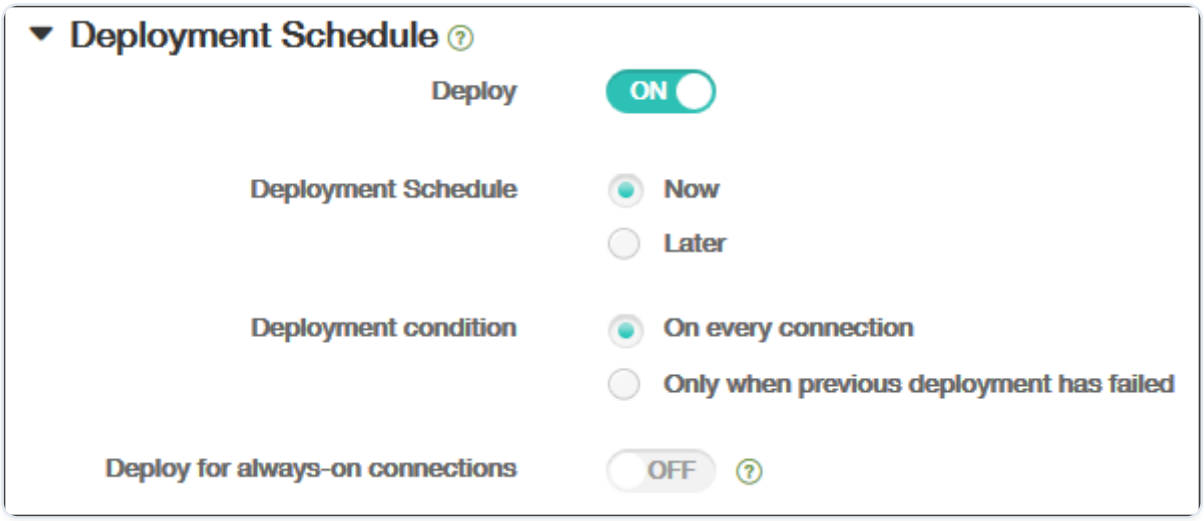
Grupos de entrega para receber atribuição de aplicativo não aparece até que você selecione um grupo de entrega.



6. Na página **Atribuições**, expanda **Agendamento de Implantação** e configure as seguintes configurações:

   - Ao lado de **Implantar**, clique em **Ativado** para agendar a implantação ou clique em **Desativado** para impedir a implantação. A opção padrão é **Ativado**.
   - Ao lado de **Agendamento de implantação**, clique em **Agora** ou **Mais tarde**. A opção padrão é **Agora**.
   - Se você clicar em **Mais tarde**, clique no ícone do calendário e selecione a data e a hora para a implantação.
   - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou clique em **Somente quando a implantação anterior falhou**. A opção padrão é **Em cada conexão**.
   - Ao lado de **Implantar para conexão sempre ativa**, clique em **Ativado** ou **Desativado**. A opção padrão é **Desativado**.

   > **Nota:**
   >
   > Esta opção se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**. A opção sempre ativa não está disponível para dispositivos iOS.
   >
   > O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você fizer se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**, que não se aplica ao iOS.



7. Clique em **Salvar**.

   A política aparece na tabela **Políticas de Dispositivo**.

Remover uma política de dispositivo de um dispositivo

As etapas para remover uma política de dispositivo de um dispositivo dependem da plataforma.

- Android

  Para remover uma política de dispositivo de um dispositivo Android, use a política de desinstalação de dispositivo do XenMobile. Para obter mais informações, consulte a política de desinstalação de dispositivo do XenMobile.

- iOS e macOS

  Para remover uma política de dispositivo de um dispositivo iOS ou macOS, use a política de dispositivo de Remoção de Perfil. Em dispositivos iOS e macOS, todas as políticas fazem parte do perfil MDM. Assim, você pode criar uma política de dispositivo de Remoção de Perfil apenas para a política que deseja remover. O restante das políticas e o perfil permanecem no dispositivo. Para obter informações, consulte política de dispositivo de Remoção de Perfil.

- Windows 10 e Windows 11

  Não é possível remover diretamente uma política de dispositivo de um dispositivo Windows Desktop ou Tablet. No entanto, você pode usar um dos seguintes métodos:

  - Cancelar o registro do dispositivo e, em seguida, enviar um novo conjunto de políticas para o dispositivo. Os usuários então se registram novamente para continuar.
  - Enviar uma ação de segurança para apagar seletivamente o dispositivo específico. Essa ação remove todos os aplicativos e dados corporativos do dispositivo. Em seguida, você

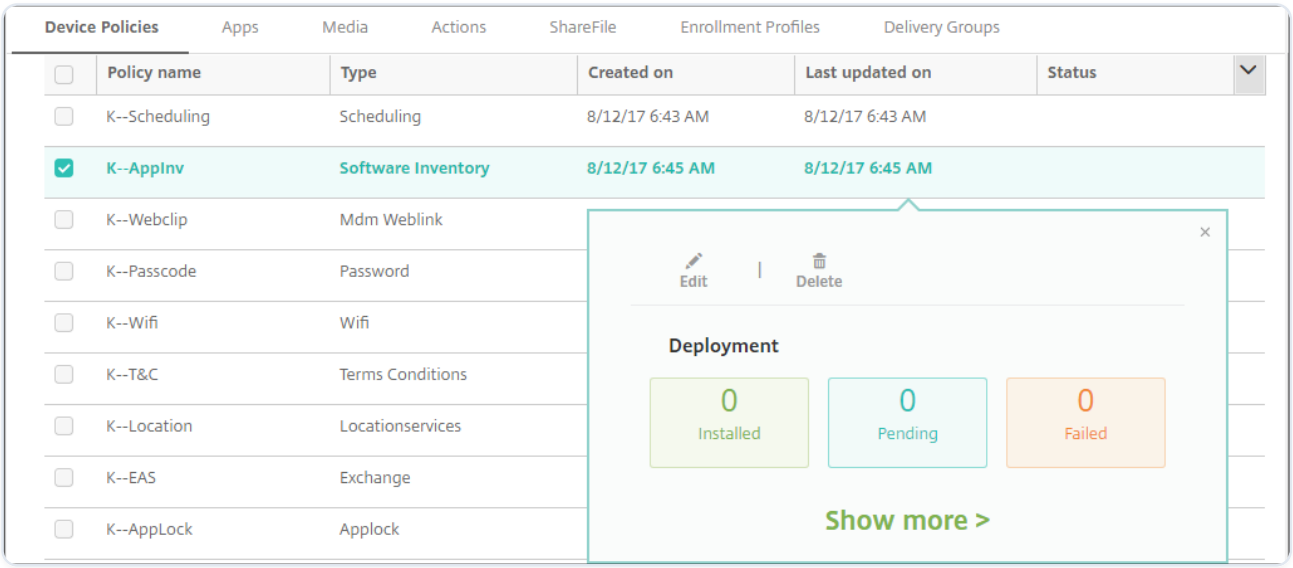
remove a política de dispositivo de um grupo de entrega que contém apenas esse dispositivo e envia o grupo de entrega para o dispositivo. Os usuários então se registram novamente para continuar.

- Chrome OS

  Para remover uma política de dispositivo de um dispositivo Chrome OS, você pode remover a política de dispositivo de um grupo de entrega que contém apenas esse dispositivo. Em seguida, você envia o grupo de entrega para o dispositivo.

Editar uma política de dispositivo

Para editar uma política, selecione a caixa de seleção ao lado de uma política para exibir o menu de opções acima da lista de políticas. Ou, clique em uma política na lista para exibir o menu de opções à direita da listagem.



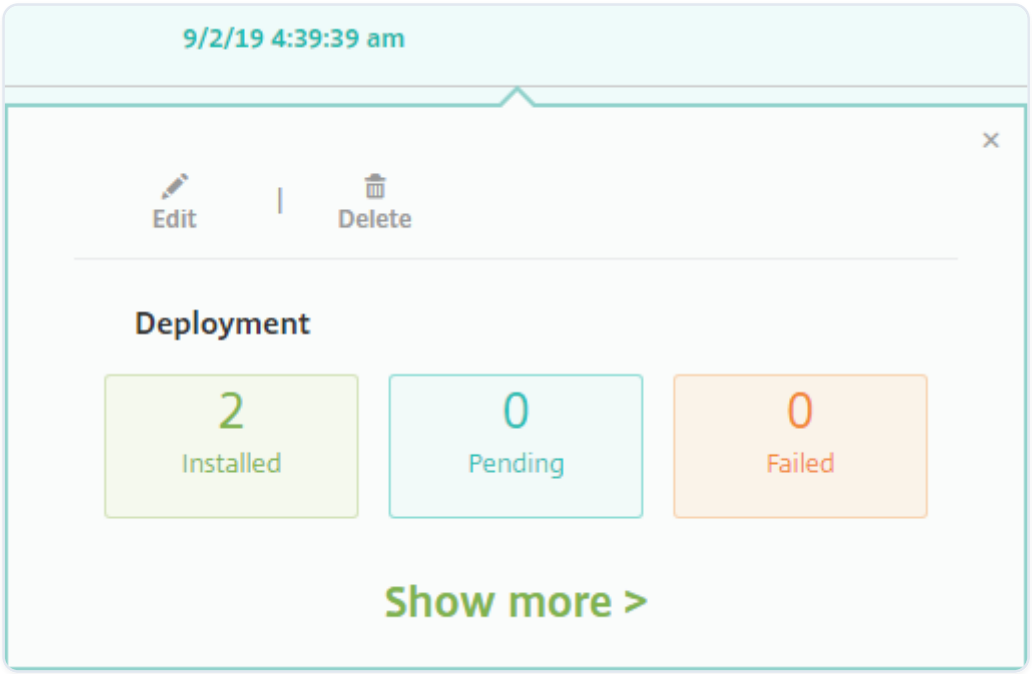
Para visualizar os detalhes da política, clique em **Mostrar mais**.

Para editar todas as configurações de uma política de dispositivo, clique em **Editar**.

Se você clicar em **Excluir**, uma caixa de diálogo de confirmação será exibida. Clique em **Excluir** novamente para excluir a política.

Verificar status de implantação da política

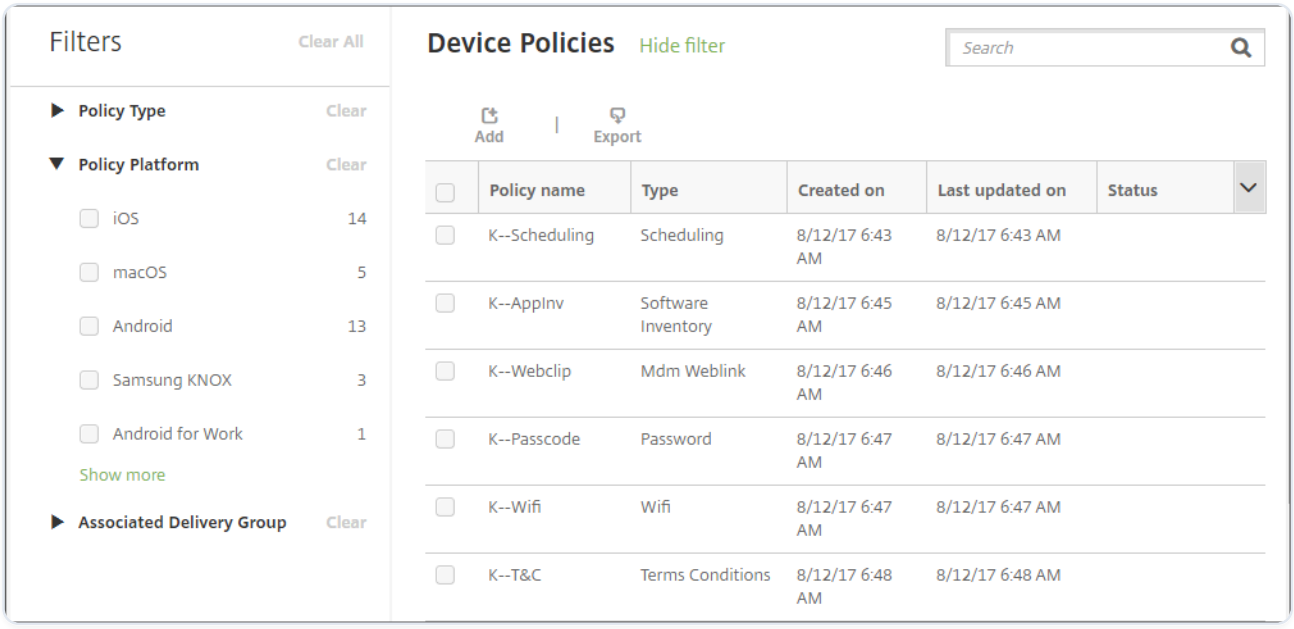
Clique em uma linha de política na página **Configurar > Políticas de Dispositivo** para verificar seu status de implantação.



Quando uma implantação de política está pendente, os usuários podem atualizar a política no Secure Hub tocando em **Preferências > Informações do Dispositivo > Atualizar política**.

Filtrar a lista de políticas de dispositivo adicionadas

Você pode filtrar a lista de políticas adicionadas por tipos de política, plataformas e grupos de entrega associados. Na página **Configurar > Políticas de Dispositivo**, clique em **Mostrar filtro**. Na lista, selecione as caixas de seleção para os itens que deseja ver.



Clique em **SALVAR ESTA EXIBIÇÃO** para salvar um filtro. O nome do filtro aparecerá em um botão abaixo do botão **SALVAR ESTA EXIBIÇÃO**.

Resumos de políticas de dispositivo

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Espelhamento AirPlay	Adiciona dispositivos AirPlay específicos (como outro computador Mac) a dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista de permissões para dispositivos supervisionados. Essa opção limita os usuários apenas aos dispositivos AirPlay na lista de permissões.
AirPrint	Adiciona impressoras AirPrint à lista de impressoras AirPrint em dispositivos iOS. Essa política facilita o suporte a ambientes onde as impressoras e os dispositivos estão em sub-redes diferentes.
Permissões de Aplicativos do Android Enterprise	Configura como as solicitações para aplicativos do Android Enterprise em perfis de trabalho manipular o que o Google chama de permissões “perigosas”.
Restrições de Aplicativos do Android Enterprise	Atualiza as restrições associadas a aplicativos Android.
APN	Determina as configurações usadas para conectar seus dispositivos ao General Packet Radio Service (GPRS) de uma operadora de telefonia específica. Essa configuração já está definida na maioria dos telefones novos. Use essa política se sua organização não usar um APN de consumidor para se conectar à internet a partir de um dispositivo móvel.
Acesso a Aplicativos	Define uma lista de aplicativos que são obrigatórios, opcionais ou impedidos no dispositivo. Você pode então criar uma ação automatizada para reagir à conformidade do dispositivo com essa lista de aplicativos.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Atributos de Aplicativos	Especifica atributos, como um ID de pacote de aplicativo gerenciado ou um identificador VPN por aplicativo, para dispositivos iOS.
Configuração de Aplicativos	Configura remotamente várias configurações e comportamentos de aplicativos que suportam configuração gerenciada. Para fazer isso, você implanta um arquivo de configuração XML (chamado de lista de propriedades, ou plist) em dispositivos iOS. Ou, você implanta pares chave/valor em telefones Windows 10, ou desktops ou tablets executando dispositivos Windows 10 ou Windows 11.
Inventário de Aplicativos	Coleta um inventário dos aplicativos em dispositivos gerenciados. O XenMobile então compara o inventário com quaisquer políticas de acesso a aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que estão em uma lista de permissão ou bloqueio de acesso a aplicativos e, em seguida, agir corretamente.
Bloqueio de Apps	Define uma lista de aplicativos que os usuários podem ou não executar em dispositivos iOS ou em certos dispositivos Android.
Uso da Rede por Aplicativos	Define regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares, em dispositivos iOS. As regras se aplicam apenas a aplicativos gerenciados. Aplicativos gerenciados são aplicativos que você implanta em dispositivos de usuário por meio do XenMobile.
Desinstalação de Aplicativos	Remove aplicativos de dispositivos de usuário.
Notificações de Aplicativos	Controla como os usuários do iOS recebem notificações de aplicativos especificados.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Atualizar aplicativos gerenciados automaticamente	Controla como os aplicativos gerenciados instalados são atualizados em dispositivos Android Enterprise.
BitLocker	Configura as configurações disponíveis na interface do BitLocker em dispositivos Windows 10 e Windows 11.
Calendário (CalDAV)	Adiciona uma conta de calendário (CalDAV) a dispositivos iOS ou macOS. A conta CalDAV permite que os usuários sincronizem dados de agendamento com qualquer servidor que suporte CalDAV.
Celular	Configura as definições de rede celular.
Gerenciador de Conexão	Especifica as configurações de conexão para aplicativos que se conectam automaticamente à internet e a redes privadas. Esta política está disponível apenas em Windows Pocket PCs.
Contatos (CardDAV)	Adiciona uma conta de contato (CardDAV) do iOS a dispositivos iOS ou macOS. A conta CardDAV permite que os usuários sincronizem dados de contato com qualquer servidor que suporte CardDAV.
Controlar Atualizações do SO	Implanta as atualizações mais recentes do SO em dispositivos compatíveis e supervisionados.
Credenciais	Permite a autenticação integrada com sua configuração PKI no XenMobile. Por exemplo, com uma entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor.
XML Personalizado	Personaliza recursos como provisionamento de dispositivos, habilitação de recursos de dispositivos, configuração de dispositivos e gerenciamento de falhas.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Defender	Configura as definições do Windows Defender para desktops e tablets com Windows 10 e Windows 11.
Atestado de Integridade do Dispositivo	Requer que os dispositivos Windows 10 e Windows 11 relatem o estado de sua saúde. Para fazer isso, eles enviam dados específicos e informações de tempo de execução para o Serviço de Atestado de Integridade (HAS) para análise. O HAS cria e retorna um Certificado de Atestado de Integridade que o dispositivo então envia para o XenMobile. Quando o XenMobile recebe o Certificado de Atestado de Integridade, com base no conteúdo desse certificado, ele pode implantar ações automáticas que você configurou.
Nome do Dispositivo	Define os nomes em dispositivos iOS e macOS para que você possa identificar os dispositivos. Você pode usar macros, texto ou uma combinação de ambos para definir um nome de dispositivo.
Configuração de Educação	Configura dispositivos de instrutores e alunos para uso com o Apple Education. Se os instrutores usarem o aplicativo Sala de Aula, a política de dispositivo de Configuração de Educação será necessária.
Exchange	Habilita o e-mail ActiveSync para o cliente de e-mail nativo no dispositivo.
Arquivos	Adiciona arquivos de script ao XenMobile que executam certas funções para os usuários. Ou, você pode adicionar arquivos de documento que deseja que os usuários de dispositivos Android possam acessar em seus dispositivos. Ao adicionar o arquivo, você também pode especificar o diretório no qual deseja que o arquivo seja armazenado no dispositivo.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
FileVault	Esta política permite habilitar a criptografia de dispositivo FileVault em dispositivos macOS registrados. Você também pode controlar quantas vezes um usuário pode pular a configuração do FileVault durante o login. Disponível para macOS 10.7 ou posterior.
Fonte	Adiciona fontes a dispositivos iOS e macOS. As fontes devem ser TrueType (.TTF) ou OpenType (.OFT). O XenMobile não oferece suporte a coleções de fontes (.TTC ou .OTC).
Layout da tela inicial	Especifica o layout de aplicativos e pastas para a tela inicial do iOS em dispositivos supervisionados com iOS 9.3 e posterior.
Importar Perfil iOS e macOS	Importa arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém políticas de segurança e restrições de dispositivo que você prepara usando o Apple Configurator.
Gerenciamento de Keyguard	Controla os recursos disponíveis para os usuários antes que eles desbloqueiem o keyguard do dispositivo e o keyguard de desafio de trabalho. Você também pode controlar os recursos do keyguard do dispositivo para dispositivos totalmente gerenciados e dedicados. Por exemplo, você pode desabilitar recursos da tela de bloqueio, como desbloqueio por impressão digital, agentes de confiança e notificações.
Quiosque	Restringe o uso de aplicativos em dispositivos Samsung SAFE. Você pode limitar os aplicativos disponíveis a um aplicativo ou a aplicativos específicos. Esta política é útil para dispositivos corporativos que se destinam a executar apenas um tipo ou classe específica de aplicativos. Esta política também permite que você escolha imagens personalizadas

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
	para a tela inicial do dispositivo e papéis de parede da tela de bloqueio para o modo quiosque.
Chave da Plataforma Knox para Empresas	Permite que você forneça as informações de licença necessárias da Plataforma Samsung Knox para Empresas (KPE).
Configuração do Launcher	Especifica as configurações para o Citrix Launcher em dispositivos Android, como os aplicativos permitidos e uma imagem de logotipo personalizada para o ícone do Launcher.
LDAP	Fornece informações sobre um servidor LDAP a ser usado para dispositivos iOS, incluindo qualquer informação de conta necessária, como o nome do host do servidor LDAP. A política também fornece um conjunto de políticas de pesquisa LDAP para usar ao consultar o servidor LDAP.
Localização	Permite que você geolocalize dispositivos em um mapa, assumindo que o dispositivo tenha GPS habilitado para o Secure Hub. Após implantar esta política no dispositivo, você pode enviar um comando de localização do XenMobile Server. O dispositivo então responde com suas coordenadas de localização. O XenMobile também oferece suporte a políticas de geofencing e rastreamento.
E-mail	Configura uma conta de e-mail em dispositivos iOS ou macOS.
Domínios Gerenciados	Define domínios gerenciados que se aplicam a e-mail e ao navegador Safari. Os domínios gerenciados ajudam a proteger dados corporativos controlando quais aplicativos podem abrir documentos baixados de domínios usando o Safari. Para dispositivos

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
	supervisionados com iOS 8 e posterior, você pode especificar URLs ou subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador.
Opções de MDM	Gerencia o Buscar Meu Telefone e o Bloqueio de Ativação do iPad em dispositivos telefônicos supervisionados com iOS 7.0 e posterior.
Informações da Organização	Especifica informações da organização para mensagens de alerta que o XenMobile implanta em dispositivos iOS.
Senha	Impõe um código PIN ou senha em um dispositivo gerenciado. Você pode definir a complexidade e os tempos limite para a senha no dispositivo.
Acesso Pessoal	Permite que os usuários se conectem à internet quando não estão no alcance de uma rede Wi-Fi. Os usuários se conectam através da conexão de dados celulares em seu dispositivo iOS, usando a funcionalidade de acesso pessoal.
Remoção de Perfil	Remove o perfil do aplicativo de dispositivos iOS ou macOS.
Perfil de Provisionamento	Especifica um perfil de provisionamento de distribuição empresarial para enviar aos dispositivos. Ao desenvolver e assinar um aplicativo empresarial iOS, você geralmente inclui um perfil de provisionamento. A Apple exige o perfil para que o aplicativo seja executado em um dispositivo iOS. Se um perfil de provisionamento estiver ausente ou tiver expirado, o aplicativo falha quando um usuário toca para abri-lo.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Remoção de Perfil de Provisionamento	Remove perfis de provisionamento do iOS.
Proxy	Especifica as configurações globais de proxy HTTP para dispositivos que executam iOS. Você pode implantar apenas uma política de proxy HTTP global por dispositivo.
Restrições	Oferece centenas de opções para bloquear e controlar recursos e funcionalidades em dispositivos gerenciados. Exemplos de opções de restrição: Desativar a câmera ou o microfone, impor regras de roaming e impor acesso a serviços de terceiros, como lojas de aplicativos.
Roaming	Configura se o roaming de voz e dados é permitido em dispositivos iOS. Se o roaming de voz estiver desativado, o roaming de dados será desativado automaticamente.
Agendamento	Necessário para que os dispositivos Android se conectem novamente ao XenMobile Server para gerenciamento de MDM, envio de aplicativos e implantação de políticas. Se você não enviar esta política para os dispositivos e não habilitar o Google FCM, um dispositivo não poderá se conectar novamente ao servidor.
SCEP	Configura dispositivos iOS e macOS para recuperar um certificado de um servidor SCEP externo. Você também pode entregar um certificado ao dispositivo usando SCEP de uma PKI conectada ao XenMobile. Para fazer isso, crie uma entidade PKI e um provedor PKI no modo distribuído.
Conta SSO	Cria contas de logon único (SSO) para que os usuários façam logon apenas uma vez para acessar o XenMobile e os recursos internos da sua empresa. Os usuários não precisam

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
	armazenar nenhuma credencial no dispositivo. O XenMobile usa as credenciais de usuário corporativo para uma conta SSO em todos os aplicativos, incluindo aplicativos da App Store. Esta política é compatível com a autenticação Kerberos. Disponível para iOS.
Calendários Assinados	Adiciona um calendário assinado à lista de calendários em dispositivos iOS. Certifique-se de assinar um calendário antes de adicioná-lo à lista de calendários assinados nos dispositivos do usuário.
Termos e Condições	Exige que os usuários aceitem as políticas específicas da sua empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos com o XenMobile, eles devem aceitar os termos e condições para registrar seus dispositivos. Recusar os termos e condições cancela o processo de registro.
Túnel	Usado apenas para Suporte Remoto. O suporte remoto permite que seus representantes de suporte técnico assumam o controle remoto de dispositivos móveis Windows CE e Android gerenciados. O suporte remoto não está disponível para implantações de XenMobile Server on-premises em cluster. O Suporte Remoto não está mais disponível para novos clientes a partir de January 1, 2019. Clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá aprimoramentos ou correções.
VPN	Fornece acesso a sistemas de back-end que usam tecnologia de gateway VPN legada. Esta política fornece detalhes de conexão do gateway VPN que você pode implantar em dispositivos. O XenMobile suporta vários provedores de VPN, incluindo Cisco

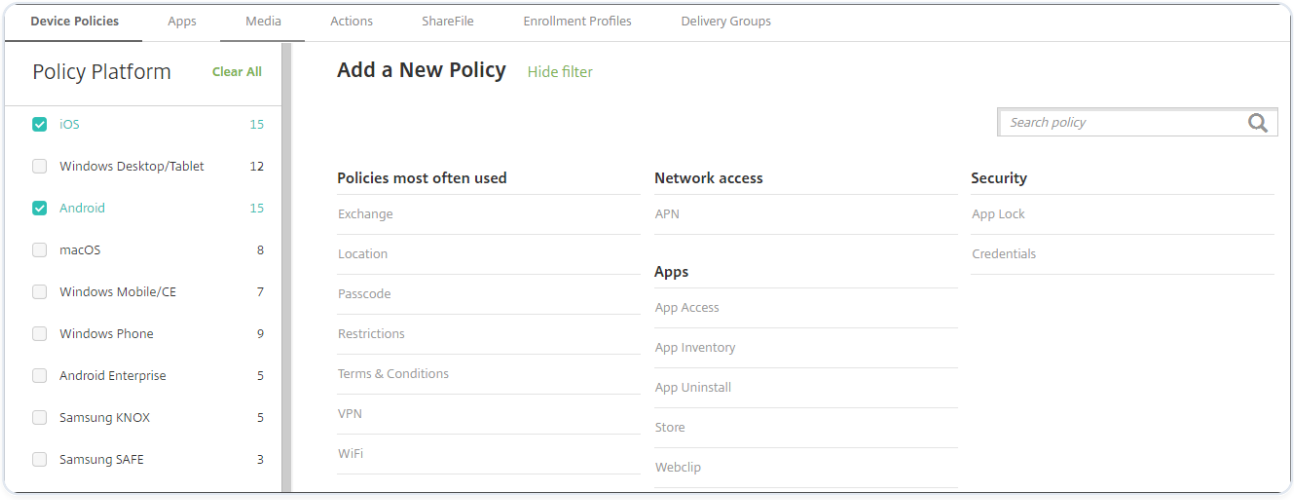
NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
	AnyConnect, Juniper e Citrix VPN. Se o seu gateway VPN suportar esta opção, você pode vincular esta política a uma CA e habilitar VPN sob demanda.
Papel de Parede	Adiciona um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio, tela inicial ou em ambas em um dispositivo iOS. Para usar papéis de parede diferentes em iPads e iPhones, crie políticas de papel de parede diferentes e implante-as nos usuários apropriados.
Filtro de Conteúdo Web	Filtra conteúdo web em dispositivos iOS. O XenMobile usa a função de filtro automático da Apple e os sites que você adiciona às listas de permissão e bloqueio. Disponível apenas para dispositivos iOS supervisionados.
Webclip	Coloca atalhos, ou web clips, para sites para que apareçam ao lado de aplicativos em dispositivos de usuário. Você pode especificar seus próprios ícones para representar os web clips para dispositivos iOS, macOS e Android. O tablet Windows requer apenas um rótulo e uma URL.
Wi-Fi	Permite que os administradores implantem detalhes do roteador Wi-Fi em dispositivos gerenciados. Os detalhes do roteador incluem SSID, dados de autenticação e dados de configuração.
Proteção de Informações do Windows	Especifica os aplicativos que exigem a Proteção de Informações do Windows no nível de imposição definido para a política. A política é para dispositivos supervisionados com Windows 10 e Windows 11.

NOME DA POLÍTICA DE DISPOSITIVO	DESCRIÇÃO DA POLÍTICA DE DISPOSITIVO
Loja XenMobile	Especifica se um web clip da Loja XenMobile aparece na tela inicial dos dispositivos do usuário.
Opções do XenMobile	Configura o comportamento do Secure Hub ao se conectar ao XenMobile a partir de dispositivos Android.
Desinstalação do XenMobile	Desinstala o XenMobile de dispositivos Android e Window Mobile/CE. Quando implantada, esta política remove o XenMobile de todos os dispositivos no grupo de implantação.

Políticas de dispositivo por plataforma

Para visualizar as políticas disponíveis por plataforma:

1. No console do XenMobile®, vá para **Configurar > Políticas de Dispositivo**.
2. Clique em **Adicionar**.
3. Cada plataforma de dispositivo aparece em uma lista no painel **Plataforma de Política**. Se esse painel não estiver aberto, clique em **Mostrar filtro**.
4. Para ver uma lista de todas as políticas disponíveis para uma plataforma, selecione essa plataforma. Para ver uma lista das políticas disponíveis para várias plataformas, selecione cada uma dessas plataformas. Uma política aparece na lista somente se for aplicável a cada plataforma selecionada.



A versão mais recente do XenMobile oferece suporte a políticas de dispositivo para as seguintes plataformas:

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung Knox
- Windows 10 e Windows 11 Desktop/Tablet

Para obter detalhes sobre os dispositivos suportados na versão mais recente do XenMobile, consulte Plataformas de dispositivos suportadas.

> **Nota:**
>
> Se o seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):
>
> Ao configurar políticas de dispositivo XenMobile para Windows 10 e Windows 11, tenha as seguintes regras em mente. Se uma política em um ou mais dispositivos registrados entrar em conflito, a política alinhada com o GPO terá precedência.

Política de dispositivo de espelhamento AirPlay

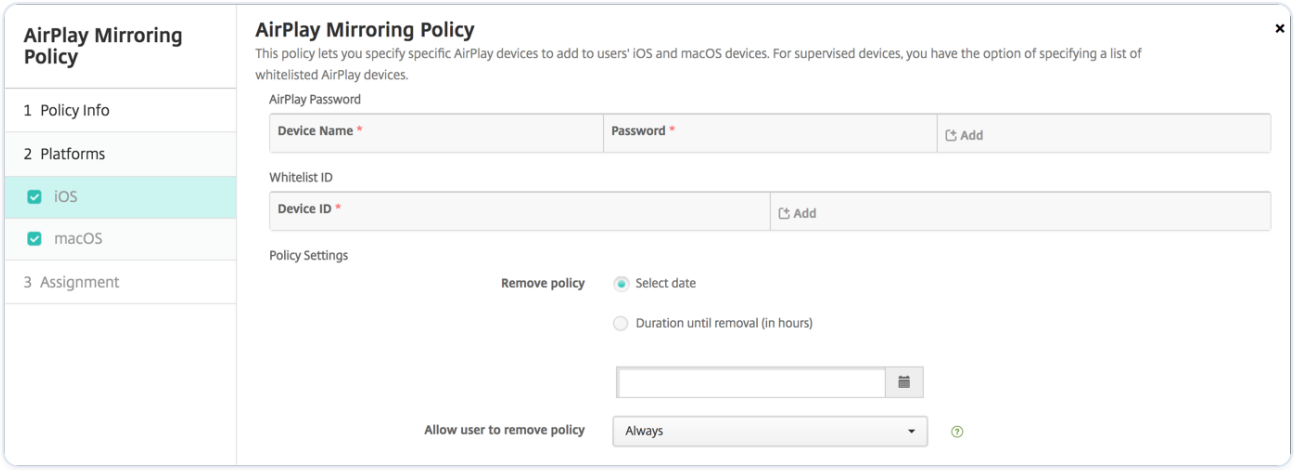
O recurso Apple AirPlay permite que os usuários espelhem exatamente o que está na tela de um dispositivo para outro computador Mac.

Você pode adicionar uma política de dispositivo no XenMobile para adicionar dispositivos AirPlay específicos (como outro computador Mac) a dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista de permissões para dispositivos supervisionados, o que limita os usuários apenas aos dispositivos AirPlay na lista de permissões. Para obter informações sobre como colocar um dispositivo no modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.

> **Nota:**
>
> Antes de prosseguir, certifique-se de ter os IDs de dispositivo e quaisquer senhas para todos os dispositivos que deseja adicionar.

> Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **Senha do AirPlay:** Para cada dispositivo que você deseja adicionar, clique em **Adicionar** e, em seguida, faça o seguinte:
  - **ID do Dispositivo:** Insira o endereço de hardware (endereço MAC) no formato xx:xx:xx:xx:xx:xx. Este campo não diferencia maiúsculas de minúsculas.
  - **Senha:** Insira uma senha opcional para o dispositivo.
  - Clique em **Adicionar** para adicionar o dispositivo ou clique em **Cancelar** para cancelar a adição do dispositivo.
- **ID da Lista de Permissões:** Esta lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nesta lista são os únicos dispositivos AirPlay disponíveis para os dispositivos dos usuários. Para cada dispositivo AirPlay que você deseja adicionar à lista, clique em **Adicionar** e, em seguida, faça o seguinte:

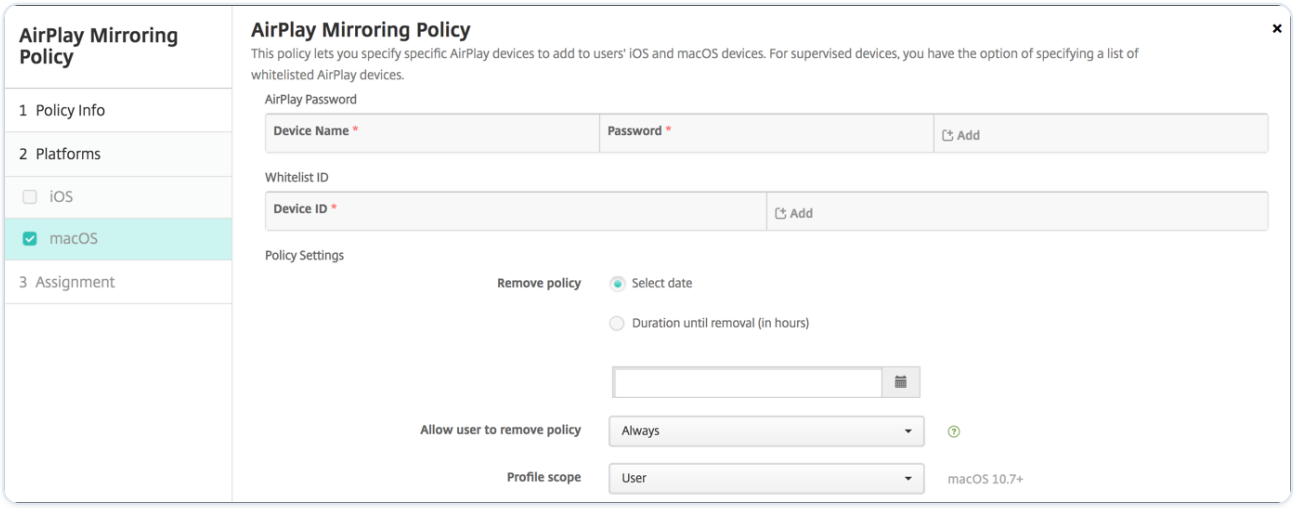
> **Nota:**

> O console do XenMobile® Server inclui os termos "lista negra" e "lista branca". Estamos alterando esses termos em uma próxima versão para "lista de bloqueio" e "lista de permissões".

  - **ID do Dispositivo:** Digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Este campo não diferencia maiúsculas de minúsculas.
  - Clique em **Adicionar** para adicionar o dispositivo ou clique em **Cancelar** para cancelar a adição do dispositivo.

- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

Configurações do macOS



- **Senha do AirPlay:** Para cada dispositivo que você deseja adicionar, clique em **Adicionar** e, em seguida, faça o seguinte:
  - **ID do Dispositivo:** Insira o endereço de hardware (endereço MAC) no formato xx:xx:xx:xx:xx:xx. Este campo não diferencia maiúsculas de minúsculas.
  - **Senha:** Insira uma senha opcional para o dispositivo.

    - Clique em **Adicionar** para adicionar o dispositivo ou clique em **Cancelar** para cancelar a adição do dispositivo.

- **ID da Lista de Permissões:** Esta lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nesta lista são os únicos dispositivos AirPlay disponíveis para os dispositivos do usuário. Para cada dispositivo AirPlay que você deseja adicionar à lista, clique em **Adicionar** e, em seguida, faça o seguinte:

    - **ID do Dispositivo:** Digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Este campo não diferencia maiúsculas de minúsculas.
    - Clique em **Adicionar** para adicionar o dispositivo ou clique em **Cancelar** para cancelar a adição do dispositivo.

- **Configurações de política**

    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**

        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

    - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
    - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Política de dispositivo AirPrint

Você pode adicionar uma política de dispositivo no XenMobile® para adicionar impressoras AirPrint à lista de impressoras AirPrint em dispositivos iOS. Essa política facilita o suporte a ambientes onde as impressoras e os dispositivos estão em sub-redes diferentes.

Esta política se aplica ao iOS 7.0 e posterior.

> **Nota:**

> Certifique-se de ter o endereço IP e o caminho do recurso para cada impressora.

> Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Destino AirPrint:** Para cada destino AirPrint que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Endereço IP:** Insira o endereço IP da impressora AirPrint.
  - **Caminho do Recurso:** Insira o Caminho do Recurso associado à impressora. Este valor corresponde ao parâmetro do registro Bonjour _ipps.tcp. Por exemplo, printers/Canon_MG5300_series ou printers/Xerox_Phaser_7600.
  - Clique em **Salvar** para adicionar a impressora ou clique em **Cancelar** para cancelar a adição da impressora.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Permissões de aplicativos do Android Enterprise

Você pode configurar como as solicitações para aplicativos do Android Enterprise que estão em perfis de trabalho manipular o que o Google chama de permissões “perigosas”. Você controla se o usuário é solicitado a conceder ou negar a solicitação de permissão do aplicativo. Este recurso se aplica a dispositivos que executam Android 7.0 e posterior.

O Google define permissões perigosas como permissões que dão ao aplicativo acesso a dados ou recursos que envolvem informações privadas do usuário ou que podem afetar os dados armazenados do usuário ou a operação de outros aplicativos. Por exemplo, a capacidade de ler os contatos do usuário é uma permissão perigosa.

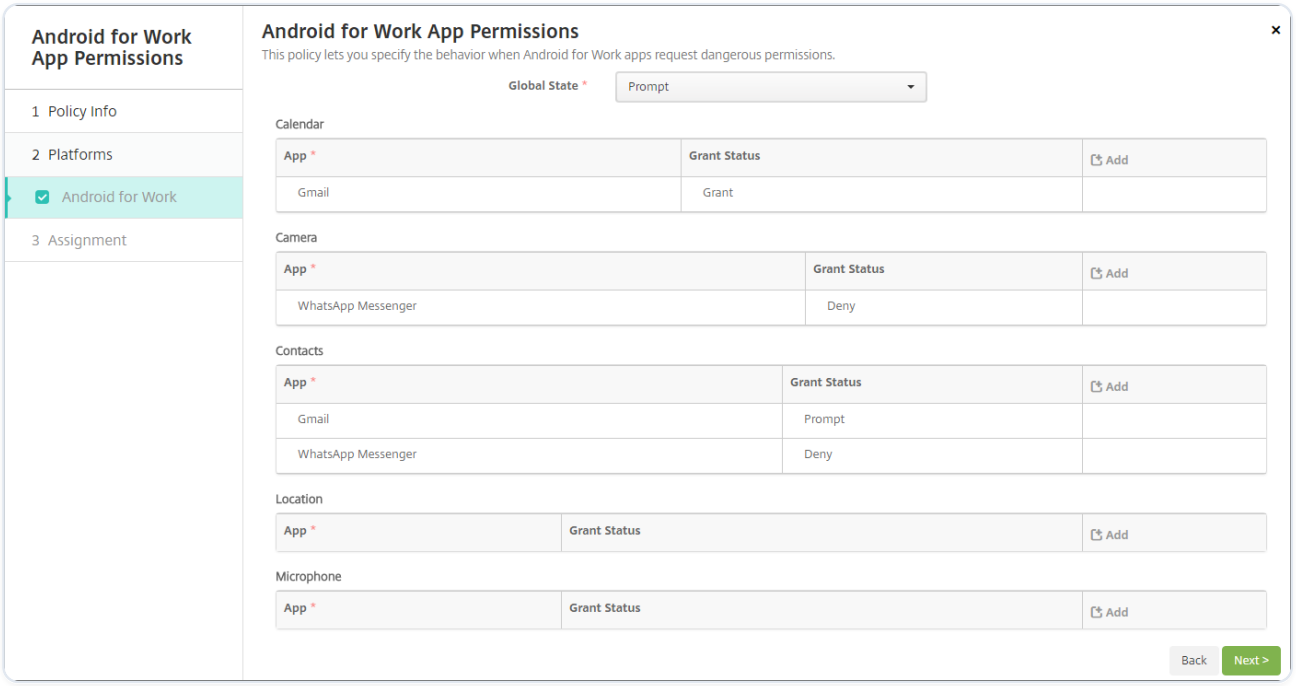
Você pode configurar um estado global que controla o comportamento de todas as solicitações de permissão perigosas para aplicativos do Android Enterprise dentro de perfis de trabalho. Você também pode controlar o comportamento das solicitações de permissão perigosas para grupos de permissão individuais, conforme definido pelo Google, para cada aplicativo. Essas configurações individuais substituem o estado global.

Para obter informações sobre como o Google define grupos de permissão, consulte “Grupos de permissão” neste guia para desenvolvedores Android.

Por padrão, os usuários são solicitados a conceder ou negar solicitações de permissão perigosas.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de Dispositivo.

Configurações do Android Enterprise



- **Estado Global:** Controla o comportamento de todas as solicitações de permissão perigosas. Na lista, clique em **Solicitar**, **Conceder** ou **Negar**.
    - **Solicitar:** Os usuários são solicitados a conceder ou negar solicitações de permissão perigosas.
    - **Conceder:** Todas as solicitações de permissão perigosas são concedidas. O usuário não é solicitado.
    - **Negar:** Todas as solicitações de permissão perigosas são negadas. O usuário não é solicitado.

O padrão é **Solicitar**.

- Defina um comportamento individual para cada grupo de permissão, para cada aplicativo. Para configurar o comportamento de um grupo de permissão: Clique em **Adicionar**. Em **Aplicativo**, escolha um aplicativo da lista. Se você configurar aplicativos de sistema do Android Enterprise, clique em **Adicionar novo** e insira o nome do pacote do aplicativo que você habilitou na política de dispositivo Restrições. Em Estado de Concessão, escolha **Solicitar**, **Conceder** ou **Negar**. Este estado de concessão substitui o estado global.
  - **Solicitar:** Os usuários são solicitados a conceder ou negar solicitações de permissão perigosas deste grupo de permissões para este aplicativo.
  - **Conceder:** As solicitações de permissão perigosas deste grupo de permissões para este aplicativo são concedidas. O usuário não é solicitado.

    > **Observação:**
    >
    > Para os dispositivos registrados no modo **Proprietário do Perfil**, a permissão **Conceder** não é aplicável para Câmera, Localização, Microfone e Sensor se o dispositivo estiver executando o Android 12 ou posterior.

  - **Negar:** As solicitações de permissão perigosas deste grupo de permissões para este aplicativo são negadas. O usuário não é solicitado.

  O padrão é **Solicitar**.
- Clique em **Salvar** ao lado do aplicativo e do estado de concessão.
- Para adicionar mais aplicativos para o grupo de permissões, clique em **Adicionar** novamente e repita estas etapas.
- Quando terminar de definir os estados de concessão para todos os grupos de permissões desejados, clique em **Avançar**.

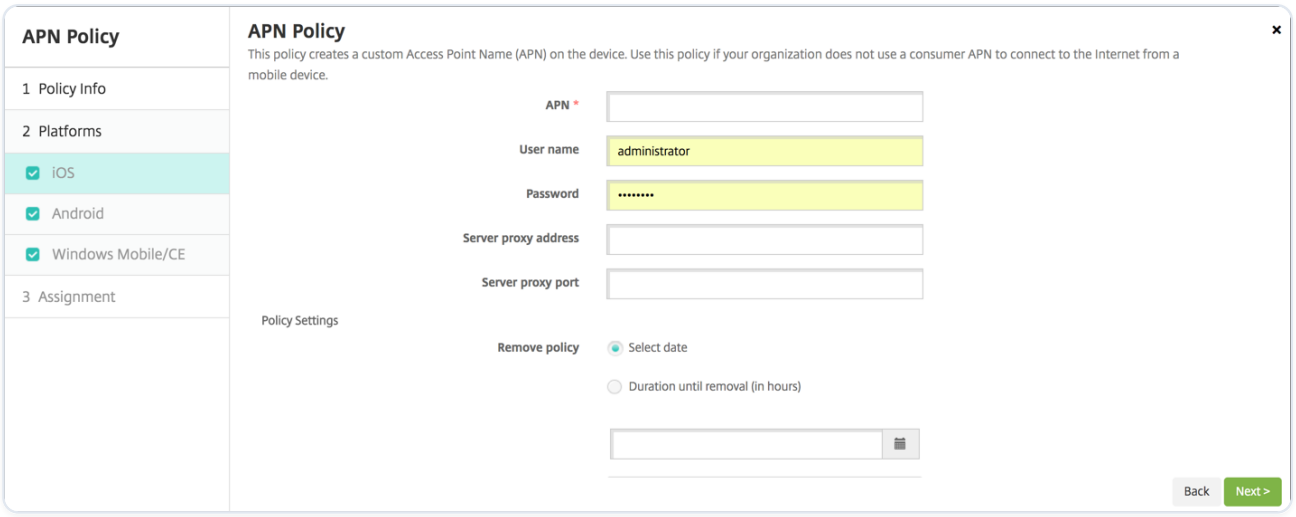
Política de dispositivo APN

Você pode adicionar uma política de dispositivo de Nome de Ponto de Acesso (APN) personalizada para dispositivos iOS e Android. Você usa esta política se sua organização não usa um APN de consumidor para se conectar à Internet a partir de um dispositivo móvel. Uma política de APN determina as configurações usadas para conectar seus dispositivos ao General Packet

Radio Service (GPRS) de uma operadora de telefone específica. Essa configuração já está definida na maioria dos telefones mais recentes.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

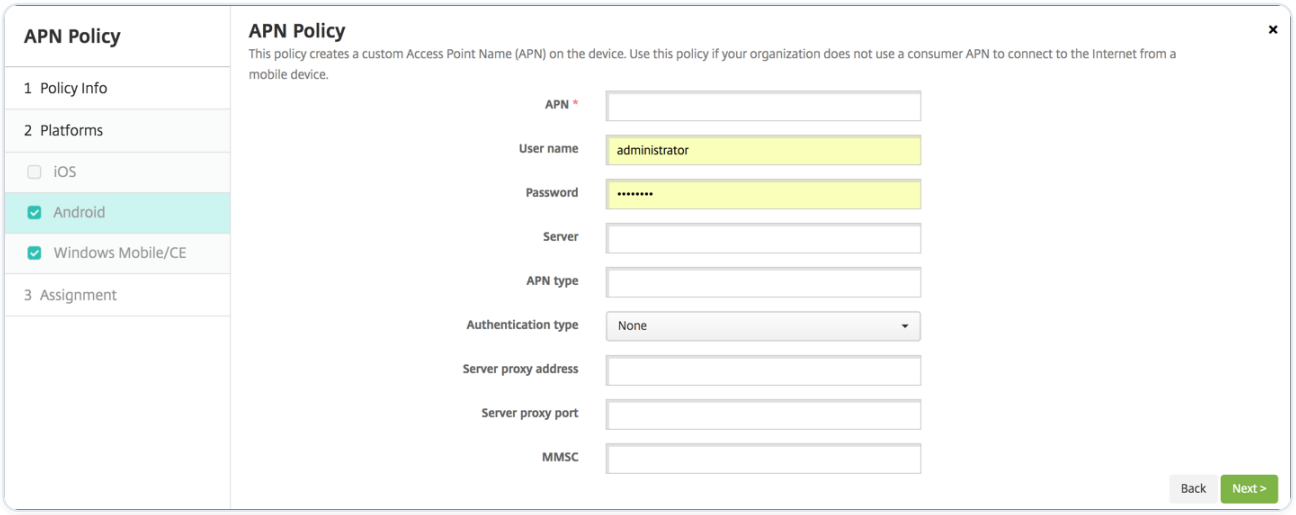
Configurações do iOS



- **APN:** Digite o nome do ponto de acesso. Este nome de APN deve corresponder a um APN iOS aceito, caso contrário, a política falhará.
- **Nome de usuário:** Esta string especifica o nome de usuário para este APN. Se o nome de usuário estiver ausente, o dispositivo solicitará a string durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se estiver ausente do payload, o dispositivo solicitará a senha durante a instalação do perfil.
- **Endereço do proxy do servidor:** O endereço IP ou URL do proxy APN.
- **Porta do proxy do servidor:** O número da porta para o proxy APN. Este número da porta do proxy do servidor é obrigatório se você inseriu um endereço de proxy do servidor.
- Em **Configurações de Política**, ao lado de **Remover política**, clique em **Selecionar data** ou **Duração até a remoção (em horas)**.
    - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para a remoção.
    - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha necessária** ou **Nunca**.
    - Se você clicar em **Senha necessária**, ao lado de **Senha de remoção**, digite a senha necessária.

- **Configurações de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do Android



- **APN:** Digite o nome do ponto de acesso. Este nome de APN deve corresponder a um APN Android aceito ou a política falhará.
- **Nome de usuário:** Esta string especifica o nome de usuário para este APN. Se o nome de usuário estiver ausente, o dispositivo solicitará a string durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se estiver ausente do payload, o dispositivo solicitará a senha durante a instalação do perfil.
- **Servidor:** Esta configuração, que antecede os smartphones, normalmente está vazia. Ela faz referência a um servidor de gateway de Wireless Application Protocol (WAP) para telefones que podem não acessar sites padrão.
- **Tipo de APN:** Esta configuração deve corresponder ao uso pretendido da operadora para o ponto de acesso. É uma string separada por vírgulas de especificadores de serviço APN e deve corresponder às definições publicadas da operadora sem fio. Os exemplos incluem:
  - *: Todo o tráfego passa por este ponto de acesso.
  - mms: O tráfego multimídia passa por este ponto de acesso.

    - default: Todo o tráfego, incluindo multimídia, passa por este ponto de acesso.
    - supl: Secure User Plane Location está associado ao GPS assistido.
    - dun: Dial Up Networking está desatualizado e deve ser raramente usado.
    - hipri" Rede de alta prioridade.
    - fota: Firmware over the air é usado para receber atualizações de firmware.

- **Tipo de autenticação:** Clique no tipo de autenticação a ser usado na lista suspensa. O padrão é Nenhum.
- **Endereço do proxy do servidor:** O endereço IP ou URL do proxy HTTP APN da operadora.
- **Porta do proxy do servidor:** O número da porta para o proxy APN. Este número da porta do proxy do servidor é obrigatório se você inseriu um endereço de proxy do servidor.
- **MMSC:** O endereço do servidor de gateway MMS fornecido pela operadora.
- **Endereço do proxy do servidor de mensagens multimídia (MMS):** Este é o servidor de serviço de mensagens multimídia para tráfego MMS. O MMS sucedeu o SMS para o envio de mensagens maiores com conteúdo multimídia, como fotos ou vídeos. Esses servidores exigem protocolos específicos (como MM1, ... MM11).
- **Porta MMS:** A porta usada para o proxy MMS.

Política de dispositivo de acesso a aplicativos

A política de dispositivo de acesso a aplicativos no XenMobile® permite definir o seguinte:

- Uma lista de aplicativos que são obrigatórios para serem instalados no dispositivo.
- Uma lista de aplicativos que podem ser instalados no dispositivo.
- Uma lista de aplicativos que não devem ser instalados no dispositivo.

Você pode então criar uma ação automatizada para reagir à conformidade do dispositivo com a lista de aplicativos. Você pode criar políticas de acesso a aplicativos para dispositivos iOS e Android.

Você só pode configurar um tipo de política de acesso por vez. Você pode adicionar uma política para uma lista de aplicativos obrigatórios, aplicativos sugeridos ou aplicativos não permitidos, mas não uma mistura dentro da mesma política de acesso a aplicativos. Se você criar uma política para cada tipo de lista, é recomendável nomear cada política com cuidado. Nomear cada política com cuidado permite que você saiba qual política no XenMobile se aplica a qual lista de aplicativos.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma

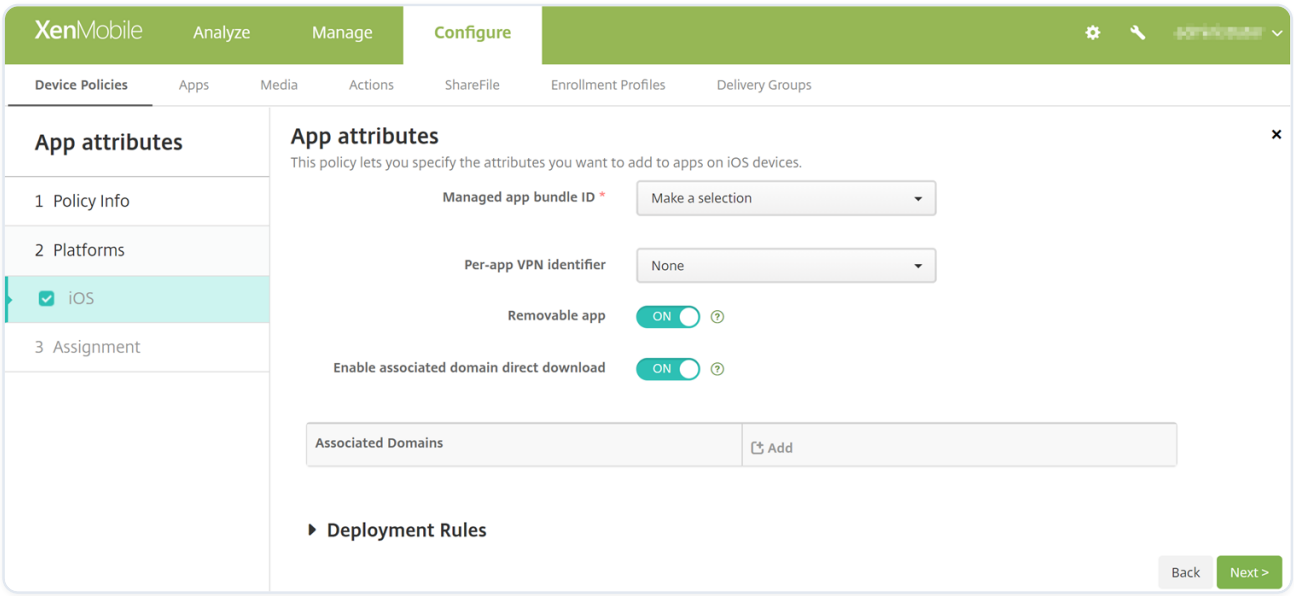
- **Política de acesso:** Clique em **Obrigatório**, **Sugerido** ou **Proibido**. O padrão é **Obrigatório**.
- Para adicionar um ou mais aplicativos à lista, clique em **Adicionar** e faça o seguinte:
  - **Nome do aplicativo:** Insira um nome de aplicativo.
  - **Identificador do aplicativo:** Insira um identificador de aplicativo opcional.
  - Clique em **Salvar** ou **Cancelar**.
  - Repita estas etapas para cada aplicativo que você deseja adicionar.

Política de dispositivo de atributos de aplicativo

A política de dispositivo de atributos de aplicativo permite especificar atributos como um ID de pacote de aplicativo gerenciado ou um identificador VPN por aplicativo para dispositivos iOS.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **ID do pacote de aplicativo gerenciado:** Especifique um aplicativo das seguintes maneiras:
  - Selecione o ID do pacote de aplicativo. As opções estão disponíveis somente depois que você habilita a política de dispositivo **Inventário de Aplicativos**, que coleta um inventário de aplicativos em dispositivos gerenciados.

    - Selecione **Adicionar novo** e, em seguida, digite o ID do pacote de aplicativo. Para encontrar um ID de pacote de aplicativo, consulte Encontrar o ID do pacote para um aplicativo na App Store.

- **Identificador VPN por aplicativo:** (Opcional) Selecione uma VPN por aplicativo para este aplicativo. As opções incluem as conexões VPN por aplicativo que você configurou na página **Políticas de Dispositivo** > **Política VPN**. Para obter mais informações, consulte Configurar uma VPN por aplicativo.
- **Aplicativo removível:** (Opcional) Especifique se o aplicativo pode ser removido pelos usuários quando é um aplicativo gerenciado. Para impedir que os usuários desinstalem o aplicativo, defina esta opção como **Desativado**. O valor padrão é **Ativado**. Disponível para iOS 14 e posterior.
- **Habilitar download direto de domínio associado:** (Opcional) Especifique se o aplicativo pode realizar a verificação de associação de site reivindicada diretamente no domínio, em vez de nos servidores da Apple. Defina esta opção como **Ativado** apenas para domínios que não podem acessar a internet. O valor padrão é **Ativado**. Disponível para iOS 14 e posterior.
- **Domínios Associados:** (Opcional) Para adicionar um Domínio Associado para este aplicativo, clique em **Adicionar** e, em seguida, digite seu nome de domínio totalmente qualificado (FQDN). Disponível para iOS 13 e posterior.

Encontrar o ID do pacote para um aplicativo na App Store

1. Localize o aplicativo na App Store e copie o número no final da URL. Por exemplo, 363501921 é o ID do aplicativo para o Citrix Workspace app.
2. Vá para `https://itunes.apple.com/lookup?id=` e cole o número após essa URL. Um arquivo TXT é baixado automaticamente para o seu computador.
3. No arquivo TXT, procure por `bundleId` e obtenha o ID do pacote do aplicativo. Por exemplo, o ID do pacote para o aplicativo Citrix Workspace é `com.citrix.ReceiveriPad`.

Política de dispositivo de configuração de aplicativo

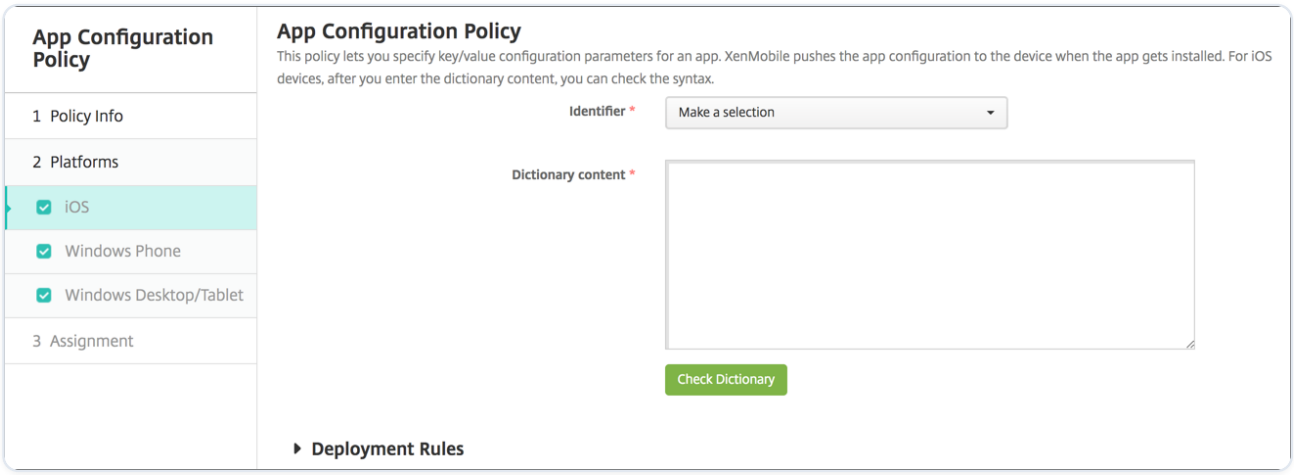
Você pode configurar remotamente aplicativos que suportam configuração gerenciada implantando:

- Um arquivo de configuração XML (chamado de lista de propriedades, ou plist) para dispositivos iOS
- Ou, pares de chave/valor para telefones ou tablets Windows 10 ou dispositivos desktop executando Windows 10 ou Windows 11.

A configuração especifica várias configurações e comportamentos no aplicativo. O XenMobile® envia a configuração para os dispositivos quando o usuário instala o aplicativo. As configurações e comportamentos reais que você pode configurar dependem do aplicativo e estão além do escopo deste artigo.

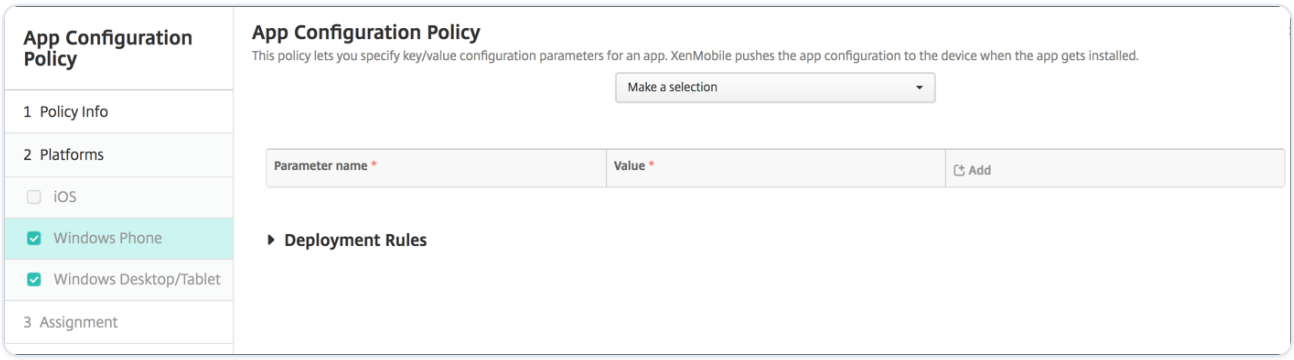
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

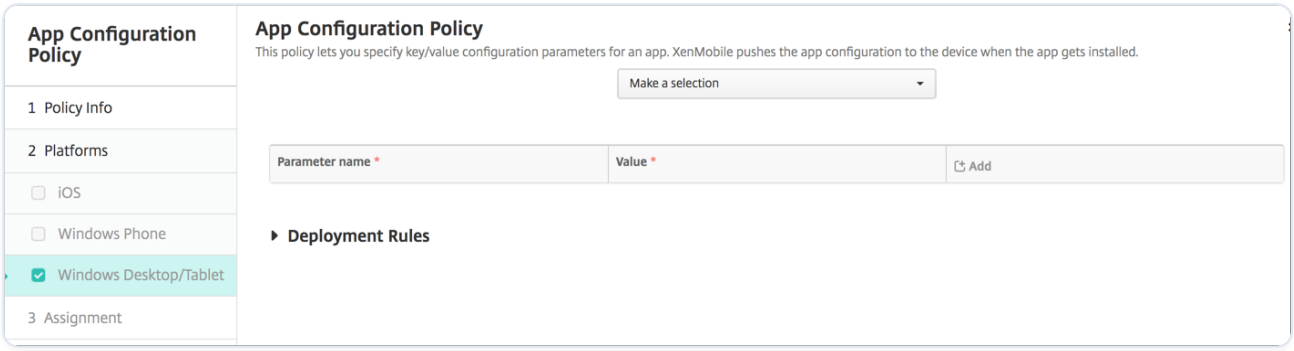
Configurações do iOS



- **Identificador:** Clique no aplicativo na lista suspensa que você deseja configurar ou clique em **Adicionar novo** para adicionar um aplicativo à lista.
  - Se você clicar em **Adicionar novo**, digite o identificador do aplicativo no campo que aparece.
- **Conteúdo do dicionário:** Digite, ou copie e cole, as informações de configuração da lista de propriedades XML (plist).
- Clique em **Verificar Dicionário**. O XenMobile verifica o XML. Se não houver erros, você verá **XML Válido** abaixo da caixa de conteúdo. Se algum erro de sintaxe aparecer abaixo da caixa de conteúdo, você deve corrigi-los antes de continuar.

Configurações de Desktop/Tablet Windows





- Na lista **Fazer uma seleção**, clique no aplicativo que você deseja configurar ou clique em **Adicionar novo** para adicionar um aplicativo à lista.
    - Se você clicar em **Adicionar novo**, digite o nome da família do pacote no campo que aparece.
- Para cada parâmetro de configuração que você deseja adicionar, clique em **Adicionar** e, em seguida, faça o seguinte:
    - **Nome do parâmetro:** Insira o nome da chave de uma configuração de aplicativo para o dispositivo Windows. Para obter informações sobre as configurações de aplicativos do Windows, consulte a documentação da Microsoft.
    - **Valor:** Insira o valor para o parâmetro especificado.
    - Clique em **Adicionar** para adicionar o parâmetro ou clique em **Cancelar** para cancelar a adição do parâmetro.

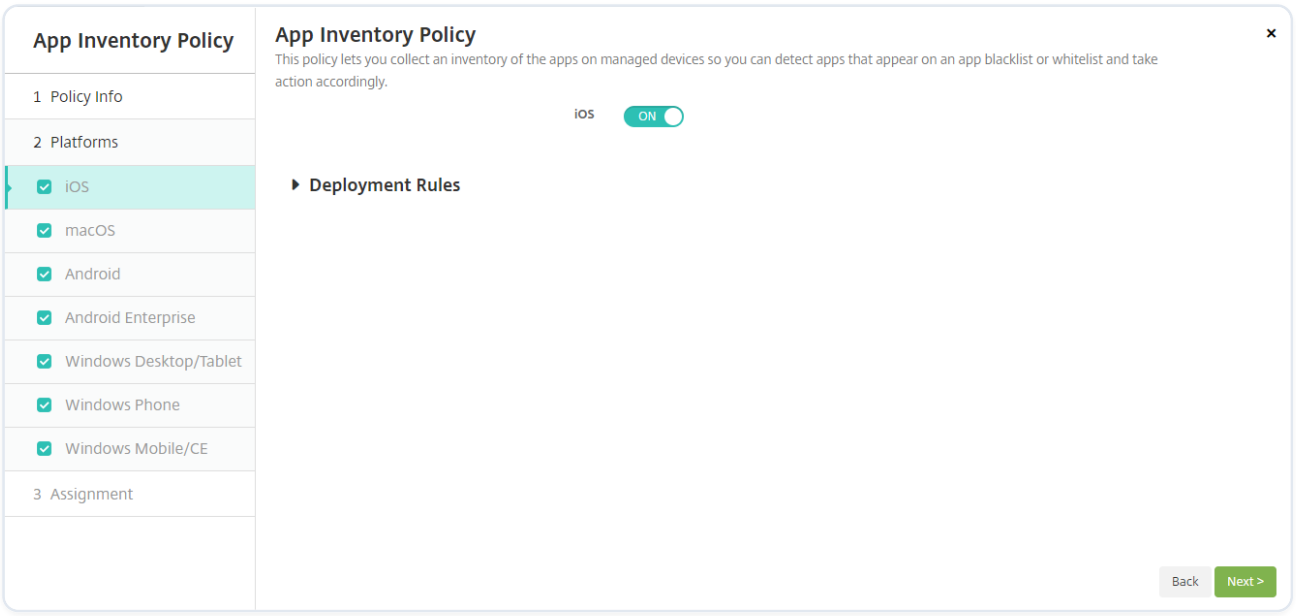
Política de dispositivo de inventário de aplicativos

A política de inventário de aplicativos permite coletar um inventário dos aplicativos em dispositivos gerenciados. O XenMobile® pode então comparar o inventário com quaisquer políticas de acesso a aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que aparecem em uma lista de permissão ou bloqueio de aplicativos e agir corretamente.

Você pode criar políticas de acesso a aplicativos para dispositivos iOS, macOS, Android, Android Enterprise ou Windows Desktop/Tablet.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma



- Para cada plataforma selecionada, mantenha a configuração padrão ou altere a configuração para **Desativado**. O padrão é **Ativado**.

Política de bloqueio de aplicativo do dispositivo

A política de bloqueio de aplicativo do dispositivo define uma lista de aplicativos que têm permissão para serem executados em um dispositivo, ou uma lista de aplicativos que são impedidos de serem executados em um dispositivo. Você pode configurar esta política para dispositivos iOS e Android, mas a forma exata como a política funciona difere para cada plataforma. Por exemplo, você não pode bloquear vários aplicativos em um dispositivo iOS.

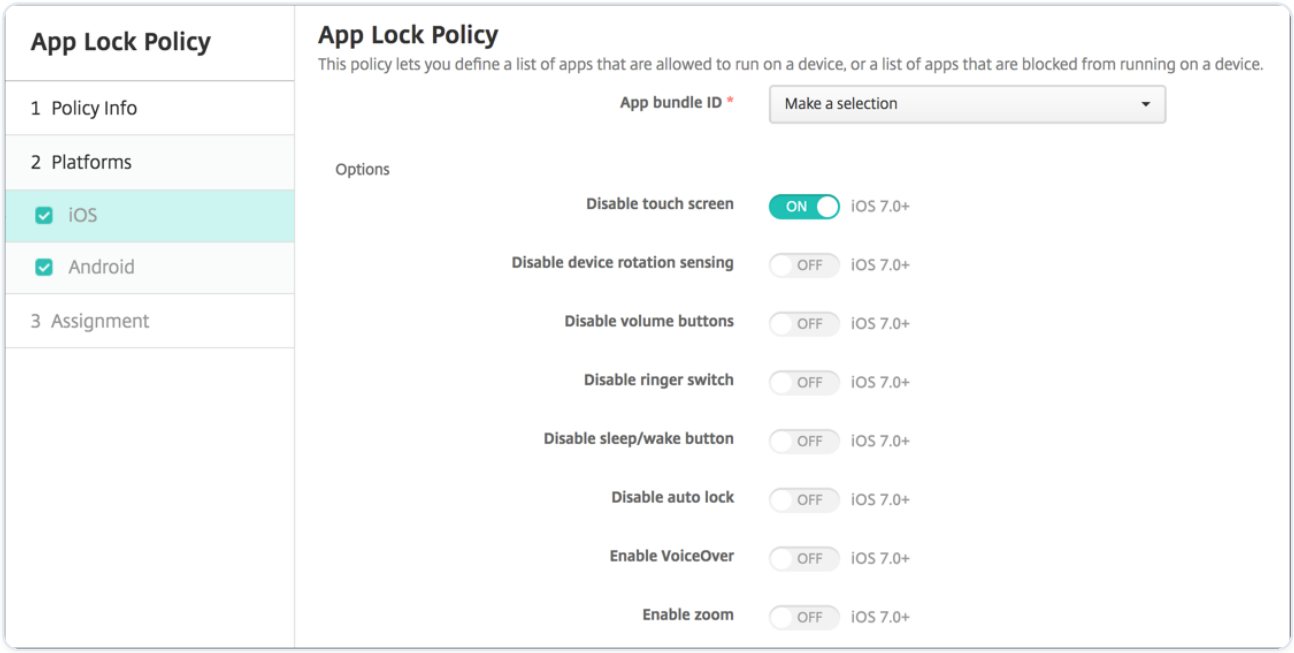
Da mesma forma, para dispositivos iOS, você pode selecionar apenas um aplicativo iOS por política. Isso significa que os usuários só podem usar seu dispositivo para executar um único aplicativo. Eles não podem realizar outras atividades no dispositivo, exceto as opções que você permite especificamente quando a política de bloqueio de aplicativo é aplicada.

Além disso, os dispositivos iOS devem ser supervisionados para aplicar políticas de Bloqueio de Aplicativo.

Embora a política de dispositivo funcione na maioria dos dispositivos Android L e M, o bloqueio de aplicativo não funciona em dispositivos Android N ou posteriores porque o Google descontinuou a API necessária.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **ID do pacote do aplicativo:** Clique no aplicativo na lista suspensa ao qual esta política se aplica ou clique em **Adicionar novo** para adicionar um aplicativo à lista. Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo que aparece.
- **Opções:** Cada uma das seguintes opções se aplica apenas ao iOS 7.0 ou posterior. Para cada opção, o padrão é **Desativado**, exceto para Desativar tela sensível ao toque, que tem como padrão **Ativado**.
    - Desativar tela sensível ao toque
    - Desativar detecção de rotação do dispositivo
    - Desativar botões de volume
    - Desativar botão de toque

      Quando o Desativar botão de toque está **Ativado**, o comportamento do toque depende da posição em que o botão estava quando foi desativado pela primeira vez.
    - Desativar botão de suspensão/ativação
    - Desativar bloqueio automático
    - Desativar VoiceOver
    - Ativar zoom
    - Ativar inversão de cores
    - Ativar AssistiveTouch
    - Ativar seleção de fala

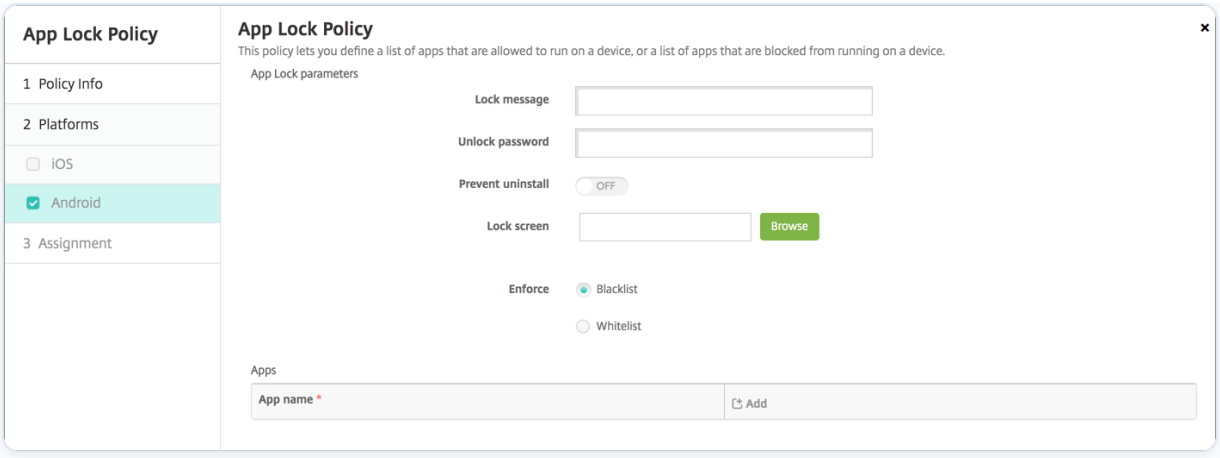
- Ativar áudio mono

- **Opções Habilitadas pelo Usuário:** Cada uma das opções a seguir se aplica apenas ao iOS 7.0 ou posterior. Para cada opção, o padrão é **Desativado**.
  - Permitir ajuste do VoiceOver
  - Permitir ajuste do zoom
  - Permitir ajuste de inversão de cores
  - Permitir ajuste do AssitiveTouch

- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do Android

> **Nota:**
>
> Não é possível bloquear o aplicativo Configurações do Android usando a política de dispositivo Bloqueio de Aplicativo.



- **Parâmetros de Bloqueio de Aplicativo**

- **Mensagem de bloqueio:** Digite uma mensagem que os usuários veem quando tentam abrir um aplicativo bloqueado.
- **Senha de desbloqueio:** Digite a senha para desbloquear o aplicativo.
- **Impedir desinstalação:** Selecione se os usuários têm permissão para desinstalar aplicativos. O padrão é **Desativado**.
- **Tela de bloqueio:** Selecione a imagem que aparece na tela de bloqueio do dispositivo clicando em Procurar e navegando até o local do arquivo.
- **Impor:** Clique em **Lista Negra** para criar uma lista de aplicativos que não têm permissão para serem executados em dispositivos ou clique em **Lista Branca** para criar uma lista de aplicativos que têm permissão para serem executados em dispositivos.

> **Nota:**
>
> O console do XenMobile® Server inclui os termos "lista negra" e "lista branca". Estamos alterando esses termos em uma próxima versão para "lista de bloqueio" e "lista de permissão".

- **Aplicativos:** Clique em **Adicionar** e, em seguida, faça o seguinte:
  - **Nome do aplicativo:** Clique no nome do aplicativo na lista suspensa para adicionar às listas de permissão ou bloqueio, ou clique em **Adicionar novo** para adicionar um aplicativo à lista de aplicativos disponíveis.
  - Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo que aparece.
  - Clique em **Salvar** ou **Cancelar**.
  - Repita estas etapas para cada aplicativo que você deseja adicionar às listas de permissão ou bloqueio.

Política de dispositivo de uso de rede de aplicativos

Você pode definir regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares em dispositivos iOS. As regras se aplicam apenas a aplicativos gerenciados. Aplicativos gerenciados são aqueles que você implanta nos dispositivos dos usuários por meio do XenMobile. Eles não incluem aplicativos que os usuários baixaram diretamente para seus dispositivos sem serem implantados por meio do XenMobile ou aqueles

aplicativos que já estão instalados nos dispositivos quando os dispositivos foram registrados no XenMobile.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

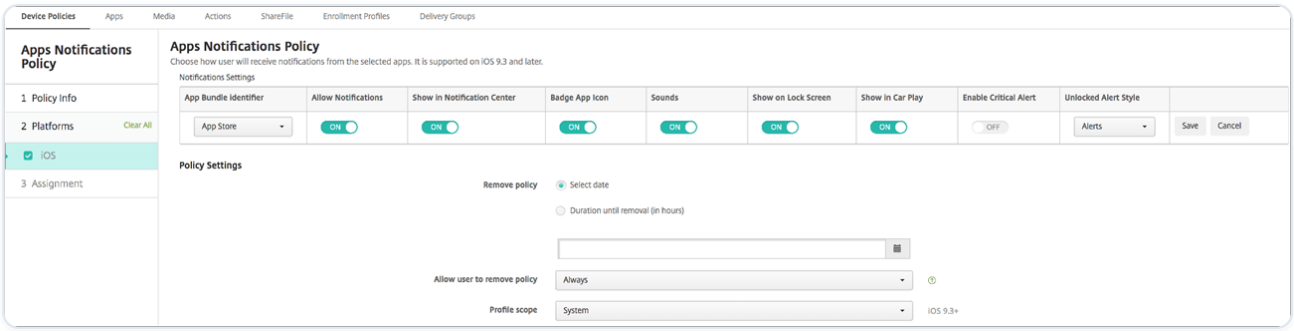
- **Permitir dados celulares em roaming:** Selecione se os aplicativos especificados podem usar uma conexão de dados celulares durante o roaming. O padrão é **Desativado**.
- **Permitir dados celulares:** Selecione se os aplicativos especificados podem usar uma conexão de dados celulares. O padrão é **Desativado**.
- **Correspondências de Identificador de Aplicativo:** Para cada aplicativo que você deseja adicionar à lista, clique em **Adicionar** e, em seguida, faça o seguinte:
  - **Identificador de Aplicativo:** Insira um identificador de aplicativo.
  - Clique em **Salvar** para salvar o aplicativo na lista ou em **Cancelar** para não salvar o aplicativo na lista.

Política de dispositivo de notificações de aplicativos

A política de notificações de aplicativos permite controlar como os usuários do iOS recebem notificações de aplicativos especificados. Esta política é compatível com dispositivos que executam iOS 9.3 ou posterior.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **Identificador do Pacote do Aplicativo:** Especifique os aplicativos aos quais você deseja aplicar esta política.
- **Permitir Notificações:** Selecione **Ativado** para permitir notificações.

- **Mostrar na Central de Notificações:** Selecione **Ativado** para mostrar notificações na central de notificações do dispositivo do usuário.
- **Ícone do Aplicativo com Selo:** Selecione **Ativado** para mostrar um ícone do aplicativo com selo com notificações.
- **Sons:** Selecione **Ativado** para incluir sons com as notificações.
- **Mostrar na Tela Bloqueada:** Selecione **Ativado** para mostrar notificações na tela bloqueada dos dispositivos do usuário.
- **Mostrar no CarPlay:** Se **Ativado**, as notificações são exibidas no Apple CarPlay. Disponível no iOS 12 e posterior. O padrão é **Ativado**.
- **Habilitar Alerta Crítico:** Se **Ativado**, um aplicativo pode marcar uma notificação como uma notificação crítica que ignora as configurações de Não Perturbe e toque. Disponível no iOS 12 e posterior. O padrão é **Desativado**.
- **Estilo de Alerta Desbloqueado:** Na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.
- **Configurações da política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
    - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Sistema**. Esta opção está disponível apenas no iOS 9.3 e posterior.

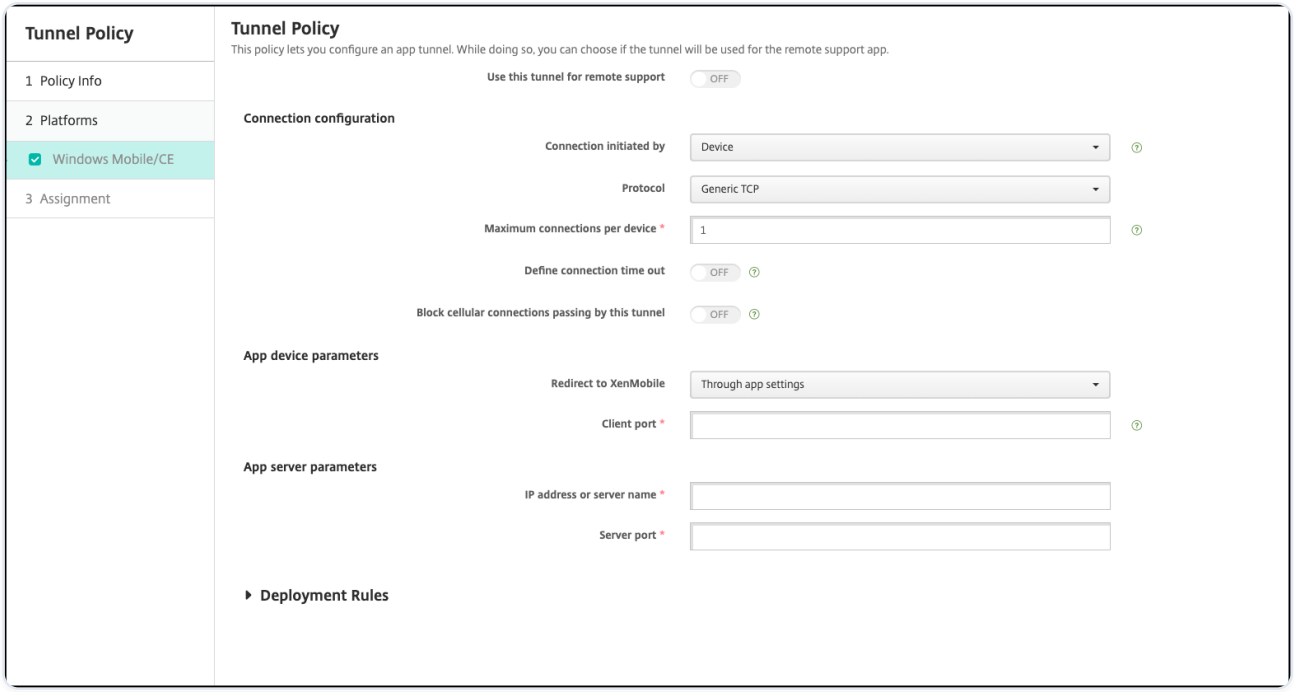
Política de túnel de dispositivo

Túneis de aplicativo (túneis de app) são projetados para aumentar a continuidade do serviço e a confiabilidade da transferência de dados para seus aplicativos móveis. Os túneis de app definem parâmetros de proxy entre o componente cliente de qualquer aplicativo de dispositivo móvel e o componente servidor do aplicativo. Você pode configurar a política de Túnel para dispositivos Android.

Qualquer tráfego de aplicativo enviado através de um túnel que você define nesta política passa pelo XenMobile® antes de ser redirecionado para o servidor que executa o aplicativo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android



- **Conexão iniciada por:** Clique em **Dispositivo** ou **Servidor** para especificar a origem que inicia a conexão.
- **Conexões máximas por dispositivo:** Digite um número para especificar quantas conexões TCP simultâneas o aplicativo pode estabelecer. Este campo se aplica apenas a conexões iniciadas pelo dispositivo.
- **Definir tempo limite de conexão:** Selecione se deseja definir um período de tempo em que um aplicativo pode ficar ocioso antes que o túnel seja fechado.
    - **Tempo limite de conexão:** Se você definir **Definir tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos que um aplicativo pode ficar ocioso antes que o túnel seja fechado.
- **Bloquear conexões celulares que passam por este túnel:** Selecione se este túnel é bloqueado durante o roaming. Conexões Wi-Fi e USB não são bloqueadas.
- **Redirecionar para XenMobile:** Selecione **Através das configurações do aplicativo**.
- **Porta do cliente:** Digite o número da porta do cliente. Geralmente, este valor é o mesmo da porta do servidor.
- **Endereço IP ou nome do servidor:** Digite o endereço IP ou o nome do servidor do aplicativo. Este campo se aplica apenas a conexões iniciadas pelo dispositivo.

- **Porta do servidor:** Digite o número da porta do servidor.

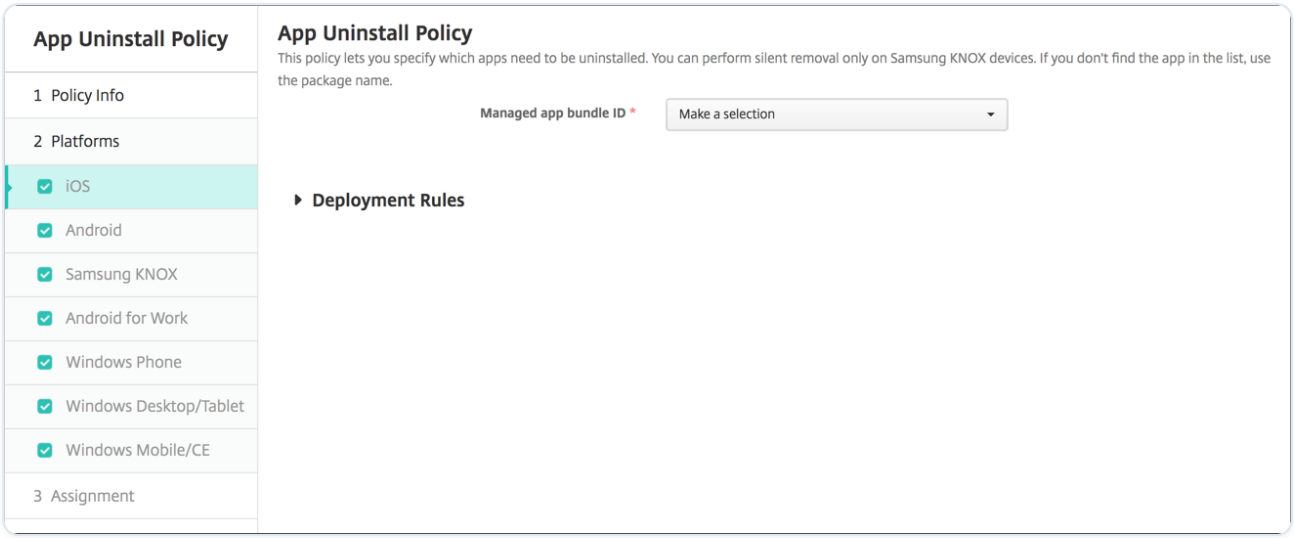
Política de desinstalação de apps

Você pode criar uma política de desinstalação de apps para plataformas iOS, Android, Samsung Knox, Android Enterprise e Windows Desktop/Tablet. Uma política de desinstalação de apps permite remover apps de dispositivos de usuário por diversos motivos. Pode ser que você não queira mais oferecer suporte a determinados apps, sua empresa pode querer substituir apps existentes por apps semelhantes de fornecedores diferentes, e assim por diante.

Os apps são removidos quando esta política é implantada nos dispositivos dos usuários. Exceto para dispositivos Samsung Knox, os usuários recebem um prompt para desinstalar o app. Os usuários de dispositivos Samsung Knox não recebem um prompt para desinstalar o app.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **ID do pacote de apps gerenciados:** Clique em um app existente na lista suspensa ou clique em **Adicionar novo**. Se não houver apps configurados para esta plataforma, a lista estará vazia e você deverá adicionar um app.
    - Ao clicar em **Adicionar**, um campo é exibido onde você pode digitar um nome de app.

Todas as outras configurações de plataforma

- **Apps para desinstalar:** Para cada app que você deseja adicionar, clique em **Adicionar** e, em seguida, faça o seguinte:

- **Nome do app:** Clique em um app existente na lista suspensa ou clique em **Adicionar novo** para inserir um novo nome de app. Se não houver apps configurados para esta plataforma, a lista estará vazia e você deverá adicionar novos apps.
- Clique em **Adicionar** para adicionar o app ou clique em **Cancelar** para cancelar a adição do app.

Desinstalar automaticamente um app Enterprise depois que o app correspondente da loja de apps pública for instalado

Você pode configurar o XenMobile® para remover a versão Enterprise dos apps Citrix® após a instalação da versão da loja de apps pública. Esse recurso impede que os dispositivos dos usuários tenham dois ícones de app idênticos após a instalação da versão da loja de apps pública.

Uma condição de implantação para a política de dispositivo de Desinstalação de App aciona o XenMobile para remover apps mais antigos dos dispositivos dos usuários após a instalação da nova versão. Esse recurso está disponível apenas para dispositivos iOS gerenciados conectados a um XenMobile Server no modo empresarial (XME).

Para configurar uma regra de implantação com a condição Nome do aplicativo instalado:

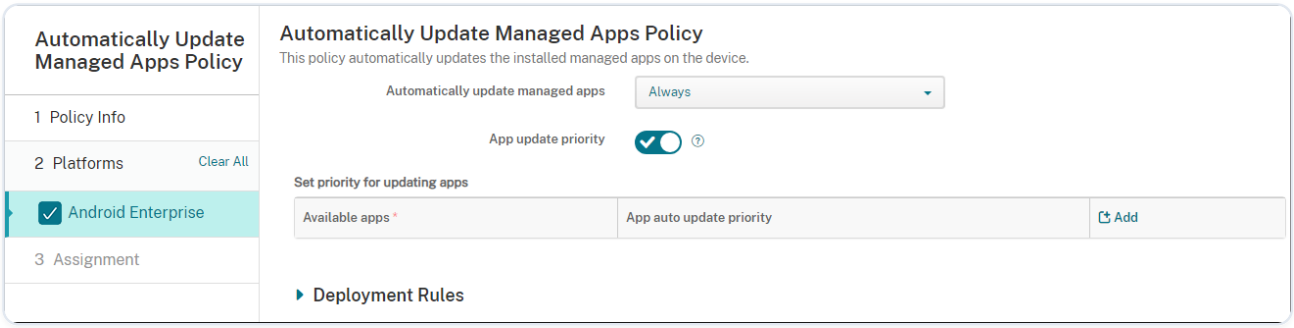
- Especifique o **ID do pacote do aplicativo gerenciado** para o aplicativo Enterprise.
- Adicione uma regra: Clique em **Nova Regra** e, em seguida, como mostrado no exemplo, escolha **Nome do aplicativo instalado** e **é igual a**. Digite o ID do pacote do aplicativo para o aplicativo da loja pública.

No exemplo, quando o aplicativo da loja pública (com.citrix.mail.ios) é instalado em um dispositivo nos grupos de entrega especificados, o XenMobile remove a versão Enterprise (com.citrix.mail).

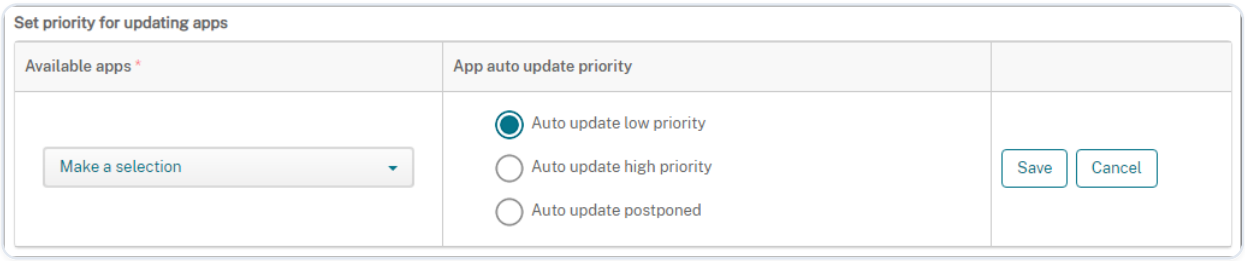
Política de dispositivo para atualização automática de aplicativos gerenciados

Esta política controla como os aplicativos gerenciados instalados são atualizados em dispositivos Android Enterprise. Você pode restringir a capacidade dos usuários de permitir atualizações automáticas de aplicativos em seus dispositivos. Se você permitir que os usuários controlem as atualizações automáticas de aplicativos em seus dispositivos, eles definirão as políticas de atualização automática de aplicativos na loja gerenciada do Google Play.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.



- **Atualizar Automaticamente Aplicativos Gerenciados**
  - **Sempre:** Habilita atualizações automáticas de aplicativos. **Sempre** é o padrão.
  - **Permitir que o usuário configure a política:** Permite que o usuário configure a política de atualização automática de aplicativos para o dispositivo na loja gerenciada do Google Play.
  - **Nunca:** Desabilita atualizações automáticas de aplicativos.
  - **Somente quando o dispositivo estiver conectado ao Wi-Fi:** Permite atualizações automáticas de aplicativos somente quando o dispositivo estiver conectado ao Wi-Fi.
- **Prioridade de atualização de aplicativo:** Se **Ativado**, você pode configurar um nível de prioridade de atualização para cada aplicativo gerenciado.
- **Definir prioridade para atualização de aplicativos:** Clique em **Adicionar** para configurar a prioridade de atualização para um aplicativo.



- **Aplicativos disponíveis:** Selecione um aplicativo no menu para configurar a prioridade de atualização.
- **Prioridade de atualização automática de aplicativo:** Selecione uma prioridade de atualização entre as seguintes:
  - **Atualização automática de baixa prioridade:** O aplicativo é atualizado quando o dispositivo está carregando, não está sendo usado ativamente e está conectado a uma rede não medida.
  - **Atualização automática de alta prioridade:** O aplicativo é atualizado o mais rápido possível, sem restrições.

    - **Atualização automática adiada:** O aplicativo não é atualizado automaticamente por um máximo de 90 dias após uma nova versão estar disponível. Após 90 dias, o aplicativo é atualizado automaticamente com baixa prioridade. Após a atualização do aplicativo, ele não é atualizado automaticamente por mais 90 dias. O usuário pode atualizar o aplicativo manualmente a qualquer momento.

- Clique em **Salvar** quando terminar. Você pode editar uma configuração clicando no ícone de lápis. Exclua a configuração clicando na lixeira.

Política de dispositivo BitLocker

O Windows 10 e o Windows 11 incluem um recurso de criptografia de disco chamado BitLocker, que oferece proteções extras de arquivos e sistema contra acesso não autorizado a um dispositivo Windows perdido ou roubado. Para maior proteção, você pode usar o BitLocker com chips Trusted Platform Module (TPM), versão 1.2 ou posterior. Um chip TPM lida com operações criptográficas e gera, armazena e limita o uso de chaves criptográficas.

A partir do Windows 10, build 1703, as políticas MDM podem controlar o BitLocker. Você usa a política de dispositivo BitLocker no XenMobile® para configurar as definições disponíveis no assistente do BitLocker em dispositivos Windows 10 e Windows 11. Por exemplo, em um dispositivo com o BitLocker ativado, o BitLocker pode solicitar aos usuários como eles desejam desbloquear sua unidade na inicialização, como fazer backup de sua chave de recuperação e como desbloquear uma unidade fixa. As configurações da política de dispositivo BitLocker também configuram se devem:

- Ativar o BitLocker em dispositivos sem um chip TPM.
- Mostrar opções de recuperação na interface do BitLocker.
- Negar acesso de gravação a uma unidade fixa ou removível quando o BitLocker não estiver ativado.

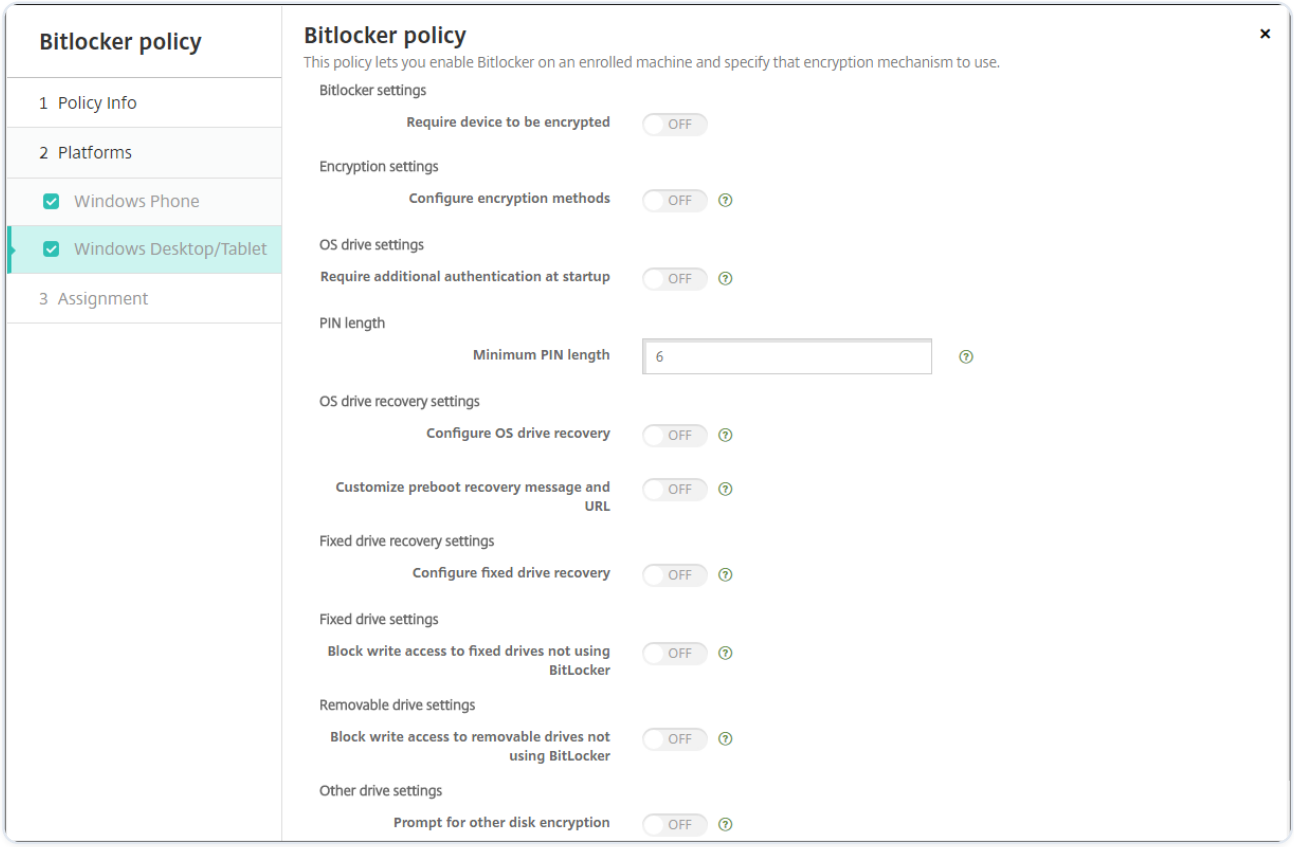
> **Nota:**
>
> Depois que a criptografia BitLocker é iniciada em um dispositivo, você não pode alterar as configurações do BitLocker no dispositivo posteriormente implantando uma política de dispositivo BitLocker atualizada.

> Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Requisitos

- A política de dispositivo BitLocker requer a edição Windows 10 ou Windows 11 Enterprise.
- Antes de implantar a política de dispositivo BitLocker, prepare seu ambiente para o uso do BitLocker. Para obter informações detalhadas da Microsoft, incluindo requisitos de sistema e configuração do BitLocker, consulte BitLocker e os artigos sob esse nó.

Configurações de Desktop e Tablet Windows



- **Exigir que o dispositivo seja criptografado:** Determina se os usuários devem ser solicitados a ativar a criptografia BitLocker no Desktop ou Tablet Windows. Se **Ativado**, o dispositivo exibe uma mensagem após a conclusão do registro, indicando que a empresa exige a criptografia do dispositivo. Se **Desativado**, o usuário não é solicitado e o BitLocker usa as configurações da política. O padrão é **Desativado**.
- **Configurar métodos de criptografia:** Determina os métodos de criptografia a serem usados para tipos de unidade específicos. Se **Desativado**, o assistente do BitLocker solicita ao usuário o método de criptografia a ser usado para um tipo de unidade. O método de criptografia para todas as unidades padrão é XTS-AES de 128 bits. O método de criptografia

para unidades removíveis padrão é AES-CBC de 128 bits. Se **Ativado**, o BitLocker usa o método de criptografia especificado na política. Se **Ativado**, estas configurações extras aparecem: **Unidade do sistema operacional**, **Unidade fixa** e **Unidade removível**. Escolha o método de criptografia padrão para cada tipo de unidade. O padrão é **Desativado**.

- **Exigir autenticação adicional na inicialização:** Especifica a autenticação adicional exigida durante a inicialização do dispositivo. Também especifica se deve permitir o BitLocker em dispositivos que não possuem um chip TPM. Se **Desativado**, dispositivos sem TPM não podem usar a criptografia BitLocker. Para obter informações sobre TPM, consulte o artigo da Microsoft, Visão geral da tecnologia Trusted Platform Module. Se **Ativado**, as seguintes configurações extras aparecem. O padrão é **Desativado**.

  - **Bloquear BitLocker em dispositivos sem chip TPM:** Em um dispositivo sem chip TPM, o BitLocker exige que os usuários criem uma senha de desbloqueio ou uma chave de inicialização. A chave de inicialização é armazenada em uma unidade USB, que o usuário deve conectar ao dispositivo antes da inicialização. A senha de desbloqueio tem um mínimo de oito caracteres. O padrão é **Desativado**.
  - **Inicialização do TPM:** Em um dispositivo com TPM, existem quatro modos de desbloqueio: Somente TPM, TPM + PIN, TPM + Chave e TPM + PIN + Chave. A inicialização do TPM é para o modo Somente TPM, no qual as chaves de criptografia são armazenadas no chip TPM. Este modo não exige que o usuário forneça mais dados de desbloqueio. O dispositivo do usuário desbloqueia automaticamente durante a reinicialização, usando a chave de criptografia do chip TPM. O padrão é **Permitir TPM**.
  - **PIN de inicialização do TPM:** Esta configuração é o modo de desbloqueio TPM + PIN. Um PIN pode ter até 20 dígitos. Use a configuração **Comprimento mínimo do PIN** para especificar o comprimento mínimo do PIN. Um usuário configura um PIN durante a configuração do BitLocker e fornece o PIN durante a inicialização do dispositivo.
  - **Chave de inicialização do TPM:** Esta configuração é o modo de desbloqueio TPM + Chave. A chave de inicialização é armazenada em uma unidade USB ou outra unidade removível, que o usuário deve conectar ao dispositivo antes da inicialização.
  - **Chave de inicialização e PIN do TPM:** Esta configuração é o modo de desbloqueio TPM + PIN + Chave.

    Se o desbloqueio for bem-sucedido, o sistema operacional começa a carregar. Se o desbloqueio falhar, o dispositivo entra no modo de recuperação.

- **Comprimento mínimo do PIN:** O comprimento mínimo do PIN de inicialização do TPM. O padrão é **6**.

- **Configurar recuperação da unidade do SO:** Se a etapa de desbloqueio falhar, o BitLocker solicitará ao usuário a chave de recuperação configurada. Esta configuração configura as opções de recuperação da unidade do sistema operacional disponíveis para os usuários se eles não tiverem a senha de desbloqueio ou a chave de inicialização USB. O padrão é **Desativado**.
    - **Permitir agente de recuperação de dados baseado em certificado:** Especifica se deve permitir um agente de recuperação de dados baseado em certificado. Adicione um agente de recuperação de dados das Políticas de Chave Pública, que está no Console de Gerenciamento de Política de Grupo (GPMC) ou no Editor de Política de Grupo Local. Para obter mais informações sobre agentes de recuperação de dados, consulte o artigo da Microsoft, Configurações de Política de Grupo do BitLocker. O padrão é **Desativado**.
    - **Criar senha de recuperação de 48 bits para recuperação da unidade do SO:** Especifica se deve permitir ou exigir que os usuários usem uma senha de recuperação. O BitLocker gera a senha e a armazena em um arquivo ou conta da Microsoft Cloud. O padrão é **Permitir senha de 48 dígitos**.
    - **Criar chave de recuperação de 256 bits:** Especifica se deve permitir ou exigir que os usuários usem uma chave de recuperação. Uma chave de recuperação é um arquivo BEK, que é armazenado em uma unidade USB. O padrão é **Permitir chave de recuperação de 256 bits**.
    - **Ocultar opções de recuperação da unidade do SO:** Especifica se deve mostrar ou ocultar as opções de recuperação na interface do BitLocker. Se **Ativado**, nenhuma opção de recuperação aparece na interface do BitLocker. Nesse caso, registre o dispositivo no Active Directory, salve as opções de recuperação no Active Directory e defina **Salvar informações de recuperação no AD DS** como **Ativado**. O padrão é **Desativado**.
    - **Salvar informações de recuperação no AD DS:** Especifica se deve salvar as opções de recuperação nos Serviços de Domínio do Active Directory. O padrão é **Desativado**.
    - **Configurar informações de recuperação armazenadas no AD DS:** Especifica se o BitLocker deve armazenar a senha de recuperação ou a senha de recuperação e o pacote de chaves nos Serviços de Domínio do Active Directory. O armazenamento do pacote de chaves oferece suporte à recuperação de dados de uma unidade fisicamente corrompida. O padrão é **Fazer backup da senha de recuperação**.
    - **Habilitar BitLocker após armazenar informações de recuperação no AD DS:** Especifica se deve impedir que os usuários habilitem o BitLocker, a menos que o dispositivo esteja conectado ao domínio e o backup das informações de recuperação do

BitLocker no Active Directory seja bem-sucedido. Se **Ativado**, um dispositivo deve ser ingressado no domínio antes de iniciar o BitLocker. O padrão é **Desativado**.

- **Personalizar mensagem e URL de recuperação de pré-inicialização:** Especifica se o BitLocker mostra uma mensagem e URL personalizados na tela de recuperação. Se **Ativado**, as seguintes configurações adicionais aparecem: **Usar mensagem e URL de recuperação padrão**, **Usar mensagem e URL de recuperação vazios**, **Usar mensagem de recuperação personalizada** e **Usar URL de recuperação personalizada**. Se **Desativado**, a mensagem e o URL de recuperação padrão são exibidos. O padrão é **Desativado**.
- **Configurar recuperação de unidade fixa:** Configura as opções de recuperação para usuários de uma unidade fixa criptografada com BitLocker. O BitLocker não exibe uma mensagem aos usuários sobre a criptografia de unidade fixa. Para desbloquear uma unidade durante a inicialização, um usuário fornece uma senha ou cartão inteligente. As configurações de desbloqueio da inicialização, que não estão nesta política, aparecem na interface do BitLocker quando um usuário habilita a criptografia BitLocker em uma unidade fixa. Para obter informações sobre as configurações relacionadas, consulte **Configurar recuperação de unidade do SO**, anteriormente nesta lista. O padrão é **Desativado**.
- **Bloquear acesso de gravação a unidades fixas que não usam BitLocker:** Se **Ativado**, os usuários podem gravar em unidades fixas somente quando essas unidades são criptografadas com BitLocker. O padrão é **Desativado**.
- **Bloquear acesso de gravação a unidades removíveis que não usam BitLocker:** Se **Ativado**, os usuários podem gravar em unidades removíveis somente quando essas unidades são criptografadas com BitLocker. Configure esta configuração de acordo com se sua organização permite acesso de gravação em outras unidades removíveis da organização. O padrão é **Desativado**.
- **Solicitar outra criptografia de disco:** Permite desabilitar o prompt de aviso para outras criptografias de disco em dispositivos. O padrão é **Desativado**.

Política de dispositivo de Calendário (CalDav)

Você pode adicionar uma política de dispositivo no XenMobile® para adicionar uma conta de calendário (CalDAV) aos dispositivos iOS ou macOS dos usuários para permitir que eles sincronizem dados de agendamento com qualquer servidor que suporte CalDAV.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Descrição da conta:** Digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** Digite o endereço do servidor CalDAV. Este campo é obrigatório.
- **Porta:** Digite a porta na qual se conectar ao servidor CalDAV. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** Digite a URL base para o calendário do usuário.
- **Nome de usuário:** Digite o nome de logon do usuário. Este campo é obrigatório.
- **Senha:** Digite uma senha de usuário opcional.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor CalDAV. O padrão é **Ativado**.
- **Configurações da política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** Digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** Digite o endereço do servidor CalDAV. Este campo é obrigatório.
- **Porta:** Digite a porta na qual se conectar ao servidor CalDAV. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** Digite a URL base para o calendário do usuário.
- **Nome de usuário:** Digite o nome de logon do usuário. Este campo é obrigatório.
- **Senha:** Digite uma senha de usuário opcional.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor CalDAV. O padrão é **Ativado**.
- **Configurações da política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**

- **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
- **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

- **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seu dispositivo. Selecione **Sempre**, **Requer senha** ou **Nunca** no menu. Se você selecionar **Requer senha**, digite uma senha no campo **Senha de remoção**.
- **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Política de dispositivo celular

Esta política permite configurar as definições de rede celular num dispositivo iOS.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Definições do iOS

- **APN de Anexo**
  - **Nome:** Um nome para esta configuração.
  - **Tipo de autenticação:** Clique em Challenge Handshake Authentication Protocol (**CHAP**) ou Password Authentication Protocol (**PAP**) na lista suspensa. O padrão é **PAP**.
  - **Nome de usuário** e **Senha:** O nome de usuário e a senha a serem usados para autenticação.
- **APN**
  - **Nome:** Um nome para a configuração do Nome do Ponto de Acesso (APN).
  - **Tipo de autenticação:** Clique em **CHAP** ou **PAP** na lista suspensa. O padrão é **PAP**.
  - **Nome de usuário** e **Senha:** O nome de usuário e a senha a serem usados para autenticação.
  - **Servidor proxy:** O endereço de rede do servidor proxy.
  - **Porta do servidor proxy:** A porta do servidor proxy.

- **Definições da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de agendamento de conexão

> **Importante:**
>
> A Citrix recomenda que você use o Firebase Cloud Messaging (FCM) para controlar as conexões de dispositivos Android, Android Enterprise e Chrome OS para o XenMobile Server. Para obter informações sobre como usar o FCM, consulte Firebase Cloud Messaging.
>
> Se você optar por não usar o FCM, poderá criar políticas de agendamento de conexão para controlar como e quando os dispositivos dos usuários se conectam ao XenMobile® Server.

Você pode especificar que os usuários conectem seus dispositivos manualmente ou que os dispositivos se conectem dentro de um período de tempo definido.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma

- **Exigir que os dispositivos se conectem:** Clique na opção que você deseja definir para este agendamento.
  - **Sempre:** Mantenha a conexão ativa permanentemente. O XenMobile no dispositivo do usuário tenta se reconectar ao XenMobile Server após uma perda de conexão de rede e monitora a conexão transmitindo pacotes de controle em intervalos regulares. A Citrix® recomenda esta opção para segurança otimizada. Ao escolher **Sempre**, use também para o dispositivo **Política de Túnel**, a configuração **Definir tempo limite de conexão** para garantir que a conexão não esteja esgotando a bateria. Ao manter a conexão ativa, você

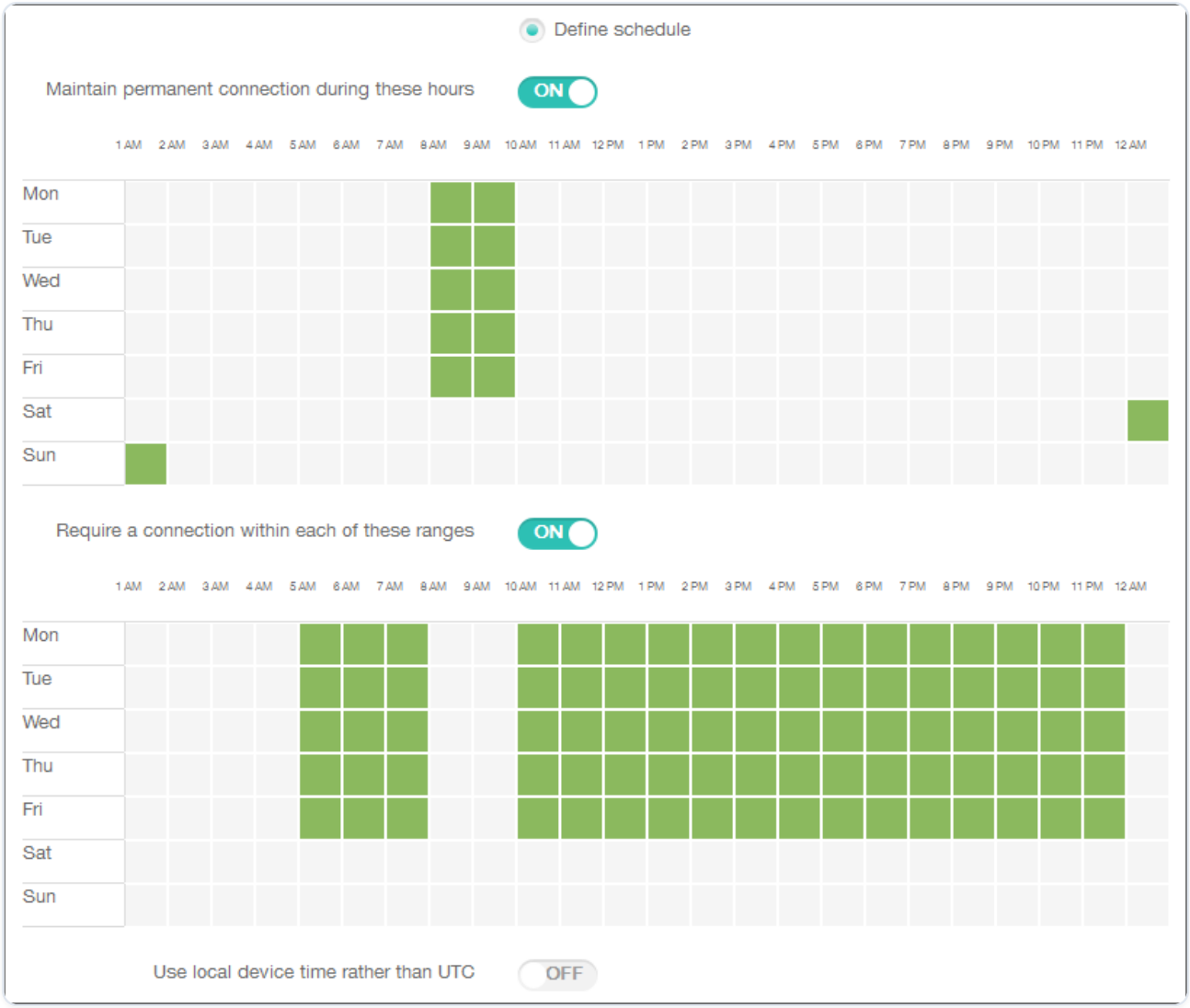
pode enviar comandos de segurança como limpeza ou bloqueio para o dispositivo sob demanda. Você também deve selecionar a opção **Agendamento de Implantação Implantar para conexões sempre ativas** em cada política implantada no dispositivo.

- **Nunca:** Conecte-se manualmente. Os usuários devem iniciar a conexão a partir do XenMobile em seus dispositivos. A Citrix não recomenda esta opção para implantações de produção porque ela impede a implantação de políticas de segurança nos dispositivos, de modo que os usuários nunca recebem novos aplicativos ou políticas.
- **A cada:** Conecte-se no intervalo designado. Quando esta opção está em vigor e você envia uma política de segurança, como um bloqueio ou uma limpeza, o XenMobile processa a ação no dispositivo na próxima vez que o dispositivo se conectar. Ao selecionar esta opção, o campo **Conectar a cada N minutos** aparece, onde você deve inserir o número de minutos após os quais o dispositivo deve se reconectar. O padrão é **20**.
- **Definir agendamento:** Quando ativado, o XenMobile no dispositivo do usuário tenta se reconectar ao XenMobile Server após uma perda de conexão de rede e monitora a conexão transmitindo pacotes de controle em intervalos regulares dentro do período de tempo que você definir. Consulte Definindo um período de tempo de conexão, a seguir, para saber como definir um período de tempo de conexão.
  - **Manter conexão permanente durante estas horas:** Os dispositivos dos usuários devem estar conectados durante o período de tempo definido.
  - **Exigir uma conexão dentro de cada um desses intervalos:** Os dispositivos dos usuários devem estar conectados pelo menos uma vez em qualquer um dos períodos de tempo definidos.
  - **Usar a hora local do dispositivo em vez de UTC:** Sincronize os períodos de tempo definidos com a hora local do dispositivo em vez do Tempo Universal Coordenado (UTC).

Definindo um período de conexão

Ao habilitar as seguintes opções, uma linha do tempo aparece onde você pode definir os períodos que deseja. Você pode habilitar uma ou ambas as opções para exigir uma conexão permanente durante horários específicos ou para exigir uma conexão dentro de determinados períodos. Cada quadrado na linha do tempo representa 30 minutos, então se você quiser uma conexão entre 8:00 AM e 9:00 AM todos os dias da semana, você clica nos dois quadrados na linha do tempo entre 8 AM e 9 AM todos os dias da semana.

Por exemplo, as duas linhas do tempo na figura a seguir exigem uma conexão permanente entre 8:00 AM e 9:00 AM todos os dias da semana, uma conexão permanente entre 12:00 AM de sábado e 1:00 AM de domingo, e pelo menos uma conexão todos os dias da semana entre 5:00 AM e 8:00 AM ou entre 10:00 AM e 11:00 PM.



Política de dispositivo de Contatos (CardDAV)

Você pode adicionar uma política de dispositivo no XenMobile® para adicionar uma conta de contatos (CardDAV) do iOS aos dispositivos iOS ou macOS dos usuários, permitindo que eles sincronizem dados de contato com qualquer servidor que suporte CardDAV.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Descrição da conta:** Digite uma descrição da conta. Este campo é obrigatório.

- **Nome do host:** Digite o endereço do servidor CardDAV. Este campo é obrigatório.
- **Porta:** Digite a porta na qual se conectar ao servidor CardDAV. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** Digite a URL base para o calendário do usuário.
- **Nome de usuário:** Digite o nome de logon do usuário. Este campo é obrigatório.
- **Senha:** Digite uma senha de usuário opcional.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor CardDAV. O padrão é **Ativado**.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** Digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** Digite o endereço do servidor CardDAV. Este campo é obrigatório.
- **Porta:** Digite a porta na qual se conectar ao servidor CardDAV. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** Digite a URL base para o calendário do usuário.
- **Nome de usuário:** Digite o nome de logon do usuário. Este campo é obrigatório.
- **Senha:** Digite uma senha de usuário opcional.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor CardDAV. O padrão é **Ativado**.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.

- **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

- **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
- **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Política de dispositivo de Controle de Atualizações do SO

A política de dispositivo de Controle de Atualizações do SO permite implantar:

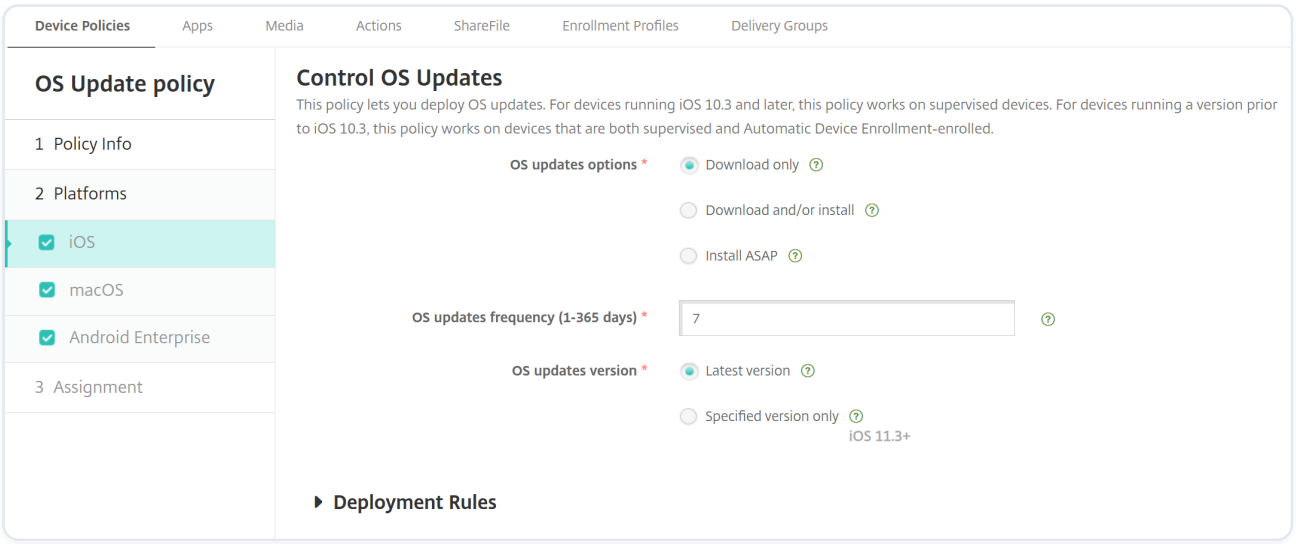
- As atualizações mais recentes do SO para dispositivos iOS supervisionados.

  A política de dispositivo de Atualização do SO funciona apenas para dispositivos supervisionados registrados no Programa de Implantação da Apple.
- As atualizações mais recentes do SO e de aplicativos para dispositivos macOS registrados no DEP executando macOS 10.11.5 e posterior.
- As atualizações mais recentes do SO para dispositivos Android Enterprise Work Managed.

  Para dispositivos Android Enterprise Work Managed, o XenMobile® envia a política de Controle de Atualizações do SO para o Secure Hub, que então aplica a política ao dispositivo. A página **Gerenciar** > **Dispositivos** mostra quando o XenMobile Server envia a política e quando o dispositivo a recebe.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **Opções de atualização do SO:**
  - **Somente download:** Baixe as atualizações mais recentes do SO para dispositivos supervisionados de acordo com a frequência de atualização do SO sem instalá-las.
  - **Baixar e/ou instalar:** Baixe as atualizações mais recentes do SO para dispositivos supervisionados de acordo com a frequência de atualização do SO. O dispositivo solicitará que você instale as atualizações. O prompt fica visível depois que você desbloqueia o dispositivo.
  - **Instalar o mais rápido possível:** Permite instalar imediatamente as atualizações do SO baixadas anteriormente.
- **Frequência de atualização do SO:** Determina com que frequência o XenMobile verifica e atualiza o SO do dispositivo. O padrão é **7** dias.
- **Versão das atualizações do SO:** Especifica a versão do SO a ser usada para atualizar os dispositivos iOS supervisionados. O padrão é **Versão mais recente**.
  - **Versão mais recente:** Selecione para atualizar para a versão mais recente do SO.
  - **Somente versão específica:** Selecione para atualizar para uma versão específica do SO e, em seguida, digite o número da versão. Esta opção é aplicável para iOS 11.3 ou posterior.

Configurações do macOS

Imagem da tela de configuração de Políticas de Dispositivo(/en-us/xenmobile/server/media/control-os-update-macos-platform.png)

- **Opções de atualização do SO:** Ambas as opções baixam as atualizações mais recentes do macOS de acordo com a **frequência de atualização do SO**. Você pode optar por instalar as atualizações ou notificar o usuário através da App Store de que as atualizações estão disponíveis.
- **Frequência de atualização do SO:** Determina com que frequência o XenMobile verifica e atualiza o SO do dispositivo. O padrão é **7** dias.

Obter status para ações de atualização do iOS e macOS

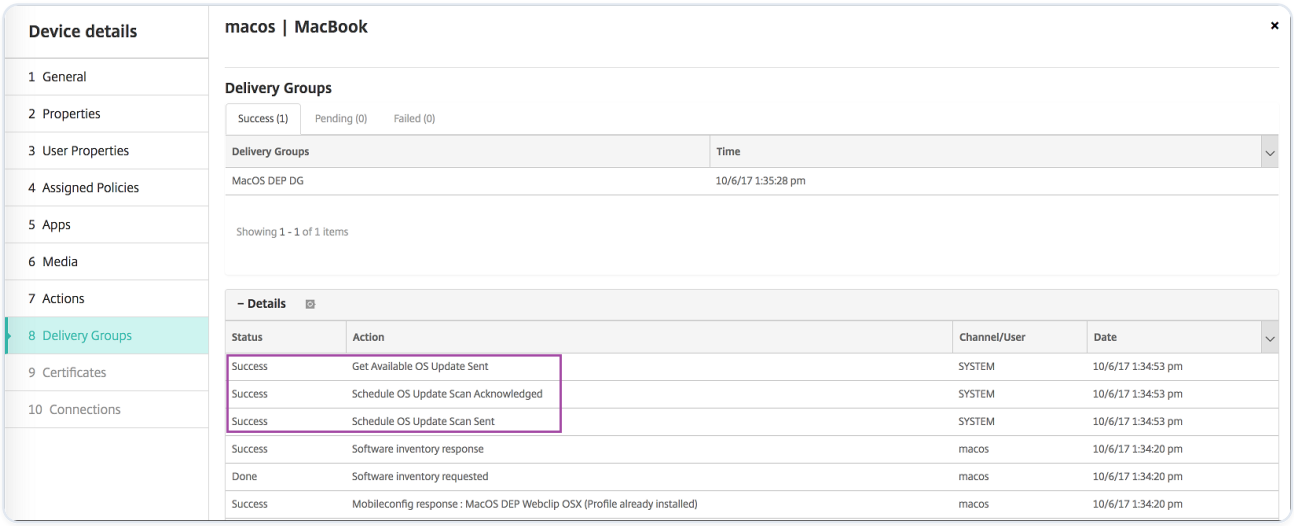
Para iOS e macOS, o XenMobile não implanta a política de Controle de Atualizações do SO nos dispositivos. Em vez disso, o XenMobile usa a política para enviar estes comandos MDM aos dispositivos:

- Agendar Verificação de Atualização do SO: Solicita que o dispositivo faça uma verificação em segundo plano para atualizações do SO. (opcional para iOS)
- Atualizações do SO Disponíveis: Consulta o dispositivo para obter uma lista de atualizações do SO disponíveis.
- Agendar Atualização do SO: Solicita que o dispositivo faça atualizações do macOS, atualizações de aplicativos ou ambos. Assim, o SO do dispositivo determina quando ele deve baixar ou instalar as atualizações do SO e dos aplicativos.

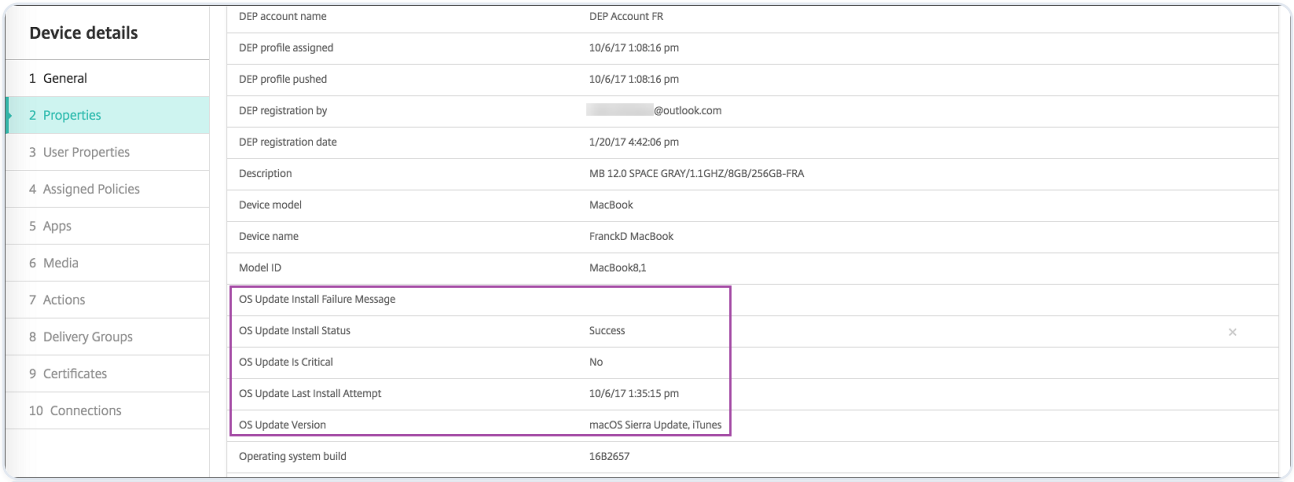
A página **Gerenciar > Dispositivos > Detalhes do dispositivo (Geral)** mostra o status das verificações de atualização do SO agendadas e disponíveis, e das atualizações agendadas do macOS e de aplicativos.

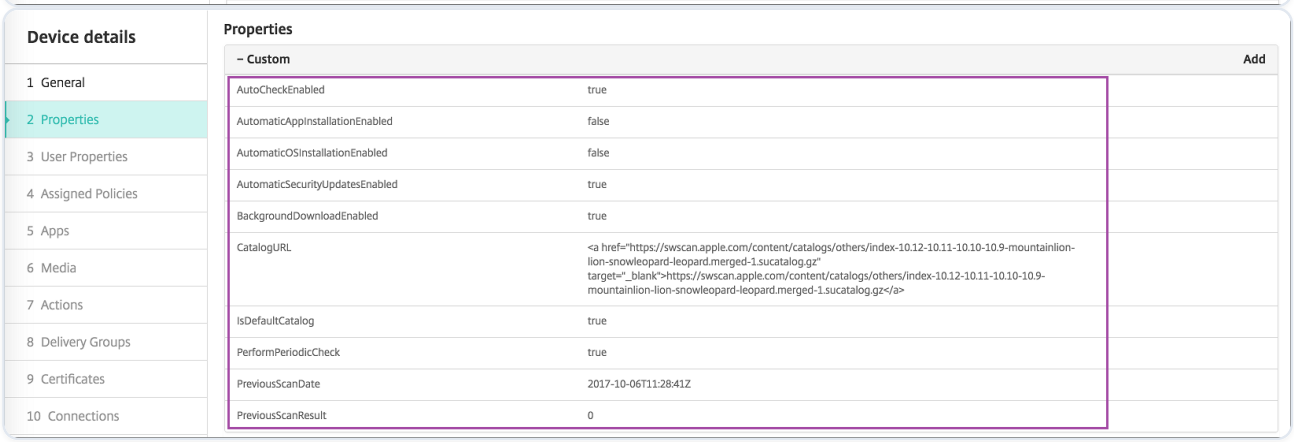
Imagem da tela de detalhes do dispositivo(/en-us/xenmobile/server/media/control-os-update-general.png)

Para mais detalhes sobre o status das ações de atualização, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Grupos de Entrega)**.

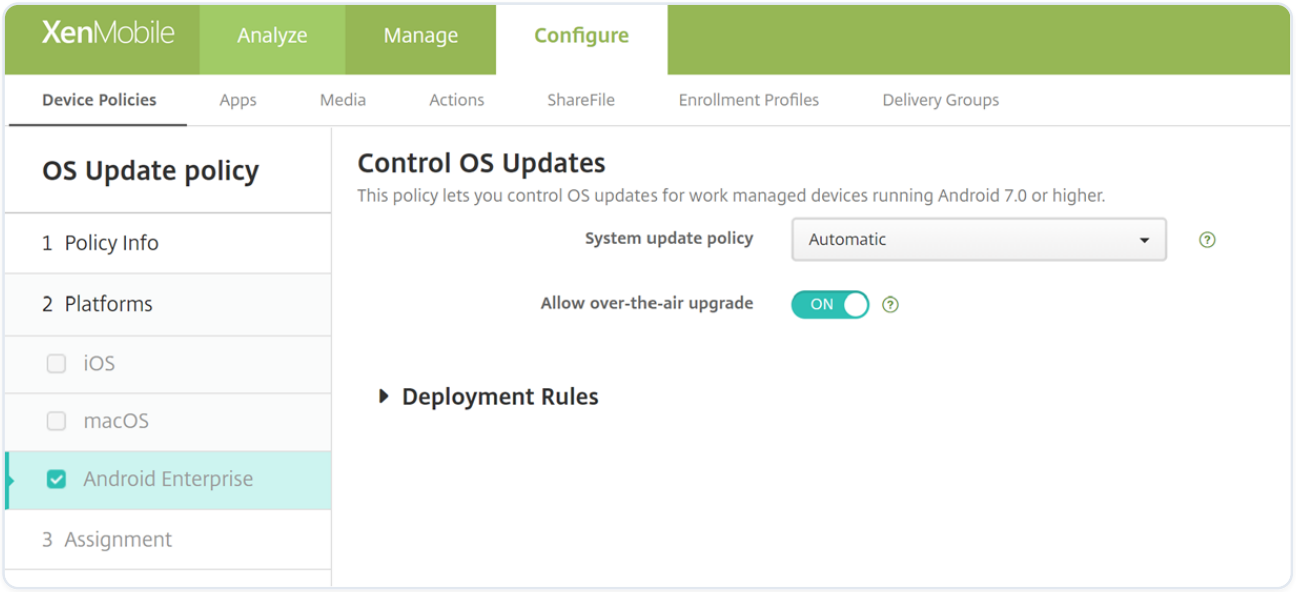


Para detalhes como atualizações de SO disponíveis e a última tentativa de instalação, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Propriedades)**.





Configurações do Android Enterprise



- **Política de atualização do sistema:** Determina quando as atualizações do sistema ocorrem. Se você habilitar a configuração **Control Enterprise FOTA**, as atualizações ocorrerão automaticamente, independentemente da configuração para esta opção.
  - **Automático:** Instala uma atualização quando ela está disponível.
  - **Com janela:** Instala uma atualização automaticamente dentro da janela de manutenção diária especificada em **Hora de início** e **Hora de término**.
    - **Hora de início:** O início da janela de manutenção, medido como o número de minutos (**0** - **1440**) a partir da meia-noite no horário local do dispositivo. O padrão é **0**.
    - **Hora de término:** O fim da janela de manutenção, medido como o número de minutos (**0** - **1440**) a partir da meia-noite no horário local do dispositivo. O padrão é **120**.
  - **Adiar:** Permite que um usuário adie uma atualização por até 30 dias.
  - **Padrão:** Define a política de atualização para o padrão do sistema.
- **Permitir atualização over-the-air:** Se desativado, os dispositivos do usuário não podem receber atualizações de software sem fio. O padrão é **Ativado**.

Política de dispositivo de credenciais

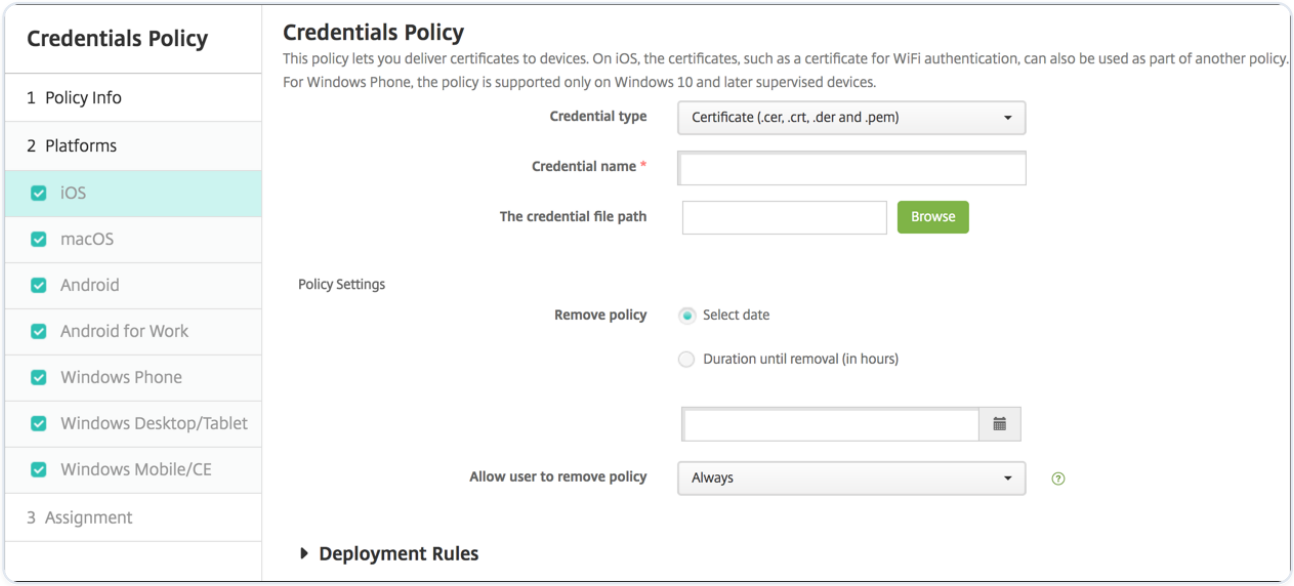
As políticas de dispositivo de credenciais apontam para uma PKI configurada no XenMobile. Por exemplo, sua configuração de PKI pode incluir uma entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor. Para obter mais informações sobre credenciais, consulte Certificados e autenticação.

Cada plataforma suportada requer um conjunto diferente de valores, que são descritos neste artigo.

> **Nota:**
>
> Antes de criar esta política, você precisa das informações de credenciais que planeja usar para cada plataforma, além de quaisquer certificados e senhas.

> Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



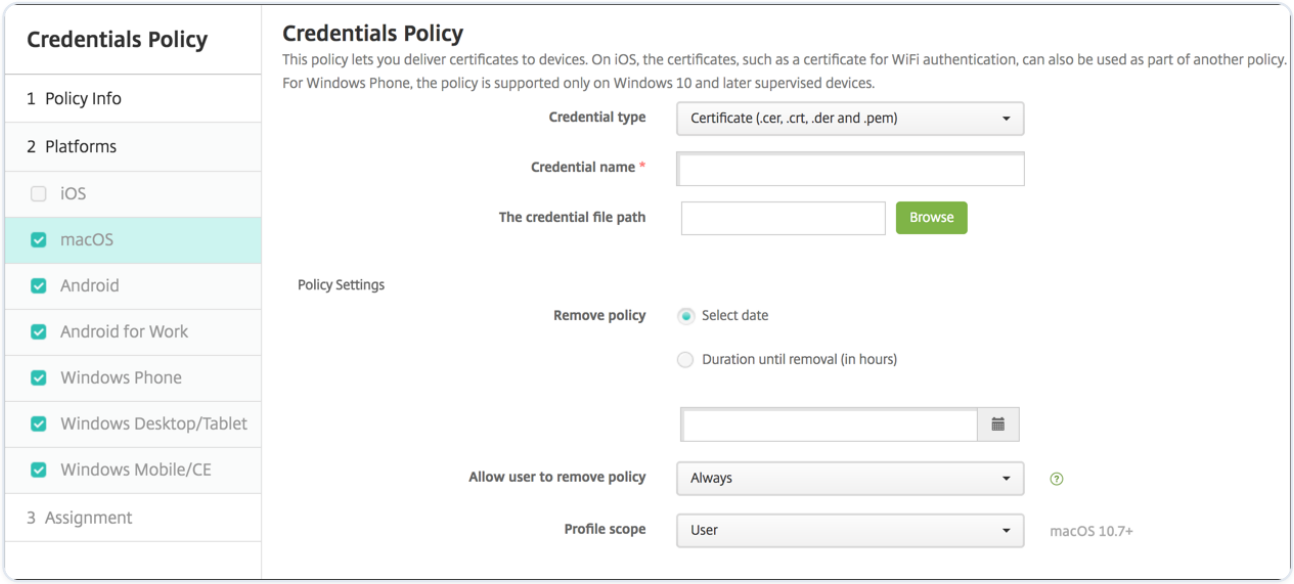
Configure as seguintes configurações:

- **Tipo de credencial:** Clique no tipo de credencial na lista suspensa que você deseja usar com esta política e, em seguida, insira as seguintes informações para a credencial selecionada:
  - **Certificado**
    - **Nome da credencial:** Insira um nome exclusivo para a credencial.
    - **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em Procurar e navegando até o local do arquivo.
  - **Keystore**
    - **Nome da credencial:** Insira um nome exclusivo para a credencial.

    - **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em Procurar e navegando até o local do arquivo.
    - **Senha:** Insira a senha do keystore para a credencial.
  - **Certificado do servidor**
    - **Certificado do servidor:** Clique no certificado na lista suspensa que você deseja usar.
  - **Provedor de credenciais**
    - **Provedor de credenciais:** Clique no nome do provedor de credenciais na lista suspensa.

- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS



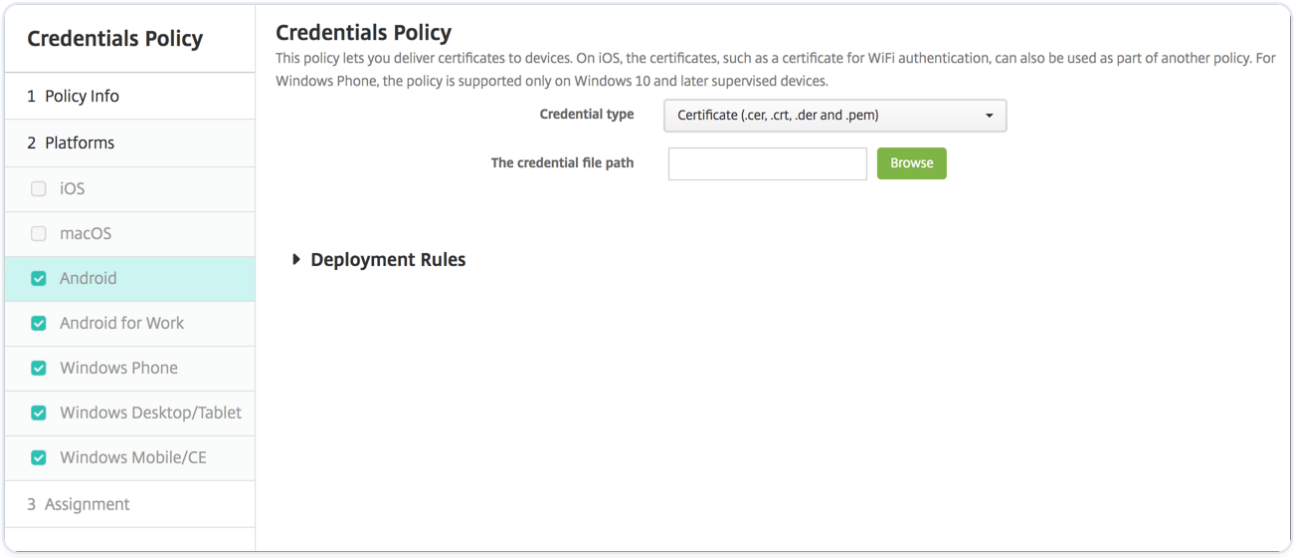
Configure as seguintes configurações:

- **Tipo de credencial:** Clique no tipo de credencial na lista suspensa que você deseja usar com esta política e, em seguida, insira as seguintes informações para a credencial selecionada:

- **Certificado**
  - **Nome da credencial:** Insira um nome exclusivo para a credencial.
  - **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em **Procurar** e navegando até o local do arquivo.
- **Keystore**
  - **Nome da credencial:** Insira um nome exclusivo para a credencial.
  - **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em **Procurar** e navegando até o local do arquivo.
  - **Senha:** Insira a senha do keystore para a credencial.
- **Certificado do servidor**
  - **Certificado do servidor:** Clique no certificado na lista suspensa que você deseja usar.
- **Provedor de credenciais**
  - **Provedor de credenciais:** Clique no nome do provedor de credenciais na lista suspensa.

- **Configurações de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.
  - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

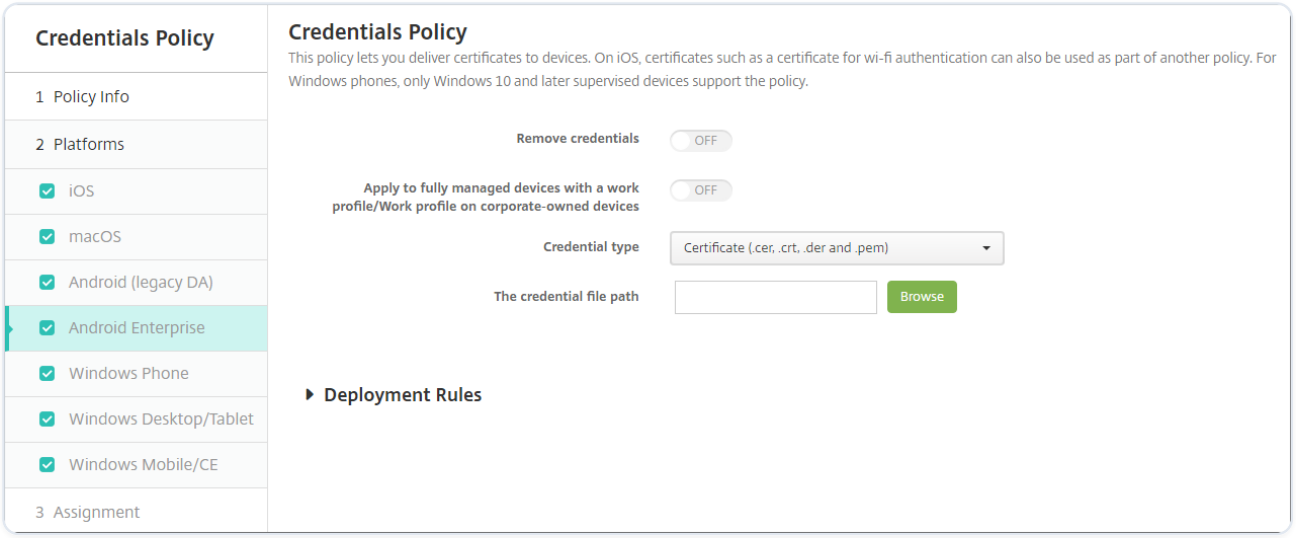
Configurações do Android



Configure as seguintes configurações:

- **Tipo de credencial:** Clique no tipo de credencial na lista suspensa que você deseja usar com esta política e, em seguida, insira as seguintes informações para a credencial selecionada:
  - **Certificado**
    - **Nome da credencial:** Digite um nome exclusivo para a credencial.
    - **Caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em Procurar e, em seguida, navegando até o local do arquivo.
  - **Keystore**
    - **Nome da credencial:** Digite um nome exclusivo para a credencial.
    - **Caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
    - **Senha:** Digite a senha do keystore para a credencial.
  - **Certificado do servidor**
    - **Certificado do servidor:** Clique no certificado na lista suspensa que você deseja usar.
  - **Provedor de credenciais**
    - **Provedor de credenciais:** Clique no nome do provedor de credenciais na lista suspensa.

Configurações do Android Enterprise



Configure estas definições para determinar como o XenMobile® aplica as definições de credenciais:

- **Remover credenciais:** Defina como **Ativado** para configurar as seguintes definições. O padrão é **Desativado**.
    - **Remover credenciais de usuário:** Remove certificados do armazenamento de chaves gerenciado. O padrão é **Desativado**.
    - **Remover certificados raiz confiáveis:** Desinstala todos os certificados de CA não pertencentes ao sistema. O padrão é **Desativado**.
- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa:** Permite configurar as definições da política de credenciais para dispositivos totalmente gerenciados com perfis de trabalho. Quando esta definição está **Ativada**, as definições de credenciais que você configura se aplicam apenas ao perfil de trabalho. Quando esta definição está **Desativada**, as definições de credenciais que você configura se aplicam apenas ao dispositivo. O padrão é **Desativado**.

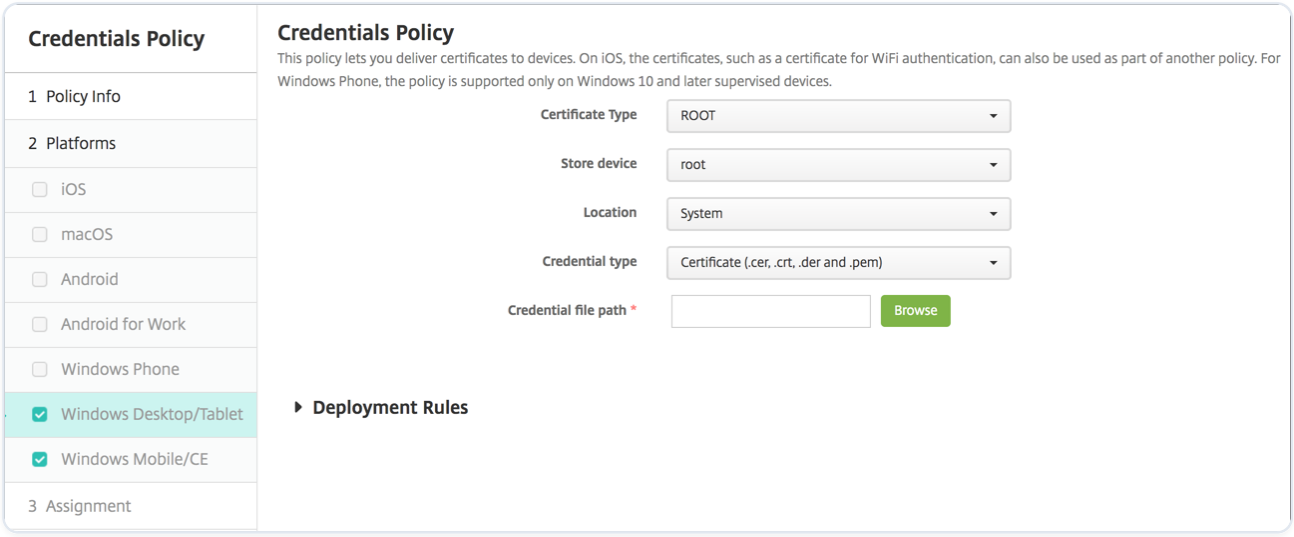
Configure as definições de credenciais:

- **Tipo de credencial:** Clique no tipo de credencial na lista suspensa que você deseja usar com esta política e, em seguida, insira as seguintes informações para a credencial selecionada:
    - **Certificado**
        - **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
    - **Keystore**

- **O caminho do arquivo de credencial:** Selecione o arquivo de credencial clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
- **Alias do certificado:** Um alias de certificado facilita o acesso dos aplicativos ao certificado. Configure um alias de certificado na política de dispositivo de Configuração Gerenciada. Em seguida, digite o alias no campo **Alias do certificado** na política de dispositivo de Credenciais. Os aplicativos recuperam o certificado e autenticar a VPN sem qualquer ação dos usuários.
- **Senha:** Digite a senha do keystore para a credencial.

- **Certificado do servidor**
  - **Certificado do servidor:** Clique no certificado na lista suspensa que você deseja usar.
- **Provedor de credenciais**
  - **Alias do certificado:** Um alias de certificado facilita o acesso dos aplicativos ao certificado. Configure um alias de certificado na política de dispositivo de Configuração Gerenciada. Em seguida, digite o alias no campo **Alias do certificado** na política de dispositivo de Credenciais. Os aplicativos recuperam o certificado e autenticar a VPN sem qualquer ação dos usuários.
  - **Provedor de credenciais:** Clique no nome do provedor de credenciais na lista suspensa.
  - **Aplicativos para usar certificados:** Para especificar aplicativos que têm acesso silencioso às credenciais deste provedor: Clique em **Adicionar**, selecione um aplicativo e clique em **Salvar**.

Configurações de Desktop/Tablet Windows



- **Tipo de certificado:** Clique em **ROOT** ou **CLIENT** na lista suspensa.
- Se você clicar em **ROOT**, configure estas configurações:
  - **Dispositivo de armazenamento:** Clique em **root**, **My** ou **CA** na lista suspensa para o local do armazenamento de certificados para a credencial. **My** armazena o certificado nos armazenamentos de certificados dos usuários.
  - **Localização:** Para tablets Windows 10 e Windows 11, **Sistema** é o único local.
  - **Tipo de credencial:** Para tablets Windows 10 e Windows 11, **Certificado** é o único tipo de credencial.
  - **Caminho do arquivo de credencial:** Selecione o arquivo de certificado clicando em **Procurar** e navegando até o local do arquivo.
- Se você clicar em **CLIENTE**, configure estas configurações:
- **Local:** Para tablets Windows 10 e Windows 11, **Sistema** é o único local.
- **Tipo de credencial:** Para tablets Windows 10 e Windows 11, **Keystore** é o único tipo de credencial.
- **Nome da credencial:** Digite o nome da credencial. Este campo é obrigatório.
- **Caminho do arquivo de credencial:** Selecione o arquivo de certificado clicando em **Procurar** e navegando até o local do arquivo.
- **Senha:** Digite a senha associada à credencial. Este campo é obrigatório.

Política de dispositivo XML personalizada

Você pode criar políticas XML personalizadas no XenMobile® para personalizar os seguintes recursos em dispositivos Windows compatíveis:

- Provisionamento, que inclui a configuração do dispositivo e a ativação ou desativação de recursos
- Configuração do dispositivo, que inclui permitir que os usuários alterem configurações e parâmetros do dispositivo
- Atualizações de software, que incluem o fornecimento de novos softwares ou correções de bugs a serem carregados no dispositivo, incluindo aplicativos e software do sistema
- Gerenciamento de falhas, que inclui o recebimento de relatórios de erro e status do dispositivo

> **Nota:**

Ao criar seu conteúdo XML, use o caractere \% com cautela. O caractere \% é um caractere reservado do XML, usado apenas para escapar caracteres especiais do XML. Para usar \% em um nome, codifique-o como \%25.

Para dispositivos Windows: Você cria sua configuração XML personalizada usando a API Open Mobile Alliance Device Management (OMA DM) no Windows. A criação de XML personalizado com a API OMA DM está além do escopo deste tópico. Para obter mais informações sobre como usar a API OMA DM, consulte Gerenciamento de Dispositivos OMA no site da Microsoft Developer Network.

Nota:

Para Windows 10 RS2 Phone: Depois que uma política XML personalizada ou política de Restrições que desativa o Internet Explorer é implantada no telefone, o navegador permanece ativado. Para contornar esse problema, reinicie o telefone. Este é um problema de terceiros.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de Desktop/Tablet Windows

- **Conteúdo XML:** Digite, ou recorte e cole, o código XML personalizado que você deseja adicionar à política.

  Depois de clicar em **Avançar**, o XenMobile verifica a sintaxe do conteúdo XML. Quaisquer erros de sintaxe aparecem abaixo da caixa de conteúdo. Corrija todos os erros antes de continuar.

  Se não houver erros de sintaxe, a página de atribuição da **Política XML Personalizada** será exibida.

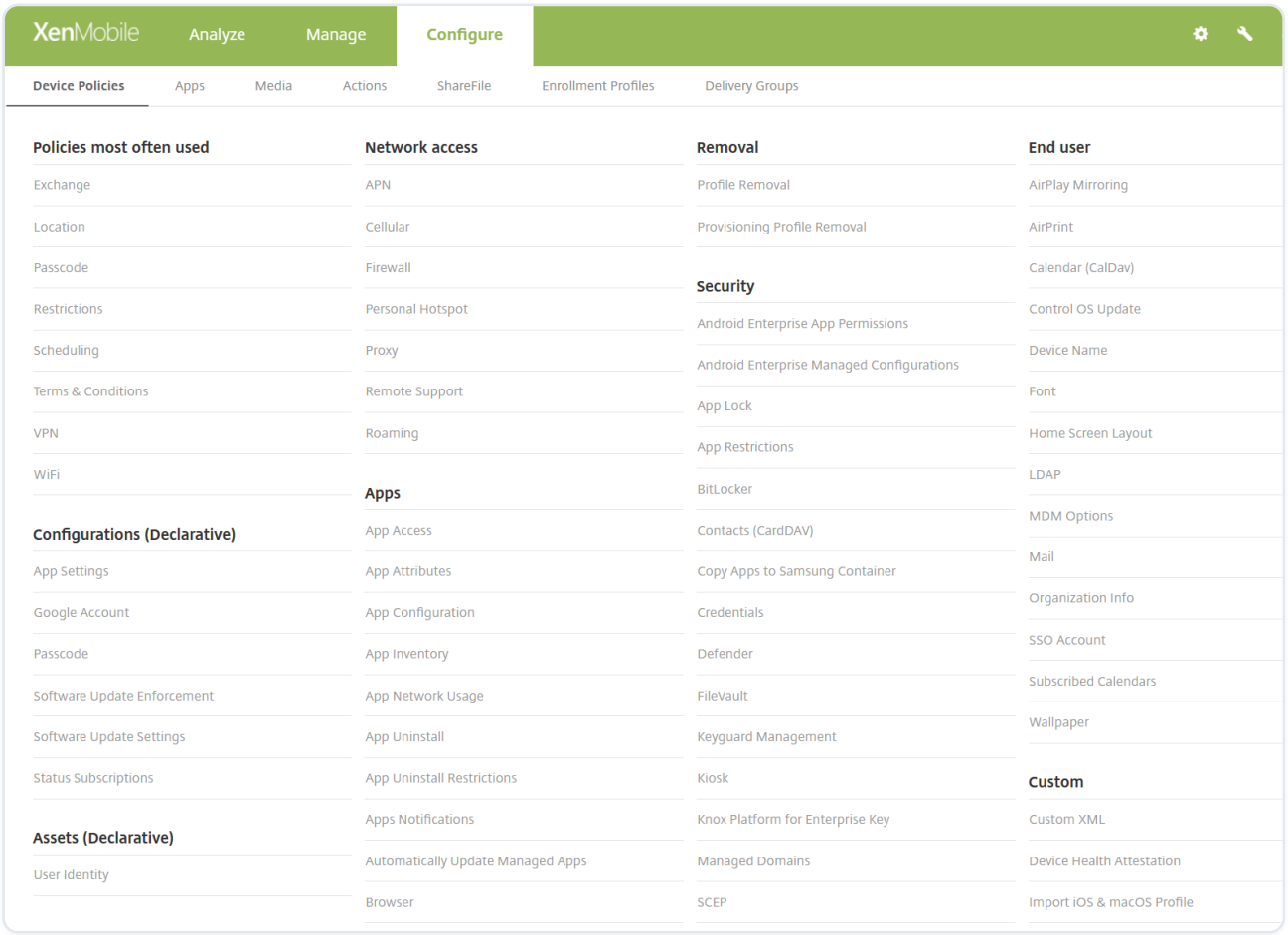
Políticas de Gerenciamento Declarativo de Dispositivos

A Apple anunciou o Gerenciamento Declarativo de Dispositivos (DDM) no iOS 15, usando um paradigma de modelo de dados declarativo. Este paradigma permite que os servidores evitem os problemas comuns de desempenho e escalabilidade tipicamente associados à serialização de

comandos e à sondagem de dispositivos via MDM. Para mais informações, consulte Aproveitando o modelo de dados de gerenciamento declarativo para escalar dispositivos.

As seguintes políticas de dispositivo declarativas são suportadas quando você habilita o recurso DDM:

- Configurações de Aplicativo
- Conta Google
- Código de Acesso
- Aplicação de Atualização de Software
- Configurações de Atualização de Software
- Assinaturas de Status
- Identidade do Usuário



Política de dispositivo de Configurações de Aplicativo

A política de dispositivo de Configurações de Aplicativo permite configurar listas de permissão e negação de aplicativos usando o Gerenciamento Declarativo de Dispositivos da Apple. Ela

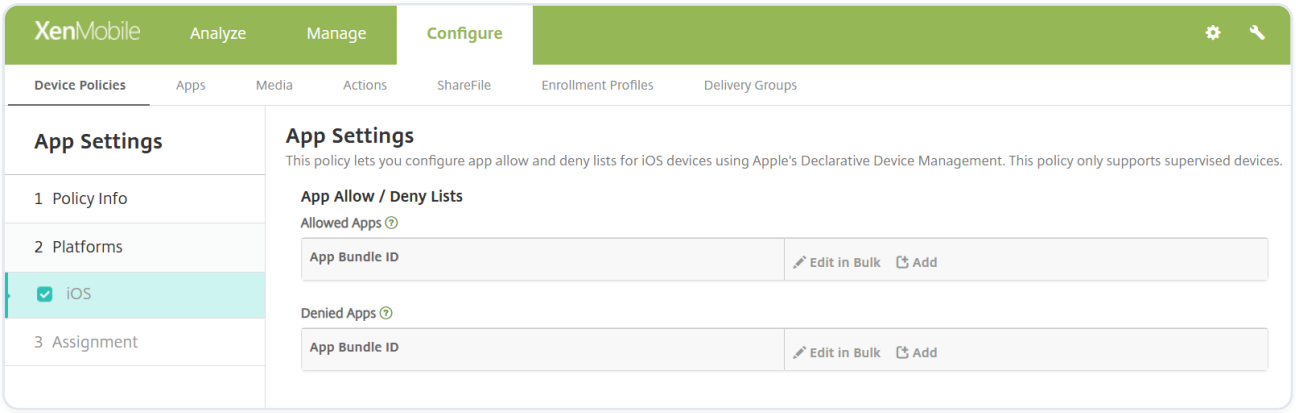
substitui as chaves de restrição `allowListedAppBundleIDs` e `blockedAppBundleIDs` descontinuadas. Esta política suporta apenas dispositivos supervisionados.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 9 ou posterior.
- A propriedade do servidor `ios.mdm.ios27.ddm.support` está definida como **True**.
- Disponível para iOS 27 ou posterior e iPadOS 27 ou posterior. Suporta apenas dispositivos supervisionados.

Configurações do iOS



- **Listas de Permissão / Negação de Aplicativos:**
  - **Aplicativos Permitidos:** Se presente, o dispositivo exibe ou inicia apenas aplicativos com IDs de pacote na lista. Inclua o valor `com.apple.webapp` para permitir todos os webclips. Isso se aplica a aplicativos da App Store, aplicativos de marketplace e aplicativos instalados localmente (usando Configurator, Xcode e assim por diante).
    - **ID do Pacote do Aplicativo:** Para adicionar um ID do Pacote do Aplicativo, clique em **Adicionar**, digite um ID do Pacote do Aplicativo e clique em **Salvar**. Repita esse processo para cada ID do pacote do aplicativo que você deseja adicionar. Você também pode clicar em **Editar em Massa**, inserir ou colar IDs de pacote de aplicativos, um por linha ou separados por vírgulas, e clicar em **Salvar**.
  - **Aplicativos Negados:** Se presente, o dispositivo impede a exibição ou o lançamento de aplicativos com IDs de pacote na lista. Inclua o valor `com.apple.webapp` para restringir todos os webclips. Isso se aplica a aplicativos da App Store, aplicativos de marketplace e aplicativos instalados localmente (usando Configurator, Xcode e assim por diante).

Nota:

- Negar aplicativos do sistema pode desabilitar outras funcionalidades. Por exemplo, negar o aplicativo da App Store pode impedir que os usuários aceitem os termos e condições do Programa de Compra por Volume (VPP) baseado no usuário.
- Recomendamos que você configure a Lista de Permissão de Aplicativos ou a Lista de Negação de Aplicativos, mas não ambas.

Política de dispositivo de conta Google

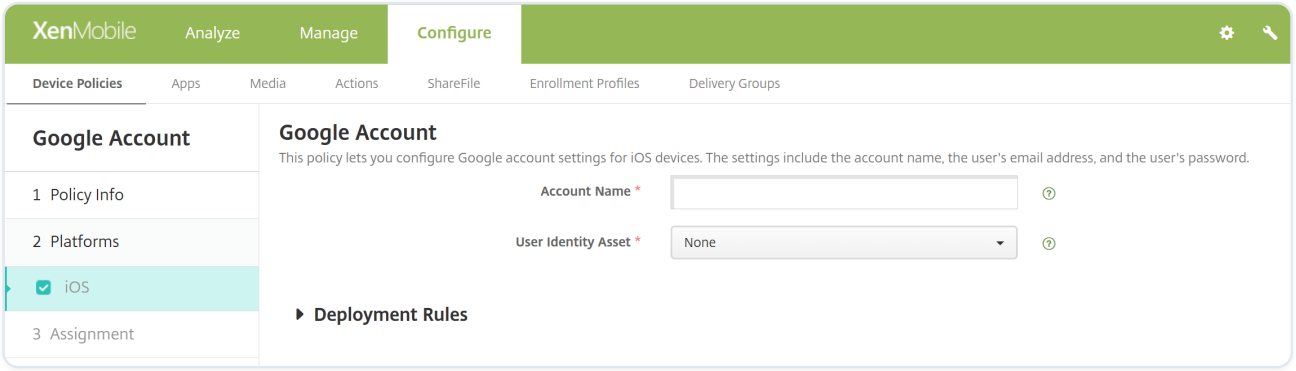
A política de dispositivo de conta Google permite configurar as definições da conta Google para dispositivos iOS. As definições incluem o nome da conta e o ativo de identidade do usuário que configura o endereço de e-mail e o nome completo do usuário.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- A propriedade do servidor `ios.mdm.declarative.management` está definida como **True**.
- A política de Identidade do Usuário está configurada. Consulte Política de dispositivo de Identidade do Usuário.

Configurações do iOS



- **Nome da Conta:** Digite o nome da conta Google.
- **Ativo de Identidade do Usuário:** Na lista, selecione o ativo de identidade do usuário criado pela política de Identidade do Usuário, que contém o endereço de e-mail e o nome completo do usuário. O padrão é **Nenhum**.

Política de dispositivo de senha

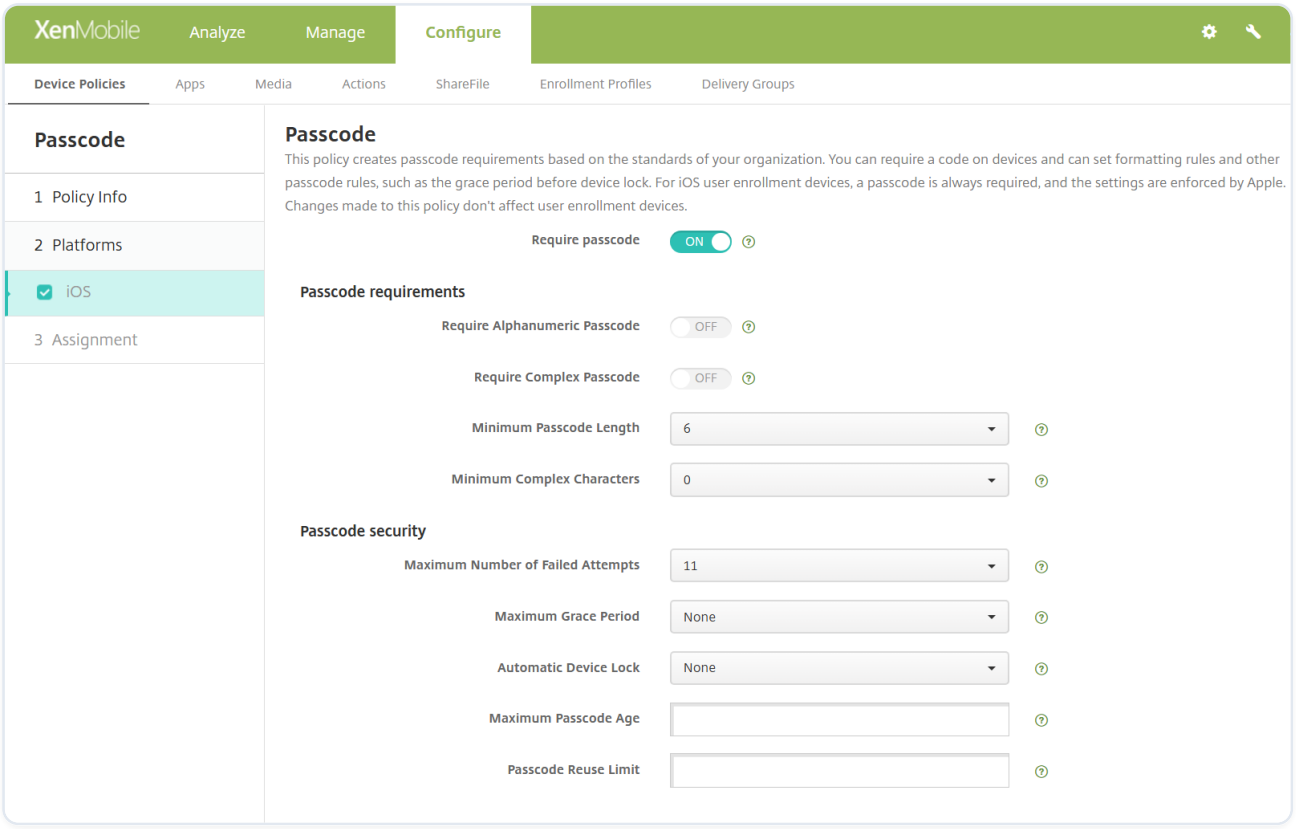
A política de dispositivo de senha cria requisitos de senha com base nos padrões da sua organização. Você pode exigir um código nos dispositivos e pode definir regras de formatação e outras regras de senha, como o período de carência antes do bloqueio do dispositivo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- A propriedade do servidor `ios.mdm.declarative.management` está definida como **True**.

Configurações do iOS



- **Exigir senha:** Selecione esta opção para exigir uma senha e para exibir as opções de configuração para uma política de dispositivo de senha do iOS. Se **Ativado**, exige que o usuário defina uma senha sem quaisquer requisitos sobre o comprimento ou a qualidade da senha e a página se expande para permitir que você configure as configurações de requisitos de senha e segurança de senha. O padrão é **Ativado**.
- **Requisitos de senha**

- **Exigir senha alfanumérica:** Selecione se deseja exigir que a senha consista em pelo menos um caractere alfabético e pelo menos um número. O padrão é **Desativado**.
- **Exigir senha complexa:** Selecione se deseja exigir uma senha complexa. Uma senha complexa é aquela que não contém caracteres repetidos ou caracteres crescentes ou decrescentes (como 123 ou CBA), e deve conter pelo menos um caractere não numérico e não alfabético. O padrão é **Desativado**.
- **Comprimento mínimo da senha:** Selecione o número mínimo de caracteres que uma senha pode conter. O padrão é **6**.
- **Mínimo de caracteres complexos:** Selecione o número mínimo de caracteres complexos na senha. Um caractere complexo é um caractere diferente de um número ou uma letra, como &, %, $, e #. O padrão é **0**.

- **Segurança da senha**
  - **Número Máximo de Tentativas Falhas:** Selecione o número de tentativas de senha falhas que o sistema permite ao usuário antes que o iOS apague o dispositivo. Se você não alterar esta configuração, após seis tentativas falhas, o dispositivo impõe um atraso de tempo antes que o usuário possa inserir uma senha novamente. O atraso de tempo aumenta a cada tentativa falha. Após a tentativa falha final, o sistema apaga com segurança todos os dados e configurações do dispositivo iOS. O atraso de tempo da senha começa após a sexta tentativa, então se este valor for seis ou menor, o sistema não tem atraso de tempo e aciona a exclusão ou bloqueio assim que o usuário excede o limite. O padrão é **11**.
  - **Período Máximo de Carência:** Selecione o período máximo durante o qual o usuário pode desbloquear o dispositivo sem uma senha. Selecione **imediatamente** para nenhum período de carência, e o dispositivo exigirá uma senha imediatamente. O padrão é **Nenhum**, o que significa que o usuário pode selecionar qualquer período.
  - **Bloqueio Automático do Dispositivo:** Selecione o período máximo durante o qual o dispositivo pode ficar inativo antes que o sistema o bloqueie automaticamente. Quando o dispositivo atinge este limite, ele é bloqueado e o usuário deve inserir a senha para desbloqueá-lo. O padrão é **Nenhum**, o que significa que o usuário pode selecionar qualquer período.
  - **Idade Máxima da Senha:** Selecione o número máximo de dias que a senha pode permanecer inalterada. Após este número de dias, o sistema força o usuário a alterar a senha antes de desbloquear o dispositivo. Os valores válidos são 0–730. Um valor de **0** força uma alteração imediata da senha. O padrão é vazio, o que significa que não há restrição de idade da senha.

- **Limite de Reutilização de Senha:** Selecione o número de entradas de senha históricas que o sistema verifica ao validar uma nova senha. O dispositivo recusa uma nova senha se ela corresponder a uma senha usada anteriormente dentro do intervalo de histórico de senhas especificado. Os valores válidos são 1–50. O padrão é vazio, o que significa que o sistema não realiza nenhuma verificação histórica.

> **Nota:**
>
> Se a mesma configuração for enviada como um perfil MDM e uma configuração declarativa para um dispositivo, as mesmas regras se aplicam como se a configuração tivesse sido entregue por vários perfis. Por exemplo, se as políticas de senha forem configuradas por um perfil (via política de Senha) e uma configuração (via política de Senha declarativa), as políticas são mescladas e as configurações mais rigorosas são aplicadas.

Política de dispositivo de Imposição de Atualização de Software

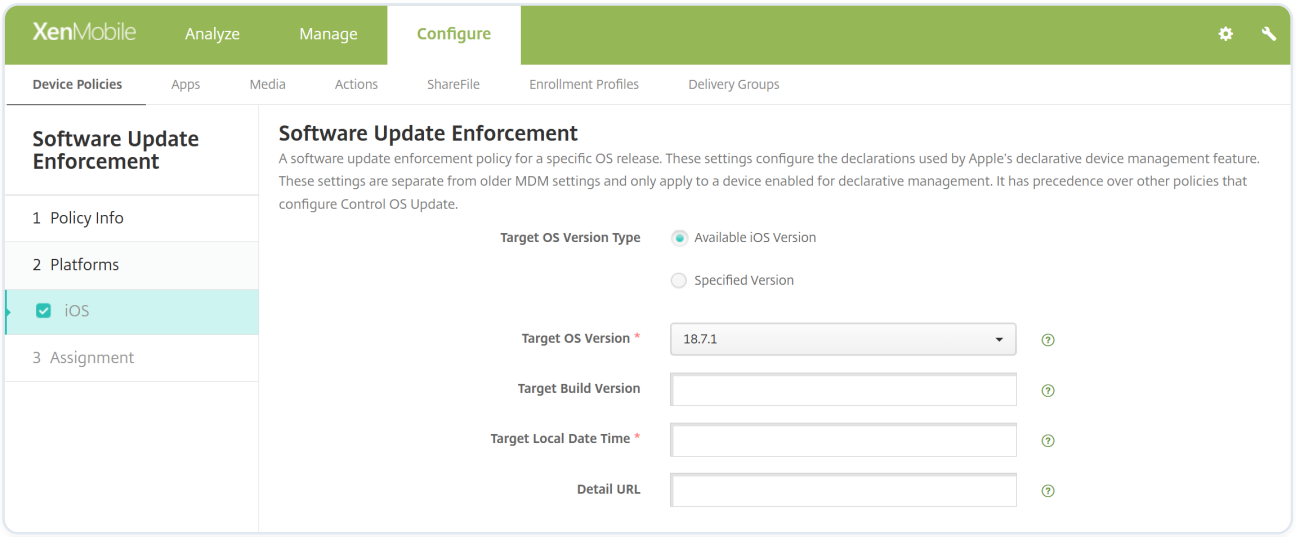
A política de dispositivo de imposição de atualização de software para uma versão específica do sistema operacional permite que os administradores de TI gerenciem as atualizações de dispositivos iOS, permitindo-lhes controlar quais atualizações são aplicadas e definir prazos para a conclusão de todas as atualizações. Essas configurações configuram as declarações usadas pelo recurso de gerenciamento declarativo de dispositivos da Apple. Essas configurações são separadas das configurações MDM mais antigas e se aplicam apenas a um dispositivo habilitado para gerenciamento declarativo. Ela tem precedência sobre a política de Controle de Atualização do SO para a mesma configuração.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- A propriedade do servidor `ios.mdm.declarative.management` está definida como **True**.
- Disponível para **iOS 17.0** ou posterior e **iPadOS 17.0** ou posterior.

Configurações do iOS



- **Tipo de Versão do SO de Destino:** Especifique como configurar a versão do SO de destino. O padrão é **Versão do iOS Disponível**.
  - **Versão do iOS Disponível:** Se **Ativado**, liste as versões do SO de destino disponíveis em **Versão do SO de Destino**.
  - **Versão Especificada:** Se **Ativado**, insira manualmente a versão do SO com o formato sugerido.
- **Versão do SO de Destino: (Obrigatório)** Selecione ou digite a versão do SO de destino para a qual o dispositivo deve ser atualizado no momento apropriado. Este é o número da versão do SO, por exemplo, 17.7. Também pode incluir um identificador de versão suplementar, por exemplo, 17.7.2.
- **Versão de Build de Destino:** Digite a versão de build de destino para a qual o dispositivo deve ser atualizado no momento apropriado, por exemplo, 20A242. O sistema usa a versão de build para testes durante os períodos de seeding. A versão de build pode incluir um identificador de versão suplementar, por exemplo, 20A242a. Se a versão de build não for consistente com a versão do SO de destino especificada na chave TargetOSVersion, a versão do SO de destino terá precedência.
- **Data e Hora Local de Destino: (Obrigatório)** Digite o valor da data e hora local que especifica quando forçar a instalação da atualização de software. Use o formato aaaa-mm-ddThh:mm:ss, que é derivado do RFC3339, mas não inclui um deslocamento de fuso horário. Se o usuário não iniciar a atualização de software antes deste horário, o dispositivo a instalará forçadamente.
- **URL de Detalhes:** Digite a URL de uma página da web que mostra os detalhes fornecidos pela organização sobre a atualização imposta.

Nota:

Tanto a política de Imposição de Atualização de Software quanto a política de Controle de Atualização do SO podem gerenciar as atualizações do SO em dispositivos. No entanto, a política de Imposição de Atualização de Software tem precedência sobre a política de Controle de Atualização do SO. Se ambas as políticas forem implantadas com a mesma configuração, a configuração na política de Controle de Atualização do SO será substituída e não terá efeito. Para obter mais informações, consulte a Transição para o gerenciamento declarativo de dispositivos.

Além disso, existem algumas diferenças entre a política de Imposição de Atualização de Software e a política de Controle de Atualização do SO.

TIPO DE POLÍTICA	IMPOSIÇÃO DE ATUALIZAÇÃO DE SOFTWARE	CONTROLE DE ATUALIZAÇÃO DO SO
Tipo de Dispositivo	Dispositivo Supervisionado ou Não Supervisionado	Dispositivo Supervisionado
Impor um prazo de atualização	✓	✗
Inserir uma URL de ajuda	✓	✗
Especificar o número da versão da compilação	✓	✗
Implantar automaticamente a atualização mais recente	✗	✓
Versão mínima suportada	iOS 17.0	iOS 10.3 (supervisionado)

Política de dispositivo de Configurações de Atualização de Software

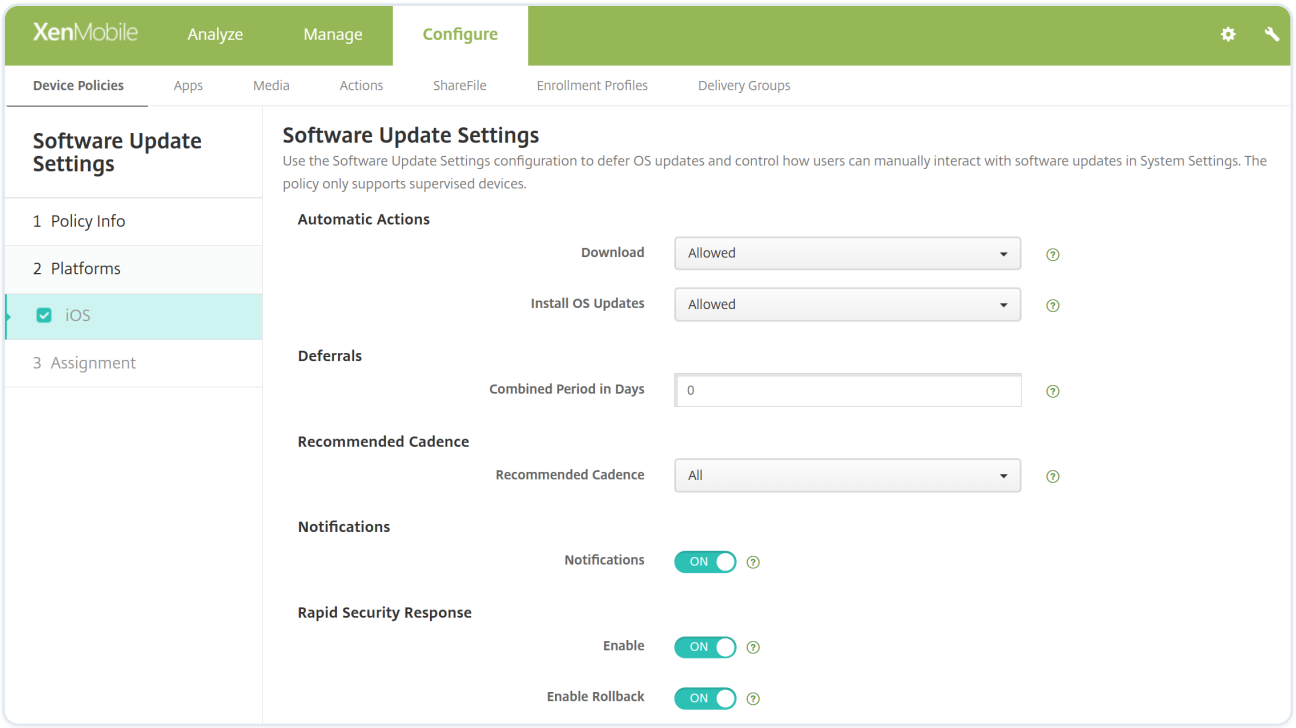
A política de dispositivo de Configurações de Atualização de Software pode ser usada para adiar atualizações do SO e controlar como os usuários podem interagir manualmente com as atualizações de software nas Configurações do Sistema. A política oferece suporte apenas a dispositivos supervisionados.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- As propriedades do servidor `ios.mdm.declarative.management` e `ios.mdm.software.update.settings` estão definidas como **True**.
- Disponível para **iOS 18.0** ou posterior e **iPadOS 18.0** ou posterior, suporta apenas dispositivos supervisionados.

Configurações do iOS



- **Ações Automáticas**
  - **Download:** Especifique se o usuário pode controlar os downloads automáticos de atualizações disponíveis. O padrão é **Permitido**.
    - **Permitido** - o usuário pode ativar ou desativar downloads automáticos.
    - **Sempre Ativado** - os downloads automáticos estão sempre ativados.
    - **Sempre Desativado** - os downloads automáticos estão sempre desativados.
  - **Instalar Atualizações do SO:** Especifique se o usuário pode controlar a instalação automática de atualizações disponíveis. O padrão é **Permitido**.

    - **Permitido** - o usuário pode ativar ou desativar a instalação automática.
    - **SempreAtivado** - as instalações automáticas estão sempre ativadas.
    - **SempreDesativado** - as instalações automáticas estão sempre desativadas.

- **Adiamentos**

    - **Período Combinado em Dias:** Especifique o número de dias para adiar uma atualização de software principal ou secundária do SO no dispositivo. Quando definido, as atualizações de software só aparecem após o atraso especificado, após o lançamento da atualização de software. Disponível no iOS 18 e posterior. Os valores válidos são 0–90. O padrão é **0**, o que significa que nenhum atraso é esperado.

- **Cadência Recomendada**

    - **Cadência Recomendada:** Especifique como o dispositivo mostra as atualizações de software ao usuário. Quando mais de uma atualização está disponível, o dispositivo se comporta da seguinte forma. O padrão é **Todos**.
        - **Todos** - Mostra todas as versões de atualização de software.
        - **Mais Antigo** - Mostra apenas a versão de atualização de software mais antiga (com número menor).
        - **Mais Recente** - Mostra apenas a versão de atualização de software mais recente (com número maior).

- **Notificações**

    - **Notificações:** Se **Ativado**, o dispositivo mostra todas as notificações de imposição de atualização de software. Se **Desativado**, o dispositivo mostra apenas as notificações acionadas uma hora antes do prazo de imposição e a notificação de contagem regressiva para reinício. O padrão é **Ativado**.

- **Resposta Rápida de Segurança**

    - **Ativar:** Se **Desativado**, as Respostas Rápidas de Segurança não são oferecidas para instalação pelo usuário. O sistema ainda pode instalar Respostas Rápidas de Segurança com configurações `com.apple.configuration.softwareupdate.enforcement.specific`. Se **Ativado**, o sistema oferece Respostas Rápidas de Segurança ao usuário. O padrão é **Ativado**.

- **Ativar Reversão:** Se **Desativado**, o sistema não oferece reversões de Resposta Rápida de Segurança ao usuário. Se **Ativado**, o sistema oferece reversões de Resposta Rápida de Segurança ao usuário. O padrão é **Ativado**.

Política de dispositivo de Assinaturas de Status

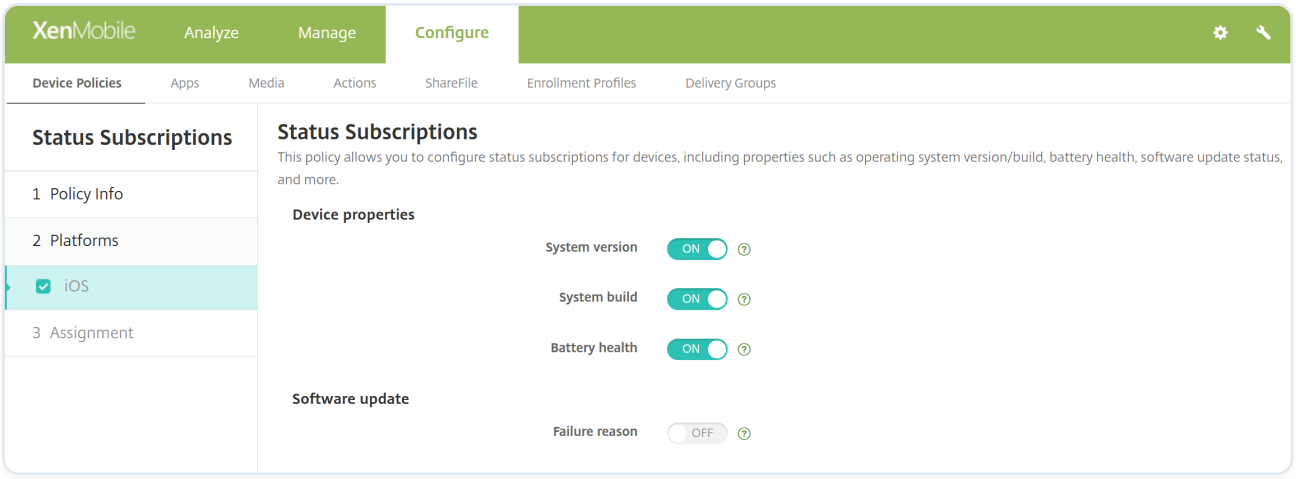
A política de dispositivo de Assinaturas de Status permite configurar assinaturas de status para dispositivos, incluindo propriedades como versão/compilação do sistema operacional, saúde da bateria, status de atualização de software e muito mais.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- A propriedade do servidor `ios.mdm.declarative.management` está definida como **True**.

Configurações do iOS



- **Propriedades do dispositivo**
  - **Versão do sistema:** Se **Ativado**, o dispositivo reportará a versão do sistema operacional (por exemplo, 18.0), que será exibida na seção Informações do Sistema das Propriedades do Dispositivo. Isso é útil porque o dispositivo a reportará automaticamente quando ocorrer uma atualização de versão. O padrão é **Ativado**. Disponível para iOS 15 e posterior.
  - **Compilação do sistema:** Se **Ativado**, o dispositivo reportará a versão de compilação do sistema operacional (por exemplo, 18F132), que será exibida na seção Informações do Sistema das Propriedades do Dispositivo. Isso é útil porque o dispositivo a reportará automaticamente quando ocorrer uma atualização de versão. O padrão é **Ativado**. Disponível para iOS 15 e posterior.

  - **Saúde da bateria:** Se **Ativado**, uma nova configuração **Saúde da Bateria** é adicionada às Propriedades do Dispositivo. Esta configuração permite que os administradores visualizem o status de saúde da bateria dos dispositivos iOS registrados navegando até **Gerenciar > Dispositivos > Propriedades > Bateria > Saúde da bateria**. O padrão é **Ativado**. Disponível para iOS 17 e posterior.

- **Atualização de software**

  - **Motivo da falha:** Se **Ativado**, o dispositivo reportará o motivo de uma atualização do SO falha, que será exibido na seção de informações de Atualizações de Software das Propriedades do Dispositivo. O padrão é **Desativado**. Disponível para iOS 17 e posterior.

Política de dispositivo de Identidade do Usuário

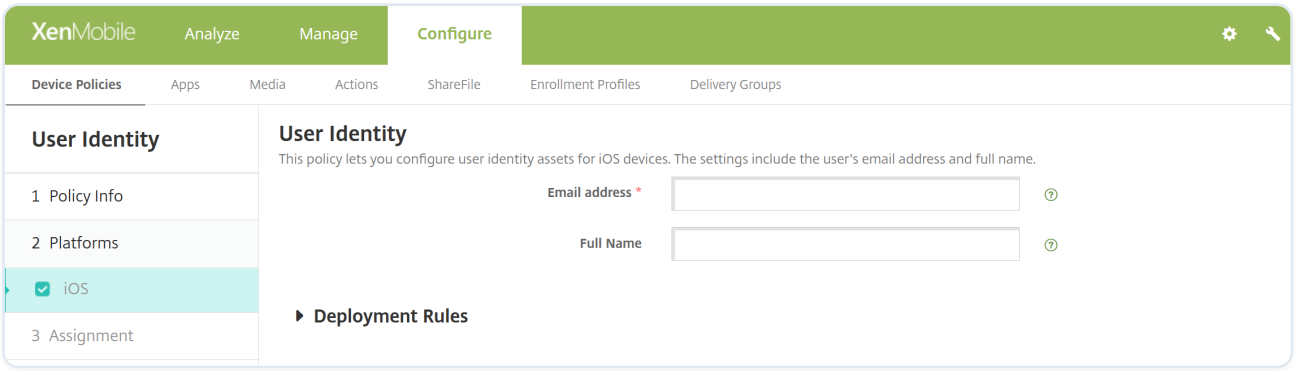
A política de dispositivo de Identidade do Usuário permite configurar ativos de identidade de usuário para dispositivos iOS. As configurações incluem o endereço de e-mail e o nome completo do usuário.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

- XenMobile Server 10.16 Rolling Patch 8 ou posterior.
- A propriedade do servidor `ios.mdm.declarative.management` está definida como **True**.

Configurações do iOS



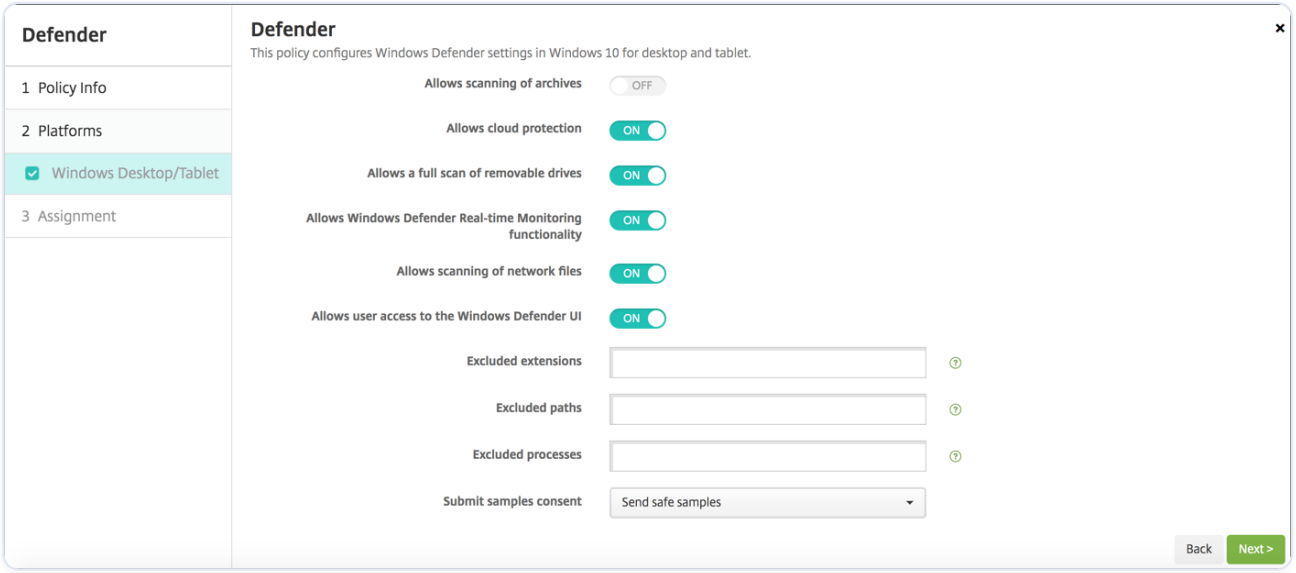
- **Endereço de e-mail:** Digite o endereço de e-mail do usuário. Este campo é obrigatório.
- **Nome Completo:** Digite o nome completo do usuário.

Política de dispositivo do Defender

O Windows Defender é uma proteção contra malware incluída no Windows 10 e Windows 11. Você pode usar a política de dispositivo XenMobile®, Defender, para configurar a política do Microsoft Defender para Windows 10 e Windows 11 para desktop e tablet.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de Desktop e Tablet do Windows



- **Permite a verificação de arquivos:** Permite ou não que o Defender verifique arquivos compactados. O padrão é **Desativado**.
- **Permite a proteção na nuvem:** Permite ou não que o Defender envie informações à Microsoft sobre atividades de malware. O padrão é **Ativado**.
- **Permite uma verificação completa de unidades removíveis:** Permite ou não que o Defender verifique unidades removíveis, como pen drives. O padrão é **Ativado**.
- **Permite a funcionalidade de Monitoramento em Tempo Real do Windows Defender:** O padrão é **Ativado**.
- **Permite a verificação de arquivos de rede:** Permite ou não que o Defender verifique arquivos de rede. O padrão é **Ativado**.
- **Permite o acesso do usuário à interface do usuário do Windows Defender:** Especifica se os usuários podem acessar a interface do usuário do Windows Defender. Essa configuração entra em vigor na próxima vez que o dispositivo do usuário for iniciado. Se essa configuração estiver **Desativada**, os usuários não receberão nenhuma notificação do Windows Defender. O padrão é **Ativado**.

- **Extensões excluídas:** As extensões a serem excluídas de verificações em tempo real ou agendadas. Para separar as extensões, use o caractere **\|**. Por exemplo, "lib\|obj".
- **Caminhos excluídos:** Os caminhos a serem excluídos de verificações em tempo real ou agendadas. Para separar os caminhos, use o caractere **\|**. Por exemplo, "C:\\Example\|C:\ \Example1".
- **Processos excluídos:** Os processos a serem excluídos de verificações em tempo real ou agendadas. Para separar os processos, use o caractere **\|**. Por exemplo, "C:\\Example.exe\|C:\ \Example1.exe".
- **Consentimento para envio de amostras:** Controla se arquivos que podem exigir análise adicional para determinar se são maliciosos devem ser enviados à Microsoft. Opções: **Sempre perguntar**, **Enviar amostras seguras**, **Nunca enviar**, **Enviar todas as amostras**. O padrão é **Enviar amostras seguras**.

Política de dispositivo de Atestado de Integridade do Dispositivo

No XenMobile®, você pode exigir que dispositivos Windows 10 e Windows 11 relatem o estado de sua integridade, fazendo com que esses dispositivos enviem dados específicos e informações de tempo de execução para o Serviço de Atestado de Integridade (HAS) para análise. O HAS cria e retorna um Certificado de Atestado de Integridade que o dispositivo então envia para o XenMobile. Quando o XenMobile recebe o Certificado de Atestado de Integridade, com base no conteúdo do Certificado de Atestado de Integridade, ele pode implantar ações automáticas que você configurou anteriormente.

Os dados verificados pelo HAS são:

- AIK Presente
- Status do BitLocker
- Depuração de Inicialização Habilitada
- Versão da Lista de Revisão do Gerenciador de Inicialização
- Integridade de Código Habilitada
- Versão da Lista de Revisão da Integridade de Código
- Política do Programa de Implantação da Apple
- Driver ELAM Carregado
- Emitido Em
- Depuração de Kernel Habilitada

- PCR
- Contagem de Redefinições
- Contagem de Reinicializações
- Modo de Segurança Ativado
- Hash SBCP
- Inicialização Segura Ativada
- Assinatura de Teste Ativada
- VSM Ativado
- WinPE Ativado

Para obter mais informações, consulte a página da Microsoft CSP de Atestado de Integridade do Dispositivo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Para configurar o DHA usando o Microsoft Cloud

Adicione uma política de Atestado de Integridade do Dispositivo e configure esta definição para cada plataforma que escolher:

- **Habilitar Atestado de Integridade do Dispositivo:** Selecione se deseja exigir o Atestado de Integridade do Dispositivo. O padrão é **Desativado**.

Para configurar o DHA usando um servidor DHA Windows local

Para habilitar o DHA localmente, primeiro você configura um servidor DHA. Em seguida, você cria uma política do XenMobile Server para habilitar o serviço DHA local.

1. Para configurar um servidor DHA, você instala a função de servidor DHA em uma máquina executando o Windows Server 2016 Technical Preview 5 ou posterior. Para obter instruções, consulte Configurar um servidor de Atestado de Integridade do Dispositivo local.
2. Adicionar uma política de Atestado de Integridade do Dispositivo e configurar estas definições:
    - **Habilitar Atestado de Integridade do Dispositivo:** Defina como **Ativado**.
    - **Configurar Serviço de Atestado de Integridade Local:** Defina como **Ativado**.
    - **FQDN do Serviço DHA Local:** Digite o nome de domínio totalmente qualificado do servidor DHA que você configurou.

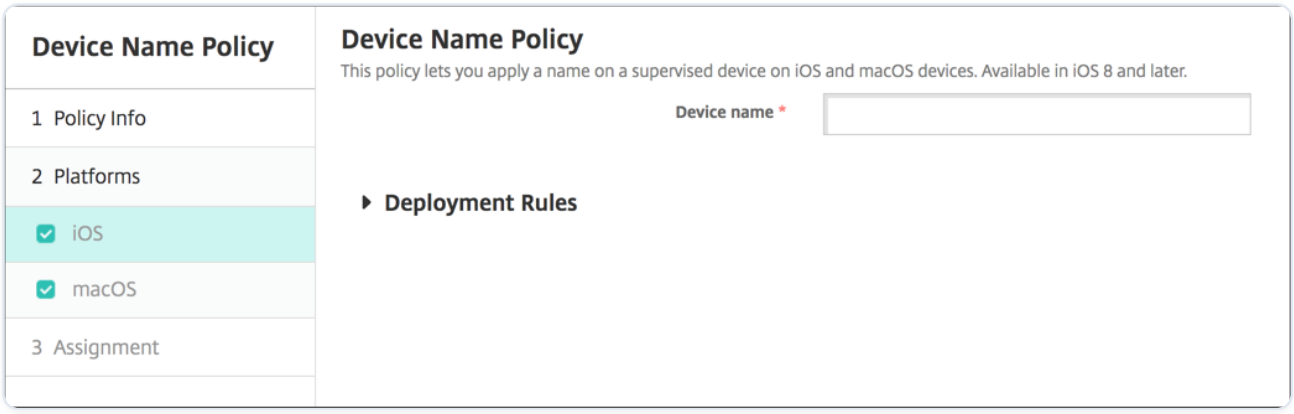
- **Versão da API DHA Local:** Selecione a versão do serviço DHA instalado no servidor DHA.

Política de nome de dispositivo

Você pode definir os nomes em dispositivos iOS e macOS supervisionados para que possa identificar facilmente os dispositivos. Você pode usar macros, texto ou uma combinação de ambos para definir o nome do dispositivo. Por exemplo, para definir o nome do dispositivo como o número de série do dispositivo, você deve usar ${device.serialnumber}. Para definir o nome do dispositivo como uma combinação do nome do usuário e do seu domínio, você deve usar ${user.username}@example.com. Para obter mais informações sobre macros, consulte Macros no XenMobile.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS e macOS



- **Nome do dispositivo:** Digite a macro, uma combinação de macros ou uma combinação de macros e texto para nomear cada dispositivo de forma exclusiva. Por exemplo, use ${device.serialnumber} para definir os nomes dos dispositivos como o número de série de cada dispositivo, ou use ${device.serialnumber} ${ user.username } para incluir o nome do usuário no nome do dispositivo.

Política de dispositivo de Configuração de Educação

A política de dispositivo de Configuração de Educação define:

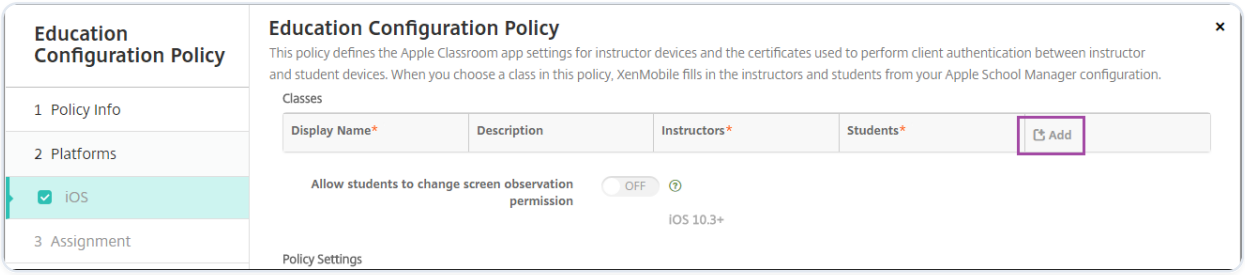
- As configurações do aplicativo Apple Classroom para dispositivos de instrutor.
- Os certificados usados para fazer a autenticação de cliente entre dispositivos de instrutor e de aluno.

Quando você escolhe uma turma nesta política, o console XenMobile® preenche os instrutores e alunos da sua configuração do Apple School Manager. Crie uma política se as configurações do aplicativo Apple Classroom nesta política forem as mesmas para todas as turmas.

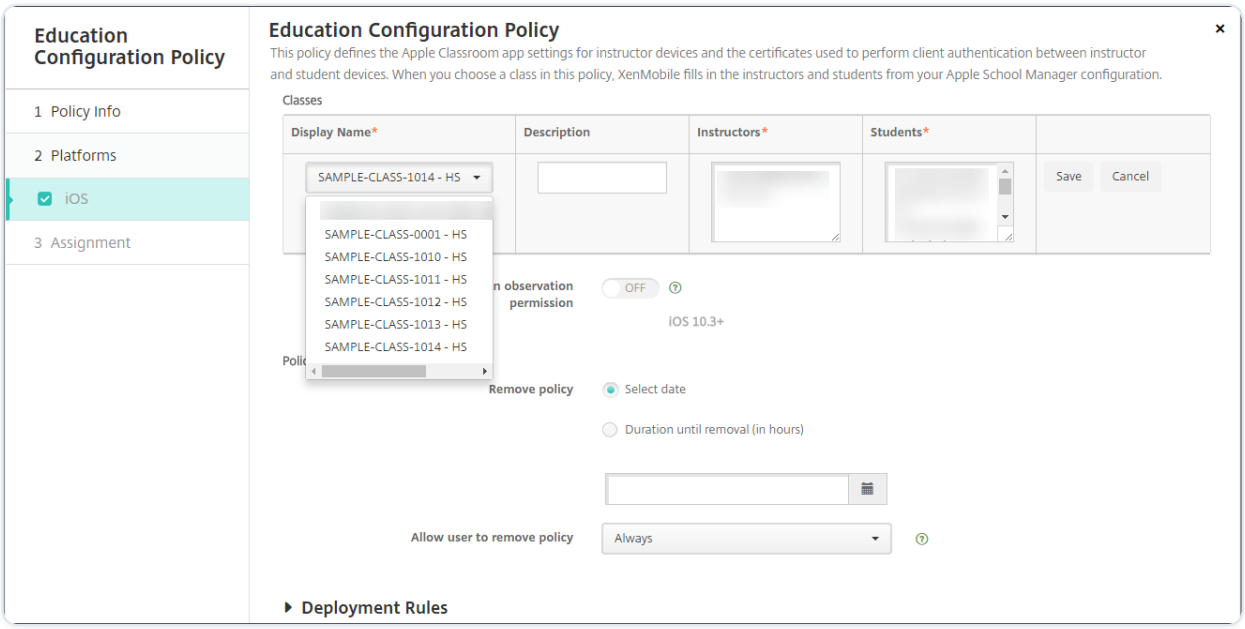
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

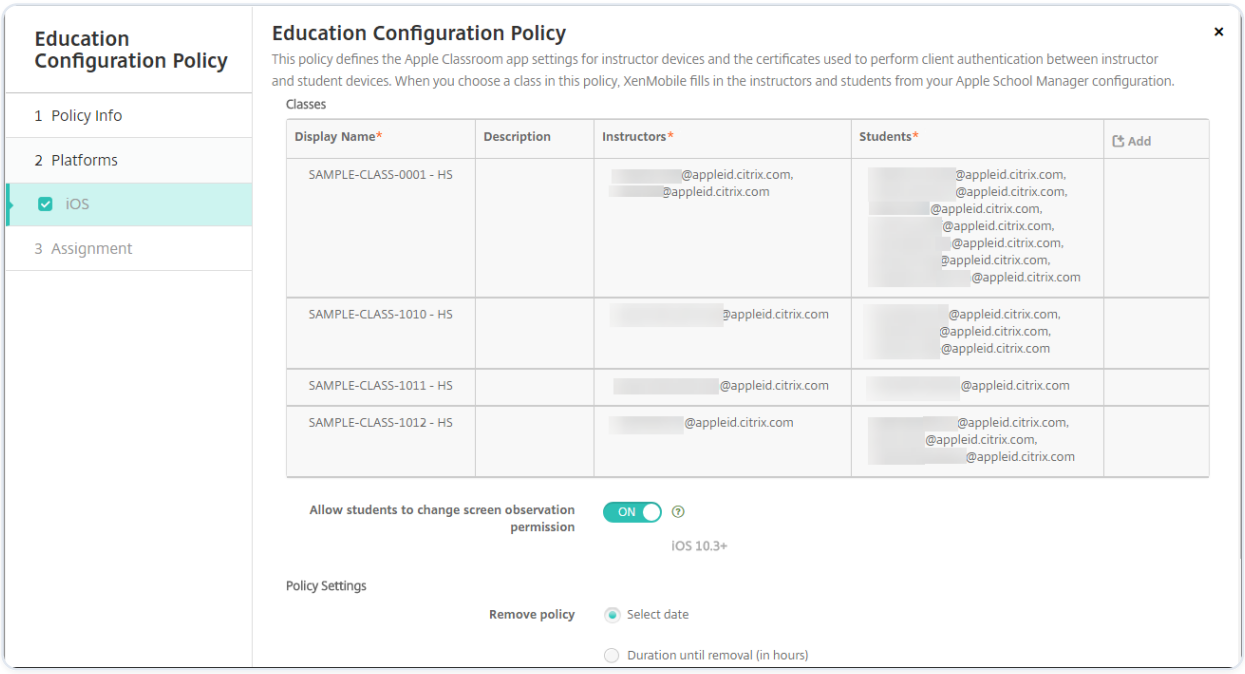
- **Turmas:** Para adicionar uma turma, clique em **Adicionar**.



Em seguida, clique na lista **Nome de Exibição**. Uma lista de turmas obtidas da sua conta conectada do Apple School Manager é exibida.



Quando você escolhe uma turma em **Nome de Exibição**, o XenMobile preenche os instrutores e alunos. Continue adicionando turmas.

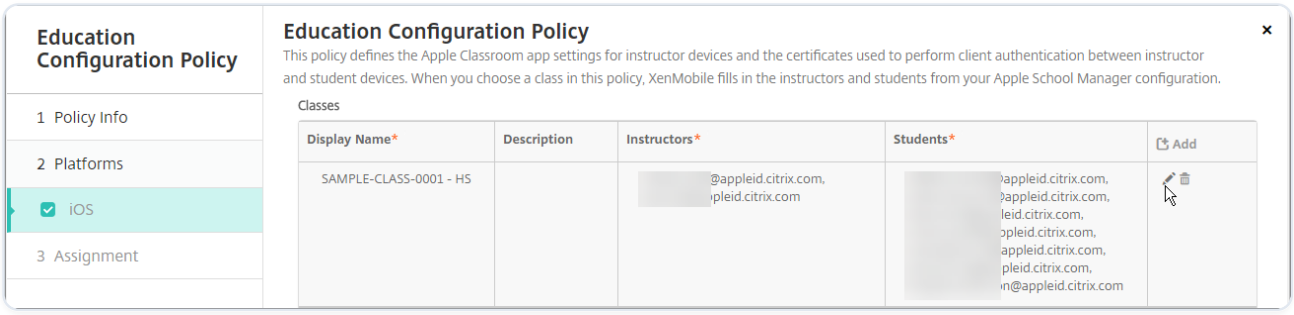


- **Permitir que os alunos alterem a permissão de observação de tela:** Se **Ativado**, os alunos matriculados em turmas gerenciadas podem escolher se permitem que seu professor observe as telas de seus dispositivos. O padrão é **Desativado**.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

Para editar informações da turma na política

Você pode adicionar uma descrição a uma turma (o "Nome de exibição" no aplicativo Sala de Aula). Você também pode adicionar ou remover instrutores e alunos. O XenMobile não salva essas alterações em sua conta do Apple School Manager. Para obter mais informações, consulte "Gerenciar dados de instrutores, alunos e turmas" em Integrar com recursos do Apple Education.

Passe o mouse sobre a coluna **Adicionar** para a turma que você deseja editar e, em seguida, clique no ícone de lápis.



Para excluir uma turma da política, passe o mouse sobre a coluna **Adicionar** para a turma que você deseja excluir e, em seguida, clique no ícone de lixeira.

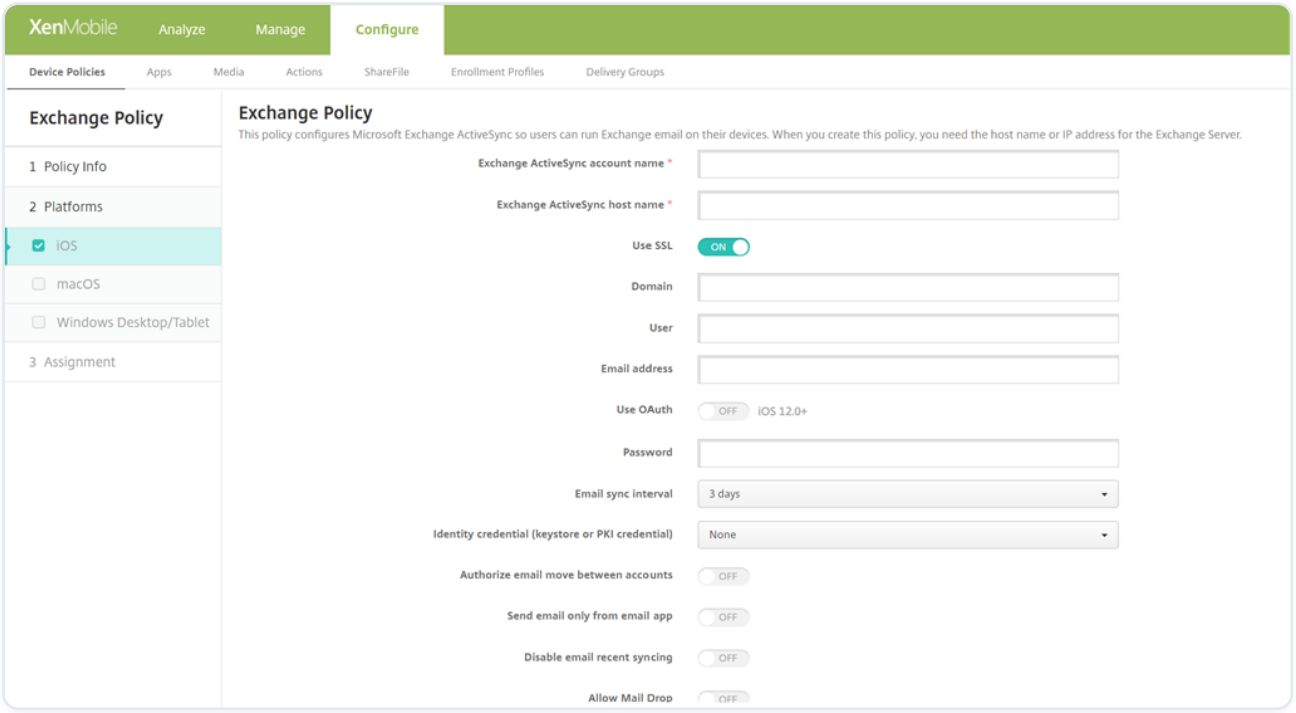
Política de dispositivo Exchange

Você pode usar a política de dispositivo Exchange ActiveSync para configurar um cliente de e-mail em dispositivos de usuário para permitir que eles acessem seu e-mail corporativo hospedado no Exchange. Você pode criar políticas para iOS, macOS, Android Enterprise, Samsung SAFE, Samsung Knox e Windows Tablet. Cada plataforma requer um conjunto diferente de valores, que são descritos em detalhes nas seções a seguir.

Para criar esta política, você precisa do nome do host ou do endereço IP do Exchange Server. Para obter informações sobre as configurações do ActiveSync, consulte o artigo da Microsoft ActiveSync CSP.

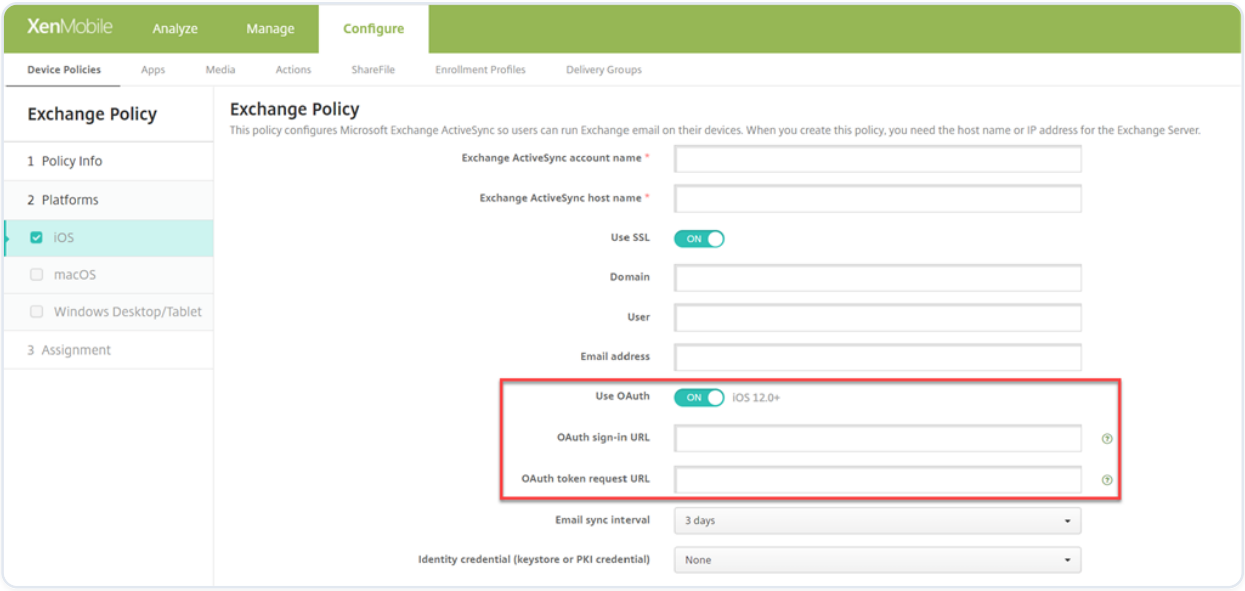
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **Nome da conta Exchange ActiveSync:** Digite a descrição da conta de e-mail que é exibida nos dispositivos do usuário.
- **Nome do host Exchange ActiveSync:** Digite o endereço do servidor de e-mail.
- **Usar SSL:** Selecione se deseja proteger as conexões entre os dispositivos do usuário e o Exchange Server. O padrão é **Ativado**.
- **Domínio:** Insira o domínio em que o Exchange Server está. Você pode usar a macro de sistema $user.domainname neste campo para pesquisar automaticamente os nomes de domínio do usuário.
- **Usuário:** Especifique o nome de usuário para a conta de usuário do Exchange. Você pode usar a macro de sistema $user.username neste campo para pesquisar automaticamente os nomes de usuário.
- **Endereço de e-mail:** Especifique o endereço de e-mail completo. Você pode usar a macro de sistema $user.mail neste campo para pesquisar automaticamente as contas de e-mail do usuário.
- **Usar OAuth:** Se definido como **Ativado**, a conexão usa OAuth para autenticação. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
    - **URL de login OAuth**: Especifica a URL a ser carregada em um webview para autenticar usando OAuth quando o Serviço AutoDiscovery não é usado. Este campo aparece apenas quando **Usar OAuth** está definido como **Ativado**.

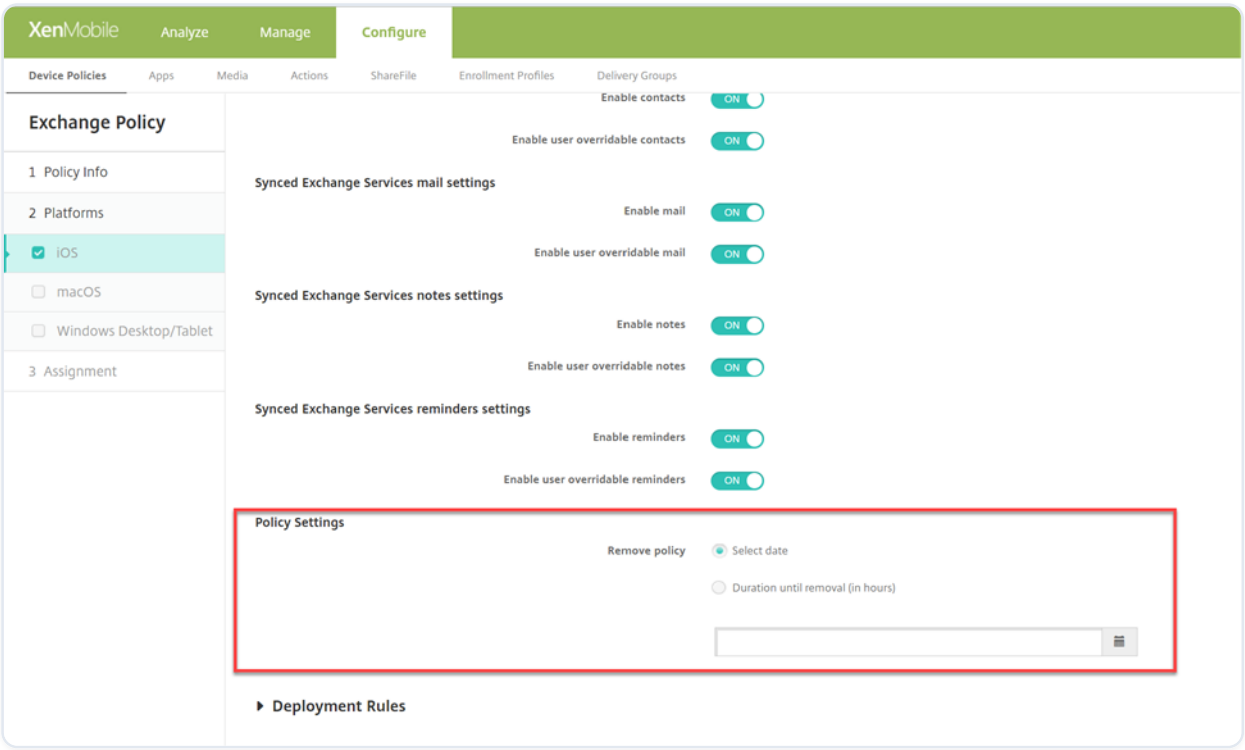
- **URL de solicitação de token OAuth**: Especifica a URL que a conta pode usar para solicitações de token OAuth. Este campo aparece apenas quando **Usar OAuth** está definido como **Ativado**.



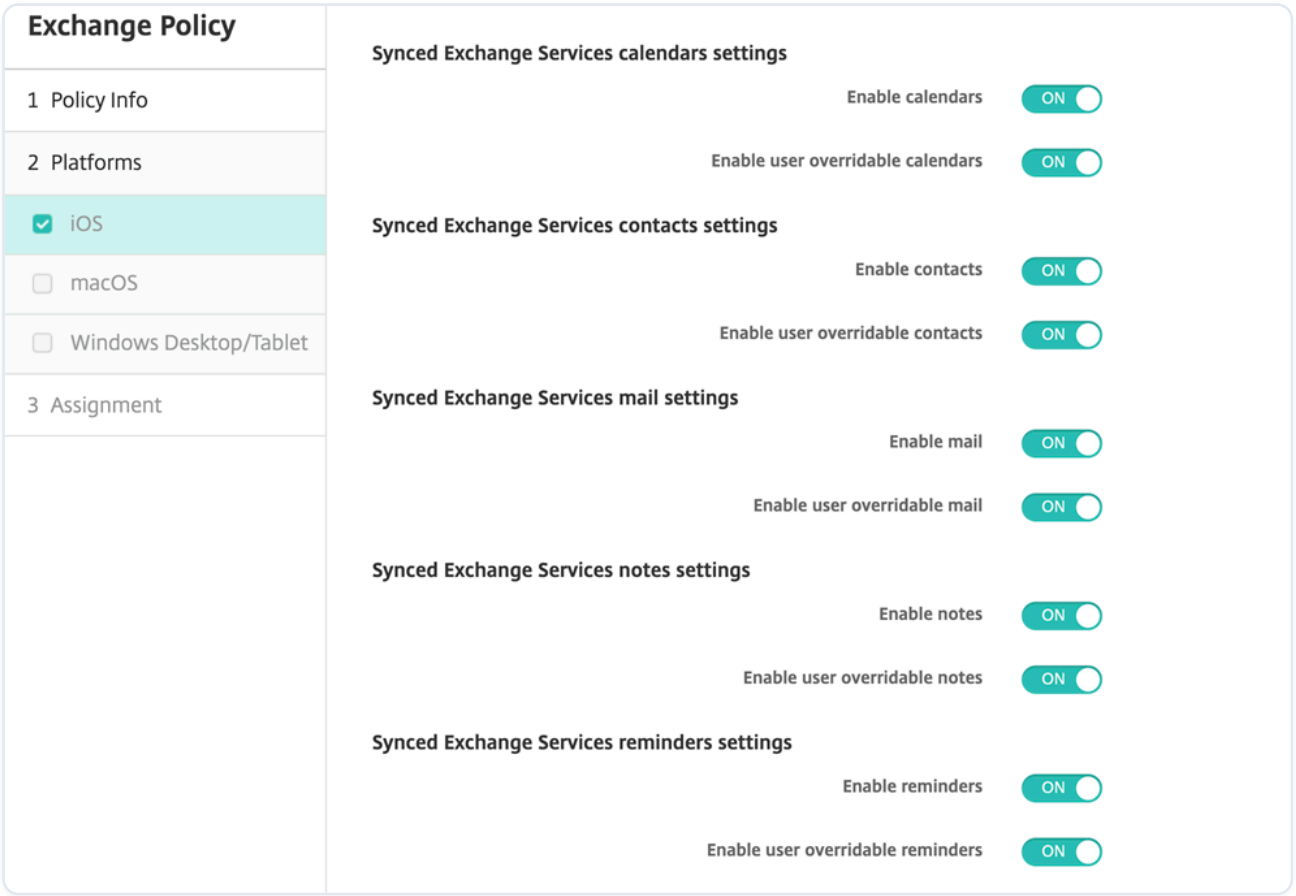
- **Senha:** Insira uma senha opcional para a conta de usuário do Exchange. Essa configuração não aparece quando **Usar OAuth** está **Ativado**.
- **Intervalo de sincronização de e-mail:** Na lista, escolha a frequência com que um e-mail é sincronizado com o Exchange Server. O padrão é **3 dias**.
- **Credencial de identidade (repositório de chaves ou PKI):** Clique em uma credencial de identidade opcional na lista suspensa se você configurou um provedor de identidade para o XenMobile. Este campo é obrigatório apenas quando o Exchange exige autenticação de certificado de cliente. O padrão é **Nenhum**.
- **Autorizar movimentação de e-mail entre contas:** Selecione se deseja permitir que os usuários movam e-mails desta conta para outra conta e encaminhem e respondam de uma conta diferente. O padrão é **Desativado**.
- **Enviar e-mail apenas do aplicativo de e-mail:** Selecione se deseja restringir os usuários ao aplicativo de e-mail do iOS para enviar e-mails. O padrão é **Desativado**.
- **Desativar sincronização recente de e-mail:** Selecione se deseja impedir que os usuários sincronizem endereços recentes. O padrão é **Desativado**. Esta opção se aplica apenas ao iOS 6.0 e posterior.
- **Permitir Mail Drop:** Selecione se deseja permitir que a conta use o Mail Drop. O padrão é **Desativado**.
- **Habilitar Assinatura S/MIME:** Selecione se esta conta oferece suporte à assinatura S/MIME. O padrão é **Ativado**. Quando definido como **Ativado**, os seguintes campos aparecem.

- **Credencial de identidade de assinatura:** Escolha a credencial de assinatura a ser usada.
- **Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
- **UUID do Certificado de Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.

- **Habilitar Criptografia S/MIME:** Selecione se esta conta oferece suporte à criptografia S/MIME. O padrão é **Desativado**. Quando definido como **Ativado**, os seguintes campos aparecem.
  - **Credencial de identidade de criptografia:** Escolha a credencial de criptografia a ser usada.
  - **Habilitar alternância S/MIME por mensagem:** Quando definido como **Ativado**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que eles compõem. O padrão é **Desativado**.
  - **S/MIME Encrypt By Default User Overrideable:** Se definido como **On**, os usuários podem, nas configurações de seus dispositivos, selecionar se o S/MIME está ativado por padrão. O padrão é **Off**. Esta opção se aplica ao iOS 12.0 e posterior.
  - **S/MIME Encryption Certificate UUID User Overrideable:** Se definido como **On**, os usuários podem ativar e desativar a identidade e a criptografia S/MIME nas configurações de seus dispositivos. O padrão é **Off**. Esta opção se aplica ao iOS 12.0 e posterior.
- **Configurações de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.



Serviços Exchange Sincronizados



- **Configurações de calendários dos Serviços Exchange Sincronizados**
  - **Habilitar calendários**: Permite habilitar ou desabilitar o serviço *Calendários* para a conta. O valor padrão é **ON**. Se for definido como **OFF**, o serviço *Calendários* será desabilitado

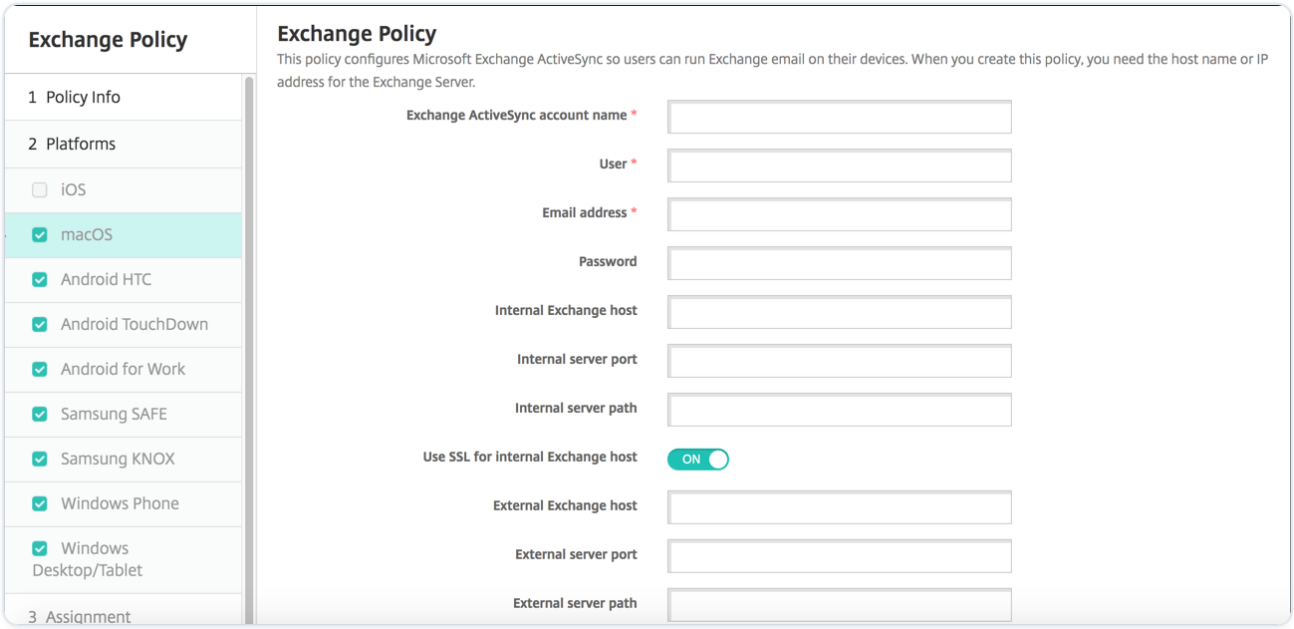
para a conta. O serviço *Calendários* pode ser habilitado novamente nas configurações, somente se o botão **Habilitar calendários substituíveis pelo usuário** estiver definido como **ON**.

- **Habilitar calendários substituíveis pelo usuário**: Permite alterar o estado do serviço *Calendários* para a conta nas configurações. O valor padrão é **ON**. Se for definido como **OFF**, você não poderá alterar o estado do serviço *Calendários*.

- **Configurações de contatos dos Serviços Exchange Sincronizados**
  - **Habilitar contatos**: Permite habilitar ou desabilitar o serviço *Contatos* para a conta. O valor padrão é **ON**. Se for definido como **OFF**, o serviço *Contatos* será desabilitado para a conta. O serviço *Contatos* pode ser habilitado novamente nas configurações, somente se o botão **Habilitar contatos substituíveis pelo usuário** estiver definido como **ON**.
  - **Habilitar contatos substituíveis pelo usuário**: Permite alterar o estado do serviço *Contatos* para a conta nas configurações. O valor padrão é **ON**. Se for definido como **OFF**, você não poderá alterar o estado do serviço *Calendários*.
- **Configurações de e-mail dos Serviços Exchange Sincronizados**
  - **Habilitar e-mail**: Permite habilitar ou desabilitar o serviço de *E-mail* para a conta. O valor padrão é **ON**. Se estiver definido como **OFF**, o serviço de *E-mail* será desabilitado para a conta. O serviço de *E-mail* pode ser habilitado novamente nas configurações, somente se o botão **Habilitar e-mail substituível pelo usuário** estiver definido como **ON**.
  - **Habilitar e-mail substituível pelo usuário**: Permite alterar o estado do serviço de *E-mail* para a conta nas configurações. O valor padrão é **ON**. Se estiver definido como **OFF**, você não poderá alterar o estado do serviço de *E-mail*.
- **Configurações de notas dos Serviços Exchange Sincronizados**
  - **Habilitar notas**: Permite habilitar ou desabilitar o serviço de *Notas* para a conta. O valor padrão é **ON**. Se estiver definido como **OFF**, o serviço de *Notas* será desabilitado para a conta. O serviço de *Notas* pode ser habilitado novamente nas configurações, somente se o botão **Habilitar notas substituíveis pelo usuário** estiver definido como **ON**.
  - **Habilitar notas substituíveis pelo usuário**: Permite alterar o estado do serviço de *Notas* para a conta nas configurações. O valor padrão é **ON**. Se estiver definido como **OFF**, você não poderá alterar o estado do serviço de *Notas*.
- **Configurações de lembretes dos Serviços Exchange Sincronizados**

- **Habilitar lembretes**: Permite habilitar ou desabilitar o serviço de *Lembretes* para a conta. O valor padrão é **ON**. Se estiver definido como **OFF**, o serviço de *Lembretes* será desabilitado para a conta. O serviço de *Lembretes* pode ser habilitado novamente nas configurações, somente se o botão **Habilitar lembretes substituíveis pelo usuário** estiver definido como **ON**.
- **Habilitar lembretes substituíveis pelo usuário**: Permite alterar o estado do serviço de *Lembretes* para a conta nas configurações. O valor padrão é **ON**. Se estiver definido como **OFF**, você não poderá alterar o estado do serviço de *Lembretes*.

Configurações do macOS

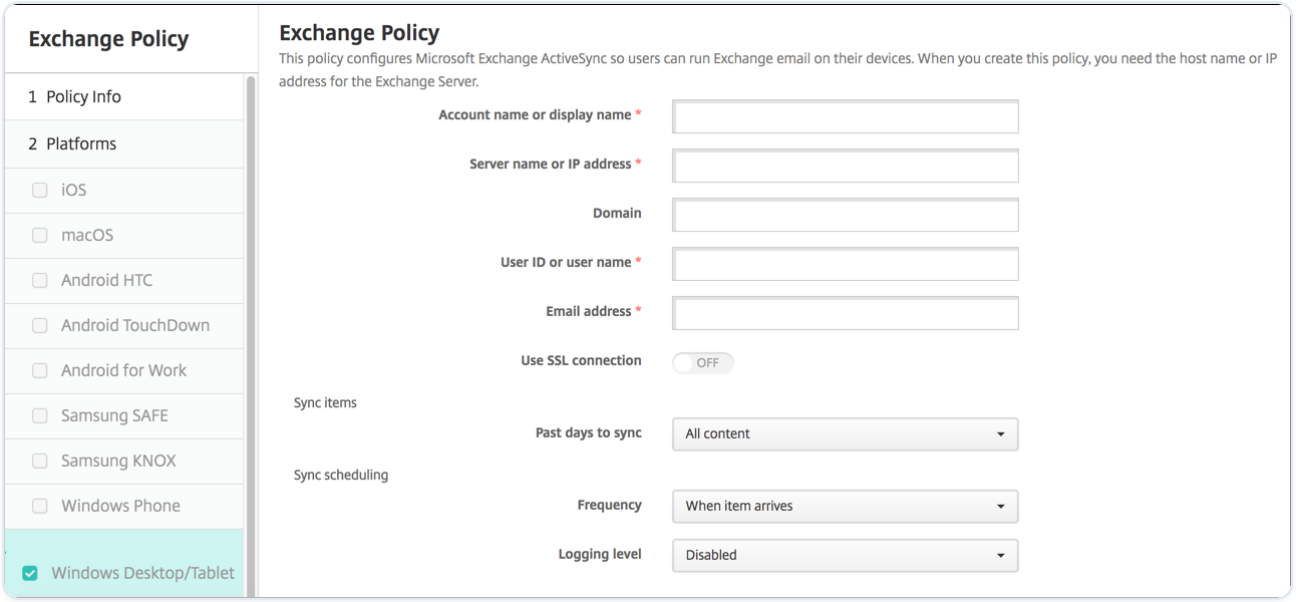


- **Nome da conta Exchange ActiveSync:** Digite a descrição da conta de e-mail que é exibida nos dispositivos do usuário.
- **Usuário:** Especifique o nome de usuário para a conta de usuário do Exchange. Você pode usar a macro de sistema $user.username neste campo para pesquisar automaticamente os nomes de usuário.
- **Endereço de e-mail:** Especifique o endereço de e-mail completo. Você pode usar a macro de sistema $user.mail neste campo para pesquisar automaticamente as contas de e-mail do usuário.
- **Usar OAuth:** Se definido como **On**, a conexão usa OAuth para autenticação. O padrão é **Off**. Esta opção se aplica ao macOS 10.14 e posterior.
- **URL de Login OAuth:** Especifica a URL a ser carregada em uma webview para autenticar usando OAuth quando o Serviço AutoDiscovery não é usado. Este campo aparece quando **Usar OAuth** está definido como **Ativado**.

- **Senha:** Insira uma senha opcional para a conta de usuário do Exchange. Esta configuração não aparece quando **Usar OAuth** está **Ativado**.
- **Host interno do Exchange:** Se você quiser que os nomes de host interno e externo do Exchange sejam diferentes, digite um nome de host interno do Exchange opcional.
- **Porta do servidor interno:** Se você quiser que as portas do servidor interno e externo do Exchange sejam diferentes, digite um número de porta do servidor interno do Exchange opcional.
- **Caminho do servidor interno:** Se você quiser que os caminhos do servidor interno e externo do Exchange sejam diferentes, digite um caminho do servidor interno do Exchange opcional.
- **Usar SSL para host interno do Exchange:** Selecione se deseja proteger as conexões entre os dispositivos do usuário e o host interno do Exchange. O padrão é **Ativado**.
- **Host externo do Exchange:** Se você quiser que os nomes de host interno e externo do Exchange sejam diferentes, digite um nome de host externo do Exchange opcional.
- **Porta do servidor externo:** Se você quiser que as portas do servidor interno e externo do Exchange sejam diferentes, digite um número de porta do servidor externo do Exchange opcional.
- **Caminho do servidor externo:** Se você quiser que os caminhos do servidor interno e externo do Exchange sejam diferentes, digite um caminho do servidor externo do Exchange opcional.
- **Usar SSL para host externo do Exchange:** Selecione se deseja proteger as conexões entre os dispositivos do usuário e o host interno do Exchange. O padrão é **Ativado**.
- **Permitir Mail Drop:** Selecione se deseja permitir que os usuários compartilhem arquivos sem fio entre dois Macs, sem precisar se conectar a uma rede existente. O padrão é **Desativado**.
- **Configurações de política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.
    - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.

- **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Configurações de Desktop/Tablet Windows



Nota:

Esta política não permite que você defina a senha do usuário. Os usuários devem definir esse parâmetro em seus dispositivos depois que você enviar a política.

- **Nome da conta ou nome de exibição:** Digite o nome da conta do Exchange ActiveSync.
- **Nome do servidor ou endereço IP:** Digite o nome do host ou endereço IP do Exchange Server.
- **Domínio:** Insira o domínio onde o Exchange Server está. Você pode usar a macro de sistema $user.domainname neste campo para pesquisar automaticamente os nomes de domínio do usuário.
- **ID de usuário ou nome de usuário:** Especifique o nome de usuário para a conta de usuário do Exchange. Você pode usar a macro de sistema $user.username neste campo para pesquisar automaticamente os nomes de usuário.
- **Endereço de e-mail:** Especifique o endereço de e-mail completo. Você pode usar a macro de sistema $user.mail neste campo para pesquisar automaticamente as contas de e-mail do usuário.

- **Usar conexão SSL:** Selecione se deseja proteger as conexões entre os dispositivos do usuário e o Exchange Server. O padrão é **Desativado**.
- **Dias anteriores para sincronizar:** Na lista, clique em quantos dias anteriores para sincronizar todo o conteúdo do dispositivo com o Exchange Server. O padrão é **Todo o conteúdo**.
- **Frequência:** Na lista, clique no agendamento a ser usado ao sincronizar dados enviados ao dispositivo do Exchange Server. O padrão é **Quando chegar**.
- **Nível de log:** Clique em **Desativado**, **Básico** ou **Avançado** na lista suspensa para especificar o nível de detalhe ao registrar a atividade do Exchange. O **padrão é Desativado**.

Política de dispositivo de arquivos

Você pode adicionar e implantar arquivos para que os usuários acessem em seus dispositivos Android e Android Enterprise. Você especifica o diretório onde deseja armazenar o arquivo no dispositivo. Por exemplo, você deseja que os usuários recebam um documento da empresa ou um arquivo .pdf. Implante o arquivo nos dispositivos e informe aos usuários onde o arquivo está localizado.

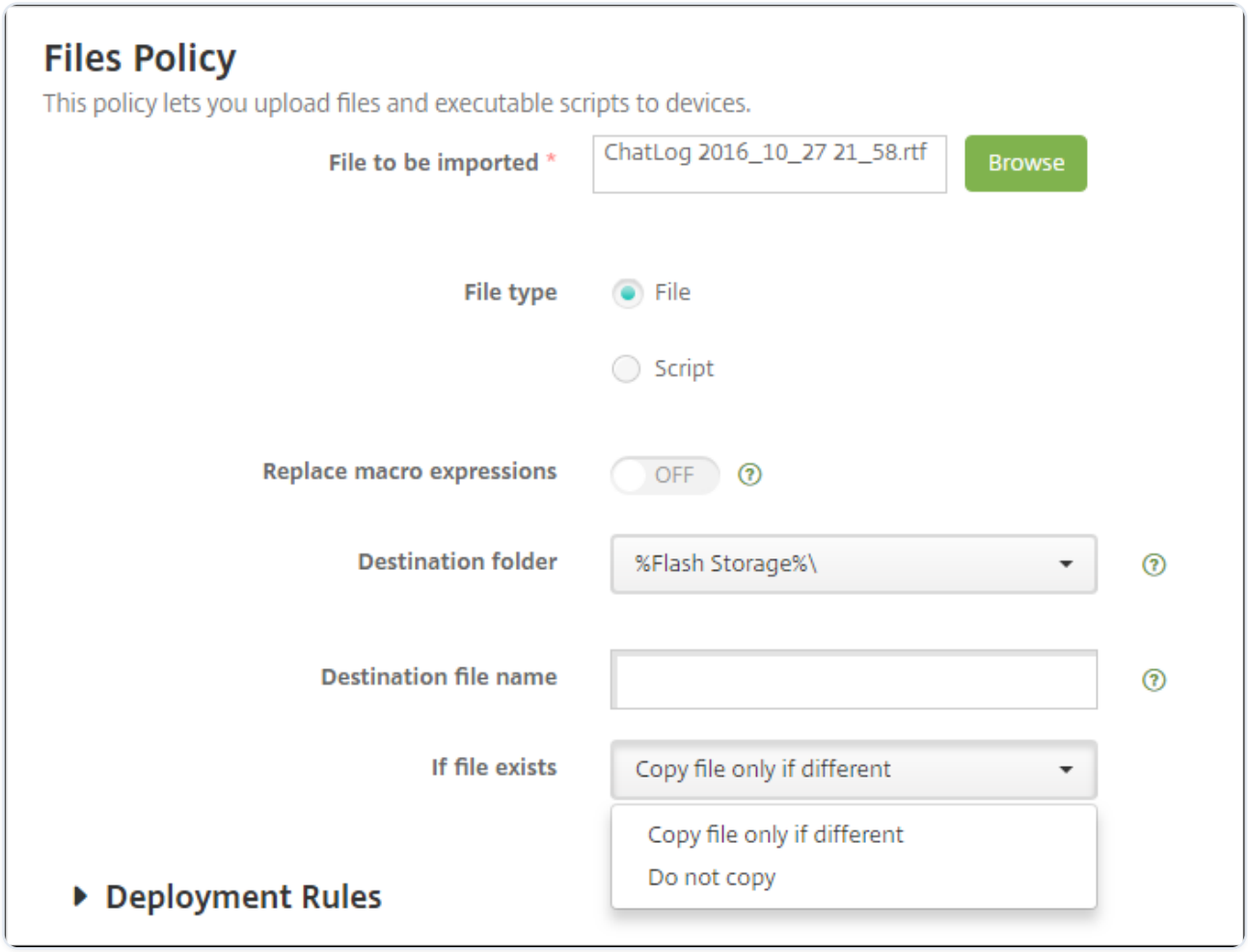
Dispositivos Android não suportam a execução de scripts nativamente. Os usuários precisam de software de terceiros para executar scripts.

Você pode adicionar os seguintes tipos de arquivo com esta política:

- Arquivos baseados em texto (.xml, .html, .py e assim por diante)
- Outros arquivos, como documentos, imagens, planilhas ou apresentações

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android Enterprise



- **Arquivo a ser importado:** Para selecionar o arquivo a ser importado, clique em **Procurar** e navegar até o local do arquivo.
- **Tipo de arquivo:** Selecione **Arquivo**.
- **Pasta de destino:** Na lista, selecione o local onde armazenar o arquivo carregado ou clique em **Adicionar novo** para escolher um local de arquivo não listado. Você pode usar as macros %XenMobile Folder%\ ou %Flash Storage%\ como o início de qualquer identificador de caminho.
- **Nome do arquivo de destino:** Opcional. Se você precisar alterar um nome de arquivo antes de implantá-lo em um dispositivo, digite o nome do arquivo.
- **Se o arquivo existir:** Na lista, selecione se deseja copiar um arquivo existente. O padrão é **Copiar arquivo somente se diferente**.

Configurações do Android

- **Arquivo a ser importado:** Selecione o arquivo a ser importado clicando em **Procurar** e navegando até o local do arquivo.

- **Tipo de arquivo:** Selecione **Arquivo**.
- **Pasta de destino:** Na lista, selecione o local onde armazenar o arquivo carregado ou clique em **Adicionar novo** para escolher um local de arquivo não listado. ALÉM DISSO, você pode usar as macros %XenMobile Folder%\\ ou %Flash Storage%\\ como o início de um identificador de caminho.
- **Nome do arquivo de destino:** Opcionalmente, digite um nome diferente para o arquivo se ele precisar ser alterado antes de ser implantado em um dispositivo.
- **Copiar arquivo somente se diferente:** Na lista, selecione se deseja copiar o arquivo caso ele seja diferente do arquivo existente. O padrão é copiar o arquivo somente se ele for diferente.

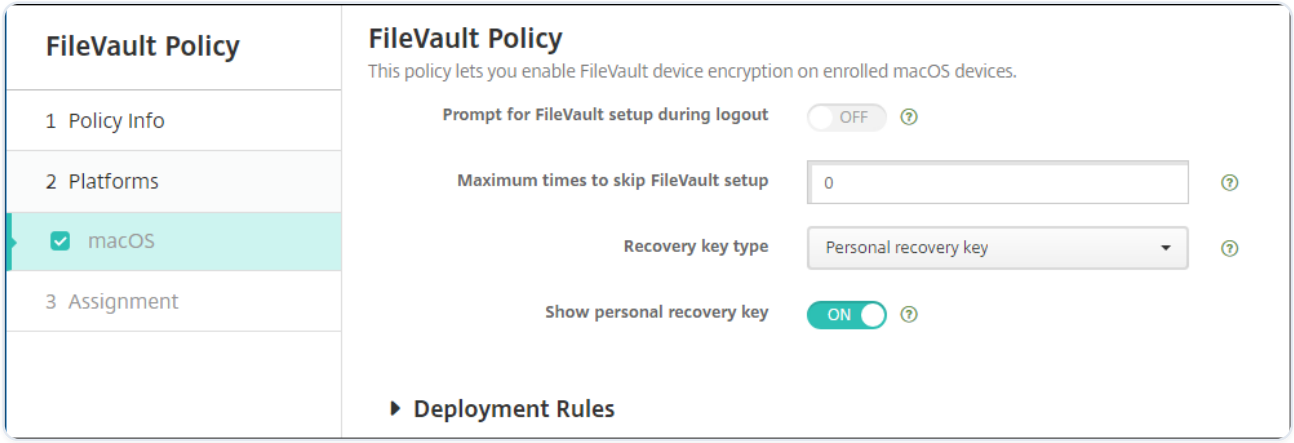
Política de dispositivo FileVault

O recurso de Criptografia de Disco FileVault do macOS protege o volume do sistema criptografando seu conteúdo. Com o FileVault ativado em um dispositivo macOS, um usuário faz login com a senha de sua conta toda vez que o dispositivo é iniciado. Se o usuário perder a senha, uma chave de recuperação permite que ele desbloqueie o disco e redefina sua senha.

A política de dispositivo XenMobile, FileVault, habilita as telas de configuração do usuário do FileVault e configura definições como chaves de recuperação. Para obter mais informações sobre o FileVault, consulte o site de suporte da Apple, `<https://support.apple.com>`.

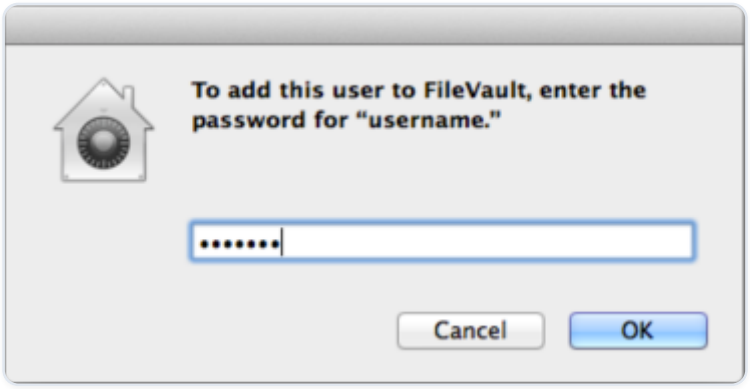
Para adicionar a política FileVault, vá para **Configurar > Políticas de Dispositivo**.

Configurações do macOS

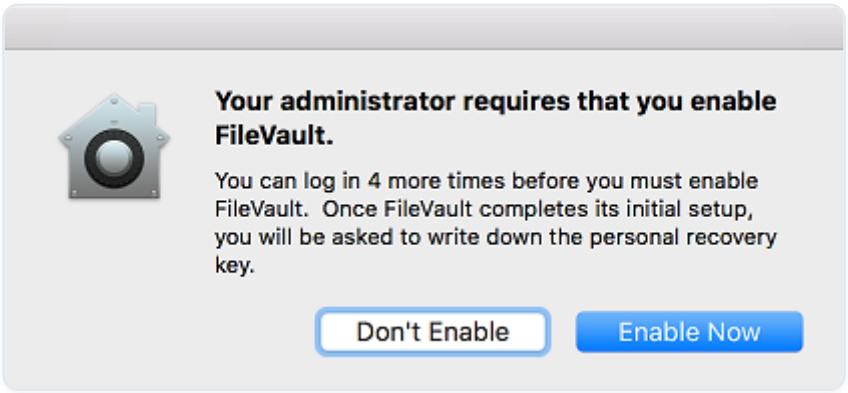


- **Solicitar configuração do FileVault durante o logout:** Se **Ativado**, solicita ao usuário que habilite o FileVault durante os próximos N logouts, conforme especificado pela opção **Número máximo de vezes para ignorar a configuração do FileVault**. Se **Desativado**, o prompt de senha do FileVault não aparece.

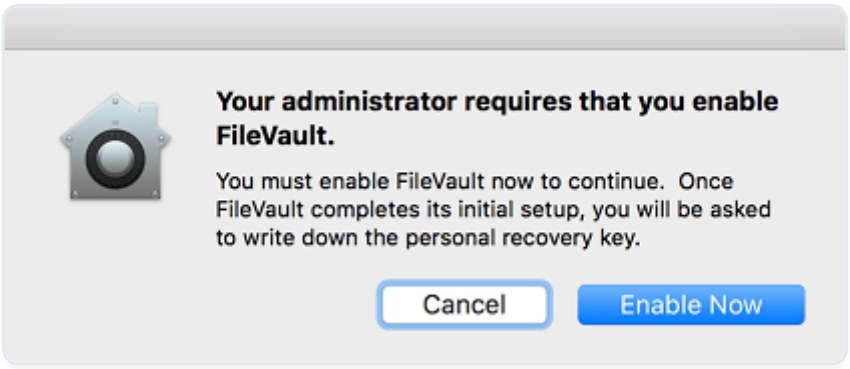
Depois de implantar a política FileVault com esta configuração ativada, a seguinte tela aparece quando um usuário faz logout do dispositivo. A tela oferece ao usuário a opção de habilitar o FileVault antes de fazer logout.

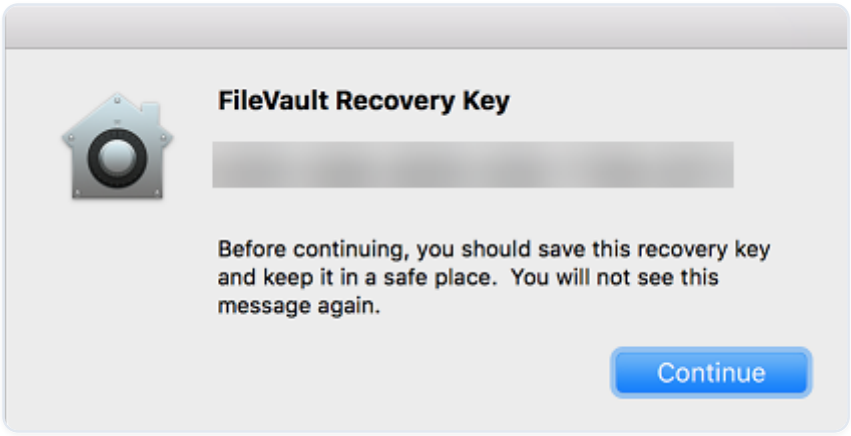


Se o valor de **Número máximo de vezes para ignorar a configuração do FileVault** não for 0: Depois de implantar a política FileVault com esta configuração desativada e, em seguida, o usuário fazer login, a seguinte tela aparece.



Se o valor de **Número máximo de vezes para ignorar a configuração do FileVault** for 0 ou o usuário tiver ignorado a configuração o número máximo de vezes, a seguinte tela aparece.





Política de dispositivo de fonte

Você pode adicionar uma política de dispositivo no XenMobile® para adicionar mais fontes a dispositivos iOS e macOS. As fontes devem ser TrueType (`.ttf`) ou OpenType (`.oft`). Coleções de fontes (`.ttc` ou `.otc`) não são suportadas.

Para iOS, esta política se aplica apenas ao iOS 7.0 e posterior.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Nome visível para o usuário:** Digite o nome que os usuários veem em suas listas de fontes.
- **Arquivo de fonte:** Selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Nome visível para o usuário:** Digite o nome que os usuários veem em suas listas de fontes.

- **Arquivo de fonte:** Selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.
  - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

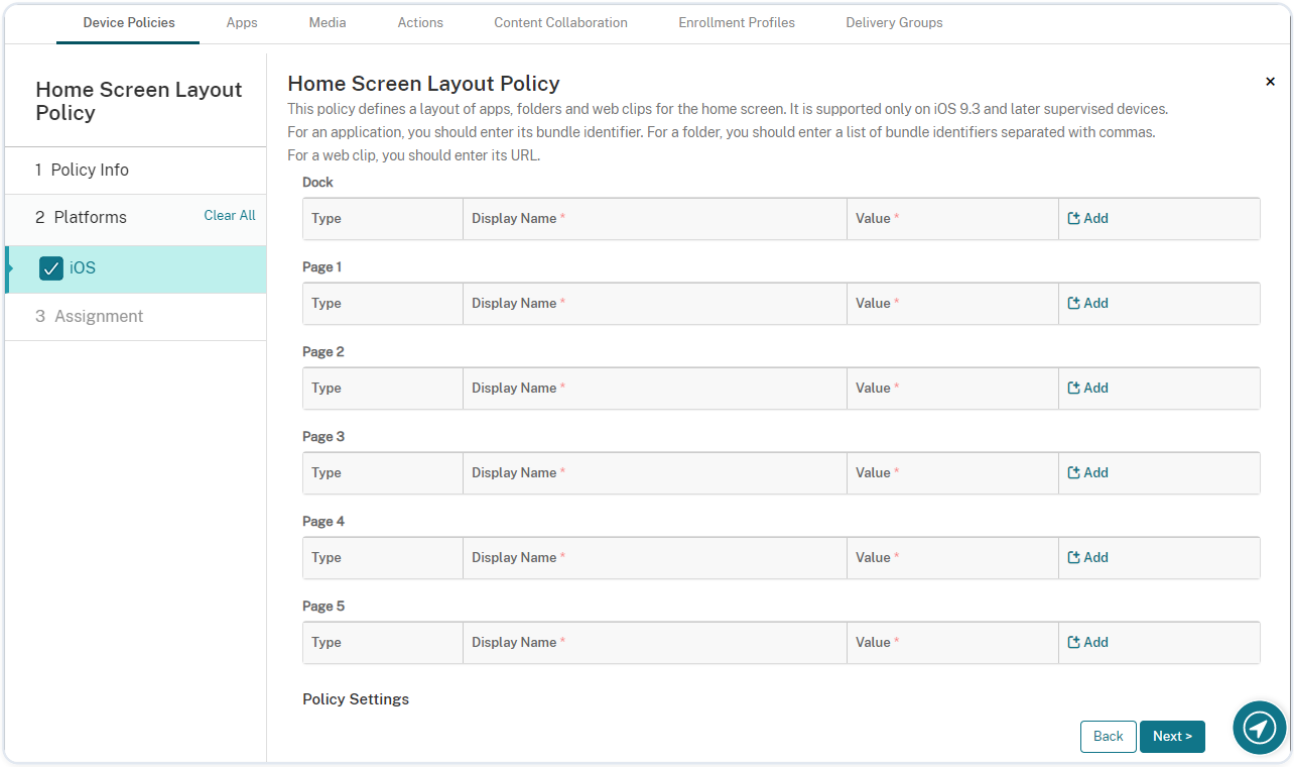
Política de dispositivo de layout da tela inicial

Você pode especificar o layout de aplicativos e pastas para a tela inicial do iOS. A política de dispositivo **Layout da tela inicial** é para dispositivos supervisionados com iOS 9.3 e posterior.

> **Importante:**
>
> A implantação de várias políticas de Layout da Tela Inicial em um dispositivo resulta em um erro do iOS no dispositivo. Essa limitação se aplica independentemente de você definir a tela inicial por meio desta política do XenMobile® ou por meio do Apple Configurator.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

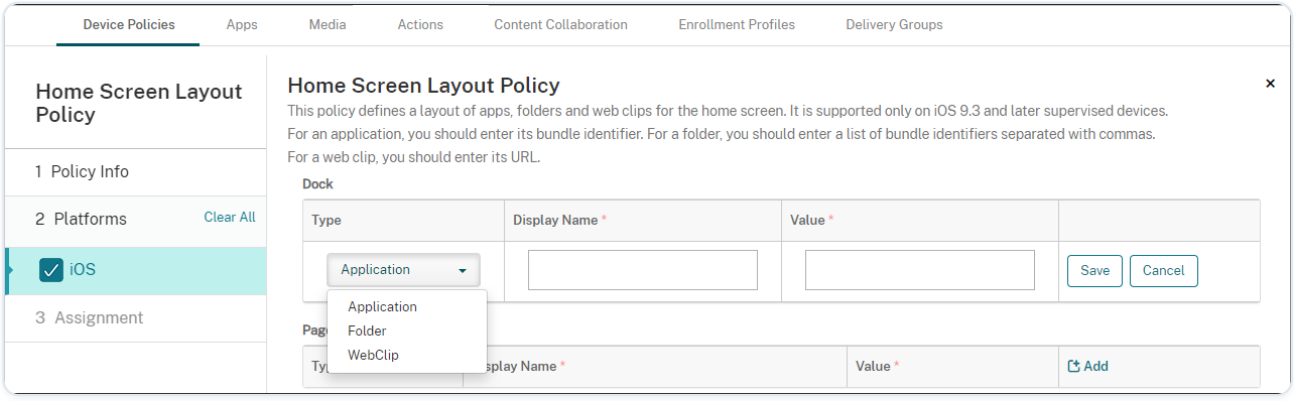
Configurações do iOS



- Para cada uma das áreas da tela que você deseja configurar (como **Dock** ou **Página 1**), clique em **Adicionar**.
- **Tipo:** Escolha **Aplicativo**, **Pasta** ou **web clip**.

  A configuração **Uso restrito de aplicativos > Permitir apenas alguns aplicativos** na política de dispositivo de Restrições pode impedir que os web clips apareçam corretamente na tela inicial. Para que os web clips apareçam corretamente, faça o seguinte:

  - Defina **Uso restrito de aplicativos** como **Permitir todos os aplicativos** ou **Não permitir alguns aplicativos**.
  - Com **Uso restrito de aplicativos** definido como **Permitir apenas alguns aplicativos**, adicione um aplicativo com o ID do pacote `com.apple.webapp` para permitir web clips.



- **Nome de Exibição:** O nome a ser exibido na tela inicial para o aplicativo ou pasta.

- **Valor:** Para aplicativos, digite o identificador do pacote. Para pastas, digite uma lista de identificadores de pacote, separados por vírgulas. Para web clips, digite o ID do pacote `com.apple.webClip.managed` e configure a URL do web clip na política de web clip. Se mais de um valor de web clip existir com a mesma URL, o comportamento será indefinido em dispositivos iOS 11.3 e posteriores.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no iOS 9.3 e posterior.

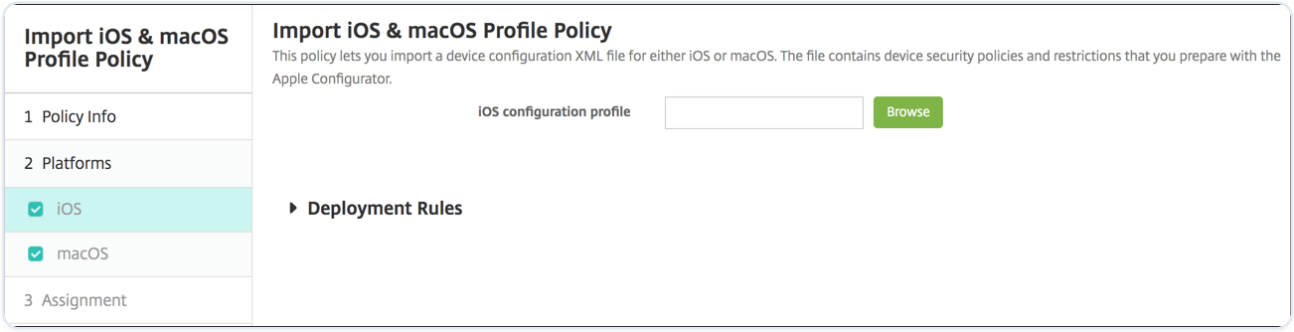
Importar política de dispositivo de perfil iOS e macOS

Você pode importar arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém políticas de segurança e restrições de dispositivo que você prepara com o Apple Configurator.

Você pode colocar um dispositivo iOS no modo Supervisionado com o Apple Configurator, conforme descrito posteriormente neste artigo. Para obter mais informações sobre como usar o Apple Configurator para criar um arquivo de configuração, consulte Suporte do Configurator da Apple.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS e macOS



- **Perfil de configuração do iOS** ou **perfil de configuração do macOS:** Para selecionar o arquivo de configuração a ser importado, clique em **Procurar** e navegar até o local do arquivo.

Colocar um dispositivo iOS no modo Supervisionado com o Apple Configurator

Para usar o Apple Configurator, você precisa de um computador Apple executando macOS 10.7.2 ou posterior.

> **Importante:**
>
> Colocar um dispositivo no modo Supervisionado instala a versão selecionada do iOS no dispositivo, apagando completamente todos os dados de usuário ou aplicativos armazenados anteriormente no dispositivo.

1. Instale o Apple Configurator do iTunes.
2. Conecte o dispositivo iOS ao seu computador Apple.
3. Inicie o Apple Configurator. O Configurator mostra que você tem um dispositivo para preparar para supervisão.
4. Para preparar o dispositivo para supervisão:
    a. Alterne o controle **Supervision** para **Ativado**. A Citrix® recomenda que você escolha essa configuração se pretende manter o controle do dispositivo de forma contínua, reaplicando uma configuração regularmente.
    b. Opcionalmente, forneça um nome para o dispositivo.
    c. No iOS, clique em **Mais recente** para a versão mais recente do iOS que você deseja instalar.
5. Quando estiver pronto para preparar o dispositivo para supervisão, clique em **Preparar**.

Política de dispositivo de Gerenciamento de Keyguard

O keyguard do Android gerencia as telas de bloqueio do dispositivo e do desafio de trabalho. Esta política permite gerenciar recursos para o keyguard do perfil de trabalho do Android Enterprise e o keyguard avançado do dispositivo. Você pode controlar:

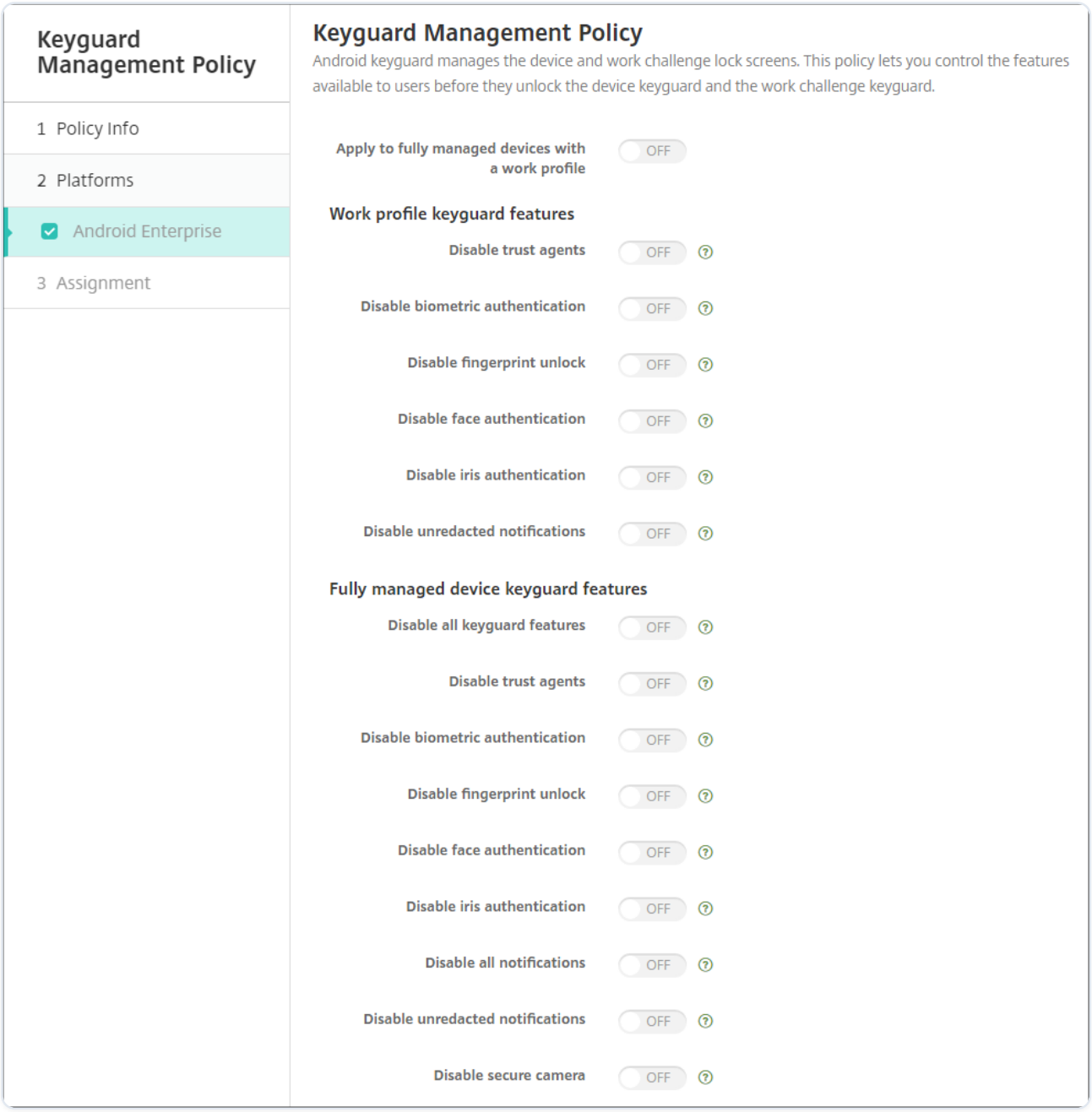
- Gerenciamento de keyguard em dispositivos com perfil de trabalho. Você pode especificar os recursos disponíveis para os usuários antes que eles desbloqueiem o keyguard do dispositivo

e o keyguard do desafio de trabalho. Por exemplo, por padrão, os usuários podem usar o desbloqueio por impressão digital e visualizar notificações não editadas na tela de bloqueio.

- Gerenciamento de keyguard em dispositivos totalmente gerenciados e dedicados. Você pode especificar os recursos disponíveis, como agentes de confiança e câmera segura, antes que eles desbloqueiem a tela do keyguard. Ou, você pode optar por desabilitar todos os recursos do keyguard.
- Gerenciamento de keyguard em dispositivos totalmente gerenciados com perfis de trabalho. Você pode usar uma política de Gerenciamento de Keyguard para aplicar configurações separadas ao dispositivo e ao perfil de trabalho.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android Enterprise



- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho:** Permite configurar as configurações da política de dispositivo de Gerenciamento de Keyguard para dispositivos totalmente gerenciados com perfis de trabalho.

  Quando esta configuração é definida como **Ativado**, você pode aplicar configurações separadas ao dispositivo e ao perfil de trabalho em dispositivos totalmente gerenciados com perfis de trabalho.

  Quando esta configuração é definida como **Desativado**, você pode aplicar configurações a dispositivos com perfil de trabalho ou a dispositivos totalmente gerenciados. As configurações que você configura para perfis de trabalho se aplicam apenas a dispositivos com perfil de

trabalho. As configurações que você configura para dispositivos totalmente gerenciados se aplicam apenas a dispositivos totalmente gerenciados.

O padrão é **Desativado**.

- **Recursos do keyguard do perfil de trabalho:** Controla se os seguintes recursos estão disponíveis antes que um usuário desbloqueie o keyguard do perfil de trabalho (tela de bloqueio).
  - **Desabilitar agentes de confiança:** Se **Desativado**, os agentes de confiança podem operar em telas de keyguard seguras quando um desafio é definido no perfil de trabalho. Defina como **Ativado** para desabilitar todos os agentes de confiança no perfil de trabalho. O padrão é **Desativado**.
  - **Desabilitar autenticação biométrica:** Se **Desativado**, a autenticação biométrica está disponível em telas de keyguard seguras quando um desafio é definido no perfil de trabalho. Defina como **Ativado** para desabilitar a autenticação biométrica no perfil de trabalho. Esta configuração desabilita o desbloqueio por impressão digital, autenticação facial e autenticação de íris. O padrão é **Desativado**. Para Android 9.0 e posterior.
  - **Desativar desbloqueio por impressão digital:** Se **Ativado**, o desbloqueio por impressão digital não estará disponível nas telas de bloqueio seguras quando um desafio for definido no perfil de trabalho. Defina como **Desativado** para ativar o desbloqueio por impressão digital no perfil de trabalho. O padrão é **Desativado**.
  - **Desativar autenticação facial:** Se **Desativado**, a autenticação facial estará disponível nas telas de bloqueio seguras quando um desafio for definido no perfil de trabalho. Defina como **Ativado** para desativar a autenticação facial no perfil de trabalho. O padrão é **Desativado**. Para Android 9.0 e posterior.
  - **Desativar autenticação de íris:** Se **Desativado**, a autenticação de íris estará disponível nas telas de bloqueio seguras quando um desafio for definido no perfil de trabalho. Defina como **Ativado** para desativar a autenticação de íris no perfil de trabalho. O padrão é **Desativado**. Para Android 9.0 e posterior.
  - **Desativar notificações não editadas:** Se **Desativado**, notificações editadas e não editadas aparecerão nas telas de bloqueio seguras. Defina como **Ativado** para desativar notificações não editadas e mostrar apenas notificações editadas. O padrão é **Desativado**.
- **Recursos de tela de bloqueio de dispositivo totalmente gerenciado:** Controla se os seguintes recursos estão disponíveis antes que um usuário desbloqueie a tela de bloqueio do dispositivo. Esses recursos se aplicam a dispositivos totalmente gerenciados ou dedicados.

- **Desativar todos os recursos da tela de bloqueio:** Se **Desativado**, todas as personalizações de tela de bloqueio atuais e futuras estarão disponíveis nas telas de bloqueio seguras. Defina como **Ativado** para desativar todas as personalizações da tela de bloqueio. O padrão é **Desativado**.
- **Desativar agentes de confiança:** Se **Desativado**, os agentes de confiança podem operar nas telas de bloqueio seguras. Defina como **Ativado** para desativar os agentes de confiança. O padrão é **Desativado**.
- **Desativar autenticação biométrica:** Se **Desativado**, a autenticação biométrica estará disponível nas telas de bloqueio seguras quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação biométrica no dispositivo. Isso desativa o desbloqueio por impressão digital, a autenticação facial e a autenticação de íris. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desativar desbloqueio por impressão digital:** Se **Desativado**, o desbloqueio por impressão digital estará disponível nas telas de bloqueio seguras quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar o desbloqueio por impressão digital no dispositivo. O padrão é **Desativado**.
- **Desativar autenticação facial:** Se **Desativado**, a autenticação facial estará disponível nas telas de bloqueio seguras quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação facial no dispositivo. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desativar autenticação de íris:** Se **Desativado**, a autenticação de íris estará disponível nas telas de bloqueio seguras quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação de íris no dispositivo. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desativar todas as notificações:** Se **Desativado**, todas as notificações aparecerão nas telas de bloqueio seguras. Defina como **Ativado** para mostrar todas as notificações. O padrão é **Desativado**.
- **Desativar notificações não editadas:** Se **Desativado**, notificações editadas e não editadas aparecerão nas telas de bloqueio seguras. Defina como **Ativado** para desativar notificações não editadas e mostrar apenas notificações editadas. O padrão é **Desativado**.
- **Desativar câmera segura:** Se **Desativado**, a câmera segura estará disponível nas telas de bloqueio seguras. Defina como **Ativado** para desativar a câmera segura. O padrão é **Desativado**.

Política de dispositivo Kiosk

A política Kiosk permite restringir dispositivos ao modo Kiosk, limitando os aplicativos que podem ser executados. O XenMobile® não controla qual parte do dispositivo é bloqueada no modo Kiosk. O dispositivo gerencia as configurações do **modo Kiosk** depois que você implanta a política.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Para adicionar uma política de dispositivo Kiosk

Todos os aplicativos que você especificar para o modo Kiosk já devem estar instalados nos dispositivos do usuário.

Algumas opções se aplicam apenas à API 4.0 e posterior do Samsung Mobile Device Management (MDM).

Configurações do Android Enterprise

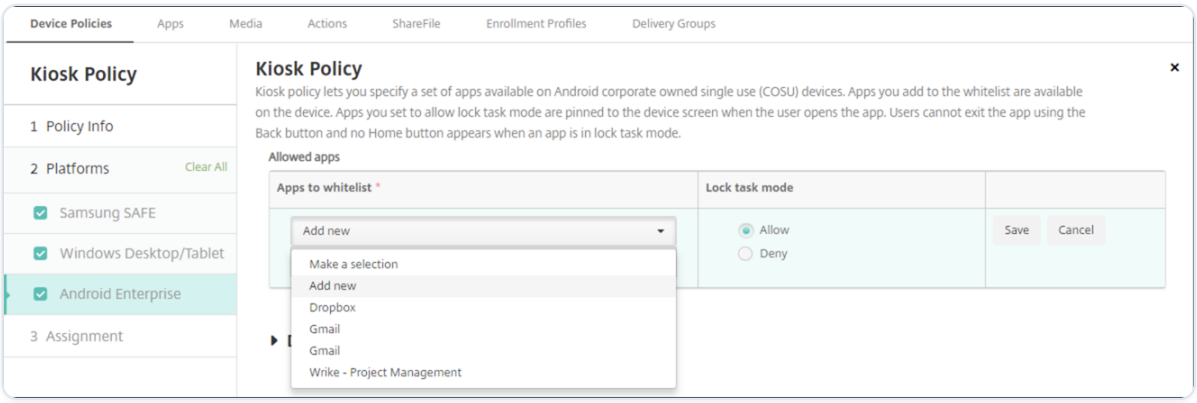
Você pode permitir aplicativos e definir o modo de bloqueio de tarefas para dispositivos Android Enterprise dedicados, também conhecidos como dispositivos de uso único de propriedade corporativa (COSU). Por padrão, o Secure Hub e os serviços do Google Play estão na lista de permissões.

Para permitir um aplicativo, clique em **Adicionar**. Você pode permitir vários aplicativos. Para obter mais informações, consulte Android Enterprise.

> **Nota:**
>
> O console do XenMobile Server inclui os termos "lista negra" e "lista branca". Estamos alterando esses termos em uma próxima versão para "lista de bloqueio" e "lista de permissões".

- **Aplicativos para lista branca:** Insira o nome do pacote do aplicativo que você deseja adicionar à lista branca ou selecione o aplicativo na lista.
  - Clique em **Adicionar novo** para inserir o nome do pacote do aplicativo aprovado para aparecer na lista.
  - Selecione o aplicativo existente na lista. A lista mostra os aplicativos que são carregados no XenMobile Server. Por padrão, o Secure Hub e os serviços do Google Play estão na

lista branca.



- **Modo de bloqueio de tarefas:** Escolha **Permitir** para definir que o aplicativo seja fixado na tela do dispositivo quando o usuário iniciar o aplicativo. Escolha **Negar** para definir que o aplicativo não seja fixado. Por padrão, o Secure Hub e os serviços do Google Play são permitidos. O padrão é **Permitir**.

Quando um aplicativo está no modo de tarefa bloqueada, ele é fixado na tela do dispositivo quando o usuário o abre. Nenhum botão Início aparece e o botão **Voltar** é desativado. O usuário sai do aplicativo usando uma ação programada no aplicativo, como sair da conta.

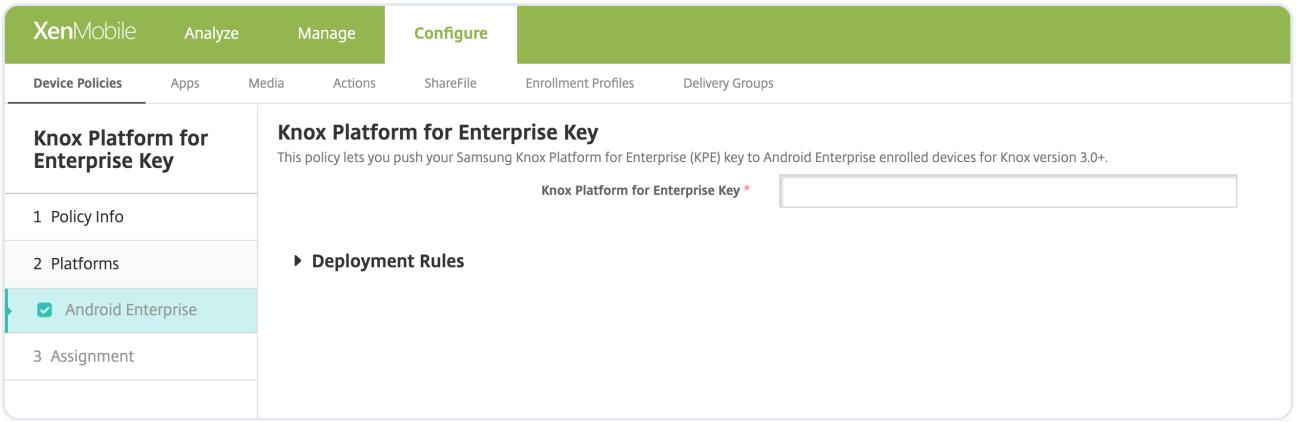
Política de dispositivo Chave da Plataforma Knox para Empresas

Esta política permite que você forneça as informações de licença necessárias da Samsung Knox Platform for Enterprise (KPE).

Para adicionar ou configurar esta política, vá para **Configurar** > **Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android Enterprise

Esta política permite que você envie sua chave de licença da Samsung Knox Platform for Enterprise (KPE) para os dispositivos registrados na plataforma Android Enterprise para Samsung Knox versão 3.0 ou posterior.



Chave da Plataforma Knox para Empresas: Insira a chave da Samsung Knox Platform for Enterprise (KPE) que você deseja enviar para o dispositivo Android Enterprise. Solicite uma chave de licença KPE em Chave da Samsung Knox Platform for Enterprise (KPE).

Política de dispositivo de configuração do Launcher

O Citrix Launcher permite personalizar a experiência do usuário para dispositivos Android implantados pelo XenMobile. O Citrix Launcher e a política de dispositivo de Configuração do Launcher não são compatíveis com o Android Enterprise.

Você pode adicionar uma política de Configuração do Launcher para controlar estes recursos do Citrix Launcher:

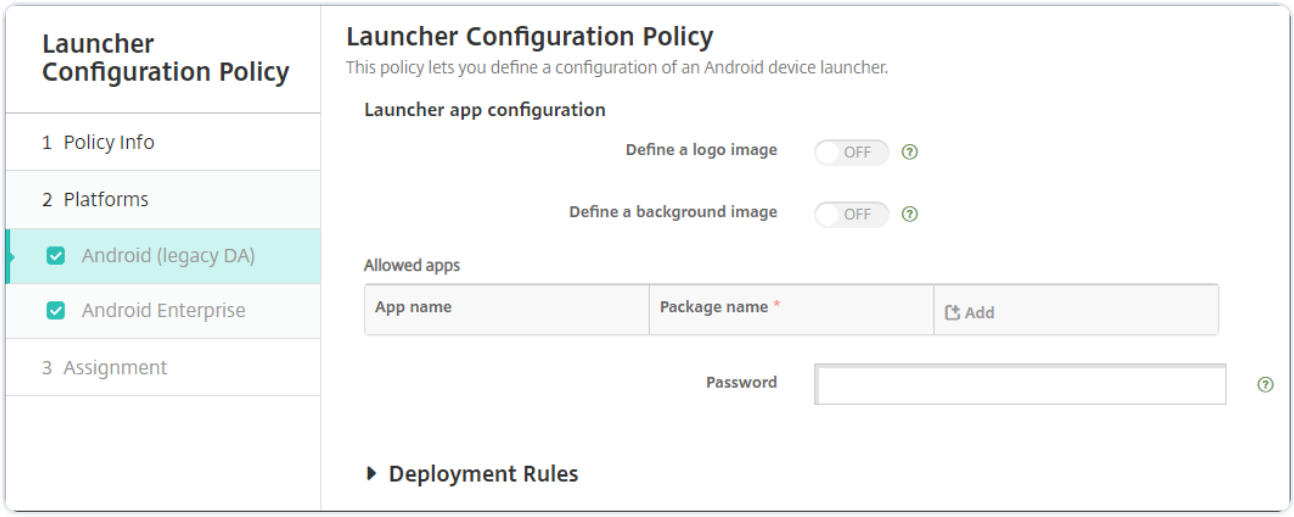
- Gerenciar dispositivos Android para que os usuários possam acessar apenas os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizada para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizada para o Citrix Launcher.
- Especifique uma senha que os usuários devem inserir para sair do launcher.

Embora o Citrix Launcher permita aplicar essas restrições no nível do dispositivo, o launcher concede aos usuários a flexibilidade operacional de que precisam por meio do acesso integrado às configurações do dispositivo, como configurações de Wi-Fi, configurações de Bluetooth e configurações de senha do dispositivo. O Citrix Launcher não se destina a ser uma camada extra de segurança além do que a plataforma do dispositivo já oferece.

Depois de implantar o Citrix Launcher, o XenMobile o instala, substituindo o launcher Android padrão.

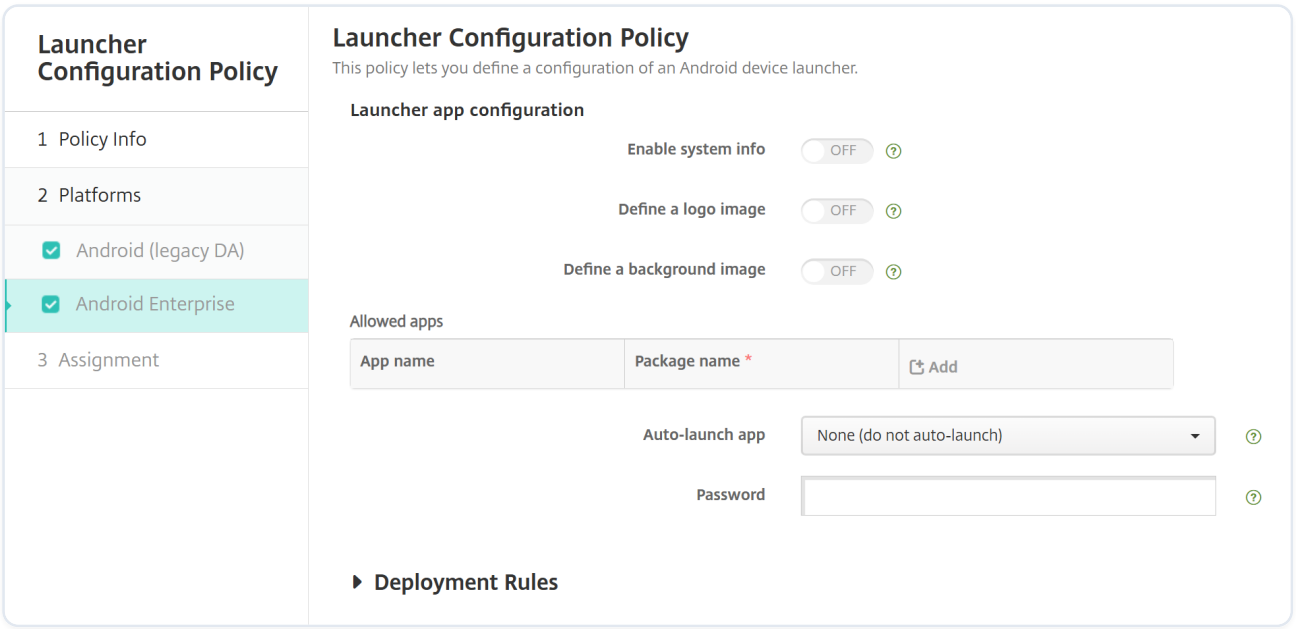
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android



- **Definir uma imagem de logotipo:** Selecione se deseja usar uma imagem de logotipo personalizada para o ícone do Citrix Launcher. O padrão é **Desativado**.
- **Imagem do logotipo:** Ao habilitar **Definir uma imagem de logotipo**, selecione o arquivo de imagem clicando em **Procurar** e navegando até o local do arquivo. Os tipos de arquivo suportados são PNG, JPG, JPEG e GIF.
- **Definir uma imagem de plano de fundo:** Selecione se deseja usar uma imagem personalizada para o plano de fundo do Citrix Launcher. O padrão é **Desativado**.
- **Imagem de plano de fundo:** Ao habilitar **Definir uma imagem de plano de fundo**, selecione o arquivo de imagem clicando em **Procurar** e navegando até o local do arquivo. Os tipos de arquivo suportados são PNG, JPG, JPEG e GIF.
- **Aplicativos permitidos:** Para cada aplicativo que você deseja permitir no Citrix Launcher, clique em **Adicionar** e faça o seguinte:
  - **Novo aplicativo a adicionar:** Insira o nome completo do aplicativo a ser adicionado. Por exemplo, com.android.calendar para o aplicativo de calendário do Android.
  - Clique em **Salvar** para adicionar o aplicativo ou clique em **Cancelar** para cancelar a adição do aplicativo.
- **Senha:** A senha que um usuário deve inserir para sair do Citrix Launcher.

Configurações do Android Enterprise



- **Habilitar informações do sistema:** Selecione se deseja exibir as informações do sistema na barra de status do Citrix Launcher. O padrão é **Desativado**. Requer Secure Hub 26.8 ou posterior.
- **Definir uma imagem de logotipo:** Selecione se deseja usar uma imagem de logotipo personalizada para o ícone do Citrix Launcher. O padrão é **Desativado**.
- **Imagem do logotipo:** Ao habilitar **Definir uma imagem de logotipo**, selecione o arquivo de imagem clicando em **Procurar** e navegando até o local do arquivo. Os tipos de arquivo suportados são PNG, JPG, JPEG e GIF.
- **Definir uma imagem de fundo:** Selecione se deseja usar uma imagem personalizada para o plano de fundo do Citrix Launcher. O padrão é **Desativado**.
- **Imagem de fundo:** Ao habilitar **Definir uma imagem de fundo**, selecione o arquivo de imagem clicando em **Procurar** e navegando até o local do arquivo. Os tipos de arquivo suportados são PNG, JPG, JPEG e GIF.
- **Aplicativos permitidos:** Para cada aplicativo que você deseja permitir no Citrix Launcher, clique em **Adicionar** e faça o seguinte:
  - **Novo aplicativo a adicionar:** Insira o nome completo do aplicativo a ser adicionado. Por exemplo, com.android.calendar para o aplicativo de calendário do Android.
  - Clique em **Salvar** para adicionar o aplicativo ou clique em **Cancelar** para cancelar a adição do aplicativo.

- **Aplicativo de inicialização automática:** Selecione um dos **Aplicativos permitidos** para iniciar automaticamente quando o Citrix Launcher for iniciado. O padrão é **Nenhum** (não iniciar automaticamente). Requer Citrix Launcher 26.8 ou posterior.
- **Senha:** A senha que um usuário deve inserir para sair do Citrix Launcher.

Política de dispositivo LDAP

Você cria uma política LDAP para dispositivos iOS no XenMobile® para fornecer informações sobre um servidor LDAP a ser usado, incluindo qualquer informação de conta necessária. A política também fornece um conjunto de políticas de pesquisa LDAP para usar ao consultar o servidor LDAP.

Você precisa do nome do host LDAP antes de configurar esta política.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Descrição da conta:** Insira uma descrição opcional da conta.
- **Nome de usuário da conta:** Insira um nome de usuário opcional.
- **Senha da conta:** Insira uma senha opcional. Use este campo apenas com perfis criptografados.
- **Nome do host LDAP:** Insira o nome do host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor LDAP. O padrão é **Ativado**.
- **Configurações de pesquisa:** Adicione configurações de pesquisa para usar ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa quiser, mas deve adicionar pelo menos uma configuração de pesquisa para tornar a conta útil. Clique em **Adicionar** e, em seguida, faça o seguinte:
    - **Descrição:** Insira uma descrição da configuração de pesquisa. Este campo é obrigatório.
    - **Escopo:** Escolha **Base**, **Um nível** ou **Subárvore** para definir a profundidade da pesquisa na árvore LDAP. O padrão é **Base**.
        - **Base** pesquisa o nó apontado pela base de pesquisa.
        - **Um nível** pesquisa o nó Base e um nível abaixo dele.

    - **Subtree** pesquisa o nó Base, mais todos os seus filhos, independentemente da profundidade.

  - **Base de pesquisa:** Insira o caminho para o nó no qual iniciar a pesquisa. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.
  - Clique em **Salvar** para adicionar a configuração de pesquisa ou clique em **Cancelar** para cancelar a adição da configuração de pesquisa.
  - Repita estas etapas para cada configuração de pesquisa que você deseja adicionar.

- **Configurações de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** Insira uma descrição opcional da conta.
- **Nome de usuário da conta:** Insira um nome de usuário opcional.
- **Senha da conta:** Insira uma senha opcional. Use este campo apenas com perfis criptografados.
- **Nome do host LDAP:** Insira o nome do host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer com o servidor LDAP. O padrão é **Ativado**.
- **Configurações de pesquisa:** Adicione configurações de pesquisa para usar ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa desejar, mas deve adicionar pelo menos uma configuração de pesquisa para tornar a conta útil. Clique em **Adicionar** e, em seguida, faça o seguinte:
  - **Descrição:** Insira uma descrição da configuração de pesquisa. Este campo é obrigatório.
  - **Escopo:** Escolha **Base**, **Um nível** ou **Subárvore** para definir a profundidade da pesquisa na árvore LDAP. O padrão é **Base**.
    - **Base** pesquisa o nó apontado pela base de pesquisa.

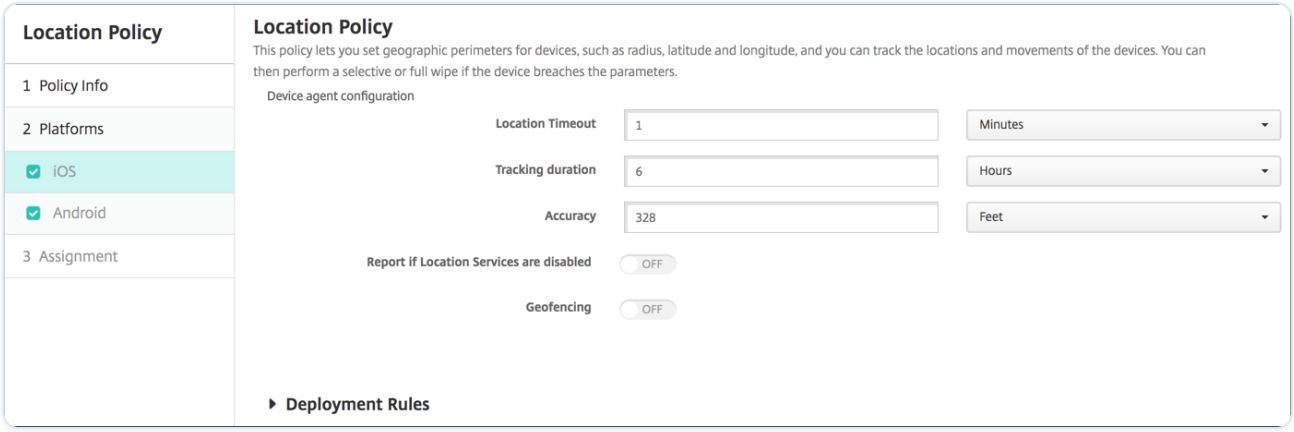
    - **Um nível** pesquisa o nó Base e um nível abaixo dele.
    - **Subárvore** pesquisa o nó Base, mais todos os seus filhos, independentemente da profundidade.
  - **Base de pesquisa:** Insira o caminho para o nó onde iniciar a pesquisa. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.
  - Clique em **Salvar** para adicionar a configuração de pesquisa ou clique em **Cancelar** para cancelar a adição da configuração de pesquisa.
  - Repita estas etapas para cada configuração de pesquisa que você deseja adicionar.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.
  - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seu dispositivo. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Política de dispositivo de localização

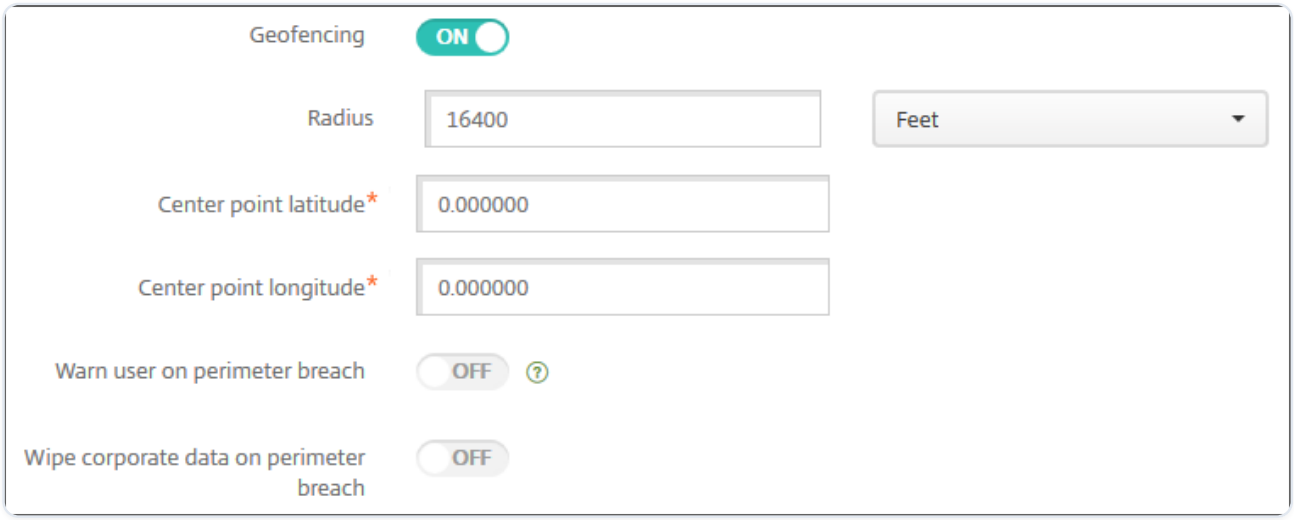
Você cria políticas de dispositivo de localização no XenMobile para impor limites geográficos. Quando os usuários violam o limite definido, também chamado de *cerca geográfica* (geofence), o XenMobile pode realizar certas ações. Por exemplo, você pode configurar a política para emitir uma mensagem de aviso aos usuários quando eles violam o perímetro definido. Você também pode configurar a política para apagar os dados corporativos dos usuários quando eles violam um perímetro, imediatamente ou após um atraso. Para obter informações sobre ações de segurança, como habilitar o rastreamento e a localização de um dispositivo, consulte Ações de segurança.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



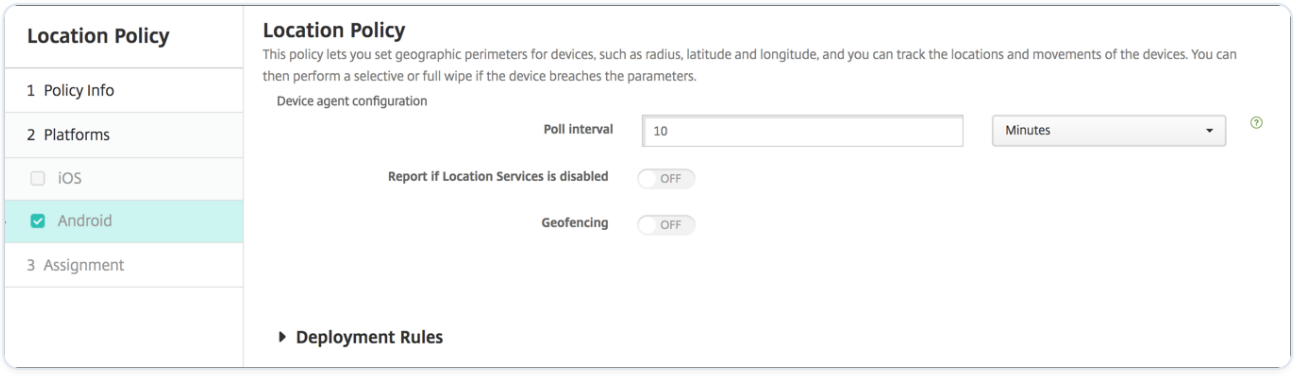
- **Tempo limite de localização:** Digite um número e, em seguida, na lista, clique em **Segundos** ou **Minutos** para definir a frequência com que o XenMobile® tenta corrigir a localização do dispositivo. Os valores válidos são 60–900 segundos ou 1–15 minutos. O padrão é 1 minuto.
- **Duração do rastreamento:** Digite um número e, em seguida, na lista, clique em **Horas** ou **Minutos** para definir por quanto tempo o XenMobile rastreia o dispositivo. Os valores válidos são 1–6 horas ou 10–360 minutos. O padrão é 6 horas.
- **Precisão:** Digite um número e, em seguida, na lista, clique em **Metros**, **Pés** ou **Jardas** para definir a que distância de um dispositivo o XenMobile rastreia o dispositivo. Os valores válidos são 10–5000 jardas ou metros, ou 30–15000 pés. O padrão é 328 pés.
- **Relatar se os Serviços de Localização estão desativados:** Selecione se o dispositivo envia um relatório ao XenMobile quando o GPS está desativado. O padrão é **Desativado**.
- **Cerca geográfica**



Ao habilitar a Cerca geográfica, configure estas definições:

- **Raio:** Digite um número e, em seguida, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Os valores válidos para o raio são:
  - 164–164000 pés
  - 50–50000 metros
  - 54–54680 jardas
  - 1–31 milhas
- **Latitude do ponto central:** Digite uma latitude, como 37.787454, para definir a latitude do ponto central da cerca geográfica.
- **Longitude do ponto central:** Digite uma longitude, como 122.402952, para definir a longitude do ponto central da cerca geográfica.
- **Avisar usuário sobre violação de perímetro:** Selecione se deseja emitir uma mensagem de aviso quando os usuários violarem o perímetro definido. O padrão é **Desativado**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **Limpar dados corporativos na violação de perímetro:** Selecione se deseja limpar os dispositivos dos usuários quando eles violarem o perímetro. O padrão é **Desativado**. Ao habilitar esta opção, o campo **Atraso na limpeza local** aparece.
  - Digite um número e, em seguida, na lista, clique em **Segundos** ou **Minutos** para definir o período de atraso antes de limpar os dados corporativos dos dispositivos dos usuários. Essa configuração oferece aos usuários a oportunidade de retornar ao local permitido antes que o XenMobile limpe seletivamente seus dispositivos. O padrão é 0 segundos.

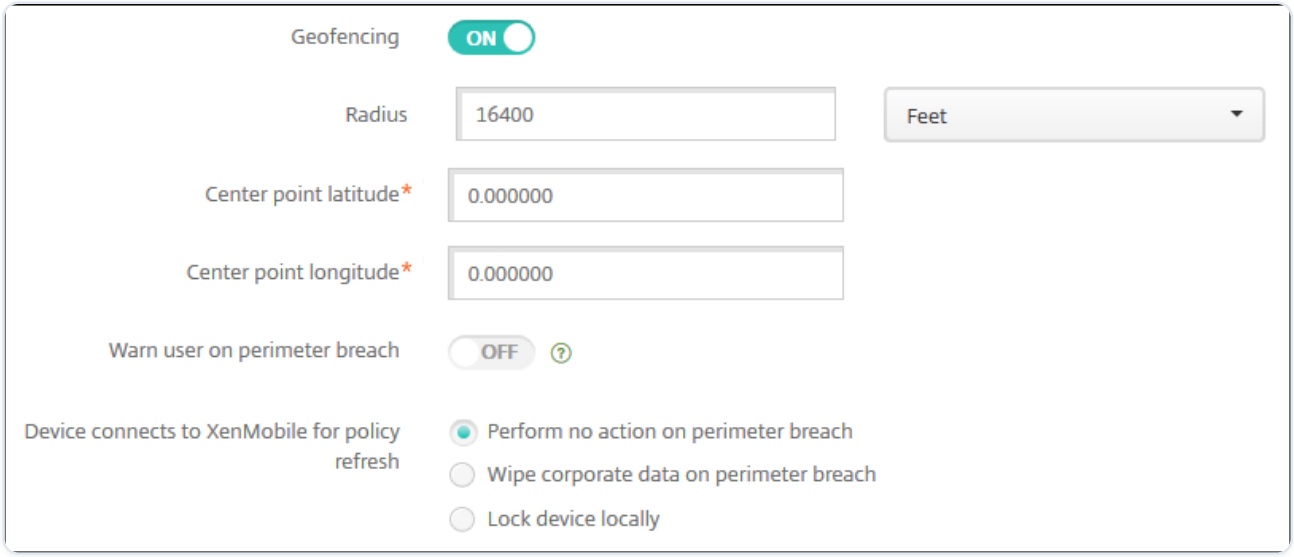
Configurações do Android



- **Intervalo de sondagem:** Digite um número e, em seguida, na lista, clique em **Minutos**, **Horas** ou **Dias** para definir a frequência com que o XenMobile tenta corrigir a localização do dispositivo. Os valores válidos são 1–1440 minutos, 1–24 horas ou qualquer número de dias.

O padrão é 10 minutos. Definir este valor para menos de 10 minutos pode afetar negativamente a vida útil da bateria do dispositivo.

- **Relatar se os Serviços de Localização estão desativados:** Selecione se o dispositivo envia um relatório ao XenMobile quando o GPS está desativado. O padrão é **Desativado**.
- **Cerca geográfica**



Ao habilitar a Cerca geográfica, configure estas definições:

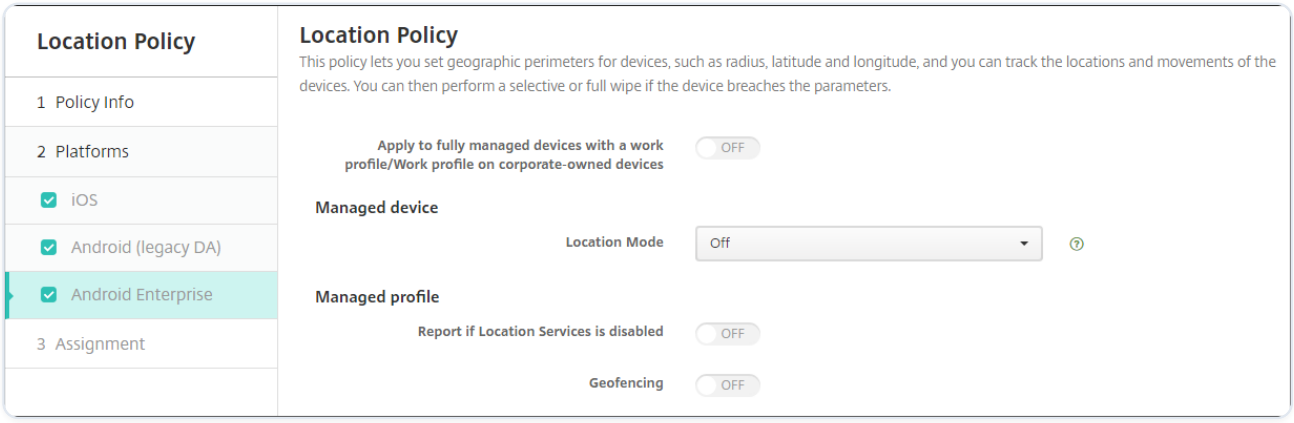
- **Raio:** Digite um número e, em seguida, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Os valores válidos para o raio são:
  - 164–164000 pés
  - 1–50 quilômetros
  - 50–50000 metros
  - 54–54680 jardas
  - 1–31 milhas
- **Latitude do ponto central:** Digite uma latitude, como 37.787454, para definir a latitude do ponto central da cerca geográfica.
- **Longitude do ponto central:** Digite uma longitude, como 122.402952, para definir a longitude do ponto central da cerca geográfica.
- **Alertar usuário sobre violação de perímetro:** Selecione se deseja emitir uma mensagem de aviso quando os usuários violarem o perímetro definido. O padrão é **Desativado**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **Dispositivo se conecta ao XenMobile para atualização de política:** Selecione uma das seguintes opções para quando os usuários violarem o perímetro:

- **Não executar nenhuma ação na violação de perímetro:** Não faça nada. Esta configuração é a padrão.
- **Limpar dados corporativos na violação de perímetro:** Limpe os dados corporativos após um período de tempo especificado. Quando você habilita esta opção, o campo **Atraso na limpeza local** aparece.
  - Digite um número e, em seguida, na lista, clique em Segundos ou Minutos para definir o período de tempo de atraso antes de limpar os dados corporativos dos dispositivos dos usuários. Essa configuração oferece aos usuários a oportunidade de retornar ao local permitido antes que o XenMobile limpe seletivamente seus dispositivos. O padrão é 0 segundos.
- **Atraso no bloqueio:** Bloqueie os dispositivos dos usuários após um período de tempo especificado. Quando você habilita esta opção, o campo **Atraso no bloqueio** aparece.
  - Digite um número e, em seguida, na lista, clique em Segundos ou Minutos para definir o período de tempo de atraso antes de bloquear os dispositivos dos usuários. Essa configuração oferece aos usuários a oportunidade de retornar ao local permitido antes que o XenMobile bloqueie seus dispositivos. O padrão é 0 segundos.

Configurações do Android Enterprise

Para que o rastreamento de localização do Android funcione, certifique-se de que os seguintes requisitos sejam atendidos:

- Android 8.5 ou posterior
- A configuração **Permitir compartilhamento de localização** ativada na política de dispositivo Restrições para Android Enterprise
- Agendamento de conexão (Firebase Cloud Messaging recomendado)



Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho

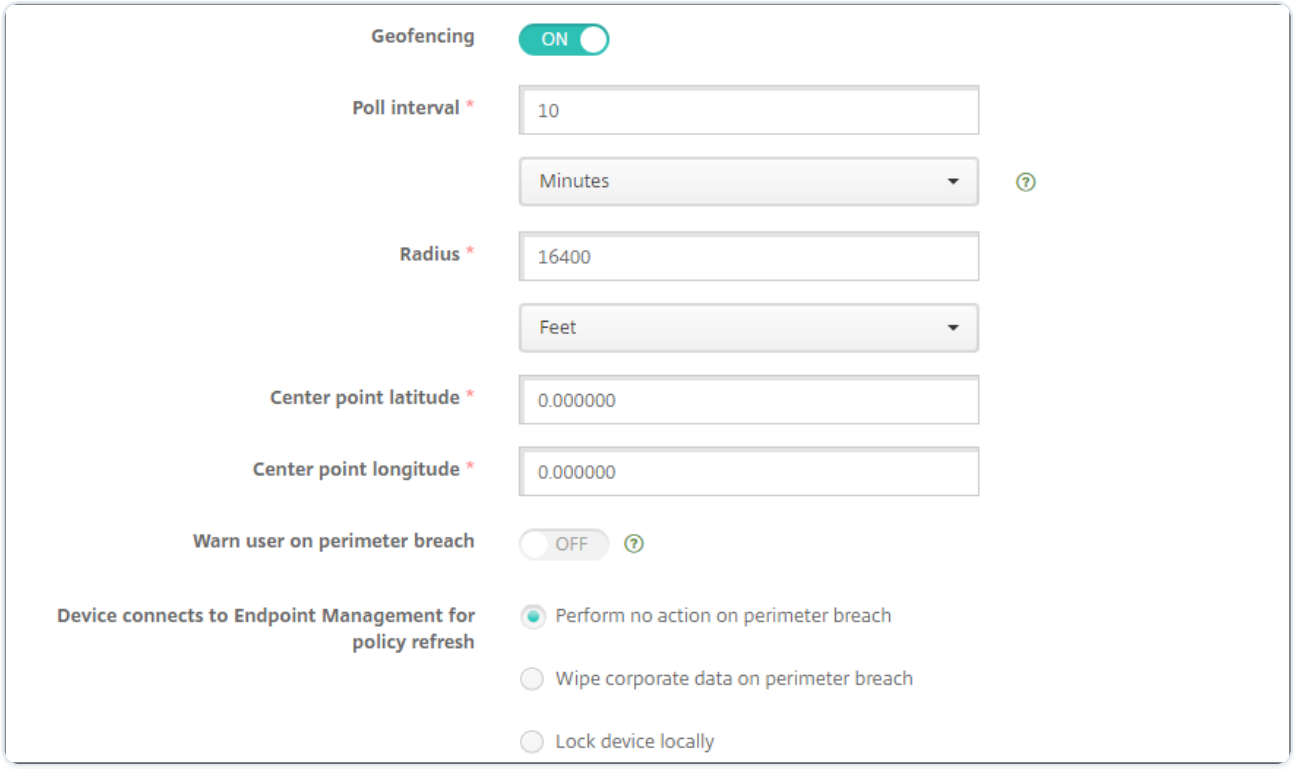
Para dispositivos totalmente gerenciados com perfis de trabalho, apenas a configuração do modo de localização está disponível.

- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa:** Permite configurar o modo de localização para dispositivos totalmente gerenciados com perfis de trabalho. Quando esta configuração está ativada, configure as configurações do modo de localização para o perfil de trabalho:
  - **Relatar se os Serviços de Localização estão desativados:** Selecione se o dispositivo envia um relatório para o XenMobile Server quando o usuário desativa o GPS. O padrão é **Desativado**.
  - **Geocercamento:** Consulte as configurações neste artigo em Dispositivo gerenciado.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa** está desativado, as configurações se aplicam ao dispositivo gerenciado e ao perfil de trabalho, conforme mostrado nas seções a seguir. O padrão é **Desativado**.

Dispositivo gerenciado

- **Modo de Localização:** Especifique o grau de detecção de localização a ser ativado. Você pode usar a ação de segurança **Localizar** apenas quando o modo de localização estiver definido como Alta Precisão ou Economia de Bateria. O padrão é Alta Precisão.
  - **Alta Precisão:** Ativa todos os métodos de detecção de localização, incluindo GPS, redes e outros sensores.
  - **Somente Sensores:** Ativa apenas GPS e outros sensores.
  - **Economia de bateria:** Habilita apenas o provedor de localização de rede.
  - **Desativado:** Desabilita a detecção de localização.
- **Geocercamento:**



Ao habilitar o **Geocercamento**, configure estas definições:

- **Intervalo de sondagem:** Digite um número e clique em **Minutos**, **Horas** ou **Dias** para definir a frequência com que o XenMobile Server tenta corrigir a localização do dispositivo. Os valores válidos são 1 a 1440 minutos, 1 a 24 horas ou qualquer número de dias. O padrão é **10 minutos**. Definir este valor para menos de 10 minutos pode afetar negativamente a vida útil da bateria do dispositivo.
- **Raio:** Digite um número e clique nas unidades a serem usadas para medir o raio. O padrão é **16400 pés** (**5000 metros**). Os valores válidos para o raio são:
  - 164–164000 pés
  - 1–50 quilômetros
  - 50–50000 metros
  - 54–54680 jardas
  - 1–31 milhas
- **Latitude do ponto central:** Digite uma latitude, como 37.787454, para definir a latitude do ponto central do geocerca. Para consultar o valor, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Proteger** e, em seguida, clique em **Localizar**. Após localizar o dispositivo, o XenMobile Server relata a localização do dispositivo na página **Detalhes > Geral** do dispositivo, em **Segurança**.

- **Longitude do ponto central:** Digite uma longitude, como 122.402952, para definir a longitude do ponto central do geocerca.
- **Alertar usuário sobre violação de perímetro:** Selecione se deseja emitir uma mensagem de aviso quando os usuários violarem o perímetro definido. O padrão é **Desativado**. Nenhuma conexão com o XenMobile Server é necessária para exibir a mensagem de aviso.
- **O dispositivo se conecta ao XenMobile Server para atualização de política:** Selecione uma das seguintes opções para quando os usuários violarem o perímetro:
  - **Não executar nenhuma ação em caso de violação do perímetro:** Não fazer nada. Esta configuração é o padrão.
  - **Limpar dados corporativos em caso de violação do perímetro:** Limpar dados corporativos após um período de tempo especificado. Ao habilitar esta opção, o campo **Atraso na limpeza local** aparece.
    - Digite um número e clique em **Segundos** ou **Minutos** para definir o período de tempo de atraso antes de limpar os dados corporativos dos dispositivos dos usuários. O atraso dá aos usuários a oportunidade de retornar ao local permitido antes que o XenMobile Server limpe seletivamente seus dispositivos. O padrão é **0 segundos**.
  - **Bloquear dispositivo localmente:** Bloquear os dispositivos dos usuários após um período de tempo especificado. Ao habilitar esta opção, o campo **Atraso no bloqueio** aparece.
    - Digite um número e clique em **Segundos** ou **Minutos** para definir o período de tempo de atraso antes de bloquear os dispositivos dos usuários. O atraso dá aos usuários a oportunidade de retornar ao local permitido antes que o XenMobile Server bloqueie seus dispositivos. O padrão é **0 segundos**.

Perfil gerenciado

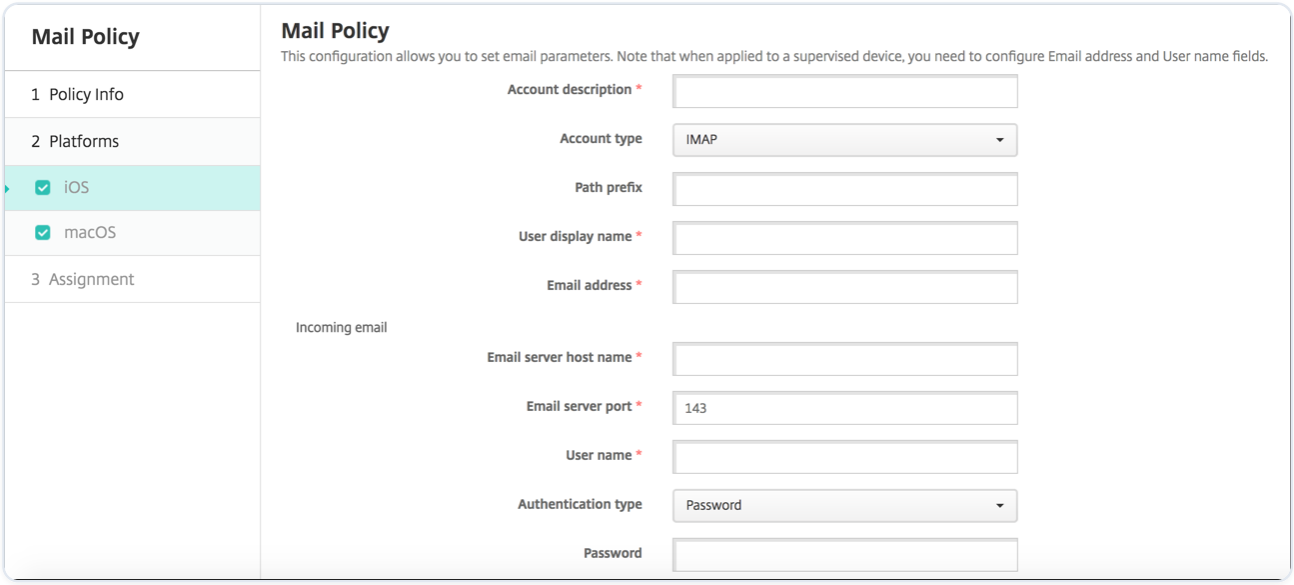
- **Relatar se os Serviços de Localização estão desativados:** Selecione se o dispositivo envia um relatório ao XenMobile Server quando o usuário desativa o GPS. O padrão é **Desativado**.
- **Geofencing:** Consulte as configurações neste artigo em Dispositivo gerenciado.

Política de dispositivo de e-mail

Você pode adicionar uma política de dispositivo de e-mail no XenMobile® para configurar uma conta de e-mail em dispositivos iOS ou macOS.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS e macOS



- **Descrição da conta:** Digite uma descrição da conta que aparece nos aplicativos Mail e Ajustes. Este campo é obrigatório.
- **Tipo de conta:** Escolha **IMAP** ou **POP** para selecionar o protocolo a ser usado para contas de usuário. O padrão é **IMAP**. Ao selecionar **POP**, a opção de prefixo de **Caminho** a seguir desaparece.
- **Prefixo do caminho:** Digite **INBOX** ou o prefixo do caminho da sua conta de e-mail IMAP. Este campo é obrigatório.
- **Nome de exibição do usuário:** Digite o nome de usuário completo a ser usado para mensagens e outros fins. Este campo é obrigatório.
- **Endereço de e-mail:** Digite o endereço de e-mail completo para a conta. Este campo é obrigatório.
- **Configurações de e-mail de entrada**
  - **Nome do host do servidor de e-mail:** Digite o nome do host ou endereço IP do servidor de e-mail de entrada. Este campo é obrigatório.
  - **Porta do servidor de e-mail:** Digite o número da porta do servidor de e-mail de entrada. O padrão é **143**. Este campo é obrigatório.
  - **Nome de usuário:** Digite o nome de usuário para a conta de e-mail. Este nome geralmente é o mesmo que o endereço de e-mail até o caractere @. Este campo é obrigatório.
  - **Tipo de autenticação:** Escolha o tipo de autenticação a ser usado. O padrão é **Senha**. Quando **Nenhum** é selecionado, o campo **Senha** a seguir desaparece.
  - **Senha:** Digite uma senha opcional para o servidor de e-mail de entrada.

- **Usar SSL:** Selecione se o servidor de e-mail de entrada usa autenticação Secure Socket Layer. O padrão é **Desativado**.

- **Configurações de e-mail de saída**
  - **Nome do host do servidor de e-mail:** Digite o nome do host ou endereço IP do servidor de e-mail de saída. Este campo é obrigatório.
  - **Porta do servidor de e-mail:** Digite o número da porta do servidor de e-mail de saída. Se nenhuma porta for inserida, a porta padrão para o protocolo fornecido será usada.
  - **Nome de usuário:** Digite o nome de usuário para a conta de e-mail. Este nome é geralmente o mesmo que o endereço de e-mail até o caractere @. Este campo é obrigatório.
  - **Tipo de autenticação:** Escolha o tipo de autenticação a ser usado. O padrão é **Senha**.
  - **Senha:** Digite uma senha opcional para o servidor de e-mail de saída.
  - **Senha de saída igual à de entrada:** Selecione se as senhas de entrada e saída são as mesmas. O padrão é **Desativado**, o que significa que as senhas são diferentes.
  - **Usar SSL:** Selecione se o servidor de e-mail de saída usa autenticação Secure Socket Layer. O padrão é **Desativado**.

- **Política**
  - **Autorizar movimentação de e-mail entre contas:** Selecione se deseja permitir que os usuários movam e-mails desta conta para outra conta e para encaminhar e responder de uma conta diferente. O padrão é **Desativado**.
  - **Enviar e-mail apenas do aplicativo de e-mail:** Selecione se deseja restringir os usuários ao aplicativo de e-mail do iOS para enviar e-mails.
  - **Desativar sincronização de e-mails recentes:** Selecione se deseja impedir que os usuários sincronizem endereços recentes. O padrão é **Desativado**. Esta opção se aplica apenas ao iOS 6.0 e posterior.
  - **Permitir Mail Drop:** Selecione se deseja permitir o uso do Apple Mail Drop para dispositivos com iOS 9.2 e posterior. O padrão é **Desativado**.
  - **Habilitar Assinatura S/MIME:** Selecione se esta conta oferece suporte à assinatura S/MIME. O padrão é **Ativado**. Quando definido como **Ativado**, os seguintes campos aparecem.
    - **Credencial de identidade de assinatura:** Escolha a credencial de assinatura a ser usada.

    - **Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
    - **UUID do Certificado de Assinatura S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.

  - **Habilitar Criptografia S/MIME:** Selecione se esta conta oferece suporte à criptografia S/MIME. O padrão é **Desativado**. Quando definido como **Ativado**, os seguintes campos aparecem.

    - **Credencial de identidade de criptografia:** Escolha a credencial de criptografia a ser usada.
    - **Habilitar alternância S/MIME por mensagem:** Quando definido como **Ativado**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que eles compõem. O padrão é **Desativado**.
    - **Criptografia S/MIME por Padrão Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem, nas configurações de seus dispositivos, selecionar se o S/MIME está ativado por padrão. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.
    - **UUID do Certificado de Criptografia S/MIME Substituível pelo Usuário:** Se definido como **Ativado**, os usuários podem ativar e desativar a identidade e a criptografia S/MIME nas configurações de seus dispositivos. O padrão é **Desativado**. Esta opção se aplica ao iOS 12.0 e posterior.

- **Configurações de Política**

  - **Remover política:** Para remover a política posteriormente, você pode configurar esta definição para remover a política em uma **Data selecionada** ou por uma **Duração até a remoção (em horas)**.
  - **Permitir que o usuário remova a política:** Permitir que os usuários removam a política de e-mail **Sempre**, somente com uma **Senha necessária**, ou **Nunca**.
  - **Escopo do perfil:** Somente para macOS, escolha se a política se aplica no nível de **Usuário** ou em todo o **Sistema**.

Política de configurações gerenciadas

A política de dispositivo de configurações gerenciadas controla várias opções de configuração de aplicativo e restrições de aplicativo. O desenvolvedor do aplicativo define as opções e dicas de ferramentas disponíveis para um aplicativo. Se uma dica de ferramenta mencionar o uso de um "valor de modelo", use a macro XenMobile correspondente. Para obter mais informações, consulte Visão geral da configuração remota (no site do desenvolvedor Android) e Macros.

As configurações do aplicativo podem incluir itens como:

- Configurações de e-mail do aplicativo
- Permitir ou bloquear URLs para um navegador da web
- Opção para controlar a sincronização de conteúdo do aplicativo por meio de uma conexão celular ou apenas por uma conexão Wi-Fi

Para obter informações sobre as configurações que aparecem para seus aplicativos, entre em contato com o desenvolvedor do aplicativo.

Pré-requisitos

- Conclua as tarefas de configuração do Android Enterprise no Google e conecte o Android Enterprise ao Google Play gerenciado. Para obter mais informações, consulte Android Enterprise.
- Adicione aplicativos Android Enterprise ao XenMobile. Para obter mais informações, consulte Adicionar aplicativos ao XenMobile.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Requisitos para VPNs por aplicativo

Para criar uma VPN por aplicativo para AE, você precisa realizar etapas adicionais, além de configurar a política de configurações gerenciadas. Além disso, você deve verificar se os seguintes pré-requisitos são atendidos:

- Citrix Gateway local
- Os seguintes aplicativos estão instalados no dispositivo:
  - Citrix SSO
  - Citrix Secure Hub™

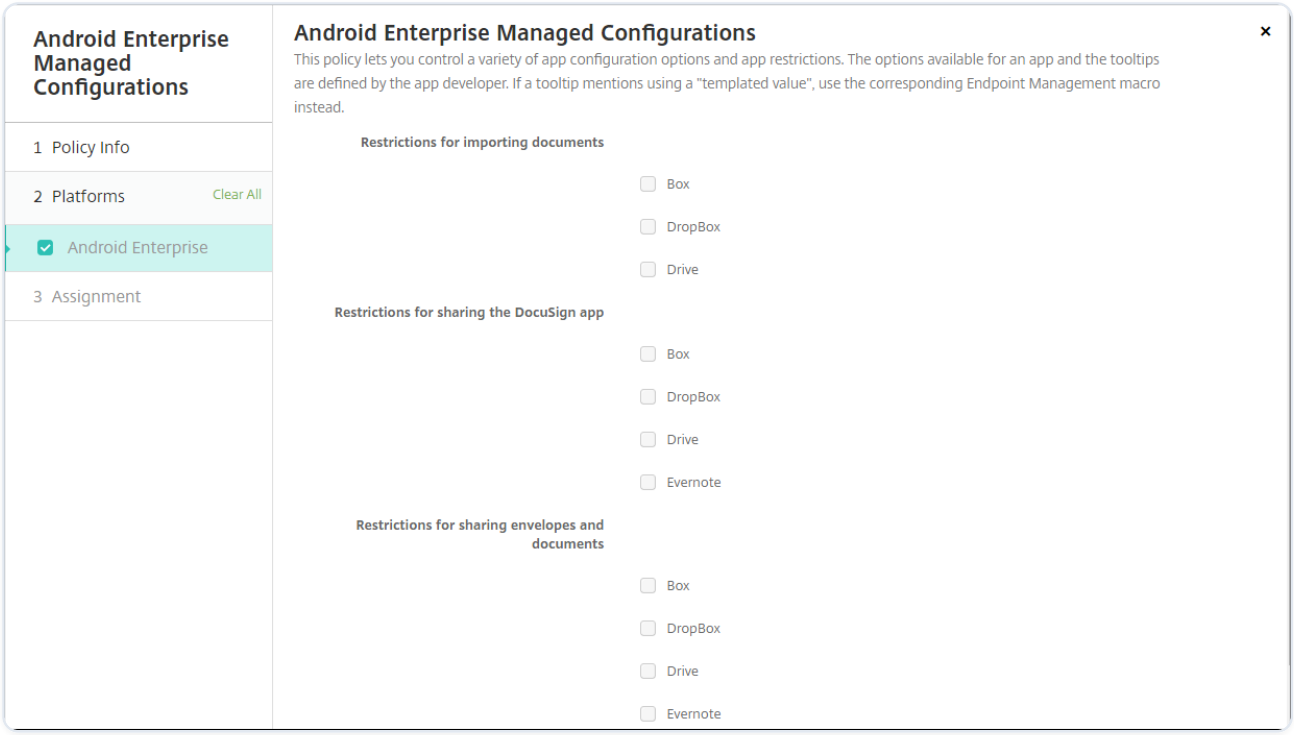
Um fluxo de trabalho geral para configurar uma VPN por aplicativo para dispositivos AE é o seguinte:

1. Configure um perfil VPN conforme descrito neste artigo.
2. Configure o Citrix ADC para aceitar tráfego da VPN por aplicativo. Para obter detalhes, consulte Configuração completa de VPN no Citrix Gateway.

Configurações do Android Enterprise

Depois de escolher adicionar uma política de dispositivo de configurações gerenciadas, um prompt para selecionar um aplicativo é exibido. Se não houver aplicativos Android Enterprise adicionados ao XenMobile®, você não poderá continuar.

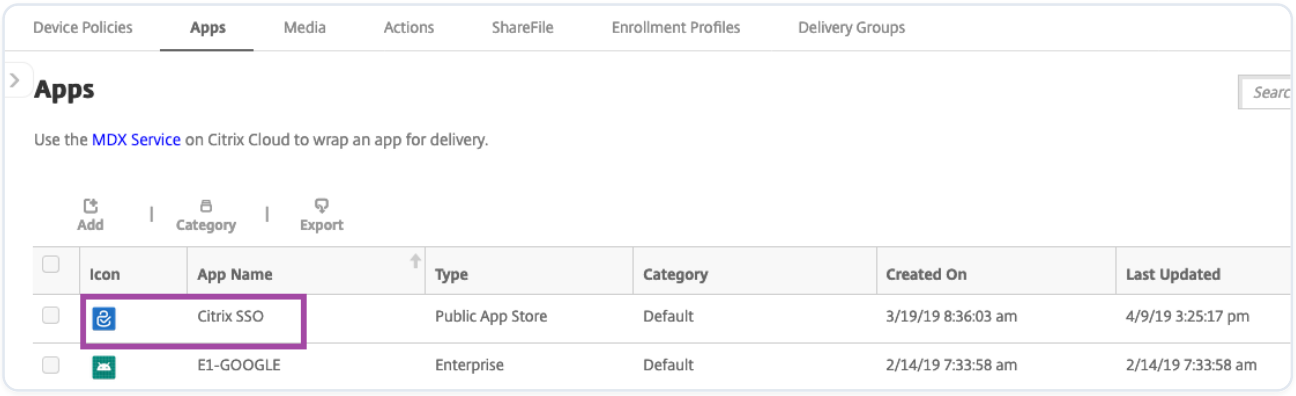
Depois de selecionar um aplicativo, configure as configurações da política. As configurações são específicas para cada aplicativo.



Configurar perfis VPN para Android Enterprise

Disponibilize perfis VPN para dispositivos Android Enterprise usando o aplicativo Citrix SSO com a política de dispositivo de configuração gerenciada.

Comece adicionando o Citrix SSO ao console do XenMobile como um aplicativo da Google Play Store. Consulte Adicionar um aplicativo da loja de aplicativos pública.



Criar uma configuração gerenciada do Android Enterprise para Citrix SSO

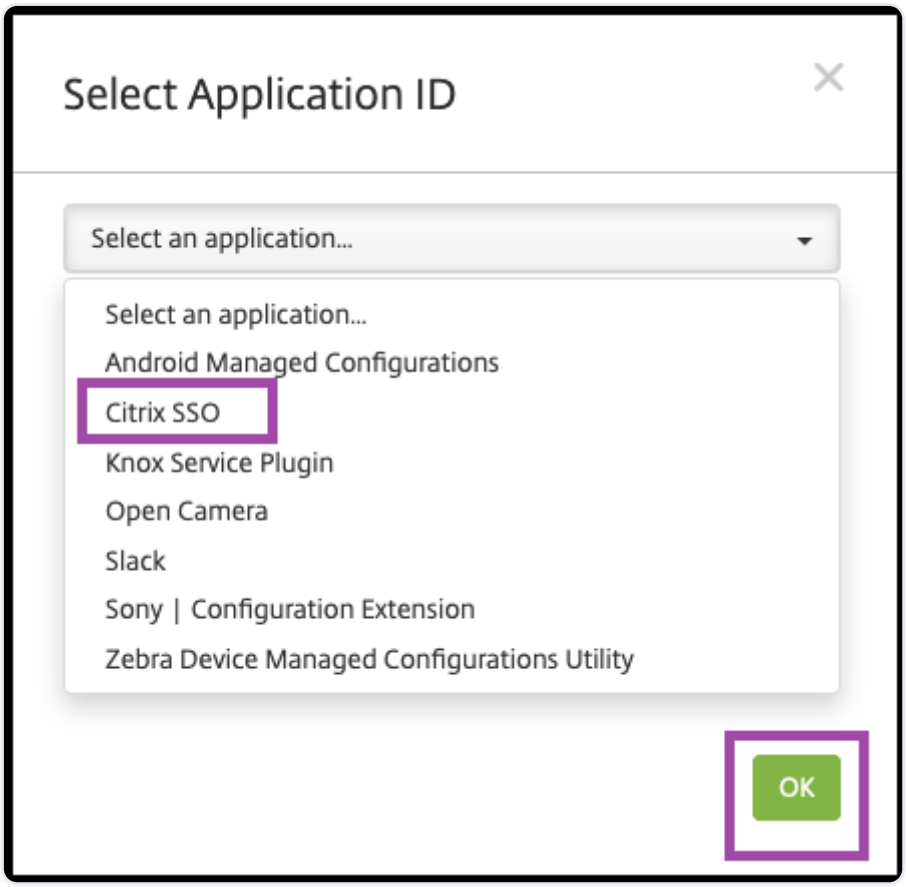
Configure a política de dispositivo de configurações gerenciadas para o Citrix SSO para criar perfis VPN. Dispositivos que têm o aplicativo Citrix SSO instalado e a política implantada têm acesso aos perfis VPN que você criar.

Você precisa do FQDN e da porta do seu Citrix Gateway.

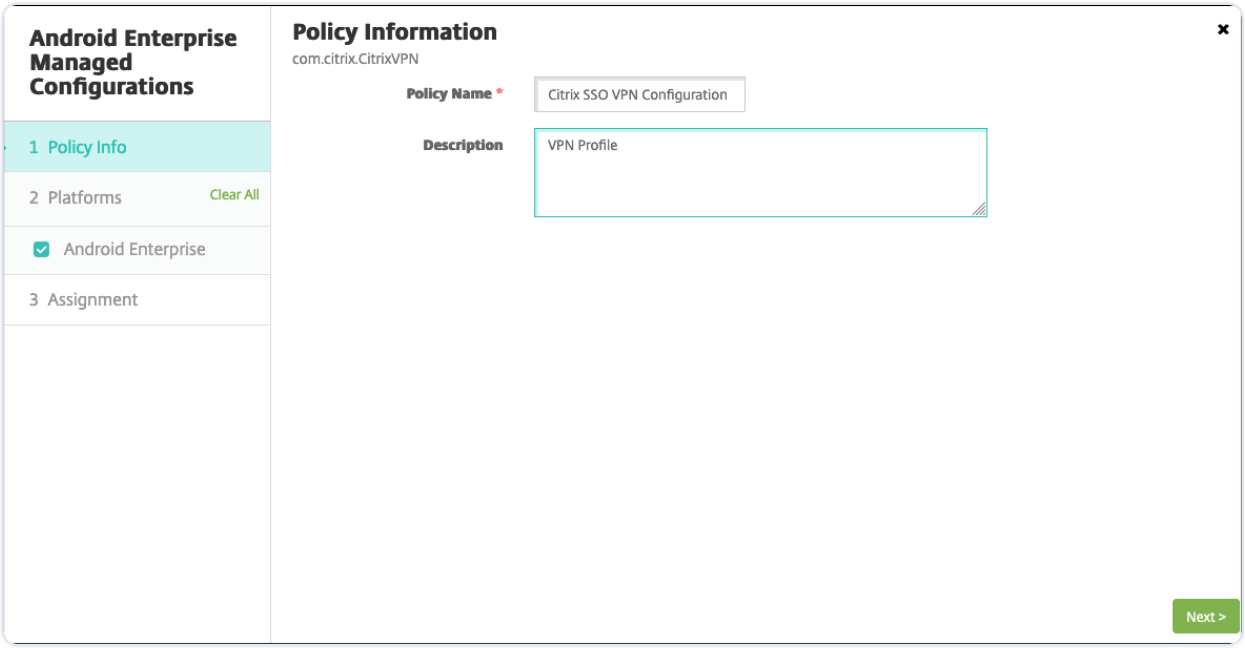
1. No console do XenMobile, clique em **Configurar > Políticas de Dispositivo**. Clique em **Adicionar**.
2. Selecione **Android Enterprise**. Clique em **Configurações Gerenciadas**.



3. Quando a janela **Selecionar ID do Aplicativo** aparecer, escolha **Citrix SSO** na lista e clique em **OK**.



4. Digite um nome e uma descrição para sua configuração de VPN do Citrix SSO. Clique em **Avançar**.



5. Configure os parâmetros do perfil VPN.

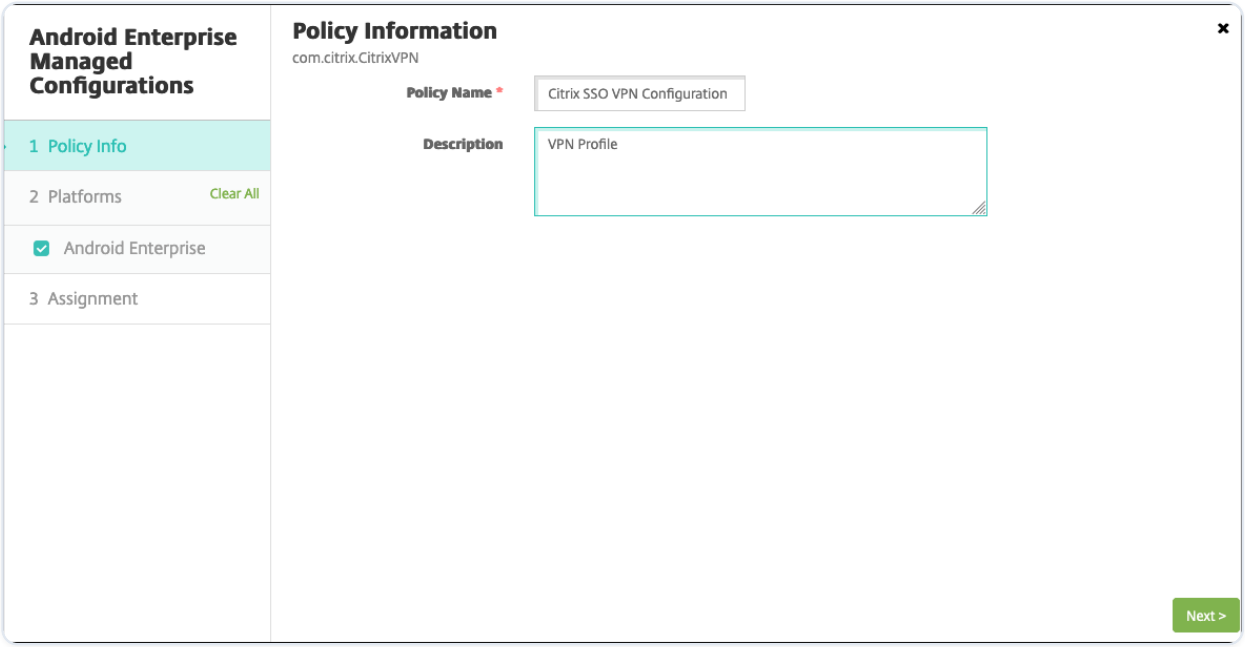
   - **Nome do Perfil VPN.** Digite um nome para o perfil VPN. Se você estiver criando mais de um perfil VPN, use um nome exclusivo para cada um. Se você não fornecer um nome, o

endereço que você inserir no campo **Endereço do Servidor** será usado como o nome do perfil VPN.

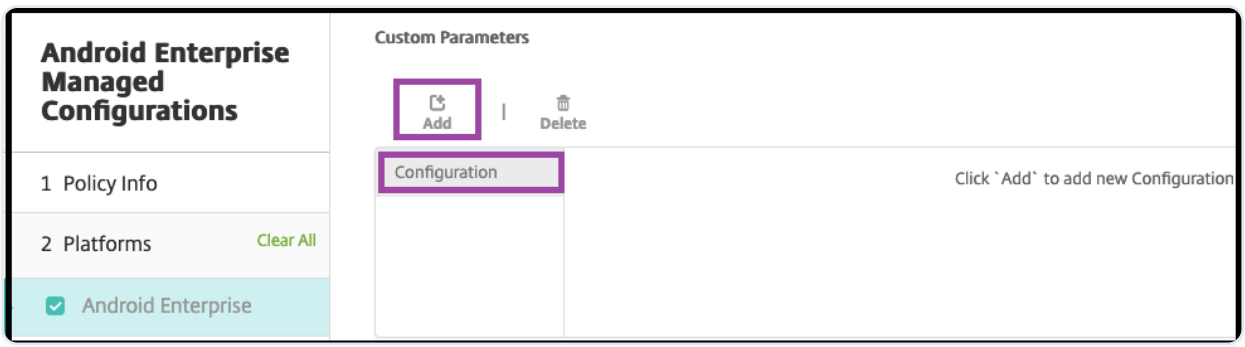
- **Endereço do Servidor(*).** Digite o FQDN do seu Citrix Gateway. Se a porta do seu Citrix Gateway não for 443, digite também a sua porta. Use o formato de URL. Por exemplo, `https://gateway.mycompany.com:8443`.
- **Nome de Usuário (opcional).** Forneça o nome de usuário que os usuários finais usam para autenticar no Citrix Gateway. Você pode usar a macro do XenMobile {user.username} para este campo. (Consulte Macros.) Se você não fornecer um nome de usuário, os usuários serão solicitados a fornecer um nome de usuário ao se conectar ao Citrix Gateway.
- **Senha (opcional).** Forneça a senha que os usuários finais usam para autenticar no Citrix Gateway. Se você não fornecer uma senha, os usuários serão solicitados a fornecer uma senha ao se conectar ao Citrix Gateway.
- **Alias do Certificado (opcional).** Digite um alias de certificado. O alias do certificado facilita o acesso do aplicativo ao certificado. Quando o mesmo alias de certificado é usado com a política de dispositivo Credenciais, o aplicativo recupera o certificado e autentica a VPN sem qualquer ação dos usuários.
- **Tipo de VPN por Aplicativo (opcional).** Se você estiver usando uma VPN por aplicativo para restringir quais aplicativos usam esta VPN, você pode configurar esta definição. Se você selecionar **Permitir**, o tráfego de rede para os nomes de pacote de aplicativos listados na **lista de aplicativos PerAppVPN** é roteado através da VPN. O tráfego de rede de todos os outros aplicativos é roteado para fora da VPN. Se você selecionar **Não permitir**, o tráfego de rede para os nomes de pacote de aplicativos listados na **lista de aplicativos PerAppVPN** é roteado para fora da VPN. O tráfego de rede de todos os outros aplicativos é roteado através da VPN. O padrão é **Permitir**.
- **Lista de aplicativos PerAppVPN.** Uma lista de aplicativos cujo tráfego é permitido ou bloqueado na VPN, dependendo do valor de **Tipo de VPN por aplicativo**. Liste os nomes dos pacotes de aplicativos separados por vírgulas ou ponto e vírgula. Os nomes dos pacotes de aplicativos diferenciam maiúsculas de minúsculas e devem aparecer nesta lista exatamente como aparecem na Google Play Store. Esta lista é opcional. Mantenha esta lista vazia para provisionar VPN em todo o dispositivo.
- **Perfil VPN padrão.** Digite o nome do perfil VPN a ser usado quando os usuários tocarem no botão de conexão na interface do usuário do aplicativo Citrix SSO em vez de tocar em um perfil específico. Se este campo for deixado em branco, o perfil principal será usado para a conexão. Se apenas um perfil for configurado, ele será marcado como o perfil

padrão. Para uma VPN sempre ativa, este campo deve ser definido com o nome do perfil VPN a ser usado para estabelecer uma VPN sempre ativa.

- **Desabilitar Perfis de Usuário.** Se esta configuração estiver ATIVADA, os usuários não poderão criar suas próprias VPNs em seus dispositivos. Se esta configuração estiver DESATIVADA, os usuários poderão criar suas próprias VPNs em seus dispositivos. O padrão é DESATIVADO.
- **Bloquear Servidores Não Confiáveis.** Esta configuração está DESATIVADA ao usar um certificado autoassinado para o Citrix Gateway ou quando o certificado raiz da CA que emite o certificado do Citrix Gateway não está na lista de CAs do sistema. Se esta configuração estiver ATIVADA, o sistema operacional Android valida o certificado do Citrix Gateway. Se a validação falhar, a conexão não será permitida. O valor padrão é ATIVADO.

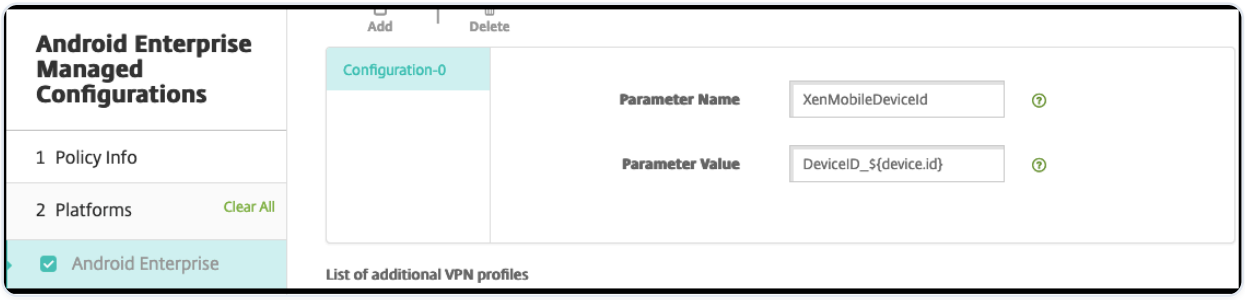


6. Opcionalmente, crie parâmetros personalizados. Os parâmetros personalizados **XenMobileDeviceId** e **UserAgent** são suportados. Selecione a configuração VPN atual e clique em **Adicionar**.



a. Crie um parâmetro personalizado:

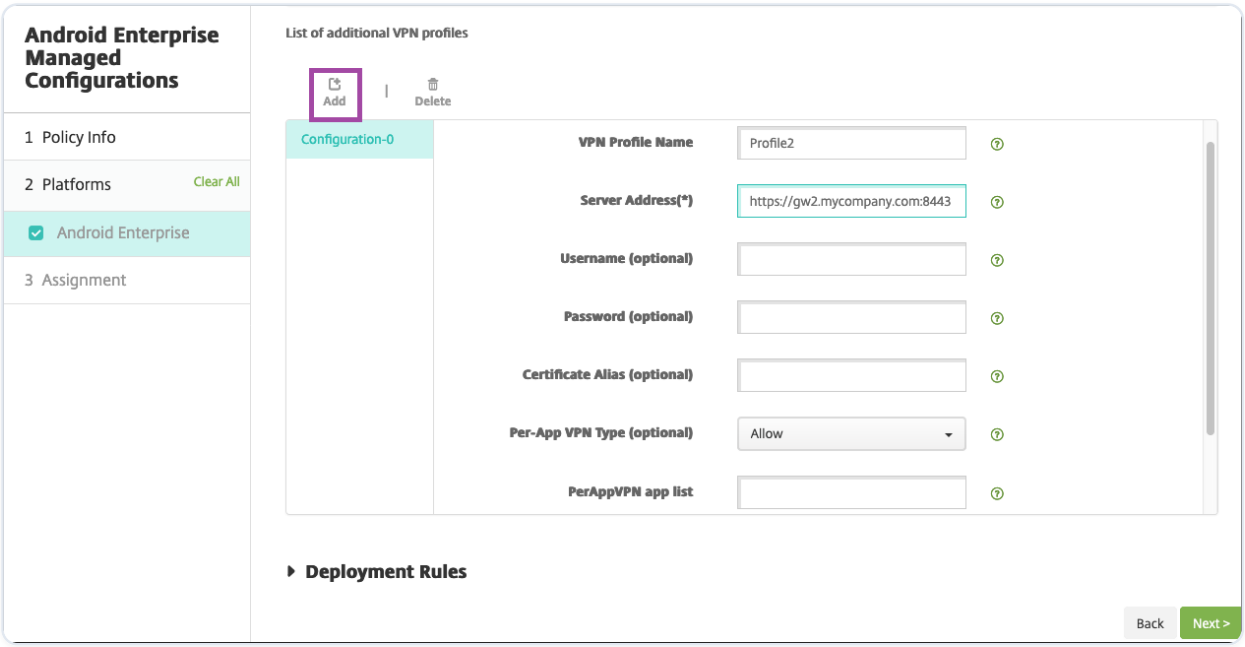
- **Nome do parâmetro.** Digite **XenMobileDeviceId**. Este campo é o ID do dispositivo a ser usado para a Verificação de Acesso à Rede com base no registro do dispositivo no XenMobile. Se o XenMobile registrar e gerenciar o dispositivo, a conexão VPN será permitida. Caso contrário, a autenticação será negada no momento do estabelecimento da VPN.
- **Valor do parâmetro** Para que o XenMobile determine o estado de registro e gerenciamento dos dispositivos, o valor de XenMobileDeviceID é definido como `DeviceID_${device.id}`.



a. Para criar outro parâmetro personalizado, clique em **Adicionar** novamente. Crie este parâmetro personalizado.

- **Nome do parâmetro.** Digite **UserAgent**. Este texto é anexado ao cabeçalho HTTP User-Agent para fazer uma verificação extra no Citrix Gateway. O valor deste texto é anexado ao cabeçalho HTTP User-Agent pelo aplicativo Citrix SSO durante a comunicação com o Citrix Gateway.
- **Valor do parâmetro.** Digite o texto que você deseja anexar ao cabeçalho HTTP User-Agent. Este texto deve estar em conformidade com as especificações do HTTP User-Agent.

7. Opcionalmente, crie mais configurações de perfil VPN. Clique em **Adicionar** abaixo da lista de configurações. Uma nova configuração aparece na lista. Selecione a nova configuração e repita a etapa 5 e, opcionalmente, a etapa 6.



8. Quando você tiver criado todos os perfis VPN desejados, clique em **Avançar**.
9. Configure as regras de implantação para esta configuração gerenciada para o Citrix SSO.
10. Clique em **Salvar**.

Esta configuração gerenciada para o Citrix SSO agora aparece na sua lista de políticas de dispositivo configuradas.

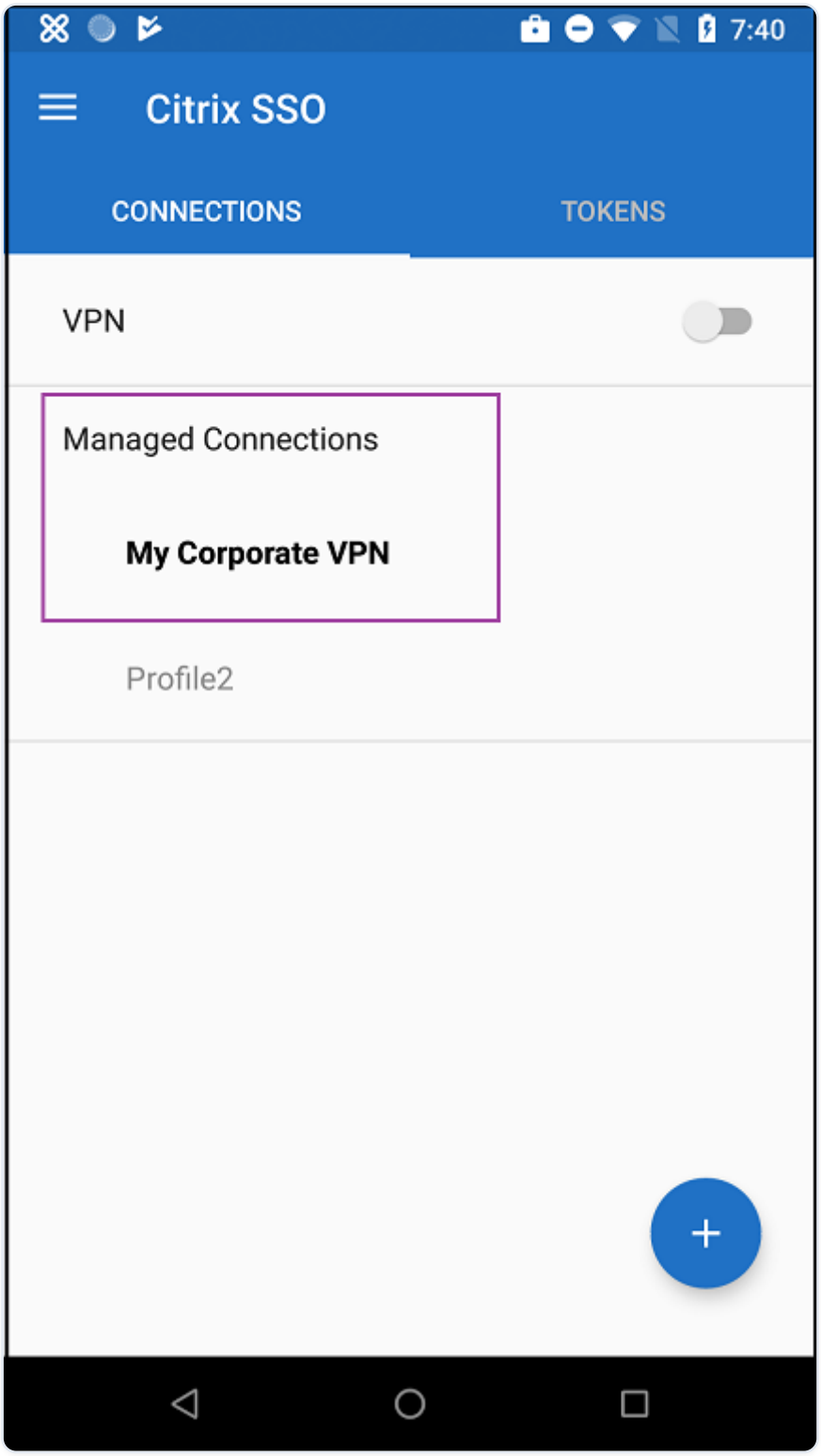
Para habilitar o always-on para os perfis VPN que você configurou, defina a política de dispositivo de opções do XenMobile.

> **Nota:** O Citrix Secure Hub 19.5.5 ou superior é necessário para VPN always-on para Android Enterprise.

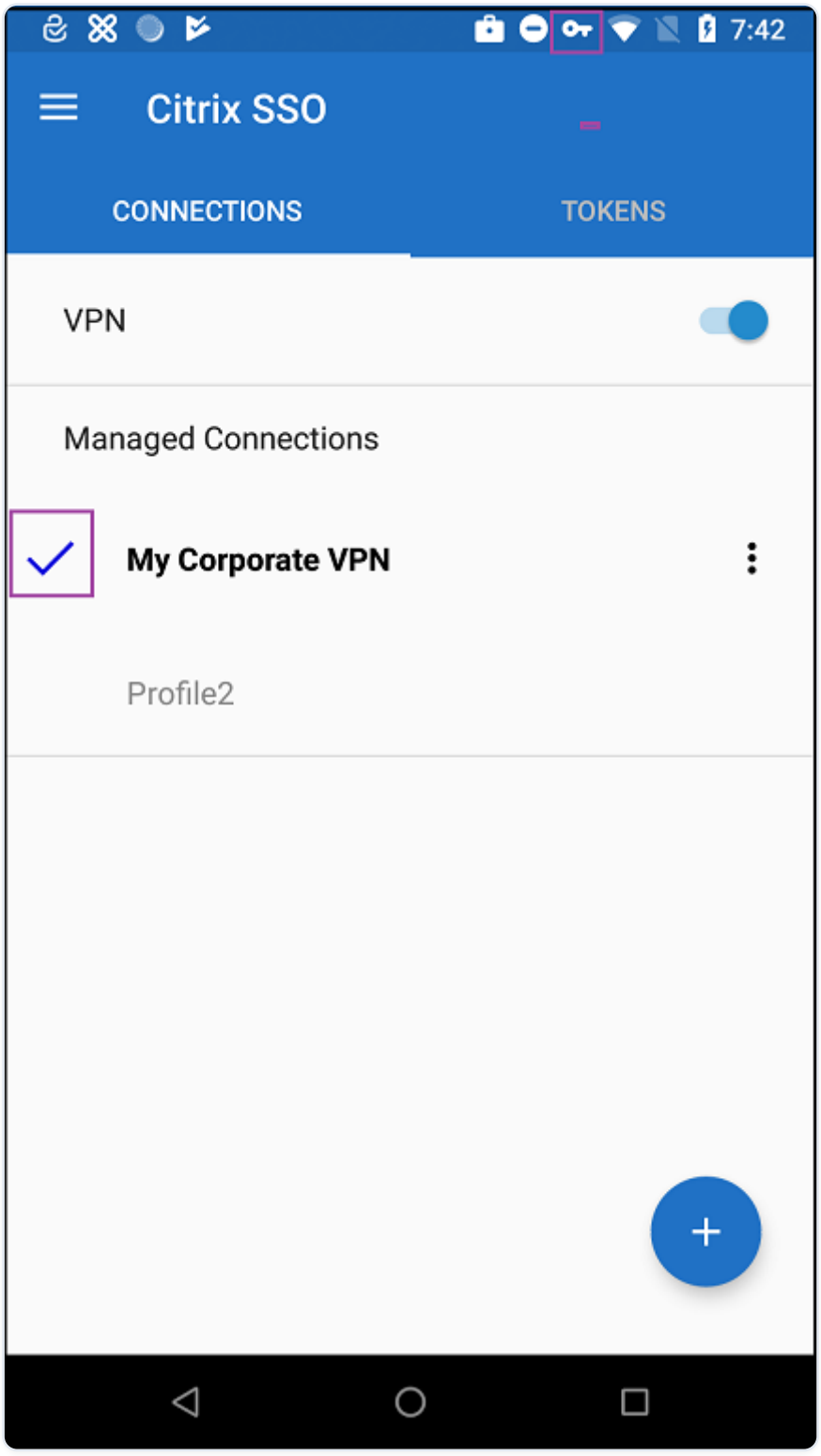
Acessando perfis VPN do dispositivo

Para acessar os perfis VPN que você criou, os usuários do Android Enterprise instalam o Citrix SSO da Google Play Store.

O perfil ou perfis VPN que você configurou aparecem na área **Conexões Gerenciadas** do aplicativo. Os usuários tocam no perfil VPN para se conectar usando esse perfil VPN.



Depois que os usuários se autenticam e se conectam, uma marca de seleção aparece ao lado do perfil VPN. O ícone de chave indica que a VPN está conectada.



Gerenciar dispositivos Android Zebra usando o Zebra OEMConfig

Gerencie dispositivos Android Zebra usando a ferramenta administrativa Zebra Technologies OEMConfig. Para obter informações sobre o aplicativo Zebra OEMConfig, consulte o site da Zebra Technologies.

O XenMobile oferece suporte à versão 9.2 e superior do Zebra OEMConfig. Para obter informações sobre os requisitos de sistema para instalar o Zebra OEMConfig em dispositivos, consulte Configuração do OEMConfig no site da Zebra Technologies.

Comece adicionando o aplicativo Zebra OEMConfig ao console do XenMobile como um aplicativo da Google Play Store. Consulte Adicionar um aplicativo da loja de aplicativos pública.

Crie uma configuração gerenciada do Android Enterprise para o aplicativo Zebra OEMConfig

Configure a política de dispositivo de configurações gerenciadas para o aplicativo Zebra OEMConfig. A política se aplica a dispositivos Zebra que têm o aplicativo Zebra OEMConfig instalado e a política implantada.

1. No console do XenMobile, clique em **Configurar > Políticas de Dispositivo**. Clique em **Adicionar**.
2. Selecione **Android Enterprise**. Clique em **Configurações Gerenciadas**.



3. Quando a janela **Selecionar ID do Aplicativo** aparecer, escolha **ZebraOEMConfig powered by MX** na lista e clique em **OK**.
4. Digite um nome e uma descrição para sua configuração do Zebra OEMConfig. Clique em **Avançar**.
5. Digite um nome para a configuração do Zebra OEMConfig.
6. Configure os parâmetros disponíveis. Por exemplo:
    - Para desativar a câmera na parte frontal do dispositivo, selecione **Configuração da Câmera** e defina **Uso da Câmera Frontal** como **Desativado**.
    - Para alterar o formato da hora dos dispositivos, selecione **Configuração do Relógio** e defina **Formato da Hora** como **12** para formato de 12 horas ou **24** para formato de 24 horas.

Para obter uma lista e descrições de todas as configurações disponíveis, consulte Configurações Gerenciadas da Zebra no site da Zebra Technologies.

1. Opcionalmente, crie mais configurações do Zebra OEMConfig. Clique em **Adicionar** abaixo da lista de configurações. Uma nova configuração aparece na lista. Selecione a nova configuração e configure os parâmetros.

2. Quando você tiver criado todas as configurações do Zebra OEMConfig que deseja, clique em **Avançar**.
3. Configure as regras de implantação para esta configuração gerenciada para o Zebra OEMConfig.
4. Clique em **Salvar**.

Política de dispositivo de domínios gerenciados

Você pode definir domínios gerenciados que se aplicam a e-mail e ao navegador Safari. Os domínios gerenciados ajudam a proteger os dados corporativos controlando quais aplicativos podem abrir documentos baixados de domínios usando o Safari.

Para dispositivos supervisionados com iOS 8 e posterior, você especifica URLs ou subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador. Para dispositivos supervisionados com iOS 9.3 e posterior, você pode especificar as URLs das quais os usuários podem salvar senhas no Safari.

Para as etapas sobre como configurar um dispositivo iOS para o modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.

Quando um usuário envia um e-mail para um destinatário cujo domínio não está na lista de domínios de e-mail gerenciados, a mensagem é sinalizada no dispositivo do usuário para avisá-lo de que está enviando uma mensagem para alguém fora do seu domínio corporativo.

Para itens como documentos, anexos ou downloads: Quando um usuário abre um item usando o Safari de um domínio da web que está na lista de domínios da web gerenciados, o aplicativo corporativo apropriado abre o item. Se o item não for de um domínio da web na lista de domínios da web gerenciados, o usuário não poderá abrir o item com um aplicativo corporativo. Ele deve usar um aplicativo pessoal e não gerenciado.

Para dispositivos supervisionados, mesmo que você não especifique domínios de preenchimento automático de senha do Safari: Se o dispositivo estiver configurado como multiusuário efêmero, os usuários não poderão salvar senhas. No entanto, se o dispositivo não estiver configurado como multiusuário efêmero, os usuários poderão salvar todas as senhas.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

Para especificar domínios:

FORMATO	DESCRIÇÃO
`example.com`	Trate qualquer caminho em `example.com` como gerenciado, mas não `site.example.com/`.
`foo.example.com`	Tratar qualquer caminho abaixo de `foo.example.com` como gerenciado, mas não `example.com/` ou `bar.example.com/`.
`*.example.com`	Tratar qualquer caminho abaixo de `foo.example.com` ou `bar.example.com` como gerenciado, mas não `example.com/`.
`example.com/sub`	Tratar `example.com/sub` e qualquer caminho abaixo dele como gerenciado, mas não `example.com/`.
`foo.example.com/sub`	Tratar qualquer caminho abaixo de `foo.example.com/sub` como gerenciado, mas não `example.com`, `example.com/sub`, `foo.example.com/` ou `bar.example.com/sub`.
`*.example.com/sub`	Tratar qualquer caminho abaixo de `foo.example.com/sub` ou `bar.example.com/sub` como gerenciado, mas não `example.com` ou `foo.example.com/`.

Regras:

- O "www." inicial e as barras finais em URLs são ignorados quando os domínios são comparados.
- Se uma entrada tiver um número de porta, apenas os endereços que especificam esse número de porta são considerados gerenciados. Caso contrário, apenas as portas padrão são consideradas gerenciadas (porta 80 para http e porta 443 para https). Por exemplo, o padrão `*.example.com:8080` corresponde a `https://site.example.com:8080/page.html`, mas

não a `https://site.example.com/page.html`, mas o padrão `*.example.com` corresponde a `https://site.example.com/page.html` e `https://site.example.com/page.html`, mas não a `https://site.example.com:8080/page.html`.

- As definições de domínio da web do Safari gerenciado são cumulativas. Os padrões definidos por todos os payloads de domínio da web do Safari gerenciado são usados para corresponder a uma solicitação de URL.

Configurações:

- **Domínios Gerenciados**
  - **Domínios de e-mail não marcados:** Para cada domínio de e-mail que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
    - **Domínio de e-mail gerenciado:** Digite o domínio de e-mail.
    - Clique em **Salvar** para salvar o domínio de e-mail ou clique em **Cancelar** para não salvar o domínio de e-mail.
  - **Domínios da Web do Safari gerenciados:** Para cada domínio da web que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
    - **Domínio da Web gerenciado:** Digite o domínio da web.
    - Clique em **Salvar** para salvar o domínio da web ou clique em **Cancelar** para não salvar o domínio da web.
  - **Domínios de preenchimento automático de senha do Safari:** Para cada domínio de preenchimento automático que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
    - **Domínio de preenchimento automático de senha do Safari:** Digite o domínio de preenchimento automático.
    - Clique em **Salvar** para salvar o domínio de preenchimento automático ou clique em **Cancelar** para não salvar o domínio de preenchimento automático.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.

- **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de máximo de usuários residentes

A política de dispositivo de máximo de usuários residentes é para dispositivos compartilhados que executam iOS (iPadOS). Para obter mais informações sobre iPads Compartilhados, consulte Integrar com recursos do Apple Education.

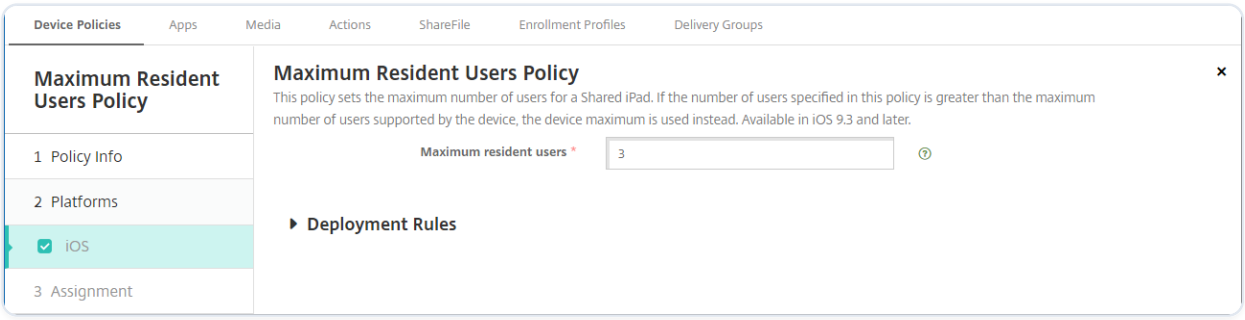
Esta política deve ser implantada quando o iPad estiver na fase de "aguardando configuração" durante o Assistente de Configuração. A Apple não permite que esta política seja implantada depois que os iPads Compartilhados são registrados.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Máximo de Usuários Residentes:** O número máximo de usuários para um iPad Compartilhado. Se o número de usuários especificado nesta política for maior que o número máximo de usuários suportados pelo dispositivo: o Citrix Endpoint Management usa o máximo do dispositivo. O padrão é **5** usuários.

  A Apple recomenda que você mantenha o valor de Máximo de usuários residentes o mais baixo possível. Um valor baixo maximiza a quantidade de armazenamento do iPad para cada usuário. Além disso, um valor baixo minimiza a comunicação com o iCloud e proporciona uma experiência de login mais rápida. Para obter informações sobre como a Apple lida com o armazenamento compartilhado em um iPad, consulte `<https://developer.apple.com/education/shared-ipad/>`.



Política de dispositivo de opções MDM

Você pode criar uma política de dispositivo no XenMobile para gerenciar o Bloqueio de Ativação do Buscar Meu iPhone/iPad em dispositivos iOS 7.0 e posteriores supervisionados. Para obter as etapas sobre como definir um dispositivo iOS para o modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.

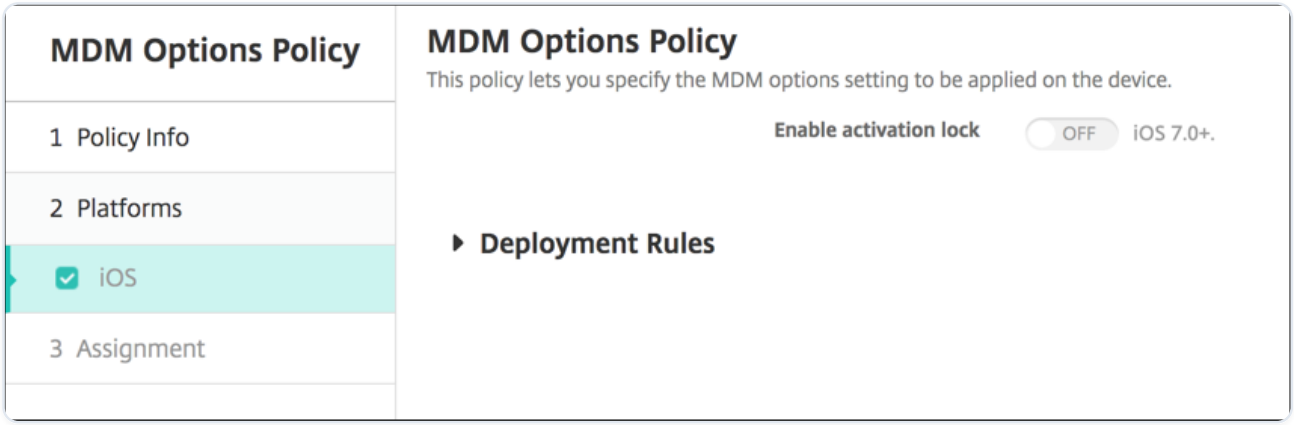
O Bloqueio de Ativação é um recurso do Buscar Meu iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação exige o ID Apple e a senha do usuário antes que alguém possa desativar o Buscar Meu iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos que sua organização possui, ignorar um Bloqueio de Ativação é necessário para, por exemplo, redefinir ou realocar dispositivos.

Para habilitar o Bloqueio de Ativação, você configura e implanta a política de dispositivo XenMobile® MDM Options. Você pode então gerenciar um dispositivo a partir do console XenMobile sem as credenciais Apple do usuário. Para ignorar o requisito de credencial Apple de um Bloqueio de Ativação, emita a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Por exemplo, se o usuário devolver um telefone perdido ou para configurar o dispositivo antes ou depois de uma Limpeza Completa: Quando o telefone solicitar a credencial da conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **Habilitar Bloqueio de Ativação:** Selecione se deseja habilitar o Bloqueio de Ativação nos dispositivos aos quais você implanta esta política. O padrão é **Desativado**.

Depois de habilitar o Bloqueio de Ativação implantando a política de dispositivo de opções MDM: A ação de segurança **Ignorar Bloqueio de Ativação** aparece quando você seleciona esses dispositivos na página **Gerenciar > Dispositivos** e clica em **Segurança**. Um Ignorar Bloqueio de Ativação permite remover o Bloqueio de Ativação de dispositivos supervisionados antes da ativação do dispositivo sem saber o ID Apple e a senha dos usuários do dispositivo. Você pode enviar um Ignorar Bloqueio de Ativação para um dispositivo antes ou depois de uma Limpeza Completa. Para obter mais informações, consulte Ignorar um bloqueio de ativação do iOS no artigo de ações de segurança.

Política de dispositivo de informações da organização

Você pode adicionar uma política de dispositivo no XenMobile® para especificar as informações da sua organização para mensagens de alerta que são enviadas do XenMobile para dispositivos iOS. A política está disponível para dispositivos iOS 7 e posteriores.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

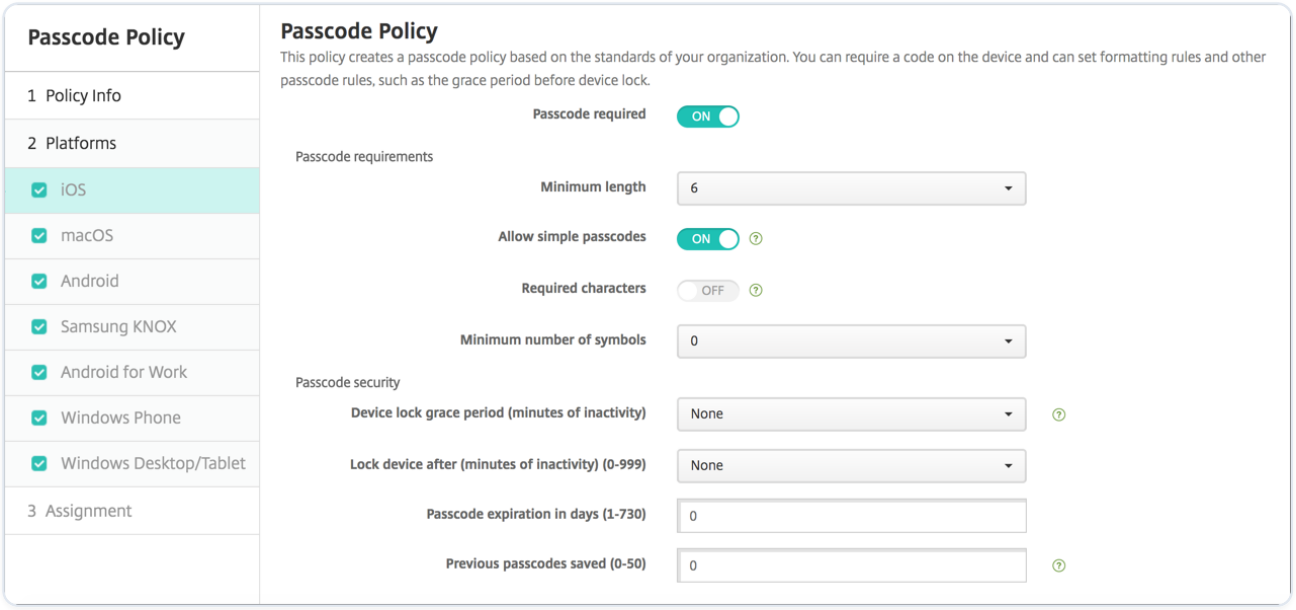
- **Nome:** Digite o nome da organização que executa o XenMobile.
- **Endereço:** Digite o endereço da organização.
- **Telefone:** Digite o número de telefone de suporte da organização.
- **E-mail:** Digite o endereço de e-mail de suporte.
- **Mágica:** Digite uma palavra ou frase que descreva os serviços gerenciados pela organização.

Política de senha de dispositivo

Você cria uma política de senha no XenMobile com base nos padrões da sua organização. Você pode exigir senhas nos dispositivos dos usuários e pode definir várias regras de formatação e senha. Você pode criar políticas para iOS, macOS, Android, Samsung Knox, Android Enterprise e Windows desktop/tablet. Cada plataforma requer um conjunto diferente de valores, que são descritos neste artigo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

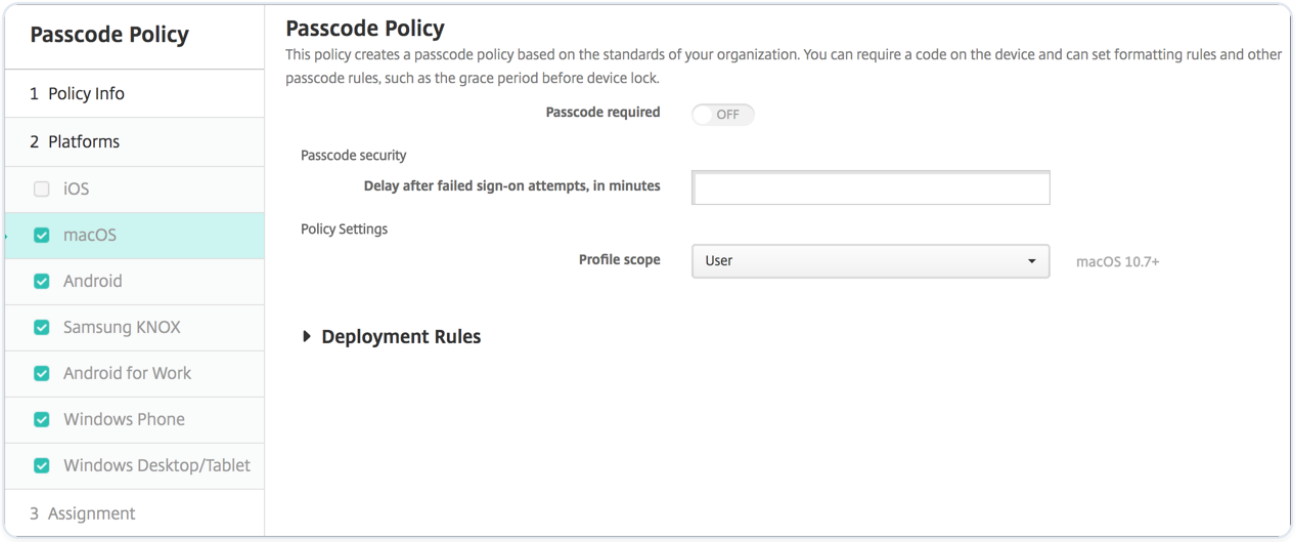
Configurações do iOS



- **Senha necessária:** Selecione esta opção para exigir uma senha e para exibir as opções de configuração para uma política de senha de dispositivo iOS. A página se expande para permitir que você configure as configurações de requisitos de senha, segurança de senha e configurações de política.
- **Requisitos de senha**
  - **Comprimento mínimo:** Clique no comprimento mínimo da senha na lista suspensa. O padrão é **6**.
  - **Permitir senhas simples:** Selecione se deseja permitir senhas simples. Senhas simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **Ativado**.
  - **Caracteres obrigatórios:** Selecione se deseja exigir que as senhas tenham pelo menos uma letra. O padrão é **Desativado**.
  - **Número mínimo de símbolos:** Na lista, clique no número de símbolos que a senha deve ter. O padrão é **0**.
- **Segurança da senha**
  - **Período de carência de bloqueio do dispositivo (minutos de inatividade):** Na lista, clique na duração do tempo antes que os usuários precisem inserir uma senha para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
  - **Bloquear dispositivo após (minutos de inatividade):** Na lista, clique na duração do tempo que um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é Nenhum.

- **Expiração da senha em dias (1-730):** Digite o número de dias após os quais a senha expira. Os valores válidos são 1–730. O padrão é **0**, o que significa que a senha nunca expira.
- **Senhas anteriores salvas (0-50):** Digite o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 0–50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
- **Número máximo de tentativas de logon falhas:** Na lista, clique no número de vezes que um usuário pode falhar ao fazer logon com êxito, após o qual o dispositivo é totalmente apagado. O padrão é **Não definido**.

Configurações do macOS



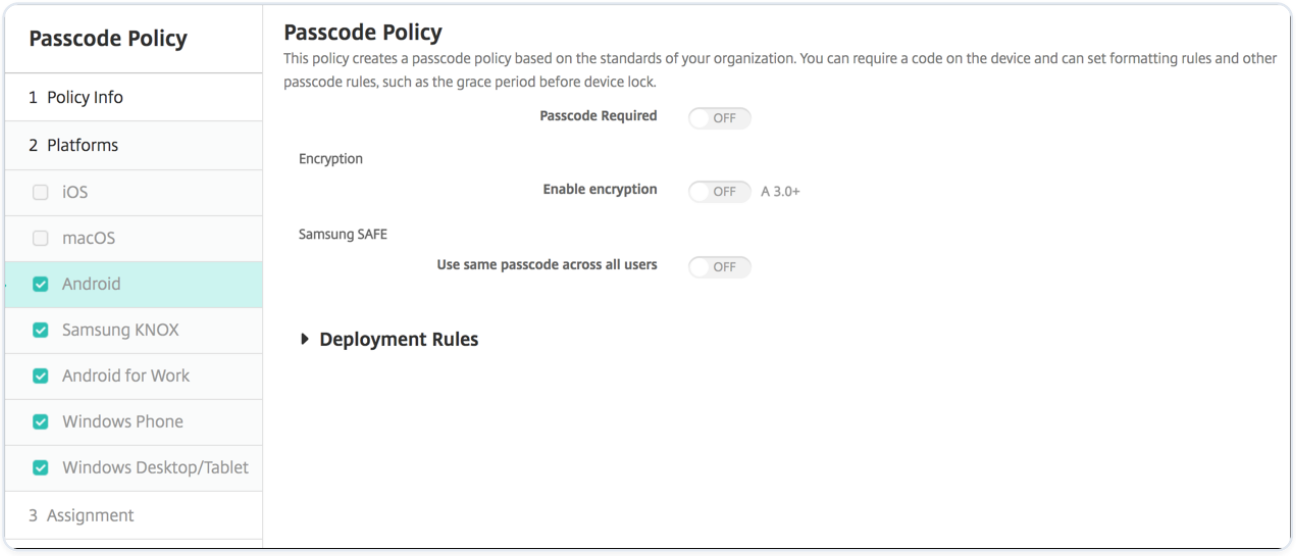
- **Código de acesso obrigatório:** Selecione esta opção para exigir um código de acesso e para exibir as opções de configuração para uma política de dispositivo de código de acesso do iOS. A página se expande para permitir que você configure as configurações de requisitos de código de acesso, segurança de código de acesso e configurações de política.
- Se você não habilitar **Código de acesso obrigatório**, ao lado de **Atraso após tentativas de logon falhas, em minutos**, digite o número de minutos de atraso antes de permitir que os usuários insiram novamente seus códigos de acesso.
- Se você habilitar **Código de acesso obrigatório**, configure as seguintes configurações:
- **Requisitos de código de acesso**
  - **Comprimento mínimo:** Na lista, clique no comprimento mínimo do código de acesso. O padrão é **6**.

- **Permitir códigos de acesso simples:** Selecione se deseja permitir códigos de acesso simples. Códigos de acesso simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **Ativado**.
- **Caracteres obrigatórios:** Selecione se deseja exigir que os códigos de acesso tenham pelo menos uma letra. O padrão é **Desativado**.
- **Número mínimo de símbolos:** Na lista, clique no número de símbolos que o código de acesso deve ter. O padrão é **0**.

- **Segurança do código de acesso**
  - **Período de carência de bloqueio do dispositivo (minutos de inatividade):** Na lista, clique na duração do tempo antes que os usuários precisem inserir um código de acesso para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
  - **Bloquear dispositivo após (minutos de inatividade):** Na lista, clique na duração do tempo que um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
  - **Expiração da senha em dias (1-730):** Digite o número de dias após os quais a senha expira. Os valores válidos são 1–730. O padrão é **0**, o que significa que a senha nunca expira.
  - **Senhas anteriores salvas (0-50):** Digite o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 0–50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Número máximo de tentativas de logon com falha:** Na lista, clique no número de vezes que um usuário pode falhar ao fazer logon com sucesso, após o qual o dispositivo é bloqueado. O padrão é **Não definido**.
  - **Atraso após tentativas de logon com falha, em minutos:** Digite o número de minutos de atraso antes de permitir que um usuário insira novamente uma senha.
  - **Forçar redefinição de senha:** Na próxima vez que um usuário se autenticar, ele deverá redefinir sua senha.

- **Configurações de política**
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Configurações do Android



Observação:

A configuração padrão para Android é **Desativado**.

- **Senha necessária:** Selecione esta opção para exigir uma senha e exibir as opções de configuração para uma política de dispositivo de senha do Android. A página se expande para permitir que você configure as configurações de requisitos de senha, segurança de senha, criptografia e Samsung SAFE.
- **Requisitos de senha**
  - **Comprimento mínimo:** Selecione o comprimento mínimo da senha na lista suspensa. O padrão é 6.
  - **Reconhecimento biométrico:** Selecione se deseja habilitar o reconhecimento biométrico. Se você habilitar esta opção, o campo Caracteres necessários ficará oculto. O padrão é **Desativado**.
  - **Caracteres obrigatórios:** Selecione **Nenhuma Restrição**, **Números e letras**, **Somente números** ou **Somente letras** na lista suspensa para configurar como as senhas são compostas. O padrão é Nenhuma restrição.
  - **Regras avançadas:** Selecione se deseja aplicar regras avançadas de senha. Esta opção está disponível para Android 3.0 e posterior. O padrão é **Desativado**.
  - Ao habilitar **Regras avançadas,** em cada uma das listas a seguir, clique no número mínimo de cada tipo de caractere que uma senha deve ter:

- **Símbolos:** O número mínimo de símbolos.
- **Letras:** O número mínimo de letras.
- **Letras minúsculas:** O número mínimo de letras minúsculas.
- **Letras maiúsculas:** O número mínimo de letras maiúsculas.
- **Números ou símbolos:** O número mínimo de números ou símbolos.
- **Números:** O número mínimo de números.

- **Segurança da senha**
  - **Bloquear dispositivo após (minutos de inatividade):** Na lista, clique na duração de tempo que um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**
  - **Expiração da senha em dias (1-730):** Digite o número de dias após os quais a senha expira. Os valores válidos são 1–730. O padrão é **0**, o que significa que a senha nunca expira.
  - **Senhas anteriores salvas (0-50):** Digite o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 0–50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de tentativas de logon falhas:** Na lista, clique no número de vezes que um usuário pode falhar ao fazer login com sucesso, após o qual o dispositivo é apagado. O padrão é **Não definido**.
- **Criptografia**
  - **Habilitar criptografia:** Selecione se deseja habilitar a criptografia. Esta opção está disponível para Android 3.0 e posterior. A opção está disponível independentemente da configuração **Senha necessária**.

    Para criptografar seus dispositivos, os usuários devem começar com a bateria carregada e manter o dispositivo conectado durante a hora ou mais que a criptografia leva. Se eles interromperem o processo de criptografia, poderão perder alguns ou todos os dados em seus dispositivos. Depois que um dispositivo é criptografado, o processo não pode ser revertido, exceto realizando uma redefinição de fábrica, que apaga todos os dados do dispositivo.
- **Samsung SAFE**

> **Nota:**

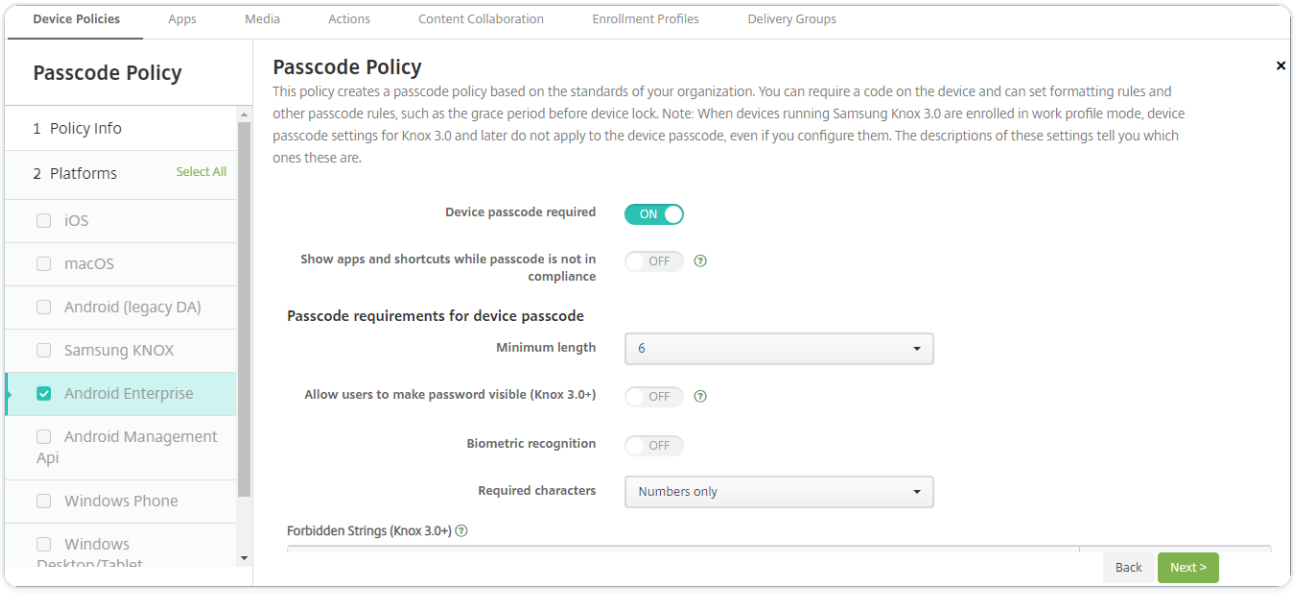
> Como solução alternativa para desabilitar o reconhecimento facial ou de íris em dispositivos Samsung SAFE: Crie uma política de dispositivo de Restrições para Samsung SAFE. Na política de Restrições, ative **Desabilitar Aplicativos** e adicione `com.samsung.android.bio.face.service` ou `com.samsung.android.server.iris` à tabela. Em seguida, implante a política de Restrições.

- **Usar a mesma senha para todos os usuários:** Selecione se deseja usar a mesma senha para todos os usuários. O padrão é **Desativado**. Esta configuração se aplica apenas a dispositivos Samsung SAFE e está disponível independentemente da configuração **Senha necessária**.
- Ao habilitar **Usar a mesma senha para todos os usuários**, digite a senha a ser usada por todos os usuários no campo **Senha**.
- Ao habilitar **Senha necessária**, configure as seguintes configurações do Samsung SAFE:
  - **Caracteres alterados:** Digite o número de caracteres que os usuários devem alterar em relação à senha anterior. O padrão é **0**.
  - **Número de vezes que um caractere pode ocorrer:** Digite o número máximo de vezes que um caractere pode ocorrer em uma senha. O padrão é **0**.
  - **Comprimento da sequência alfabética:** Digite o comprimento máximo de uma sequência alfabética em uma senha. O padrão é **0**.
  - **Comprimento da sequência numérica:** Digite o comprimento máximo de uma sequência numérica em uma senha. O padrão é **0**.
  - **Permitir que os usuários tornem a senha visível:** Selecione se os usuários podem tornar suas senhas visíveis. O padrão é **Ativado**.
  - **Configurar autenticação biométrica**. Selecione se deseja habilitar a autenticação biométrica. O padrão é **Desativado**. Se você definir como **Ativado**, poderá configurar estas opções:
    - **Permitir impressão digital**. Selecione para permitir que os usuários se autenticar usando uma impressão digital.
    - **Permitir íris**. Selecione para permitir que os usuários se autenticarm usando uma íris.
  - **Cadeias de caracteres proibidas:** Você cria cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras e fáceis de adivinhar,

como "password", "pwd", "welcome", "123456", "111111". Para cada cadeia de caracteres que você deseja negar, clique em **Adicionar** e, em seguida, faça o seguinte:

- **Cadeias de caracteres proibidas:** Digite a cadeia de caracteres que os usuários talvez não usem.
- Clique em **Salvar** para adicionar a cadeia de caracteres ou clique em **Cancelar** para cancelar a adição da cadeia de caracteres.

Configurações do Android Enterprise



Para dispositivos Android Enterprise, você pode exigir uma senha para o dispositivo ou um desafio de segurança para o perfil de trabalho do Android Enterprise, ou ambos.

Para dispositivos que executam Android 9.0 ou posterior e Samsung Knox 3.0 ou posterior, configure as definições para Samsung Knox na página **Android Enterprise**. Para dispositivos que executam versões anteriores do Android ou Samsung Knox, use a página **Samsung Knox**.

> **Observação:**
>
> Quando dispositivos que executam Samsung Knox 3.0 são registrados como dispositivos de perfil de trabalho, as configurações de senha do dispositivo para Knox 3.0 e posterior não se aplicam à senha do dispositivo, mesmo que você as configure.

- **Senha do Dispositivo Necessária:** Exige uma senha no dispositivo. Quando esta configuração está **Ativada**, configure as definições em **Requisitos de senha para a senha do dispositivo** e **Segurança de senha para a senha do dispositivo**. O padrão é **Desativado**.

- **Mostrar aplicativos e atalhos enquanto a senha não está em conformidade:** Quando esta configuração está **Ativada**, aplicativos e atalhos no dispositivo não são ocultados, mesmo quando a senha não está em conformidade. Quando esta configuração está **Desativada**, aplicativos e atalhos são ocultados quando a senha não está em conformidade. Se você ativar esta configuração, a Citrix® recomenda que você crie uma ação automatizada para marcar o dispositivo como fora de conformidade quando a senha não estiver em conformidade. O padrão é **Desativado**.
- **Requisitos de senha para a senha do dispositivo:**
  - **Comprimento mínimo:** Especifica o comprimento mínimo da senha. O padrão é 6.
  - **Permitir que os usuários tornem a senha visível:** Para dispositivos que executam Samsung Knox 3.0 e posterior que têm uma chave de licença Knox válida configurada. Apenas para dispositivos totalmente gerenciados. Esta configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Permite que os usuários tornem a senha visível. O padrão é **Desativado**.
  - **Reconhecimento biométrico:** Habilita o reconhecimento biométrico. Se esta configuração estiver **Ativada**, o campo **Caracteres obrigatórios** fica oculto. O padrão é **Desativado**.
  - **Caracteres obrigatórios:** Especifica os tipos de caracteres exigidos para senhas. Na lista, escolha **Sem restrição**, **Números e letras**, **Somente números** ou **Somente letras**. Use **Sem restrições** apenas para dispositivos com Android 7.0. O Android 7.1 e posterior não respeitam a configuração **Sem restrições**. O padrão é **Números e letras**.
  - **Cadeias de caracteres proibidas:** Para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Esta configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica cadeias de caracteres que os usuários não podem usar como senhas. Você cria cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras e fáceis de adivinhar, como "password", "pwd", "welcome", "123456", "111111". Para cada cadeia de caracteres que você deseja negar: clique em **Adicionar**. Digite a cadeia de caracteres que você não deseja que os usuários usem; clique em **Salvar** para adicionar a cadeia de caracteres ou clique em **Cancelar** para cancelar a adição da cadeia de caracteres.
  - **Regras avançadas:** Aplica regras avançadas para os tipos de caracteres que podem ocorrer em senhas. Quando esta configuração estiver **Ativada**, configure as configurações em **Número mínimo de** e **Número máximo de**. Esta configuração não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **Desativado**.
  - **Número mínimo de:**

    - **Símbolos:** Especifica o número mínimo de símbolos. O padrão é **0**.
    - **Letras:** Especifica o número mínimo de letras. O padrão é **0**.
    - **Letras minúsculas:** Especifica o número mínimo de letras minúsculas. O padrão é **0**.
    - **Letras maiúsculas:** Especifica o número mínimo de letras maiúsculas. O padrão é **0**.
    - **Números ou símbolos:** Especifica o número mínimo de números ou símbolos. O padrão é **0**.
    - **Números:** Especifica o número mínimo de números. O padrão é **0**.
    - **Caracteres alterados:** Para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Esta configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica o número de caracteres que os usuários devem alterar em relação à sua senha anterior. O padrão é **0**.

  - **Número máximo de:** Para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Esta configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho.

    - **Número de vezes que um caractere pode ocorrer:** Especifica o número máximo de vezes que um caractere pode ocorrer em uma senha. O padrão é **0**, o que significa que não há limite máximo.
    - **Comprimento da sequência alfabética:** Especifica o comprimento máximo de uma sequência alfabética em uma senha. O padrão é **0**, o que significa que não há limite máximo.
    - **Comprimento da sequência numérica:** Especifica o comprimento máximo de uma sequência numérica em uma senha. O padrão é **0**, o que significa que não há limite máximo.

- **Segurança da senha para a senha do dispositivo:**

  - **Limpar o dispositivo após (tentativas de logon com falha):** Especifica o número de vezes que um usuário pode falhar ao fazer logon, após o qual o dispositivo é totalmente limpo. O padrão é **Não definido**.
  - **Bloquear dispositivo após (minutos de inatividade) (0-999):** Especifica o número de minutos que um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.

- **Expiração da senha em dias (1-730):** Especifica o número de dias após os quais a senha expira. Os valores válidos são 1–730. O padrão é **0**, o que significa que a senha nunca expira.
- **Senhas anteriores salvas (0-50):** Especifica o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 0–50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
- **Bloquear o dispositivo após (tentativas de logon com falha)** Para dispositivos que executam Samsung Knox 3.0 e posterior que têm uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica o número de vezes que um usuário pode falhar ao fazer logon, após o qual o dispositivo é bloqueado. O padrão é **Não definido**.

- **Desafio de segurança do perfil de trabalho:** Exige que os usuários concluam um desafio de segurança para acessar aplicativos em execução em um perfil de trabalho do Android Enterprise. Para dispositivos que executam Android 7.0 e posterior. Quando esta configuração está **Ativada**, configure as configurações em **Requisitos de senha para desafio de segurança do perfil de trabalho** e **Segurança da senha para desafio de segurança do perfil de trabalho**. O padrão é **Desativado**.
- **Requisitos de senha para desafio de segurança do perfil de trabalho:**
  - **Comprimento mínimo:** Especifica o comprimento mínimo da senha. O padrão é 6.
  - **Permitir que os usuários tornem a senha visível:** Para dispositivos que executam Knox 3.0 e posterior que têm uma chave de licença Knox válida configurada. Permite que os usuários tornem a senha visível. O padrão é **Desativado**.
  - **Reconhecimento biométrico:** Habilita o reconhecimento biométrico. Se esta configuração estiver **Ativada**, o campo **Caracteres obrigatórios** fica oculto. O padrão é **Desativado**.
  - **Caracteres obrigatórios:** Especifica os tipos de caracteres necessários para senhas. Na lista, escolha **Sem restrição**, **Números e letras**, **Somente números** ou **Somente letras**. Use **Sem restrições** apenas para dispositivos que executam Android 7.0. Android 7.1 e posterior não respeitam a configuração **Sem restrições**. O padrão é **Números e letras**.
  - **Cadeias de caracteres proibidas:** Para dispositivos que executam Knox 3.0 e posterior que têm uma chave de licença Knox válida configurada. Especifica cadeias de caracteres que os usuários não podem usar como senhas. Você cria cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras e fáceis de adivinhar, como "password", "pwd", "welcome", "123456", "111111". Para cada cadeia de caracteres

que você deseja negar: clique em **Adicionar**. Digite a cadeia de caracteres que você não deseja que os usuários usem; clique em **Salvar** para adicionar a cadeia de caracteres ou clique em **Cancelar** para cancelar a adição da cadeia de caracteres.

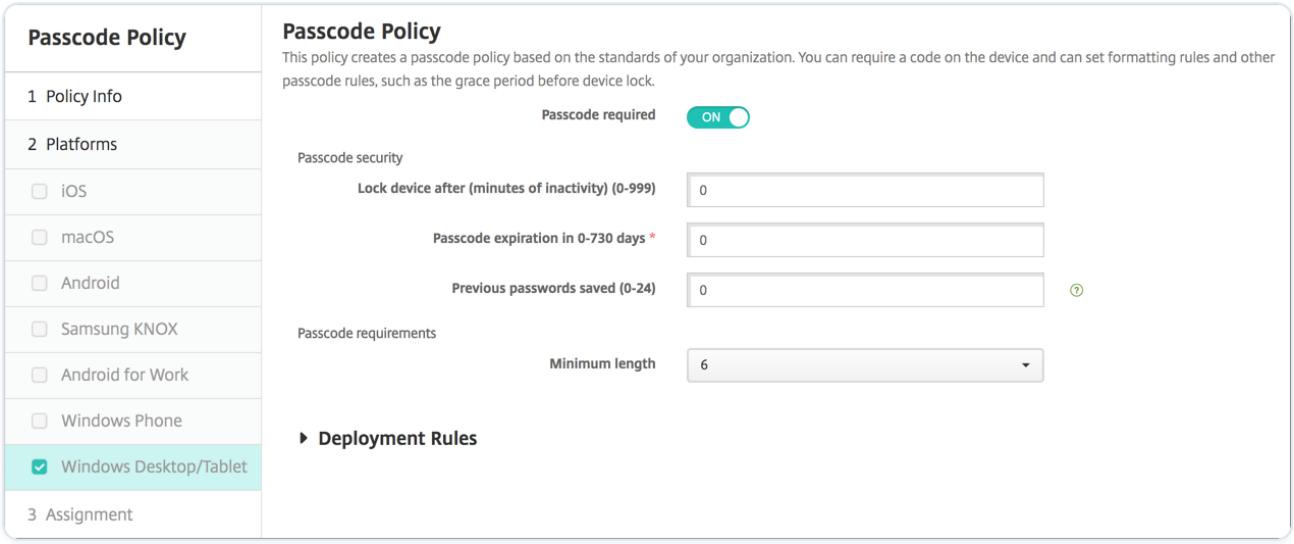
- **Regras avançadas:** Aplica regras avançadas para os tipos de caracteres que podem ocorrer em senhas. Quando esta configuração está **Ativada**, configure as configurações em **Número mínimo de** e **Número máximo de**. Esta configuração não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **Desativado**.
- **Número mínimo de:**
  - **Símbolos:** Especifica o número mínimo de símbolos. O padrão é **0**.
  - **Letras:** Especifica o número mínimo de letras. O padrão é **0**.
  - **Letras minúsculas:** Especifica o número mínimo de letras minúsculas. O padrão é **0**.
  - **Letras maiúsculas:** Especifica o número mínimo de letras maiúsculas. O padrão é **0**.
  - **Números ou símbolos:** Especifica o número mínimo de números ou símbolos. O padrão é **0**.
  - **Números:** Especifica o número mínimo de números. O padrão é **0**.
  - **Caracteres alterados:** Para dispositivos que executam o Knox 3.0 e posterior e que têm uma chave de licença Knox válida configurada. Especifica o número de caracteres que os usuários devem alterar em relação à senha anterior. O padrão é **0**.
- **Número máximo de:** Para dispositivos que executam o Knox 3.0 e posterior e que têm uma chave de licença Knox válida configurada.
  - **Número de vezes que um caractere pode ocorrer:** Especifica o número máximo de vezes que um caractere pode ocorrer em uma senha. O padrão é **0**, o que significa que não há limite máximo.
  - **Comprimento da sequência alfabética:** Especifica o comprimento máximo de uma sequência alfabética em uma senha. O padrão é **0**, o que significa que não há limite máximo.
  - **Comprimento da sequência numérica:** Especifica o comprimento máximo de uma sequência numérica em uma senha. O padrão é **0**, o que significa que não há limite máximo.
- **Habilitar senha unificada:** Se **Ativado**, os usuários usam uma senha para o dispositivo e o perfil de trabalho. Se **Desativado**:
  - Os usuários devem usar senhas diferentes para o dispositivo e o perfil de trabalho.

- A configuração **Usar um bloqueio** no dispositivo, que os usuários definem se desejam usar uma senha para o dispositivo e o perfil de trabalho, é desabilitada. O usuário não pode habilitá-la.
- Se o requisito de senha para o desafio de segurança do perfil de trabalho for mais complexo do que a senha do dispositivo: Os usuários com a configuração **Usar um bloqueio** ativada são solicitados a alterar as senhas do perfil de trabalho.

O padrão é **Desativado**. Disponível a partir do Android 9.0.

- **Segurança de senha para o desafio de segurança do perfil de trabalho**
  - **Limpar o contêiner após (tentativas de logon falhas):** Especifica o número de vezes que um usuário pode falhar ao fazer logon, após o qual o perfil de trabalho e seus dados são apagados do dispositivo. Os usuários devem reinicializar o perfil de trabalho após a limpeza. O padrão é **Não definido**.
  - **Bloquear contêiner após (minutos de inatividade):** Especifica o número de minutos que um dispositivo pode ficar inativo antes que o perfil de trabalho seja bloqueado. O padrão é **Nenhum**.
  - **Expiração da senha em dias (1-730):** Especifica o número de dias após os quais a senha expira. Os valores válidos são 1–730. O padrão é **0**, o que significa que a senha nunca expira.
  - **Senhas anteriores salvas (0-50):** Especifica o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 0–50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Bloquear o contêiner após (tentativas de logon falhas):** Para dispositivos que executam o Knox 3.0 e posterior e que têm uma chave de licença Knox válida configurada. Especifica o número de vezes que um usuário pode falhar ao fazer logon, após o qual o dispositivo é bloqueado. O padrão é **Não definido**.

Configurações de Desktop/Tablet Windows



- **Não permitir logon de conveniência:** Selecione se deseja permitir que os usuários acessem seus dispositivos com senhas de imagem ou logons biométricos. O padrão é **Desativado**.
- **Comprimento mínimo da senha:** Selecione o comprimento mínimo da senha na lista suspensa. O padrão é **6**.
- **Máximo de tentativas de senha antes da limpeza:** Na lista, clique no número de vezes que um usuário pode falhar ao fazer login com sucesso, após o qual os dados corporativos são apagados do dispositivo. O padrão é **4**.
- **Expiração da senha em dias (0-730):** Digite o número de dias após os quais a senha expira. Os valores válidos são 0–730. O padrão é **0**, o que significa que a senha nunca expira.
- **Histórico de senhas: (1-24):** Digite o número de senhas usadas a serem salvas. Os usuários não podem usar nenhuma senha encontrada nesta lista. Os valores válidos são 1–24. Você deve inserir um número entre 1 e 24 neste campo. O padrão é **0**.
- **Inatividade máxima antes do bloqueio do dispositivo em minutos (1-999):** Digite a duração em minutos que um dispositivo pode ficar inativo antes de ser bloqueado. Os valores válidos são 1–999. Você deve inserir um número entre 1 e 999 neste campo. O padrão é **0**.

Política de dispositivo de hotspot pessoal

Você pode permitir que os usuários se conectem à Internet quando não estiverem no alcance de uma rede Wi-Fi, usando a conexão de dados celulares através da funcionalidade de hotspot pessoal de seus dispositivos iOS. Disponível no iOS 7.0 e posterior.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

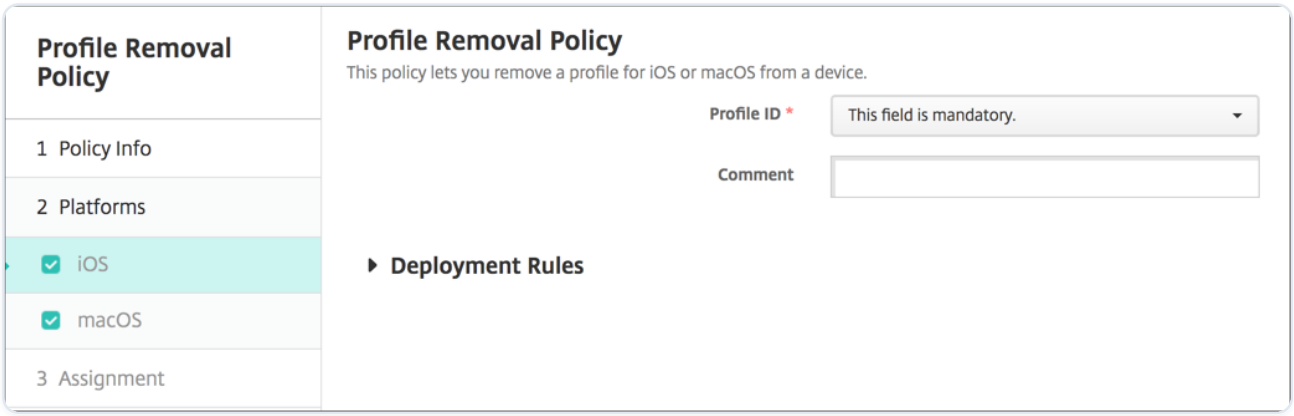
Desabilitar hotspot pessoal: Selecione se deseja desabilitar a funcionalidade de hotspot pessoal nos dispositivos dos usuários. O padrão é **Desativado**, que desliga o hotspot pessoal nos dispositivos dos usuários. Esta política não desabilita a funcionalidade. Os usuários ainda podem usar o hotspot pessoal em seus dispositivos. Mas quando a política é implantada, o hotspot pessoal é desativado para que não permaneça ligado por padrão.

Política de dispositivo de remoção de perfil

Você pode criar uma política de dispositivo de remoção de perfil de aplicativo no XenMobile. A política, quando implantada, remove o perfil do aplicativo dos dispositivos iOS ou macOS dos usuários.

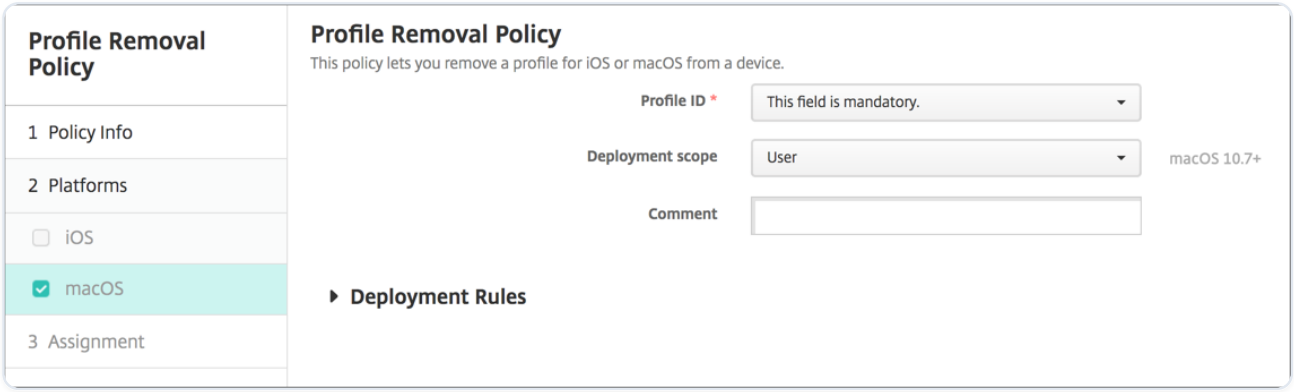
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



- **ID do Perfil:** Selecione o ID do perfil do aplicativo na lista suspensa. Este campo é obrigatório.
- **Comentário:** Digite um comentário opcional.

Configurações do macOS



- **ID do Perfil:** Selecione o ID do perfil do aplicativo na lista suspensa. Este campo é obrigatório.
- **Escopo de implantação:** Selecione **Usuário** ou **Sistema** na lista suspensa. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.
- **Comentário:** Digite um comentário opcional.

Política de dispositivo de perfil de provisionamento

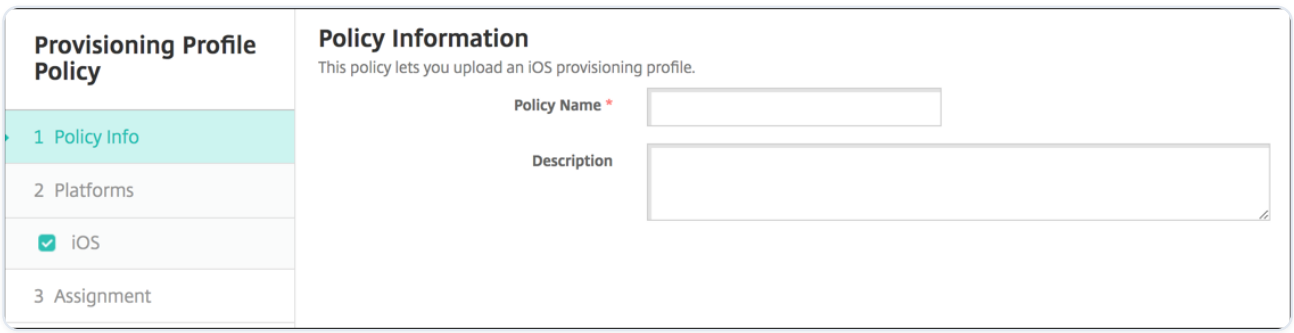
Ao desenvolver e assinar um aplicativo empresarial iOS, você geralmente inclui um perfil de provisionamento de distribuição empresarial, que a Apple exige para que o aplicativo seja executado em um dispositivo iOS. Se um perfil de provisionamento estiver ausente ou tiver expirado, o aplicativo falhará quando um usuário tocar para abri-lo.

O principal problema com os perfis de provisionamento é que eles expiram um ano após serem gerados no Apple Developer Portal e você deve acompanhar as datas de expiração de todos os seus perfis de provisionamento em todos os dispositivos iOS registrados por seus usuários. O acompanhamento das datas de expiração não envolve apenas o controle das datas de expiração reais, mas também quais usuários estão usando qual versão do aplicativo. Duas soluções são enviar perfis de provisionamento por e-mail aos usuários ou colocá-los em um portal da web para download e instalação. Essas soluções funcionam, mas são propensas a erros porque exigem que os usuários reajam às instruções em um e-mail ou acessem o portal da web para baixar o perfil correto e, em seguida, instalá-lo.

Para tornar esse processo transparente para os usuários, no XenMobile®, você pode instalar e remover perfis de provisionamento com políticas de dispositivo. Perfis ausentes ou expirados são removidos conforme necessário e os perfis atualizados são instalados nos dispositivos dos usuários, de modo que tocar em um aplicativo simplesmente o abre para uso.

Antes de criar uma política de perfil de provisionamento, você deve criar um arquivo de perfil de provisionamento. Para obter mais informações, consulte o artigo da Apple sobre como criar um perfil de provisionamento de desenvolvimento no site do Desenvolvedor Apple.

Configurações do iOS



- **Perfil de provisionamento do iOS:** Selecione o arquivo de perfil de provisionamento para importar clicando em **Procurar** e, em seguida, navegando até o local do arquivo.

Política de dispositivo de remoção de perfil de provisionamento

Você pode remover perfis de provisionamento iOS com políticas de dispositivo. Para obter mais informações sobre perfis de provisionamento, consulte Política de dispositivo de perfil de provisionamento.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Perfil de provisionamento iOS:** Clique no perfil de provisionamento na lista suspensa que você deseja remover.
- **Comentário:** Opcionalmente, adicione um comentário.

Política de dispositivo proxy

Você pode adicionar uma política de dispositivo no XenMobile para especificar configurações globais de proxy HTTP para dispositivos que executam iOS 6.0 ou posterior. Você pode implantar apenas uma política global de proxy HTTP por dispositivo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

Antes de implantar esta política, certifique-se de definir todos os dispositivos iOS para os quais você deseja configurar um proxy HTTP global no modo Supervisionado. Para obter detalhes, consulte Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator ou Implantar dispositivos por meio do Apple Deployment Program.

Defina as regras de implantação para registrar dispositivos antes de enviar a política de Proxy para os dispositivos.

Configurações do iOS

- **Configuração de proxy:** Clique em **Manual** ou **Automático** para definir como o proxy será configurado nos dispositivos dos usuários.

    - Se você clicar em **Manual**, configure estas definições:
        - **Nome do host ou endereço IP do servidor proxy:** Digite o nome do host ou o endereço IP do servidor proxy. Este campo é obrigatório.
        - **Porta do servidor proxy:** Digite o número da porta do servidor proxy. Este campo é obrigatório.
        - **Nome de usuário:** Digite um nome de usuário opcional para autenticar no servidor proxy.
        - **Senha:** Digite uma senha opcional para autenticar no servidor proxy.
    - Se você clicar em **Automático**, configure estas definições:
        - **URL PAC do proxy:** Digite a URL do arquivo PAC que define a configuração do proxy.
        - **Permitir conexão direta se o PAC estiver inacessível:** Selecione se deseja permitir que os usuários se conectem diretamente ao destino caso o arquivo PAC esteja inacessível. O padrão é **Ativado**. Esta opção está disponível apenas no iOS 7.0 e posterior.

- **Permitir ignorar o proxy para acessar redes cativas:** Selecione se deseja permitir ignorar o proxy para acessar redes cativas. O padrão é **Desativado**.
- **Configurações da política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de restrições de dispositivo

A política de restrições de dispositivo permite ou restringe certos recursos ou funcionalidades em dispositivos de usuário, como a câmera. Você também pode definir restrições de segurança, além de restrições de conteúdo de mídia e restrições sobre os tipos de aplicativos que os usuários podem e não podem instalar. A maioria das configurações de restrição é padronizada para **Ativado**, ou *permite*. As principais exceções são o recurso iOS Security - Force e todos os recursos do Windows Tablet, que são padronizados para **Desativado**, ou *restringe*.

Para Windows 10 RS2 Phone: Depois que uma política XML personalizada ou política de restrições que desabilita o Internet Explorer é implantada no telefone, o navegador permanece habilitado. Para contornar esse problema, reinicie o telefone. Este é um problema de terceiros.

Dica:

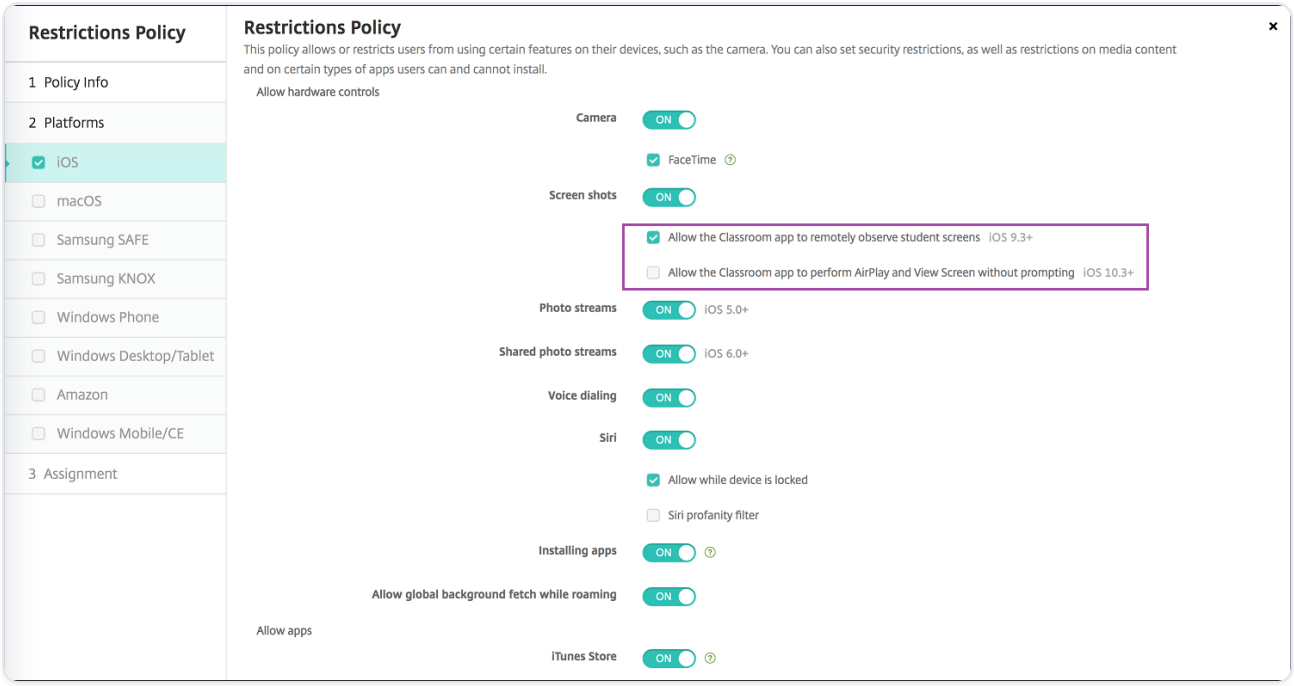
Qualquer opção para a qual você seleciona **Ativado** significa que o usuário pode realizar a operação ou usar o recurso. Por exemplo:

Câmera. Se **Ativado**, o usuário pode usar a câmera em seu dispositivo. Se **Desativado**, o usuário não pode usar a câmera em seu dispositivo.

Capturas de tela. Se **Ativado**, o usuário pode tirar capturas de tela em seu dispositivo. Se **Desativado**, o usuário não pode tirar capturas de tela em seu dispositivo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS



Algumas configurações da política de restrições do iOS se aplicam apenas a versões específicas do iOS, conforme observado aqui e na página da política de Restrições do console XenMobile®.

As configurações da política de restrições do iOS podem ser aplicadas quando o dispositivo está registrado no modo de registro de usuário, modo não supervisionado (MDM completo) ou modo supervisionado. A tabela a seguir mostra os modos de registro disponíveis para cada configuração da política de restrições para iOS 13 e posterior.

Conforme observado na tabela, algumas configurações que estavam anteriormente disponíveis nos modos não supervisionado e supervisionado estão disponíveis apenas no modo supervisionado a partir do iOS 13. As seguintes regras se aplicam:

- Se um dispositivo iOS 13+ supervisionado se registrar no XenMobile, as configurações serão aplicadas ao dispositivo.
- Se um dispositivo iOS 13+ não supervisionado se registrar no XenMobile, as configurações não serão aplicadas ao dispositivo.
- Se um dispositivo iOS 12 (ou inferior) já inscrito no XenMobile e depois atualizado para iOS 13, não há alterações. As configurações se aplicam ao dispositivo como antes da atualização.

Para obter informações sobre como configurar um dispositivo iOS para o modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Permitir controles de hardware			
Câmera	Não	Sim	Sim
FaceTime	Não	Não (novo no iOS 13)	Sim
Permitir Controle Remoto do FaceTime	Não	Não	Sim
Capturas de tela	Sim	Não	Sim
Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Permitir que o aplicativo Sala de Aula execute AirPlay e Visualizar Tela sem solicitar	Não	Não	Sim
Fluxos de fotos	Não	Sim	Sim
Fluxos de fotos compartilhados	Não	Sim	Sim
Permitir sessão temporária de iPad compartilhado	Não	Sim	Sim
Discagem por voz	Não	Sim	Sim
Siri	Sim	Sim	Sim
Permitir enquanto o dispositivo estiver bloqueado	Sim	Sim	Sim
Filtro de palavrões da Siri	Não	Não	Sim
Instalando aplicativos	Não	Não (novo no iOS 13)	Sim
Mercado de Aplicativos Alternativo	Não	Não	Sim
Aplicativos de Distribuição Web	Não	Não	Sim
Permitir busca global em segundo plano durante o roaming	Não	Sim	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Permitir aplicativos			
iTunes Store	Não	Não (novo no iOS 13)	Sim
Compras no aplicativo	Não	Sim	Sim
Exigir senha do iTunes para compras	Não	Sim	Sim
Safari	Não	Não (novo no iOS 13)	Sim
Autopreenchimento	Não	Não (novo no iOS 13)	Sim
Forçar aviso de fraude	Sim	Sim	Sim
Ativar JavaScript	Não	Sim	Sim
Bloquear pop-ups	Não	Sim	Sim
Aceitar cookies	Não	Sim	Sim
Rede - Permitir ações do iCloud			
Documentos e dados do iCloud	Não	Não (novo no iOS 13)	Sim
Backup do iCloud	Não	Sim	Sim
Chaveiro de fotos do iCloud	Não	Sim	Sim
Biblioteca de fotos do iCloud	Não	Sim	Sim
Segurança - Forçar			

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Backups criptografados	Sim	Sim	Sim
Rastreamento de anúncios limitado	Não	Sim	Sim
Senha no primeiro emparelhamento AirPlay	Sim	Sim	Sim
Apple Watch emparelhado para usar Detecção de Pulso	Sim	Sim	Sim
Compartilhamento de documentos gerenciados usando AirDrop	Sim	Sim	Sim
Segurança - Permitir			
Aceitar certificados SSL não confiáveis	Não	Sim	Sim
Atualização automática das configurações de confiança de certificado	Não	Sim	Sim
Exigir área de transferência gerenciada	Sim	Sim	Sim
Documentos de aplicativos gerenciados em	Sim	Sim	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
aplicativos não gerenciados			
Aplicativos não gerenciados leem contatos gerenciados	Não	Não	Sim
Aplicativos gerenciados escrevem contatos não gerenciados	Não	Não	Sim
Documentos de aplicativos não gerenciados em aplicativos gerenciados	Sim	Sim	Sim
Envio de diagnóstico para a Apple	Sim	Sim	Sim
Touch ID para desbloquear o dispositivo	Não	Sim	Sim
Desbloqueio automático	Não	Sim	Sim
Notificações do Passbook quando bloqueado	Não	Sim	Sim
Handoff	Não	Sim	Sim
Sincronização do iCloud para aplicativos gerenciados	Sim	Sim	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Backup para livros corporativos	Sim	Sim	Sim
Sincronização de notas e destaques para livros corporativos	Sim	Sim	Sim
Resultados da Internet no Spotlight	Não	Sim	Sim
Confiança em aplicativos empresariais	Não	Sim	Sim
Permitir publicidade personalizada da Apple	Não	Sim	Sim
Configurações somente supervisionadas - Permitir			
Permitir modificação de eSIM	Não	Não	Sim
Preservar eSIM ao apagar	Não	Não	Sim
Apagar todo o conteúdo e configurações	Não	Não	Sim
Configurando restrições	Não	Não	Sim
Podcasts	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Instalando perfis de configuração	Não	Não	Sim
Modificação de impressão digital	Não	Não	Sim
Instalando aplicativos do dispositivo	Não	Não	Sim
Atalhos de teclado	Não	Não	Sim
Apple Watch emparelhado	Não	Não	Sim
Modificação de senha	Não	Não	Sim
Modificação do nome do dispositivo	Não	Não	Sim
Modificação de papel de parede	Não	Não	Sim
Download automático de aplicativos	Não	Não	Sim
AirDrop	Não	Não	Sim
iMessage	Não	Não	Sim
Conteúdo gerado pelo usuário da Siri	Não	Não	Sim
iBooks	Não	Não	Sim
Remoção de aplicativos	Não	Sim	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Game Center	Não	Não (novo no iOS 13)	Sim
Adicionar amigos	Não	Não	Sim
Jogos multijogador	Não	Não (novo no iOS 13)	Sim
Modificar configurações da conta	Não	Não	Sim
Modificar configurações de dados celulares do aplicativo	Não	Não	Sim
Permitir conexões de unidade de rede	Não	Não	Sim
Permitir conexões de dispositivo USB	Não	Não	Sim
Permitir Buscar Meu Dispositivo	Não	Não	Sim
Permitir Buscar Meus Amigos	Não	Não	Sim
Modificar as configurações de Buscar Meus Amigos	Não	Não	Sim
Emparelhamento com hosts que não são do Configurator	Não	Não	Sim
Teclados preditivos	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Autocorreções do teclado	Não	Não	Sim
Verificação ortográfica do teclado	Não	Não	Sim
Permitir teclado QuickPath	Não	Não	Sim
Pesquisa de definição	Não	Não	Sim
ID do pacote de aplicativo único	Não	Não	Sim
Notícias	Não	Não	Sim
Serviço Apple Music	Não	Não	Sim
iTunes Radio	Não	Não	Sim
Modificação de notificações	Não	Não	Sim
Uso restrito de aplicativos	Não	Não	Sim
Modificação de envio de diagnóstico	Não	Não	Sim
Modificação de Bluetooth	Não	Não	Sim
Permitir ditado	Não	Não	Sim
Forçar Wi-Fi ativado	Não	Não	Sim
Conectar-se apenas a redes Wi-Fi	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
instaladas por uma política de Wi-Fi			
Permitir que o aplicativo Sala de Aula execute AirPlay e Visualizar Tela sem solicitar	Não	Não	Sim
Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar	Não	Não	Sim
Entrar automaticamente nas turmas do aplicativo Sala de Aula sem solicitar	Não	Não	Sim
Permitir AirPrint	Não	Não	Sim
Permitir o armazenamento de credenciais do AirPrint no Keychain	Não	Não	Sim
Permitir a descoberta de impressoras AirPrint usando iBeacons	Não	Não	Sim
Permitir AirPrint apenas para destinos com certificados confiáveis	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Adicionar configurações de VPN	Não	Não	Sim
Modificar configurações do plano de celular	Não	Não	Sim
Remover aplicativos do sistema	Não	Não	Sim
Configurar novos dispositivos próximos	Não	Não	Sim
Permitir modo restrito USB	Não	Não	Sim
Forçar atualizações de software atrasadas	Não	Não	Sim
Atraso forçado na atualização de software	Não	Não	Sim
Forçar permissão de solicitação da sala de aula para sair das aulas	Não	Não	Sim
Forçar autenticação antes do preenchimento automático	Não	Não	Sim
Forçar data e hora automáticas	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Preenchimento automático de senha	Não	Não	Sim
Solicitações de proximidade de senha	Não	Não	Sim
Compartilhamento de Senha	Não	Não	Sim
Modificar configurações de Hotspot pessoal	Não	Não	Sim
Permitir inicialização para recuperação por um dispositivo não emparelhado	Não	Não	Sim
Instalar resposta de segurança rápida	Não	Não	Sim
Remover resposta de segurança rápida	Não	Não	Sim
Permitir proteção de privacidade de e-mail	Não	Não	Sim
NFC	Não	Não	Sim
Permitir App clips	Não	Não	Sim
Genmoji	Não	Não	Sim
Image Playground	Não	Não	Sim
Image Wand	Não	Não	Sim
Espelhamento do iPhone	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Resultados de Escrita Manual Personalizados	Não	Não	Sim
Ferramentas de Escrita	Não	Não	Sim
Gravação de Chamadas	Não	Não	Sim
Aplicativos a Serem Ocultados	Não	Não	Sim
Aplicativos a Serem Bloqueados	Não	Não	Sim
Resumo de E-mail	Não	Não	Sim
Mensagens RCS	Não	Não	Sim
Permitir integrações de inteligência externa	Não	Não	Sim
Permitir login em integrações de inteligência externa	Não	Não	Sim
Permitir Respostas Inteligentes de E-mail	Não	Não	Sim
Permitir Transcrição de Notas	Não	Não	Sim
Permitir Resumo do Safari	Não	Não	Sim
Permitir resumo de inteligência visual	Não	Não	Sim

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Permitir Resumo da Transcrição de Notas	Não	Não	Sim
Permitir Relatório de Inteligência da Apple	Não	Não	Sim
Permitir Modificação do Aplicativo de Chamada Padrão	Não	Não	Sim
Permitir Modificação do Aplicativo de Mensagens Padrão	Não	Não	Sim
Permitir IDs de Workspace de Inteligência Externa	Não	Não	Sim
Modificação do Navegador Padrão	Não	Não	Sim
Permitir Correio de Voz ao Vivo	Não	Não	Sim
Segurança - Mostrar na tela de bloqueio			
Central de Controle	Sim	Sim	Sim
Notificação	Sim	Sim	Sim
Visualização Hoje	Sim	Sim	Sim
Conteúdo de mídia - Permitir			

CONFIGURAÇÃO	INSCRIÇÃO DO USUÁRIO	NÃO SUPERVISIONADO	SUPERVISIONADO
Música explícita, podcasts e material do iTunes U	Não	Não (novo no iOS 13)	Sim
Conteúdo sexual explícito no iBooks	Não	Sim	Sim
Região de classificações	Não	Sim	Sim
Filmes	Não	Sim	Sim
Programas de TV	Não	Sim	Sim
Aplicativos	Não	Sim	Sim

- **Permitir controles de hardware**
  - **Câmera:** Permite que os usuários usem a câmera em seus dispositivos.
    - **FaceTime:** Permite que os usuários usem o FaceTime em seus dispositivos. Para dispositivos iOS supervisionados.
    - **Permitir Controle Remoto do FaceTime:** Permite que uma sessão remota do FaceTime solicite o controle do dispositivo. Para dispositivos iOS supervisionados. Disponível para iOS 18.4 e posterior.
  - **Capturas de tela:** Permite que os usuários tirem capturas de tela em seus dispositivos.
    - **Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos:** Se esta restrição não estiver selecionada, um instrutor não poderá usar o aplicativo Sala de Aula para observar remotamente as telas dos alunos. A configuração padrão é selecionada, um instrutor pode usar o aplicativo Sala de Aula para observar as telas dos alunos. A configuração para **Permitir que o aplicativo Sala de Aula execute AirPlay e Visualizar Tela sem solicitar** determina se os alunos recebem um prompt para dar permissão ao instrutor. Para dispositivos iOS supervisionados.
    - **Permitir que o aplicativo Sala de Aula execute AirPlay e Visualizar Tela sem solicitar:** Se esta restrição estiver selecionada, o instrutor poderá executar AirPlay e

Visualizar Tela em um dispositivo de aluno, sem solicitar permissão. A configuração padrão é desmarcada. Para dispositivos iOS supervisionados.

- **Fluxos de fotos:** Permite que os usuários usem o MyPhotoStream para compartilhar fotos via iCloud com todos os seus dispositivos iOS.
- **Fluxos de fotos compartilhados:** Permite que os usuários usem o Compartilhamento de Fotos do iCloud para compartilhar fotos com colegas de trabalho, amigos e familiares.
- **Permitir sessão temporária de iPad compartilhado:** Impede o acesso a sessões temporárias em iPads compartilhados quando a configuração é **Desativado**. O padrão é **Ativado**.
- **Discagem por voz:** Habilita a discagem por voz nos dispositivos do usuário.
- **Siri:** Permite que os usuários usem a Siri.
  - **Permitir com o dispositivo bloqueado:** Permite que os usuários usem a Siri enquanto seus dispositivos estão bloqueados.
  - **Filtro de palavrões da Siri:** Habilita o filtro de palavrões da Siri. O padrão é restringir esse recurso, o que significa que nenhuma filtragem de palavrões é feita.

    Para obter mais informações sobre a Siri e segurança, consulte Políticas de Siri e ditado.
- **Instalação de aplicativos:** Permite que os usuários instalem aplicativos. Para dispositivos iOS supervisionados.
- **Mercado de aplicativos alternativo:** Impede a instalação de aplicativos de mercados alternativos da web e impede que quaisquer aplicativos de mercados alternativos instalados instalem aplicativos. Este recurso está disponível a partir do iOS 17.4 e versões posteriores. O padrão é **Ativado**. Para dispositivos iOS supervisionados.
- **Aplicativos de distribuição web:** Permite que os administradores de clientes bloqueiem aplicativos de terceiros distribuídos pela web em dispositivos iOS. Isso é aplicável para as versões 17.5 e posteriores do iOS. Para obter mais informações, consulte Restrições.
- **Permitir busca em segundo plano global durante o roaming:** Permite que os dispositivos sincronizem automaticamente as contas de e-mail com o iCloud enquanto o dispositivo está em roaming. Quando **Desativado**, desabilita a atividade de busca em segundo plano global quando um telefone iOS está em roaming. O padrão é **Ativado**.

- **Permitir aplicativos**

- **iTunes Store:** Permite que os usuários acessem a iTunes Store. Para dispositivos iOS supervisionados.
- **Compras no aplicativo:** Permite que os usuários façam compras no aplicativo.
  - **Exigir senha do iTunes para compras:** Exige uma senha para compras no aplicativo. O padrão é restringir esse recurso, o que significa que nenhuma senha é exigida para compras no aplicativo.
- **Safari:** Permite que os usuários acessem o Safari. Para dispositivos iOS supervisionados.
  - **Preenchimento automático:** Permite que os usuários configurem o preenchimento automático para nomes de usuário e senhas no Safari.
  - **Forçar aviso de fraude:** Se esta configuração estiver ativada e os usuários visitarem um site de phishing suspeito, o Safari alerta os usuários. O padrão é restringir este recurso, o que significa que nenhum aviso é emitido.
  - **Ativar JavaScript:** Permitir que o JavaScript seja executado no Safari.
  - **Bloquear pop-ups:** Bloquear pop-ups ao visualizar sites. O padrão é restringir este recurso, o que significa que os pop-ups não são bloqueados.
- **Aceitar cookies:** Defina em que medida os cookies são aceitos. Na lista, escolha uma opção para permitir ou restringir cookies. A opção padrão é **Sempre**, que permite que todos os sites salvem cookies no Safari. Outras opções são **Somente site atual**, **Nunca** e **Somente de sites visitados**.

- **Rede - Permitir ações do iCloud**
  - **Documentos e dados do iCloud:** Permitir que os usuários sincronizem documentos e dados com o iCloud. Para dispositivos iOS supervisionados.
  - **Backup do iCloud:** Permitir que os usuários façam backup de seus dispositivos no iCloud.
  - **Chaveiro do iCloud:** Permitir que os usuários armazenem senhas, rede Wi-Fi, cartão de crédito e outras informações no Chaveiro do iCloud.
  - **Biblioteca de fotos na nuvem:** Permitir que os usuários acessem sua biblioteca de fotos do iCloud.
- **Segurança - Forçar**

  O padrão é restringir os seguintes recursos, o que significa que nenhum recurso de segurança está ativado.
  - **Backups criptografados:** Forçar que os backups para o iCloud sejam criptografados.

- **Rastreamento de anúncios limitado:** Bloquear o rastreamento de anúncios direcionados.
- **Senha no primeiro emparelhamento do AirPlay:** Exigir que os dispositivos habilitados para AirPlay sejam verificados com um código único na tela antes que possam usar o AirPlay.
- **Apple Watch emparelhado para usar Detecção de Pulso:** Exigir que um Apple Watch emparelhado use a **Detecção de Pulso**.
- **Compartilhamento de documentos gerenciados usando AirDrop:** Definir esta opção como **Ativado** faz com que o AirDrop apareça como um destino de soltura não gerenciado.

- **Segurança - Permitir**
  - **Aceitar certificados SSL não confiáveis:** Permitir que os usuários aceitem certificados SSL não confiáveis de sites.
  - **Atualização automática das configurações de confiança de certificado:** Permitir que certificados confiáveis sejam atualizados automaticamente.
  - **Exigir área de transferência gerenciada:** Se Ativado, permitir que a funcionalidade de copiar e colar siga as mesmas restrições que você aplica a **Documentos de aplicativos gerenciados em aplicativos não gerenciados** e **Documentos de aplicativos não gerenciados em aplicativos gerenciados**. O padrão é **Desativado**. Por exemplo, você configura o seguinte:
    - **Exigir área de transferência gerenciada**: Ativado
    - **Documentos de aplicativos gerenciados em aplicativos não gerenciados**: Desativado
    - **Documentos de aplicativos não gerenciados em aplicativos gerenciados**: Ativado

    > **Observação:**
    >
    > Depois de implantar a política em dispositivos iOS, os usuários não podem copiar e colar dados de aplicativos gerenciados para aplicativos não gerenciados, mas podem copiar e colar dados de aplicativos não gerenciados para aplicativos gerenciados.

  - **Documentos de aplicativos gerenciados em aplicativos não gerenciados:** Permitir que os usuários movam dados de aplicativos gerenciados (corporativos) para aplicativos não gerenciados (pessoais).

- **Documentos de aplicativos não gerenciados em aplicativos gerenciados:** Permitir que os usuários movam dados de aplicativos não gerenciados (pessoais) para aplicativos gerenciados (corporativos).
- **Envio de diagnóstico para a Apple:** Permitir que dados de diagnóstico anônimos sobre os dispositivos dos usuários sejam enviados para a Apple.
- **Touch ID para desbloquear dispositivo:** Permitir que os usuários usem suas impressões digitais para desbloquear seus dispositivos.
- **Desbloqueio automático:** Se **Desativado**, o usuário não pode usar o Apple Watch para desbloquear um iPhone emparelhado. O padrão é **Ativado**. Disponível para iOS 14.5 ou posterior.
- **Notificações do Passbook quando bloqueado:** Permitir que as notificações do Passbook apareçam na tela de bloqueio.
- **Handoff:** Permitir que os usuários transfiram atividades de um dispositivo iOS para outro dispositivo iOS próximo.
- **Sincronização do iCloud para aplicativos gerenciados:** Permitir que os usuários sincronizem aplicativos gerenciados com o iCloud.
- **Backup para livros corporativos:** Permitir que livros corporativos sejam copiados para o iCloud.
- **Sincronização de notas e destaques para livros corporativos:** Permitir que notas e destaques que os usuários adicionaram a livros corporativos sejam sincronizados com o iCloud.
- **Confiança em aplicativos corporativos:** Permitir que aplicativos corporativos sejam confiáveis. Aplicativos corporativos são quaisquer aplicativos feitos sob medida para sua organização. Eles podem ser feitos internamente ou podem ser desenvolvidos e comprados de um fornecedor externo. Para obter informações adicionais, consulte Instalar aplicativos corporativos personalizados no iOS.
- **Resultados da Internet no Spotlight:** Permitir que o Spotlight mostre resultados de pesquisa da Internet, além dos resultados do dispositivo.
- **Aplicativos não gerenciados leem contatos gerenciados:** Opcional. Disponível apenas se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver desabilitado. Se esta política estiver habilitada, aplicativos não gerenciados podem ler dados dos contatos de contas gerenciadas. O padrão é **Desativado**. Disponível a partir do iOS 12.

- **Aplicativos gerenciados gravam contatos não gerenciados:** Opcional. Se habilitado, permite que aplicativos gerenciados gravem contatos nos contatos de contas não gerenciadas. Se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver habilitado, esta restrição não terá efeito. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Permitir publicidade personalizada da Apple:** Se **Desativado**, os dados dos usuários não são usados pela plataforma de publicidade da Apple para exibir anúncios personalizados. O padrão é **Ativado**. Disponível para iOS 14.0 ou posterior.

- **Configurações somente para dispositivos supervisionados - Permitir**

  Essas configurações se aplicam apenas a dispositivos supervisionados. Para as etapas sobre como definir um dispositivo iOS para o modo supervisionado, consulte Para colocar um dispositivo iOS no modo supervisionado usando o Apple Configurator.

  - **Permitir modificação de eSIM:** Permitir que os usuários alterem as configurações de eSIM em seus dispositivos.
  - **Preservar eSIM ao apagar:** Se **Ativado**, o sistema preserva o eSIM ao apagar o dispositivo devido a muitas tentativas de senha falhas ou à opção Apagar Conteúdo e Ajustes em **Ajustes** > **Geral** > **Redefinir**. O padrão é **Desativado**.

  > **Observação:**
  >
  > O sistema não preserva o eSIM se o **Buscar Meu** iniciar a exclusão do dispositivo.

  - **Apagar todo o conteúdo e ajustes:** Permite que os usuários apaguem todo o conteúdo e ajustes de seus dispositivos.
  - **Configurar restrições:** Permite que os usuários configurem controles parentais em seus dispositivos.
  - **Podcasts:** Permite que os usuários baixem e sincronizem podcasts.
  - **Instalar perfis de configuração:** Permite que os usuários instalem um perfil de configuração diferente daquele implantado por você.
  - **Modificação de impressão digital:** Permite que os usuários alterem ou excluam sua impressão digital do Touch ID.

- **Instalar aplicativos do dispositivo:** Permite que os usuários instalem aplicativos. Desabilitar esta configuração impede que os usuários finais instalem novos aplicativos. A App Store é desabilitada e seu ícone é removido da Tela de Início.
- **Atalhos de teclado:** Permite que os usuários criem atalhos de teclado personalizados para palavras ou frases que usam com frequência.
- **Apple Watch emparelhado:** Permite que os usuários emparelhem um Apple Watch a um dispositivo supervisionado.
- **Modificação de senha:** Permite que os usuários alterem a senha em um dispositivo supervisionado.
- **Modificação do nome do dispositivo:** Permite que os usuários alterem o nome de seu dispositivo.
- **Modificação de papel de parede:** Permite que os usuários alterem o papel de parede em seus dispositivos.
- **Download automático de aplicativos:** Permite que os aplicativos sejam baixados.
- **AirDrop:** Permite que os usuários compartilhem fotos, vídeos, sites, localizações e muito mais com dispositivos iOS próximos.
- **iMessage:** Permite que os usuários enviem mensagens de texto via Wi-Fi com o iMessage.
- **Conteúdo gerado pelo usuário da Siri:** Permitir que a Siri consulte conteúdo gerado pelo usuário da web. Consumidores, não jornalistas tradicionais; produzem conteúdo gerado pelo usuário. Por exemplo, o conteúdo encontrado no Twitter ou Facebook é gerado pelo usuário.
- **iBooks:** Permitir que os usuários usem o aplicativo iBooks.
- **Remoção de aplicativos:** Permitir que os usuários removam aplicativos de seus dispositivos.
- **Game Center:** Permitir que os usuários joguem online através do Game Center em seus dispositivos.
  - **Adicionar amigos:** Permitir que os usuários enviem uma notificação a um amigo para jogar.
  - **Jogos multiplayer:** Permitir que os usuários iniciem jogos multiplayer em seus dispositivos.
- **Modificação das configurações da conta:** Permitir que os usuários modifiquem as configurações da conta de seus dispositivos.

- **Modificação das configurações de dados celulares do aplicativo:** Permitir que os usuários modifiquem como os aplicativos usam dados celulares.
- **Permitir conexões de unidade de rede:** Impede a conexão a unidades de rede no aplicativo Arquivos quando a configuração está **Desativada**. O padrão é **Ativado**.
- **Permitir conexões de dispositivos USB:** Impede a conexão a quaisquer dispositivos USB conectados no aplicativo Arquivos quando a configuração está **Desativada**. O padrão é **Ativado**.
- **Permitir Buscar Meu Dispositivo:** Desativa a opção **Buscar Meu Dispositivo** no aplicativo Buscar quando a configuração está **Desativada**. O padrão é **Ativado**.
- **Permitir Buscar Meus Amigos:** Desativa a opção **Buscar Meus Amigos** no aplicativo Buscar quando a configuração está **Desativada**. O padrão é **Ativado**.
- **Modificação das configurações de Buscar Meus Amigos:** Permitir que os usuários alterem suas configurações de Buscar Meus Amigos.
- **Emparelhamento com hosts não-Configurator:** Permitir que o administrador controle com quais dispositivos um dispositivo de usuário pode emparelhar. Desativar esta configuração impede o emparelhamento, exceto com o host supervisor executando o Apple Configurator. Se nenhum certificado de host supervisor estiver configurado, todo o emparelhamento será desativado.
- **Teclados preditivos:** Permitir que os dispositivos do usuário usem o teclado preditivo para sugerir palavras enquanto digitam. Desative esta opção em situações como a administração de testes padronizados, onde você não deseja que os usuários tenham acesso a palavras sugeridas.
- **Correções automáticas do teclado:** Permitir que os dispositivos do usuário usem a correção automática do teclado. Desative esta opção em situações como a administração de testes padronizados, onde você não deseja que os usuários tenham acesso à correção automática.
- **Verificação ortográfica do teclado:** Permitir que os dispositivos do usuário usem a verificação ortográfica durante a digitação. Desative esta opção em situações como a administração de testes padronizados, onde você não deseja que os usuários tenham acesso ao verificador ortográfico.
- **Permitir teclado QuickPath:** Desativa o teclado QuickPath quando a configuração está **Desativada**. O padrão é **Ativado**.
- **Pesquisa de definição:** Permitir que os dispositivos do usuário usem a pesquisa de definição durante a digitação. Desative esta opção em situações como a administração de

testes padronizados, onde você não deseja que os usuários pesquisem definições enquanto digitam.

- **ID do pacote de aplicativo único:** Crie uma lista de aplicativos que têm permissão para manter o controle sobre o dispositivo e impedir a interação com outros aplicativos ou funções. Para adicionar um aplicativo, clique em **Adicionar**, digite um **Nome do aplicativo** e clique em **Salvar**. Repita esse processo para cada aplicativo que deseja adicionar.
- **Notícias:** Permitir que os usuários usem o aplicativo Notícias.
- **Serviço Apple Music:** Permitir que os usuários usem o serviço Apple Music. Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássico.
- **iTunes Radio:** Permitir que os usuários usem o iTunes Radio.
- **Modificação de notificações:** Permitir que os usuários modifiquem as configurações de notificação.
- **Uso de aplicativo restrito:** Permitir que os usuários usem todos os aplicativos ou usem ou não usem aplicativos, com base nos IDs de pacote que você fornecer. Aplica-se apenas a dispositivos supervisionados. Se você selecionar **Permitir apenas alguns aplicativos**, adicione um aplicativo com o ID de pacote `com.apple.webapp` para permitir web clips.

> **Nota:**
>
> A partir do iOS 11, a Apple introduziu alterações nas políticas disponíveis para restrições de aplicativos. A Apple não permite mais remover o acesso ao aplicativo Ajustes e ao aplicativo Telefone restringindo o pacote de aplicativo iOS apropriado.
>
> Depois de configurar a política de dispositivo de Restrições para bloquear alguns aplicativos e, em seguida, implantar a política: Se você quiser permitir alguns ou todos esses aplicativos posteriormente, alterar e implantar a política de dispositivo de Restrições não altera as restrições. Nesse caso, o iOS não aplica as alterações ao perfil do iOS. Para continuar, use a política de Remoção de Perfil para remover o Perfil do iOS e, em seguida, implante a política de dispositivo de Restrições atualizada.

Se você alterar esta configuração para **Permitir apenas alguns aplicativos:** Antes de implantar esta política, aconselhe os usuários de dispositivos registrados usando o Programa de Implantação da Apple a fazer login em suas contas Apple a partir do Assistente de Configuração. Caso contrário, os usuários podem ter que desativar a

autenticação de dois fatores em seus dispositivos para fazer login em suas contas Apple e acessar aplicativos permitidos.

- **Modificação de envio de diagnóstico:** Permitir que os usuários modifiquem as configurações de envio de diagnóstico e análise de aplicativos no painel **Ajustes > Diagnóstico e Uso**.
- **Modificação de Bluetooth:** Permitir que os usuários modifiquem as configurações de Bluetooth.
- **Permitir ditado:** Somente supervisionado. Se esta restrição for definida como **Desativado**, a entrada de ditado não é permitida, incluindo fala para texto. A configuração padrão é **Ativado**.
- **Forçar Wi-Fi ativado:** Impede que o Wi-Fi seja ativado ou desativado em Ajustes ou na Central de Controle. A ativação do modo avião não tem efeito sobre esta restrição, o que não impede que você escolha a qual rede Wi-Fi se conectar. O padrão é **Desativado**.
- **Conectar-se apenas a redes Wi-Fi instaladas por uma política de Wi-Fi:** Opcional. Somente supervisionado. Se esta restrição for definida como **Ativado**, o dispositivo pode se conectar a redes Wi-Fi somente quando elas foram configuradas por meio de um perfil de configuração. A configuração padrão é **Desativado**.
- **Permitir que o aplicativo Sala de Aula execute AirPlay e Visualizar Tela sem solicitar:** Se esta restrição for selecionada, o instrutor pode executar AirPlay e Visualizar Tela em um dispositivo de aluno, sem solicitar permissão. A configuração padrão é desmarcada. Para dispositivos iOS supervisionados.
- **Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar:** Se esta restrição for definida como **Ativado**, o aplicativo Sala de Aula bloqueia automaticamente os dispositivos dos usuários em um aplicativo e bloqueia o dispositivo, sem solicitar aos usuários. A configuração padrão é **Desativado**. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Entrar automaticamente nas turmas do aplicativo Sala de Aula sem solicitar:** Se esta restrição for definida como **Ativado**, o aplicativo Sala de Aula adiciona automaticamente os usuários às turmas, sem solicitar aos usuários. A configuração padrão é **Desativado**. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Permitir AirPrint:** Se esta restrição for definida como **Desativado**, os usuários não podem imprimir com AirPrint. A configuração padrão é **Ativado**. Quando esta restrição está **Ativado**, estas restrições extras aparecem. Para dispositivos supervisionados executando iOS 11 (versão mínima).

- **Permitir armazenamento de credenciais AirPrint no Keychain:** Se esta restrição for desmarcada, o nome de usuário e a senha do AirPrint não são armazenados no Keychain. A configuração padrão é selecionada. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Permitir descoberta de impressoras AirPrint usando iBeacons:** Se esta restrição for desmarcada, a descoberta de impressoras AirPrint por iBeacon é desativada. Isso impede que beacons Bluetooth AirPrint espúrios realizem phishing de tráfego de rede. A configuração padrão é selecionada. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Permitir AirPrint apenas para destinos com certificados confiáveis:** Se esta restrição for selecionada, os usuários podem usar AirPrint para imprimir apenas em destinos com certificados confiáveis. A configuração padrão é desmarcada. Para dispositivos supervisionados executando iOS 11 (versão mínima).

- **Adicionar configurações de VPN:** Se esta restrição for definida como **Desativado**, os usuários não podem criar configurações de VPN. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Modificar configurações de plano de celular:** Se esta restrição for definida como **Desativado**, os usuários não podem modificar as configurações do plano de celular. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Remover aplicativos do sistema:** Se esta restrição for definida como **Desativado**, os usuários não podem remover aplicativos do sistema de seus dispositivos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Configurar novos dispositivos próximos:** Se esta restrição for definida como Desativado, os usuários não podem configurar novos dispositivos próximos. A configuração padrão é Ativado. Para dispositivos supervisionados executando iOS 11 (versão mínima).
- **Permitir modo restrito USB:** Se **Desativado**, o dispositivo pode sempre se conectar a acessórios USB enquanto bloqueado. O padrão é **Ativado**. Disponível apenas para dispositivos iOS 11.3 e posteriores supervisionados.
- **Forçar atualizações de software atrasadas:** Se **Ativado**, atrasa a visibilidade das Atualizações de Software para o usuário. Com esta restrição em vigor, o usuário não vê uma atualização de software até o número especificado de dias após a data de lançamento da atualização de software. O padrão é **Desativado**. Disponível apenas para dispositivos iOS 11.3 e posteriores supervisionados.

- **Atraso forçado de atualização de software (dias):** Permite especificar o número de dias para atrasar uma atualização de software no dispositivo. O atraso máximo é de **90** dias. O padrão é **30** dias. Disponível apenas para dispositivos iOS 11.3 e posteriores supervisionados.
- **Forçar solicitação de permissão do Classroom para sair das aulas:** Se **Ativado**, um aluno matriculado em um curso não gerenciado com o Classroom deve solicitar permissão ao professor ao tentar sair do curso. O padrão é **Desativado**. Disponível apenas para dispositivos iOS 11.3 e posteriores supervisionados.
- **Forçar autenticação antes do preenchimento automático:** Se **Ativado**, o usuário precisa autenticar antes que o sistema possa preencher automaticamente senhas ou informações de cartão de crédito no Safari e em aplicativos. Suportado apenas em dispositivos com Face ID ou Touch ID. O padrão é **Desativado**.
- **Forçar data e hora automáticas:** Permite definir automaticamente a data e a hora em dispositivos supervisionados. Se **Ativado**, os usuários do dispositivo não podem desativar **Definir Automaticamente** em **Geral > Data e Hora**. O fuso horário no dispositivo é atualizado apenas quando o dispositivo pode determinar sua localização. Ou seja, quando um dispositivo tem uma conexão celular ou uma conexão Wi-Fi com serviços de localização ativados. O padrão é **Desativado**. Disponível apenas para dispositivos iOS 12 e posteriores supervisionados.
- **Preenchimento Automático de Senhas:** Opcional. Se desativado, os usuários não podem usar os recursos de Preenchimento Automático de Senhas ou Senhas Fortes Automáticas. O padrão é **Ativado**. Disponível a partir do iOS 12.
- **Solicitações de proximidade de senha:** Opcional. Se desativado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do iOS 12.
- **Compartilhamento de Senhas:** Opcional. Se desativado, os usuários não podem compartilhar suas senhas usando o recurso Senhas do AirDrop. O padrão é **Ativado**. Disponível a partir do iOS 12.
- **Modificar configurações de Hotspot pessoal:** Desativa modificações na configuração de hotspot pessoal quando ela está **Desativada**. O padrão é **Ativado**.
- **Permitir inicialização em recuperação por um dispositivo não emparelhado:** Se **Ativado**, permite que os dispositivos sejam inicializados em recuperação por um dispositivo não emparelhado. O padrão é **Desativado**. Disponível para iOS 14.5 ou posterior.

- **Instalar resposta de segurança rápida:** Se **Desativado**, proíbe a instalação de respostas de segurança rápidas. O padrão é **Ativado**.
- **Remover resposta de segurança rápida:** Se **Desativado**, proíbe a remoção de respostas de segurança rápidas. O padrão é **Ativado**.
- **Permitir proteção de privacidade de e-mail:** Se **Desativado**, desativa a Proteção de Privacidade de E-mail no dispositivo. O padrão é **Ativado**. Disponível para iOS 15.2 ou posterior.
- **NFC:** Se **Desativado**, desativa o NFC. O padrão é **Ativado**. Disponível para iOS 14.2 ou posterior.
- **Permitir App Clips**: Se **Desativado**, impede que um usuário adicione qualquer App Clip e remove quaisquer App Clips existentes no dispositivo. O padrão é **Ativado**. Disponível para iOS 14.0 ou posterior.
- **Genmoji:** Se **Desativado**, proíbe a criação de novos Genmoji. Disponível para iOS 18 ou posterior.
- **Image Playground:** Se **Desativado**, proíbe o uso da geração de imagens. Disponível para iOS 18 ou posterior.
- **Image Wand:** Se **Desativado**, proíbe o uso do Image Wand. Disponível para iOS 18 ou posterior.
- **Espelhamento do iPhone:** Se **Desativado**, proíbe o uso do Espelhamento do iPhone. Quando usado no iOS, isso impede que o iPhone espelhe para qualquer Mac. Disponível para iOS 18 ou posterior.
- **Resultados de Escrita Personalizada:** Se **Desativado**, impede que o sistema gere texto com a caligrafia do usuário. Disponível para iOS 18 ou posterior.
- **Ferramentas de Escrita:** Se **Desativado**, desabilita as ferramentas de escrita do Apple Intelligence. Disponível para iOS 18 ou posterior.
- **Gravação de Chamadas:** Se **Desativado**, desabilita a gravação de chamadas. Requer um dispositivo supervisionado. Disponível para iOS 18.1 ou posterior.
- **Aplicativos a Serem Ocultados:** Se **Desativado**, proíbe a capacidade do usuário de ocultar aplicativos. Quando usado no iOS, isso impede que o usuário oculte aplicativos, mas ainda permite que ele os deixe na Biblioteca de Aplicativos enquanto os remove da tela inicial. Requer um dispositivo supervisionado. Disponível para iOS 18 ou posterior.
- **Aplicativos a Serem Bloqueados:** Se **Desativado**, proíbe a capacidade do usuário de bloquear aplicativos. Quando usado no iOS, isso impede que o usuário bloqueie aplicativos

e, como resultado, também impede a ocultação de aplicativos. Requer um dispositivo supervisionado. Disponível para iOS 18 ou posterior.

- **Resumo de E-mail:** Se **Desativado**, proíbe a capacidade de criar manualmente resumos de mensagens de e-mail. Quando usado no iOS, isso não afeta a geração automática de resumos. Requer um dispositivo supervisionado. Disponível para iOS 18.1 ou posterior.
- **Mensagens RCS:** Se **Desativado**, impede o uso de mensagens RCS. Requer um dispositivo supervisionado. Disponível para iOS 18.1 ou posterior.
- **Permitir integrações de inteligência externa:** Se **Desativado**, desabilita o uso de serviços de inteligência externos baseados em nuvem com a Siri. O padrão é **Ativado**. Disponível para iOS 18.2 e posterior.
- **Permitir login em integrações de inteligência externa:** Se **Desativado**, força os provedores de inteligência externa para o modo anônimo. Se um usuário já estiver logado em um provedor de inteligência externa, a aplicação desta restrição fará com que ele seja desconectado na próxima tentativa de solicitação. O padrão é **Ativado**. Disponível para iOS 18.2 e posterior.
- **Permitir Respostas Inteligentes no Mail:** Se **Desativado**, desabilita as respostas inteligentes no Mail. O padrão é **Ativado**. Disponível para iOS 18.2 e posterior.
- **Permitir Transcrição de Notas:** Se **Desativado**, desabilita a transcrição em Notas. O padrão é **Ativado**. Disponível para iOS 18.2 e posterior.
- **Permitir Resumo do Safari:** Se **Desativado**, o sistema desabilita a capacidade de resumir conteúdo no Safari. O padrão é **Ativado**. Disponível para iOS 18.4 e posterior.
- **Permitir resumo de inteligência visual:** Se **Desativado**, o sistema desabilita o resumo de inteligência visual. O padrão é **Ativado**. Disponível para iOS 18.3 e posterior.
- **Permitir Resumo de Transcrição de Notas:** Se **Desativado**, desabilita o resumo de transcrição em Notas. O padrão é **Ativado**. Disponível para iOS 18.3 e posterior.
- **Permitir Relatório de Inteligência da Apple:** Se **Desativado**, o sistema desabilita os relatórios de Inteligência da Apple. O padrão é **Ativado**. Disponível para iOS 18.4 e posterior.
- **Permitir Modificação do Aplicativo de Chamada Padrão:** Se **Desativado**, desabilita a modificação da preferência do aplicativo de chamada padrão. O comando de Configurações MDM para definir a preferência do aplicativo de chamada padrão ainda funciona quando isso é aplicado. O padrão é **Ativado**. Disponível para iOS 18.4 e posterior.

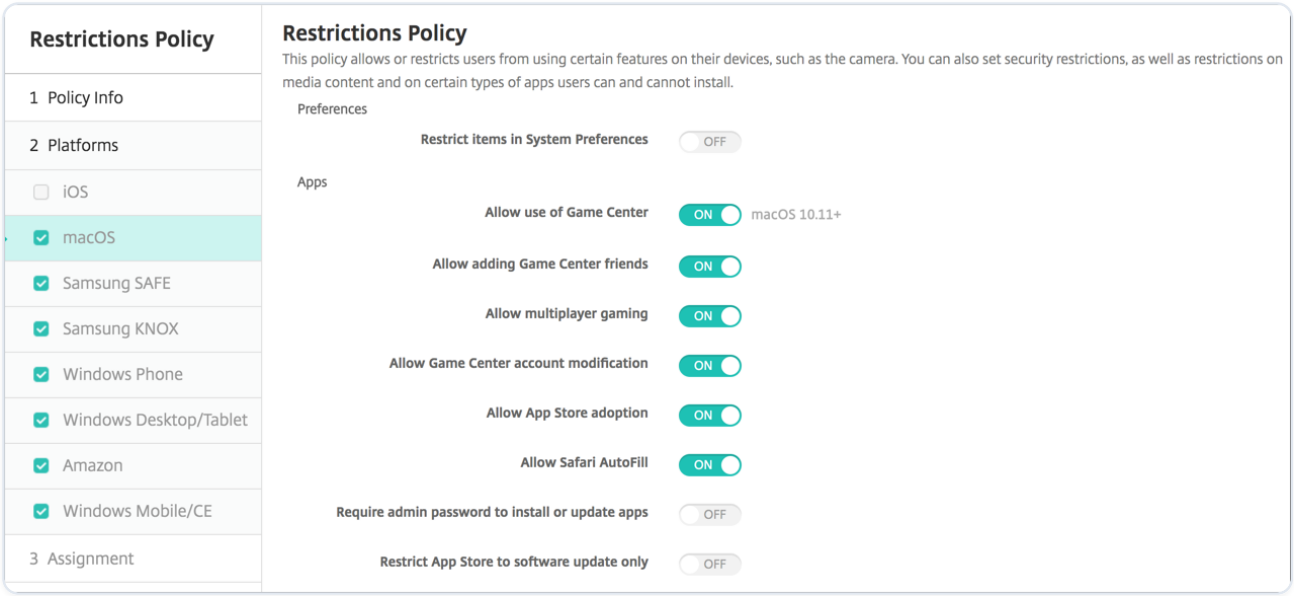
- **Permitir Modificação do Aplicativo de Mensagens Padrão:** Se **Desativado**, desabilita a modificação da preferência do aplicativo de mensagens padrão. O comando de Configurações MDM para definir a preferência do aplicativo de mensagens padrão ainda funciona quando isso é aplicado. O padrão é **Ativado**. Disponível para iOS 18.4 e posterior.
- **Permitir IDs de Espaço de Trabalho de Inteligência Externa:** Um array de strings, mas atualmente restrito a um único elemento. Se presente, a Inteligência da Apple permite apenas que o ID do espaço de trabalho de integração externa fornecido seja usado e exige um login para fazer solicitações; o usuário será obrigado a fazer login em integrações que suportam login. Múltiplas cargas úteis se combinam usando uma operação de interseção. Isso significa que o conjunto permitido de IDs de espaço de trabalho pode se tornar o conjunto vazio se valores conflitantes forem especificados em múltiplas cargas úteis. Disponível para iOS 18.3 e posterior.
  - **ID do Espaço de Trabalho de Inteligência Externa:** Para adicionar um ID de espaço de trabalho de inteligência externa, clique em **Adicionar**, digite um **ID do Espaço de Trabalho de Inteligência Externa** e clique em **Salvar**. Repita esse processo para cada ID de espaço de trabalho que você deseja adicionar.
- **Modificação do Navegador Padrão:** Se **Desativado**, proíbe a modificação da preferência do navegador padrão. Quando usado no iOS, isso ainda permite que o comando de Configurações MDM defina a preferência do navegador padrão. Requer um dispositivo supervisionado. Disponível para iOS 18.2 ou posterior.
- **Permitir Correio de Voz ao Vivo:** Se **Desativado**, o sistema desabilita o correio de voz ao vivo no dispositivo. O padrão é **Ativado**. Disponível para iOS 17.2 e posterior.

- **Segurança - Mostrar na tela de bloqueio**
  - **Central de Controle:** Permitir acesso à Central de Controle na tela de bloqueio. A Central de Controle permite que os usuários modifiquem facilmente as configurações de Modo Avião, Wi-Fi, Bluetooth, Modo Não Perturbe e Rotação de Bloqueio.
  - **Notificação:** Permitir notificações na tela de bloqueio.
  - **Visualização Hoje:** Permitir a Visualização Hoje, que agrega informações como o clima e os itens da agenda do dia atual, na tela de bloqueio.
- **Conteúdo de mídia - Permitir**
  - **Música explícita, podcasts e material do iTunes U:** Permitir material explícito nos dispositivos dos usuários.

- **Conteúdo sexual explícito no iBooks:** Permitir que material explícito seja baixado do iBooks.
- **Região de classificações:** Defina a região de onde as classificações de controle parental são obtidas. Na lista, clique em um país para definir a região de classificações. O padrão é **Estados Unidos**.
- **Filmes:** Defina se filmes são permitidos nos dispositivos dos usuários. Se filmes forem permitidos, opcionalmente defina o nível de classificação para filmes. Na lista, clique em uma opção para permitir ou restringir filmes no dispositivo. O padrão é Permitir todos os filmes.
- **Programas de TV:** Defina se programas de TV são permitidos nos dispositivos dos usuários. Se programas de TV forem permitidos, opcionalmente defina o nível de classificação para programas de TV. Na lista, clique em uma opção para permitir ou restringir programas de TV no dispositivo. O padrão é Permitir todos os programas de TV.
- **Aplicativos:** Defina se aplicativos são permitidos nos dispositivos dos usuários. Se aplicativos forem permitidos, opcionalmente defina o nível de classificação para aplicativos. Na lista, clique em uma opção para permitir ou restringir aplicativos no dispositivo. O padrão é Permitir todos os aplicativos.

- **Configurações de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
  - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no iOS 9.3 e posterior.

Configurações do macOS



- **Preferências**
  - **Restringir itens em Preferências do Sistema:** Permite ou restringe o acesso do usuário às Preferências do Sistema. O padrão é **Desativado**, o que permite aos usuários acesso total às Preferências do Sistema. Se ativado, configure as seguintes configurações.
    - **Painel de Preferências do Sistema:** Selecione se as configurações que você selecionar estão ativadas ou desativadas. O padrão é ativar todas as configurações, que estão **Ativadas** por padrão.
      - Usuários e Grupos
      - Geral
      - Acessibilidade
      - App Store
      - Atualização de Software
      - Bluetooth
      - CDs e DVDs
      - Data e Hora
      - Mesa e Protetor de Tela
      - Monitores
      - Dock
      - Economia de Energia

    - Extensões
    - FibreChannel
    - iCloud
    - Tinta
    - Contas de Internet
    - Teclado
    - Idioma e Texto
    - Mission Control
    - Mouse
    - Rede
    - Notificações
    - Controles Parentais
    - Impressoras e Scanners
    - Perfis
    - Segurança e Privacidade
    - Compartilhamento
    - Som
    - Dicção e Fala
    - Spotlight
    - Disco de Inicialização
    - Time Machine
    - Trackpad
    - Xsan

- **Aplicativos**
    - **Permitir o uso do Game Center:** Permite que os usuários joguem online através do Game Center. O padrão é **Ativado**.
    - **Permitir adicionar amigos no Game Center:** Permite que os usuários enviem uma notificação a um amigo para jogar. O padrão é **Ativado**.
    - **Permitir jogos multiplayer:** Permite que os usuários iniciem jogos multiplayer. O padrão é **Ativado**.

- **Permitir modificação da conta do Game Center:** Permite que os usuários modifiquem as configurações da conta do Game Center. O padrão é **Ativado**.
- **Permitir adoção da App Store:** Permite ou restringe que a App Store adote aplicativos que já existem no OS X. O padrão é **Ativado**.
- **Permitir Preenchimento Automático do Safari:** Permite que o Safari preencha automaticamente campos em sites com senhas, endereços e outras informações básicas que ele armazenou. O padrão é **Ativado**.
- **Exigir senha de administrador para instalar ou atualizar aplicativos:** Exige uma senha de administrador para instalar ou atualizar aplicativos. O padrão é **Desativado**, o que significa que nenhuma senha de administrador é necessária.
- **Restringir a App Store apenas para atualização de software:** Restringe a App Store apenas a atualizações, o que desativa todas as abas na App Store, exceto Atualizações. O padrão é **Desativado**, o que permite acesso total à App Store.
- **Restringir quais aplicativos podem ser abertos:** Restringe ou permite os aplicativos que os usuários podem usar. O padrão é DESATIVADO, o que permite que todos os aplicativos sejam usados. Se ativado, configure as seguintes configurações:
  - **Aplicativos Permitidos:** Clique em **Adicionar**, insira o nome e o ID do pacote para um aplicativo permitido para iniciar e, em seguida, clique em **Salvar**. Repita esta etapa para cada aplicativo permitido para iniciar.
  - **Pastas Não Permitidas:** Clique em **Adicionar**, digite o caminho do arquivo para uma pasta à qual você deseja restringir o acesso do usuário (por exemplo, /Applications/Utilities) e, em seguida, clique em **Salvar**. Repita esta etapa para todas as pastas às quais você não deseja que os usuários acessem.
  - **Pastas Permitidas:** Clique em **Adicionar**, digite o caminho do arquivo para uma pasta à qual você deseja conceder acesso ao usuário e, em seguida, clique em **Salvar**. Repita esta etapa para todas as pastas às quais você deseja que os usuários acessem.

- **Widgets**
  - **Permitir que apenas os seguintes widgets do Dashboard sejam executados:** Permite ou restringe quais widgets do Dashboard, como Relógio Mundial ou Calculadora, os usuários podem executar. O padrão é **Desativado**, o que permite que os usuários executem todos os widgets. Se ativado, configure a seguinte configuração:

    - **Widgets Permitidos:** Clique em **Adicionar**, digite o nome e o ID de um widget que pode ser executado e, em seguida, clique em **Salvar**. Repita esta etapa para cada widget que você deseja executar no Dashboard.

- **Mídia**
    - **Permitir AirDrop:** Permite que os usuários compartilhem fotos, vídeos, sites, localizações e muito mais com dispositivos iOS próximos.
- **Compartilhamento**
    - **Ativar automaticamente novos serviços de compartilhamento:** Selecione se deseja ativar automaticamente os serviços de compartilhamento.
    - **E-mail:** Selecione se deseja permitir uma caixa de correio compartilhada.
    - **Facebook:** Selecione se deseja permitir uma conta do Facebook compartilhada.
    - **Serviços de Vídeo - Flickr, Vimeo, Tudou e Youku:** Selecione se deseja permitir serviços de vídeo compartilhados.
    - **Adicionar ao Aperture:** Selecione se deseja permitir a capacidade compartilhada de adicionar ao Aperture.
    - **Sina Weibo:** Selecione se deseja permitir uma conta de microblogging compartilhada do Sina Weibo.
    - **Twitter:** Selecione se deseja permitir uma conta compartilhada do Twitter.
    - **Mensagens:** Selecione se deseja permitir acesso compartilhado a mensagens.
    - **Adicionar ao iPhoto:** Selecione se deseja permitir a capacidade compartilhada de adicionar ao iPhoto.
    - **Adicionar à Lista de Leitura:** Selecione se deseja permitir a capacidade compartilhada de adicionar à Lista de Leitura.
    - **AirDrop:** Selecione se deseja permitir uma conta compartilhada do AirDrop.
- **Funcionalidade**
    - **Bloquear imagem da área de trabalho:** Selecione se os usuários podem alterar a imagem da área de trabalho. O padrão é **Desativado**, o que significa que os usuários podem alterar a imagem da área de trabalho.
    - **Permitir uso da câmera:** Selecione se os usuários podem usar a câmera em seus Macs. O padrão é **Desativado**, o que significa que os usuários não podem usar a câmera.

- **Permitir Apple Music:** Permite que os usuários usem o serviço Apple Music (macOS 10.12 e posterior). Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássico. Aplica-se apenas a dispositivos supervisionados. O padrão é **Ativado**.
- **Permitir Sugestões do Spotlight:** Selecione se os usuários podem usar as Sugestões do Spotlight para pesquisar em seus Macs e para fornecer Sugestões do Spotlight da Internet, iTunes e App Store. O padrão é **Desativado**, o que impede os usuários de usar as Sugestões do Spotlight.
- **Permitir Pesquisa:** Selecione se os usuários podem pesquisar as definições de palavras com o menu de contexto ou o menu de pesquisa do Spotlight. O padrão é DESATIVADO, o que impede os usuários de usar a Pesquisa em seus Macs.
- **Permitir uso da senha do iCloud para contas locais:** Selecione se os usuários podem usar seu ID Apple e senha do iCloud para fazer login em seus Macs. A ativação desta política significa que os usuários usam apenas um ID e senha para *todas* as telas de login em seus Macs. O padrão é **Ativado**, o que permite aos usuários usar seu ID Apple e senha do iCloud para acessar seus Macs.
- **Permitir documentos e dados do iCloud:** Selecione se deseja permitir que os usuários acessem documentos e dados armazenados no iCloud em seus Macs. O padrão é **Desativado**, o que impede os usuários de usar documentos e dados do iCloud em seus Macs.
    - **Permitir iCloud Desktop e Documentos:** (macOS 10.12.4 e posterior) O padrão é selecionado.
- **Permitir Sincronização do Chaveiro do iCloud:** Permitir a sincronização do Chaveiro do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir iCloud Mail:** Permitir que os usuários usem o iCloud Mail (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Contatos do iCloud:** Permitir que os usuários usem os Contatos do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Calendários do iCloud:** Permitir que os usuários usem os Calendários do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Lembretes do iCloud:** Permitir que os usuários usem os Lembretes do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Favoritos do iCloud:** Permitir que os usuários sincronizem com os Favoritos do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.

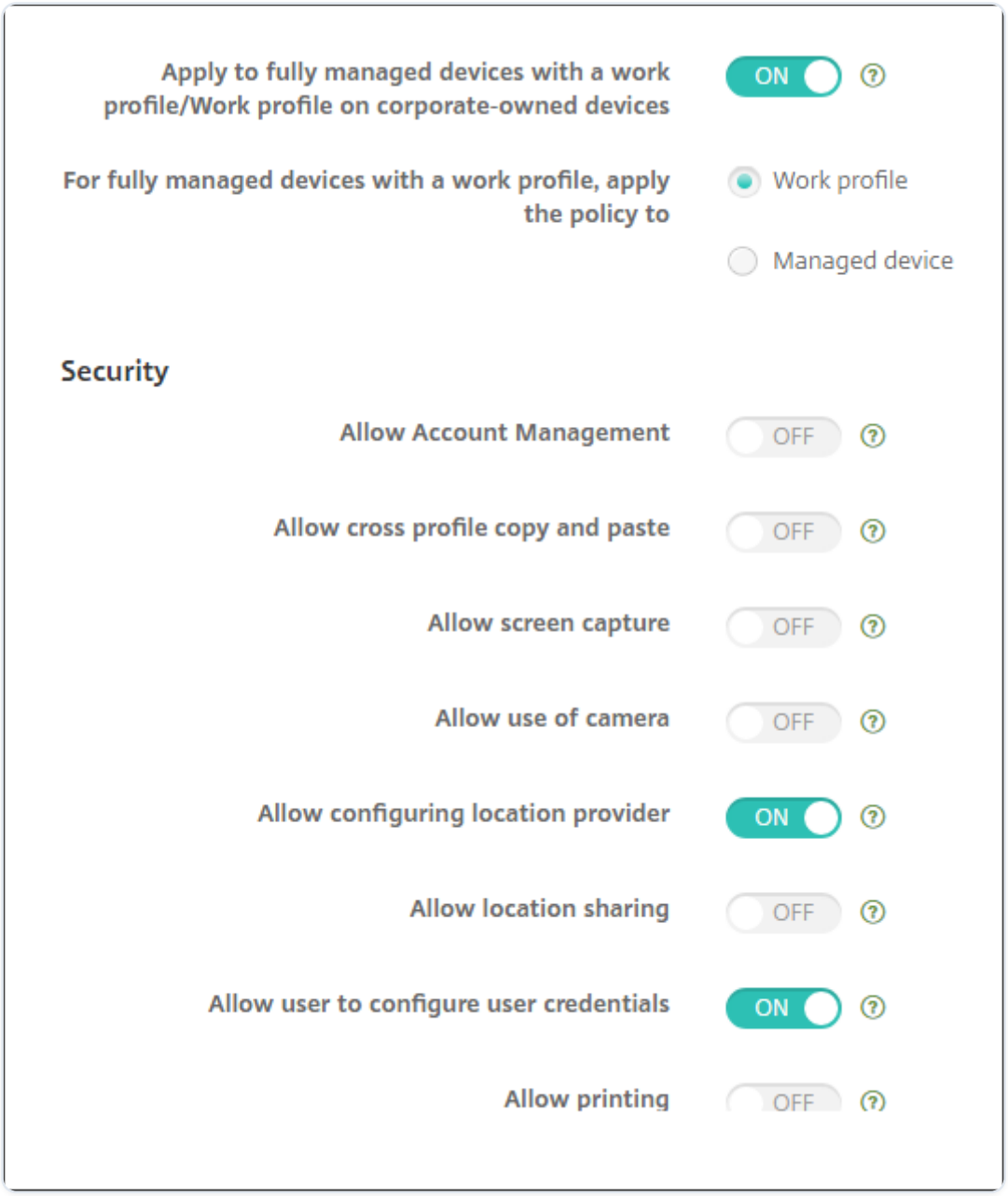
- **Permitir Notas do iCloud:** Permitir que os usuários usem as Notas do iCloud (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Fotos do iCloud:** Se você alterar esta configuração para **Desativado**, todas as fotos não totalmente baixadas da Biblioteca de Fotos do iCloud serão removidas do armazenamento local do dispositivo (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Desbloqueio Automático:** Para obter informações sobre esta opção e o Apple Watch, consulte https://www.imore.com/auto-unlock (macOS 10.12 e posterior). O padrão é **Ativado**.
- **Permitir Touch ID para Desbloquear Mac:** (macOS 10.12.4 e posterior). O padrão é **Ativado**.
- **Forçar atualizações de software atrasadas:** Se **Ativado**, esta configuração atrasa a visibilidade das Atualizações de Software para o usuário. Os usuários não veem uma atualização de software até o número especificado de dias após a data de lançamento da atualização de software. O padrão é **Desativado**. Disponível apenas para dispositivos supervisionados executando macOS 10.13.4 e posterior.
- **Atraso forçado da atualização de software (dias):** Especifica quantos dias atrasar uma atualização de software no dispositivo. O máximo é 90 dias. O padrão é **30**. Disponível apenas para dispositivos supervisionados executando macOS 10.13.4 e posterior.
- **Preenchimento Automático de Senhas:** Opcional. Se desativado, os usuários não podem usar os recursos de Preenchimento Automático de Senhas ou Senhas Fortes Automáticas. O padrão é **Ativado**. Disponível a partir do macOS 10.14.
- **Solicitações de proximidade de senha:** Opcional. Se desativado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do macOS 10.14.
- **Compartilhamento de Senhas:** Opcional. Se desativado, os usuários não podem compartilhar suas senhas usando o recurso Senhas do AirDrop. O padrão é **Ativado**. Disponível a partir do macOS 10.14.
- **Image Playground:** Se **Desativado**, proíbe o uso da geração de imagens. O padrão é **Ativado**. Disponível apenas para dispositivos supervisionados executando macOS 15 e posterior.
- **Espelhamento de iPhone:** Se **Desativado**, proíbe o uso do Espelhamento de iPhone. Quando usado no macOS, isso impede que o Mac espelhe qualquer iPhone. O padrão é **Ativado**. Disponível apenas para dispositivos supervisionados executando macOS 15 e posterior.

- **Ferramentas de Escrita:** Se **Desativado**, desativa as ferramentas de escrita do Apple Intelligence. O padrão é **Ativado**. Disponível apenas para dispositivos supervisionados executando macOS 15 e posterior.
- **Permitir Modificação de Compartilhamento de Mídia:** Se **Desativado**, impede a modificação das configurações de Compartilhamento de Mídia. O padrão é **Ativado**. Disponível para macOS 15.1 e posterior.
- **Forçar Ignorar Alerta de Captura de Tela:** Se **Ativado**, ignora a apresentação de um alerta de captura de tela. O padrão é **Desativado**. Disponível para macOS 15.1 e posterior.
- **Resumo de E-mail:** Se **Desativado**, desativa a capacidade de criar resumos de mensagens de e-mail manualmente. Isso não afeta a geração automática de resumos. O padrão é **Ativado**. Disponível para macOS 15.1 ou posterior.

Configurações do Android

- **Câmera:** Permite que os usuários usem a câmera em seus dispositivos. Se **Desativado**, a câmera é desativada. O padrão é **Ativado**.

Configurações do Android Enterprise



Quando um dispositivo Android novo ou redefinido de fábrica se registra no modo de perfil de trabalho, os dispositivos que executam Android 9.0-10.x se registram como dispositivos totalmente gerenciados com um perfil de trabalho. Os dispositivos que executam Android 11+ se registram como perfil de trabalho em dispositivos de propriedade corporativa. A política de restrição pode ser aplicada ao perfil de trabalho no dispositivo ou ao dispositivo gerenciado.

Em dispositivos registrados no modo de perfil de trabalho em dispositivos de propriedade corporativa, as seguintes restrições estão disponíveis apenas para o perfil de trabalho:

- Permitir serviço de backup
- Habilitar aplicativos do sistema

- Impedir que o bloqueio de tela bloqueie o dispositivo
- Permitir o uso da barra de status
- Manter a tela do dispositivo ligada
- Permitir que o usuário controle as configurações do aplicativo
- Permitir que o usuário configure as credenciais do usuário
- Permitir configuração de VPN
- Permitir armazenamento em massa USB
- Permitir redefinição de fábrica
- Permitir desinstalação de aplicativo
- Acessar aplicativo de e-mail de perfis de trabalho e pessoal
- Permitir aplicativos que não são do Google Play
- Permitir copiar e colar entre perfis
- Habilitar verificação de aplicativo
- Permitir gerenciamento de conta
- Permitir impressão
- Permitir NFC
- Permitir adicionar usuários

Por padrão, as configurações de **Depuração USB e Fontes Desconhecidas** são desabilitadas em um dispositivo quando ele é registrado no Android Enterprise no modo de perfil de trabalho.

Para dispositivos que executam Android 9.0-10.x e Samsung Knox 3.0 ou posterior, configure as configurações para Samsung Knox e Samsung SAFE na página **Android Enterprise**. Para dispositivos que executam versões anteriores do Android ou Samsung Knox, use as páginas **Samsung Knox** e **Samsung SAFE**.

As restrições da Samsung não se aplicam a dispositivos registrados no perfil de trabalho no modo de dispositivos de propriedade corporativa. Use o Knox Service Plugin (KSP) para aplicar restrições da Samsung a esses dispositivos. Para obter mais informações, consulte a documentação da Samsung.

Recomendamos que você use o Samsung Knox 3.4 ou superior para os recursos de gerenciamento mais recentes do Samsung Knox.

- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa:** Permite que as configurações da política de restrições sejam configuradas para dispositivos totalmente gerenciados com perfis de trabalho. Quando esta configuração está **Ativada**, selecione uma destas configurações:
  - **Perfil de trabalho:** As configurações de restrições que você configura se aplicam apenas ao perfil de trabalho no dispositivo.
  - **Gerenciar dispositivo:** As configurações de restrições que você configura se aplicam apenas ao dispositivo.

  Quando esta configuração está **Desativada**, as configurações de credenciais que você configura se aplicam ao dispositivo, exceto para configurações que se aplicam explicitamente ao perfil de trabalho. O padrão é **Desativado**.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa** estiver desativado, configure estas configurações:

- **Segurança**
  - **Permitir gerenciamento de conta:** Permite que uma conta seja adicionada no perfil de trabalho e em dispositivos gerenciados. O padrão é **Desativado**.
  - **Permitir copiar e colar entre perfis:** Se **Ativado**, os usuários podem copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
  - **Permitir captura de tela:** Permite que os usuários gravem ou capturem a tela do dispositivo. O padrão é **Desativado**.
  - **Permitir o uso da câmera:** Permite que os usuários tirem fotos e gravem vídeos com a câmera do dispositivo. O padrão é **Desativado**.
  - **Permitir configuração de VPN:** Permite que os usuários criem configurações de VPN. Para dispositivos com perfil de trabalho executando Android 6 e posterior e para dispositivos totalmente gerenciados. O padrão é **Ativado**.
  - **Permitir serviço de backup:** Permite que os usuários façam backup de dados de aplicativos e do sistema em seus dispositivos. O padrão é **Ativado**.
  - **Permitir NFC:** Permite que os usuários enviem páginas da web, fotos, vídeos ou outro conteúdo de seus dispositivos para outro dispositivo usando Near Field Communication (NFC). Para MDM 4.0 e posterior. O padrão é **Ativado**.

- **Permitir configuração do provedor de localização:** Permite que os usuários ativem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.
- **Permitir compartilhamento de localização:** Para perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.

> **Dica:**
>
> Você pode criar políticas de dispositivo de Localização no XenMobile para impor limites geográficos. Consulte Política de dispositivo de Localização.

- **Permitir que o usuário configure credenciais de usuário:** Especifique se os usuários podem configurar credenciais no keystore gerenciado. O padrão é **Ativado**.
- **Permitir impressão:** Se **Ativado**, a configuração permite que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Desativado**. Disponível para: Android 9 e posterior.
- **Permitir depuração USB:** O padrão é **Desativado**.

- **Aplicativos**
  - **Habilitar aplicativos do sistema:** Permite que os usuários executem aplicativos pré-instalados do dispositivo. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.
    - **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que você deseja habilitar no dispositivo. Defina **Habilitar aplicativos do sistema** como **Ativado** e adicione o nome do pacote do aplicativo. Para pesquisar o nome do pacote de um aplicativo do sistema, você pode usar o Android Debug Bridge (`adb`) para chamar o comando do gerenciador de pacotes do Android (`pm`). Por exemplo, `adb shell "pm list packages -f name"`, onde "name" faz parte do nome do pacote. Para obter mais informações, consulte `<https://developer.android.com/studio/command-line/adb>`. Para dispositivos Android Enterprise, você pode restringir as permissões de aplicativos usando a política Permissões de aplicativos do Android Enterprise.
  - **Desabilitar aplicativos:** Bloqueia uma lista especificada de aplicativos de serem executados em dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e, em seguida, clique em **Adicionar** na tabela **Lista de aplicativos**.

    - **Lista de aplicativos:** Uma lista dos aplicativos que você deseja bloquear. Defina **Desabilitar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos substitui a lista de aplicativos anterior. Por exemplo: Se você desabilitar com.example1 e com.example2, e depois alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example.2.

  - **Habilitar verificação de aplicativo:** Permite que o SO verifique aplicativos para detectar comportamento malicioso. O padrão é **Ativado**.
  - **Habilitar aplicativos Google:** Permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
  - **Permitir aplicativos fora da Google Play:** Permite a instalação de aplicativos de lojas que não sejam a Google Play. O padrão é **Desativado**.
  - **Permitir controle do usuário sobre as configurações do aplicativo:** Permite que os usuários desinstalem aplicativos, desabilitem aplicativos, limpem cache e dados, forcem a parada de qualquer aplicativo e limpem os padrões. Os usuários realizam essas ações a partir do aplicativo Configurações. O padrão é **Desativado**.
  - **Permitir desinstalação de aplicativo:** Permite que os usuários desinstalem aplicativos da Managed Google Play Store. O padrão é **Desativado**. Para exibir esta configuração, habilite a propriedade do servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.
  - **Acessar aplicativo de e-mail de perfis de trabalho e pessoal**: Permite que os usuários acessem e usem o aplicativo de e-mail do perfil de trabalho a partir do seu perfil pessoal quando a configuração estiver **Ativada**. O padrão é **Desativado**.

- **Perfil de trabalho BYOD**

  - **Permitir widgets de aplicativos do perfil de trabalho na tela inicial:** Se esta configuração estiver **Ativada**, os usuários podem colocar widgets de aplicativos do perfil de trabalho na tela inicial do dispositivo. Se esta configuração estiver **Desativada**, os usuários não podem colocar widgets de aplicativos do perfil de trabalho na tela inicial do dispositivo. O padrão é **Desativado**.

    - **Aplicativos com widgets permitidos:** Uma lista dos aplicativos que você deseja permitir na tela inicial. Defina **Permitir widgets de aplicativos do perfil de trabalho na tela inicial** como **Ativado** e adicione o aplicativo. Clique em **Adicionar** e selecione um aplicativo cujos widgets você deseja permitir na tela inicial da lista. Clique em **Salvar**. Repita esse processo para permitir mais widgets de aplicativos.

- **Permitir contatos do perfil de trabalho nos contatos do dispositivo:** Mostra contatos do perfil gerenciado do Android Enterprise no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O padrão é **Desativado**.

- **Somente dispositivo totalmente gerenciado**
  - **Permitir adicionar usuários:** Permite que os usuários adicionem novos usuários em um dispositivo. O padrão é **Ativado**.
  - **Permitir roaming de dados:** Permite que os usuários usem dados celulares durante o roaming. O padrão é Desativado, o que desabilita o roaming nos dispositivos dos usuários. O padrão é **Desativado**.
  - **Permitir SMS:** Permite que os usuários enviem e recebam mensagens SMS. O padrão é **Desativado**.
  - **Permitir o uso da barra de status:** Se **Ativado**, esta configuração habilita a barra de status em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). Esta configuração desabilita notificações, configurações rápidas e outras sobreposições de tela que permitem sair do modo de tela cheia. Os usuários podem ir para as configurações do sistema e ver as notificações. Para Android 6.0 e posterior. O padrão é **Desativado**.
  - **Permitir Bluetooth:** Permite que os usuários usem o Bluetooth. O padrão é **Ativado**.
    - **Permitir compartilhamento Bluetooth:** Se não selecionado, os usuários não podem estabelecer compartilhamento Bluetooth de saída em seu dispositivo. O padrão é selecionado. Para exibir esta configuração, habilite a propriedade do servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.
  - **Permitir configuração de data e hora:** Permite que os usuários alterem a data e a hora em seus dispositivos. O padrão é **Ativado**.
  - **Permitir redefinição de fábrica:** Permite que os usuários façam uma redefinição de fábrica em seus dispositivos. O padrão é **Ativado**.
  - **Manter a tela do dispositivo ligada:** Se esta configuração estiver definida como **Ativado**, a tela do dispositivo permanece ligada quando o dispositivo está conectado. O padrão é **Desativado**.
  - **Permitir armazenamento em massa USB:** Permite a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador por meio de uma conexão USB. O padrão é **Ativado**.

- **Permitir microfone:** Permite que os usuários usem o microfone em seus dispositivos. O padrão é **Ativado**.
- **Permitir tethering:** Permite que os usuários configurem pontos de acesso portáteis e compartilhem dados. O padrão é **Desativado**.
- **Impedir que o bloqueio de tela bloqueie o dispositivo:** Se **Ativado**, esta configuração desabilita o bloqueio de tela na tela de bloqueio em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). O padrão é **Desativado**.
- **Permitir alterações de Wi-Fi:** Se **Ativado**, os usuários podem ligar ou desligar o Wi-Fi e conectar-se a redes Wi-Fi. O padrão é **Ativado**.
- **Permitir transferência de arquivos:** Permite transferências de arquivos via USB. O padrão é **Desativado**.

- **Samsung**
  - **Habilitar TIMA Keystore:** O TIMA Keystore fornece armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Pares de chaves RSA e certificados são roteados para o provedor de armazenamento de chaves padrão para armazenamento. O padrão é **Desativado**.
  - **Permitir lista de compartilhamento:** Permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
  - **Habilitar log de auditoria:** Habilita a criação de logs de auditoria de eventos para análise forense de um dispositivo. O padrão é **Desativado**.
- **Samsung: Somente dispositivo totalmente gerenciado**
  - **Habilitar verificação de inicialização confiável ODE:** Use a verificação de inicialização confiável ODE para estabelecer uma cadeia de confiança do bootloader à imagem do sistema. O padrão é **Ativado**.
  - **Permitir apenas chamadas de emergência:** Permite que os usuários ativem o modo Somente Chamada de Emergência em seus dispositivos. O padrão é **Desativado**.
  - **Permitir recuperação de firmware:** Permite que os usuários recuperem o firmware em seus dispositivos. O padrão é **Ativado**.
  - **Permitir criptografia rápida:** Permite a criptografia apenas do espaço de memória usado. Esta criptografia contrasta com a criptografia de disco completo, que criptografa todos os dados. Esses dados incluem configurações, dados de aplicativos, arquivos e aplicativos baixados, mídia e outros arquivos. O padrão é **Ativado**.

- **Habilitar modo Common Criteria:** Coloca um dispositivo no Modo Common Criteria. A configuração Common Criteria impõe processos de segurança rigorosos. O padrão é **Ativado**.
- **Habilitar banner de reinicialização:** Exibe uma mensagem de notificação ou banner de uso do sistema aprovado pelo DoD quando os dispositivos dos usuários são reiniciados. O padrão é **Desativado**.
- **Permitir alterações de configurações:** Permite que os usuários alterem as configurações em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Habilitar uso de dados em segundo plano:** Permite que os aplicativos sincronizem dados em segundo plano. para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Permitir área de transferência:** Permite que os usuários copiem dados para a área de transferência em seus dispositivos.
  - **Permitir compartilhamento da área de transferência:** Permite que os usuários compartilhem conteúdo da área de transferência entre seus dispositivos e um computador (MDM 4.0 e posterior).
- **Permitir tecla inicial:** Permite que os usuários usem a tecla **Home** em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Permitir localização simulada:** Permite que os usuários simulem sua localização GPS. Para dispositivos totalmente gerenciados. O padrão é **Desativado**.
- **NFC:** Permite que os usuários usem NFC em seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Permitir desligamento:** Permite que os usuários desliguem seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Permitir Wi-Fi Direct:** Permite que os usuários se conectem diretamente a outro dispositivo por meio de sua conexão Wi-Fi. O padrão é **Ativado**. Se **Ativado**, você deve habilitar a configuração **Permitir alterações de Wi-Fi**.
- **Permitir cartão SD:** Permite que os usuários usem um cartão SD, se disponível, com seus dispositivos. O padrão é **Ativado**.
- **Permitir armazenamento host USB:** Permite que os dispositivos dos usuários atuem como host USB quando um dispositivo USB se conecta a eles. Os dispositivos dos usuários então fornecem energia ao dispositivo USB. O padrão é **Ativado**.
- **Permitir discador de voz:** Permite que os usuários usem o discador de voz em seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**.

- **Permitir S Beam:** Permite que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir S Voice:** Permite que os usuários usem o assistente pessoal inteligente e o navegador de conhecimento em seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir tethering USB:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão USB. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
- **Permitir tethering Bluetooth:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão Bluetooth. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
  - **Permitir compartilhamento Bluetooth:** Se não selecionado, os usuários não podem estabelecer compartilhamento Bluetooth de saída em seu dispositivo. O padrão é selecionado. Para exibir esta configuração, habilite a propriedade de servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.
- **Permitir tethering Wi-Fi:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão Wi-Fi. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
- **Permitir MMS de entrada:** Permite que os usuários recebam mensagens MMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir MMS de saída:** Permite que os usuários enviem mensagens MMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir SMS de entrada:** Permite que os usuários recebam mensagens SMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir SMS de saída:** Permite que os usuários enviem mensagens SMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Configurar redes móveis:** Permite que os usuários usem sua conexão de dados celulares. O padrão é **Desativado**.
- **Limite diário (MB):** Insira o número de MB de dados móveis que os usuários podem usar por dia. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).
- **Limite semanal (MB):** Insira o número de MB de dados móveis que os usuários podem usar por semana. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).

- **Limite mensal (MB):** Insira o número de MB de dados móveis que os usuários podem usar por mês. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).
- **Permitir apenas conexões VPN seguras:** Permite que os usuários usem apenas conexões seguras (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir gravação de áudio:** Permite que os usuários gravem áudio com seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**. Se **Ativado**, você deve ativar a configuração **Permitir microfone**.
- **Permitir gravação de vídeo:** Permite que os usuários gravem vídeo com seus dispositivos (MDM 4.0 e posterior). O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir uso da câmera**.
- **Permitir mensagens push em roaming:** Permite que os usuários usem dados celulares para push. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.
- **Permitir sincronização automática em roaming:** Permite que os usuários usem dados celulares para sincronização. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.
- **Permitir chamadas de voz em roaming:** Permite que os usuários usem dados celulares para chamadas de voz. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.

- **Samsung: Contêiner Knox/Dispositivo totalmente gerenciado**
  - **Habilitar verificação de revogação:** Habilita a verificação de certificados revogados. O padrão é **Desativado**.
- **Samsung: Apenas contêiner Knox**
  - **Mover aplicativos para o contêiner:** Permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação multifator:** Os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação para contêiner:** Use um método de autenticação diferente do método usado para desbloquear o dispositivo para abrir o contêiner KNOX. O padrão é **Ativado**.
  - **Habilitar teclado seguro:** Força os usuários a usar um teclado seguro dentro do contêiner Knox. O padrão é **Ativado**.

- **Samsung: DeX**
  - **Habilitar Samsung DeX:** Permite que dispositivos compatíveis com Knox sejam executados no modo Samsung DeX. Requer Samsung Knox 3.1 (versão mínima). O padrão é **Ativado**. Para obter informações sobre os requisitos de dispositivo do Samsung DeX e como configurá-lo, consulte a documentação para desenvolvedores da Samsung.
    - **Permitir Ethernet somente no modo DeX:** Habilita o uso de Ethernet no modo Samsung DeX. Dados celulares, Wi-Fi e tethering (Wi-Fi, Bluetooth e USB) são restritos no modo DeX. O padrão é desmarcado.
    - **Carregar imagem do logotipo DeX:** Selecione esta configuração para especificar uma imagem .png a ser usada como ícone para o Samsung DeX.
    - **Tempo limite da tela DeX (segundos):** Especifique a quantidade de tempo ocioso, em segundos, após o qual a tela DeX é desligada. Para desativar o tempo limite, digite **0**. O padrão é **1200** segundos (20 minutos).
    - **Adicionar atalho de aplicativo no Samsung DeX:** Especifique um nome de pacote de aplicativo para adicionar um atalho para o aplicativo ao DeX. Para pesquisar um nome de pacote de aplicativo, vá ao Google Play e selecione o aplicativo. A URL inclui o nome do pacote: `https://play.google.com/store/apps/details?id=<package.name>`.
    - **Remover atalho de aplicativo no Samsung DeX:** Especifique um nome de pacote de aplicativo para remover um atalho do DeX. Vá ao Google Play para pesquisar nomes de pacotes de aplicativos.
    - **Pacotes de aplicativos a serem desabilitados no Samsung DeX:** Especifique uma lista separada por vírgulas dos pacotes de aplicativos que você deseja bloquear no modo Samsung DeX. Por exemplo: `"com.android.chrome", "com.google.android.gm"`.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** estiver ativado e **Para dispositivos totalmente gerenciados com um perfil de trabalho, aplicar a política a** estiver definido como **Perfil de trabalho**, configure estas definições:

- **Segurança**
  - **Permitir gerenciamento de conta:** Permite que uma conta seja adicionada no perfil de trabalho e em dispositivos gerenciados. O padrão é **Desativado**.

- **Permitir copiar e colar entre perfis:** Se **Ativado**, os usuários podem copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
- **Permitir captura de tela:** Permite que os usuários gravem ou tirem uma captura de tela do dispositivo. O padrão é **Desativado**.
- **Permitir o uso da câmera:** Permite que os usuários tirem fotos e gravem vídeos com a câmera do dispositivo. O padrão é **Desativado**.
- **Permitir a configuração do provedor de localização:** Permite que os usuários ativem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.
- **Permitir o compartilhamento de localização:** Para perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.

> **Dica:**
>
> Você pode criar políticas de dispositivo de Localização no XenMobile para impor limites geográficos. Consulte Política de dispositivo de localização.

- **Permitir que o usuário configure credenciais de usuário:** Especifique se os usuários podem configurar credenciais no keystore gerenciado. O padrão é **Ativado**.
- **Permitir impressão:** Se **Ativado**, a configuração permite que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Desativado**. Disponível para: Android 9 e posterior.

- **Aplicativos**
  - **Habilitar aplicativos do sistema:** Permite que os usuários executem aplicativos pré-instalados no dispositivo. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.
    - **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que você deseja habilitar no dispositivo. Defina **Habilitar aplicativos do sistema** como **Ativado** e adicione o nome do pacote do aplicativo. Para procurar o nome do pacote de um aplicativo do sistema, você pode usar o Android Debug Bridge (`adb`) para chamar o comando do gerenciador de pacotes do Android (`pm`). Por exemplo, `adb shell "pm list packages -f name"`, onde "name" faz parte do nome do pacote. Para obter mais informações, consulte `<https://developer.android.com/studio/command-`

`line/adb>`. Para dispositivos Android Enterprise, você pode restringir as permissões de aplicativos usando a política Permissões de aplicativos do Android Enterprise.

- **Desabilitar aplicativos:** Bloqueia uma lista especificada de aplicativos de serem executados em dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e clique em **Adicionar** na tabela **Lista de aplicativos**.
  - **Lista de aplicativos:** Uma lista dos aplicativos que você deseja bloquear. Defina **Desabilitar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: Se você desabilitar com.example1 e com.example2, e depois alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example.2.
- **Habilitar verificação de aplicativos:** Permite que o SO escaneie aplicativos para detectar comportamento malicioso. O padrão é **Ativado**.
- **Habilitar aplicativos do Google:** Permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
- **Permitir aplicativos fora da Google Play:** Permite a instalação de aplicativos de lojas que não sejam a Google Play. O padrão é **Desativado**.
- **Permitir controle do usuário sobre as configurações do aplicativo:** Permite que os usuários desinstalem aplicativos, desativem aplicativos, limpem cache e dados, forcem a parada de qualquer aplicativo e limpem os padrões. Os usuários realizam essas ações a partir do aplicativo Configurações. O padrão é **Desativado**.
- **Permitir desinstalação de aplicativo:** Permite que os usuários desinstalem aplicativos da Managed Google Play Store. O padrão é **Desativado**. Para exibir essa configuração, habilite a propriedade do servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.
- **Acessar aplicativo de e-mail de perfis de trabalho e pessoal:** Permite que os usuários acessem e usem o aplicativo de e-mail do perfil de trabalho a partir do seu perfil pessoal quando a configuração estiver **Ativada**. O padrão é **Desativado**.

- **Perfil de trabalho BYOD**
  - **Permitir widgets de aplicativos do perfil de trabalho na tela inicial:** Se esta configuração estiver **Ativada**, os usuários podem colocar widgets de aplicativos do perfil de trabalho na tela inicial do dispositivo. Se esta configuração estiver **Desativada**, os

usuários não podem colocar widgets de aplicativos do perfil de trabalho na tela inicial do dispositivo. O padrão é **Desativado**.

- **Aplicativos com widgets permitidos:** Uma lista dos aplicativos que você deseja permitir na tela inicial. Defina **Permitir widgets de aplicativos do perfil de trabalho na tela inicial** como **Ativado** e adicione o aplicativo. Clique em **Adicionar** e selecione um aplicativo cujos widgets você deseja permitir na tela inicial da lista. Clique em **Salvar**. Repita esse processo para permitir mais widgets de aplicativos.

- **Permitir contatos do perfil de trabalho nos contatos do dispositivo:** Exibe contatos do perfil gerenciado do Android Enterprise no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O padrão é **Desativado**.

- **Samsung**

  - **Habilitar TIMA Keystore:** O TIMA Keystore fornece armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Pares de chaves RSA e certificados são roteados para o provedor de armazenamento de chaves padrão para armazenamento. O padrão é **Desativado**.
  - **Permitir lista de compartilhamento:** Permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
  - **Habilitar log de auditoria:** Habilita a criação de logs de auditoria de eventos para análise forense de um dispositivo. O padrão é **Desativado**.

- **Samsung: Contêiner Knox/Dispositivo totalmente gerenciado**

  - **Habilitar verificação de revogação:** Habilita a verificação de certificados revogados. O padrão é **Desativado**.

- **Samsung: Somente contêiner Knox**

  - **Mover aplicativos para o contêiner:** Permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação multifator:** Os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação para contêiner:** Use um método de autenticação diferente do método usado para desbloquear o dispositivo para abrir o contêiner KNOX. O padrão é **Ativado**.
  - **Habilitar teclado seguro:** Força os usuários a usar um teclado seguro dentro do contêiner Knox. O padrão é **Ativado**.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** estiver ativado e **Para dispositivos totalmente gerenciados com um perfil de trabalho, aplicar a política a** estiver definido como **Dispositivo gerenciado**, configure estas definições:

- **Segurança**
  - **Permitir gerenciamento de conta:** Permite que uma conta seja adicionada no perfil de trabalho e em dispositivos gerenciados. O padrão é **Desativado**.
  - **Permitir copiar e colar entre perfis:** Se **Ativado**, os usuários podem copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
  - **Permitir captura de tela:** Permite que os usuários gravem ou capturem a tela do dispositivo. O padrão é **Desativado**.
  - **Permitir uso da câmera:** Permite que os usuários tirem fotos e gravem vídeos com a câmera do dispositivo. O padrão é **Desativado**.
  - **Permitir configuração de VPN:** Permite que os usuários criem configurações de VPN. Para dispositivos com perfil de trabalho executando Android 6 e posterior e para dispositivos totalmente gerenciados. O padrão é **Ativado**.
  - **Permitir serviço de backup:** Permite que os usuários façam backup de dados de aplicativos e do sistema em seus dispositivos. O padrão é **Ativado**.
  - **Permitir NFC:** Permite que os usuários enviem páginas da web, fotos, vídeos ou outro conteúdo de seus dispositivos para outro dispositivo usando Near Field Communication (NFC). Para MDM 4.0 e posterior. O padrão é **Ativado**.
  - **Permitir configuração do provedor de localização:** Permite que os usuários liguem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.
  - **Permitir compartilhamento de localização:** Para perfis gerenciados, o proprietário do dispositivo pode substituir esta configuração. O padrão é **Desativado**.

    > **Dica:**
    >
    > Você pode criar políticas de dispositivo de Localização no XenMobile para impor limites geográficos. Consulte Política de dispositivo de localização.

  - **Permitir que o usuário configure credenciais de usuário:** Especifique se os usuários podem configurar credenciais no keystore gerenciado. O padrão é **Ativado**.

- **Permitir impressão:** Se **Ativado**, a configuração permite que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Desativado**. Disponível para: Android 9 e posterior.
- **Permitir depuração USB:** O padrão é **Desativado**.

- **Aplicativos**
  - **Habilitar aplicativos do sistema:** Permite que os usuários executem aplicativos de dispositivo pré-instalados. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.
    - **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que você deseja habilitar no dispositivo. Defina **Habilitar aplicativos do sistema** como **Ativado** e adicione o nome do pacote do aplicativo. Para procurar o nome do pacote de um aplicativo do sistema, você pode usar o Android Debug Bridge (`adb`) para chamar o comando do gerenciador de pacotes do Android (`pm`). Por exemplo, `adb shell "pm list packages -f name"`, onde "nome" faz parte do nome do pacote. Para obter mais informações, consulte `<https://developer.android.com/studio/command-line/adb>`. Para dispositivos Android Enterprise, você pode restringir as permissões de aplicativos usando a política Permissões de aplicativos do Android Enterprise.
  - **Desabilitar aplicativos:** Bloqueia uma lista especificada de aplicativos de serem executados em dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e clique em **Adicionar** na tabela **Lista de aplicativos**.
    - **Lista de aplicativos:** Uma lista dos aplicativos que você deseja bloquear. Defina **Desabilitar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: Se você desabilitar com.example1 e com.example2, e depois alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example.2.
  - **Habilitar verificação de aplicativo:** Permite que o SO verifique aplicativos para detectar comportamento malicioso. O padrão é **Ativado**.
  - **Habilitar aplicativos do Google:** Permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
  - **Permitir aplicativos fora da Google Play:** Permite a instalação de aplicativos de lojas diferentes da Google Play. O padrão é **Desativado**.

- **Permitir controle do usuário sobre as configurações do aplicativo:** Permite que os usuários desinstalem aplicativos, desabilitem aplicativos, limpem cache e dados, forcem a parada de qualquer aplicativo e limpem os padrões. Os usuários realizam essas ações a partir do aplicativo Configurações. O padrão é **Desativado**.
- **Permitir desinstalação de aplicativo:** Permite que os usuários desinstalem aplicativos de dentro da Managed Google Play Store. O padrão é **Desativado**. Para exibir essa configuração, habilite a propriedade do servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.

- **Somente dispositivo totalmente gerenciado**
  - **Permitir adicionar usuários:** Permite que os usuários adicionem novos usuários em um dispositivo. O padrão é **Ativado**.
  - **Permitir roaming de dados:** Permite que os usuários usem dados de celular durante o roaming. O padrão é Desativado, o que desabilita o roaming nos dispositivos dos usuários. O padrão é **Desativado**.
  - **Permitir SMS:** Permite que os usuários enviem e recebam mensagens SMS. O padrão é **Desativado**.
  - **Permitir o uso da barra de status:** Se **Ativado**, esta configuração habilita a barra de status em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). Esta configuração desabilita notificações, configurações rápidas e outras sobreposições de tela que permitem sair do modo de tela cheia. Os usuários podem ir para as configurações do sistema e ver as notificações. Para Android 6.0 e posterior. O padrão é **Desativado**.
  - **Permitir Bluetooth:** Permite que os usuários usem Bluetooth. O padrão é **Ativado**.
    - **Permitir compartilhamento Bluetooth:** Se não selecionado, os usuários não podem estabelecer compartilhamento Bluetooth de saída em seu dispositivo. O padrão é selecionado. Para exibir esta configuração, habilite a propriedade do servidor `afw.restriction.policy.v2`. Para obter mais informações sobre as propriedades do servidor, consulte Propriedades do servidor.
  - **Permitir configurar data e hora:** Permite que os usuários alterem a data e a hora em seus dispositivos. O padrão é **Ativado**.
  - **Permitir redefinição de fábrica:** Permite que os usuários façam uma redefinição de fábrica em seus dispositivos. O padrão é **Ativado**.

- **Manter a tela do dispositivo ligada:** Se esta configuração estiver definida como **Ativado**, a tela do dispositivo permanece ligada quando o dispositivo está conectado. O padrão é **Desativado**.
- **Permitir armazenamento em massa USB:** Permite a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador por meio de uma conexão USB. O padrão é **Ativado**.
- **Permitir microfone:** Permite que os usuários usem o microfone em seus dispositivos. O padrão é **Ativado**.
- **Permitir tethering:** Permite que os usuários configurem hotspots portáteis e compartilhem dados. O padrão é **Desativado**. Quando esta configuração está ativada, estas configurações estão disponíveis para dispositivos Samsung:
- **Impedir que o keyguard bloqueie o dispositivo:** Se **Ativado**, esta configuração desabilita o keyguard na tela de bloqueio em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). O padrão é **Desativado**.
- **Permitir alterações de Wi-Fi:** Se **Ativado**, os usuários podem ligar ou desligar o Wi-Fi e conectar-se a redes Wi-Fi. O padrão é **Ativado**.
- **Permitir transferência de arquivos:** Permite transferências de arquivos via USB. O padrão é **Desativado**.

- **Samsung**
  - **Habilitar TIMA Keystore:** O TIMA Keystore fornece armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Os pares de chaves RSA e os certificados são roteados para o provedor de armazenamento de chaves padrão para armazenamento. O padrão é **Desativado**.
  - **Permitir lista de compartilhamento:** Permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
  - **Habilitar log de auditoria:** Permite a criação de logs de auditoria de eventos para análise forense de um dispositivo. O padrão é **Desativado**.
- **Samsung: Somente dispositivo totalmente gerenciado**
  - **Habilitar verificação de inicialização confiável ODE:** Use a verificação de inicialização confiável ODE para estabelecer uma cadeia de confiança do bootloader para a imagem do sistema. O padrão é **Ativado**.
  - **Permitir apenas chamadas de emergência:** Permite que os usuários ativem o modo Somente Chamada de Emergência em seus dispositivos. O padrão é **Desativado**.

- **Permitir recuperação de firmware:** Permite que os usuários recuperem o firmware em seus dispositivos. O padrão é **Ativado**.
- **Permitir criptografia rápida:** Permite a criptografia apenas do espaço de memória usado. Esta criptografia contrasta com a criptografia de disco completo, que criptografa todos os dados. Esses dados incluem configurações, dados de aplicativos, arquivos e aplicativos baixados, mídia e outros arquivos. O padrão é **Ativado**.
- **Habilitar modo Common Criteria:** Coloca um dispositivo no Modo Common Criteria. A configuração Common Criteria impõe processos de segurança rigorosos. O padrão é **Ativado**.
- **Habilitar banner de reinicialização:** Exibe uma mensagem de notificação de uso do sistema aprovada pelo DoD ou um banner quando os dispositivos dos usuários são reiniciados. O padrão é **Desativado**.
- **Permitir alterações de configurações:** Permite que os usuários alterem as configurações em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Habilitar uso de dados em segundo plano:** Permite que os aplicativos sincronizem dados em segundo plano. para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Permitir área de transferência:** Permite que os usuários copiem dados para a área de transferência em seus dispositivos. O padrão é **Ativado**.
    - **Permitir compartilhamento da área de transferência:** Permite que os usuários compartilhem conteúdo da área de transferência entre seus dispositivos e um computador (MDM 4.0 e posterior).
- **Permitir tecla inicial:** Permite que os usuários usem a tecla **Home** em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Permitir localização simulada:** Permite que os usuários simulem sua localização GPS. Para dispositivos totalmente gerenciados. O padrão é **Desativado**.
- **NFC:** Permite que os usuários usem NFC em seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Permitir desligamento:** Permite que os usuários desliguem seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Permitir Wi-Fi Direct:** Permite que os usuários se conectem diretamente a outro dispositivo através de sua conexão Wi-Fi. O padrão é **Ativado**. Se **Ativado**, você deve habilitar a configuração **Permitir alterações de Wi-Fi**.

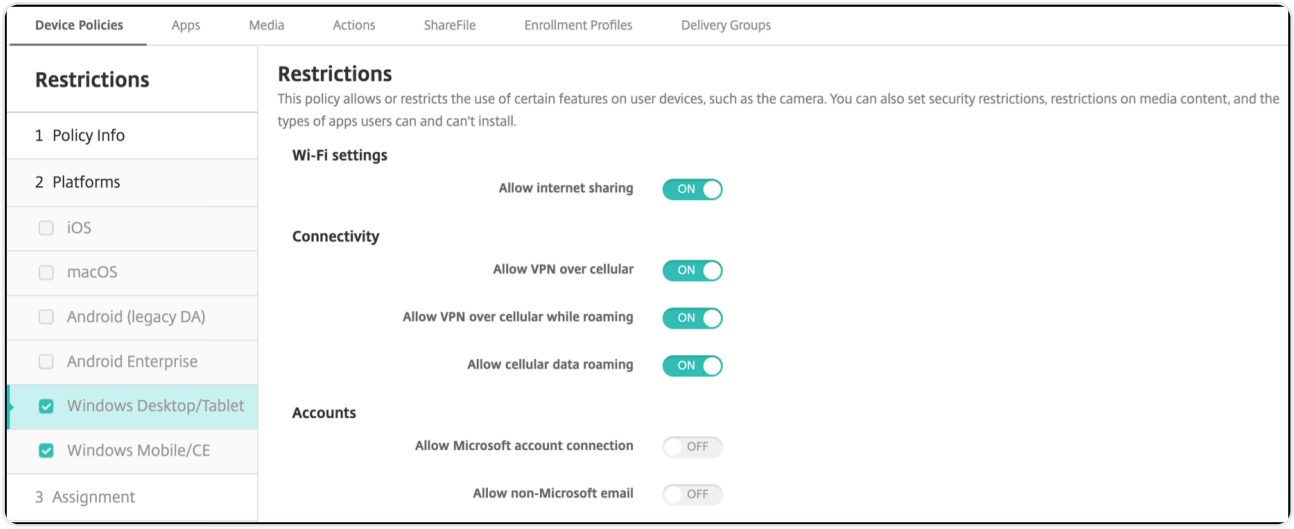
- **Permitir cartão SD:** Permite que os usuários usem um cartão SD, se disponível, com seus dispositivos. O padrão é **Ativado**.
- **Permitir armazenamento host USB:** Permite que os dispositivos dos usuários atuem como host USB quando um dispositivo USB se conecta a eles. Os dispositivos dos usuários então fornecem energia ao dispositivo USB. O padrão é **Ativado**.
- **Permitir discador de voz:** Permite que os usuários usem o discador de voz em seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir S Beam:** Permite que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir S Voice:** Permite que os usuários usem o assistente pessoal inteligente e o navegador de conhecimento em seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir tethering USB:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão USB. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
- **Permitir tethering Bluetooth:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão Bluetooth. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
- **Permitir tethering Wi-Fi:** Permite que os usuários compartilhem uma conexão de dados móveis com outro dispositivo usando sua conexão Wi-Fi. O padrão é **Desativado**. Se **Ativado**, a configuração **Permitir tethering** também deve estar **Ativada**.
- **Permitir MMS de entrada:** Permite que os usuários recebam mensagens MMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir MMS de saída:** Permite que os usuários enviem mensagens MMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir SMS de entrada:** Permite que os usuários recebam mensagens SMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Permitir SMS de saída:** Permite que os usuários enviem mensagens SMS. O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir SMS**.
- **Configurar redes móveis:** Permite que os usuários usem sua conexão de dados móveis. O padrão é **Desativado**.
- **Limite por dia (MB):** Insira o número de MB de dados móveis que os usuários podem usar por dia. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).

- **Limite por semana (MB):** Insira o número de MB de dados móveis que os usuários podem usar por semana. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).
- **Limite por mês (MB):** Insira o número de MB de dados móveis que os usuários podem usar por mês. O padrão é 0, o que desativa este recurso (MDM 4.0 e posterior).
- **Permitir apenas conexões VPN seguras:** Permite que os usuários usem apenas conexões seguras (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir gravação de áudio:** Permite que os usuários gravem áudio com seus dispositivos (MDM 4.0 e posterior). O padrão é **Ativado**. Se **Ativado**, você deve ativar a configuração **Permitir microfone**.
- **Permitir gravação de vídeo:** Permite que os usuários gravem vídeo com seus dispositivos (MDM 4.0 e posterior). O padrão é **Desativado**. Se **Ativado**, você deve ativar a configuração **Permitir uso da câmera**.
- **Permitir mensagens push em roaming:** Permite que os usuários usem dados móveis para push. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.
- **Permitir sincronização automática em roaming:** Permite que os usuários usem dados móveis para sincronização. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.
- **Permitir chamadas de voz em roaming:** Permite que os usuários usem dados móveis para chamadas de voz. O padrão é **Desativado**. Se **Ativado**, você deve habilitar a configuração **Permitir roaming de dados**.

- **Samsung: Contêiner Knox/Dispositivo totalmente gerenciado**
  - **Habilitar verificação de revogação:** Habilita a verificação de certificados revogados. O padrão é **Desativado**.
- **Samsung: Somente contêiner Knox**
  - **Mover aplicativos para o contêiner:** Permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação multifator:** Os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir seus dispositivos. O padrão é **Ativado**.
  - **Impor autenticação para o contêiner:** Use um método de autenticação diferente do método usado para desbloquear o dispositivo para abrir o contêiner KNOX. O padrão é **Ativado**.

- **Habilitar teclado seguro:** Força os usuários a usar um teclado seguro dentro do contêiner Knox. O padrão é **Ativado**.

Configurações de Desktop/Tablet Windows



- **Configurações de Wi-Fi**
  - **Permitir compartilhamento de Internet:** Permite que um dispositivo compartilhe sua conexão de internet com outros dispositivos, transformando-o em um ponto de acesso Wi-Fi.
- **Conectividade**
  - **Permitir VPN sobre dados móveis:** Permite que o dispositivo se conecte via VPN a uma rede de dados móveis.
  - **Permitir VPN sobre dados móveis em roaming:** Permite que o dispositivo se conecte via VPN quando o dispositivo estiver em roaming em redes de dados móveis.
  - **Permitir roaming de dados móveis:** Permite que os usuários usem dados móveis em roaming.
- **Contas**
  - **Permitir conexão de conta Microsoft:** Permite que o dispositivo use uma conta Microsoft para autenticação de conexão e serviços não relacionados a e-mail.
  - **Permitir e-mail não Microsoft:** Permite que o usuário adicione contas de e-mail não Microsoft.
- **Sistema**

  - **Permitir cartão de armazenamento:** Permite que o dispositivo use um cartão de armazenamento.
  - **Telemetria:** Selecione uma opção na lista suspensa para permitir ou restringir o dispositivo de enviar informações de telemetria. O padrão é **Permitido**. Outras opções são **Não permitido** e **Permitido, exceto para solicitação de dados secundários**.
  - **Permitir serviços de localização:** Permite serviços de localização.
  - **Permitir visualização de compilações internas:** Permite que os usuários visualizem compilações internas da Microsoft.

- **Câmera:**
  - **Permitir uso da câmera:** Permite que os usuários usem a câmera do dispositivo.
- **Bluetooth:**
  - **Permitir modo detectável:** Permite que dispositivos Bluetooth encontrem o dispositivo local.
  - **Nome do dispositivo local:** Um nome para o dispositivo local.
- **Experiência:**
  - **Permitir Cortana:** Permite que os usuários acessem a Cortana, a assistente pessoal inteligente e navegadora de conhecimento.
  - **Permitir descoberta de dispositivo:** Permite a descoberta de rede do dispositivo.
  - **Permitir cancelamento manual de registro MDM:** Permite que os usuários cancelem manualmente o registro de seus dispositivos no XenMobile MDM.
  - **Permitir sincronização de configurações do dispositivo:** Permite que os usuários sincronizem configurações entre dispositivos Windows 10 e Windows 11 durante o roaming.
- **Acima do Bloqueio:**
  - **Permitir notificações pop-up:** Permite notificações pop-up na tela de bloqueio.
- **Aplicativos**
  - **Permitir atualização automática da loja de aplicativos:** Permite que os aplicativos da loja de aplicativos sejam atualizados automaticamente.
- **Privacidade:**

- **Permitir personalização de entrada:** Permite que o serviço de personalização de entrada seja executado, para melhorar as entradas preditivas, como teclado de caneta e toque, com base no que o usuário digita.

- **Configurações:**
  - **Permitir reprodução automática:** Permite que os usuários alterem as configurações de Reprodução Automática.
  - **Permitir Data Sense:** Permite que os usuários alterem as configurações do Data Sense.
  - **Permitir data e hora:** Permite que os usuários alterem as configurações de data e hora.
  - **Permitir idioma:** Permite que os usuários alterem as configurações de idioma.
  - **Permitir energia e suspensão:** Permite que os usuários alterem as configurações de energia e suspensão.
  - **Permitir região:** Permite que os usuários alterem as configurações de região.
  - **Permitir opções de login:** Permite que os usuários alterem as configurações de login.
  - **Permitir local de trabalho:** Permite que os usuários alterem as configurações de local de trabalho.
  - **Permitir sua conta:** Permite que os usuários alterem as configurações da conta.

Política de dispositivo de roaming

Você pode adicionar uma política de dispositivo no XenMobile para configurar se o roaming de voz e dados será permitido nos dispositivos iOS dos usuários. Quando o roaming de voz é desabilitado, o roaming de dados é automaticamente desabilitado. Para iOS, esta política está disponível apenas em dispositivos iOS 5.0 e posteriores.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

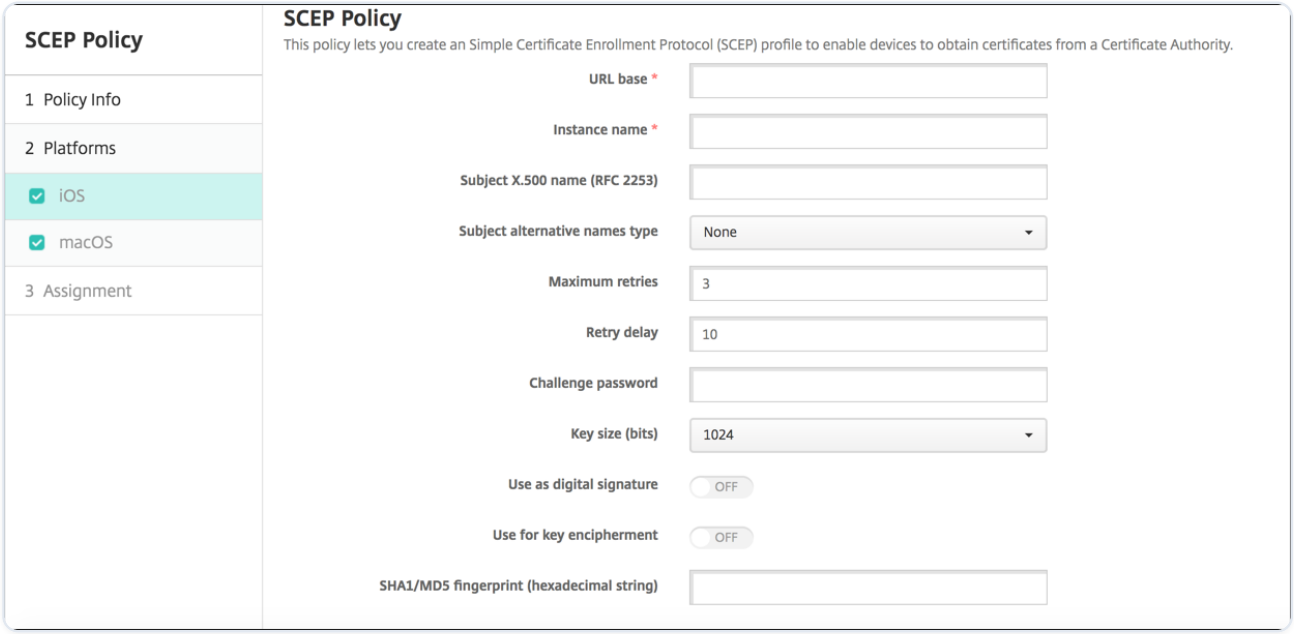
- **Desabilitar roaming de voz:** Selecione se deseja desabilitar o roaming de voz. Quando esta opção está habilitada, o roaming de dados é automaticamente desabilitado. O padrão é **Desativado**, o que permite o roaming de voz.
- **Desabilitar roaming de dados:** Selecione se deseja desabilitar o roaming de dados. Esta opção está disponível apenas quando o roaming de voz está habilitado. O padrão é **Desativado**, o que permite o roaming de dados.

Política de dispositivo SCEP

Esta política permite configurar dispositivos iOS e macOS para recuperar um certificado usando o Protocolo Simples de Registro de Certificados (SCEP) de um servidor SCEP externo. Se você deseja entregar um certificado ao dispositivo usando SCEP de uma PKI conectada ao XenMobile, você deve criar uma entidade PKI e um provedor PKI no modo distribuído. Para obter detalhes, consulte Entidades PKI.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

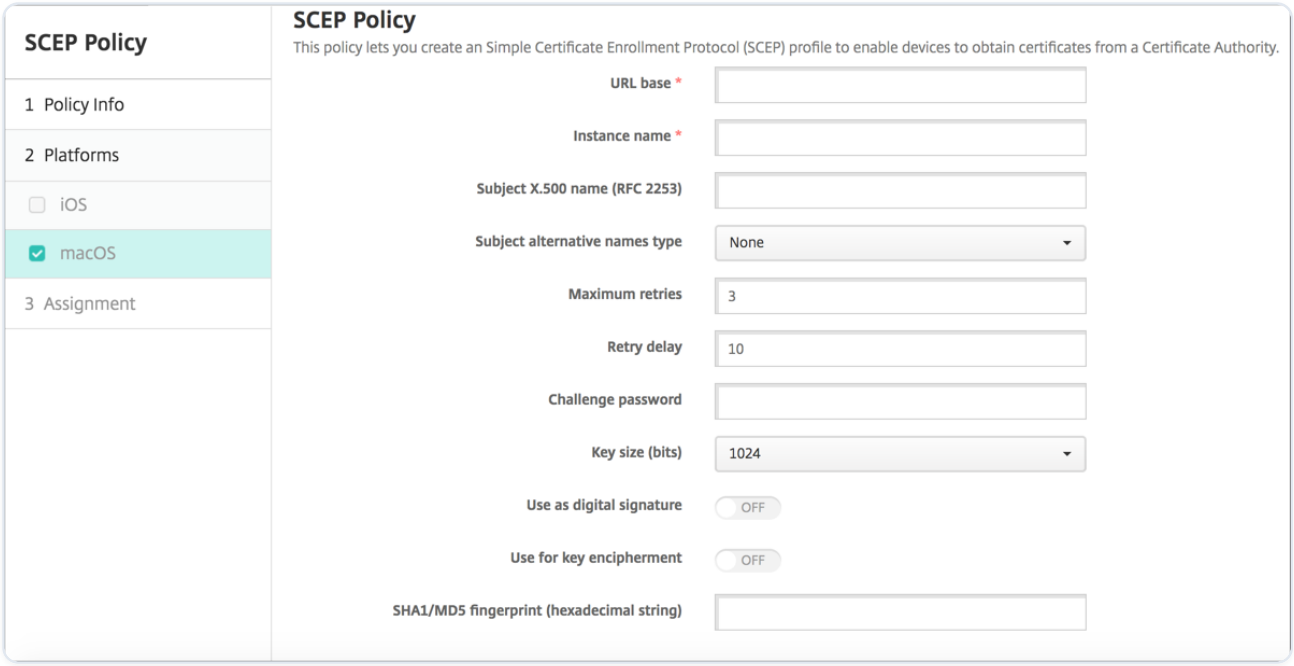


- **URL base:** Digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas, via HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), então pode ser seguro enviar a solicitação sem criptografia. No entanto, se a senha de uso único puder ser reutilizada, você deve usar HTTPS para proteger a senha. Esta etapa é obrigatória.
- **Nome da instância:** Digite qualquer string que o servidor SCEP reconheça. Por exemplo, pode ser um nome de domínio como example.org. Se uma CA tiver vários certificados de CA, você pode usar este campo para distinguir o domínio necessário. Esta etapa é obrigatória.
- **Nome do assunto X.500 (RFC 2253):** Digite a representação de um nome X.500 representado como um array de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que pode ser traduzido para: \[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]. Você pode representar OIDs como números

pontilhados com atalhos para país (C), localidade (L), estado (ST), organização (O), unidade organizacional (OU) e nome comum (CN).

- **Tipo de nomes alternativos do assunto:** Clique em um tipo de nome alternativo na lista suspensa. A política SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela CA para emitir um certificado. Você pode especificar **Nenhum**, **Nome RFC 822**, **Nome DNS** ou **URI**.
- **Máximo de tentativas:** Digite o número de vezes que um dispositivo pode tentar novamente quando o servidor SCEP envia uma resposta PENDENTE. O padrão é **3**.
- **Atraso de nova tentativa:** Digite o número de segundos a aguardar entre as tentativas subsequentes. A primeira tentativa é feita sem atraso. O padrão é **10**.
- **Senha de desafio:** Insira um segredo pré-compartilhado.
- **Tamanho da chave (bits):** Selecione **2048** ou superior como o tamanho da chave em bits.
- **Usar como assinatura digital:** Especifique se você deseja que o certificado seja usado como uma assinatura digital. Se alguém estiver usando o certificado para verificar uma assinatura digital, como verificar se um certificado foi emitido por uma CA, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de usar a chave pública para descriptografar o hash.
- **Usar para cifragem de chave:** Especifique se você deseja que o certificado seja usado para cifragem de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se um dado foi criptografado usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para cifragem de chave. Caso contrário, a operação falha.
- **Impressão digital SHA1/MD5 (string hexadecimal):** Se sua CA usar HTTP, use este campo para fornecer a impressão digital do certificado da CA, que o dispositivo usa para confirmar a autenticidade da resposta da CA durante o registro. Você pode inserir uma impressão digital SHA1 ou MD5, ou pode selecionar um certificado para importar sua assinatura.
- **Configurações de política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS



- **URL base:** Digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas, via HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), então pode ser seguro enviar a solicitação não criptografada. No entanto, se a senha de uso único puder ser reutilizada, você deve usar HTTPS para proteger a senha. Esta etapa é obrigatória.
- **Nome da instância:** Digite qualquer string que o servidor SCEP reconheça. Por exemplo, pode ser um nome de domínio como example.org. Se uma CA tiver vários certificados de CA, você pode usar este campo para distinguir o domínio necessário. Esta etapa é obrigatória.
- **Nome do assunto X.500 (RFC 2253):** Digite a representação de um nome X.500 representado como um array de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se traduziria em: \[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]. Você pode representar OIDs como números pontilhados com atalhos para país (C), localidade (L), estado (ST), organização (O), unidade organizacional (OU) e nome comum (CN).
- **Tipo de nomes alternativos do assunto:** Clique em um tipo de nome alternativo na lista suspensa. A política SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela CA para emitir um certificado. Você pode especificar **Nenhum**, **Nome RFC 822**, **Nome DNS** ou **URI**.
- **Tentativas máximas:** Digite o número de vezes que um dispositivo pode tentar novamente quando o servidor SCEP envia uma resposta PENDENTE. O padrão é **3**.
- **Atraso de nova tentativa:** Digite o número de segundos a aguardar entre as tentativas subsequentes. A primeira tentativa é feita sem atraso. O padrão é **10**.

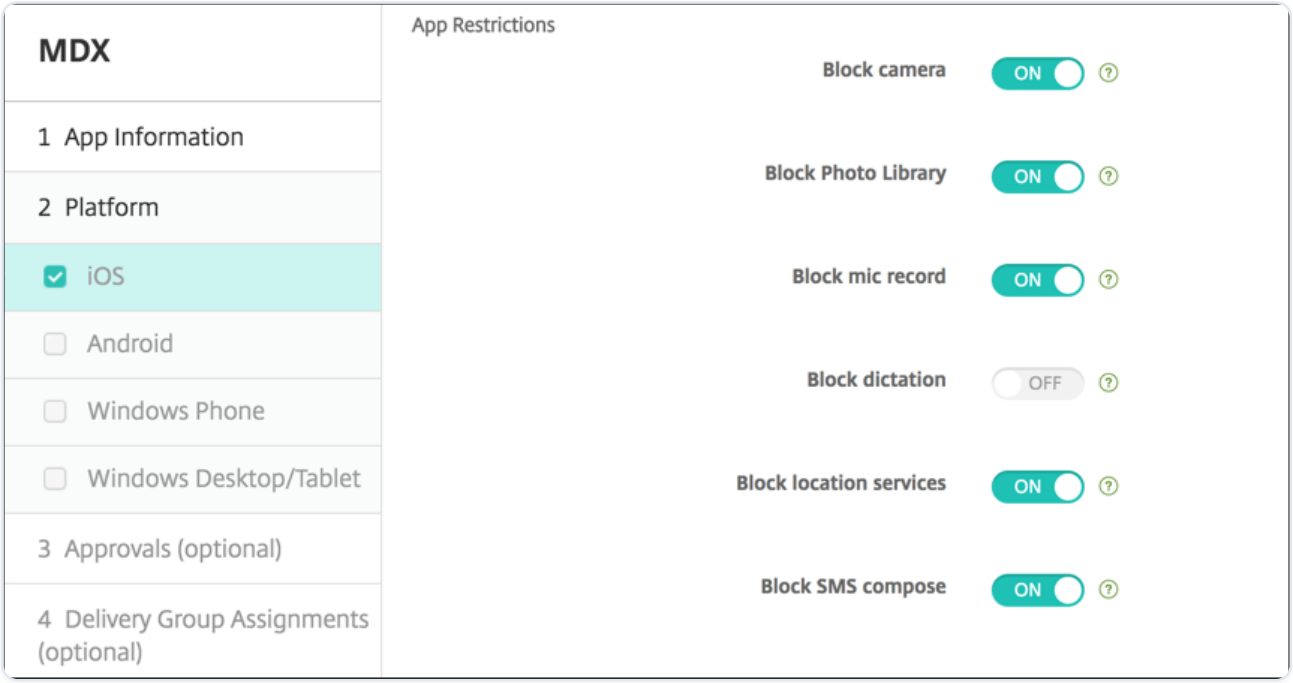
- **Senha de desafio:** Digite um segredo pré-compartilhado.
- **Tamanho da chave (bits):** Selecione **2048** ou superior como o tamanho da chave em bits.
- **Usar como assinatura digital:** Especifique se você deseja que o certificado seja usado como uma assinatura digital. Se alguém estiver usando o certificado para verificar uma assinatura digital, como verificar se um certificado foi emitido por uma CA, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de usar a chave pública para descriptografar o hash.
- **Usar para cifragem de chave:** Especifique se você deseja que o certificado seja usado para cifragem de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se um dado foi criptografado usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para cifragem de chave. Caso contrário, a operação falha.
- **Impressão digital SHA1/MD5 (cadeia hexadecimal):** Se sua CA usa HTTP, use este campo para fornecer a impressão digital do certificado da CA, que o dispositivo usa para confirmar a autenticidade da resposta da CA durante o registro. Você pode inserir uma impressão digital SHA1 ou MD5, ou pode selecionar um certificado para importar sua assinatura.
- **Configurações de política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.
    - **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
    - **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Políticas de Siri e ditado

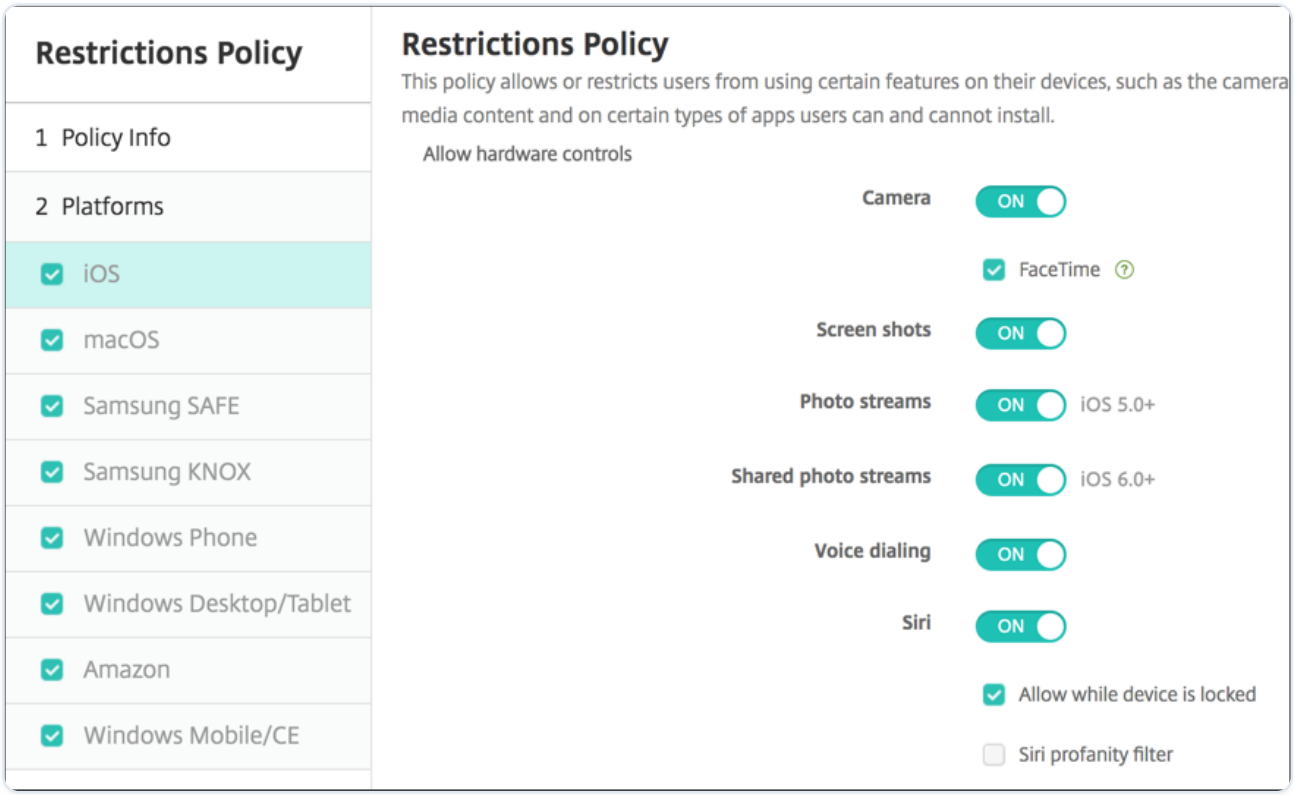
Quando os usuários perguntam algo à Siri ou ditam texto em dispositivos iOS gerenciados, a Apple coleta os dados de voz para melhorar a Siri. Os dados de voz passam pelos serviços baseados em nuvem da Apple e, portanto, existem fora do contêiner seguro do XenMobile®. O texto resultante do ditado, no entanto, permanece dentro do contêiner.

O XenMobile permite que você bloqueie os serviços de Siri e ditado, conforme suas necessidades de segurança exigirem.

Em implantações MAM, a política **Bloquear ditado** para cada aplicativo está **Ativada** por padrão, o que desabilita o microfone do dispositivo. Defina-a como **Desativada** se quiser permitir o ditado. Você pode encontrar a política no console do XenMobile em **Configurar > Aplicativos**. Selecione o aplicativo, clique em **Editar** e, em seguida, clique em **iOS**.



Em implantações MDM, você também pode desabilitar a Siri com a política de Siri em **Configurar > Políticas de Dispositivo**. O uso da Siri é permitido por padrão.



Alguns pontos a serem considerados ao decidir se deve permitir Siri e ditado:

- De acordo com informações que a Apple tornou públicas, a Apple mantém os dados de clipes de voz da Siri e do ditado por até dois anos. Os dados são atribuídos a um número aleatório para representar o usuário, e os arquivos de voz são associados a esse número aleatório. Para mais informações, consulte este artigo da Wired, Apple revela por quanto tempo a Siri mantém seus dados.
- Você pode revisar a política de privacidade da Apple acessando **Ajustes > Geral > Teclados** em qualquer dispositivo iOS e tocando no link em **Ativar Ditado**.

Política de dispositivo de conta SSO

Você cria contas de logon único (SSO) no XenMobile® para permitir que os usuários façam logon uma única vez para acessar o XenMobile e os recursos internos da sua empresa a partir de vários aplicativos. Os usuários não precisam armazenar nenhuma credencial no dispositivo. As credenciais de usuário corporativo da conta SSO são usadas em todos os aplicativos, incluindo aplicativos da App Store. Esta política foi projetada para funcionar com um back-end de autenticação Kerberos.

Esta política se aplica apenas ao iOS 7.0 e posterior.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Nome da conta:** Insira o nome da conta SSO Kerberos que aparece nos dispositivos dos usuários. Este campo é obrigatório.
- **Nome principal do Kerberos:** Insira o nome principal do Kerberos. Este campo é obrigatório.
- **Credencial de identidade (Keystore ou credencial PKI):** Clique em uma credencial de identidade opcional na lista suspensa que pode ser usada para renovar a credencial Kerberos sem interação do usuário.
- **Realm Kerberos:** Insira o realm Kerberos para esta política. Este valor de configuração é tipicamente o nome do seu domínio em letras maiúsculas (por exemplo, EXAMPLE.COM). Este campo é obrigatório.
- **URLs permitidas:** Para cada URL para a qual você deseja exigir SSO, clique em **Adicionar** e faça o seguinte:
  - **URL permitida:** Insira uma URL para a qual você deseja exigir SSO quando um usuário visita a URL a partir do dispositivo iOS.

    Por exemplo, quando um usuário tenta navegar para um site e o site inicia um desafio Kerberos: Se esse site não estiver na lista de URLs, o dispositivo iOS não tentará o SSO fornecendo o token Kerberos que o Kerberos pode ter armazenado em cache no dispositivo de um logon Kerberos anterior. A correspondência deve ser exata na parte do host da URL. Por exemplo, `https://shopping.apple.com` é válido, mas `https://*.apple.com` não é.

    Além disso, se o Kerberos não for ativado com base na correspondência de host, a URL ainda retornará a uma chamada HTTP padrão. Isso pode significar quase qualquer coisa, incluindo um desafio de senha padrão ou um erro HTTP se a URL estiver configurada apenas para SSO usando Kerberos.
  - Clique em **Adicionar** para adicionar a URL ou clique em **Cancelar** para cancelar a adição da URL.
- **Identificadores de aplicativo:** Para cada aplicativo que tem permissão para usar este login, clique em **Adicionar** e faça o seguinte:
  - **Identificador de Aplicativo:** Insira um identificador de aplicativo para um aplicativo que tem permissão para usar este login. Se você não adicionar nenhum identificador de aplicativo, este login corresponderá a **todos** os identificadores de aplicativo.
  - Clique em **Adicionar** para adicionar o identificador de aplicativo ou clique em **Cancelar** para cancelar a adição do identificador de aplicativo.

- **Configurações de política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo da loja

Você pode criar uma política no XenMobile® para especificar se os dispositivos iOS, Android ou Windows Tablet exibem um web clip da XenMobile Store na tela inicial dos dispositivos.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma

Para cada plataforma que você configurar, selecione se um web clip da XenMobile Store aparece nos dispositivos do usuário. O padrão é **Ativado**.

Política de dispositivo de calendários assinados

Você pode adicionar uma política de dispositivo no XenMobile para adicionar um calendário assinado à lista de calendários nos dispositivos iOS. A lista de calendários públicos aos quais você pode assinar está disponível em www.apple.com/downloads/macosx/calendars.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisito

Você deve ter assinado um calendário antes de poder adicioná-lo à lista de calendários assinados nos dispositivos do usuário.

Configurações do iOS

- **Descrição:** Insira uma descrição do calendário. Este campo é obrigatório.

- **URL:** Insira o URL do calendário. Você pode inserir um URL `webcal://` ou um link `https://` para um arquivo iCalendar (.ics). Este campo é obrigatório.
- **Nome de usuário:** Insira o nome de logon do usuário. Este campo é obrigatório.
- **Senha:** Insira uma senha de usuário opcional.
- **Usar SSL:** Selecione se deseja usar uma conexão Secure Socket Layer para o calendário. O padrão é **Desativado**.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de termos e condições

Você cria políticas de dispositivo de termos e condições no XenMobile® quando deseja que os usuários aceitem as políticas específicas da sua empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos no XenMobile, eles são apresentados aos termos e condições e devem aceitá-los para registrar seus dispositivos. Recusar os termos e condições cancela o processo de registro.

Você pode criar diferentes políticas de termos e condições em diferentes idiomas se sua empresa tiver usuários internacionais e você quiser que eles aceitem os termos e condições em seus idiomas nativos. Você deve fornecer um arquivo para cada combinação de plataforma e idioma que planeja implantar. Para dispositivos Android e iOS, você deve fornecer arquivos PDF. Para dispositivos Windows, você deve fornecer arquivos de texto (.txt) e arquivos de imagem que os acompanham.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS e Android

- **Arquivo a ser importado:** Selecione o arquivo de termos e condições para importar clicando em **Procurar** e, em seguida, navegando até o local do arquivo.

- **Termos e Condições Padrão:** Selecione se este arquivo é o documento padrão para usuários que são membros de vários grupos com diferentes termos e condições. O padrão é **Desativado**.

Configurações de Tablet Windows

- **Arquivo a ser importado:** Selecione o arquivo de termos e condições para importar clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
- **Imagem:** Selecione o arquivo de imagem para importar clicando em **Procurar** e, em seguida, navegando até o local do arquivo.
- **Termos e Condições Padrão:** Selecione se este arquivo é o documento padrão para usuários que são membros de vários grupos com diferentes termos e condições. O padrão é **Desativado**.

Política de dispositivo VPN

A política de dispositivo VPN configura as definições de rede privada virtual (VPN) que permitem que os dispositivos dos usuários se conectem com segurança aos recursos corporativos. Você pode configurar a política de dispositivo VPN para as seguintes plataformas. Cada plataforma requer um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Requisitos para VPNs por aplicativo

Você configura o recurso VPN por aplicativo para as seguintes plataformas por meio de políticas VPN:

- iOS
- macOS
- Android (DA herdado)
- Samsung SAFE
- Samsung Knox

Para configurar VPNs para dispositivos Android Enterprise, crie uma política de dispositivo de configurações gerenciadas para o aplicativo Citrix SSO. Consulte Configurar perfis VPN para Android Enterprise.

As opções de VPN por aplicativo estão disponíveis para certos tipos de conexão. A tabela a seguir indica quando as opções de VPN por aplicativo estão disponíveis.

PLATAFORMA	TIPO DE CONEXÃO	OBSERVAÇÃO
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO ou SSL Personalizado.	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA ou SSL Personalizado.	
Android (DA herdado)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	Tipo de VPN definido como **Genérico**
Samsung Knox	IPSEC, SSL	Tipo de VPN definido como **Genérico**

Para criar uma VPN por aplicativo para dispositivos iOS e Android (DA herdado) usando o aplicativo Citrix SSO, você precisa realizar etapas extras, além da configuração da política de VPN. Além disso, você deve verificar se os seguintes pré-requisitos são atendidos:

- Citrix Gateway local
- Os seguintes aplicativos estão instalados no dispositivo:
  - Citrix SSO
  - Citrix Secure Hub™

Um fluxo de trabalho geral para configurar uma VPN por aplicativo para dispositivos iOS e Android usando o aplicativo Citrix SSO é o seguinte:

1. Configure uma política de dispositivo VPN conforme descrito neste artigo.
   - Para *iOS*, consulte Configurar o protocolo Citrix SSO para iOS. Depois de configurar o protocolo Citrix SSO para iOS por meio de uma política de dispositivo VPN, você também deve criar uma política de Atributos de Aplicativo para associar um aplicativo à política de

VPN por aplicativo. Para obter mais informações, consulte Configurar uma VPN por aplicativo.

- Para o campo **Tipo de autenticação para a conexão**, se você selecionar **Certificado**, primeiro você deve configurar a autenticação baseada em certificado para o Endpoint Management. Consulte Certificado de cliente ou certificado mais autenticação de domínio.

- Para *Android (DA herdado)*, consulte Configurar o protocolo Citrix SSO para Android.
  - Para o campo **Tipo de autenticação para a conexão**, se você selecionar **Certificado** ou **Senha e Certificado**, primeiro você deve configurar a autenticação baseada em certificado para o Endpoint Management. Consulte Certificado de cliente ou certificado mais autenticação de domínio.

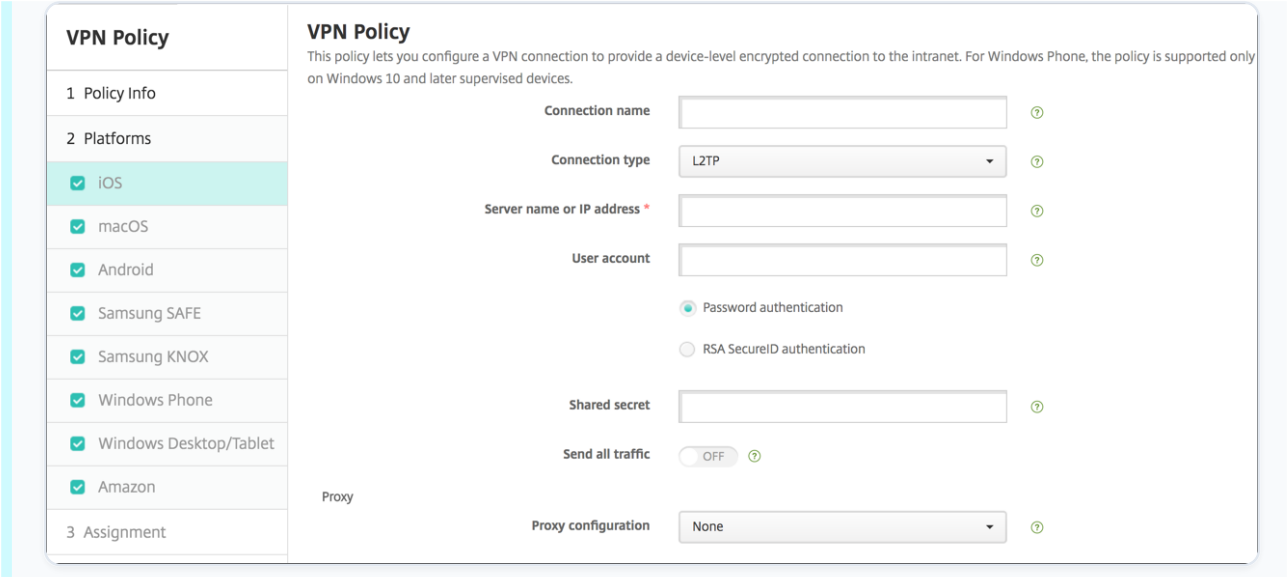
2. Configure o Citrix ADC para aceitar o tráfego da VPN por aplicativo. Para obter detalhes, consulte Configuração completa de VPN no Citrix Gateway.

Configurações do iOS

Para se preparar para atualizações de dispositivo para iOS 12:

O tipo de conexão Citrix VPN na política de dispositivo VPN para iOS não oferece suporte ao iOS 12. Siga estas etapas para excluir sua política de dispositivo VPN existente e criar uma política de dispositivo VPN com o tipo de conexão Citrix SSO:

1. Exclua sua política de dispositivo VPN para iOS.
2. Adicione uma política de dispositivo VPN para iOS. Configurações importantes:
   - **Tipo de conexão** = **Citrix SSO**
   - **Habilitar VPN por aplicativo** = **Ativado**
   - **Tipo de provedor** = **Túnel de pacote**
3. Adicione uma política de dispositivo de Atributos de Aplicativo para iOS. Para **Identificador de VPN por aplicativo**, escolha **iOS_VPN**.



- **Nome da conexão:** Digite um nome para a conexão.
- **Tipo de conexão:** Na lista, selecione o protocolo a ser usado para esta conexão. O padrão é **L2TP**.
  - **L2TP:** Protocolo de Tunelamento de Camada 2 com autenticação de chave pré-compartilhada.
  - **PPTP:** Tunelamento Ponto a Ponto.
  - **IPSec:** Sua conexão VPN corporativa.
  - **Cisco Legacy AnyConnect:** Este tipo de conexão exige que o cliente VPN Cisco Legacy AnyConnect esteja instalado no dispositivo do usuário. A Cisco está descontinuando o cliente Cisco Legacy AnyConnect que era baseado em uma estrutura VPN agora obsoleta. Para obter mais informações, consulte o artigo de suporte `<https://support.citrix.com/article/CTX227708>`.

    Para usar o cliente Cisco AnyConnect atual, use um **Tipo de conexão** de **SSL Personalizado**. Para as configurações necessárias, consulte “Configurar protocolo SSL Personalizado” nesta seção.
  - **Juniper SSL:** Cliente VPN SSL da Juniper Networks.
  - **F5 SSL:** Cliente VPN SSL da F5 Networks.
  - **SonicWALL Mobile Connect:** Cliente VPN unificado da Dell para iOS.
  - **Ariba VIA:** Cliente de Acesso Virtual à Internet da Ariba Networks.
  - **IKEv2 (somente iOS):** Internet Key Exchange versão 2 somente para iOS.
  - **AlwaysOn IKEv2:** Acesso sempre ativo usando IKEv2.

- **AlwaysOn IKEv2 Dual Configuration:** Acesso sempre ativo usando configuração dupla IKEv2.
- **Citrix SSO:** Cliente Citrix SSO para iOS 12 e posterior.
- **SSL Personalizado:** Secure Socket Layer personalizado. Este tipo de conexão é necessário para o cliente Cisco AnyConnect que tem um ID de pacote de **com.cisco.anyconnect**. Especifique um **Nome de conexão** de **Cisco AnyConnect**. Você também pode implantar a política de VPN e habilitar um filtro de Controle de Acesso à Rede (NAC) para dispositivos iOS. O filtro bloqueia uma conexão VPN para dispositivos que têm aplicativos não compatíveis instalados. A configuração requer configurações específicas para a política de VPN do iOS, conforme descrito na seção iOS a seguir. Para obter mais informações sobre outras configurações necessárias para habilitar o filtro NAC, consulte Controle de Acesso à Rede.

As seções a seguir listam as opções de configuração para cada um dos tipos de conexão precedentes.

Configurar Protocolo L2TP para iOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- Selecione **Autenticação por senha** ou **Autenticação RSA SecurID**.
- **Segredo compartilhado:** Digite a chave de segredo compartilhado IPsec.
- **Enviar todo o tráfego:** Selecione se deseja enviar todo o tráfego pela VPN. O padrão é **Desativado**.

Configurar Protocolo PPTP para iOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- Selecione **autenticação por senha** ou **autenticação RSA SecurID**.
- **Nível de criptografia:** Na lista, selecione um nível de criptografia. O padrão é **Nenhum**.
  - **Nenhum:** Não usar criptografia.
  - **Automático:** Use o nível de criptografia mais forte compatível com o servidor.
  - **Máximo (128 bits):** Sempre use criptografia de 128 bits.

- **Enviar todo o tráfego:** Selecione se deseja enviar todo o tráfego pela VPN. O padrão é **Desativado**.

Configurar Protocolo IPsec para iOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de Usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Segredo Compartilhado** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Segredo Compartilhado**.
- Se você habilitar **Segredo Compartilhado**, configure estas configurações:
  - **Nome do grupo:** Digite um nome de grupo opcional.
  - **Segredo compartilhado:** Digite uma chave de segredo compartilhado opcional.
  - **Usar autenticação híbrida:** Selecione se deseja usar autenticação híbrida. Com a autenticação híbrida, o servidor primeiro se autentica para o cliente, e então o cliente se autentica para o servidor. O padrão é **Desativado**.
  - **Solicitar senha:** Selecione se deseja solicitar as senhas dos usuários quando eles se conectarem à rede. O padrão é **Desativado**.
- Se você habilitar **Certificado**, configure estas definições:
  - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
  - **Solicitar PIN ao conectar:** Selecione se deseja exigir que os usuários insiram seu PIN ao se conectar à rede. O padrão é **Desativado**.
  - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectam à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** está **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**.
- **Correspondência de aplicativo sob demanda habilitada:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.

- **Domínios do Safari:** Clique em **Adicionar** para adicionar um nome de domínio do Safari.

Configurar o protocolo Cisco AnyConnect legado para iOS

Para fazer a transição do cliente Cisco AnyConnect legado para o novo cliente Cisco AnyConnect, use o protocolo SSL personalizado.

- **Identificador de pacote do provedor:** Para o cliente AnyConnect legado, o ID do pacote é com.cisco.anyconnect.gui.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Grupo:** Digite um nome de grupo opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
    - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
    - Se você habilitar **Certificado**, configure estas definições:
        - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
        - **Solicitar PIN ao conectar:** Selecione se deseja solicitar o PIN aos usuários quando eles se conectarem à rede. O padrão é **Desativado**.
        - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
    - **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
    - **Tipo de provedor:** Selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.

- **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o Protocolo SSL Juniper para iOS

- **Identificador de pacote do provedor:** Se o seu perfil de VPN por aplicativo tiver o identificador de pacote de um aplicativo com vários provedores de VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Realm:** Digite um nome de realm opcional.
- **Função:** Digite um nome de função opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN deles quando se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:

- **Correspondência de aplicativo sob demanda habilitada:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
- **Tipo de provedor:** Selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
- **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar protocolo F5 SSL para iOS

- **Identificador de pacote do provedor:** Se o seu perfil VPN por aplicativo tiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectam à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** está **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
  - **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.
  - **Tipo de provedor:** Selecione se a VPN por aplicativo é fornecida como um **proxy de aplicativo** ou como um **túnel de pacote**. O padrão é **proxy de aplicativo**.
  - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar protocolo SonicWALL para iOS

- **Identificador de pacote do provedor:** Se o seu perfil VPN por aplicativo tiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Grupo de logon ou domínio:** Digite um grupo de logon ou domínio opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para

obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você definir esta opção como ATIVADO, configure estas definições:
  - **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.
  - **Tipo de provedor:** Selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
  - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o protocolo Ariba VIA para iOS

- **Identificador de pacote do provedor:** Se o seu perfil VPN por aplicativo tiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.

    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar as definições de Habilitar VPN sob demanda para iOS.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:

    - **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.
    - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:

        - **Domínio:** Digite o domínio a ser adicionado.
        - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar protocolos IKEv2 para iOS

Esta seção inclui configurações usadas para os protocolos IKEv2, AlwaysOn IKEv2 e AlwaysOn IKEv2 Dual Configuration. Para o protocolo AlwaysOn IKEv2 Dual Configuration, configure todas essas configurações para redes celulares e Wi-Fi.

- **Permitir que o usuário desative a conexão automática:** Para os protocolos AlwaysOn. Selecione se deseja permitir que os usuários desativem a conexão automática à rede em seus dispositivos. O padrão é **Desativado**.
- **Nome do host ou endereço IP do servidor:** Digite o nome do servidor ou o endereço IP do servidor VPN.
- **Identificador Local:** O FQDN ou endereço IP para o cliente IKEv2. Este campo é obrigatório.
- **Identificador Remoto:** O FQDN ou endereço IP para o servidor VPN. Este campo é obrigatório.
- **Autenticação do Dispositivo:** Escolha **Segredo Compartilhado**, **Certificado** ou **Certificado do dispositivo baseado no identificador do dispositivo** para o tipo de autenticação desta conexão. O padrão é **Segredo Compartilhado**.

    - Se você escolher **Segredo Compartilhado**, digite uma chave de segredo compartilhado opcional.

  - Se você escolher **Certificado**, escolha uma **Credencial de identidade** para usar. O padrão é **Nenhum.**
  - Se você escolher **Certificado do Dispositivo Baseado no Identificador do Dispositivo**, escolha o **Tipo de identidade do dispositivo** a ser usado. O padrão é **IMEI**. Para usar esta opção, importe certificados em massa usando a API REST. Consulte Carregar certificados para dispositivos iOS em massa com a API REST. Disponível apenas quando você seleciona **Always On IKEv2**.

- **Autenticação Estendida Habilitada:** Selecione se deseja habilitar o Protocolo de Autenticação Estendida (EAP). Se você escolher **Ativado**, digite a **Conta de usuário** e a **Senha de autenticação**.
- **Intervalo de Detecção de Peer Inativo:** Escolha com que frequência um dispositivo peer é contatado para garantir que ele permaneça acessível. O padrão é **Nenhum**. As opções são:
  - **Nenhum:** Desativa a detecção de peer inativo.
  - **Baixo:** Contata o peer a cada 30 minutos.
  - **Médio:** Contata o par a cada 10 minutos.
  - **Alto:** Contata o par a cada 1 minuto.
- **Desabilitar Mobilidade e Multihoming:** Escolha se deseja desabilitar este recurso.
- **Usar atributos de sub-rede interna IPv4/IPv6:** Escolha se deseja habilitar este recurso.
- **Desabilitar redirecionamentos:** Escolha se deseja desabilitar os redirecionamentos.
- **Habilitar NAT keepalive enquanto o dispositivo está inativo:** Para os protocolos AlwaysOn. Os pacotes keepalive mantêm os mapeamentos NAT para conexões IKEv2. O chip envia esses pacotes em intervalos regulares quando o dispositivo está ativo. Se esta configuração estiver ativada, o chip envia pacotes keepalive mesmo enquanto o dispositivo está inativo. O intervalo padrão é de 20 segundos via Wi-Fi e 110 segundos via celular. Você pode alterar o intervalo usando o parâmetro de intervalo de NAT keepalive.
- **Intervalo de NAT keepalive (segundos):** O padrão é 20 segundos.
- **Habilitar Perfect Forward Secrecy:** Escolha se deseja habilitar este recurso.
- **Endereços IP do servidor DNS:** Opcional. Uma lista de strings de endereços IP do servidor DNS. Esses endereços IP podem incluir uma mistura de endereços IPv4 e IPv6. Clique em **Adicionar** para digitar um endereço.
- **Nome de domínio:** Opcional. O domínio principal do túnel.

- **Domínios de pesquisa:** Opcional. Uma lista de strings de domínio usadas para qualificar totalmente nomes de host de rótulo único.
- **Anexar domínios de correspondência suplementares à lista do resolvedor:** Opcional. Determina se a lista de domínios de correspondência suplementares deve ser adicionada à lista de domínios de pesquisa do resolvedor. O padrão é **Ativado**.
- **Domínios de correspondência suplementares:** Opcional. Uma lista de strings de domínio usadas para determinar quais consultas DNS devem usar as configurações do resolvedor DNS nos endereços do servidor DNS. Esta chave cria uma configuração de DNS dividido onde apenas os hosts em certos domínios são resolvidos usando o resolvedor DNS do túnel. Os hosts que não estão em um dos domínios desta lista são resolvidos usando o resolvedor padrão do sistema.

Se este parâmetro tiver uma string vazia, essa string será o domínio padrão. É assim que uma configuração de túnel dividido pode direcionar todas as consultas DNS para os servidores DNS da VPN antes dos servidores DNS primários. Se o túnel VPN for a rota padrão da rede, os servidores DNS listados se tornarão o resolvedor padrão. Nesse caso, a lista de domínios de correspondência suplementares é ignorada.

- **Parâmetros IKE SA** e **Parâmetros Child SA**. Configure estas definições para cada opção de parâmetros de Associação de Segurança (SA):
  - **Algoritmo de Criptografia:** Na lista, selecione o algoritmo de criptografia IKE a ser usado. O padrão é **3DES**.
  - **Algoritmo de Integridade:** Na lista, selecione o algoritmo de integridade a ser usado. O padrão é **SHA1-96**.
  - **Grupo Diffie Hellman:** Na lista, selecione o número do grupo Diffie Hellman. O padrão é **2**.
  - **Tempo de Vida do IKE em Minutos:** Digite um número inteiro entre 10 e 1440 representando o tempo de vida da SA (intervalo de nova chave). O padrão é **1440** minutos.
- **Exceções de Serviço:** Para os protocolos AlwaysOn. As exceções de serviço são serviços de sistema que estão isentos da VPN AlwaysOn. Configure estas configurações de exceções de serviço:
  - **Correio de Voz:** Na lista, selecione como manipular a exceção de correio de voz. O padrão é **Permitir tráfego via túnel**.
  - **AirPrint:** Na lista, selecione como manipular a exceção do AirPrint. O padrão é **Permitir tráfego via túnel**.

  - **Permitir tráfego de folha web cativa fora do túnel VPN:** Selecione se deseja permitir que os usuários se conectem a hotspots públicos fora do túnel VPN. O padrão é **Desativado**.
  - **Permitir tráfego de todos os aplicativos de rede cativa fora do túnel VPN:** Selecione se deseja permitir todos os aplicativos de rede de hotspot fora do túnel VPN. O padrão é **Desativado**.
  - **Identificadores de pacote de aplicativos de rede cativa:** Para cada identificador de pacote de aplicativo de rede de hotspot que os usuários têm permissão para acessar, clique em **Adicionar** e digite o **Identificador de Pacote** do aplicativo de rede de hotspot. Clique em **Salvar** para salvar o identificador de pacote do aplicativo.

- **VPN por aplicativo**. Configure estas configurações para tipos de conexão IKEv2.
  - **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**.
  - **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
  - **Domínios Safari:** Clique em **Adicionar** para adicionar um nome de domínio Safari.
- **Configuração de proxy:** Escolha como a conexão VPN é roteada através de um servidor proxy. O padrão é **Nenhum**.

Configurar protocolo Citrix SSO para iOS

O cliente Citrix SSO está disponível na Apple Store em `<https://apps.apple.com/us/app/citrix-sso/id1333396910>`.

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:

    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum.**
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **DESATIVADO.**
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **DESATIVADO.** Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda para iOS.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você definir esta opção como ATIVADO, configure as seguintes definições:
    - **Correspondência de aplicativo sob demanda habilitada:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.
    - **Tipo de provedor:** Selecione se a VPN por aplicativo é fornecida como um **proxy de aplicativo** ou como um **túnel de pacote**. O padrão é **proxy de aplicativo**.
    - **Tipo de provedor:** Defina como **Túnel de pacote**.
    - **Domínios Safari:** Para cada domínio Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
        - **Domínio:** Digite o domínio a ser adicionado.
        - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

- **XML personalizado:** Para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e especifique os pares chave/valor. Os parâmetros disponíveis são:
    - **disableL3:** Desativa a VPN no nível do sistema. Permite apenas VPN por aplicativo. Nenhum **Valor** é necessário.
    - **useragent:** Associa a esta política de dispositivo quaisquer políticas do Citrix Gateway direcionadas a clientes de plug-in VPN. Para solicitações iniciadas pelo plug-in, o **Valor** para esta chave é adicionado automaticamente ao plug-in VPN.

Configurar protocolo SSL personalizado para iOS

Para fazer a transição do cliente Cisco Legacy AnyConnect para o cliente Cisco AnyConnect:

1. Configure a política de dispositivo VPN com o protocolo SSL personalizado. Implante a política em dispositivos iOS.
2. Carregue o cliente Cisco AnyConnect de `<https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>`, adicione o aplicativo ao XenMobile e, em seguida, implante o aplicativo em dispositivos iOS.
3. Remova a política de dispositivo VPN antiga dos dispositivos iOS.

Configurações:

- **Identificador SSL personalizado (formato DNS reverso):** Defina como o identificador de pacote. Para o cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de Pacote do Provedor:** Se o aplicativo especificado em **Identificador SSL personalizado** tiver vários provedores VPN do mesmo tipo (proxy de aplicativo ou túnel de pacote), especifique este identificador de pacote. Para o cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação para esta conexão. O padrão é **Senha**.
    - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
    - Se você habilitar **Certificado**, configure estas configurações:
        - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum.**
        - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN deles quando se conectarem à rede. O padrão é **DESATIVADO.**
        - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **DESATIVADO.** Para obter informações sobre como configurar as configurações quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar as configurações de Habilitar VPN sob demanda para iOS.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você definir esta opção como ON, configure as seguintes configurações:

- **Aplicativo de correspondência sob demanda habilitado:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.
- **Tipo de Provedor:** Um tipo de provedor indica se o provedor é um serviço VPN ou um serviço de proxy. Para serviço VPN, escolha **Packet tunnel**. Para serviço de proxy, escolha **App proxy**. Para o cliente Cisco AnyConnect, escolha **Packet tunnel**.
- **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

- **XML Personalizado:** Para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do parâmetro:** Digite o nome do parâmetro a ser adicionado.
  - **Valor:** Digite o valor associado a **Nome do parâmetro**.
  - Clique em **Salvar** para salvar o parâmetro ou clique em **Cancelar** para não salvar o parâmetro.

Configurar a política de dispositivo VPN para oferecer suporte a NAC

1. O **Tipo de conexão** de **SSL Personalizado** é necessário para configurar o filtro NAC.
2. Especifique um **Nome de conexão** de **VPN**.
3. Para **Identificador SSL personalizado**, digite **com.citrix.NetScalerGateway.ios.app**
4. Para **Identificador de pacote do provedor**, digite **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Os valores nas etapas 3 e 4 vêm da instalação necessária do Citrix SSO para filtragem NAC. Você não configura uma senha de autenticação. Para obter mais informações sobre como usar a função NAC, consulte Controle de Acesso à Rede.

Configurar opções de VPN sob demanda para iOS

- **Domínio Sob Demanda:** Para cada domínio e ação associada a ser tomada quando os usuários se conectam, clique em **Adicionar** e faça o seguinte:
- **Domínio:** Digite o domínio a ser adicionado.

- **Ação:** Na lista, selecione uma das ações possíveis:
  - **Sempre estabelecer:** O domínio sempre aciona uma conexão VPN.
  - **Nunca estabelecer:** O domínio nunca aciona uma conexão VPN.
  - **Estabelecer se necessário:** O domínio aciona uma tentativa de conexão VPN se a resolução do nome de domínio falhar. A falha ocorre quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
- **Regras sob demanda**
  - **Ação:** Na lista, selecione a ação a ser tomada. O padrão é **EvaluateConnection.** As ações possíveis são:
    - **Permitir:** Permite que a VPN sob demanda se conecte quando acionada.
    - **Conectar:** Inicia incondicionalmente uma conexão VPN.
    - **Desconectar:** Remove a conexão VPN e não reconecta sob demanda enquanto a regra corresponder.
    - **EvaluateConnection:** Avalia o array ActionParameters para cada conexão.
    - **Ignorar:** Mantém qualquer conexão VPN existente ativa, mas não reconecta sob demanda enquanto a regra corresponder.
  - **DNSDomainMatch:** Para cada domínio com o qual a lista de domínios de pesquisa de um dispositivo pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
    - **Domínio DNS:** Digite o nome do domínio. Você pode usar o prefixo curinga "*" para corresponder a vários domínios. Por exemplo, *.example.com corresponde a mydomain.example.com, yourdomain.example.com e herdomain.example.com.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
  - **DNSServerAddressMatch:** Para cada endereço IP com o qual qualquer um dos servidores DNS especificados da rede pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
    - **Endereço do Servidor DNS:** Digite o endereço do servidor DNS que você deseja adicionar. Você pode usar o sufixo curinga "*" para corresponder a servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede de classe A.

    - Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar o endereço do servidor DNS.

- **InterfaceTypeMatch:** Na lista, selecione o tipo de hardware da interface de rede primária em uso. O padrão é **Não especificado**. Os valores possíveis são:
    - **Não especificado:** Corresponde a qualquer hardware de interface de rede. Esta opção é o padrão.
    - **Ethernet:** Corresponde apenas ao hardware da interface de rede Ethernet.
    - **WiFi:** Corresponde apenas ao hardware da interface de rede Wi-Fi.
    - **Celular:** Corresponde apenas ao hardware da interface de rede Celular.
- **SSIDMatch:** Para cada SSID a ser correspondido com a rede atual que você deseja adicionar, clique em **Adicionar** e faça o seguinte.
    - **SSID:** Digite o SSID a ser adicionado. Se a rede não for uma rede Wi-Fi, ou se o SSID não aparecer, a correspondência falhará. Deixe esta lista vazia para corresponder a qualquer SSID.
    - Clique em **Salvar** para salvar o SSID ou clique em **Cancelar** para não salvar o SSID.
- **URLStringProbe:** Digite um URL para buscar. Se este URL for buscado com sucesso sem redirecionamento, esta regra corresponde.
- **ActionParameters : Domains:** Para cada domínio que o EvaluateConnection verifica e que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
    - **Domain:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
- **ActionParameters : DomainAction:** Na lista, selecione o **comportamento da VPN** para os domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
    - **ConnectIfNeeded:** O domínio aciona uma tentativa de conexão VPN se a resolução do nome de domínio falhar. A falha ocorre quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
    - **NeverConnect:** O domínio nunca aciona uma conexão VPN.
- **Action Parameters: RequiredDNSServers:** Para cada endereço IP de servidor DNS a ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:

        - **DNS Server:** Válido apenas quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Este servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida em resposta. Este servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
        - Clique em **Salvar** para salvar o servidor DNS ou clique em **Cancelar** para não salvar o servidor DNS.
    - **ActionParameters : RequiredURLStringProbe:** Opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) para sondar, usando uma solicitação GET. Se o nome do host da URL não puder ser resolvido, o servidor estiver inacessível ou o servidor não responder, uma conexão VPN será estabelecida. Válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
    - **OnDemandRules : XML content:** Digite ou copie e cole as regras de configuração XML sob demanda.
        - Clique em **Verificar Dicionário** para validar o código XML. Você verá XML Válido no texto verde abaixo da caixa de texto **Conteúdo XML** se o XML for válido. Se não for válido, você verá uma mensagem de erro no texto laranja descrevendo o erro.

- **Proxy**
    - **Configuração de proxy:** Na lista, selecione como a conexão VPN é roteada por um servidor proxy. O padrão é **Nenhum**.
        - Se você habilitar **Manual**, configure estas definições:
            - **Nome do host ou endereço IP para o servidor proxy:** Digite o nome do host ou endereço IP para o servidor proxy. Este campo é obrigatório.
            - **Porta para o servidor proxy:** Digite o número da porta do servidor proxy. Este campo é obrigatório.
            - **Nome de usuário:** Digite um nome de usuário opcional para o servidor proxy.
            - **Senha:** Digite uma senha opcional para o servidor proxy.
        - Se você configurar **Automático**, configure esta definição:
            - **URL do servidor proxy:** Digite a URL para o servidor proxy. Este campo é obrigatório.

- **Configurações de Política**

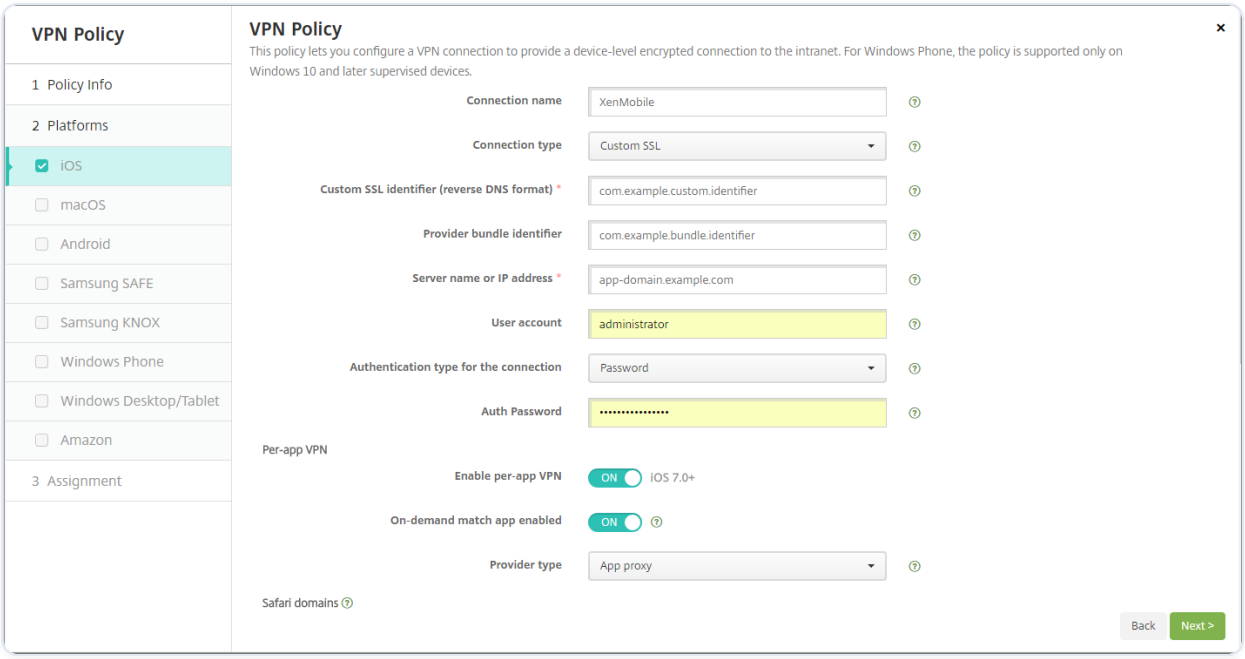
- Em **Configurações de Política**, ao lado de **Remover política**, selecione **Selecionar data** ou **Duração até a remoção (em horas)**.
- Se você selecionar **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
- Na lista **Permitir que o usuário remova a política**, selecione **Sempre**, **Senha necessária** ou **Nunca**.
- Se você selecionar **Senha necessária**, ao lado de **Senha de remoção**, digite a senha necessária.

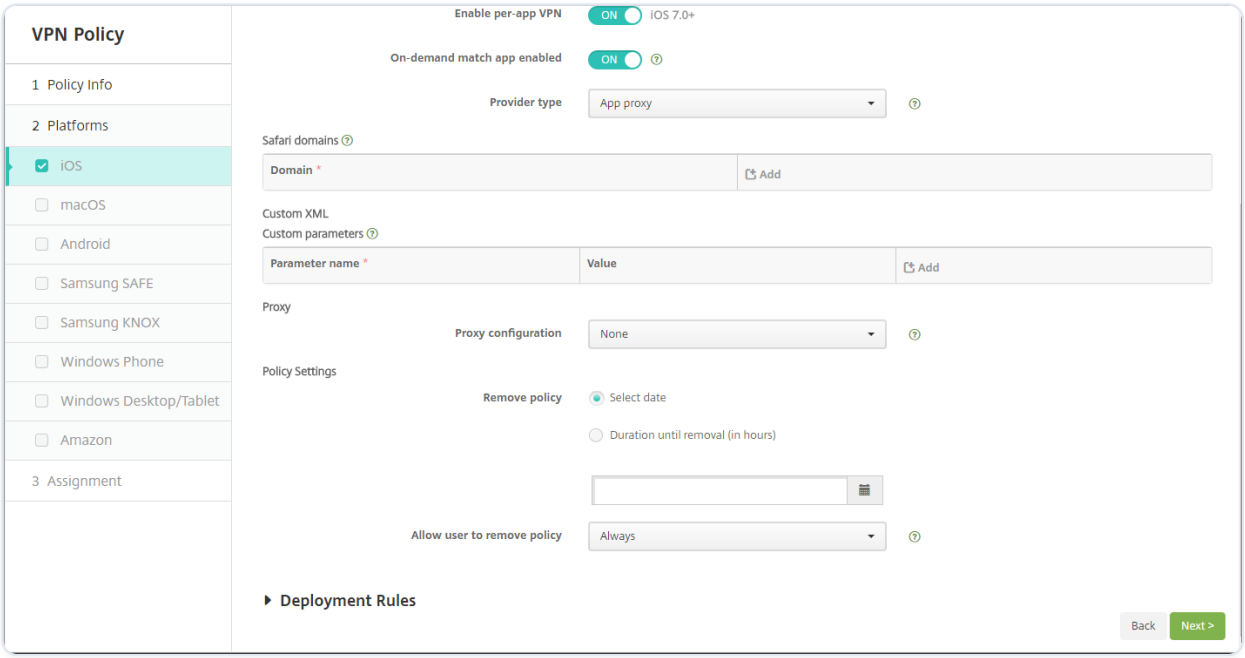
Configurar uma VPN por aplicativo

As opções de VPN por aplicativo para iOS estão disponíveis para estes tipos de conexão: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO e Custom SSL.

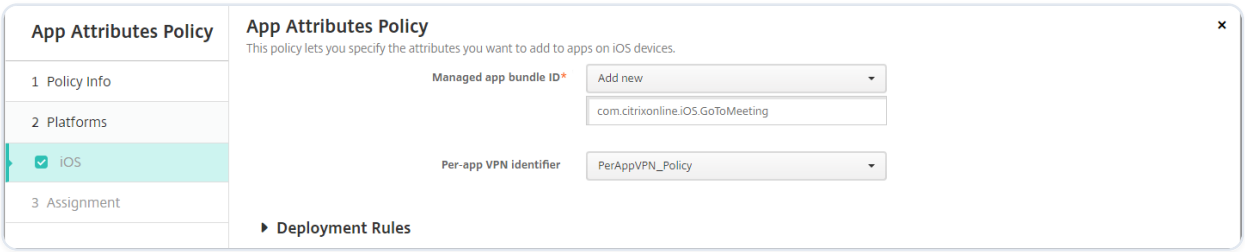
Para configurar uma VPN por aplicativo:

1. Em **Configurar > Políticas de Dispositivo**, crie uma política de VPN. Por exemplo:



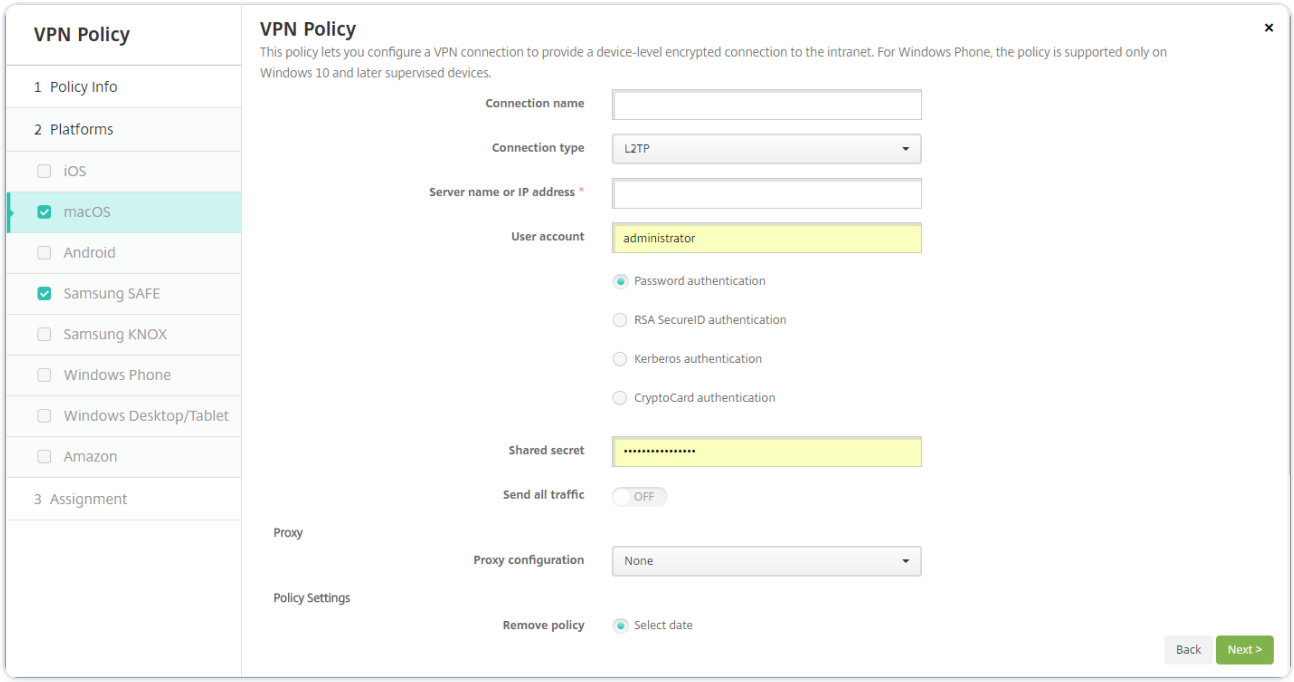


2. Em **Configurar > Políticas de Dispositivo**, crie uma política de Atributos de Aplicativo para associar um aplicativo à política de VPN por aplicativo. Para **Identificador de VPN por aplicativo**, escolha o nome da política de VPN criada na Etapa 1. Para **ID do pacote de aplicativo gerenciado**, escolha na lista de aplicativos ou digite o ID do pacote de aplicativo. (Se você implantar uma política de Inventário de Aplicativos iOS, a lista de aplicativos terá aplicativos.)



- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS



- **Nome da conexão:** Digite um nome para a conexão.
- **Tipo de conexão:** Na lista, selecione o protocolo a ser usado para esta conexão. O padrão é L2TP.
    - **L2TP:** Protocolo de Tunelamento de Camada 2 com autenticação de chave pré-compartilhada.
    - **PPTP:** Tunelamento Ponto a Ponto.
    - **IPSec:** Sua conexão VPN corporativa.
    - **Cisco AnyConnect:** Cliente VPN Cisco AnyConnect.
    - **Juniper SSL:** Cliente VPN SSL Juniper Networks.
    - **F5 SSL:** Cliente VPN SSL F5 Networks.
    - **SonicWALL Mobile Connect:** Cliente VPN unificado da Dell para iOS.
    - **Ariba VIA:** Cliente de Acesso Virtual à Internet da Ariba Networks.
    - **Citrix VPN:** Cliente VPN Citrix.
    - **SSL Personalizado:** Secure Socket Layer Personalizado.

As seções a seguir listam as opções de configuração para cada um dos tipos de conexão precedentes.

Configurar Protocolo L2TP para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- Selecione **Autenticação por senha**, **Autenticação RSA SecurID**, **Autenticação Kerberos** ou **Autenticação CryptoCard**. O padrão é **Autenticação por senha**.
- **Segredo compartilhado:** Digite a chave de segredo compartilhado IPsec.
- **Enviar todo o tráfego:** Selecione se deseja enviar todo o tráfego pela VPN. O padrão é **Desativado**.

Configurar Protocolo PPTP para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- Selecione **Autenticação por senha**, **Autenticação RSA SecurID**, **Autenticação Kerberos** ou **Autenticação CryptoCard**. O padrão é **Autenticação por senha**.
- **Nível de criptografia:** Selecione o nível de criptografia desejado. O padrão é **Nenhum**.
    - **Nenhum:** Não usar criptografia.
    - **Automático:** Use o nível de criptografia mais forte suportado pelo servidor.
    - **Máximo** (128 bits): Sempre use criptografia de 128 bits.
- **Enviar todo o tráfego:** Selecione se deseja enviar todo o tráfego pela VPN. O padrão é **Desativado**.

Configurar protocolo IPsec para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Segredo Compartilhado** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Segredo Compartilhado**.
    - Se você habilitar a autenticação por **Segredo Compartilhado**, configure estas definições:
        - **Nome do grupo:** Digite um nome de grupo opcional.

- **Segredo compartilhado:** Digite uma chave de segredo compartilhado opcional.
- **Usar autenticação híbrida:** Selecione se deseja usar autenticação híbrida. Com a autenticação híbrida, o servidor primeiro se autentica para o cliente e, em seguida, o cliente se autentica para o servidor. O padrão é **Desativado**.
- **Solicitar senha:** Selecione se deseja solicitar as senhas dos usuários quando eles se conectarem à rede. O padrão é **Desativado**.

- Se você habilitar a autenticação por **Certificado**, configure estas definições:
  - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
  - **Solicitar PIN ao conectar:** Selecione se deseja exigir que os usuários insiram seu PIN ao se conectar à rede. O padrão é **Desativado**.
  - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar opções de Habilitar VPN sob demanda.

Configurar protocolo Cisco AnyConnect para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Grupo:** Digite um nome de grupo opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para

obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar opções de Habilitar VPN sob demanda.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
  - **Aplicativo de correspondência sob demanda habilitado:** Selecione se uma conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
  - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o protocolo Juniper SSL para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Realm:** Digite um nome de realm opcional.
- **Função:** Digite um nome de função opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar o PIN aos usuários quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob**

demanda estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure as seguintes definições:
  - **Correspondência de aplicativo sob demanda habilitada:** Selecione se uma conexão VPN por aplicativo é acionada automaticamente quando aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
  - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o Protocolo SSL F5 para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda.

- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
  - **Aplicativo de correspondência sob demanda habilitado:** Selecione se a conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
  - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o protocolo SonicWALL Mobile Connect para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Grupo de logon ou domínio:** Digite um grupo de logon ou domínio opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:

- **Aplicativo de correspondência sob demanda habilitado:** Selecione se a conexão VPN por aplicativo é acionada automaticamente quando aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.
- **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar o protocolo Ariba VIA para macOS

- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou o endereço IP para o servidor VPN.
- **Conta de usuário:** Digite uma conta de usuário opcional.
- **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar aos usuários o PIN quando eles se conectarem à rede. O padrão é **Desativado**.
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Desativado**. Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
  - **Correspondência de aplicativo sob demanda habilitada:** Selecione se a conexão VPN por aplicativo é acionada automaticamente quando aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede. O padrão é **Desativado**.

- **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar protocolo SSL personalizado para macOS

- **Identificador SSL personalizado (formato DNS reverso):** Digite o identificador SSL no formato DNS reverso. Este campo é obrigatório.
- **Nome do servidor ou endereço IP:** Digite o nome do servidor ou endereço IP para o servidor VPN. Este campo é obrigatório.
- **Conta de usuário:** Digite uma conta de usuário opcional.
  - **Tipo de autenticação para a conexão:** Na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação desta conexão. O padrão é **Senha**.
  - Se você habilitar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você habilitar **Certificado**, configure estas definições:
    - **Credencial de identidade:** Na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum.**
    - **Solicitar PIN ao conectar:** Selecione se deseja solicitar o PIN aos usuários quando eles se conectarem à rede. O padrão é **DESATIVADO.**
    - **Habilitar VPN sob demanda:** Selecione se deseja habilitar o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **DESATIVADO.** Para obter informações sobre como configurar as definições quando **Habilitar VPN sob demanda** estiver **Ativado**, consulte Configurar definições de Habilitar VPN sob demanda.
  - **VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. O padrão é **Desativado**. Se você habilitar esta opção, configure estas definições:
    - **Correspondência de aplicativo sob demanda habilitada:** Selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço VPN por aplicativo iniciam a comunicação de rede.

    - **Domínios do Safari:** Para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
        - **Domínio:** Digite o domínio a ser adicionado.
        - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

- **XML personalizado:** Para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
    - **Nome do parâmetro:** Digite o nome do parâmetro a ser adicionado.
    - **Valor:** Digite o valor associado a **Nome do parâmetro**.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

Configurar opções de VPN sob demanda

- **Domínio Sob Demanda:** Para cada domínio e ação associada a ser tomada quando os usuários se conectarem a eles que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
    - **Domínio:** Digite o domínio a ser adicionado.
    - **Ação:** Na lista, selecione uma das ações possíveis:
        - **Sempre estabelecer:** O domínio sempre aciona uma conexão VPN.
        - **Nunca estabelecer:** O domínio nunca aciona uma conexão VPN.
        - **Estabelecer se necessário:** O domínio aciona uma tentativa de conexão VPN se a resolução do nome de domínio falhar. A falha ocorre quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
- **Regras sob demanda**
    - **Ação:** Na lista, selecione a ação a ser tomada. O padrão é **EvaluateConnection.** As ações possíveis são:
        - **Permitir:** Permitir que a VPN sob demanda se conecte quando acionada.
        - **Conectar:** Iniciar incondicionalmente uma conexão VPN.

- **Desconectar:** Remover a conexão VPN e não reconectar sob demanda enquanto a regra corresponder.
- **EvaluateConnection:** Avaliar o array **ActionParameters** para cada conexão.
- **Ignorar:** Mantenha qualquer conexão VPN existente ativa, mas não reconecte sob demanda enquanto a regra corresponder.

- **DNSDomainMatch:** Para cada domínio com o qual a lista de domínios de pesquisa de um dispositivo de usuário pode corresponder e que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Domínio DNS:** Digite o nome do domínio. Você pode usar o prefixo curinga "*" para corresponder a vários domínios. Por exemplo, *.example.com corresponde a mydomain.example.com, yourdomain.example.com e herdomain.example.com.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
- **DNSServerAddressMatch:** Para cada endereço IP com o qual qualquer um dos servidores DNS especificados da rede pode corresponder e que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Endereço do Servidor DNS:** Digite o endereço do servidor DNS que você deseja adicionar. Você pode usar o sufixo curinga "*" para corresponder a servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede de classe A.
  - Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar o endereço do servidor DNS.
- **InterfaceTypeMatch:** Na lista, clique no tipo de hardware da interface de rede primária em uso. O padrão é **Não especificado**. Os valores possíveis são:
  - **Não especificado:** Corresponde a qualquer hardware de interface de rede. Esta opção é o padrão.
  - **Ethernet:** Corresponde apenas a hardware de interface de rede Ethernet.
  - **Wi-Fi:** Corresponde apenas a hardware de interface de rede Wi-Fi.
  - **Celular:** Corresponde apenas a hardware de interface de rede celular.
- **SSIDMatch:** Para cada SSID a ser correspondido com a rede atual que você deseja adicionar, clique em **Adicionar** e faça o seguinte.

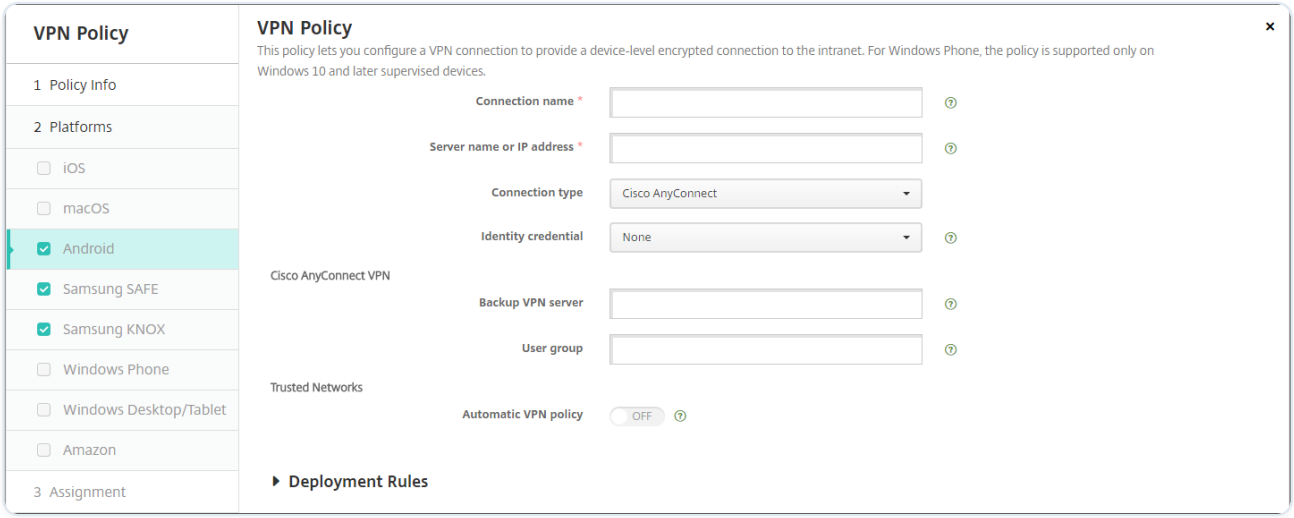
- **SSID:** Digite o SSID a ser adicionado. Se a rede não for uma rede Wi-Fi, ou se o SSID não aparecer, a correspondência falhará. Deixe esta lista vazia para corresponder a qualquer SSID.
- Clique em **Salvar** para salvar o SSID ou clique em **Cancelar** para não salvar o SSID.

- **URLStringProbe:** Digite uma URL para buscar. Se esta URL for buscada com sucesso sem redirecionamento, esta regra corresponde.
- **ActionParameters : Domains:** Para cada domínio que EvaluateConnection verifica e que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Domain:** Digite o domínio a ser adicionado.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.
- **ActionParameters : DomainAction:** Na lista, selecione o **comportamento da VPN** para os domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
  - **ConnectIfNeeded:** O domínio aciona uma tentativa de conexão VPN se a resolução do nome de domínio falhar. A falha ocorre quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
  - **NeverConnect:** O domínio nunca aciona uma conexão VPN.
- **Action Parameters: RequiredDNSServers:** Para cada endereço IP de servidor DNS a ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:
  - **DNS Server:** Válido apenas quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Este servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida em resposta. Este servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
  - Clique em **Salvar** para salvar o servidor DNS ou clique em **Cancelar** para não salvar o servidor DNS.
- **ActionParameters : RequiredURLStringProbe:** Opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) para sondar, usando uma solicitação GET. Se o nome do host da URL não puder ser resolvido, o servidor estiver inacessível ou o servidor não responder, uma conexão VPN será estabelecida. Válido apenas quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.

- **OnDemandRules : XML content:** Digite, ou copie e cole, regras XML de configuração sob demanda.
  - Clique em **Verificar Dicionário** para validar o código XML. Você verá XML Válido no texto verde abaixo da caixa de texto **Conteúdo XML** se o XML for válido. Se não for válido, você verá uma mensagem de erro no texto laranja descrevendo o erro.

- **Proxy**
  - **Proxy configuration:** Na lista, selecione como a conexão VPN é roteada através de um servidor proxy. O padrão é **Nenhum**.
    - Se você habilitar **Manual**, configure estas definições:
      - **Nome do host ou endereço IP para o servidor proxy:** Digite o nome do host ou endereço IP para o servidor proxy. Este campo é obrigatório.
      - **Porta para o servidor proxy:** Digite o número da porta do servidor proxy. Este campo é obrigatório.
      - **Nome de usuário:** Digite um nome de usuário opcional para o servidor proxy.
      - **Senha:** Digite uma senha opcional para o servidor proxy.
    - Se você configurar **Automático**, configure esta definição:
      - **URL do servidor proxy:** Digite a URL para o servidor proxy. Este campo é obrigatório.

Configurações do Android



Configurar o protocolo VPN Cisco AnyConnect para Android

- **Nome da conexão:** Digite um nome para a conexão VPN Cisco AnyConnect. Este campo é obrigatório.
- **Nome do servidor ou endereço IP:** Digite o nome ou endereço IP do servidor VPN. Este campo é obrigatório.
- **Credencial de identidade:** Na lista, selecione uma credencial de identidade.
- **Servidor VPN de backup:** Digite as informações do servidor VPN de backup.
- **Grupo de usuários:** Digite as informações do grupo de usuários.
- **Redes Confiáveis**
    - **Política de VPN automática:** Ative ou desative esta opção para definir como a VPN reage a redes confiáveis e não confiáveis. Se ativada, configure estas definições:
        - **Política de rede confiável:** Na lista, selecione a política desejada. O padrão é **Desconectar**. As opções possíveis são:
            - **Desconectar:** O cliente encerra a conexão VPN na rede confiável. Esta configuração é a padrão.
            - **Conectar:** O cliente inicia uma conexão VPN na rede confiável.
            - **Não fazer nada:** O cliente não executa nenhuma ação.
            - **Pausar:** Quando um usuário estabelece uma sessão VPN fora da rede confiável e depois entra em uma rede configurada como confiável, a sessão VPN é suspensa. Quando o usuário sai da rede confiável novamente, a sessão é retomada. Esta configuração elimina a necessidade de estabelecer uma nova sessão VPN após sair de uma rede confiável.
        - **Política de rede não confiável:** Na lista, selecione a política desejada. O padrão é **Conectar**. As opções possíveis são:
            - **Conectar:** O cliente inicia uma conexão VPN na rede não confiável.
            - **Não fazer nada:** O cliente inicia uma conexão VPN na rede não confiável. Esta opção desativa a VPN sempre ativa.
    - **Domínios confiáveis:** Para cada sufixo de domínio que a interface de rede possui quando o cliente está na rede confiável, clique em **Adicionar** para fazer o seguinte:
        - **Domínio:** Digite o domínio a ser adicionado.

    - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar o domínio.

- **Servidores confiáveis:** Para cada endereço de servidor que uma interface de rede possui quando o cliente está na rede confiável, clique em **Adicionar** e faça o seguinte:
    - **Servidores:** Digite o servidor a ser adicionado.
    - Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar o servidor.

Configurar o protocolo Citrix SSO para Android

- **Nome da conexão:** Digite um nome para a conexão VPN. Este campo é obrigatório.
- **Nome do servidor ou endereço IP:** Digite o FQDN ou o endereço IP do Citrix Gateway.
- **Tipo de autenticação para a conexão:** Escolha um tipo de autenticação e preencha qualquer um desses campos que apareçam para o tipo:
    - **Nome de usuário** e **Senha:** Digite suas credenciais VPN para os **Tipos de autenticação** de **Senha** ou **Senha e Certificado**. Opcional. Se você não fornecer as credenciais VPN, o aplicativo Citrix VPN solicitará um nome de usuário e senha.
    - **Credencial de identidade:** Aparece para os **Tipos de autenticação** de **Certificado** ou **Senha e Certificado**. Na lista, selecione uma credencial de identidade.
- **Habilitar VPN por aplicativo:** Selecione se deseja habilitar a VPN por aplicativo. Se você não habilitar uma VPN por aplicativo, todo o tráfego passará pelo túnel VPN do Citrix. Se você habilitar uma VPN por aplicativo, especifique as seguintes configurações. O padrão é **Desativado**.
    - **Lista de permissões** ou **Lista de bloqueios:** Se **Lista de permissões**, todos os aplicativos permitidos tunelam por esta VPN. Se **Lista de bloqueios**, todos os aplicativos, exceto aqueles na lista de bloqueios, tunelam por esta VPN.

      > **Nota:**
      >
      > O console do XenMobile® Server inclui os termos "blacklist" e "whitelist". Estamos alterando esses termos em uma próxima versão para "block list" e "allow list".

    - **Lista de Aplicativos:** Especifique os aplicativos permitidos ou bloqueados. Clique em **Adicionar** e digite uma lista de nomes de pacotes de aplicativos separados por vírgulas.

- **XML Personalizado:** Clique em **Adicionar** e digite os parâmetros personalizados. O XenMobile oferece suporte a esses parâmetros para Citrix VPN:
  - **DisableUserProfiles:** Opcional. Para habilitar este parâmetro, digite **Sim** para o **Valor**. Se habilitado, o XenMobile não exibe conexões VPN adicionadas pelo usuário e o usuário não pode adicionar uma conexão. Esta configuração é uma restrição global e se aplica a todos os perfis VPN.
  - **userAgent:** Um valor de string. Você pode especificar uma string de User Agent personalizada para enviar em cada solicitação HTTP. A string de user agent especificada é anexada ao user agent VPN Citrix existente.

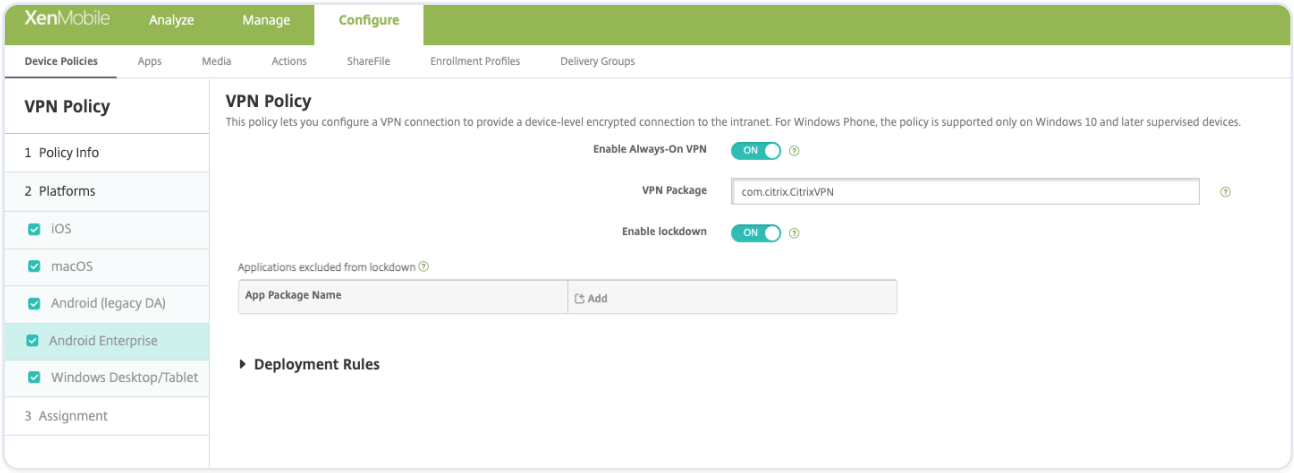
Configurar VPNs para oferecer suporte a NAC

1. Use o **Tipo de conexão SSL personalizado** para configurar o filtro NAC.
2. Especifique um **Nome de conexão** de **VPN**.
3. Para **XML personalizado**, clique em **Adicionar** e faça o seguinte:
   - **Nome do parâmetro:** Digite **XenMobileDeviceId**. Este campo é o ID do dispositivo a ser usado para a verificação NAC com base no registro do dispositivo no XenMobile. Se o XenMobile registrar e gerenciar o dispositivo, a conexão VPN será permitida. Caso contrário, a autenticação será negada no momento do estabelecimento da VPN.
   - **Valor:** Digite **DeviceID_${device.id}**, que é o valor para o parâmetro **XenMobileDeviceId**.
   - Clique em **Salvar** para salvar o parâmetro.

Configurar VPNs para Android Enterprise

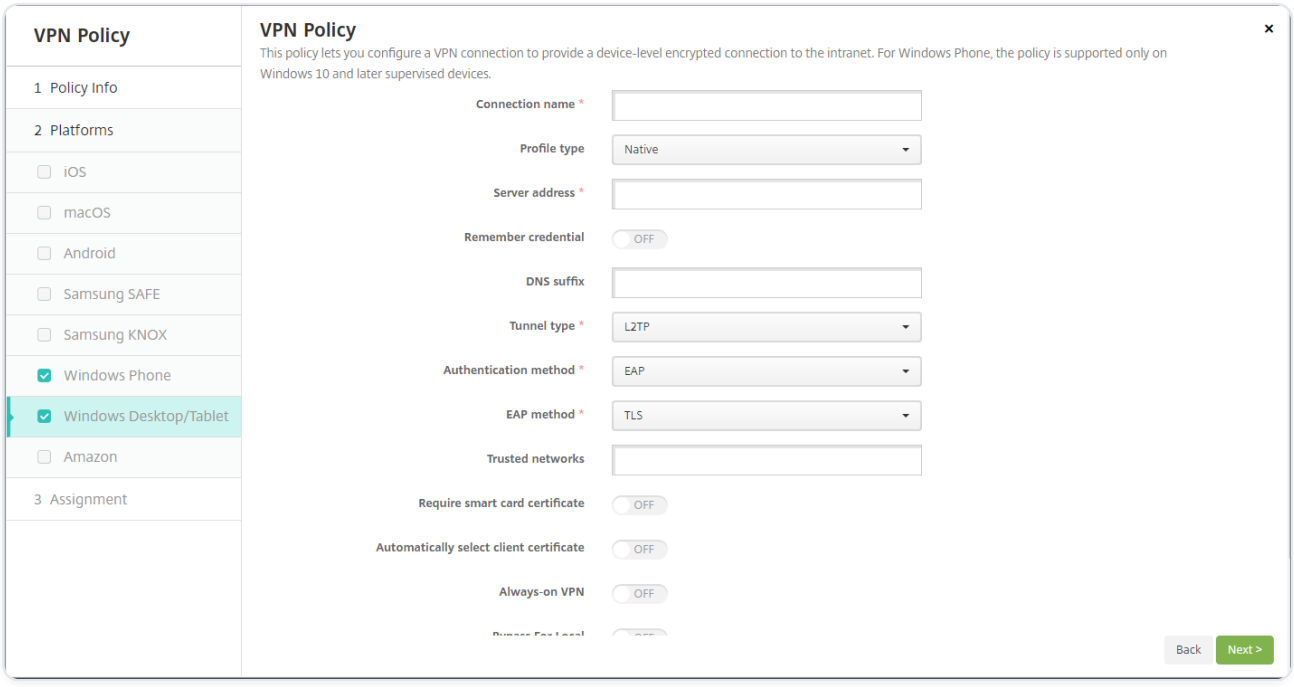
Para configurar VPNs para dispositivos Android Enterprise, crie uma política de dispositivo de configuração gerenciada para o aplicativo Citrix SSO. Consulte Configurar perfis VPN para Android Enterprise.

Configurações do Android Enterprise



- **Habilitar VPN Sempre Ativa:** Selecione se a VPN está sempre ativa. O padrão é **Desativado**. Quando habilitada, a conexão VPN permanece ativa até que o usuário a desconecte manualmente.
- **Pacote VPN:** Digite o nome do pacote para o aplicativo VPN que os dispositivos usam.
- **Habilitar bloqueio:** Se desabilitado, nenhum aplicativo pode acessar a rede se uma conexão VPN não existir. Se habilitado, os aplicativos que você configurar na seguinte configuração podem acessar a rede, mesmo que uma conexão VPN não exista. Disponível para dispositivos Android 10 e posteriores.
- **Aplicativos excluídos do bloqueio:** Clique em **Adicionar** para digitar os nomes de pacote dos aplicativos que você deseja que ignorem a configuração de bloqueio.

Configurações de Desktop/Tablet Windows



- **Nome da conexão:** Insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil:** Na lista, selecione **Nativo** ou **Plugin**. O padrão é **Nativo**.
- **Configurar tipo de perfil Nativo:** Essas configurações se aplicam à VPN integrada aos dispositivos Windows dos usuários.
    - **Endereço do servidor:** Digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
    - **Lembrar credencial:** Selecione se deseja armazenar em cache a credencial. O padrão é **Desativado**. Quando ativado, as credenciais são armazenadas em cache sempre que possível.
    - **Sufixo DNS:** Digite o sufixo DNS.
    - **Tipo de túnel:** Na lista, selecione o tipo de túnel VPN a ser usado. O padrão é **L2TP**. As opções possíveis são:
        - **L2TP:** Protocolo de Tunelamento de Camada 2 com autenticação de chave pré-compartilhada.
        - **PPTP:** Tunelamento Ponto a Ponto.
        - **IKEv2:** Troca de Chaves da Internet versão 2.
    - **Método de autenticação:** Na lista, selecione o método de autenticação a ser usado. O padrão é **EAP**. As opções possíveis são:
        - **EAP:** Protocolo de Autenticação Estendida.
        - **MSChapV2:** Use a autenticação Challenge-Handshake da Microsoft para autenticação mútua. Esta opção não está disponível quando você seleciona **IKEv2** para o tipo de túnel.
    - **Método EAP:** Na lista, selecione o método EAP a ser usado. O padrão é **TLS**. Este campo não está disponível quando a autenticação MSChapV2 está ativada. As opções possíveis são:
        - **TLS:** Segurança da Camada de Transporte
        - **PEAP:** Protocolo de Autenticação Extensível Protegido
    - **Redes confiáveis:** Digite uma lista de redes separadas por vírgulas que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estão na rede sem fio da sua empresa, eles podem acessar recursos protegidos diretamente.

- **Exigir certificado de cartão inteligente:** Selecione se deseja exigir um certificado de cartão inteligente. O padrão é **Desativado**.
- **Selecionar certificado de cliente automaticamente:** Selecione se deseja escolher automaticamente o certificado de cliente a ser usado para autenticação. O padrão é **Desativado**. Esta opção não está disponível quando você ativa **Exigir certificado de cartão inteligente**.
- **VPN sempre ativa:** Selecione se a VPN está sempre ativa. O padrão é **Desativado**. Quando ativada, a conexão VPN permanece ativa até que o usuário a desconecte manualmente.
- **Ignorar para local:** Digite o endereço e o número da porta para permitir que recursos locais ignorem o servidor proxy.

- **Configurar tipo de perfil de plug-in:** Essas configurações se aplicam a plug-ins VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
  - **Endereço do servidor:** Digite o FQDN ou endereço IP do servidor VPN. Este campo é obrigatório.
  - **Lembrar credencial:** Selecione se deseja armazenar em cache a credencial. O padrão é **Desativado**. Quando ativada, as credenciais são armazenadas em cache sempre que possível.
  - **Sufixo DNS:** Digite o sufixo DNS.
  - **ID do aplicativo cliente:** Digite o nome da família do pacote para o plug-in VPN.
  - **XML do perfil do plug-in:** Selecione o perfil de plug-in VPN personalizado a ser usado clicando em **Procurar** e navegando até o local do arquivo. Entre em contato com o provedor do plug-in para obter o formato e os detalhes.
  - **Redes confiáveis:** Digite uma lista de redes separadas por vírgulas que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estão na rede sem fio da sua empresa, eles podem acessar recursos protegidos diretamente.
  - **VPN Sempre Ativa:** Selecione se a VPN está sempre ativa. O padrão é **Desativado**. Quando ativada, a conexão VPN permanece ativa até que o usuário a desconecte manualmente.
  - **Ignorar para Local:** Digite o endereço e o número da porta para permitir que recursos locais ignorem o servidor proxy.

Política de dispositivo de papel de parede

Você pode adicionar um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio, tela inicial ou em ambas de um dispositivo iOS. Disponível no iOS 7.1.2 e posterior apenas para dispositivos supervisionados. Para usar papéis de parede diferentes em iPads e iPhones, você precisa criar políticas de papel de parede diferentes e implantá-las para os usuários apropriados.

A tabela a seguir lista as dimensões de imagem recomendadas pela Apple para dispositivos iOS.

iPhone

DISPOSITIVO	DIMENSÕES DA IMAGEM EM PIXELS
iPhone 12 Pro Max	2778 x 1284
iPhone 12 e iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2nd Gen	1334 x 750
iPhone 7 PLus, 8 PLus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

DISPOSITIVO	DIMENSÕES DA IMAGEM EM PIXELS
iPad Pro (1ª, 2ª e 3ª geração 12,9")	2732 x 2048
iPad Pro de 10,5 polegadas	2224 x 1668
iPad Pro (9,7 polegadas)	1536 x 2048
iPad Air 2	2048 x 1536

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Aplicar a:** Na lista, selecione **Tela de bloqueio**, **Tela inicial (lista de ícones)** ou **Telas de bloqueio e inicial** para definir onde o papel de parede deve aparecer.
- **Arquivo de papel de parede:** Selecione o arquivo de papel de parede clicando em **Procurar** e navegando até o local do arquivo.

Política de dispositivo de filtro de conteúdo da web

Você pode adicionar uma política de dispositivo no XenMobile para filtrar conteúdo da web em dispositivos iOS usando a função de filtro automático da Apple com sites específicos que você adiciona às listas de permissão e bloqueio. Esta política está disponível apenas em dispositivos iOS 7.0 e posteriores no modo Supervisionado. Para obter informações sobre como colocar um dispositivo iOS no modo Supervisionado, consulte Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator.

Nota:

- Dispositivos Android não suportam filtragem de conteúdo da web.
- A partir da versão 16.5 do iOS e posteriores, a política de dispositivo de Filtro de Conteúdo da Web para de reconhecer `https://localhost` na lista de permissões. Esse problema faz com que alguns aplicativos se tornem sem resposta. Além disso,

> adicionar um derivado da URL, como `http://localhost:`, `http://localhost:*`, e assim por diante, à lista de permissões não resolve o problema.

> Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Tipo de filtro:** Clique em **Integrado** ou **Plug-in** na lista suspensa e, em seguida, siga os procedimentos para a opção escolhida. O padrão é **Integrado**.

Tipo de filtro integrado

- **Filtro de Conteúdo da Web**
  - **Filtro automático ativado:** Se deve usar a função de filtro automático da Apple para analisar sites em busca de conteúdo inadequado. O padrão é **Desativado**.
  - **URLs permitidas:** Esta lista é ignorada quando **Filtro automático ativado** está definido como **Desativado**. Quando **Filtro automático ativado** está definido como **Ativado**, os itens nesta lista estão sempre acessíveis, independentemente de o filtro automático permitir o acesso ou não. Para cada URL que você deseja adicionar à lista de permissões, clique em **Adicionar** e faça o seguinte:
    - Digite a URL do site permitido. Você deve adicionar `http://` ou `https://` antes do endereço da web.
    - Clique em **Salvar** para salvar o site na lista de permissões ou clique em **Cancelar** para não salvá-lo.
  - **URLs na lista negra:** Os itens nesta lista são sempre bloqueados. Para cada URL que você deseja adicionar à lista de bloqueio, clique em **Adicionar** e faça o seguinte:
    - Insira o URL do site a ser bloqueado. Você deve adicionar `http://` ou `https://` antes do endereço da web.
    - Clique em **Salvar** para salvar o site na lista de bloqueio ou clique em **Cancelar** para não salvá-lo.

      > **Nota:**

> O console do XenMobile® Server inclui os termos "blacklist" e "whitelist". Estamos alterando esses termos em uma próxima versão para "lista de bloqueio" e "lista de permissão".

- **Lista de permissão de favoritos**
  - **Lista de Permissão de Favoritos:** Especifica os sites que os usuários podem acessar. Para habilitar o acesso a sites, adicione seus URLs.
    - **URL:** O URL de cada site que os usuários podem acessar. Por exemplo, para habilitar o acesso à loja Secure Hub, adicione o URL do XenMobile Server à lista de **URLs**. Você deve adicionar `http://` ou `https://` antes do endereço da web. Este campo é obrigatório.
    - **Pasta de favoritos:** Insira um nome opcional para a pasta de favoritos. Se este campo for deixado em branco, o favorito será adicionado ao diretório de favoritos padrão.
    - **Título:** Insira um título descritivo para o site. Por exemplo, digite "Google" para o URL `https://google.com`.
    - Clique em **Salvar** para salvar o site na lista de permissão ou clique em **Cancelar** para não salvá-lo.

Tipo de filtro de plug-in

- **Nome do filtro:** Insira um nome exclusivo para o filtro.
- **Identificador:** Insira o ID do pacote do plug-in que fornece o serviço de filtragem.
- **Endereço do serviço:** Insira um endereço de servidor opcional. Os formatos válidos são endereço IP, nome do host ou URL.
- **Nome de usuário:** Insira um nome de usuário opcional para o serviço.
- **Senha:** Insira uma senha opcional para o serviço.
- **Certificado:** Clique em um certificado de identidade opcional na lista suspensa que deve ser usado para autenticar o usuário no serviço. O padrão é **Nenhum**.
- **Filtrar tráfego WebKit:** Selecione se deseja filtrar o tráfego WebKit.
- **Filtrar tráfego de soquete:** Selecione se deseja filtrar o tráfego de soquete.
- **Dados Personalizados:** Para cada chave personalizada que você deseja adicionar ao filtro da web, clique em **Adicionar** e, em seguida, faça o seguinte:
  - **Chave:** Digite a chave personalizada.

    - **Valor:** Digite um valor para a chave personalizada.
    - Clique em **Salvar** para salvar a chave personalizada ou clique em **Cancelar** para não salvá-la.

- **Configurações da política**
    - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
        - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
        - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de web clip

Você pode colocar atalhos, ou web clips, para sites para aparecerem junto com aplicativos nos dispositivos dos usuários. Você pode especificar seus próprios ícones para representar os web clips para dispositivos iOS, iPadOS, macOS e Android. O tablet Windows requer apenas um rótulo e uma URL. Para dispositivos iOS e iPadOS, configure a política de dispositivo de layout da tela inicial para organizar os web clips que você criar. Se você restringir o acesso a aplicativos no iOS, certifique-se de configurar a política de dispositivo de restrição para permitir web clips. Para obter informações sobre como configurar essas políticas, consulte Política de dispositivo de layout da tela inicial e Política de dispositivo de restrições.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS

- **Rótulo:** Digite o rótulo que deve aparecer com o web clip.
- **URL:** Digite a URL associada ao web clip. A URL deve começar com um protocolo, por exemplo, `https://server`.
- **Removível:** Selecione se os usuários podem remover o web clip. O padrão é **Desativado**. Esta opção não é suportada em iPads compartilhados.
- **Ícone a ser atualizado:** Selecione o ícone a ser usado para o web clip clicando em **Procurar** e navegando até o local do arquivo.
- **Ícone pré-composto:** Selecione se o ícone tem efeitos (cantos arredondados, sombra projetada e brilho reflexivo) aplicados a ele. O padrão é **Desativado**, o que adiciona os efeitos.

- **Tela cheia:** Selecione se a página da web vinculada é aberta em modo de tela cheia. O padrão é **Desativado**.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
  - **Escopo do perfil:** Selecione se a política se aplica a um Usuário ou a um Sistema inteiro. O valor padrão é **Sistema**. Disponível apenas para iOS 9.3 e posterior.

Configurações do macOS

- **Rótulo:** Digite o rótulo que deve aparecer com o web clip.
- **URL:** Digite a URL associada ao web clip. A URL deve começar com um protocolo, por exemplo, `https://server`.
- **Ícone a ser atualizado:** Selecione o ícone a ser usado para o web clip clicando em Procurar e navegando até o local do arquivo.

Configurações do Android

- **Regra:** Selecione se esta política adiciona ou remove um web clip. O padrão é **Adicionar**.
- **Rótulo:** Digite o rótulo que deve aparecer com o web clip.
- **URL:** Digite a URL associada ao web clip.
- **Definir um ícone:** Selecione se deseja usar um arquivo de ícone. O padrão é **Desativado**.
- **Arquivo de ícone:** Se **Definir um ícone** estiver **Ativado**, selecione o arquivo de ícone a ser usado clicando em **Procurar** e navegando até o local do arquivo.
- **Configurações da política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.

    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra.

- **Permitir que o usuário remova a política:** Você pode selecionar quando os usuários podem remover a política de seus dispositivos. Selecione **Sempre**, **Senha necessária** ou **Nunca** no menu. Se você selecionar **Senha necessária**, digite uma senha no campo **Senha de remoção**.
- **Escopo do perfil:** Selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no macOS 10.7 e posterior.

Configurações de Desktop/Tablet Windows

- **Nome:** Digite o rótulo que deve aparecer com o web clip.
- **URL:** Digite o URL associado ao web clip.

Política de dispositivo Wi-Fi

Você cria novas ou edita políticas de dispositivo Wi-Fi existentes no XenMobile® usando a página **Configurar > Políticas de Dispositivo**. As políticas de Wi-Fi permitem que você gerencie como os usuários conectam seus dispositivos a redes Wi-Fi, definindo os seguintes itens:

- Nomes e tipos de rede
- Políticas de autenticação e segurança
- Uso de servidor proxy
- Outros detalhes relacionados ao Wi-Fi

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

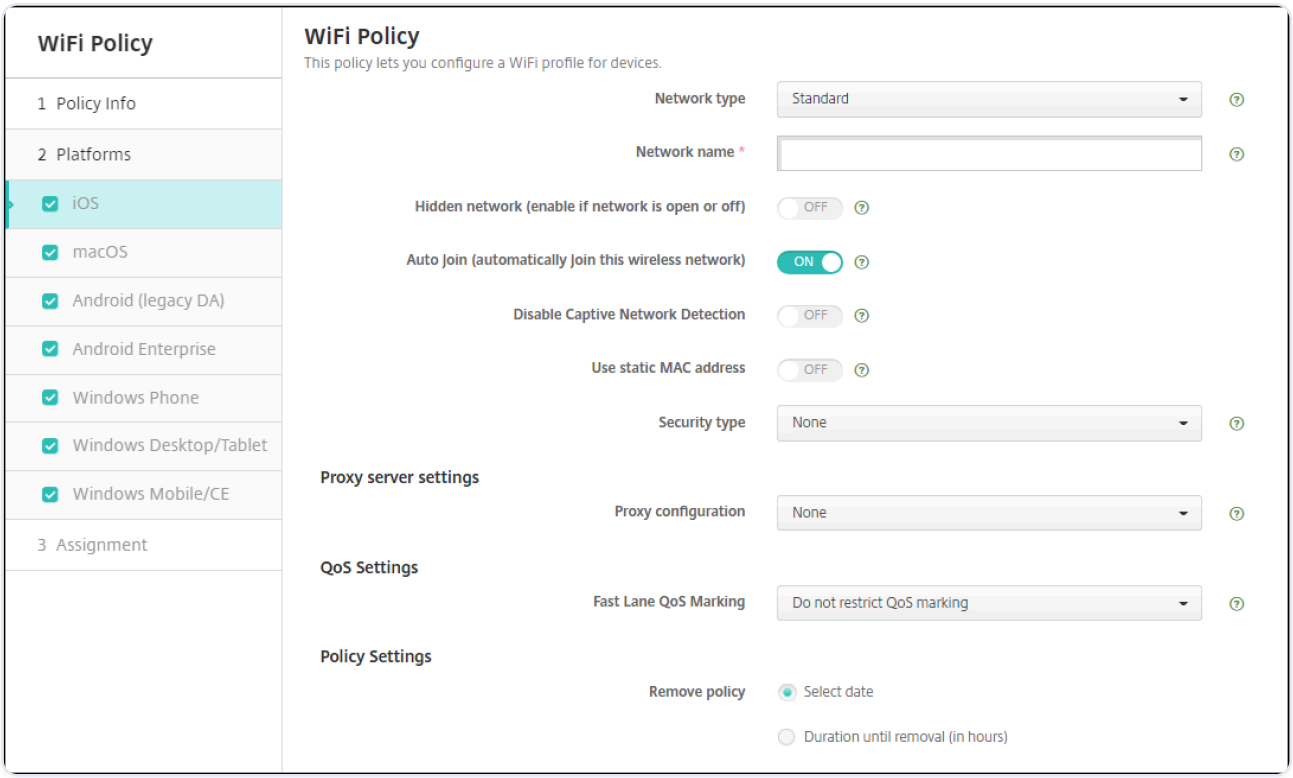
Antes de criar uma política, certifique-se de concluir estas etapas:

- Crie todos os grupos de entrega que você planeja usar.
- Conheça o nome e o tipo da rede.
- Conheça todos os tipos de autenticação ou segurança que você planeja usar.
- Conheça todas as informações de servidor proxy que você possa precisar.
- Instale todos os certificados CA necessários.

- Tenha todas as chaves compartilhadas necessárias.
- Criar a entidade PKI para autenticação baseada em certificado.
- Configurar provedores de credenciais.

Para obter mais informações, consulte Autenticação e seus subartigos.

Configurações do iOS



- **Tipo de rede:** Na lista, escolha **Padrão**, **Hotspot Legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da Rede:** Digite o SSID que é visto na lista de redes disponíveis para o dispositivo. Não se aplica a **Hotspot 2.0**.
- **Rede oculta (ativar se a rede estiver aberta ou desativada):** Escolha se a rede está oculta.
- **Entrar Automaticamente (entrar automaticamente nesta rede sem fio):** Escolha se a rede é conectada automaticamente. Se um dispositivo iOS já estiver conectado a outra rede, ele não se conectará a esta rede. O usuário deve desconectar-se da rede anterior antes que o dispositivo se conecte automaticamente. O padrão é **Ativado**.
- **Usar endereço MAC estático:** Endereços MAC são identificadores únicos que um dispositivo transmite dentro de uma rede. Para aumentar a privacidade, dispositivos iOS e iPadOS podem usar um endereço MAC diferente a cada vez que se conectam a uma rede. Se **Ativado**, o dispositivo sempre usa o mesmo endereço MAC ao se conectar a esta rede. Se **Desativado**, o

dispositivo usa um endereço MAC diferente a cada vez que se conecta a esta rede. O padrão é **Desativado**.

- **Tipo de segurança:** Na lista, escolha o tipo de segurança que você planeja usar. Não se aplica a **Hotspot 2.0**.
  - Nenhum - Não requer configuração adicional.
  - WEP
  - WPA/WPA2 Pessoal
  - Qualquer (Pessoal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise: O uso de WPA-2 Enterprise exige que você configure o Simple Certificate Enrollment Protocol (SCEP). O XenMobile pode então enviar o certificado para os dispositivos para autenticar ao servidor Wi-Fi. Para configurar o SCEP, vá para a página Distribuição em **Configurações > Provedores de Credenciais**. Para obter mais informações, consulte Provedores de credenciais.
  - Qualquer (Enterprise)

As seções a seguir listam as opções que você configura para cada um dos tipos de conexão precedentes.

Configurações de WPA, WPA Pessoal, Qualquer (Pessoal) para iOS

Senha: Digite uma senha opcional. Se você deixar este campo em branco, os usuários poderão ser solicitados a inserir suas senhas ao fazer login.

Configurações de WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para iOS

Ao escolher qualquer uma dessas configurações, suas configurações são listadas após **Configurações do servidor proxy**.

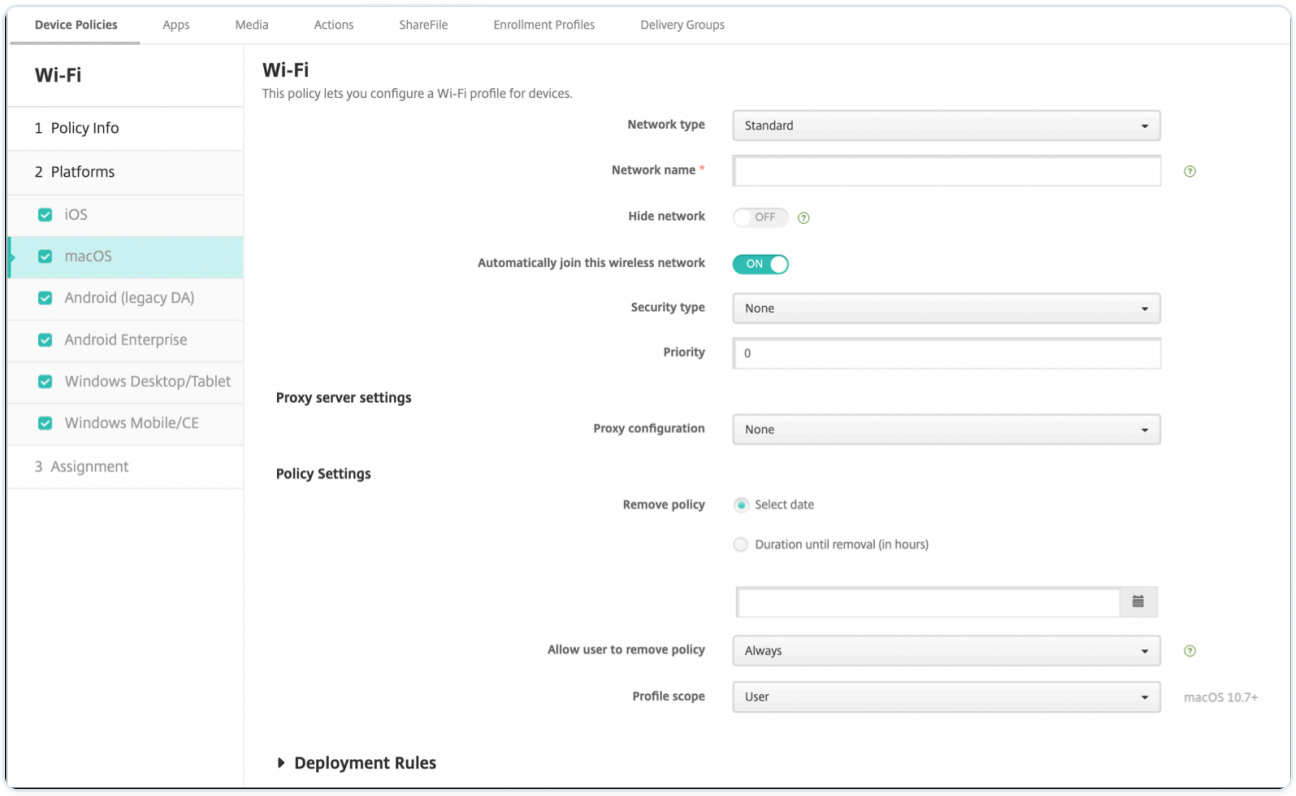
- **Protocolos, tipos de EAP aceitos:** Habilite os tipos de EAP que você deseja suportar e, em seguida, configure as configurações associadas. O padrão é **Desativado** para cada um dos tipos de EAP disponíveis.
- **Autenticação interna (TTLS):** *Necessário apenas quando você habilita o TTLS*. Na lista, escolha o método de autenticação interna a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** Escolha se deseja usar credenciais de acesso protegidas (PACs).

    - Se você escolher **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
        - Se você escolher **PAC de Provisionamento**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
            - **Provisionamento de PAC anonimamente**

- **Autenticação:**
    - **Nome de usuário:** Digite um nome de usuário.
    - **Senha por conexão:** Escolha se deseja exigir uma senha toda vez que os usuários fizerem logon.
    - **Senha:** Digite uma senha opcional. Se você deixar este campo em branco, os usuários poderão ser solicitados a digitar suas senhas ao fazer logon.
    - **Credencial de identidade (Keystore ou credencial PKI):** Na lista, escolha o tipo de credencial de identidade. O padrão é **Nenhum**.
    - **Identidade externa:** *Obrigatório somente quando você habilita* **PEAP**, **TTLS** *ou* **EAP-FAST**. Digite o nome de usuário visível externamente. Você pode aumentar a segurança digitando um termo genérico como "anônimo" para que o nome de usuário não seja visível.
    - **Exigir um certificado TLS:** Escolha se deseja exigir um certificado TLS.
- **Confiança**
    - **Certificados confiáveis:** Para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que deseja adicionar, faça o seguinte:
        - **Aplicativo:** Na lista, escolha o aplicativo que deseja adicionar.
        - Clique em **Salvar** para salvar o certificado ou clique em **Cancelar**.
    - **Nomes de certificado de servidor confiáveis:** Para adicionar nomes comuns de certificado de servidor confiáveis, clique em **Adicionar** e, para cada nome que deseja adicionar, faça o seguinte:
        - **Certificado:** Digite o nome do certificado do servidor. Você pode usar curingas para especificar o nome, como wpa.*.example.com.
        - Clique em **Salvar** para salvar o nome do certificado ou clique em **Cancelar**.
- **Permitir exceções de confiança:** Escolha se a caixa de diálogo de confiança de certificado aparece nos dispositivos dos usuários quando um certificado não é confiável. O padrão é **Ativado**.

- **Configurações do servidor proxy**
  - **Configuração de proxy:** Na lista, escolha **Nenhum**, **Manual** ou **Automático** para definir como a conexão VPN é roteada através de um servidor proxy e, em seguida, configure quaisquer opções adicionais. O padrão é **Nenhum**, o que não requer configuração adicional.
  - Se você escolher **Manual**, configure estas definições:
    - **Nome do host/endereço IP:** Digite o nome do host ou o endereço IP do servidor proxy.
    - **Porta:** Digite o número da porta do servidor proxy.
    - **Nome de usuário:** Digite um nome de usuário opcional para autenticar no servidor proxy.
    - **Senha:** Digite uma senha opcional para autenticar no servidor proxy.
  - Se você escolher **Automático**, configure estas definições:
    - **URL do servidor:** Digite a URL do arquivo PAC que define a configuração do proxy.
    - **Permitir conexão direta se o PAC estiver inacessível:** Escolha se deseja permitir que os usuários se conectem diretamente ao destino se o arquivo PAC estiver inacessível. O padrão é **Ativado**. Esta opção está disponível apenas no iOS 7.0 e posterior.
- **Definições de política**
  - **Remover política:** Escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até a remoção (em horas)**
    - **Selecionar data:** Clique no calendário para selecionar a data específica para a remoção.
    - **Duração até a remoção (em horas):** Digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Definições do macOS



- **Tipo de rede:** Na lista, escolha **Padrão**, **Hotspot Legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da rede:** Digite o SSID que é visto na lista de redes disponíveis para o dispositivo. Não se aplica a **Hotspot 2.0**.
- **Ocultar rede:** Escolha se deseja ocultar a rede.
- **Conectar-se automaticamente a esta rede sem fio:** Escolha se a rede é conectada automaticamente. Se um dispositivo já estiver conectado a outra rede, ele não se conectará a esta rede. O usuário deve desconectar-se da rede anterior antes que o dispositivo se conecte automaticamente. O padrão é **Ativado**.
- **Tipo de segurança:** Na lista, escolha o tipo de segurança que você planeja usar. Não se aplica a **Hotspot 2.0**.
  - Nenhum - Não requer configuração adicional.
  - WEP
  - WPA/WPA2 Pessoal
  - Qualquer (Pessoal)
  - WEP Corporativo
  - WPA/WPA2 Corporativo

    - Qualquer (Corporativo)

- **Prioridade:** Se você tiver várias redes, digite um número no campo **Prioridade** para definir a prioridade da conexão de rede. O dispositivo escolhe a rede com o número mais baixo.

As seções a seguir listam as opções que você configura para cada um dos tipos de conexão precedentes.

Configurações de WPA, WPA Pessoal, WPA 2 Pessoal, Qualquer (Pessoal) para macOS

- **Senha:** Digite uma senha opcional. Se você deixar este campo em branco, os usuários poderão ser solicitados a inserir suas senhas ao fazer login.

Configurações de WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para macOS

Ao escolher qualquer uma dessas configurações, as configurações delas são listadas após **Configurações do servidor proxy**.

- **Protocolos, tipos de EAP aceitos:** Habilite os tipos de EAP que você deseja suportar e, em seguida, configure as configurações associadas. O padrão é **Desativado** para cada um dos tipos de EAP disponíveis.
- **Autenticação interna (TTLS):** *Obrigatório apenas quando você habilita TTLS*. Na lista, escolha o método de autenticação interna a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** Escolha se deseja usar credenciais de acesso protegidas (PACs).
    - Se você selecionar **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
        - Se você escolher **PAC de Provisionamento**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
            - **Provisionar PAC anonimamente**
- **Autenticação:**
    - **Nome de usuário:** Digite um nome de usuário.
    - **Senha por conexão:** Escolha se deseja exigir uma senha toda vez que os usuários fizerem login.
    - **Senha:** Digite uma senha opcional. Se você deixar este campo em branco, os usuários poderão ser solicitados a inserir suas senhas ao fazer login.

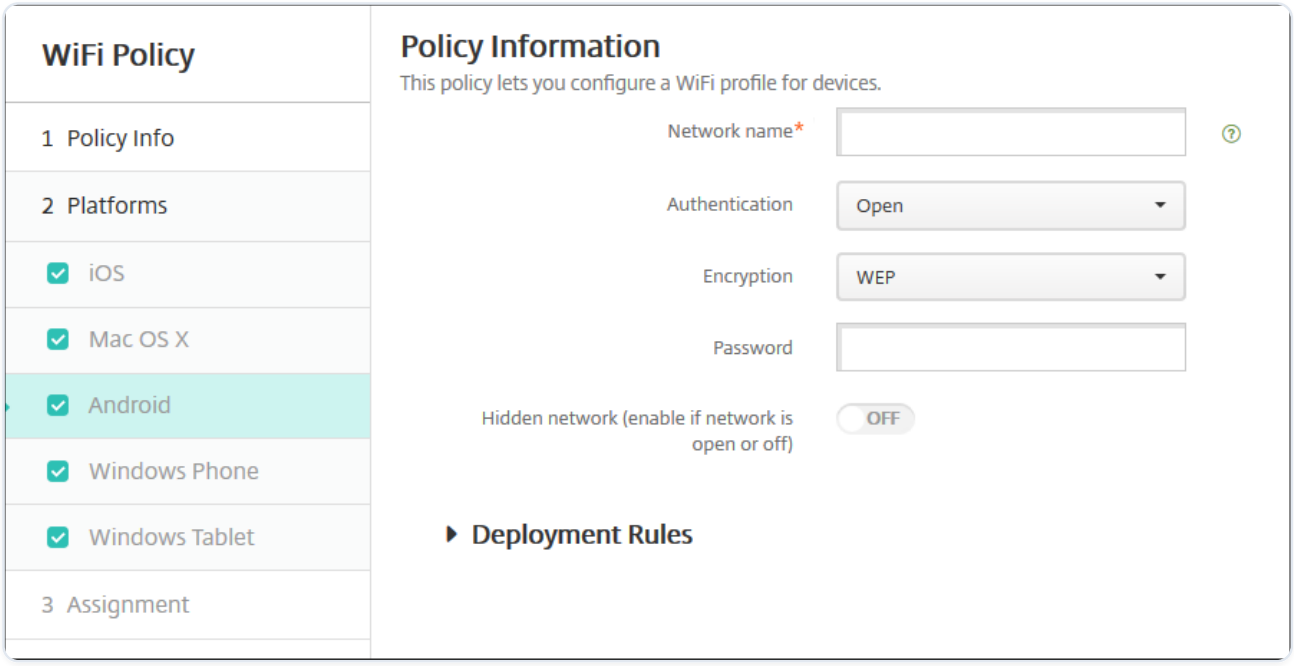
- **Credencial de identidade (Keystore ou credencial PKI):** Na lista, escolha o tipo de credencial de identidade. O padrão é **Nenhum**.
- **Identidade externa:** *Obrigatório apenas quando você habilita* **PEAP**, **TTLS** *ou* **EAP-FAST**. Digite o nome de usuário visível externamente. Você pode aumentar a segurança digitando um termo genérico como "anônimo" para que o nome de usuário não seja visível.
- **Exigir um certificado TLS:** Escolha se deseja exigir um certificado TLS.

- **Confiança**
  - **Certificados confiáveis:** Para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que deseja adicionar, faça o seguinte:
    - **Aplicativo:** Na lista, escolha o aplicativo que deseja adicionar.
    - Clique em **Salvar** para salvar o certificado ou clique em **Cancelar**.
  - **Nomes de certificado de servidor confiáveis:** Para adicionar nomes comuns de certificado de servidor confiáveis, clique em **Adicionar** e, para cada nome que deseja adicionar, faça o seguinte:
    - **Certificado:** Digite o nome do certificado do servidor que deseja adicionar. Você pode usar curingas para especificar o nome, como wpa.*.example.com.
    - Clique em **Salvar** para salvar o nome do certificado ou clique em **Cancelar**.
- **Permitir exceções de confiança:** Escolha se a caixa de diálogo de confiança do certificado aparece nos dispositivos do usuário quando um certificado não é confiável. O padrão é **Ativado**.
- **Usar como configuração de Janela de Login:** Escolha se deseja usar as mesmas credenciais inseridas na janela de login para autenticar o usuário.
- **Configurações do servidor proxy**
  - **Configuração de proxy:** Na lista, escolha **Nenhum**, **Manual** ou **Automático** para definir como a conexão VPN é roteada através de um servidor proxy e, em seguida, configure quaisquer opções adicionais. O padrão é **Nenhum**, o que não requer configuração adicional.
  - Se você escolher **Manual**, configure estas definições:
    - **Nome do host/endereço IP:** Digite o nome do host ou o endereço IP do servidor proxy.
    - **Porta:** Digite o número da porta do servidor proxy.

- **Nome de usuário:** Digite um nome de usuário opcional para autenticar no servidor proxy.
- **Senha:** Digite uma senha opcional para autenticar no servidor proxy.

- Se você escolher **Automático**, configure estas definições:
  - **URL do servidor:** Digite a URL do arquivo PAC que define a configuração do proxy.
  - **Permitir conexão direta se o PAC estiver inacessível:** Escolha se deseja permitir que os usuários se conectem diretamente ao destino se o arquivo PAC estiver inacessível. O padrão é **Ativado**. Esta opção está disponível apenas no iOS 7.0 e posterior.

Configurações do Android



- **Nome da rede:** Digite o SSID que está na lista de redes disponíveis no dispositivo do usuário.
- **Autenticação:** Na lista, escolha o tipo de segurança a ser usado com a conexão Wi-Fi.
  - Abrir
  - Compartilhado
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

As seções a seguir listam as opções que você configura para cada um dos tipos de conexão anteriores.

Configurações Abertas e Compartilhadas para Android

- **Criptografia:** Na lista, escolha **Desativado** ou **WEP**. O padrão é **WEP**.
- **Senha:** Digite uma senha opcional.

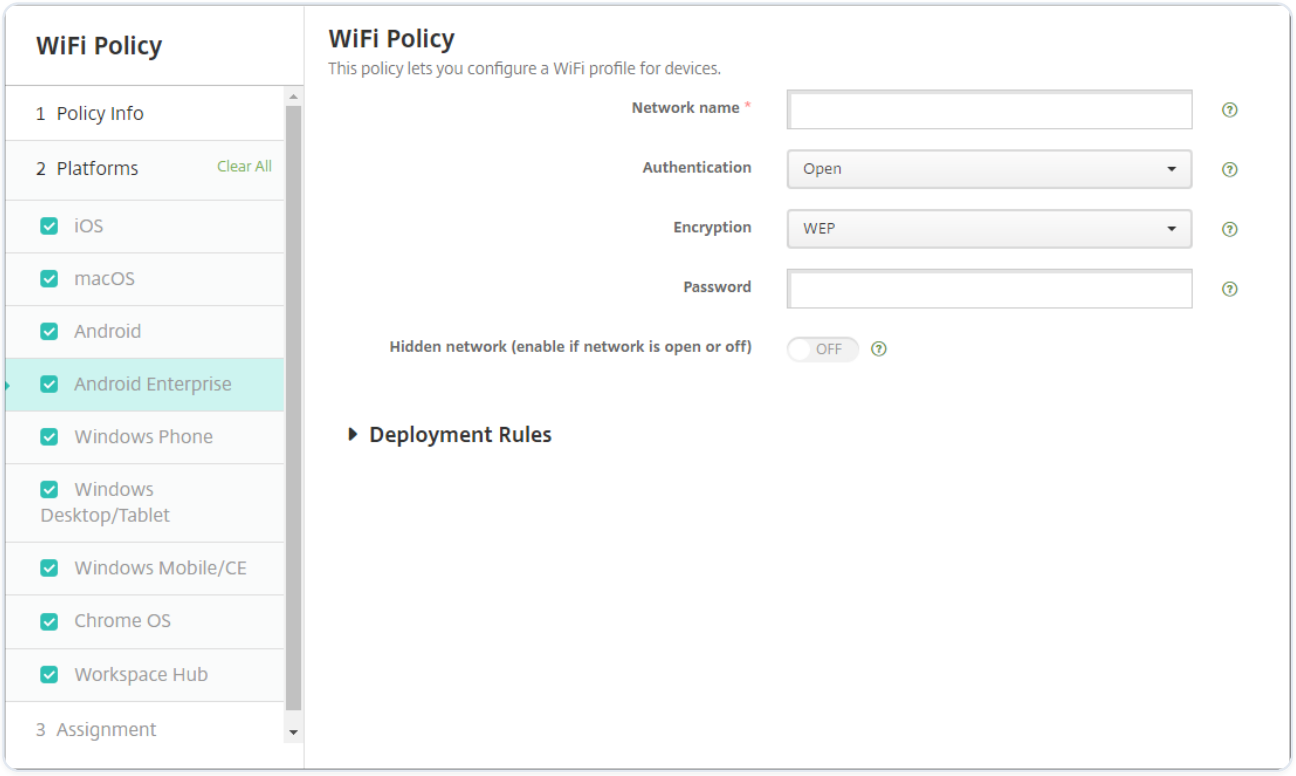
Configurações WPA, WPA-PSK, WPA2, WPA2-PSK para Android

- **Criptografia:** Na lista, escolha **TKIP** ou **AES**. O padrão é **TKIP**.
- **Senha:** Digite uma senha opcional.

Configurações 802.1x para Android

- **Tipo de EAP:** Na lista, escolha **PEAP**, **TLS** ou **TTLS**. O padrão é **PEAP**.
- **Senha:** Digite uma senha opcional.
- **Fase 2 da autenticação:** Na lista, escolha **Nenhum**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. O padrão é **PAP**.
- **Identidade:** Digite o nome de usuário e o domínio opcionais.
- **Anônimo:** Digite o nome de usuário opcional e visível externamente. Você pode aumentar a segurança digitando um termo genérico como "anônimo" para que o nome de usuário não seja visível.
- **Certificado CA:** Na lista, escolha o certificado a ser usado.
- **Credencial de identidade:** Na lista, escolha a credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Rede oculta (Habilitar se a rede estiver aberta ou desativada):** Escolha se a rede está oculta.

Configurações do Android Enterprise



- **Nome da rede:** Digite o SSID que está na lista de redes disponíveis no dispositivo do usuário.
- **Autenticação:** Na lista, escolha o tipo de segurança a ser usado com a conexão Wi-Fi.
  - Aberta
  - Compartilhada
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

As seções a seguir listam as opções que você configura para cada um dos tipos de conexão precedentes.

Configurações de Aberta e Compartilhada para Android Enterprise

- **Criptografia:** Na lista, escolha **Desativado** ou **WEP**. O padrão é **WEP**.
- **Senha:** Digite uma senha opcional.

Configurações de WPA, WPA-PSK, WPA2, WPA2-PSK para Android Enterprise

- **Criptografia:** Na lista, escolha TKIP ou AES. O padrão é TKIP.
- **Senha:** Digite uma senha opcional.

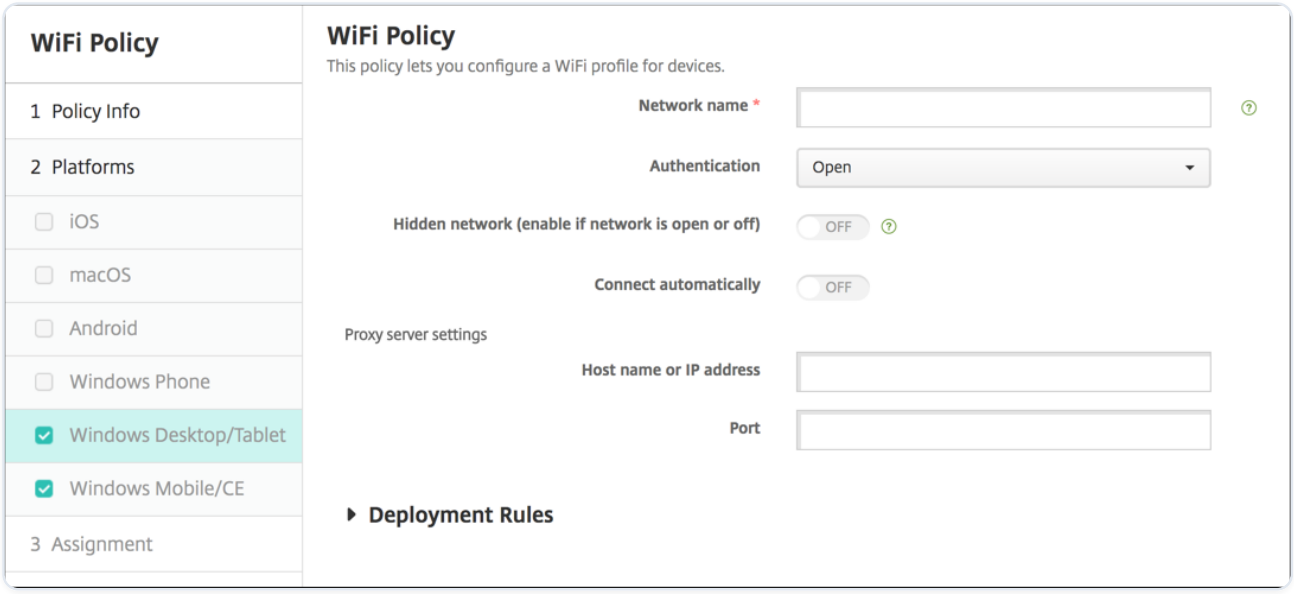
Configurações 802.1x para Android Enterprise

- **Tipo de EAP:** Na lista, escolha **PEAP**, **TLS** ou **TTLS**. O padrão é **PEAP**.
- **Senha:** Digite uma senha opcional.
- **Fase 2 de autenticação:** Na lista, escolha **Nenhum**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. O padrão é **PAP**.
- **Identidade:** Digite o nome de usuário e o domínio opcionais.
- **Anônimo:** Digite o nome de usuário opcional e visível externamente. Você pode aumentar a segurança digitando um termo genérico como “anônimo” para que o nome de usuário não seja visível.
- **Certificado CA:** Na lista, escolha o certificado a ser usado.
- **Domínio:** Digite o nome de domínio obrigatório. Para obter mais informações, consulte Domínio.

> **Observação:**
>
> Ao configurar a política de Wi-Fi em dispositivos com Android 13 ou posterior, os campos **Certificado CA** e **Domínio** devem ser atualizados obrigatoriamente. Se não forem atualizados, a configuração falhará.

- **Credencial de identidade:** Na lista, escolha a credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Rede oculta (Ativar se a rede estiver aberta ou desativada):** Escolha se a rede está oculta.

Configurações do Windows 10 e Windows 11



- **Autenticação:** Clique no tipo de segurança na lista suspensa que você deseja usar com a conexão Wi-Fi.
  - Aberta
  - WPA Pessoal
  - WPA-2 Pessoal
  - WPA Corporativo
  - WPA-2 Corporativo: O uso de WPA-2 Corporativo exige que você configure o SCEP. A configuração do SCEP permite que o XenMobile envie o certificado para os dispositivos para autenticar no servidor Wi-Fi. Para configurar o SCEP, vá para a página **Distribuição** em **Configurações > Provedores de Credenciais**. Para obter mais informações, consulte Provedores de credenciais.

As seções a seguir listam as opções que você configura para cada um dos tipos de conexão anteriores.

Configurações abertas para Windows 10 e Windows 11

- **Rede oculta (Ativar se a rede estiver aberta ou desativada):** Escolha se a rede está oculta.
- **Conectar automaticamente:** Escolha se deseja conectar-se à rede automaticamente.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows 10 e Windows 11

- **Criptografia:** Na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.

- **Rede oculta (Habilitar se a rede estiver aberta ou desativada):** Escolha se a rede está oculta.
- **Conectar automaticamente:** Escolha se deseja conectar-se à rede automaticamente.

Configurações WPA-2 Enterprise para Windows 10 e Windows 11

- **Criptografia:** Na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Tipo de EAP:** na lista, escolha **PEAP-MSCHAPv2** ou **TLS** para definir o tipo de EAP. O padrão é **PEAP-MSCHAPv2**.
- **Conectar se oculta:** Escolha se a rede está oculta.
- **Conectar automaticamente:** Escolha se deseja conectar-se à rede automaticamente.
- **Enviar certificado via SCEP:** Escolha se deseja enviar o certificado para os dispositivos do usuário usando o Protocolo de Registro Simples de Certificados (SCEP).
- **Provedor de credenciais para SCEP:** Na lista, escolha o provedor de credenciais SCEP. O padrão é **Nenhum**.

Política de dispositivo de Proteção de Informações do Windows

A Proteção de Informações do Windows (WIP), anteriormente conhecida como proteção de dados corporativos (EDP), é uma tecnologia do Windows que protege contra o vazamento potencial de dados corporativos. O vazamento de dados pode ocorrer através do compartilhamento de dados corporativos com aplicativos não protegidos pela empresa, entre aplicativos ou fora da rede da organização. Para obter mais informações, consulte Proteja seus dados corporativos usando a Proteção de Informações do Windows (WIP).

Você pode criar uma política de dispositivo no XenMobile® para especificar os aplicativos que exigem a Proteção de Informações do Windows no nível de imposição que você definir. A política de Proteção de Informações do Windows é para Tablets e Desktops supervisionados que executam o Windows 10 ou Windows 11.

O XenMobile inclui alguns aplicativos comuns e você pode adicionar outros. Você especifica para a política um nível de imposição que afeta a experiência do usuário. Por exemplo, você pode:

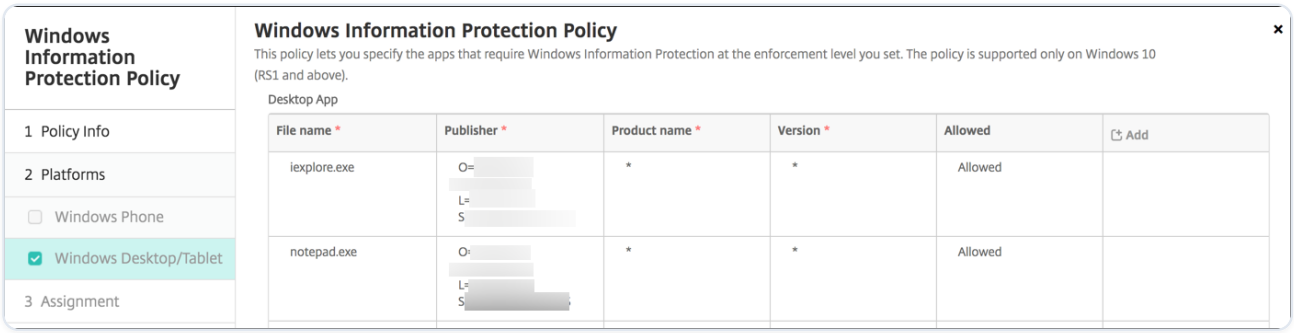
- Bloquear qualquer compartilhamento de dados inadequado.
- Avisar sobre compartilhamento de dados inadequado e permitir que os usuários ignorem a política.

- Executar o WIP silenciosamente enquanto registra e permite o compartilhamento de dados inadequado.

Para excluir aplicativos da Proteção de Informações do Windows, defina os aplicativos em arquivos XML do Microsoft AppLocker e, em seguida, importe esses arquivos para o XenMobile.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows 10 e Windows 11



- **Aplicativo de Área de Trabalho** (Windows 10 ou Windows 11 Desktop), **Aplicativo da Loja** (Windows 10 ou Windows 11 Tablet): O XenMobile inclui alguns aplicativos comuns, conforme mostrado no exemplo anterior. Você pode editar ou remover esses aplicativos conforme necessário.

  Para adicionar outros aplicativos: Na tabela **Aplicativo de Área de Trabalho** ou **Aplicativo da Loja**, clique em **Adicionar** e forneça as informações do aplicativo.

  Aplicativos **Permitidos** podem ler, criar e atualizar dados corporativos. Aplicativos **Negados** não podem acessar dados corporativos. Aplicativos **Isentos** podem ler dados corporativos, mas não podem criar ou modificar os dados.

  - **AppLocker XML:** A Microsoft fornece uma lista de aplicativos Microsoft que possuem problemas de compatibilidade conhecidos com o WIP. Para excluir esses aplicativos do WIP, clique em **Procurar** para carregar a lista. O XenMobile combina o AppLocker XML carregado e os aplicativos de área de trabalho e da loja configurados na política enviada ao dispositivo. Para obter mais informações, consulte Lista de bloqueio recomendada para Proteção de Informações do Windows.
  - **Nível de imposição:** Selecione uma opção para especificar como você deseja que o Windows Information Protection proteja e gerencie o compartilhamento de dados. O padrão é **Desativado**.
    - **0-Desativado:** O WIP está desativado e não protege nem audita seus dados.

- **1-Silencioso:** O WIP é executado silenciosamente, registra o compartilhamento inadequado de dados e não bloqueia nada. Você pode acessar os logs por meio do Reporting CSP.
- **2-Substituir:** O WIP avisa os usuários sobre o compartilhamento de dados potencialmente inseguro. Os usuários podem ignorar os avisos e compartilhar os dados. Este modo registra as ações, incluindo as substituições do usuário, no seu log de auditoria.
- **3-Bloquear:** O WIP impede que os usuários concluam o compartilhamento de dados potencialmente inseguro.

- **Nomes de domínio protegidos:** Os domínios que sua empresa usa para suas identidades de usuário. Esta lista de domínios de identidade gerenciados, juntamente com o domínio principal, compõem a identidade de sua empresa gerenciadora. O primeiro domínio na lista é a identidade corporativa principal usada na interface do usuário do Windows. Use "|" para separar os itens da lista. Por exemplo: `domain1.com | domain2.com`
- **Certificado de recuperação de dados:** Clique em **Procurar** e selecione um certificado de recuperação para usar na recuperação de dados de arquivos criptografados. Este certificado é o mesmo que o certificado do agente de recuperação de dados (DRA) para o sistema de arquivos de criptografia (EFS), apenas entregue via MDM em vez de Política de Grupo. Se um certificado de recuperação não estiver disponível, crie-o. Para obter informações, consulte "Criar um certificado de recuperação de dados" nesta seção.
- **Nomes de domínio de rede:** Uma lista de domínios que compreendem os limites da empresa. O WIP protege todo o tráfego para os domínios totalmente qualificados nesta lista. Essa configuração, com a configuração de **Intervalo de IP**, detecta se um endpoint de rede é corporativo ou pessoal em redes privadas. Use uma vírgula para separar os itens da lista. Por exemplo: corp.example.com,region.example.com
- **Intervalo de IP:** Uma lista dos intervalos IPv4 e IPv6 da empresa que definem os computadores na rede corporativa. O WIP considera esses locais como destinos seguros para o compartilhamento de dados corporativos. Use vírgulas para separar os itens da lista. Por exemplo:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **A lista de intervalos de IP é autoritativa:** Para evitar a detecção automática de intervalos de IP pelo Windows, altere esta configuração para **Ativado**. O padrão é **Desativado**.

- **Servidores proxy:** Uma lista dos servidores proxy que a empresa pode usar para recursos corporativos. Essa configuração é necessária se você usar um proxy em sua rede. Sem um servidor proxy, os recursos da empresa podem ficar indisponíveis quando um cliente está atrás de um proxy. Por exemplo, os recursos podem estar indisponíveis em certos hotspots Wi-Fi em hotéis e restaurantes. Use vírgulas para separar os itens da lista. Por exemplo:

  `proxy.example.com:80;157.54.11.118:443`

- **Servidores proxy internos:** Uma lista dos servidores proxy pelos quais seus dispositivos passam para acessar seus recursos de nuvem. O uso desse tipo de servidor indica que os recursos de nuvem aos quais você está se conectando são recursos corporativos. Não inclua nesta lista nenhum dos servidores na configuração de **Servidores proxy**, que são usados para tráfego não protegido por WIP. Use vírgulas para separar os itens da lista. Por exemplo:

  `example.internalproxy1.com;10.147.80.50`

- **Recursos de nuvem:** Uma lista de recursos de nuvem protegidos pelo WIP. Para cada recurso de nuvem, você também pode, opcionalmente, especificar um servidor proxy na lista **Servidores proxy** para rotear o tráfego para este recurso de nuvem. Todo o tráfego roteado através dos **Servidores proxy** é tratado como tráfego corporativo. Use vírgulas para separar os itens da lista. Por exemplo:

  `domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com`

- **Revogar certificado WIP no cancelamento de registro:** Especifica se as chaves de criptografia locais devem ser revogadas de um dispositivo de usuário quando ele é desregistrado do Windows Information Protection. Depois que as chaves de criptografia são revogadas, um usuário não pode acessar dados corporativos criptografados. Se **Desativado**, as chaves não são revogadas e o usuário continua a ter acesso a arquivos protegidos após o cancelamento do registro. O padrão é **Ativado**.
- **Mostrar ícones de sobreposição:** Especifica se deve incluir a sobreposição do ícone do Windows Information Protection em arquivos corporativos no Explorer e em blocos de aplicativos somente empresariais no menu Iniciar. O padrão é **Desativado**.

Criar um certificado de recuperação de dados

Um certificado de recuperação de dados é necessário para habilitar a política de **Windows Information Protection**.

1. Na máquina onde o console do XenMobile está sendo executado, abra um prompt de comando e navegar até uma pasta (diferente de Windows\\System32) onde você deseja criar um certificado.
2. Execute este comando:

   ```
   cipher /r:ESFDRA
   ```

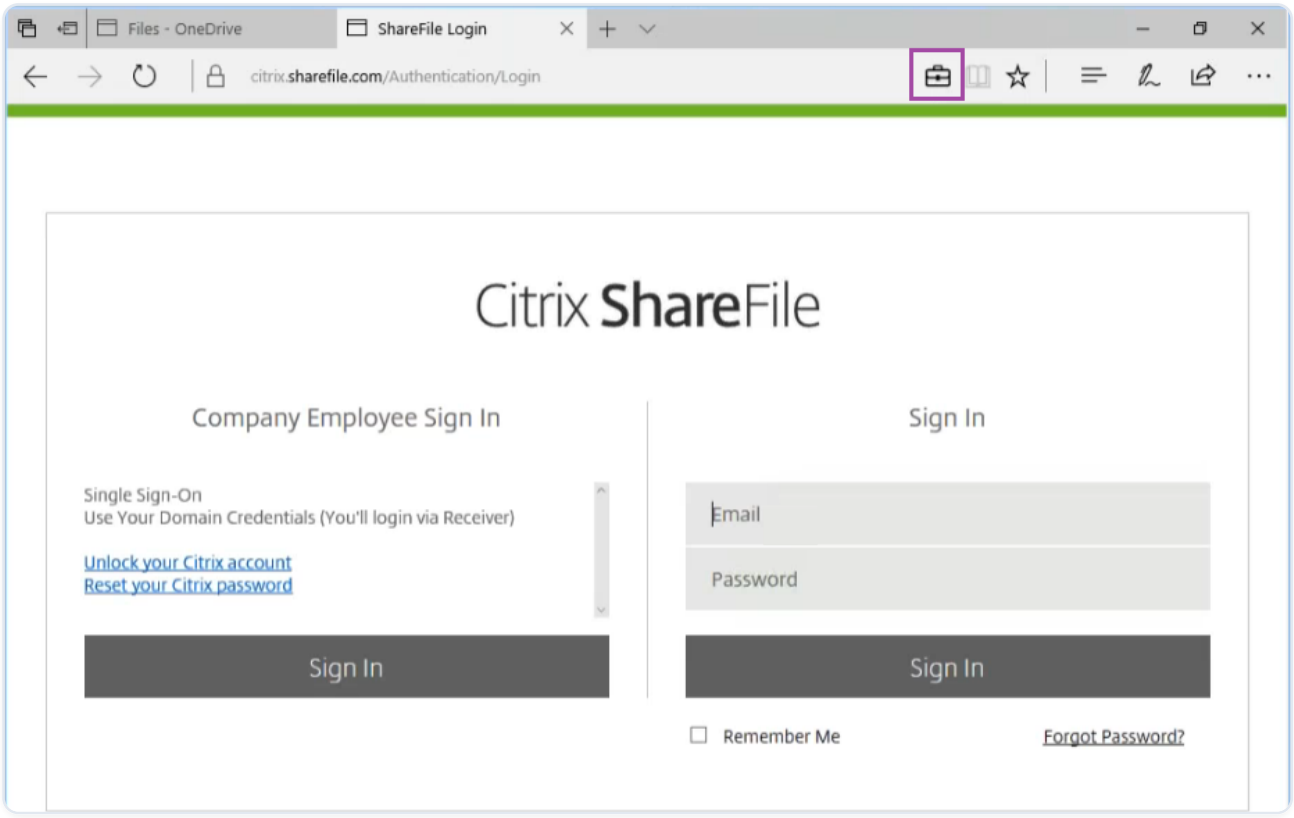
3. Quando solicitado, insira uma senha para proteger o arquivo da chave privada.

   O comando cipher cria um arquivo .cer e um arquivo .pfx.

4. No console do XenMobile, vá para **Configurações > Certificados** e importe o arquivo .cer, que se aplica a tablets Windows 10 e Windows 11.

Experiência do usuário

Quando o Windows Information Protection está em vigor, aplicativos e arquivos incluem um ícone:



Exemplo de ícone do Windows Information Protection(/en-us/xenmobile/server/media/wip-file-overlay.png)

Se um usuário copiar ou salvar um arquivo protegido em um local não protegido, a seguinte notificação aparecerá, dependendo do nível de imposição configurado.

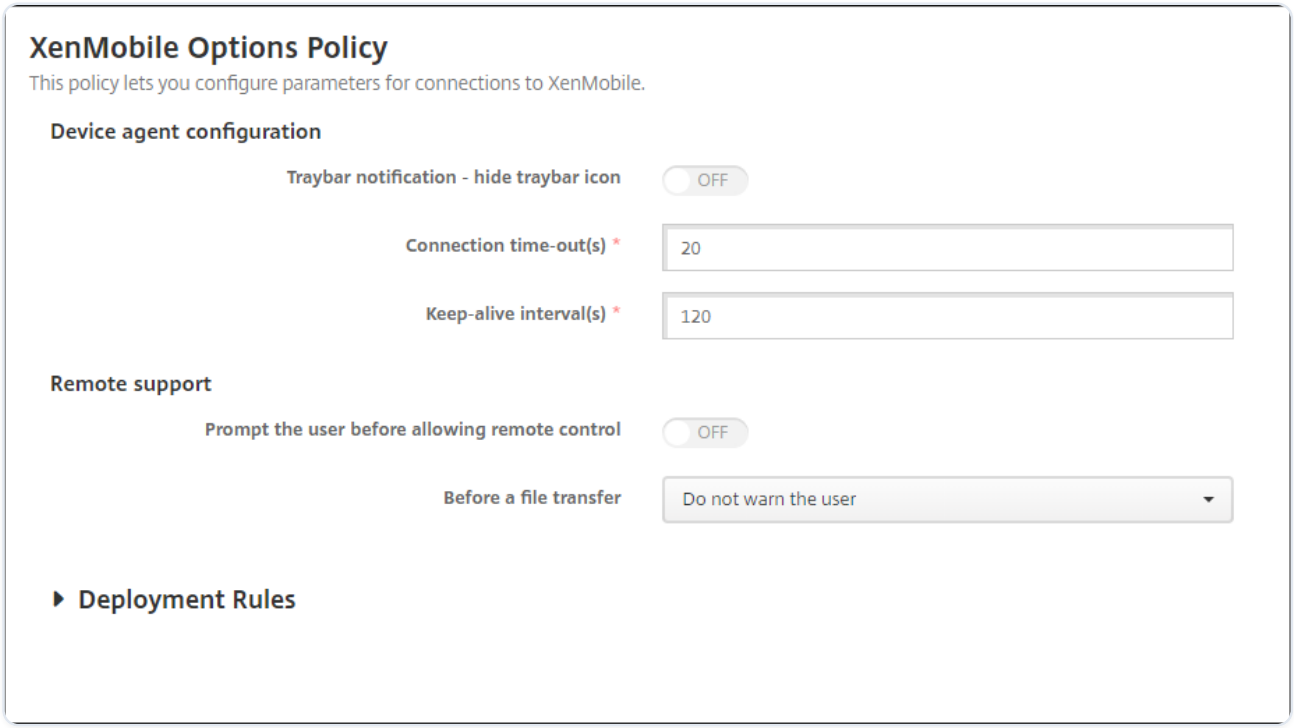
Exemplo de notificação(/en-us/xenmobile/server/media/wip-protected-content-message.png)

Política de dispositivo de opções do XenMobile®

Você adiciona uma política de opções do XenMobile para configurar o comportamento do Secure Hub ao se conectar ao XenMobile a partir de dispositivos Android.

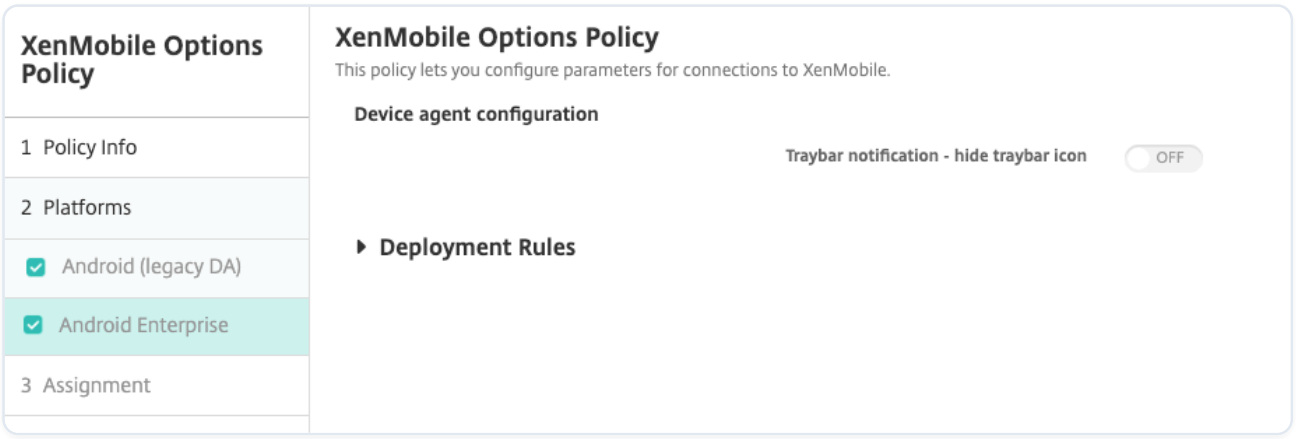
Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android



- **Notificação da barra de bandeja - ocultar ícone da barra de bandeja:** Selecione se o ícone da barra de bandeja está oculto ou visível. O padrão é **Desativado**.
- **Conexão: tempo limite (s):** Digite o tempo em segundos que uma conexão pode ficar ociosa antes que a conexão expire. O padrão é 20 segundos.
- **Intervalo de keep-alive (s):** Digite o tempo em segundos para manter uma conexão aberta. O padrão é 120 segundos.

Configurações do Android Enterprise



Compatível a partir da versão 7 do Android.

Notificação da barra de bandeja - ocultar ícone da barra de bandeja: Selecione se o ícone da barra de bandeja está oculto ou visível. O padrão é **Desativado**.

> **Nota:**
>
> Se você deseja habilitar o serviço VPN para dispositivos executando o Android Enterprise, pode habilitar a opção **Habilitar VPN Sempre Ativa** na **política de dispositivo VPN**. Se você já habilitou a opção **Habilitar VPN Sempre Ativa** na **política de dispositivo de opções do XenMobile** em uma versão anterior, certifique-se de habilitar a mesma na **política de dispositivo VPN** novamente. Para obter mais informações sobre a política de dispositivo VPN, consulte política de dispositivo VPN - configurações do Android Enterprise.

Política de desinstalação de dispositivo XenMobile®

Você pode adicionar uma política de dispositivo no XenMobile para desinstalar o XenMobile de dispositivos Android. Quando implantada, esta política remove o XenMobile de todos os dispositivos no grupo de implantação.

Para adicionar ou configurar esta política, vá para **Configurar > Políticas de Dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurar configurações do Android

- **Desinstalar o XenMobile dos dispositivos:** Selecione se deseja desinstalar o XenMobile de cada dispositivo para o qual você implanta esta política. O padrão é **Desativado**.

Adicionar apps

Adicionar aplicativos ao XenMobile® oferece recursos de gerenciamento de aplicativos móveis (MAM). O XenMobile auxilia na entrega de aplicativos, licenciamento de software, configuração e gerenciamento do ciclo de vida do aplicativo.

Habilitar aplicativos para MDX é uma parte importante da preparação da maioria dos tipos de aplicativos para distribuição em dispositivos de usuário. Para uma introdução ao MDX, consulte Sobre o MDX Toolkit e Visão geral do SDK MAM.

- A Citrix recomenda o uso do SDK MAM para habilitar aplicativos para MDX. Ou, você pode continuar a empacotar aplicativos com MDX até que o MDX Toolkit seja descontinuado. Consulte Descontinuação.
- Você não pode usar o MDX Toolkit para empacotar aplicativos de produtividade móvel Citrix®. Obtenha os arquivos MDX de aplicativos de produtividade móvel nos downloads da Citrix.

Ao adicionar aplicativos ao console do XenMobile, você:

- Configura as configurações do aplicativo
- Opcionalmente, organiza os aplicativos em categorias para organizá-los no Secure Hub
- Opcionalmente, define fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem um aplicativo
- Implanta aplicativos para os usuários

Este artigo aborda os fluxos de trabalho gerais para adicionar aplicativos. Consulte os seguintes artigos para especificidades da plataforma:

- Distribuir aplicativos Android Enterprise
- Distribuir aplicativos Apple

Tipos e recursos de aplicativos

A tabela a seguir resume os tipos de aplicativos que você pode implantar com o XenMobile.

TIPO DE APLICATIVO	FONTES	NOTAS	CONSULTE
MDX	Aplicativos iOS e Android que você desenvolve para seus usuários. Aplicativos de produtividade móvel da Citrix.	Desenvolva aplicativos iOS ou Android com o SDK MAM ou encapsule-os com o MDX Toolkit. Para os aplicativos de produtividade móvel, baixe os arquivos MDX da loja pública nos downloads da Citrix. Em seguida, adicione os aplicativos ao XenMobile.	Adicionar um aplicativo MDX
Loja de aplicativos pública	Aplicativos gratuitos ou pagos de lojas de aplicativos públicas, como Google Play ou Apple App Store.	Carregue os aplicativos, habilite-os para MDX e, em seguida, adicione os aplicativos ao XenMobile.	Adicionar um aplicativo da loja de aplicativos pública
Web e SaaS	Sua rede interna (aplicativos web) ou uma rede pública (SaaS).	O Citrix Workspace™ fornece logon único móvel para aplicativos SaaS nativos de dispositivos iOS e Android registrados no MDM. Ou, use conectores de aplicativo Security Assertion Markup Language (SAML)	Adicionar um aplicativo Web ou SaaS
Empresarial	Aplicativos privados, incluindo aplicativos Win 32, que não são	Adicione os aplicativos ao XenMobile.	Adicionar um aplicativo empresarial

TIPO DE APLICATIVO	FONTES	NOTAS	CONSULTE
	habilitados para MDX. Aplicativos privados do Android Enterprise que são habilitados para MDX. Os aplicativos empresariais residem em locais da Content Delivery Network ou em servidores XenMobile.		
Link da Web	Endereços da web da Internet, endereços da web da intranet ou aplicativos da web que não exigem logon único.	Configure links da web no XenMobile.	Adicionar um link da Web

Ao planejar a distribuição de aplicativos, considere estes recursos:

- Sobre instalações silenciosas
- Sobre aplicativos obrigatórios e opcionais
- Sobre categorias de aplicativos
- Habilitar aplicativos do Microsoft 365
- Aplicar fluxos de trabalho
- Marca da loja de aplicativos e do Citrix Secure Hub™

Sobre instalações silenciosas

A Citrix oferece suporte à instalação e atualização silenciosas de aplicativos iOS, Android Enterprise e Samsung. A instalação silenciosa significa que os usuários não são solicitados a instalar aplicativos que você implanta no dispositivo. Os aplicativos são instalados automaticamente em segundo plano.

Pré-requisitos para implementar a instalação silenciosa:

- Para iOS, coloque o dispositivo iOS gerenciado no modo supervisionado. Para obter detalhes, consulte a política de dispositivo Importar perfil iOS e macOS.
- Para Android Enterprise, os aplicativos são instalados no perfil de trabalho do Android no dispositivo. Para obter detalhes, consulte Android Enterprise.
- Para dispositivos Samsung, habilite o Samsung Knox no dispositivo.

  Para fazer isso, você define a política de dispositivo de chave de licença MDM da Samsung para gerar chaves de licença Samsung ELM e Knox. Para obter detalhes, consulte políticas de dispositivo de chave de licença MDM da Samsung.

Sobre aplicativos obrigatórios e opcionais

Ao adicionar aplicativos a um grupo de entrega, você escolhe se eles são opcionais ou obrigatórios. A Citrix recomenda implantar aplicativos como **Obrigatórios**.

- Aplicativos obrigatórios são instalados silenciosamente nos dispositivos do usuário, minimizando a interação. Ter esse recurso ativado também permite que os aplicativos sejam atualizados automaticamente.
- Aplicativos opcionais permitem que os usuários escolham quais aplicativos instalar, mas os usuários devem iniciar a instalação manualmente através do Secure Hub.

Para aplicativos marcados como obrigatórios, os usuários podem receber atualizações prontamente em situações como:

- Você carrega um novo aplicativo e o marca como obrigatório.
- Você marca um aplicativo existente como obrigatório.
- Um usuário exclui um aplicativo obrigatório.
- Uma atualização do Secure Hub está disponível.

Requisitos para a implantação forçada de aplicativos obrigatórios

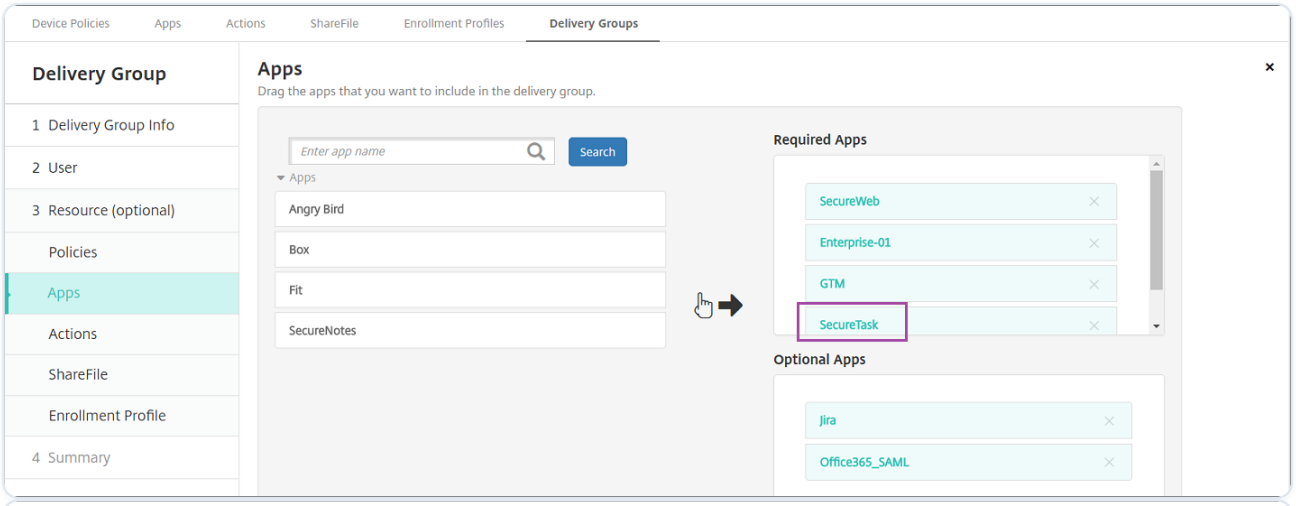
- XenMobile Server 10.6 (versão mínima)
- Secure Hub 10.5.15 para iOS e 10.5.20 para Android (versões mínimas)
- MAM SDK ou MDX Toolkit 10.6 (versão mínima)
- Propriedade de servidor personalizada, force.server.push.required.apps

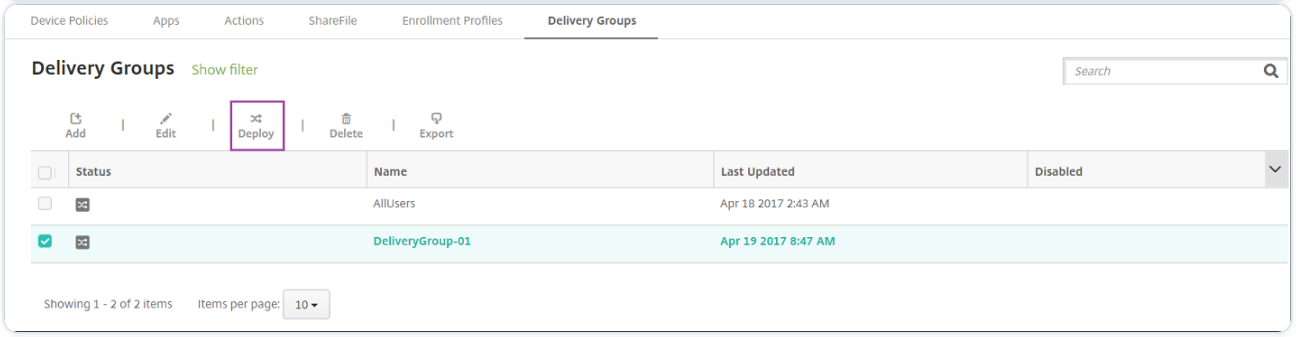
A implantação forçada de aplicativos obrigatórios é desabilitada por padrão. Para habilitar o recurso, crie uma propriedade de servidor de Chave Personalizada. Defina a **Chave** e o **Nome de exibição** como **force.server.push.required.apps** e defina o **Valor** como **true**.

- Depois de atualizar o XenMobile Server e o Secure Hub: Os usuários com dispositivos registrados devem sair e, em seguida, fazer login no Secure Hub, uma vez, para obter as atualizações de implantação de aplicativos obrigatórios.

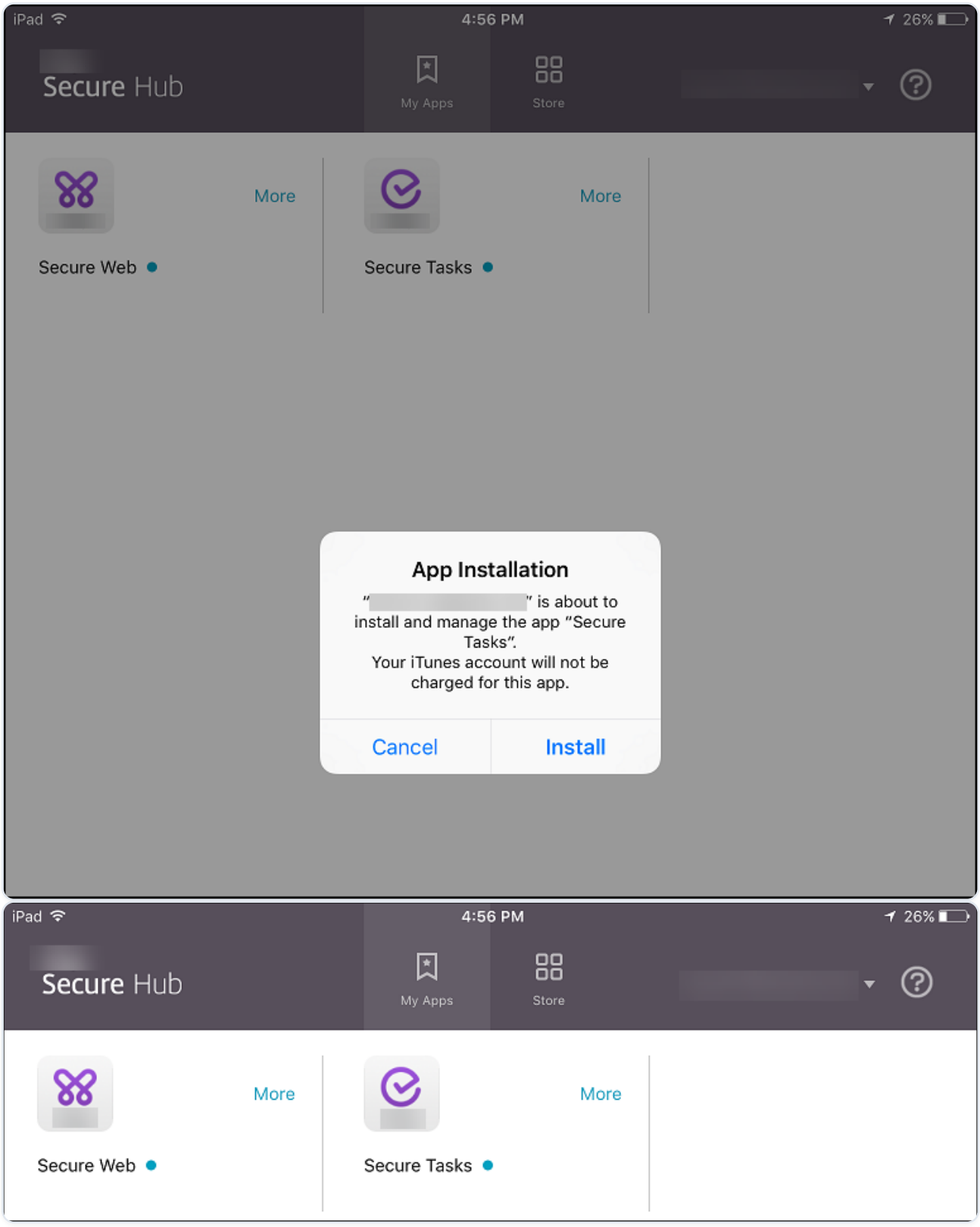
Exemplos

Os exemplos a seguir mostram a sequência de adição de um aplicativo chamado Citrix Secure Tasks a um grupo de entrega e, em seguida, a implantação do grupo de entrega.





Depois que o aplicativo de exemplo, Citrix Secure Tasks, é implantado no dispositivo do usuário, o Secure Hub solicita que o usuário instale o aplicativo.



Importante:

Aplicativos obrigatórios habilitados para MDX, incluindo aplicativos empresariais e aplicativos da loja de aplicativos pública, são atualizados imediatamente. A atualização

> ocorre mesmo que você configure uma política MDX para um período de carência de atualização de aplicativo e o usuário escolha atualizar o aplicativo mais tarde.

Fluxo de trabalho de aplicativo obrigatório do iOS para aplicativos empresariais e da loja pública

1. Implante o aplicativo XenMobile durante o registro inicial. O aplicativo obrigatório é instalado no dispositivo.
2. Atualize o aplicativo no console do XenMobile.
3. Use o console do XenMobile para implantar os aplicativos obrigatórios.
4. O aplicativo na tela inicial é atualizado. E, para aplicativos da loja pública, a atualização começa automaticamente. Os usuários não são solicitados a atualizar.
5. Os usuários abrem o aplicativo na tela inicial. Os aplicativos são atualizados imediatamente, mesmo que você defina um período de carência de atualização de aplicativo e o usuário toque para atualizar o aplicativo mais tarde.

Fluxo de trabalho de aplicativo obrigatório do Android para aplicativos empresariais

1. Implante o aplicativo XenMobile durante o registro inicial. O aplicativo obrigatório é instalado no dispositivo.
2. Use o console do XenMobile para implantar os aplicativos obrigatórios.
3. O aplicativo é atualizado. (Dispositivos Nexus solicitam a instalação de atualizações, mas dispositivos Samsung fazem uma instalação silenciosa.)
4. Os usuários abrem o aplicativo na tela inicial. Os aplicativos são atualizados imediatamente, mesmo que você defina um período de carência de atualização de aplicativo e o usuário toque para atualizar o aplicativo mais tarde. (Dispositivos Samsung fazem uma instalação silenciosa.)

Fluxo de trabalho de aplicativo obrigatório do Android para aplicativos da loja pública

1. Implantar o aplicativo XenMobile durante o registro inicial. O aplicativo necessário é instalado no dispositivo.
2. Atualize o aplicativo no console do XenMobile.

3. Use o console do XenMobile para implantar os aplicativos necessários. Ou, abra a Secure Hub Store no dispositivo. O ícone de atualização aparece na loja.
4. A atualização do aplicativo é iniciada automaticamente. (Dispositivos Nexus solicitam aos usuários que instalem a atualização.)
5. Abra o aplicativo na tela inicial. O aplicativo é atualizado. Os usuários não são solicitados a um período de carência. (Dispositivos Samsung fazem uma instalação silenciosa.)

Desinstalar um aplicativo quando ele estiver configurado como obrigatório

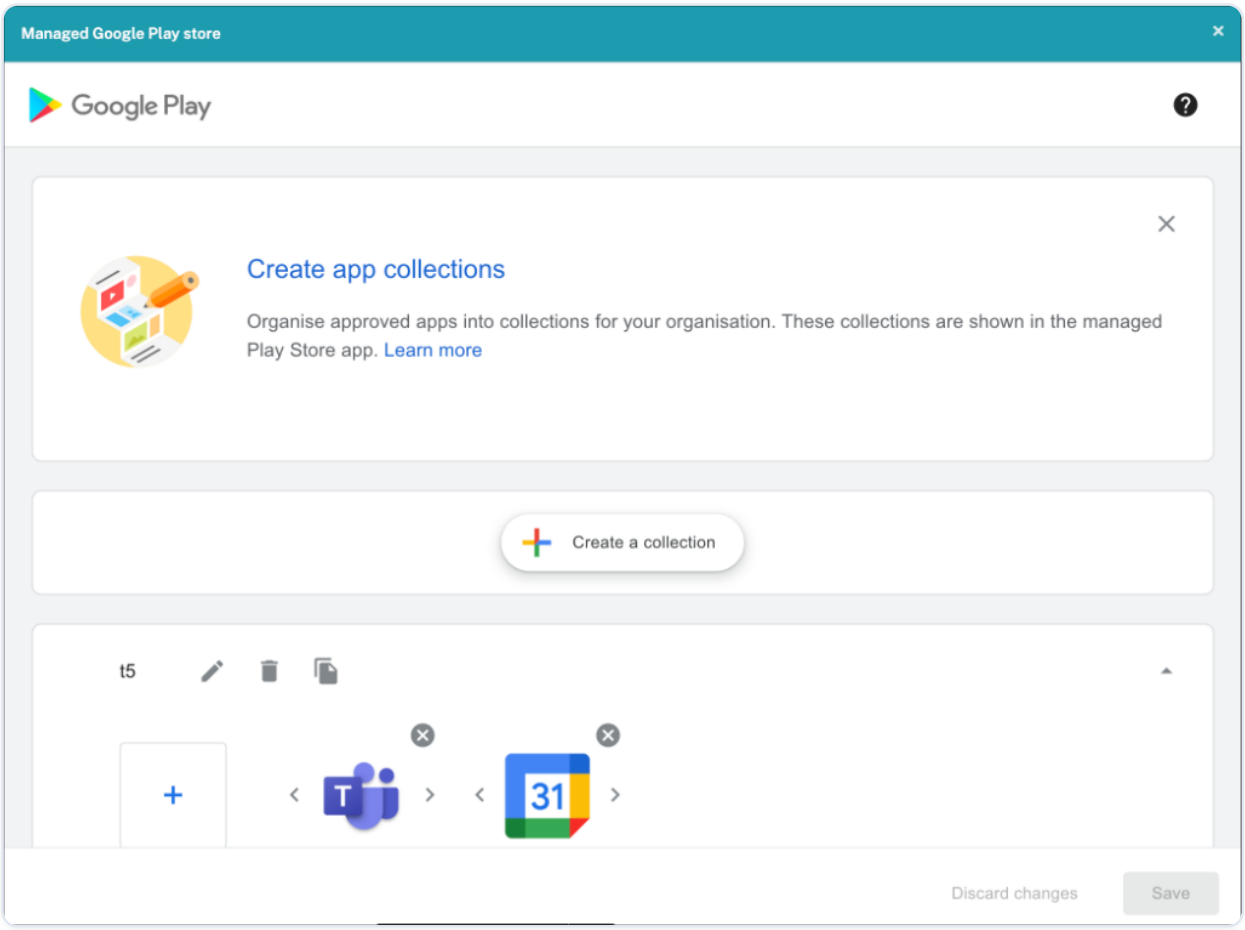
Você pode permitir que os usuários desinstalem um aplicativo configurado como obrigatório. Vá para **Configurar > Grupos de Entrega** e mova o aplicativo de **Aplicativos Obrigatórios** para **Aplicativos Opcionais**.

Recomendado: Use um grupo de entrega especial para alterar temporariamente um aplicativo para opcional, para que usuários específicos possam desinstalar o aplicativo. Você pode então alterar um aplicativo obrigatório existente para opcional, implantar o aplicativo nesse grupo de entrega e, em seguida, desinstalar o aplicativo desses dispositivos. Depois disso, se você quiser que futuros registros para esse grupo de entrega exijam o aplicativo, poderá definir o aplicativo de volta para obrigatório.

Organizar aplicativos (Android Enterprise)

Quando os usuários fazem logon no Secure Hub, eles recebem uma lista dos aplicativos, links da web e lojas que você configurou no XenMobile Server. No Android Enterprise, você pode organizar esses aplicativos em coleções para permitir que os usuários acessem apenas determinados aplicativos, lojas ou links da web. Por exemplo, você cria uma coleção de Finanças e, em seguida, adiciona aplicativos à coleção que se referem apenas a finanças. Ou, você pode configurar uma coleção de Vendas à qual você atribui aplicativos de vendas.

1. No console do XenMobile Server, clique em **Configurar > Aplicativos > Organizar Aplicativos**. A janela **Managed Google Play store** é exibida.



2. Clique em **Criar** uma coleção e selecione os aplicativos a serem adicionados a essa coleção.
3. Clique em **Salvar** quando terminar de adicionar coleções.

> **Nota:**
>
> Os administradores de TI precisam aprovar um aplicativo antes que ele possa ser adicionado a uma coleção na janela do Managed Google Play. Um administrador de TI pode aprovar um aplicativo acessando `<https://play.google.com/work>`. Em uma versão futura, você não precisará aprovar um aplicativo antes de adicioná-lo a uma coleção.

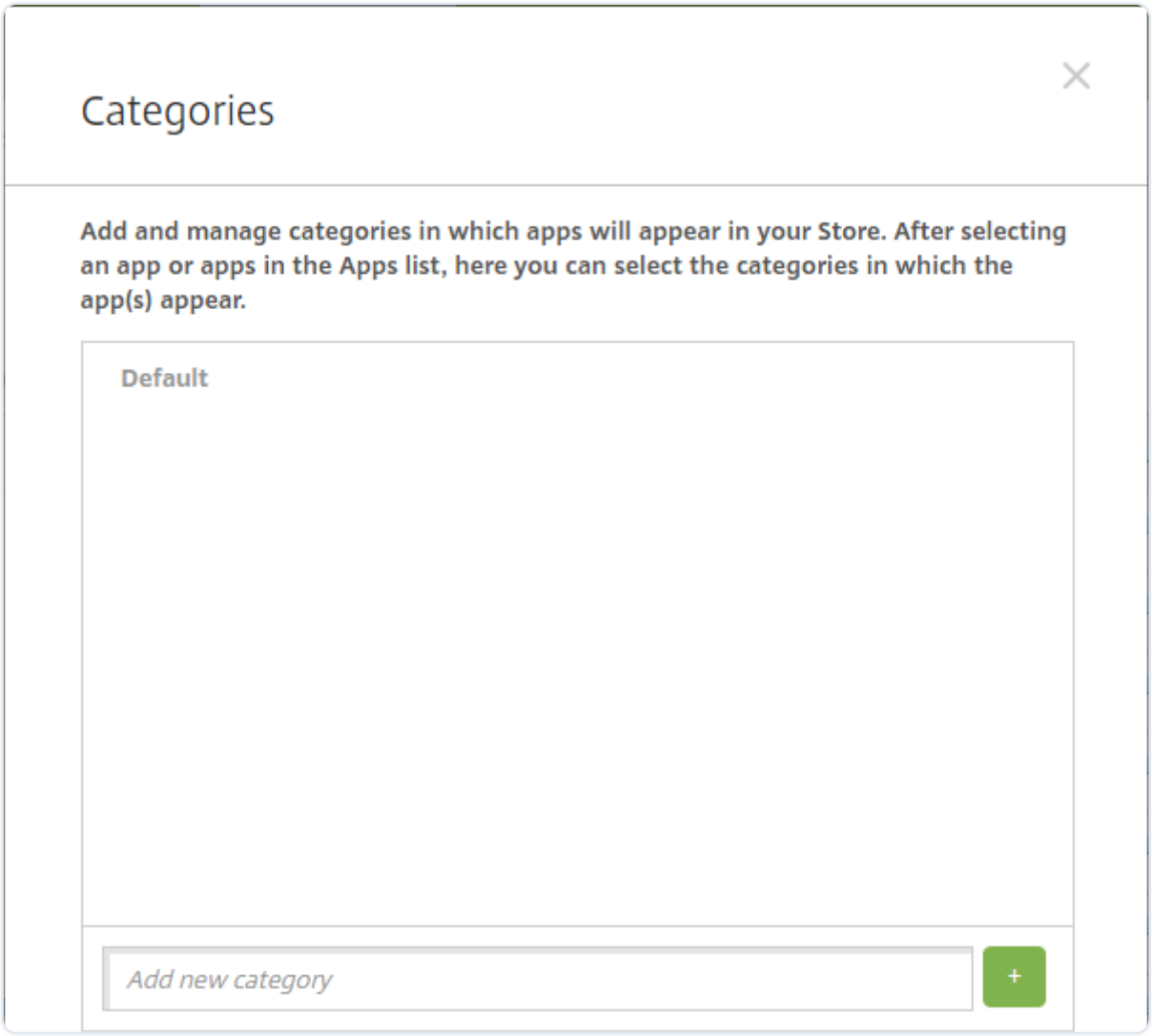
Sobre as categorias de aplicativos

Quando os usuários fazem logon no Secure Hub, eles recebem uma lista dos aplicativos, links da web e lojas que você configurou no XenMobile. Você pode usar categorias de aplicativos para permitir que os usuários acessem apenas determinados aplicativos, lojas ou links da web. Por exemplo, você pode criar uma categoria de Finanças e, em seguida, adicionar aplicativos a essa

categoria que se referem apenas a finanças. Ou, você pode configurar uma categoria de Vendas à qual atribui aplicativos de vendas.

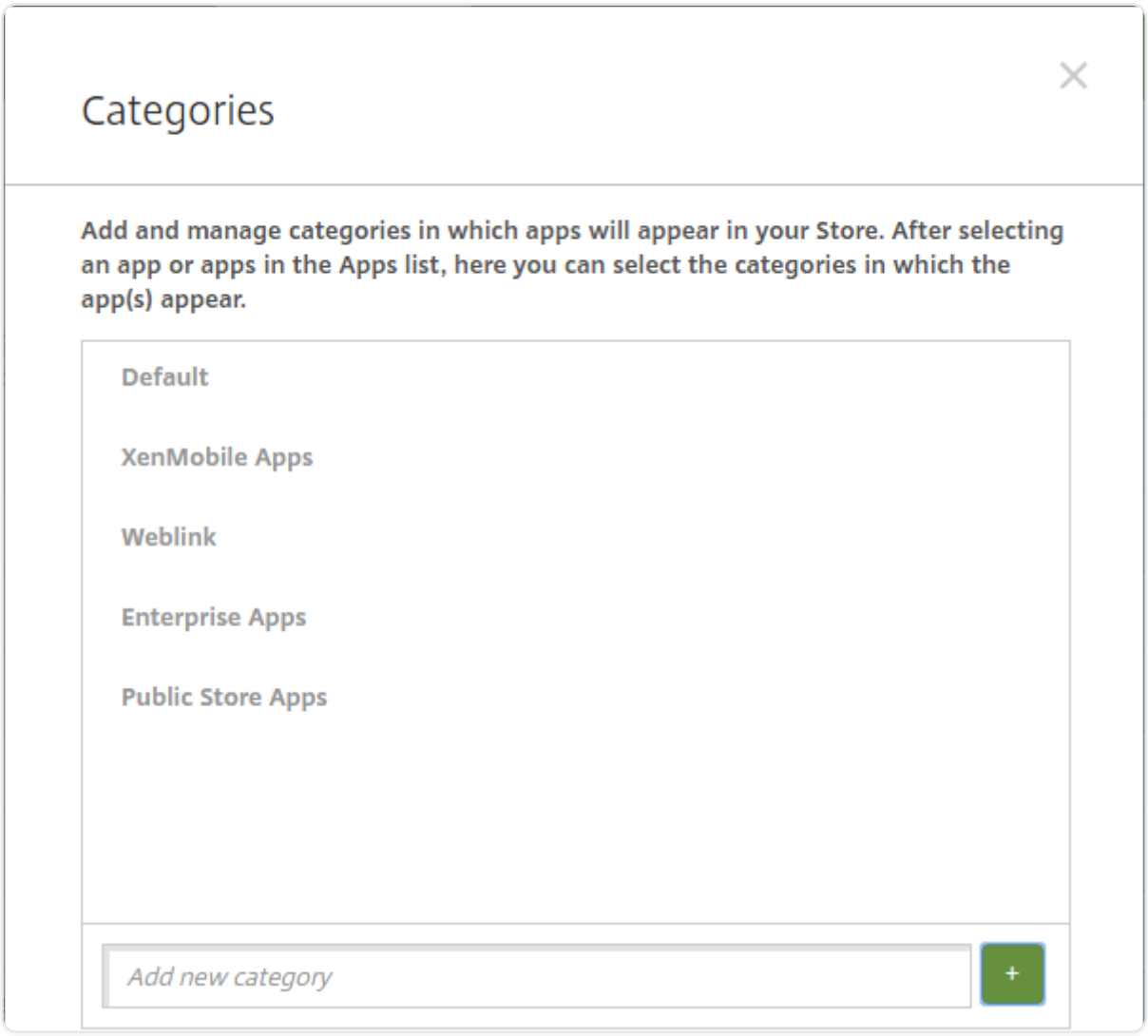
Ao adicionar ou editar um aplicativo, link da web ou loja, você pode adicionar o aplicativo a uma ou mais das categorias configuradas.

1. No console do XenMobile, clique em **Configurar > Aplicativos > Categoria**. A caixa de diálogo **Categorias** é exibida.



2. Para cada categoria que você deseja adicionar, faça o seguinte:

    - Digite o nome da categoria que você deseja adicionar no campo **Adicionar nova categoria** na parte inferior da caixa de diálogo. Por exemplo, você pode digitar Aplicativos Corporativos para criar uma categoria para aplicativos corporativos.
    - Clique no sinal de mais (+) para adicionar a categoria. A categoria recém-criada é adicionada e aparece na caixa de diálogo **Categorias**.



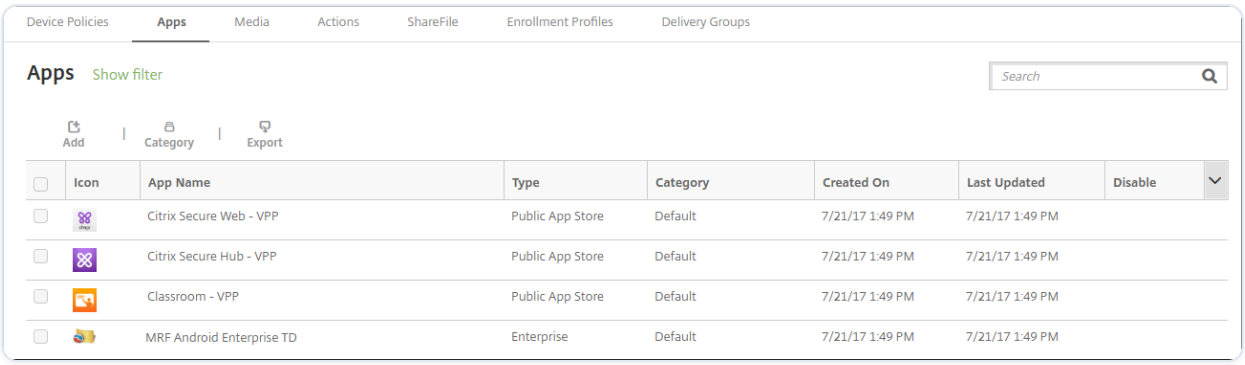
3. Quando terminar de adicionar categorias, feche a caixa de diálogo **Categorias**.
4. Na página **Aplicativos**, você pode colocar um aplicativo existente em uma nova categoria.
    - Selecione o aplicativo que você deseja categorizar.
    - Clique em **Editar**. A página **Informações do Aplicativo** é exibida.
    - Na lista **Categoria do aplicativo**, aplique a nova categoria selecionando a caixa de seleção da categoria. Desmarque as caixas de seleção de quaisquer categorias existentes que você não deseja aplicar ao aplicativo.
    - Clique na guia **Atribuições de Grupos de Entrega** ou clique em **Avançar** em cada uma das páginas seguintes para percorrer as páginas restantes de configuração do aplicativo.
    - Clique em **Salvar** na página **Atribuições de Grupos de Entrega** para aplicar a nova categoria. A nova categoria é aplicada ao aplicativo e aparece na tabela **Aplicativos**.

Adicionar um aplicativo MDX

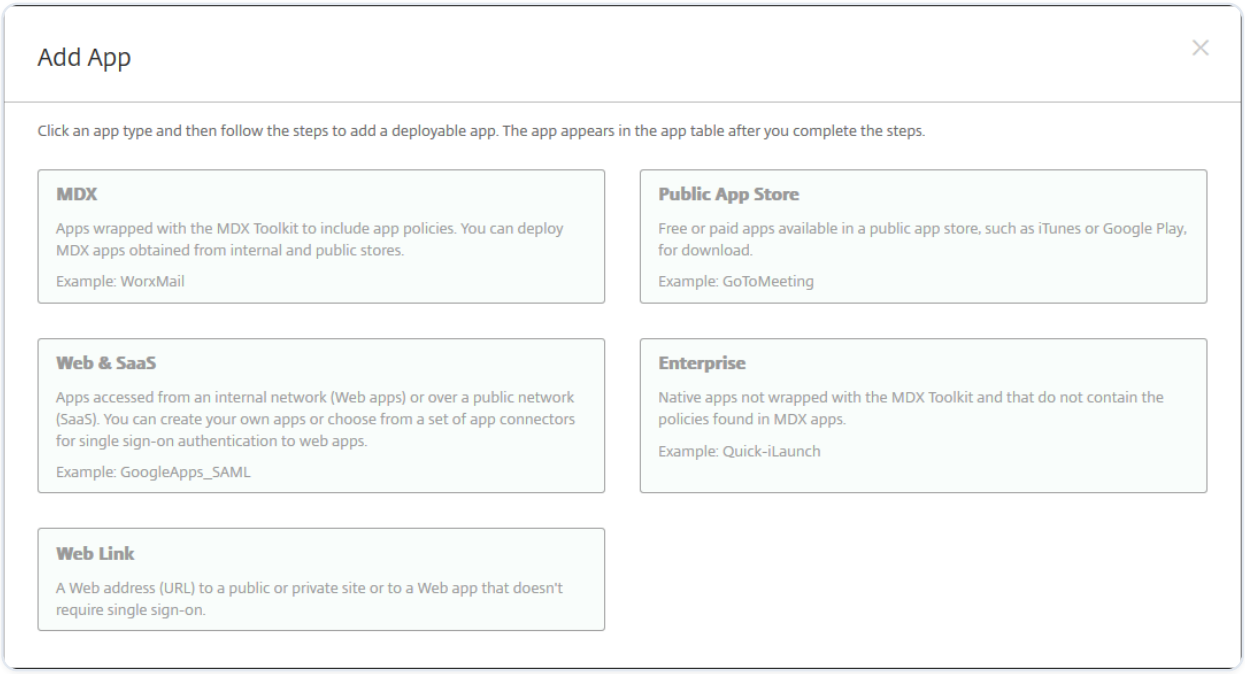
Ao receber um arquivo MDX para um aplicativo iOS ou Android, você pode carregar o aplicativo para o XenMobile. Depois de carregar o aplicativo, você pode configurar os detalhes do aplicativo e as configurações de política. Para obter mais informações sobre as políticas de aplicativo disponíveis para cada tipo de plataforma de dispositivo, consulte:

- Visão geral do SDK MAM
- Políticas MDX em um Relance

1. No console do XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



3. Clique em **MDX**. A página **Informações do Aplicativo MDX** é exibida.
4. No painel **Informações do Aplicativo**, digite as seguintes informações:

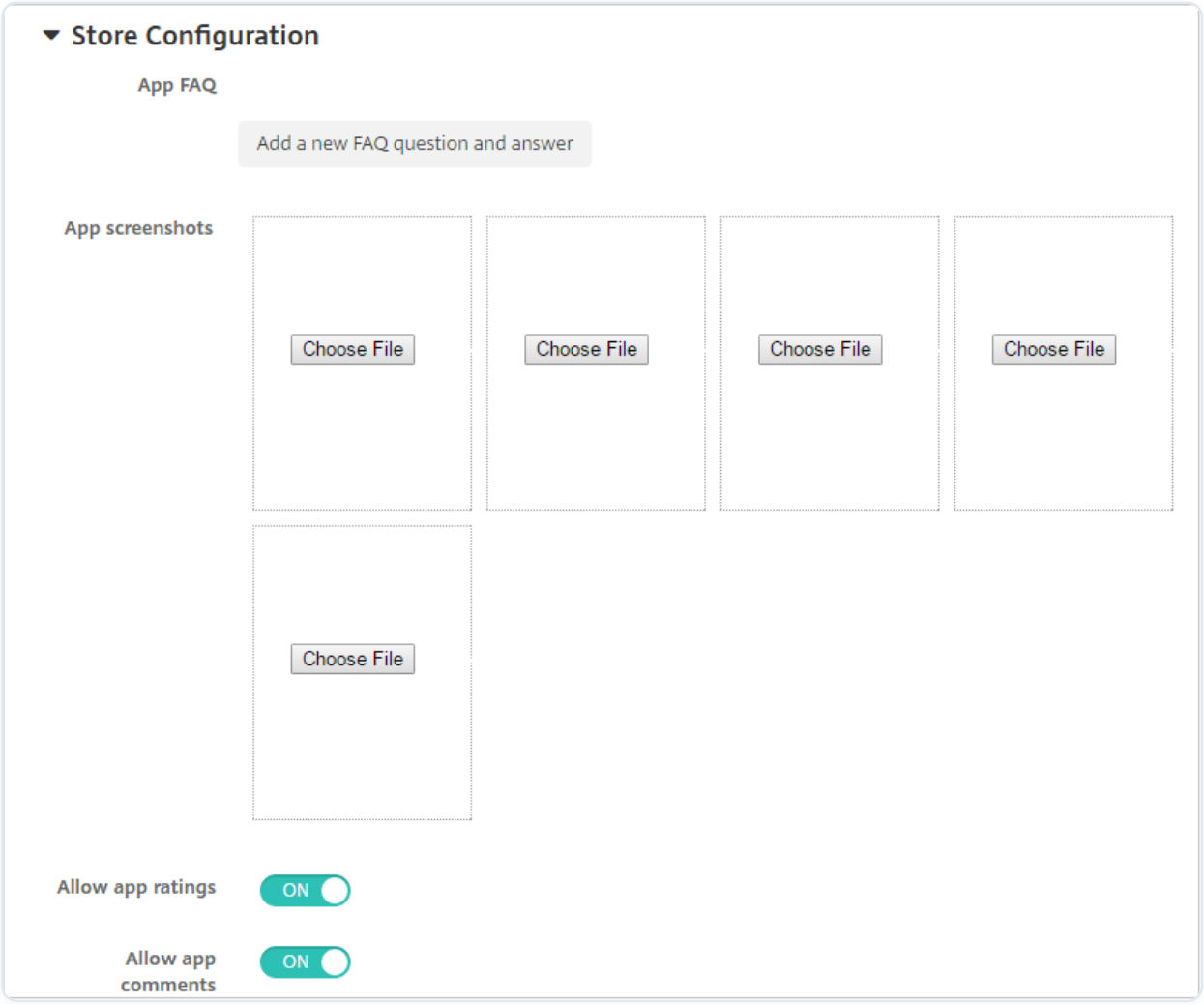
- **Nome:** Digite um nome descritivo para o aplicativo. O nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
- **Descrição:** Digite uma descrição opcional do aplicativo.
- **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

5. Clique em **Avançar**. A página **Plataformas de Aplicativos** é exibida.
6. Em **Plataformas**, selecione as plataformas que deseja adicionar. Se você estiver configurando apenas para uma plataforma, desmarque as outras.
7. Para selecionar um arquivo MDX para upload, clique em **Carregar** e navegar até o local do arquivo.
8. Na página **Detalhes do aplicativo**, configure estas definições:

- **Nome do arquivo:** Digite o nome do arquivo associado ao aplicativo.
- **Descrição do aplicativo:** Digite uma descrição para o aplicativo.
- **Versão do aplicativo:** Opcionalmente, digite o número da versão do aplicativo.
- **ID do pacote:** Digite o ID do pacote para o aplicativo, obtido na Google Play Store gerenciada.
- **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
- **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
- **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
- **Remover aplicativo se o perfil MDM for removido:** Selecione se deseja remover o aplicativo de um dispositivo iOS quando o perfil MDM for removido. O padrão é **Ativado**.
- **Impedir backup de dados do aplicativo:** Selecione se deseja impedir que os usuários façam backup dos dados do aplicativo em dispositivos iOS. O padrão é **Ativado**.
- **Faixa de produto:** Especifique qual faixa de produto você deseja enviar para dispositivos iOS. Se você tiver uma faixa projetada para testes, poderá selecioná-la e atribuí-la aos seus usuários. O padrão é **Produção**.

- **Forçar aplicativo a ser gerenciado:** Para um aplicativo que é instalado como não gerenciado, selecione se deseja solicitar aos usuários que permitam que o aplicativo seja gerenciado em dispositivos iOS não supervisionados. O padrão é **Ativado**.
- **Aplicativo implantado via compra por volume:** Selecione se deseja implantar o aplicativo usando a compra por volume da Apple. Se **Ativado**, e você implantar uma versão MDX do aplicativo e usar a compra por volume para implantar o aplicativo, o Secure Hub mostrará apenas a instância de compra por volume. O padrão é **Desativado**.

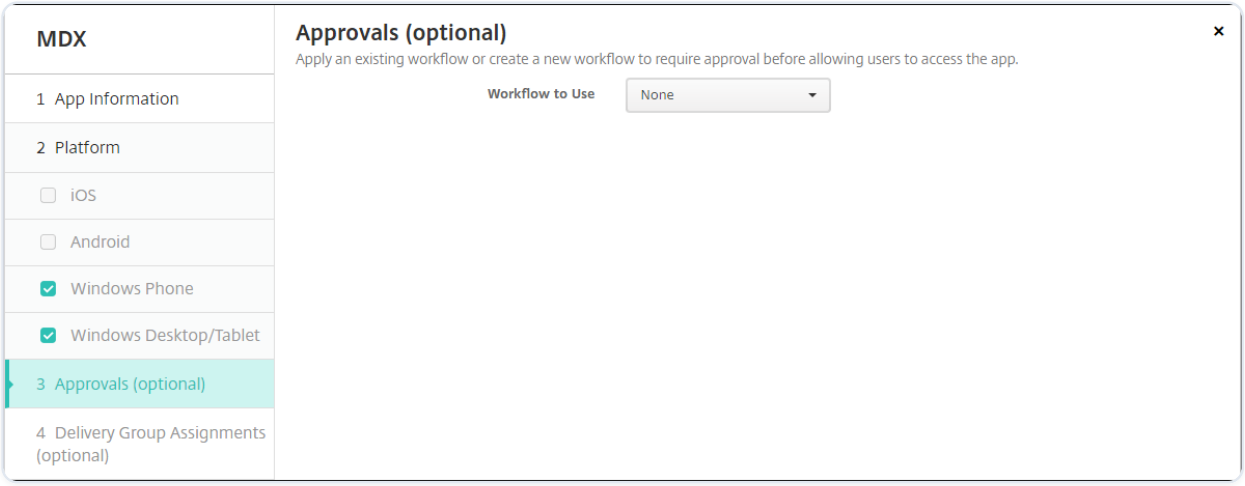
9. Configure as **Políticas MDX**. As políticas MDX variam por plataforma e incluem opções para áreas de política como autenticação, segurança do dispositivo e restrições de aplicativos. No console, cada uma das políticas possui uma dica de ferramenta que descreve a política.
10. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
11. Expanda **Configuração da Loja**.



- **Perguntas Frequentes do Aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar um FAQ para o aplicativo.

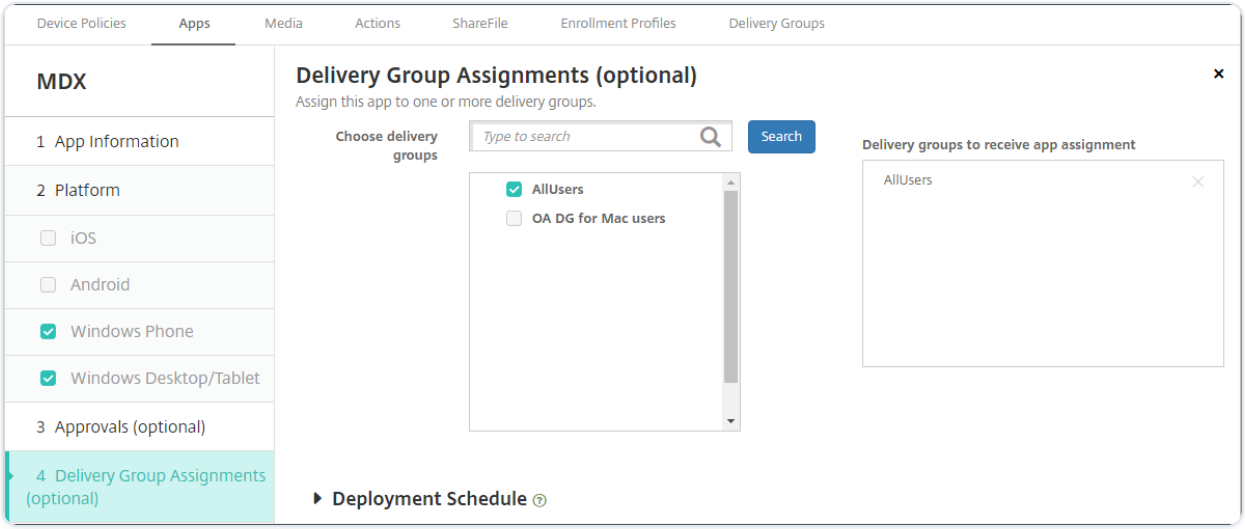
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** Permita que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

12. Clique em **Avançar**. A página **Aprovações** é exibida.



Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não quiser configurar fluxos de trabalho de aprovação, continue com a próxima etapa.

13. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.



14. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um ou mais grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
15. Expandir **Agendamento de Implantação** e configure as seguintes configurações:

- **Implantar:** Escolha se deseja implantar o aplicativo nos dispositivos. O padrão é **Ativado**.
- **Agendamento de implantação:** Escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
- **Condição de implantação:** Escolha **Em cada conexão** para implantar o aplicativo toda vez que o dispositivo se conectar. Escolha **Somente quando a implantação anterior falhou** para implantar o aplicativo quando o dispositivo não conseguiu recebê-lo anteriormente. O padrão é **Em cada conexão**.

A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você fizer se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.

16. Clique em **Salvar**.

Adicionar um aplicativo da loja de aplicativos pública

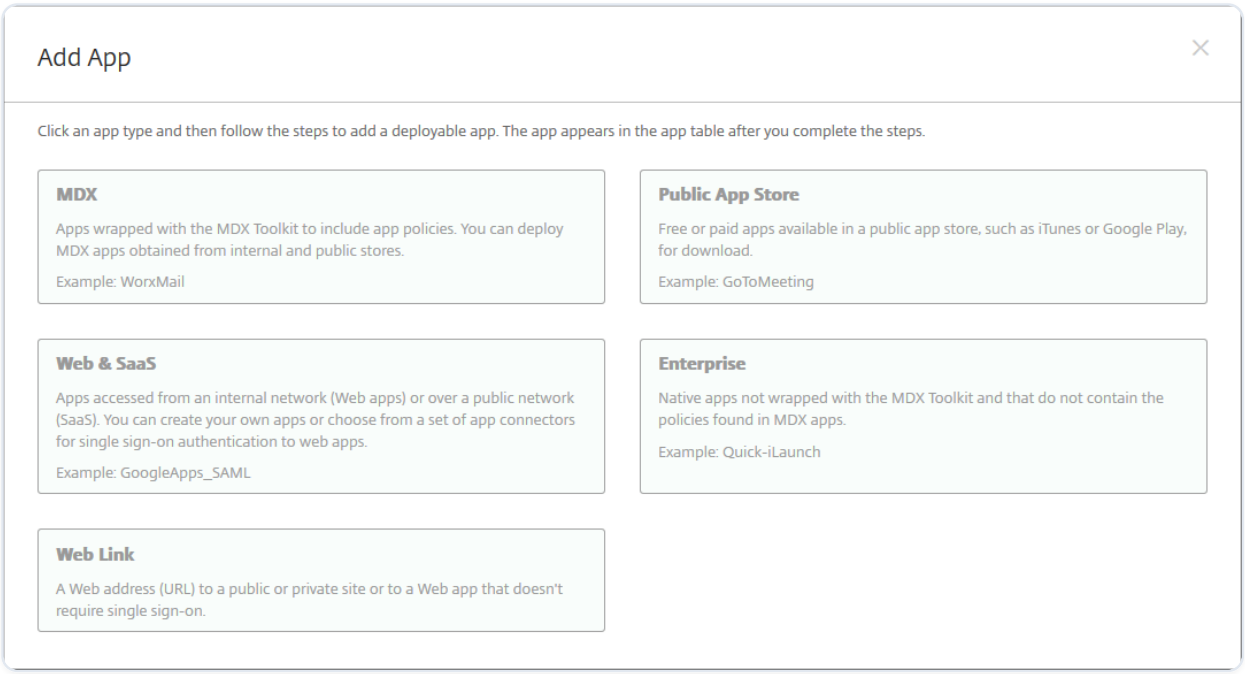
Você pode adicionar aplicativos gratuitos ou pagos ao XenMobile que estão disponíveis em uma loja de aplicativos pública, como a Apple App Store ou o Google Play.

Você pode configurar as definições para recuperar nomes e descrições de aplicativos da Apple App Store. Quando você recupera as informações do aplicativo da loja, o XenMobile sobrescreve o nome e a descrição existentes. Configure manualmente as informações do aplicativo da Google Play Store.

Ao adicionar um aplicativo pago da loja de aplicativos pública para Android Enterprise, você pode revisar o status de licenciamento de Compra em Massa. Esse status é o número total de licenças disponíveis, o número atualmente em uso e o endereço de e-mail de cada usuário que consome as licenças. O plano de Compra em Massa para Android Enterprise simplifica o processo de encontrar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Configure as informações do aplicativo e escolha as plataformas para as quais o aplicativo será entregue:

1. No console do XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



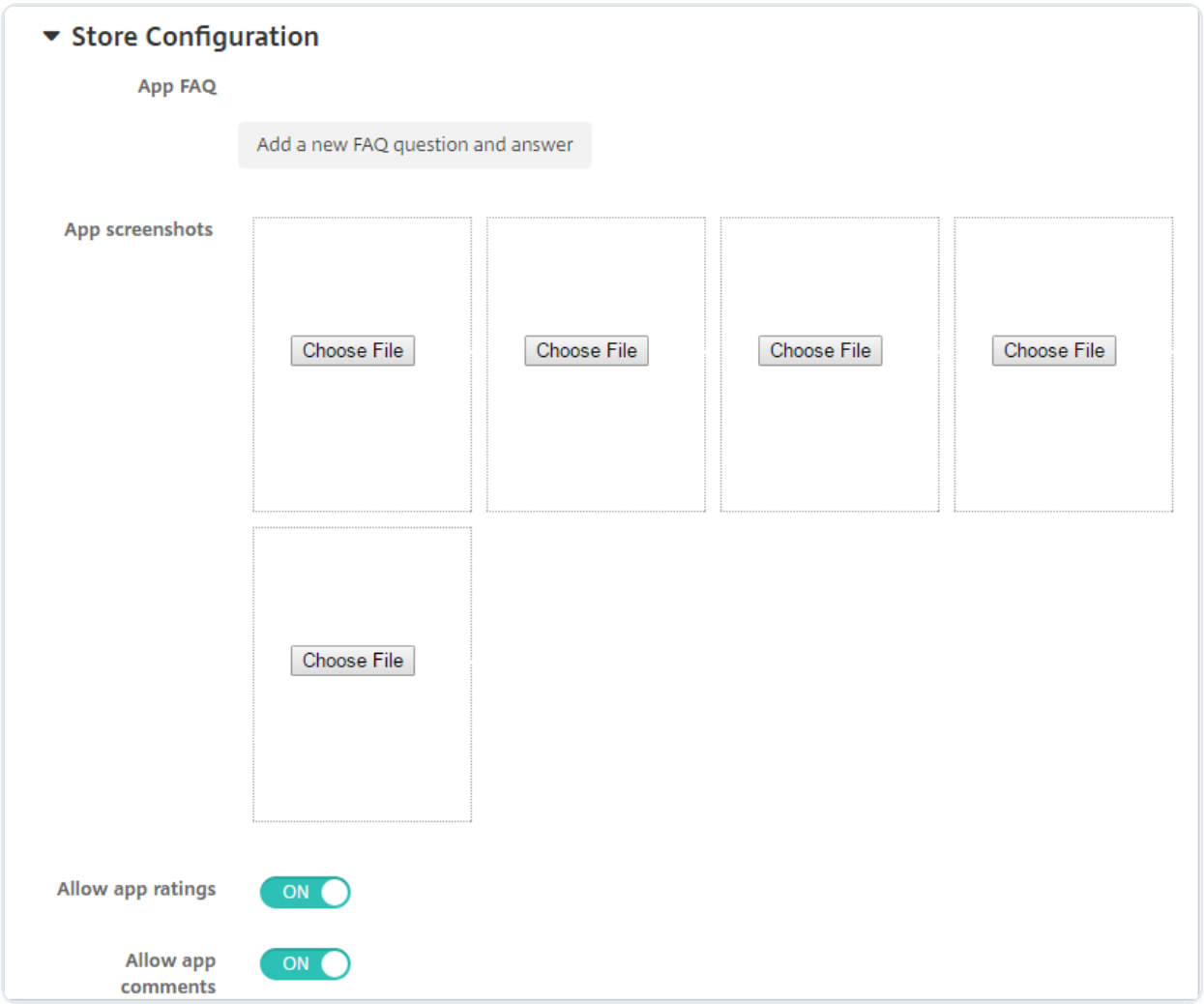
2. Clique em **Loja de Aplicativos Pública**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do Aplicativo**, digite as seguintes informações:
    - **Nome:** Digite um nome descritivo para o aplicativo. Este nome aparece em **Nome do Aplicativo** na tabela **Aplicativos**.
    - **Descrição:** Digite uma descrição opcional do aplicativo.
    - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
4. Clique em **Avançar**. A página **Plataformas de Aplicativo** é exibida.
5. Em **Plataformas**, selecione as plataformas que você deseja adicionar. Se você estiver configurando apenas para uma plataforma, desmarque as outras.

Em seguida, você configura as definições do aplicativo para cada plataforma. Consulte:

- Configurar definições de aplicativo para aplicativos do Google Play
- Aplicativos de loja de aplicativos gerenciados
- Configurar definições de aplicativo para aplicativos iOS

Ao terminar de configurar as definições para uma plataforma, defina as regras de implantação da plataforma e a configuração da loja de aplicativos.

1. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
2. Expanda **Configuração da Loja**.



- **FAQ do aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar uma FAQ para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações de aplicativos:** Permita que os usuários classifiquem o aplicativo na loja de aplicativos.
- **Permitir comentários de aplicativos:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

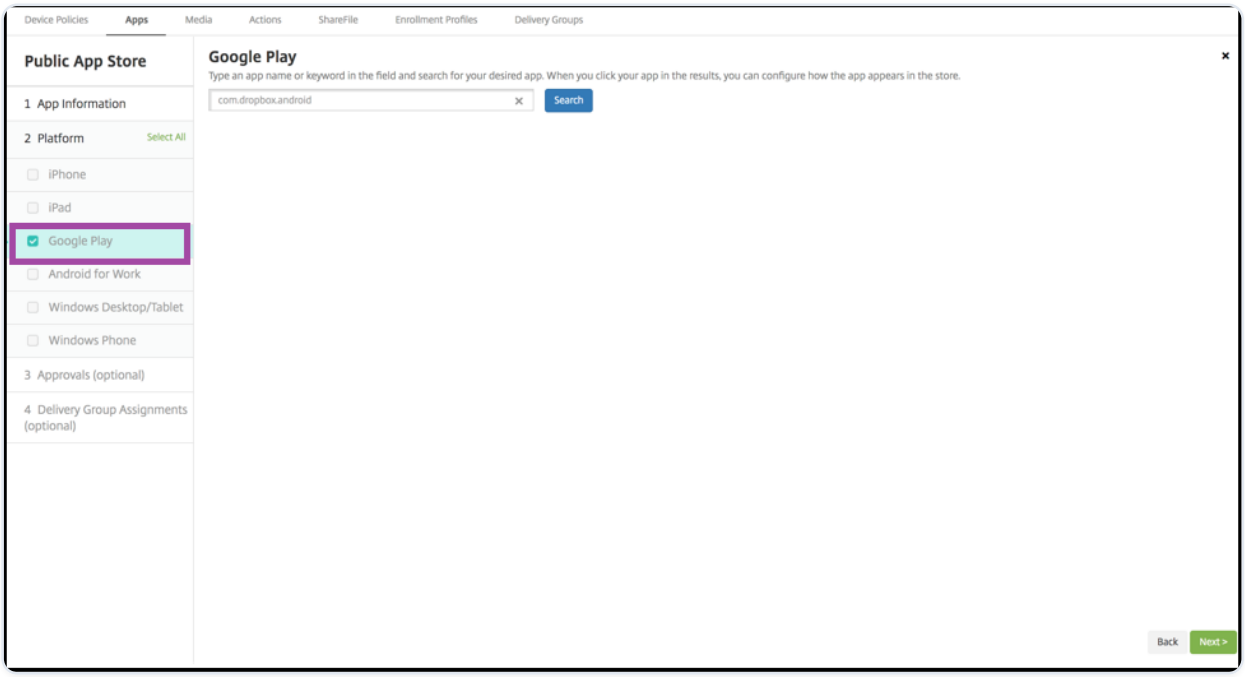
Configurar as configurações de aplicativos para aplicativos do Google Play

> **Observação:**
>
> Para tornar todos os aplicativos da Google Play Store acessíveis a partir do Google Play gerenciado, use a propriedade do XenMobile Server **Acessar todos os aplicativos na Google Play Store gerenciada**. Consulte Propriedades do servidor. Definir esta

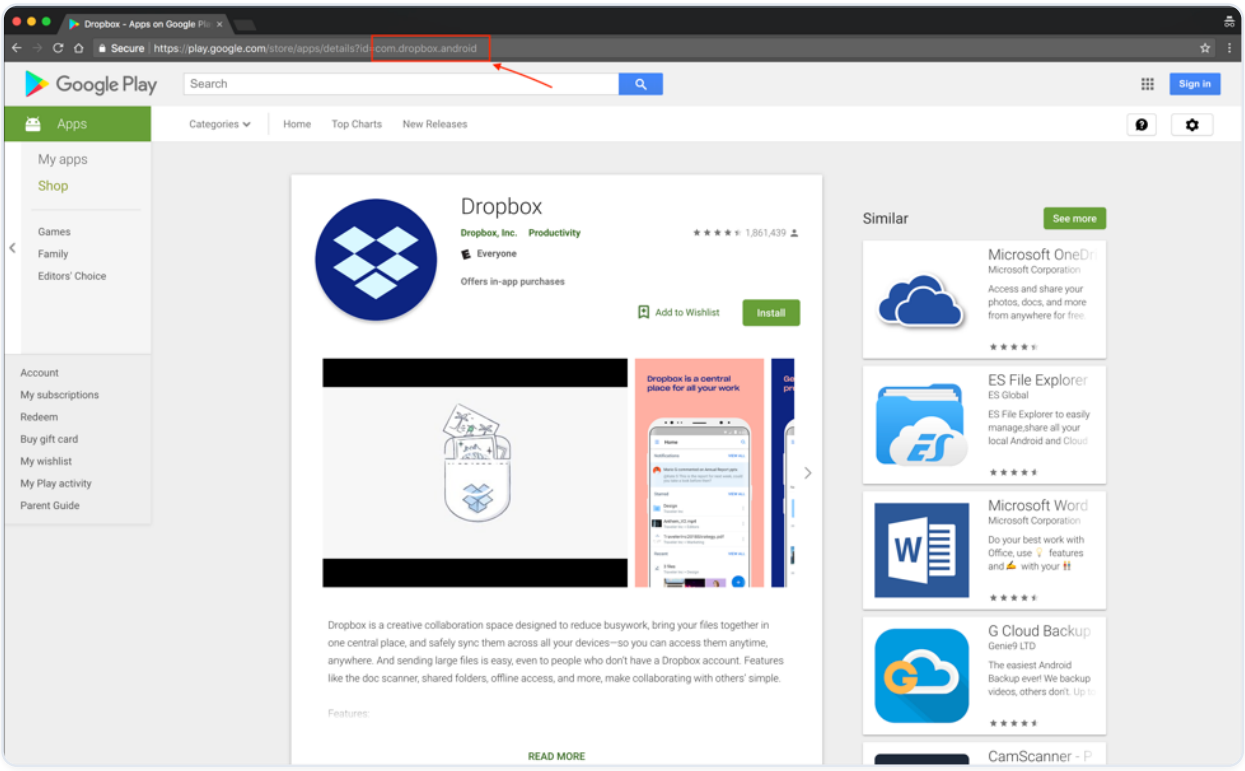
propriedade como **true** permite os aplicativos públicos da Google Play Store para todos os usuários do Android Enterprise. Você pode então usar a política de dispositivo Restrições para controlar o acesso a esses aplicativos.

A configuração das configurações de aplicativos da Google Play Store requer etapas diferentes das dos aplicativos para outras plataformas. Você deve configurar manualmente as informações do aplicativo da Google Play Store.

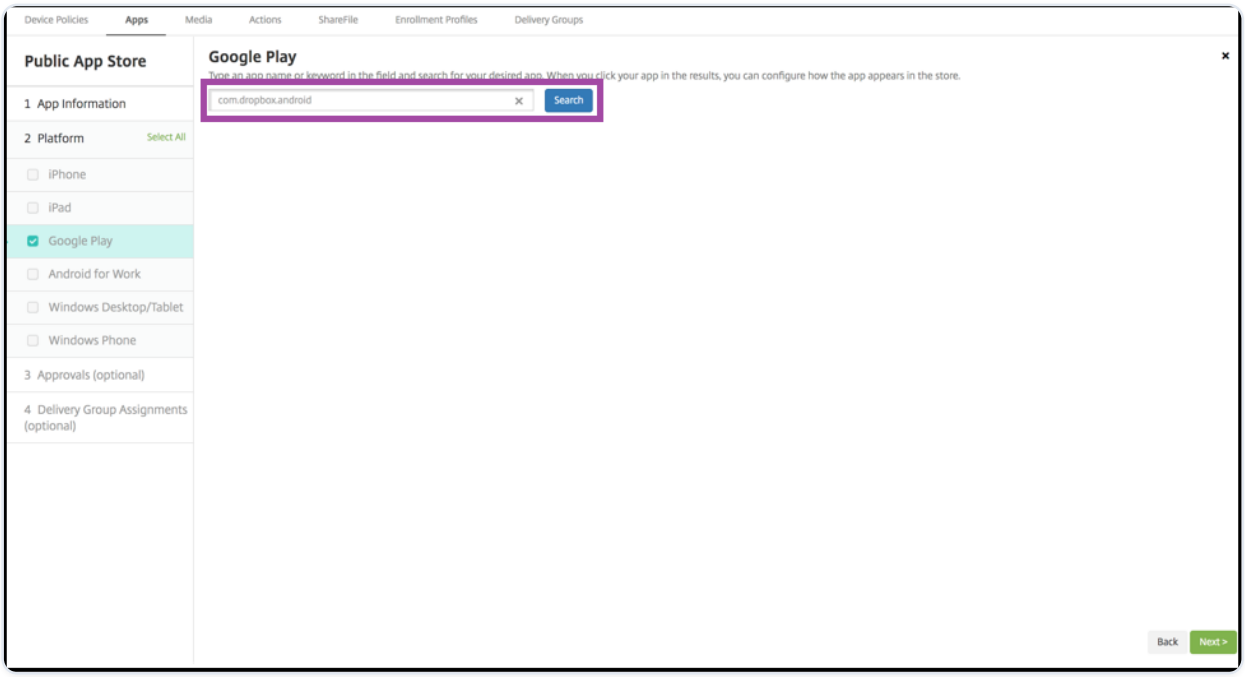
1. Certifique-se de que **Google Play** esteja selecionado em **Plataformas**.



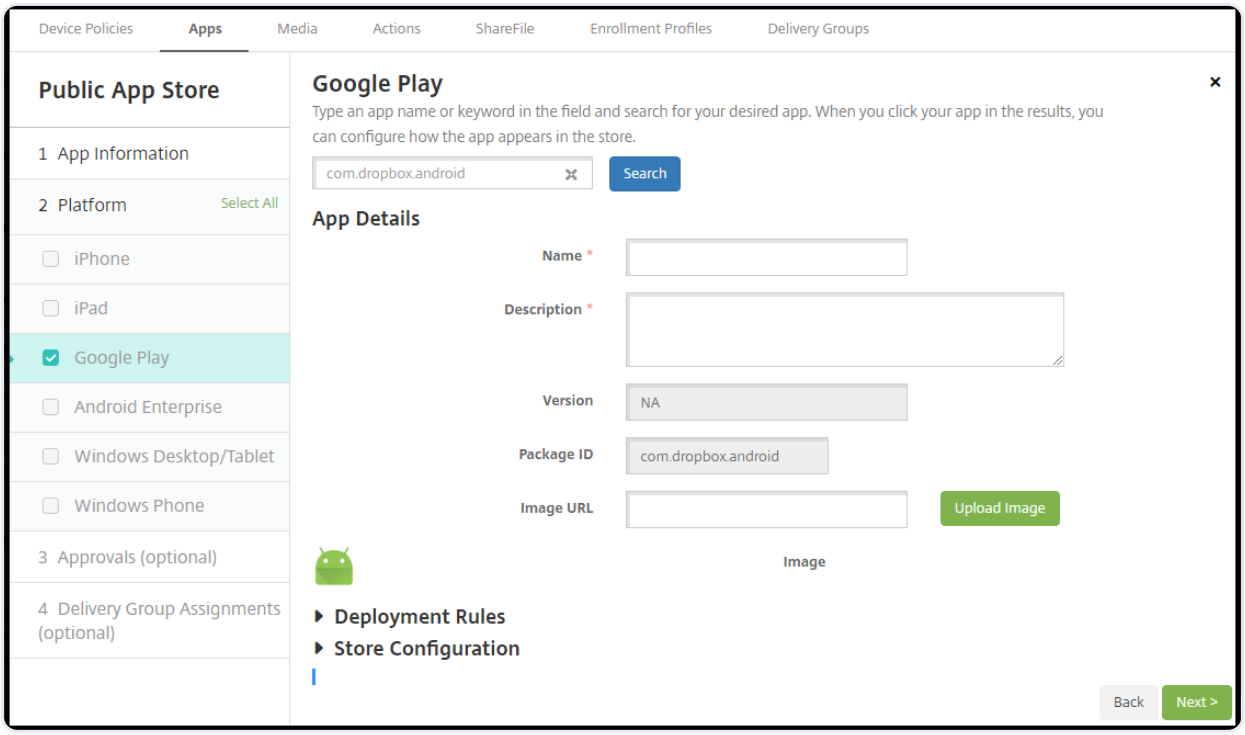
2. Vá para a Google Play Store. Na Google Play Store, copie o ID do pacote. O ID pode ser encontrado na URL do aplicativo.



3. Ao adicionar um aplicativo da Loja Pública no console do XenMobile Server, cole o ID do pacote na barra de pesquisa. Clique em **Pesquisar**.



4. Se o ID do pacote for válido, uma interface de usuário aparecerá, permitindo que você insira os detalhes do aplicativo.



5. Você pode configurar a URL da imagem para aparecer com o aplicativo na loja. Para usar a imagem da Google Play Store:

    a. Vá para a Google Play Store. Clique com o botão direito do mouse na imagem do aplicativo e copie o endereço da imagem.

    b. Cole o endereço da imagem no campo **URL da Imagem**.

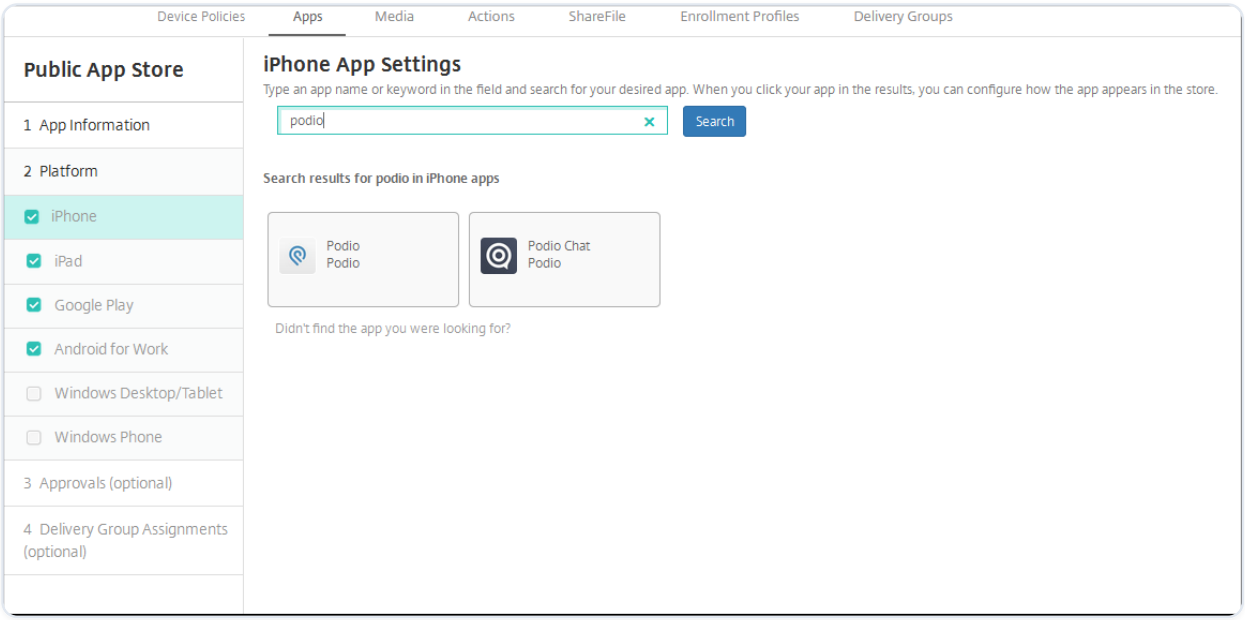
    c. Clique em **Carregar imagem**. A imagem aparece ao lado de **Imagem**.

Se você não configurar uma imagem, a imagem genérica do Android aparecerá com o aplicativo.

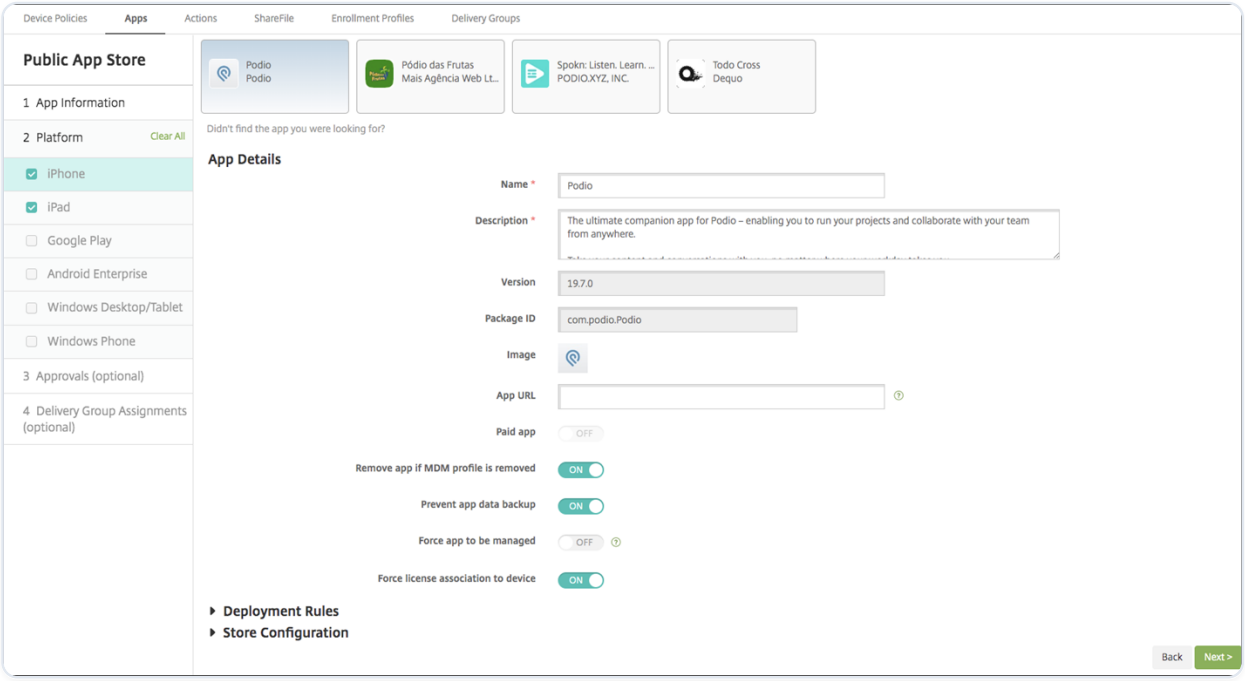
Configurar as definições do aplicativo para aplicativos iOS

1. Digite o nome do aplicativo na caixa de pesquisa e clique em **Pesquisar**. Os aplicativos que correspondem aos critérios de pesquisa aparecem. Os aplicativos que correspondem aos critérios de pesquisa aparecem.

    A figura a seguir mostra o resultado da pesquisa por **podio** em aplicativos em um iPhone.



2. Clique no aplicativo que você deseja adicionar.
3. Os campos **Detalhes do Aplicativo** são preenchidos automaticamente com informações relacionadas ao aplicativo escolhido (incluindo o nome, descrição, número da versão e imagem associada).

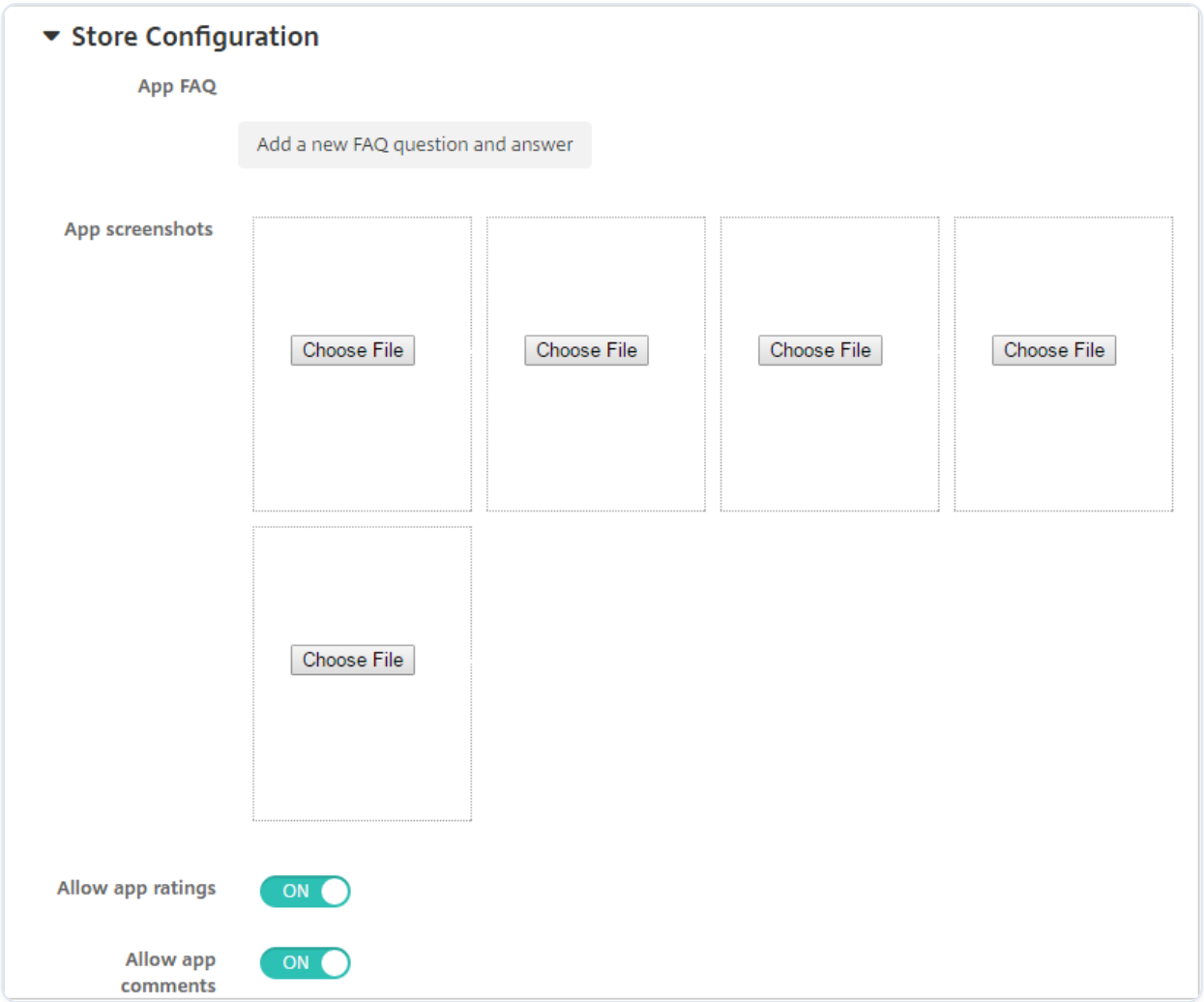


4. Configure as definições:

   - Se necessário, altere o nome e a descrição do aplicativo.
   - **Aplicativo pago:** Este campo é pré-configurado e não pode ser alterado.
   - **Remover aplicativo se o perfil MDM for removido:** Selecione se deseja remover o aplicativo se o perfil MDM for removido. O padrão é **ATIVADO**.

- **Impedir backup de dados do aplicativo:** Selecione se deseja impedir que o aplicativo faça backup de dados. O padrão é **ATIVADO**.
- **Faixa de produto:** Especifique qual faixa de produto você deseja enviar para os dispositivos dos usuários. Se você tiver uma faixa projetada para testes, poderá selecioná-la e atribuí-la aos seus usuários. O padrão é **Produção**.
- **Forçar o aplicativo a ser gerenciado:** Selecione se, quando o aplicativo for instalado sem gerenciamento, os usuários devem ser solicitados a permitir que o aplicativo seja gerenciado em dispositivos não supervisionados. O padrão é **DESATIVADO**. Disponível no iOS 9.0 e posterior.
- **Forçar licença para associação a dispositivo:** Selecione se deseja associar um aplicativo desenvolvido com associação de dispositivo habilitada a um dispositivo em vez de a um usuário. Disponível no iOS 9 e posterior. Se o aplicativo escolhido não suportar a atribuição a um dispositivo, este campo não poderá ser alterado.

5. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
6. Expanda **Configuração da Loja**.



- **Perguntas frequentes do aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar um FAQ para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** Permita que os usuários classifiquem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

7. Para iPhone ou iPad, expanda **Compra por Volume**.

   a. Para permitir que o XenMobile aplique uma licença de compra por volume para o aplicativo: Na lista **Licença de compra por volume**, clique em **Carregar uma licença de compra por volume**.

   b. Na caixa de diálogo que aparece, importe a licença.

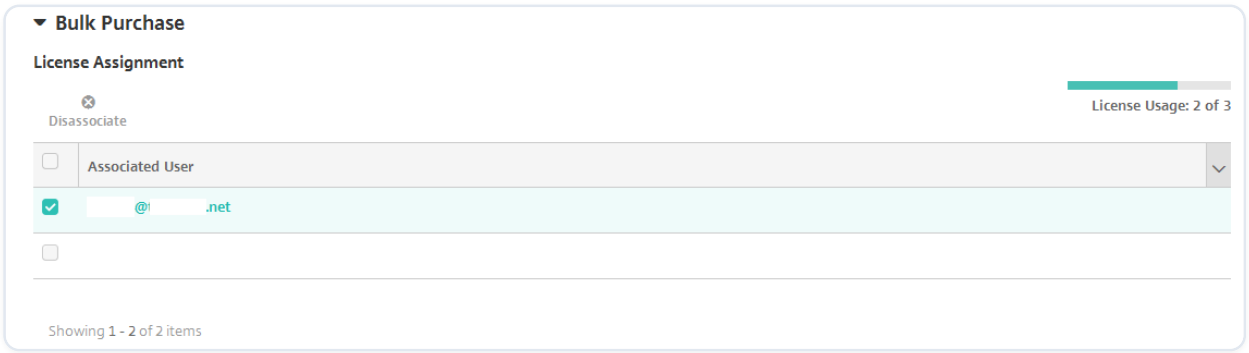
      A tabela Atribuição de Licenças mostra o número de licenças em uso para o aplicativo, do total de licenças disponíveis.

      Você pode desassociar licenças de Compra por Volume para um usuário individual. Isso encerra as atribuições de licença e libera licenças.

8. Para Android Enterprise, expanda a seção **Compra em Massa**.

   A tabela Atribuição de Licenças mostra o número de licenças em uso para o aplicativo, do total de licenças disponíveis.

   Você pode selecionar um usuário e, em seguida, clicar em **Desassociar** para encerrar a atribuição de licença e liberar uma licença para outro usuário. No entanto, você só pode desassociar a licença se o usuário não fizer parte de um grupo de entrega que contenha o aplicativo específico.



9. Depois de concluir as configurações de **Compra por Volume** ou **Compra em Massa**, clique em **Avançar**. A página **Aprovações** é exibida.

   Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não precisar de fluxos de trabalho de aprovação, continue com a próxima etapa.

10. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.
11. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um grupo ou grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
12. Expanda **Agendamento de Implantação** e configure as seguintes configurações:

    - **Implantar:** Escolha se deseja implantar o aplicativo nos dispositivos. O padrão é **Ativado**.
    - **Agendamento de implantação:** Escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
    - **Condição de implantação:** Escolha **Em cada conexão** para implantar o aplicativo toda vez que o dispositivo se conectar. Escolha **Somente quando a implantação anterior falhou** para implantar o aplicativo quando o dispositivo não conseguiu recebê-lo anteriormente. O padrão é **Em cada conexão**.

    A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

    O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você faça se aplicam a todas as plataformas, exceto para **Deploy for always-on connection**.

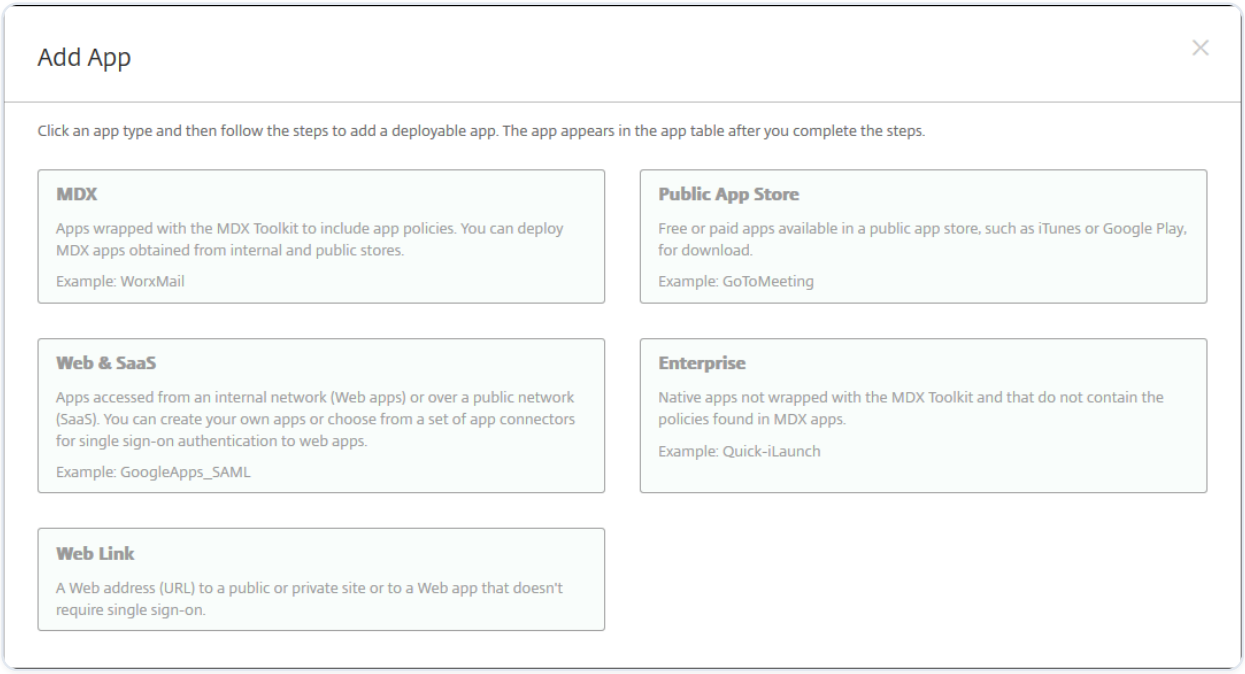
13. Clique em **Salvar**.

Adicionar um aplicativo Web ou SaaS

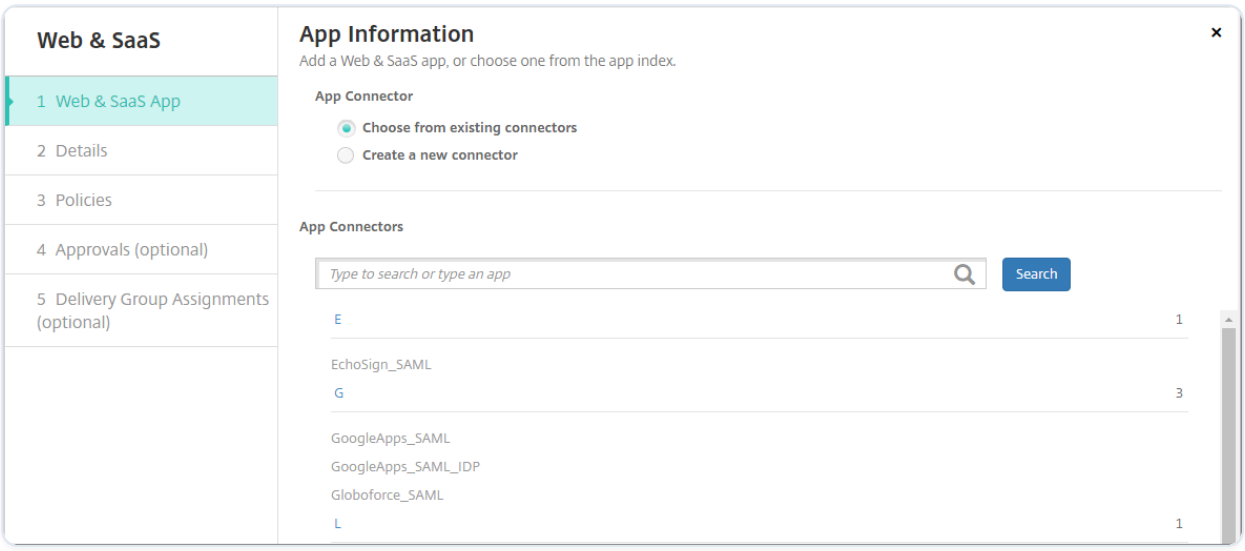
Usando o console do XenMobile, você pode conceder aos usuários autorização de logon único (SSO) para seus aplicativos móveis, corporativos, web e SaaS. Você pode habilitar aplicativos para SSO usando modelos de conector de aplicativo. Para obter uma lista de tipos de conector disponíveis no XenMobile, consulte Tipos de conector de aplicativo. Você também pode criar seu próprio conector no XenMobile ao adicionar um aplicativo Web ou SaaS.

Se um aplicativo estiver disponível apenas para SSO: Depois de salvar as configurações, o aplicativo aparece na guia **Aplicativos** no console do XenMobile.

1. No console do XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Web e SaaS**. A página **Informações do Aplicativo** é exibida.



3. Configure um conector de aplicativo existente ou novo da seguinte forma.

Para configurar um conector de aplicativo existente

1. Na página **Informações do Aplicativo**, **Escolher entre conectores existentes** já está selecionado, conforme mostrado anteriormente. Clique no conector que você deseja usar na lista **Conectores de Aplicativo**. As informações do conector do aplicativo são exibidas.

2. Configure estas configurações:

- **Nome do aplicativo:** Aceite o nome preenchido automaticamente ou digite um novo nome.
- **Descrição do aplicativo:** Aceite a descrição preenchida automaticamente ou digite uma sua.
- **URL:** Aceite a URL preenchida ou digite o endereço web para o aplicativo. Dependendo do conector que você escolher, este campo pode conter um espaço reservado que você deve substituir antes de poder ir para a próxima página.
- **Nome de domínio:** Se aplicável, digite o nome de domínio do aplicativo. Este campo é obrigatório.
- **Aplicativo hospedado na rede interna:** Selecione se o aplicativo está sendo executado em um servidor na sua rede interna. Se os usuários se conectarem de um local remoto ao aplicativo interno, eles deverão se conectar por meio do Citrix Gateway. Definir esta opção como **ON** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do Citrix Gateway. O padrão é **OFF**.
- **Categoria do aplicativo:** Na lista, clique em uma categoria opcional para aplicar ao aplicativo.
- **Provisionamento de conta de usuário:** Selecione se deseja criar contas de usuário para o aplicativo. Se você usar o conector Globoforce_SAML, deverá habilitar esta opção para garantir a integração SSO perfeita.
- Se você habilitar o **Provisionamento de conta de usuário**, configure estas definições:
  - **Conta de Serviço**
    - **Nome de usuário:** Digite o nome do administrador do aplicativo. Este campo é obrigatório.
    - **Senha:** Digite a senha do administrador do aplicativo. Este campo é obrigatório.
  - **Conta de Usuário**
    - **Quando o direito de usuário termina:** Na lista, clique na ação a ser tomada quando os usuários não tiverem mais permissão para acessar o aplicativo. O padrão é **Desabilitar conta**.
  - **Regra de Nome de Usuário**
    - Para cada regra de nome de usuário que você deseja adicionar, faça o seguinte:

    - **Atributos de usuário:** Na lista, clique no atributo de usuário a ser adicionado à regra.
    - **Comprimento (caracteres):** Na lista, clique no número de caracteres do atributo de usuário a ser usado na regra de nome de usuário. O padrão é **Todos**.
    - **Regra:** Cada atributo de usuário que você adiciona é automaticamente anexado à regra de nome de usuário.

- **Requisito de Senha**
    - **Comprimento:** Digite o comprimento mínimo da senha do usuário. O padrão é **8**.
- **Expiração da Senha**
    - **Validade (dias):** Digite o número de dias em que a senha é válida. Os valores válidos são **0–90**. O padrão é 90.
    - **Redefinir senha automaticamente após a expiração:** Selecione se deseja redefinir a senha automaticamente quando ela expirar. O padrão é **DESATIVADO**. Se você não habilitar este campo, os usuários não poderão abrir o aplicativo após a expiração de suas senhas.

Para configurar um novo conector de aplicativo

1. Na página **Informações do Aplicativo**, selecione **Criar um novo conector**. Os campos do conector do aplicativo aparecerão.

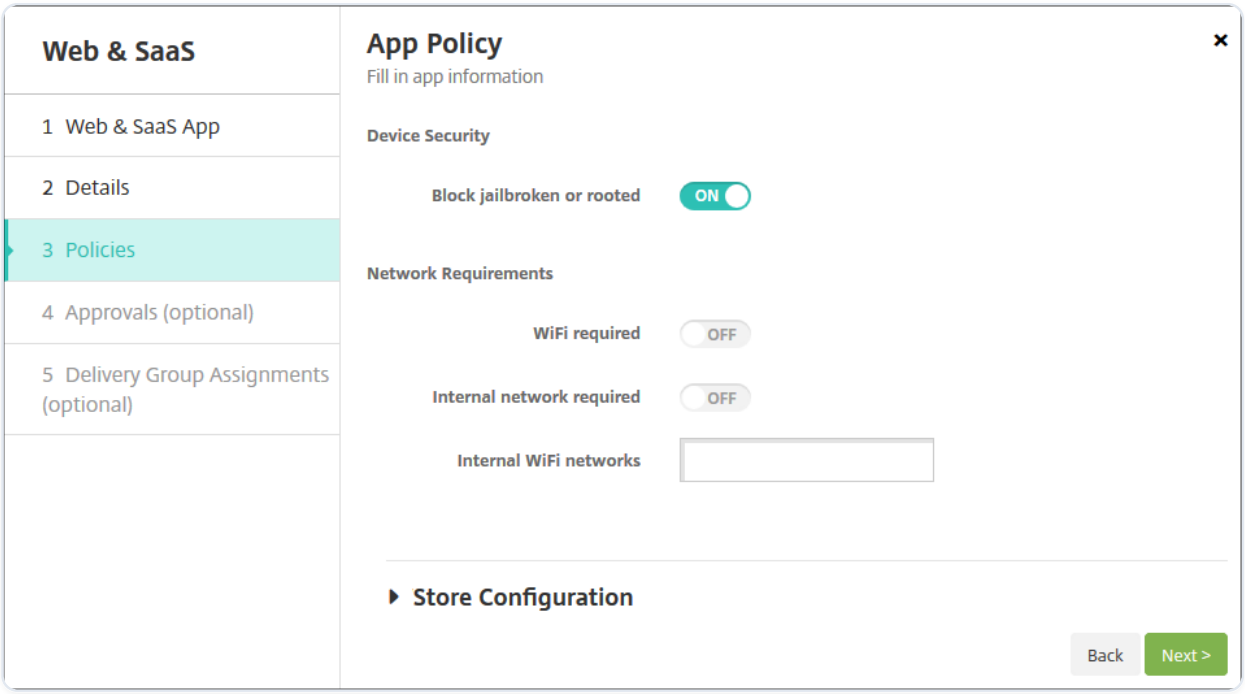
   Tela de configuração de aplicativos(/en-us/xenmobile/server/media/configure-apps-web-saas-add-app-connector.png)

2. Configure estas configurações:

    - **Nome:** Digite um nome para o conector. Este campo é obrigatório.
    - **Descrição:** Digite uma descrição para o conector. Este campo é obrigatório.
    - **URL de Logon:** Digite, ou copie e cole, a URL onde os usuários fazem logon no site. Por exemplo, se o aplicativo que você deseja adicionar tiver uma página de logon, abra um navegador da web e vá para a página de logon do aplicativo. Por exemplo, pode ser `https://www.example.com/logon`. Este campo é obrigatório.
    - **Versão SAML:** Selecione **1.1** ou **2.0**. O padrão é **1.1**.
    - **ID da Entidade:** Digite a identidade para o aplicativo SAML.

- **URL de estado de retransmissão:** Digite o endereço da web para o aplicativo SAML. A URL de estado de retransmissão é a URL de resposta do aplicativo.
- **Formato do ID de Nome:** Selecione **Endereço de E-mail** ou **Não especificado**. O padrão é **Endereço de E-mail**.
- **URL ACS:** Digite a URL do Serviço de Consumidor de Asserção do provedor de identidade ou provedor de serviços. A URL ACS fornece aos usuários capacidade de SSO.
- **Imagem:** Selecione se deseja usar a imagem padrão do Citrix ou carregar sua própria imagem de aplicativo. O padrão é Usar padrão.
  - Para carregar sua própria imagem, clique em **Procurar** e navegar até o local do arquivo. O arquivo deve ser um arquivo .PNG. Você não pode carregar um arquivo JPEG ou GIF. Ao adicionar um gráfico personalizado, você não poderá alterá-lo posteriormente.

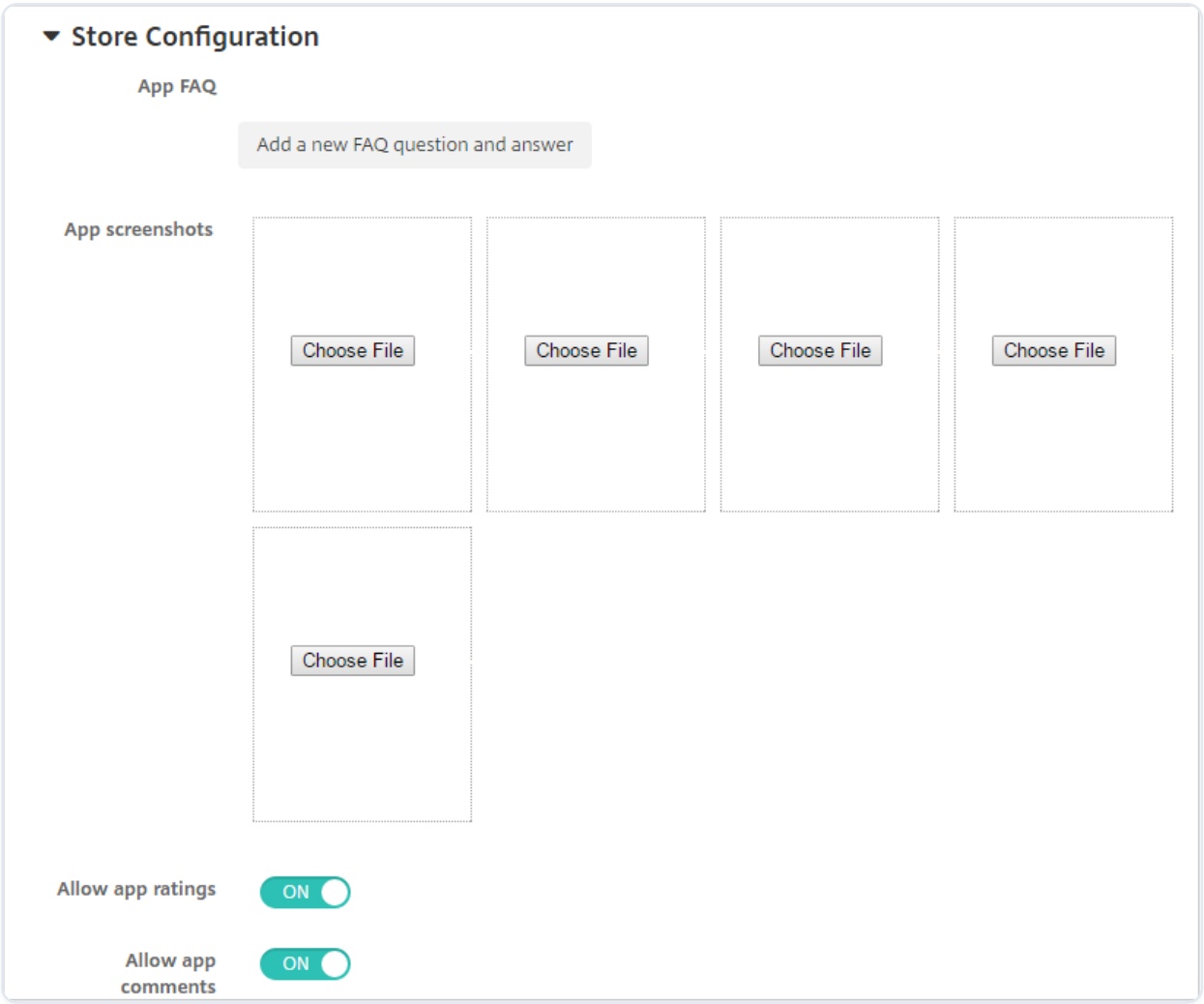
3. Quando terminar, clique em **Adicionar**. A página **Detalhes** é exibida.
4. Clique em **Avançar**. A página **Política de Aplicativo** é exibida.



5. Configure estas configurações:
   - **Segurança do Dispositivo**
   - **Bloquear jailbroken ou com root:** Selecione se deseja bloquear dispositivos com jailbreak ou root de acessar o aplicativo. O padrão é **ATIVADO**.
   - **Requisitos de Rede**

- **WiFi necessário:** Selecione se uma conexão Wi-Fi é necessária para executar o aplicativo. O padrão é **DESATIVADO**.
- **Rede interna necessária:** Selecione se uma rede interna é necessária para executar o aplicativo. O padrão é **DESATIVADO**.
- **Redes Wi-Fi internas:** Se você ativou **WiFi necessário**, digite as redes Wi-Fi internas a serem usadas.

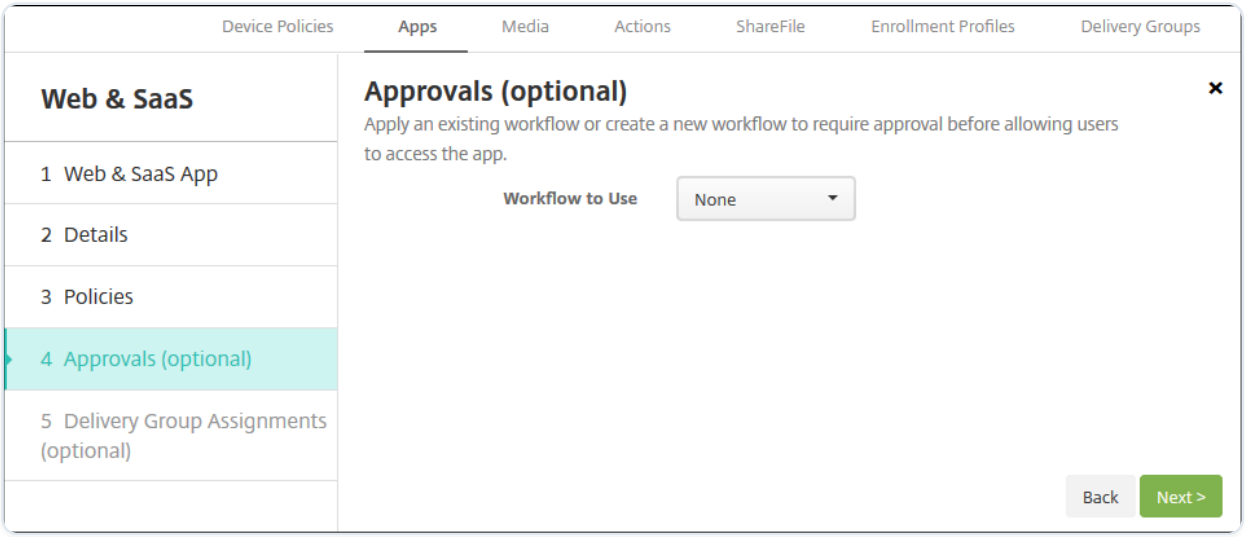
6. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
7. Expanda **Configuração da Loja**.



- **Perguntas Frequentes do Aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar um FAQ para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** Permita que os usuários classifiquem o aplicativo na loja de aplicativos.

- **Permitir comentários do aplicativo:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

8. Clique em **Avançar**. A página **Aprovações** é exibida.



Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho.

9. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.
10. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um ou mais grupos. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
11. Expanda **Agendamento de Implantação** e configure as seguintes configurações:

    - **Implantar:** Escolha se deseja implantar o aplicativo em dispositivos. O padrão é **Ativado**.
    - **Agendamento de implantação:** Escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
    - **Condição de implantação:** Escolha **Em cada conexão** para implantar o aplicativo toda vez que o dispositivo se conectar. Escolha **Somente quando a implantação anterior falhou** para implantar o aplicativo quando o dispositivo falhou em receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

    A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações que você fizer se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.

12. Clique em **Salvar**.

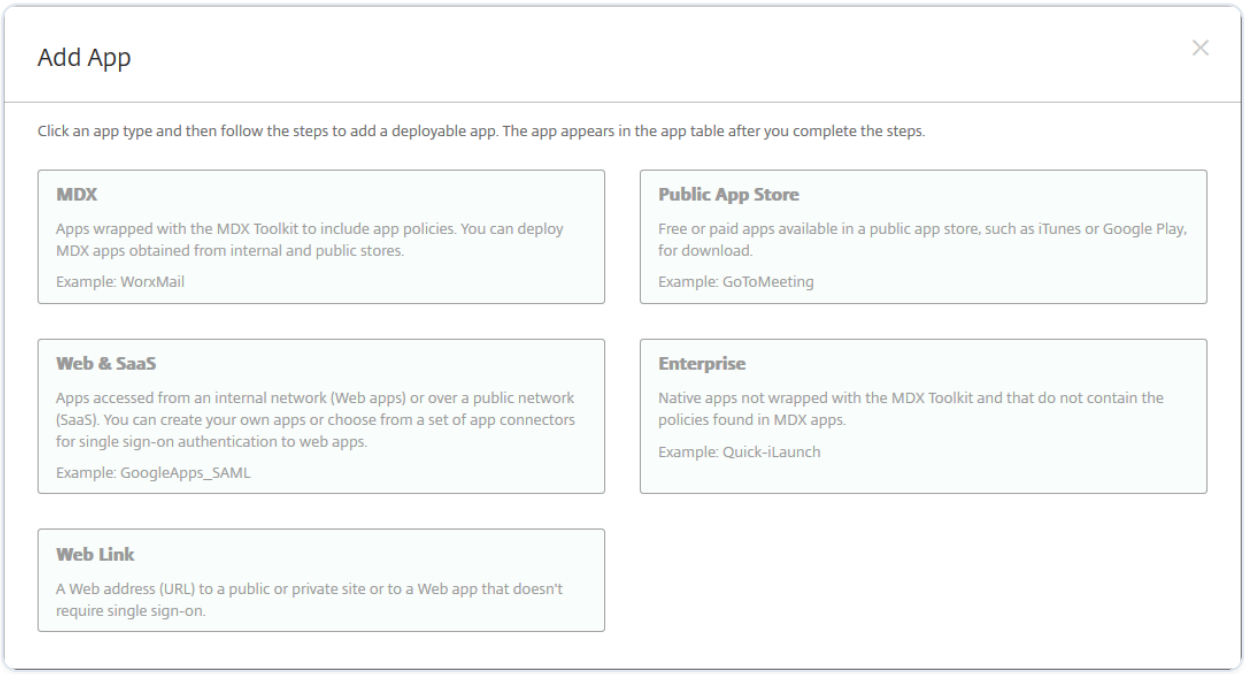
Adicionar um aplicativo empresarial

Aplicativos empresariais no XenMobile representam aplicativos nativos que não são preparados com o MAM SDK ou o MDX Toolkit. Esses aplicativos não contêm as políticas associadas aos aplicativos MDX. Você pode carregar um aplicativo empresarial na guia **Aplicativos** no console do XenMobile. Os aplicativos empresariais suportam as seguintes plataformas (e tipos de arquivo correspondentes):

- iOS (arquivo .ipa)
- Android (arquivo .apk)
- Samsung Knox (arquivo .apk)
- Android Enterprise (arquivo .apk)
- Consulte também: aplicativos privados habilitados para MDX

Não é suportado adicionar aplicativos baixados da Google Play Store como aplicativos empresariais. Em vez disso, adicione aplicativos da Google Play Store como aplicativos de loja de aplicativos públicos. Consulte Adicionar um aplicativo de loja de aplicativos público.

1. No console do XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Empresarial**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do Aplicativo**, digite as seguintes informações:

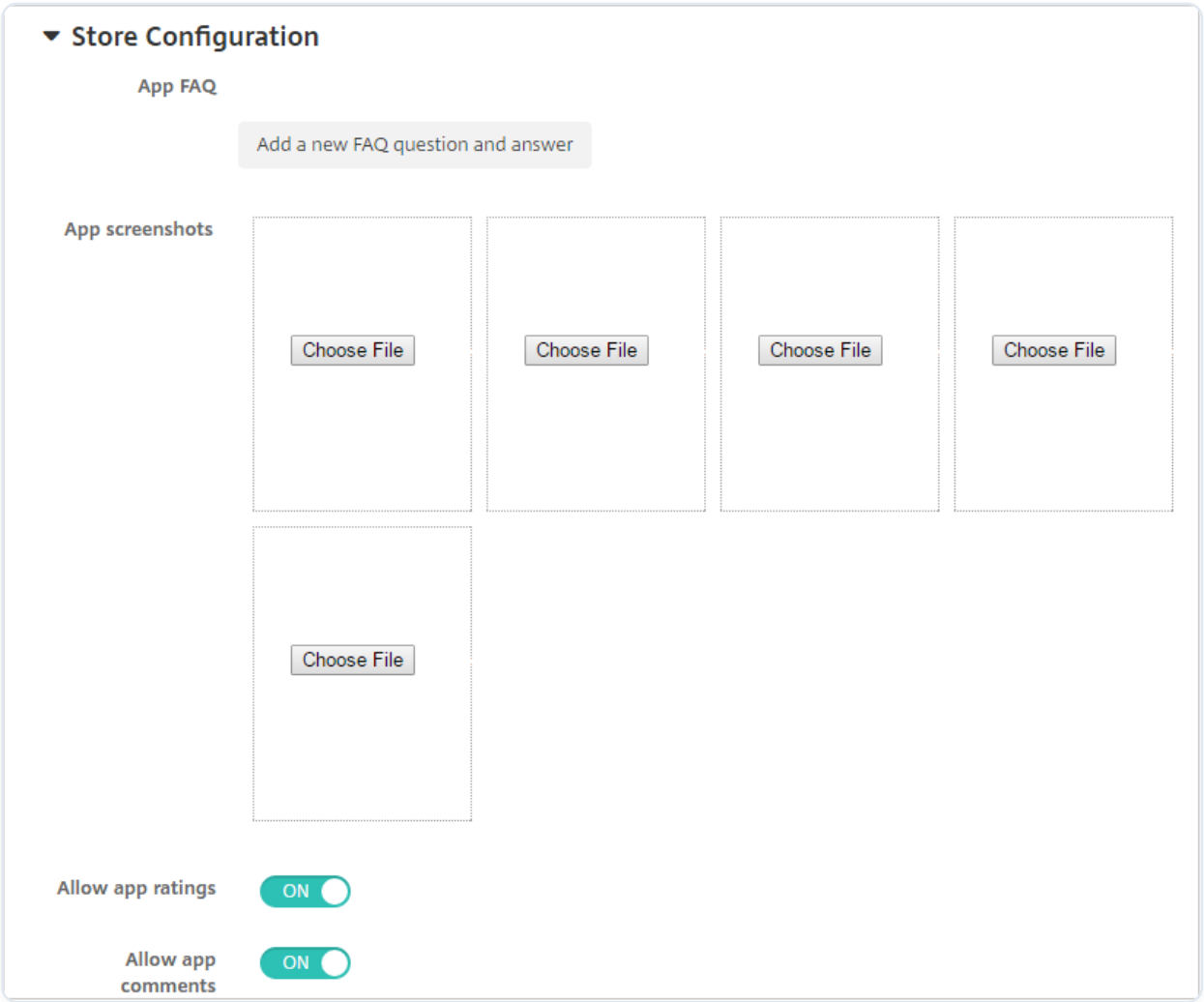
    - **Nome:** Digite um nome descritivo para o aplicativo. Este nome é listado em Nome do Aplicativo na tabela Aplicativos.
    - **Descrição:** Digite uma descrição opcional do aplicativo.
    - **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.

4. Clique em **Avançar**. A página **Plataformas de Aplicativo** é exibida.
5. Em **Plataformas**, selecione as plataformas que você deseja adicionar. Se você estiver configurando apenas para uma plataforma, desmarque as outras.
6. Para cada plataforma que você escolheu, selecione o arquivo para upload clicando em **Carregar** e navegando até o local do arquivo.
7. Clique em **Avançar**. A página de informações do aplicativo para a plataforma é exibida.
8. Configure as configurações para o tipo de plataforma, como:

    - **Nome do arquivo:** Opcionalmente, digite um novo nome para o aplicativo.
    - **Descrição do aplicativo:** Opcionalmente, digite uma nova descrição para o aplicativo.
    - **Versão do aplicativo:** Você não pode alterar este campo.
    - **Versão mínima do SO:** Opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.

- **Versão máxima do SO:** Opcionalmente, digite o sistema operacional mais recente que o dispositivo deve executar para usar o aplicativo.
- **Dispositivos excluídos:** Opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
- **ID do Pacote:** Identificador exclusivo do seu aplicativo.
- **Remover aplicativo se o perfil MDM for removido:** Selecione se deseja remover o aplicativo de um dispositivo quando o perfil MDM for removido. O padrão é **Ativado**.
- **Impedir backup de dados do aplicativo:** Selecione se deseja impedir que o aplicativo faça backup de dados. O padrão é **Ativado**.
- **Forçar gerenciamento do aplicativo:** Se você estiver instalando um aplicativo não gerenciado, selecione **Ativado** se quiser que os usuários em dispositivos não supervisionados sejam solicitados a permitir o gerenciamento do aplicativo. Se eles aceitarem o prompt, o aplicativo será gerenciado.

9. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
10. Expanda **Configuração da Loja**.



- **FAQ do aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar uma FAQ para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** Permita que os usuários classifiquem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

11. Clique em **Avançar**. A página **Aprovações** é exibida.

    Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não precisar de um fluxo de trabalho de aprovação, continue para a próxima etapa.

12. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.
13. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um grupo ou grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
14. Expanda **Agendamento de Implantação** e, em seguida, configure as seguintes configurações:

    - **Implantar:** Escolha se deseja implantar o aplicativo nos dispositivos. O padrão é **Ativado**.
    - **Agendamento de implantação:** Escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
    - **Condição de implantação:** Escolha **Em cada conexão** para implantar o aplicativo toda vez que o dispositivo se conectar. Escolha **Somente quando a implantação anterior falhou** para implantar o aplicativo quando o dispositivo não conseguiu recebê-lo anteriormente. O padrão é **Em cada conexão**.

    A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de agendamento de implantação em segundo plano em **Configurações > Propriedades do Servidor**.

    O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações feitas se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.

15. Clique em **Salvar**.

Adicionar um link da Web

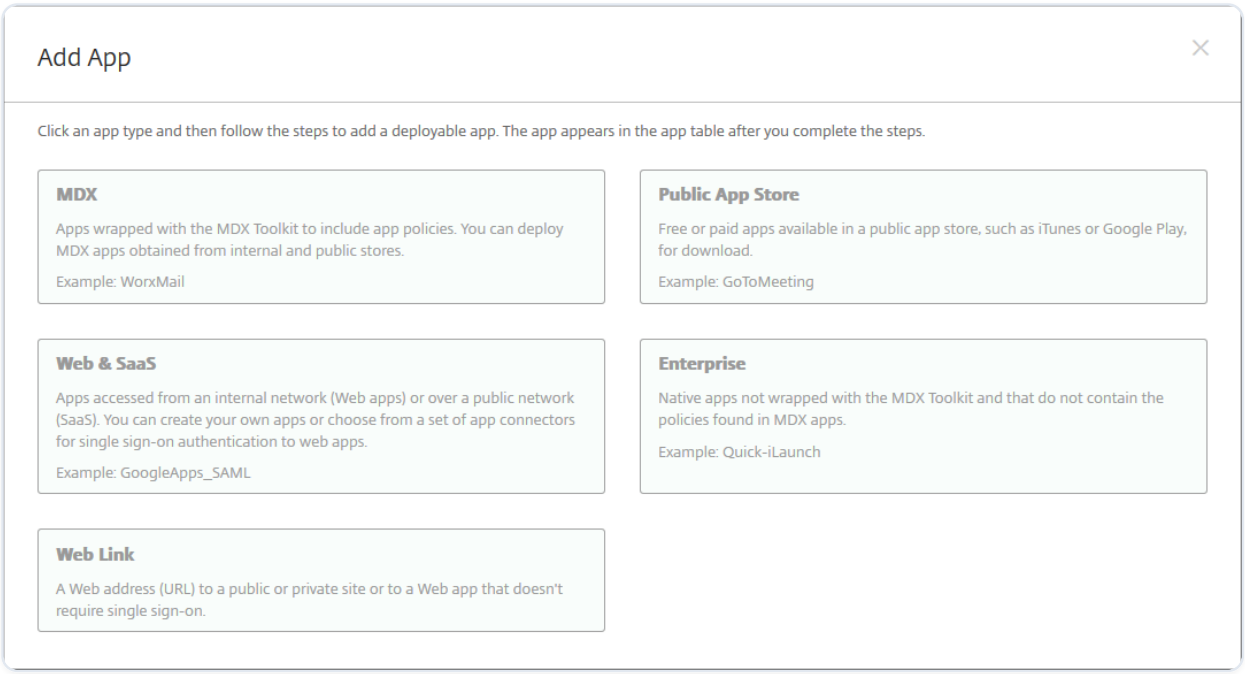
Um link da Web é um endereço da Web para um site da internet ou intranet. Um link da Web também pode apontar para um aplicativo da Web que não requer SSO. Depois de configurar um link da Web, o link aparece como um ícone na loja de aplicativos. Quando os usuários fazem logon com o Secure Hub, o link aparece com a lista de aplicativos e desktops disponíveis.

Você pode configurar links da Web na guia **Aplicativos** no console do XenMobile. Ao terminar de configurar o link da Web, ele aparece como um ícone de link na lista da tabela **Aplicativos**. Quando os usuários fazem logon com o Secure Hub, o link aparece com a lista de aplicativos e desktops disponíveis.

Para adicionar o link, forneça as seguintes informações:

- Nome do link
- Descrição do link
- Endereço da Web (URL)
- Categoria
- Função
- Imagem no formato .png (opcional)

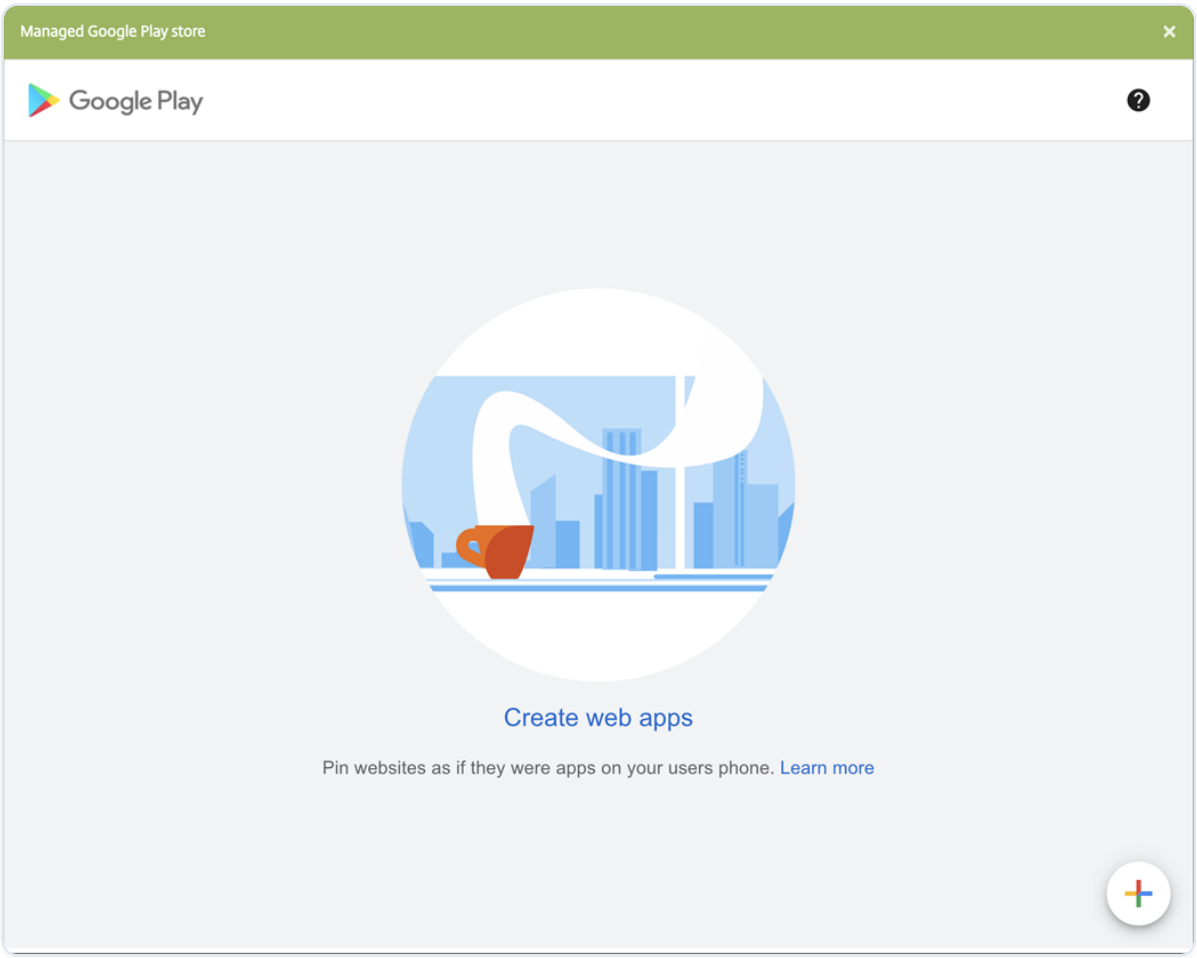
1. No console do XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Link da Web**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do Aplicativo**, digite as seguintes informações:

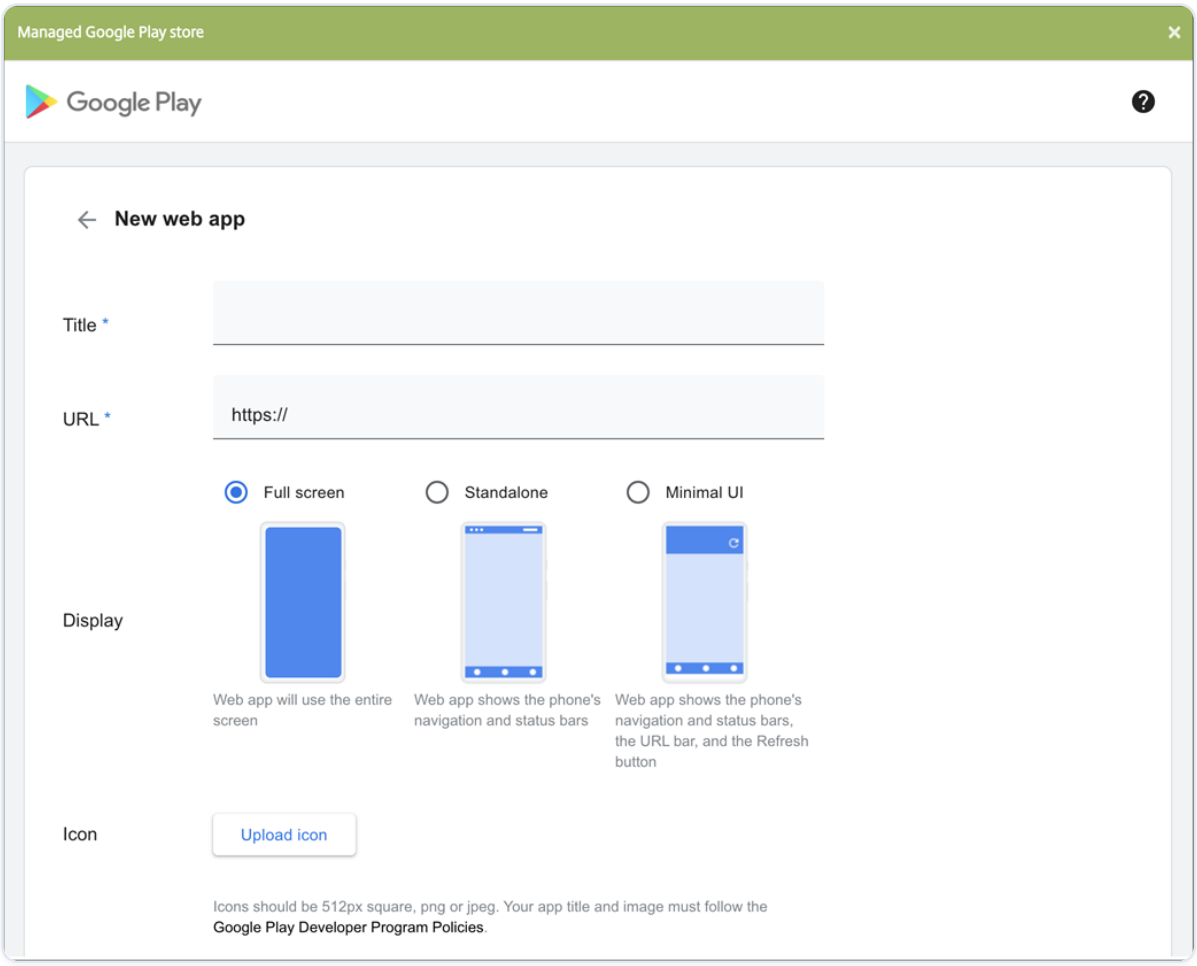
   Nome: Digite um nome descritivo para o aplicativo. Este nome é listado em Nome do Aplicativo na tabela Aplicativos. **Descrição:** Digite uma descrição opcional do aplicativo. **Categoria do aplicativo:** Opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
4. Clique em **Avançar**. A página **Plataformas de Aplicativo** é exibida.
5. Em **Plataformas**, selecione **Outras plataformas** para adicionar um aplicativo web para iOS e Android (DA herdado), ou selecione **Android Enterprise**. Desmarque a caixa de seleção que você não deseja adicionar.

   - Se você selecionar **Outras plataformas**, continue para a próxima etapa para configurar as definições.
   - Se você selecionar **Android Enterprise**, clique no botão **Carregar** para abrir a loja gerenciada do Google Play. Você não precisa se registrar para uma conta de desenvolvedor para publicar um aplicativo web. Clique no ícone **Mais** no canto inferior direito para continuar.



Configure estas definições:

- **Título:** Digite o nome para o aplicativo web.
- **URL:** Digite o endereço web para o aplicativo.
- **Exibição:** Escolha como exibir o aplicativo web nos dispositivos do usuário. As opções disponíveis são **Tela cheia**, **Autônomo** e **Interface de usuário mínima**.
- **Ícone:** Carregue sua própria imagem para representar o aplicativo web.



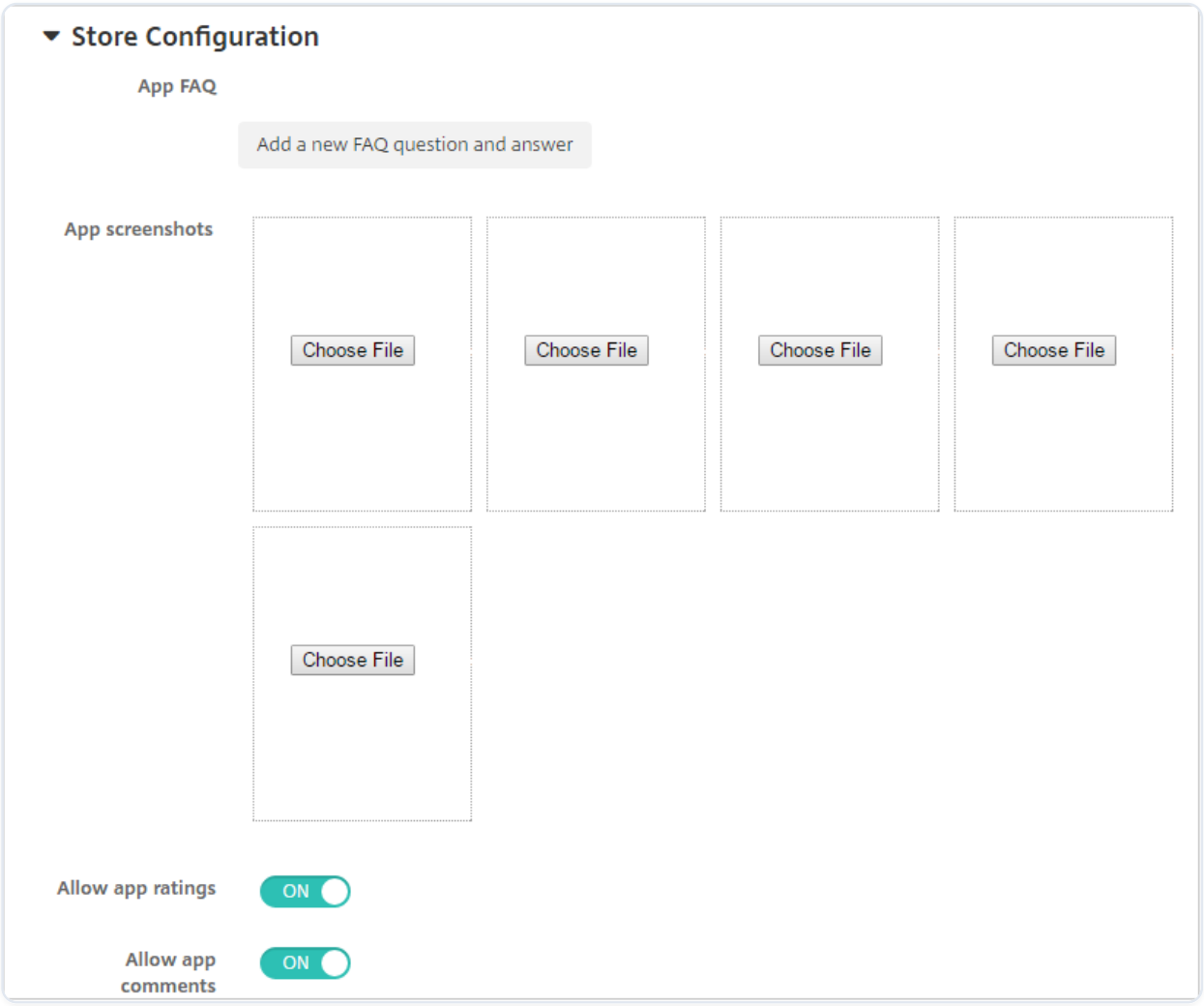
Quando terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo web seja publicado.

6. Para plataformas que não sejam o Android Enterprise, configure estas definições:

   - **Nome do aplicativo:** Aceite o nome preenchido automaticamente ou digite um novo nome.
   - **Descrição do aplicativo:** Aceite a descrição preenchida automaticamente ou digite uma sua.
   - **URL:** Aceite o URL preenchido automaticamente ou digite o endereço web do aplicativo. Dependendo do conector que você escolher, este campo pode conter um espaço reservado que você deve substituir antes de passar para a próxima página.
   - **O aplicativo está hospedado na rede interna:** Selecione se o aplicativo está sendo executado em um servidor em sua rede interna. Se os usuários se conectarem de um local remoto ao aplicativo interno, eles deverão se conectar através do Citrix Gateway. Definir esta opção como **ATIVADO** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem através do Citrix Gateway. O padrão é **DESATIVADO**.
   - **Categoria do aplicativo:** Na lista, clique em uma categoria opcional para aplicar ao aplicativo.

- **Imagem:** Selecione se deseja usar a imagem padrão do Citrix ou carregar sua própria imagem de aplicativo. O padrão é Usar padrão.
    - Para carregar sua própria imagem, clique em **Procurar** e navegar até o local do arquivo. O arquivo deve ser um arquivo .PNG. Você não pode carregar um arquivo JPEG ou GIF. Ao adicionar um gráfico personalizado, você não poderá alterá-lo posteriormente.

7. Configure as regras de implantação. Para obter informações, consulte Regras de implantação.
8. Expanda **Configuração da Loja**.



- **FAQ do aplicativo:** Clique em **Adicionar uma nova pergunta e resposta de FAQ** para criar uma FAQ para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** Adicione capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações de aplicativos:** Permita que os usuários classifiquem o aplicativo na loja de aplicativos.

- **Permitir comentários de aplicativos:** Permita que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

9. Clique em **Avançar**. A página **Atribuição de Grupo de Entrega** é exibida.
10. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione um grupo ou grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
11. Expanda **Agendamento de Implantação** e configure as seguintes configurações:

    - **Implantar:** Escolha se deseja implantar o aplicativo nos dispositivos. O padrão é **Ativado**.
    - **Agendamento de implantação:** Escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
    - **Condição de implantação:** Escolha **Em cada conexão** para implantar o aplicativo toda vez que o dispositivo se conectar. Escolha **Somente quando a implantação anterior falhou** para implantar o aplicativo quando o dispositivo não conseguiu receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

    A opção **Implantar para conexão sempre ativa** se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**.

    O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações feitas se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**.
12. Clique em **Salvar**.

Habilitar aplicativos do Microsoft 365

Você pode abrir o contêiner MDX para permitir que o Secure Mail, Secure Web e Citrix Files transfiram documentos e dados para aplicativos do Microsoft Office 365. Para obter detalhes, consulte Permitindo interação segura com aplicativos do Office 365.

Aplicar fluxos de trabalho

Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a usar:** Na lista, clique em um fluxo de trabalho existente ou clique em **Criar um novo fluxo de trabalho**. O padrão é **Nenhum**.

Se você selecionar **Criar um novo fluxo de trabalho**, configure estas definições.

- **Nome:** Digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** Opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de aprovação de e-mail:** Na lista, selecione o modelo de aprovação de e-mail a ser atribuído. Ao clicar no ícone de olho à direita deste campo, uma caixa de diálogo é exibida onde você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** Na lista, selecione o número de níveis de aprovação do gerente necessários para este fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
  - Não necessário
  - 1 nível
  - 2 níveis
  - 3 níveis
- **Selecionar domínio do Active Directory:** Na lista, selecione o domínio do Active Directory apropriado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores adicionais necessários:** Digite o nome da pessoa adicional necessária no campo de pesquisa e clique em **Pesquisar**. Os nomes são originados no Active Directory.
- Quando o nome aparecer no campo, selecione a caixa de seleção ao lado do nome. O nome e o endereço de e-mail aparecerão na lista **Aprovadores adicionais necessários selecionados**.

  Para remover uma pessoa da lista **Aprovadores adicionais obrigatórios selecionados**, faça um dos seguintes:

  - Clique em **Pesquisar** para ver uma lista de todas as pessoas no domínio selecionado.
  - Digite um nome completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar os resultados da pesquisa.
  - As pessoas na lista **Aprovadores adicionais obrigatórios selecionados** têm marcas de seleção ao lado de seus nomes na lista de resultados da pesquisa. Role a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

Marca da loja de aplicativos e do Citrix Secure Hub

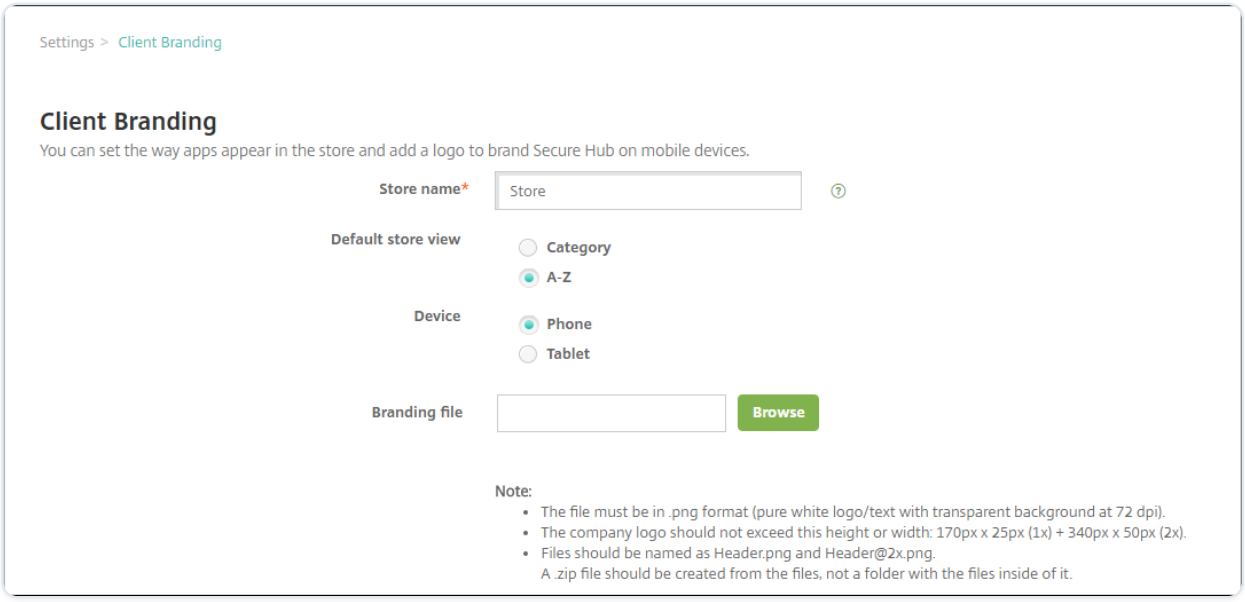
Você pode definir como os aplicativos aparecem na loja e adicionar um logotipo para personalizar o Secure Hub e a loja de aplicativos. Esses recursos de personalização estão disponíveis para dispositivos iOS e Android.

Antes de começar, certifique-se de que sua imagem personalizada esteja pronta e acessível.

A imagem personalizada deve atender a estes requisitos:

- O arquivo deve estar no formato .png
- Use um logotipo ou texto branco puro com um fundo transparente a 72 dpi.
- O logotipo da empresa não deve exceder esta altura ou largura: 170 px x 25 px (1x) e 340 px x 50 px (2x).
- Nomeie os arquivos como Header.png e `Header@2x.png`.
- Crie um arquivo .zip a partir dos arquivos, não uma pasta com os arquivos dentro dela.

1. No console do XenMobile Server, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Cliente**, clique em **Marca do Cliente**. A página **Marca do Cliente** é exibida.



Configure as seguintes configurações:

- **Nome da loja:** O nome da loja aparece nas informações da conta do usuário. Alterar o nome também altera a URL usada para acessar os serviços da loja. Geralmente, você não precisa alterar o nome padrão.

> **Importante:**
>
> O nome da loja pode conter apenas caracteres alfanuméricos.

- **Visualização padrão da loja:** Selecione **Categoria** ou **A-Z**. O padrão é **A-Z**
- **Opção de dispositivo:** Selecione **Telefone** ou **Tablet**. O padrão é **Telefone**.
- **Arquivo de identidade visual:** Selecione uma imagem ou um arquivo .zip de imagens para usar na identidade visual, clicando em **Procurar** e navegando até o local do arquivo.

3. Clique em **Salvar**.

Tipos de conector de aplicativo

A tabela a seguir lista os conectores e os tipos de conectores disponíveis no XenMobile® ao adicionar um aplicativo Web ou SaaS. Você também pode adicionar um novo conector ao XenMobile ao adicionar um aplicativo Web ou SaaS.

A tabela indica se o conector oferece suporte ao gerenciamento de contas de usuário, que permite criar novas contas automaticamente ou usando um fluxo de trabalho.

NOME DO CONECTOR	SSO SAML	OFERECE SUPORTE AO GERENCIAMENTO DE CONTAS DE USUÁRIO
EchoSign_SAML	S	S
Globoforce_SAML		**Nota:** Ao usar este conector, você deve habilitar o Gerenciamento de Usuários para Provisionamento para uma integração SSO perfeita.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S

NOME DO CONECTOR	SSO SAML	OFERECE SUPORTE AO GERENCIAMENTO DE CONTAS DE USUÁRIO
Salesforce_SAML	S	S
Salesforce_SAML_SP	S	S
SandBox_SAML	Sim	
SuccessFactors_SAML	Sim	
ShareFile_SAML	Sim	
ShareFile_SAML_SP	Sim	
WebEx_SAML_SP	Sim	Sim

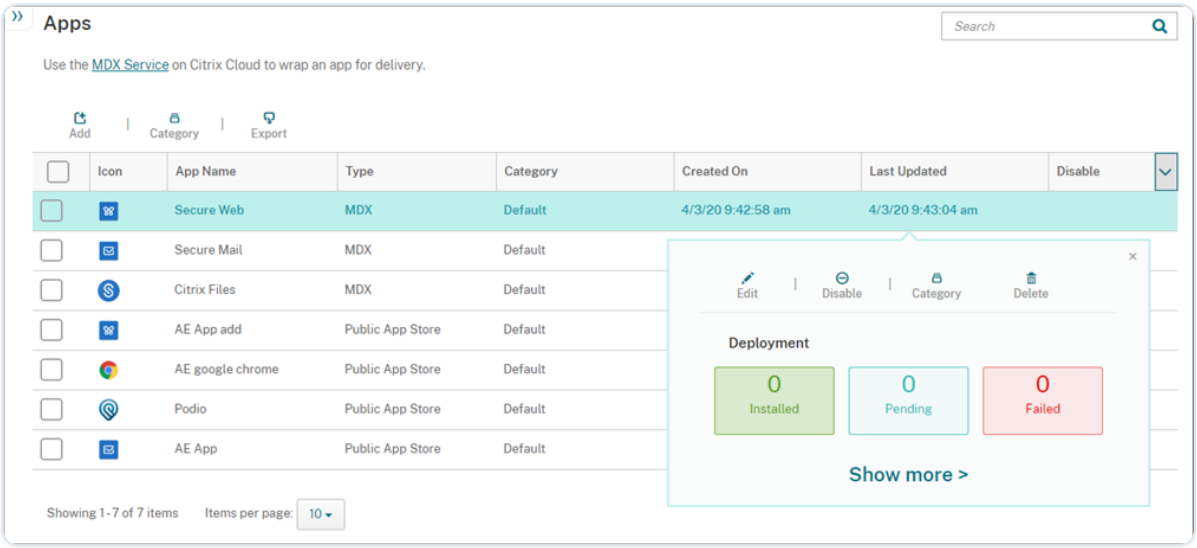
Atualizar aplicativos MDX ou empresariais

Para atualizar um aplicativo MDX ou Empresarial no XenMobile, desative o aplicativo no console do XenMobile e, em seguida, carregue a nova versão do aplicativo. Você não precisa desativar aplicativos de lojas de aplicativos públicas, como o Citrix Secure Mail.

1. No console do XenMobile®, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.
2. Para dispositivos gerenciados (dispositivos registrados no XenMobile para gerenciamento de dispositivos móveis), pule para a Etapa 3. Para dispositivos não gerenciados (dispositivos registrados no XenMobile apenas para fins de gerenciamento de aplicativos empresariais), faça o seguinte:

    a. Na tabela **Aplicativos**, selecione a caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.

    b. Clique em **Desativar** no menu que aparece.



c. Clique em **Desativar** na caixa de diálogo de confirmação. *Desativado* aparece na coluna **Desativar** para o aplicativo.



> **Observação:**
>
> Enquanto o aplicativo está desativado, os usuários não podem se reconectar ao aplicativo depois de fazerem logoff. Desativar um aplicativo é opcional, mas recomendamos desativar o aplicativo para evitar problemas com a funcionalidade do aplicativo. Por exemplo, usuários solicitando o download do aplicativo ao mesmo tempo em que você carrega a nova versão pode resultar em um problema.

3. Na tabela **Aplicativos**, clique na caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.
4. Clique em **Editar** no menu que aparece. A página **Informações do Aplicativo** é exibida com as plataformas que você escolheu originalmente para o aplicativo selecionadas.
5. Configure estas configurações:

   - **Nome:** Opcionalmente, altere o nome do aplicativo.
   - **Descrição:** Opcionalmente, altere a descrição do aplicativo.
   - **Categoria do aplicativo:** Opcionalmente, altere a categoria do aplicativo.

6. Clique em **Avançar**. A primeira página da plataforma selecionada é exibida. Faça o seguinte para cada plataforma selecionada:

    a. Escolha o arquivo de substituição que você deseja carregar clicando em **Carregar** e navegando até o local do arquivo. O aplicativo é carregado para o XenMobile.

    Se você estiver carregando um aplicativo para Android Enterprise, uma janela do Google Play gerenciado será exibida. Carregue a nova versão do aplicativo aqui. Para obter mais detalhes, consulte Distribuir aplicativos Android Enterprise.

    b. Opcionalmente, altere os detalhes do aplicativo e as configurações de política para a plataforma.

    c. Opcionalmente, configure as regras de implantação e as configurações da Loja XenMobile. Para obter informações, consulte Adicionar um aplicativo MDX em Adicionar aplicativos.

7. Clique em **Salvar**. A página **Aplicativos** é exibida.
8. Se você desabilitou o aplicativo na Etapa 2, faça o seguinte:

    a. Na tabela **Aplicativos**, clique para selecionar o aplicativo que você atualizou e, em seguida, no menu que aparece, clique em **Habilitar**.

    b. Na caixa de diálogo de confirmação que aparece, clique em **Habilitar**. Os usuários agora podem acessar o aplicativo e receber uma notificação solicitando que atualizem o aplicativo.

Citrix Launcher

Substituição do Citrix Launcher

A Citrix removeu o Citrix Launcher da loja de aplicativos em agosto de 2020. Para substituir o Citrix Launcher, você pode usar recursos que já estão disponíveis.

Para provisionar dispositivos como quiosques (dispositivos dedicados):

1. Adicione uma função RBAC que permita aos administradores do XenMobile registrar dispositivos dedicados em sua implantação do XenMobile. Consulte Provisionamento de dispositivos Android Enterprise dedicados.
2. Crie um perfil de registro com um **Tipo de registro** de **Totalmente gerenciado/Perfil de trabalho**. Consulte Para criar um perfil de registro.

3. Crie uma política de dispositivo de Quiosque para configurar um aplicativo para fixar na tela do dispositivo, ativando a configuração **Modo de bloqueio de tarefa**. Consulte Configurações do Android Enterprise.

Sobre o Citrix Launcher

O Citrix Launcher permite personalizar a experiência do usuário para dispositivos Android implantados pelo XenMobile. A versão mínima do Android suportada para o gerenciamento do Citrix Launcher pelo Secure Hub é o Android 4.0.3. O Citrix Launcher e a política de dispositivo de Configuração do Launcher não são compatíveis com o Android Enterprise.

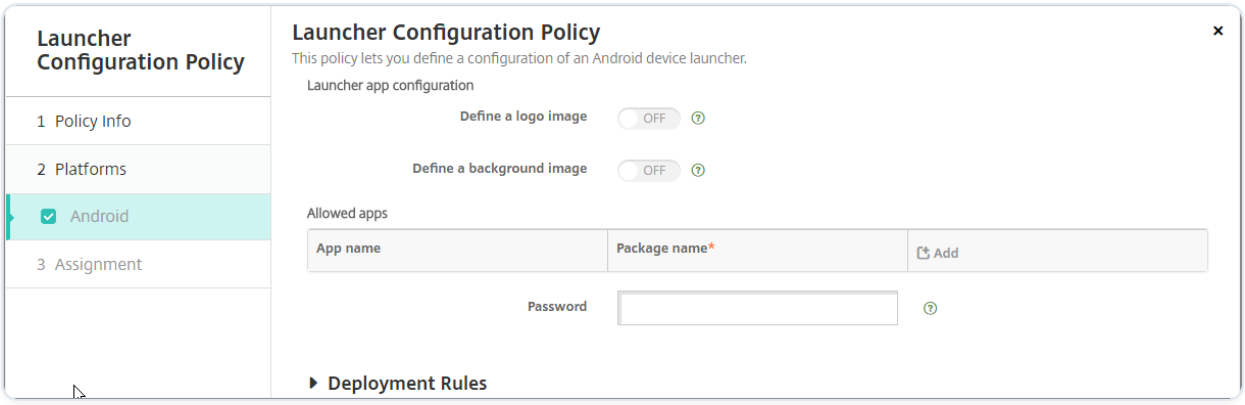
Você pode adicionar a **Política de Configuração do Launcher** para controlar estes recursos do Citrix Launcher:

- Gerenciar dispositivos Android para que os usuários possam acessar apenas os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizada para o ícone do Citrix Launcher e uma imagem de fundo personalizada para o Citrix Launcher.
- Especifique uma senha que os usuários devem inserir para sair do launcher.

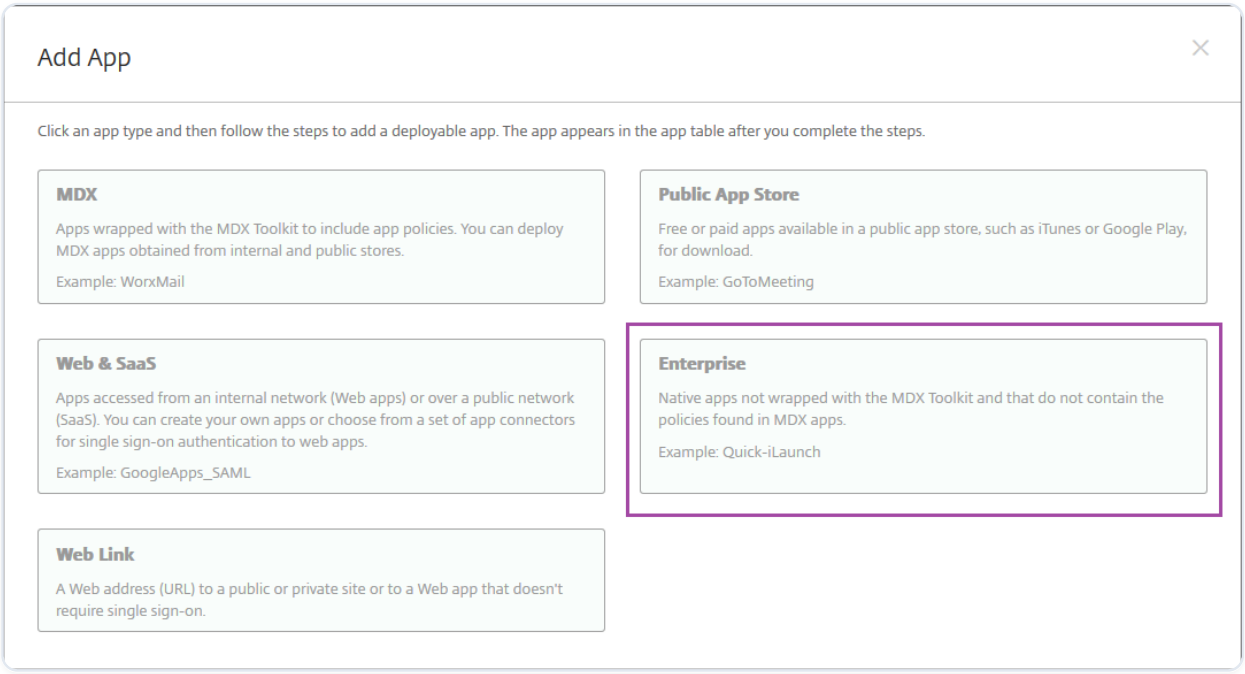
Embora o Citrix Launcher permita aplicar essas restrições no nível do dispositivo, o launcher concede aos usuários acesso integrado às configurações do dispositivo, como configurações de Wi-Fi, configurações de Bluetooth e configurações de senha do dispositivo. O Citrix Launcher não se destina a ser uma camada extra de segurança além do que a plataforma do dispositivo já oferece.

Para fornecer o Citrix Launcher a dispositivos Android, siga estas etapas gerais.

1. Para baixar o aplicativo Citrix Launcher: Vá para `<https://www.citrix.com/downloads>`. Procure por **Citrix Launcher**. O nome do arquivo é CitrixLauncher.apk. O arquivo está pronto para ser carregado no XenMobile e não requer empacotamento.
2. Adicione a política de dispositivo **Launcher Configuration Policy**. Vá para **Configurar > Políticas de Dispositivo**, clique em **Adicionar** e, na caixa de diálogo **Adicionar Nova Política**, comece a digitar **Launcher**. Para obter mais informações, consulte Política de Configuração do Launcher.

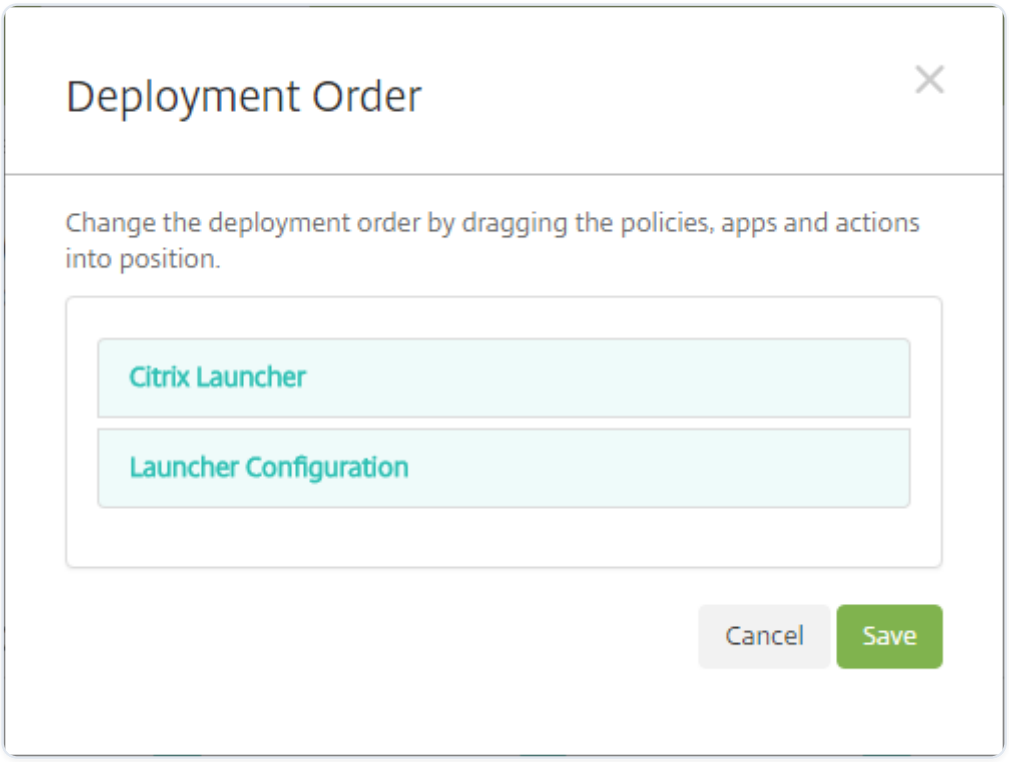


3. Adicione o aplicativo Citrix Launcher ao XenMobile como um aplicativo empresarial. Em **Configurar > Aplicativos**, clique em **Adicionar** e, em seguida, em **Empresarial**. Para obter mais informações, consulte Adicionar um aplicativo empresarial.



4. Crie um Grupo de Entrega para o Citrix Launcher com a seguinte configuração em **Configurar > Grupos de entrega**.

   - Na página **Políticas**, adicione a **Launcher Configuration Policy**.
   - Na página **Aplicativos**, arraste **Citrix Launcher** para **Aplicativos Necessários**.
   - Na página **Resumo**, clique em **Ordem de Implantação** e certifique-se de que o aplicativo **Citrix Launcher** precede a política **Launcher Configuration**.



Para obter mais informações, consulte Implantar recursos.

Compra por Volume da Apple

Você pode gerenciar o licenciamento de aplicativos iOS usando a compra por volume do Apple iOS. A solução de compra por volume simplifica o processo de encontrar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Com a compra por volume, você pode usar o XenMobile® para distribuir aplicativos da loja pública.

- A compra por volume não é suportada para o registro MAM. Você deve registrar dispositivos de compra por volume em MDM ou MDM+MAM.
- A compra por volume não é suportada para aplicativos de produtividade móvel da Citrix®.
- Embora você possa distribuir os aplicativos da loja pública do XenMobile com compra por volume, a implantação não é ideal. São necessárias melhorias no XenMobile e na loja Secure Hub para resolver as limitações.
- Para obter uma lista de problemas conhecidos na distribuição de aplicativos da loja pública do XenMobile por meio da compra por volume, consulte CTX222633 no Citrix Knowledge Center.

Com a compra por volume, você pode distribuir os aplicativos aplicáveis diretamente para seus dispositivos. Ou, você atribui conteúdo aos seus usuários usando códigos resgatáveis. Você configura as definições específicas para a compra por volume do iOS no XenMobile.

O XenMobile reimporta periodicamente as licenças de compra por volume da Apple para garantir que as licenças reflitam todas as alterações. Tais alterações incluem quando você exclui manualmente um aplicativo importado da compra por volume. Por padrão, o XenMobile atualiza a linha de base da licença de compra por volume no mínimo a cada 1440 minutos (24 horas). Você pode alterar o intervalo da linha de base da compra por volume por meio da propriedade do servidor, `VPP.baseline`. Consulte Propriedades do servidor.

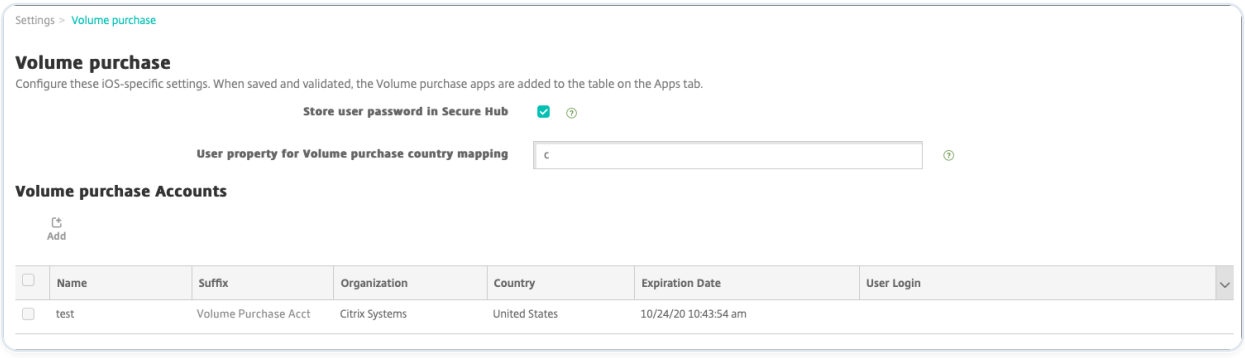
A configuração de **Atualização automática de aplicativos** também depende da propriedade do servidor `VPP.baseline` e os aplicativos são atualizados no mesmo agendamento definido nessa propriedade.

Este artigo foca no uso da compra por volume com licenças gerenciadas, o que permite usar o XenMobile para distribuir aplicativos. Se você usa atualmente códigos de resgate e deseja mudar para a distribuição gerenciada, consulte este documento de Suporte da Apple Migrar de códigos de resgate para distribuição gerenciada com a Compra por Volume.

Para obter informações sobre a compra por volume do iOS, consulte `<https://volume.itunes.apple.com/us/store>`. Para se inscrever na compra por volume, acesse `<https://deploy.apple.com/qforms/open/register/index/avs>`. Para acessar sua loja de compra por volume no iTunes, acesse `<https://volume.itunes.apple.com/?l=en>`.

Depois de salvar essas configurações de compra por volume do iOS no XenMobile, os aplicativos comprados aparecem na página **Configurar > Aplicativos** no console do XenMobile.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Compra por volume**. A página de configuração de **Compra por volume** é exibida.



3. Configure estas configurações:

   - **Armazenar senha do usuário no Secure Hub:** Selecione se deseja armazenar um nome de usuário e senha no Secure Hub para autenticação do XenMobile. O padrão é armazenar as informações usando este método seguro.

- **Propriedade do usuário para mapeamento de país de compra por volume:** Digite um código para permitir que os usuários baixem aplicativos de lojas de aplicativos específicas de cada país.

O XenMobile usa este mapeamento para escolher o pool de propriedades da compra por volume. Por exemplo, se a propriedade do usuário for Estados Unidos, esse usuário não poderá baixar aplicativos se o código de compra por volume for para o Reino Unido. Entre em contato com o administrador do seu plano de compra por volume para obter mais informações sobre o código de mapeamento de país.

4. Para cada conta de compra por volume que você deseja adicionar, clique em **Adicionar**. A caixa de diálogo **Adicionar uma conta de compra por volume** é exibida.



5. Configure estas configurações para cada conta que você adicionar:

> **Observação:**
>
> Se você usa o Apple Configurator 1, carregue um arquivo de licença: Vá para **Configurar > Aplicativos**, vá para uma página de plataforma e, em seguida, expanda **Compra por volume**.

- **Nome:** Digite o nome da conta de compra por volume.
- **Sufixo:** Digite o sufixo a ser exibido com os nomes dos aplicativos obtidos através da conta de compra por volume. Por exemplo, se você inserir **VP**, o aplicativo Secure Mail aparecerá na lista de aplicativos como **Secure Mail - VP**.
- **Token da Empresa:** Copie e cole o token de serviço de compra por volume obtido da Apple. Para obter o token: Na página **Resumo da Conta** do portal de compra por volume da Apple, clique no botão **Baixar** para gerar e baixar o arquivo de compra por volume. O arquivo contém o token de serviço e outras informações, como o código do país e a validade. Salve o arquivo em um local seguro.
- **Login do Usuário:** Digite um nome de administrador de conta de compra por volume autorizado opcional usado para importar aplicativos B2B personalizados.
- **Senha do Usuário:** Digite a senha do administrador da conta de compra por volume.
- **Atualização Automática de Aplicativos:** Se **Ativado**, os aplicativos de compra por volume são atualizados automaticamente quando uma atualização existe na loja da Apple. O padrão é **Desativado**.

6. Clique em **Salvar** para fechar a caixa de diálogo.
7. Clique em **Salvar** para salvar a configuração de compra por volume.

   Uma mensagem aparece informando que o XenMobile adiciona os aplicativos à lista na página **Configurar > Aplicativos**. Nessa página, observe que os nomes dos aplicativos da sua conta de compra por volume incluem o sufixo que você forneceu na configuração anterior.

Agora você pode configurar as definições de aplicativos de compra por volume e, em seguida, ajustar as definições do seu grupo de entrega e da política de dispositivo para aplicativos de compra por volume. Depois de concluir essas configurações, os usuários podem registrar seus dispositivos. As notas a seguir fornecem considerações para esses processos.

- Ao configurar as definições de aplicativos de compra por volume (**Configurar > Aplicativos**), ative **Forçar associação de licença ao dispositivo**.

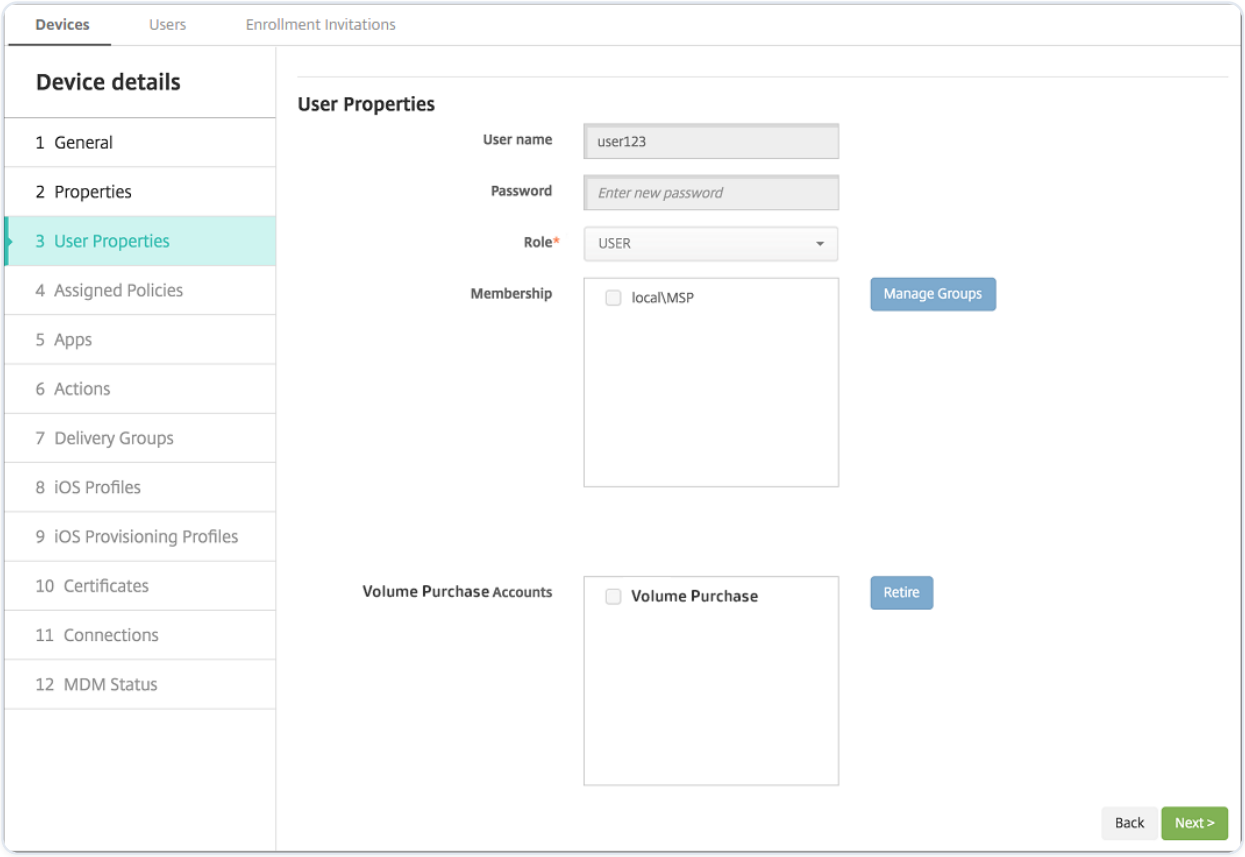
  Uma vantagem de usar o programa de compra por volume e implantação da Apple com dispositivos supervisionados: a capacidade de usar o XenMobile para atribuir o aplicativo no nível do dispositivo (em vez de no nível do usuário). Como resultado, você não precisa usar um dispositivo Apple ID. Além disso, os usuários não recebem um convite para participar da compra por volume da Apple. Os usuários também podem baixar os aplicativos sem fazer login em sua conta do iTunes.

  Para visualizar as informações de compra por volume desse aplicativo, expanda **Compra por volume**. Observe na tabela **Chaves de Licença de Compra por Volume** que a licença está associada a um dispositivo. Se o usuário remover o token e importá-lo novamente, a palavra **Oculto** aparecerá em vez do número de série, devido às restrições de privacidade da Apple.

  Para desassociar uma licença, clique na linha da licença e, em seguida, clique em **Desassociar**.

  Se você associar licenças de compra por volume a usuários, o XenMobile integrará os usuários à sua conta de compra por volume. Além disso, associa o ID do iTunes deles à conta de compra por volume. O ID do iTunes dos usuários nunca é visível para sua empresa ou para o XenMobile Server. A Apple cria a associação de forma transparente para manter a privacidade do usuário. Você pode aposentar um usuário da compra por volume da Apple para

desassociar todas as licenças da conta do usuário. Para aposentar um usuário, vá para **Gerenciar > Dispositivos**.



- Ao atribuir um aplicativo a um grupo de entrega, por padrão o XenMobile identifica o aplicativo como um aplicativo opcional. Para garantir que o XenMobile implante um aplicativo nos dispositivos, vá para **Configurar** > **Grupos de Entrega**. Na página **Aplicativos**, mova o aplicativo para a lista **Aplicativos Obrigatórios**.
- Quando uma atualização para um aplicativo está disponível, a Compra por Volume envia a atualização para o aplicativo e o atualiza automaticamente nos dispositivos. Para mais informações, consulte Verificar atualizações de aplicativos.

O XenMobile exibe um Aviso de Expiração de Licença quando a compra por volume da Apple expirou.

Verificar atualizações de aplicativos

Se você ativar a configuração **Atualização Automática de Aplicativos** ao adicionar uma conta de Compra por Volume, o XenMobile Server verificará periodicamente novas versões dos aplicativos comprados por volume (aplicativos obrigatórios) e dos aplicativos opcionais assinados na loja

Citrix Secure Hub e os atualizará. Assim que o XenMobile Server recebe uma nova versão de um aplicativo obrigatório, ele envia a nova versão para o dispositivo para instalação automaticamente, sem solicitar que você os atualize manualmente. No entanto, para atualizar automaticamente os aplicativos opcionais, a propriedade `apple.ios.optional_app_update` deve ser definida como **True**. Caso contrário, você terá que atualizar manualmente os aplicativos opcionais. Para mais informações, consulte Propriedades do servidor.

Para verificar manualmente a nova versão de qualquer aplicativo e atualizá-lo, siga os passos abaixo:

1. Clique em **Configurar** > **Aplicativos**.

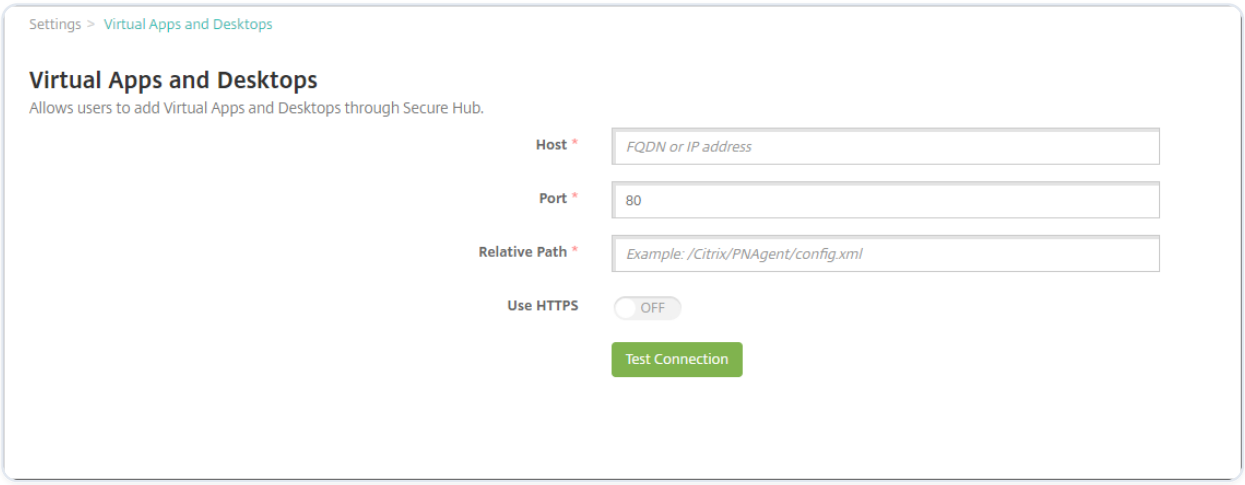
   A página **Aplicativos** é exibida.
2. Selecione um aplicativo e clique em **Editar**.
3. Vá para a página **Plataforma** e clique no botão **Verificar Atualizações** ao lado de **Versão**.
4. Na caixa de diálogo **Atualizar**, aplique a atualização se uma nova versão estiver disponível.

Aplicativos e Desktops Virtuais através do Citrix Secure Hub™

O XenMobile pode coletar aplicativos de Aplicativos e Desktops Virtuais e disponibilizá-los para usuários de dispositivos móveis na XenMobile Store. Os usuários assinam os aplicativos diretamente na XenMobile Store e os iniciam a partir do Secure Hub. O Citrix Receiver™ deve ser instalado nos dispositivos dos usuários para iniciar os aplicativos, mas não precisa ser configurado.

Para configurar essa definição, você precisa do nome de domínio totalmente qualificado (FQDN) ou endereço IP e número da porta para o site da Web Interface ou StoreFront.

1. No console web do XenMobile®, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Aplicativos e Desktops Virtuais**. A página **Aplicativos e Desktops Virtuais** é exibida.



3. Configure estas definições:

   - **Host:** Digite o nome de domínio totalmente qualificado (FQDN) ou endereço IP para o site da Web Interface ou StoreFront.
   - **Porta:** Digite o número da porta para o site da Web Interface ou StoreFront. O padrão é 80.
   - **Caminho Relativo:** Digite o caminho. Por exemplo, /Citrix/PNAgent/config.xml
   - **Usar HTTPS:** Selecione se deseja habilitar a autenticação segura entre o site da Web Interface ou StoreFront e o dispositivo cliente. O padrão é **DESATIVADO**.

4. Clique em **Testar Conexão** para verificar se o XenMobile pode se conectar ao servidor de Aplicativos e Desktops Virtuais especificado.
5. Clique em **Salvar**.

Usar ShareFile com XenMobile®

> **Aviso:**
>
> Este recurso será preterido se o ShareFile (agora Progress) descontinuar o suporte.

> O XenMobile tem duas opções para integração com o ShareFile: Citrix Files e conectores de zona de armazenamento. A integração com o Citrix Files ou conectores de zona de armazenamento requer o XenMobile Advanced Edition (local) ou o Citrix Endpoint Management™ (nuvem).

Citrix Files

Se você tiver o XenMobile Advanced Edition (local) ou o Citrix Endpoint Management (nuvem), poderá configurar o XenMobile para fornecer acesso à sua conta do Citrix Files. Essa configuração:

- Oferece aos usuários móveis acesso ao conjunto completo de recursos Enterprise, como compartilhamento de arquivos, sincronização de arquivos e conectores de zona de armazenamento.
- Pode fornecer ao Citrix Files autenticação de logon único para usuários do aplicativo XenMobile e políticas abrangentes de controle de acesso.
- Fornece configuração do Citrix Files, monitoramento do nível de serviço e monitoramento do uso de licenças por meio do console do XenMobile.

Para obter mais informações sobre como configurar o XenMobile para o Citrix Files, consulte SAML para logon único com Citrix Files.

Conectores de zona de armazenamento

Você pode configurar o XenMobile para fornecer acesso apenas aos conectores de zona de armazenamento que você cria por meio do console do XenMobile. Essa configuração:

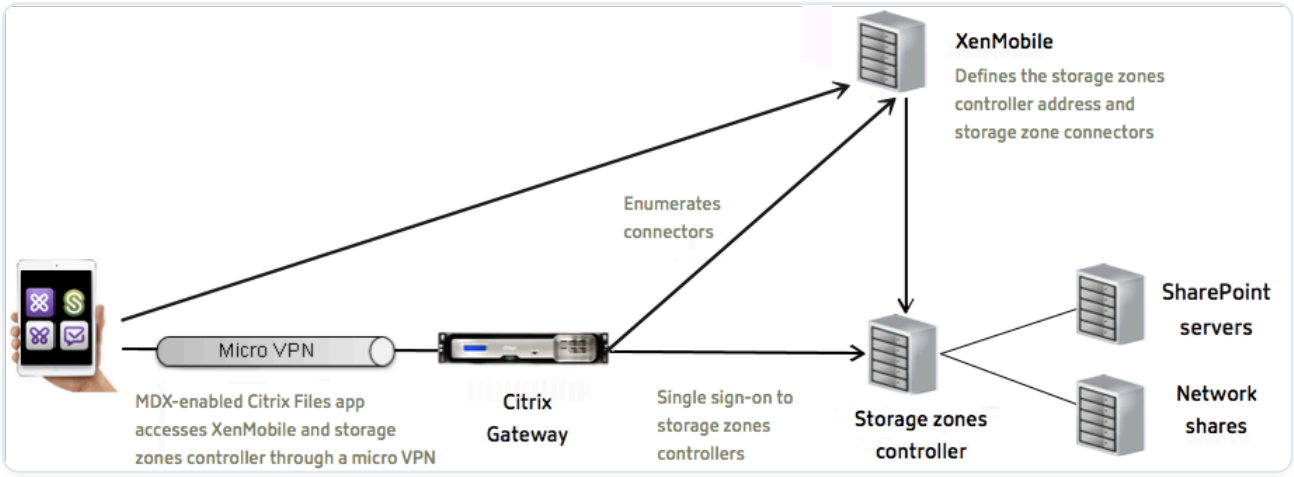
- Fornece acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos de rede.
- Não exige que você configure um subdomínio do ShareFile ou hospede dados do Citrix Files.
- Fornece acesso móvel a dados por meio dos aplicativos de produtividade móvel do Citrix Files para iOS e Android. Você pode editar documentos do Microsoft Office. Além disso, você pode visualizar e anotar arquivos PDF da Adobe a partir de dispositivos móveis.
- Em conformidade com as restrições de segurança contra vazamento de informações do usuário para fora da rede corporativa.
- Oferece configuração simples de conectores de zona de armazenamento através do console do XenMobile. Se você decidir posteriormente usar a funcionalidade completa do Citrix Files com o XenMobile, poderá alterar a configuração no console do XenMobile.
- Requer XenMobile Advanced Edition (local) ou Citrix Endpoint Management (nuvem).

Para uma integração do XenMobile apenas com conectores de zona de armazenamento:

- O ShareFile usa sua configuração de logon único para o Citrix Gateway para autenticar com o controlador de zonas de armazenamento.

- O XenMobile não autenticar via SAML porque o plano de controle do Citrix Files não é usado.

O diagrama a seguir mostra a arquitetura de alto nível para o uso do XenMobile com conectores de zona de armazenamento.



Requisitos

- Versões mínimas dos componentes:
  - XenMobile Server 10.5 (local)
  - ShareFile para iOS (MDX) 5.3
  - ShareFile para Android (MDX) 5.3
  - Controlador de zonas de armazenamento 5.0

    Este artigo fornece instruções sobre como configurar o controlador de zonas de armazenamento 5.0.

- Certifique-se de que o servidor para executar o controlador de zonas de armazenamento atenda aos requisitos do sistema. Para os requisitos, consulte Requisitos do sistema.

Os requisitos para zonas de armazenamento para Dados do Citrix Files e para zonas de armazenamento restritas não se aplicam a uma integração do XenMobile apenas com conectores de zona de armazenamento.

O XenMobile não oferece suporte a conectores Documentum.

- Para executar scripts do PowerShell:
  - Execute os scripts na versão de 32 bits (x86) do PowerShell.

Tarefas de instalação

Conclua as seguintes tarefas, na ordem apresentada, para instalar e configurar o controlador de zonas de armazenamento. Essas etapas são específicas para a integração do XenMobile apenas com conectores de zona de armazenamento. Alguns desses artigos estão na documentação do controlador de zonas de armazenamento.

1. Configurar o Citrix ADC para o controlador de zonas de armazenamento

   Você pode usar o Citrix ADC como um proxy DMZ para o controlador de zonas de armazenamento.

2. Instalar um certificado SSL

   Um controlador de zonas de armazenamento que hospeda zonas padrão requer um certificado SSL. Um controlador de zonas de armazenamento que hospeda zonas restritas e usa um endereço interno não requer um certificado SSL.

3. Preparar seu servidor

   A configuração do IIS e do ASP.NET é necessária para os conectores de zona de armazenamento.

4. Instalar o controlador de zonas de armazenamento
5. Preparar o controlador de zonas de armazenamento para uso apenas com conectores de zona de armazenamento
6. Especificar um servidor proxy para zonas de armazenamento(/pt-br/storagezones-controller/5-0/install/specify-proxy.html)

   O console dos controladores de zonas de armazenamento permite especificar um servidor proxy para os controladores de zonas de armazenamento. Você também pode especificar um servidor proxy usando outros métodos.

7. Configurar o controlador de domínio para confiar no controlador de zonas de armazenamento para delegação(/pt-br/storagezones-controller/5-0/install/configure-domain-controller.html)

   Configure o controlador de domínio para oferecer suporte à autenticação NTLM ou Kerberos em compartilhamentos de rede ou sites do SharePoint.

8. Unir um controlador de zonas de armazenamento secundário a uma zona de armazenamento(#join-a-secondary-storage-zones-controller-to-a-storage-zone)

   Para configurar uma zona de armazenamento para alta disponibilidade, conecte pelo menos dois controladores de zonas de armazenamento a ela.

Instalar o controlador de zonas de armazenamento

1. Baixe e instale o software do controlador de zonas de armazenamento:

   a. Vá para `<https://www.citrix.com/downloads>`. Pesquise por **ShareFile** e, em seguida, baixe o instalador mais recente do controlador de zonas de armazenamento.

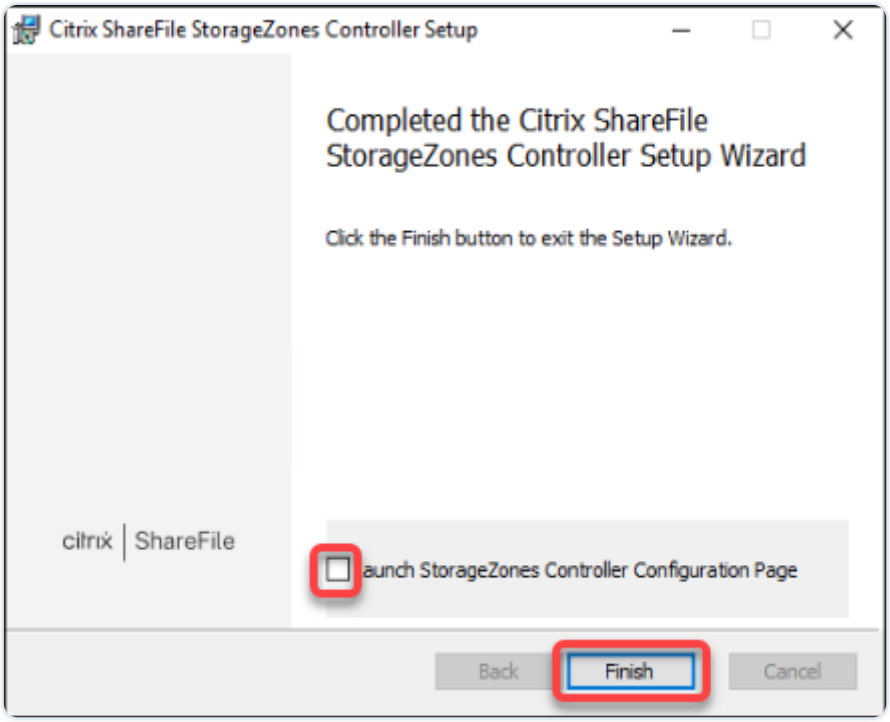
   b. A instalação do controlador de zonas de armazenamento altera o site padrão no servidor para o caminho de instalação do controlador. Habilite a **Autenticação Anônima** no site padrão.

2. No servidor onde você deseja instalar o controlador de zonas de armazenamento, execute StorageCenter.msi.

   O assistente de configuração do controlador de zonas de armazenamento é iniciado.

3. Responda aos prompts:

   - Na página **Pasta de Destino**, se o Internet Information Services (IIS) estiver instalado no local padrão, mantenha os padrões. Caso contrário, navegue até o local de instalação do IIS.
   - Quando a instalação estiver concluída, desmarque a caixa de seleção **Launch Storage Zones Controller Configuration Page** e clique em **Finish**.



4. Quando solicitado, reinicie o controlador de zonas de armazenamento.
5. Para testar se a instalação foi bem-sucedida, navegar para `https://localhost/`. Se a instalação for bem-sucedida, o logotipo do Citrix Files aparecerá.

Se o logotipo do Citrix Files não aparecer, limpe o cache do navegador e tente novamente.

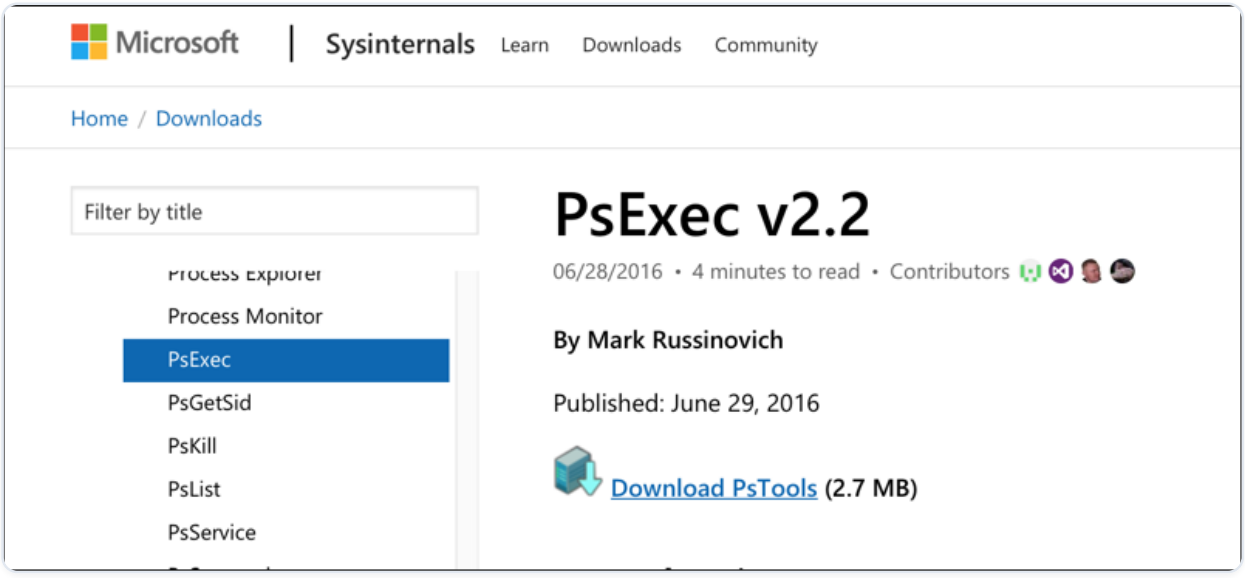
> **Importante:**
>
> Se você planeja clonar o controlador de zonas de armazenamento, capture a imagem do disco antes de continuar com a configuração do controlador de zonas de armazenamento.

Prepare o controlador de zonas de armazenamento para uso apenas com conectores de zona de armazenamento

Para uma integração apenas com conectores de zona de armazenamento, você não usa o console administrativo do controlador de zonas de armazenamento. Essa interface requer uma conta de administrador do Citrix Files, o que não é necessário para esta solução. Como resultado, você executa um script do PowerShell para preparar o controlador de zonas de armazenamento para uso sem o plano de controle do Citrix Files. O script faz o seguinte:

- Registra o controlador de zonas de armazenamento atual como um controlador de zonas de armazenamento primário. Você pode posteriormente unir controladores de zonas de armazenamento secundários ao controlador primário.
- Cria uma zona e define a senha para ela.

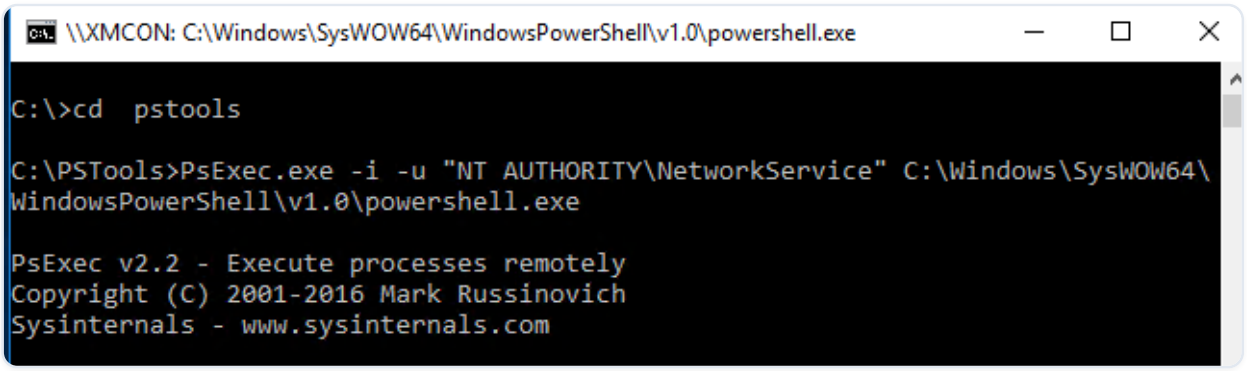
1. No seu servidor controlador de zona de armazenamento, baixe a ferramenta PsExec: navegar para Microsoft Windows Sysinternals e clique em **Download PsTools**. Extraia a ferramenta para a raiz da unidade C.



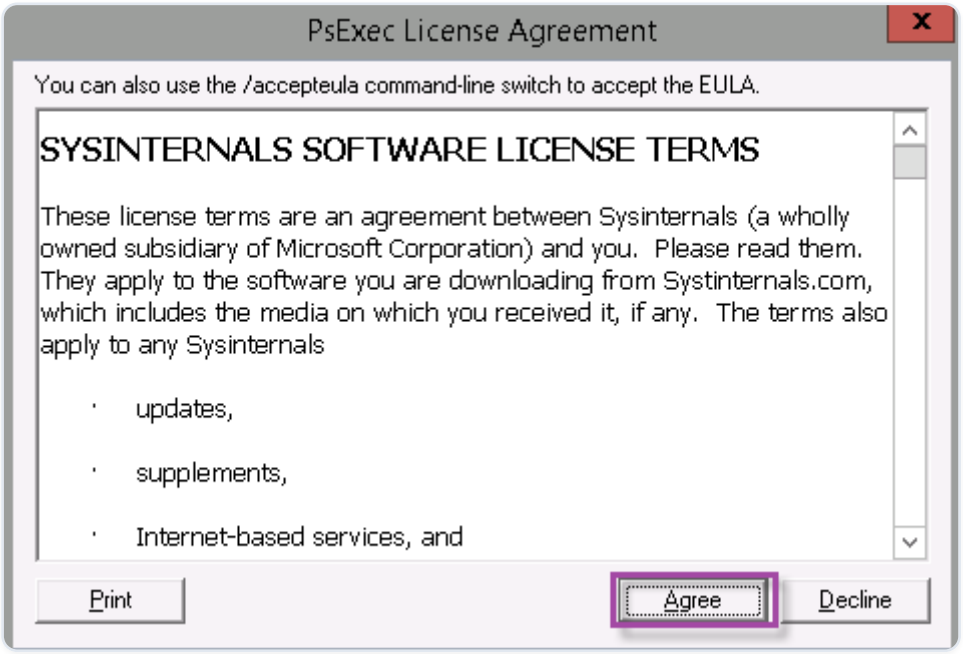
2. Execute a ferramenta PsExec: Abra o Prompt de Comando como Usuário Administrador e digite o seguinte:

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. Quando solicitado, clique em **Concordar** para executar a ferramenta Sysinternals.



Uma janela do PowerShell é aberta.

4. Na janela do PowerShell, digite o seguinte:

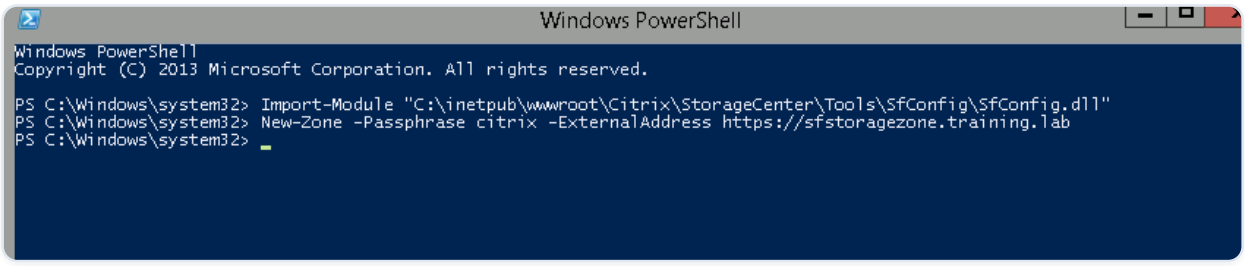
```
Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

Onde:

Frase secreta: É a frase secreta que você deseja atribuir ao site. Anote-a, pois você não pode recuperar a frase secreta do controlador. Se você perder a frase secreta, não poderá reinstalar o controlador de zonas de armazenamento. Junte mais controladores de zonas de armazenamento à zona de armazenamento ou recupere a zona de armazenamento se o servidor falhar.

ExternalAddress: É o nome de domínio totalmente qualificado externo do servidor do controlador de zonas de armazenamento.



Seu controlador de zonas de armazenamento principal está pronto.

Antes de fazer login no XenMobile para criar conectores de zonas de armazenamento: Conclua a seguinte configuração, se aplicável:

Especificar um servidor proxy para zonas de armazenamento

Configurar o controlador de domínio para confiar no controlador de zonas de armazenamento para delegação

Unir um controlador de zonas de armazenamento secundário a uma zona de armazenamento

Para criar conectores de zonas de armazenamento, consulte Definir conexões do controlador de zonas de armazenamento no XenMobile.

Unir um controlador de zonas de armazenamento secundário a uma zona de armazenamento

Para configurar uma zona de armazenamento para alta disponibilidade, conecte pelo menos dois controladores de zonas de armazenamento a ela. Para unir um controlador de zonas de armazenamento secundário a uma zona, instale um controlador de zonas de armazenamento em um segundo servidor. Em seguida, una esse controlador à zona do controlador principal.

1. Abra uma janela do PowerShell no servidor do controlador de zonas de armazenamento que você deseja unir ao servidor primário.
2. Na janela do PowerShell, digite o seguinte:

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

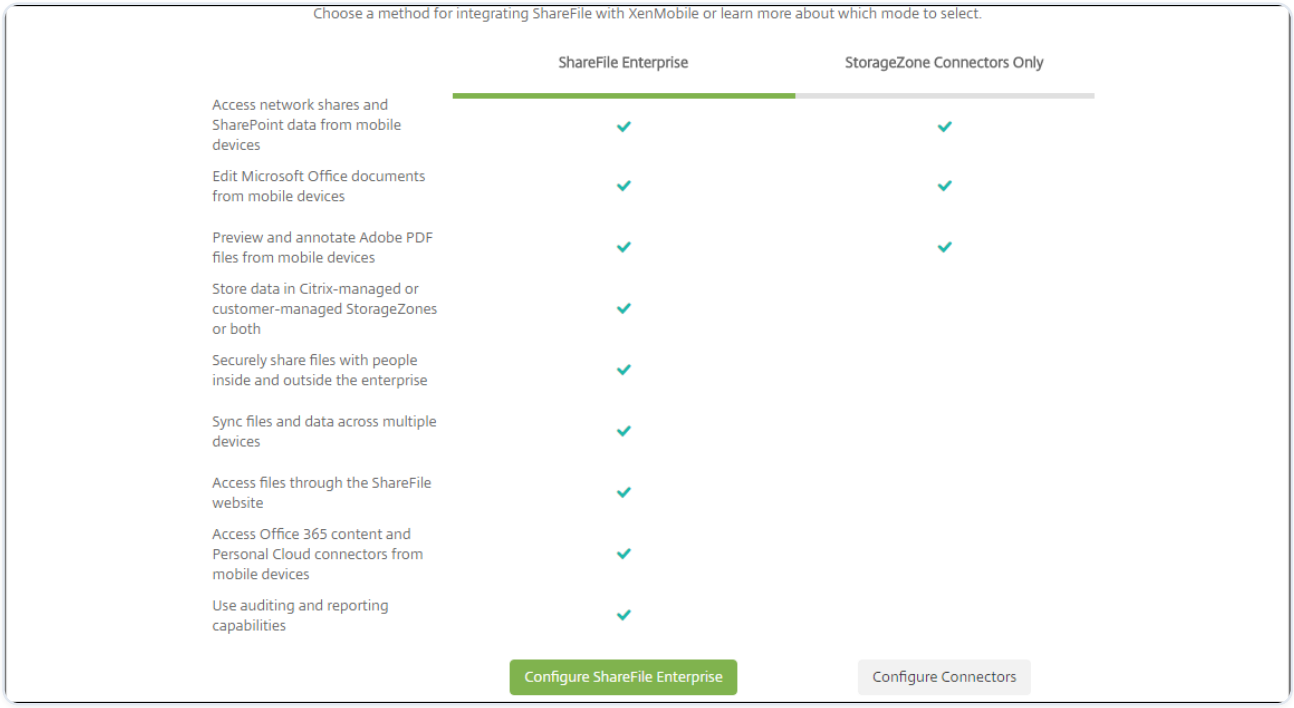
Por exemplo:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

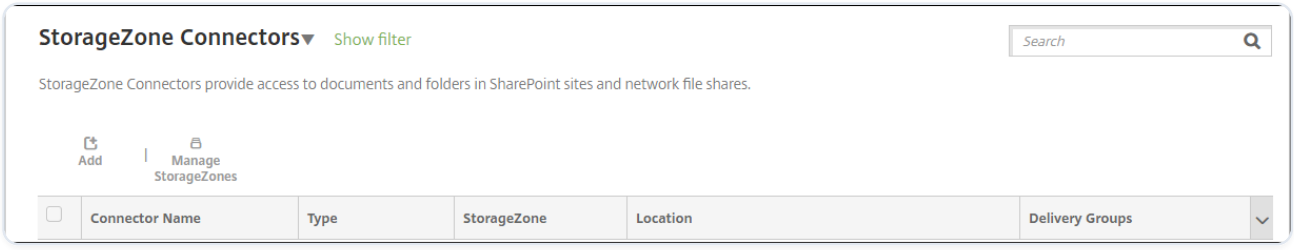
Definir conexões do controlador de zonas de armazenamento no XenMobile

Antes de adicionar conectores de zona de armazenamento, você configura as informações de conexão para cada controlador de zonas de armazenamento habilitado para conectores de zona de armazenamento. Você pode definir controladores de zonas de armazenamento conforme descrito nesta seção ou ao adicionar um conector.

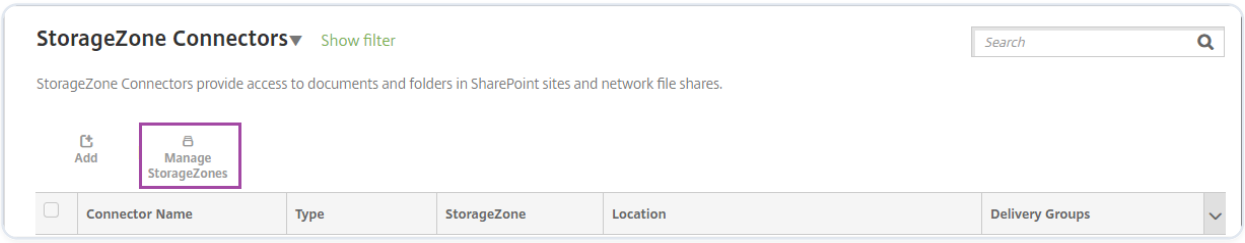
Na sua primeira visita à página **Configurar > ShareFile**, a página resume as diferenças entre usar o XenMobile para contas Enterprise e conectores de zona de armazenamento.



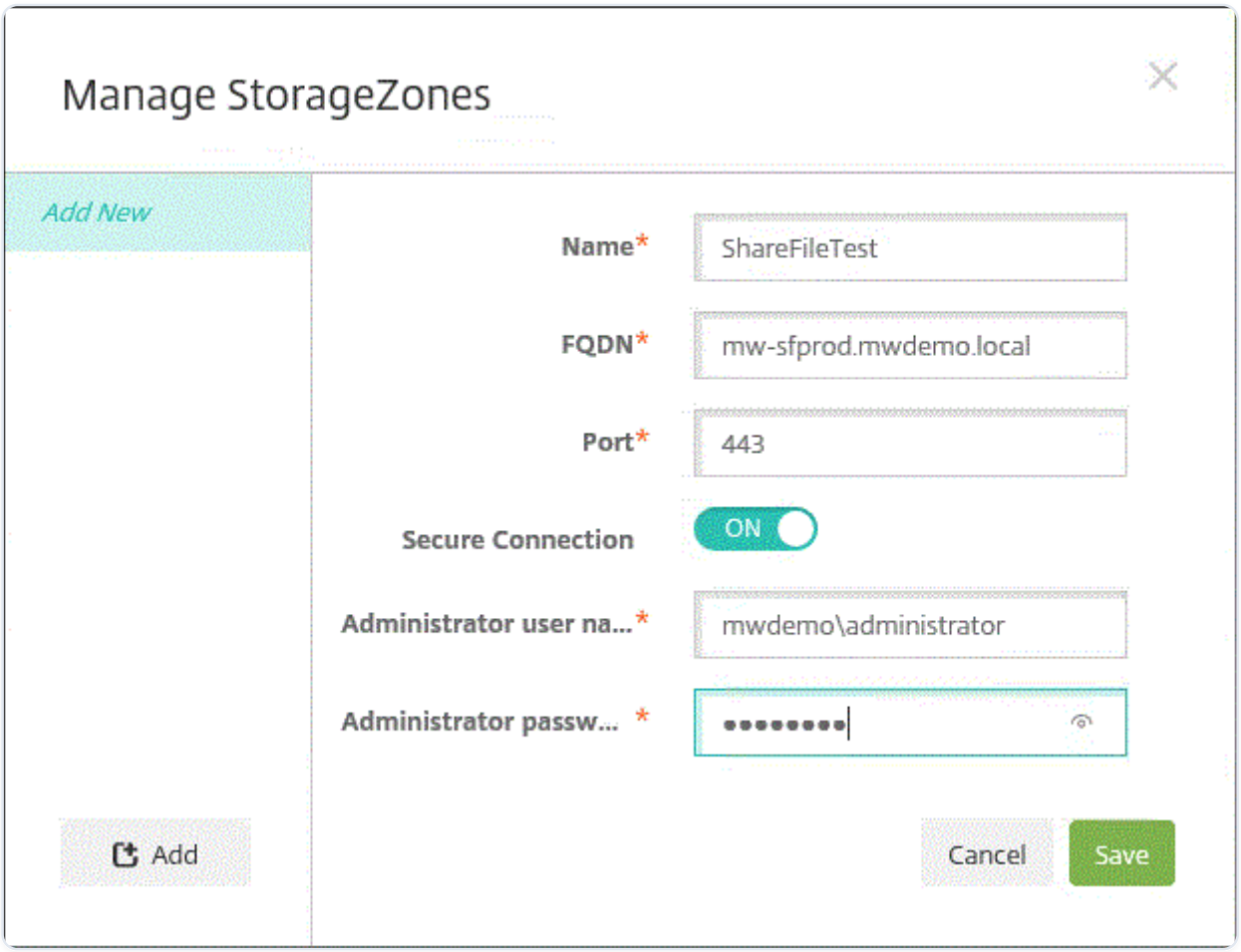
Clique em **Configurar Conectores** para continuar com as etapas de configuração neste artigo.



1. Em **Configurar > ShareFile**, clique em **Gerenciar StorageZones**.



2. Em **Gerenciar StorageZones**, adicione as informações de conexão.



- **Nome:** Um nome descritivo para a Zona de Armazenamento, usado para identificar a Zona de Armazenamento no XenMobile. Não inclua espaços ou caracteres especiais no nome.
- **FQDN e Porta:** O nome de domínio totalmente qualificado e o número da porta para um controlador de zonas de armazenamento que seja acessível a partir do Servidor XenMobile.
- **Conexão Segura:** Se você usa SSL para conexões com o controlador de zonas de armazenamento, use a configuração padrão, ON. Se você não usa SSL para conexões, altere esta configuração para OFF.
- **Nome de usuário do administrador** e **Senha do administrador:** Um nome de usuário (no formato domain\\admin) e senha da conta de serviço de administrador.

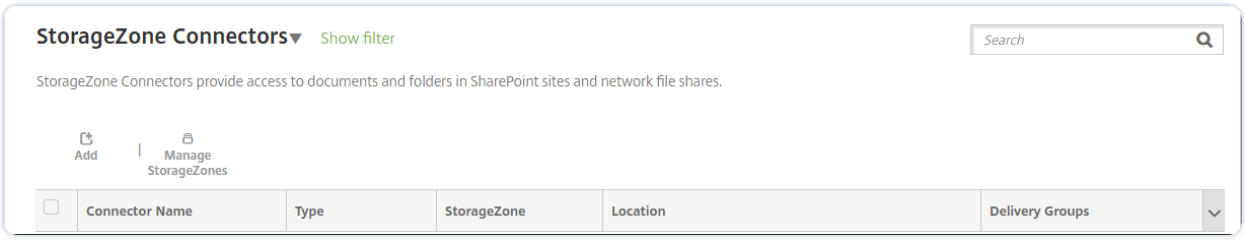
Alternativamente, uma conta de usuário com permissões de leitura e gravação nos controladores de zonas de armazenamento.

3. Clique em **Salvar**.
4. Para testar a conexão, verifique se o Servidor XenMobile pode alcançar o nome de domínio totalmente qualificado do controlador de zonas de armazenamento na porta 443.
5. Para definir outra conexão de controlador de zonas de armazenamento, clique no botão **Adicionar** em **Gerenciar Zonas de Armazenamento**.

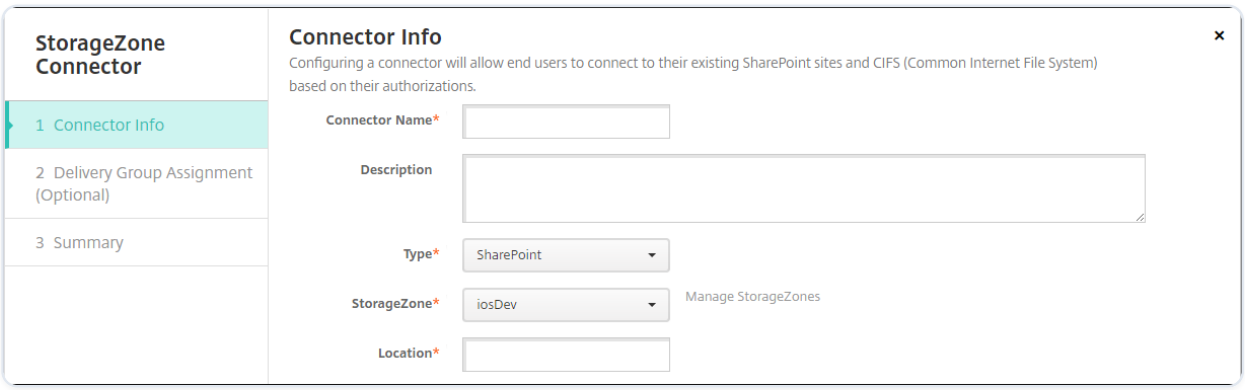
   Para editar ou excluir as informações de uma conexão de controlador de zonas de armazenamento, selecione o nome da conexão em **Gerenciar Zonas de Armazenamento**. Em seguida, clique em **Editar** ou **Excluir**.

Adicionar um conector de zona de armazenamento no XenMobile

1. Vá para **Configurar > ShareFile** e, em seguida, clique em **Adicionar**.



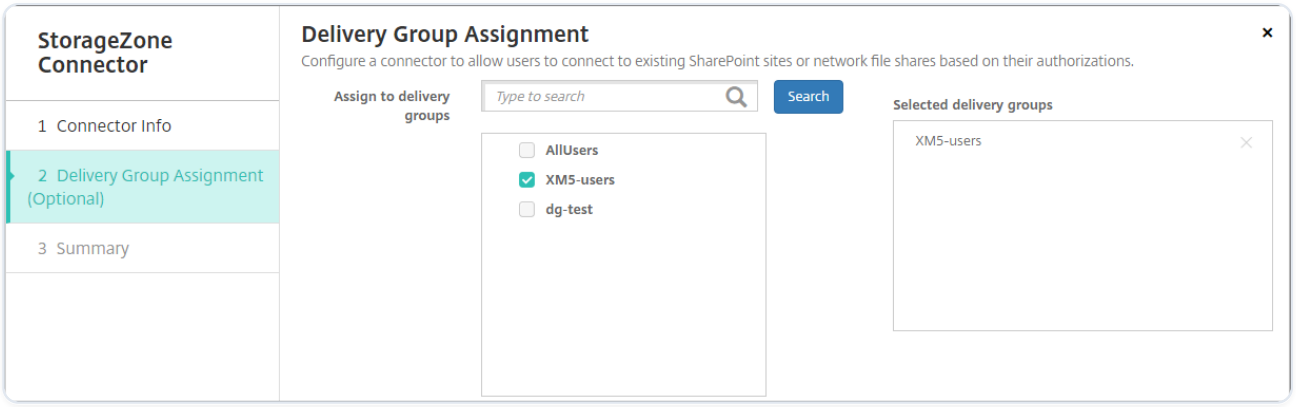
2. Na página **Informações do Conector**, configure estas definições:



- **Nome do Conector:** Um nome que identifica o conector de zona de armazenamento no XenMobile.
- **Descrição:** Notas opcionais sobre este Conector.
- **Tipo:** Escolha **SharePoint** ou **Rede**.
- **StorageZone:** Escolha a zona de armazenamento associada ao Conector. Se a zona de armazenamento não estiver listada, clique em **Gerenciar StorageZones** para definir o controlador de zonas de armazenamento.

- **Localização:** Para SharePoint, especifique a URL do site de nível raiz do SharePoint, coleção de sites ou biblioteca de documentos, no formato `https://sharepoint.company.com`. Para um compartilhamento de rede, especifique o nome de domínio totalmente qualificado do caminho da Convenção de Nomenclatura Uniforme (UNC), no formato \\\\servidor\\compartilhamento.

3. Na página **Atribuição de Grupo de Entrega**, atribua opcionalmente o Conector a grupos de entrega. Alternativamente, você pode associar conectores a grupos de entrega usando **Configurar > Grupos de Entrega**.



1. Na página **Resumo**, você pode revisar as opções configuradas. Para ajustar a configuração, clique em **Voltar**.
2. Clique em **Salvar** para salvar o Conector.
3. Teste o conector:

   a. Ao empacotar os clientes do Citrix Files, faça o seguinte:

      - Defina a política de acesso à rede como **Tunelado para a rede interna**.

      Neste modo de operação, a estrutura MDX do XenMobile intercepta todo o tráfego de rede do cliente Citrix Files. O tráfego é redirecionado através do Citrix Gateway usando uma micro VPN específica do aplicativo.

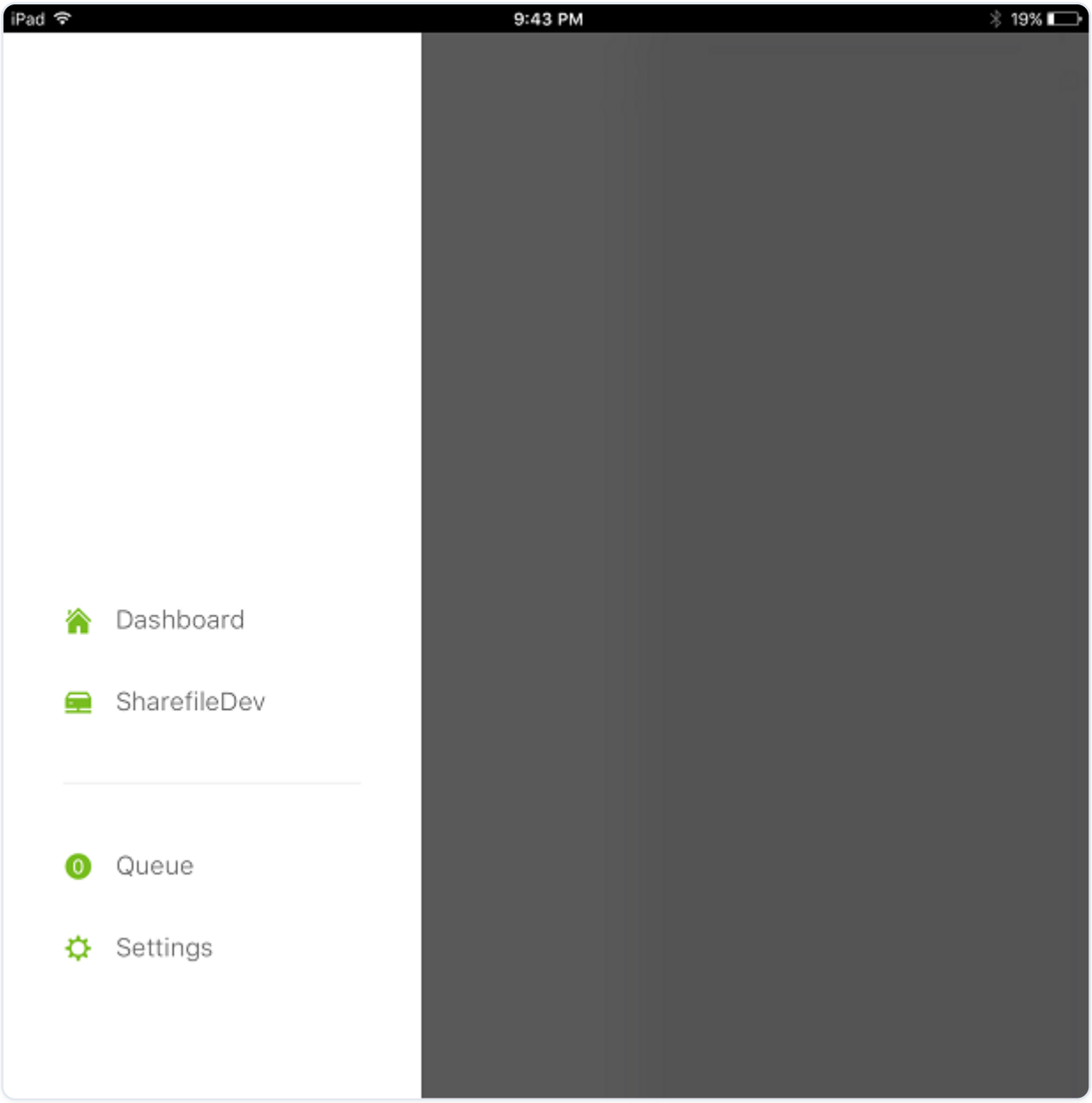
      - Defina a política de modo VPN preferencial como **Tunelado - Web SSO**.

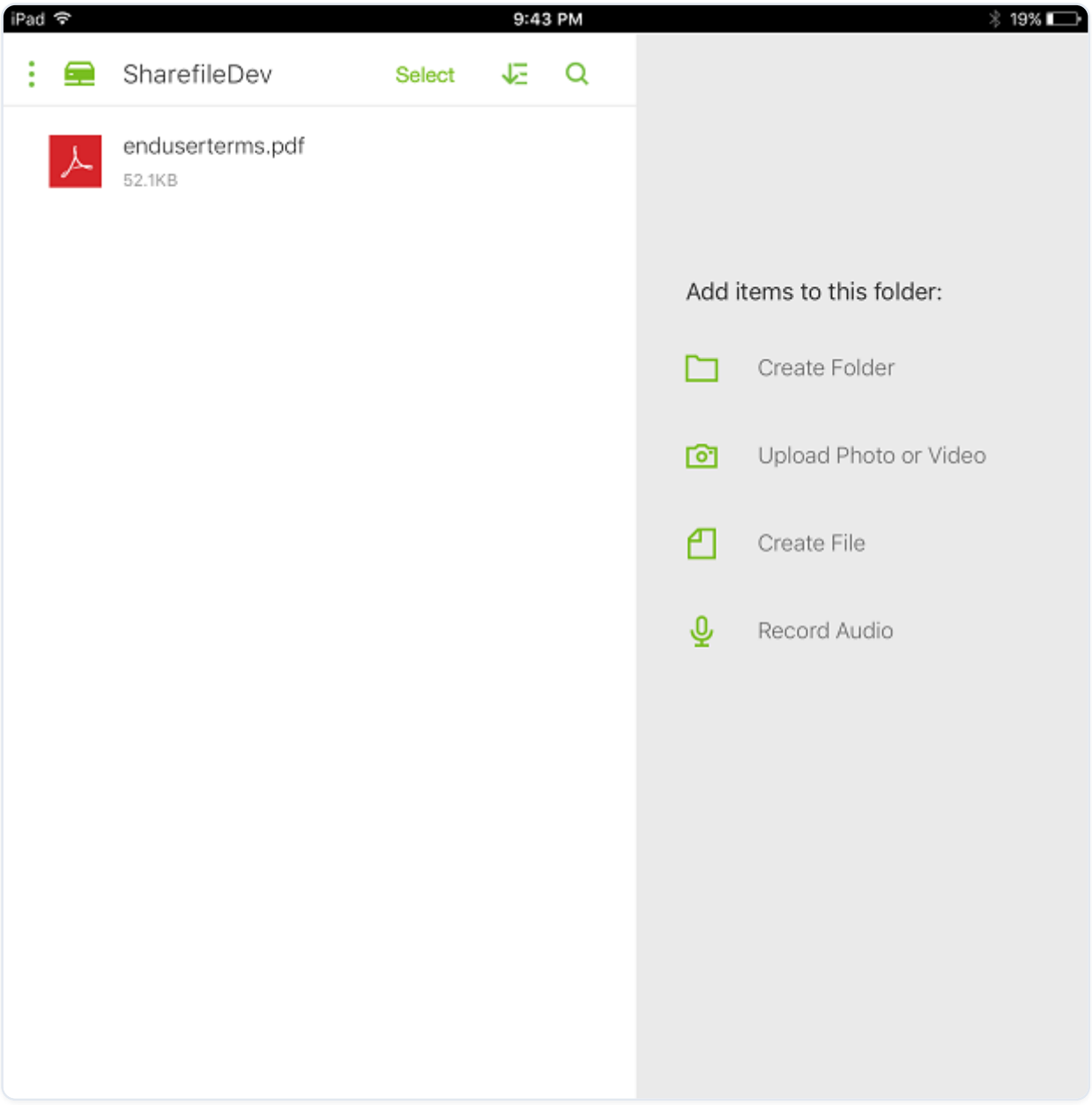
      Neste modo de tunelamento, a estrutura MDX encerra o tráfego SSL/HTTP de um aplicativo MDX. O MDX então inicia novas conexões para conexões internas em nome do usuário. Essa configuração de política permite que a estrutura MDX detecte e responda a desafios de autenticação emitidos por servidores web.

   b. Adicione os clientes do Citrix Files ao XenMobile. Para obter detalhes, consulte Integrando e entregando o Citrix Files para clientes do Endpoint Management.

c. A partir de um dispositivo compatível, verifique o logon único para o Citrix Files e conectores.

Nos exemplos a seguir, SharefileDev é o nome de um conector.

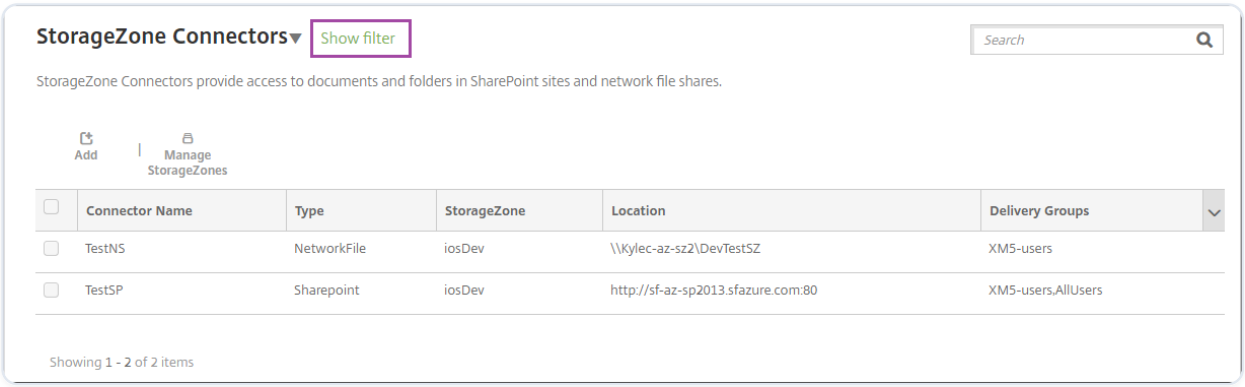




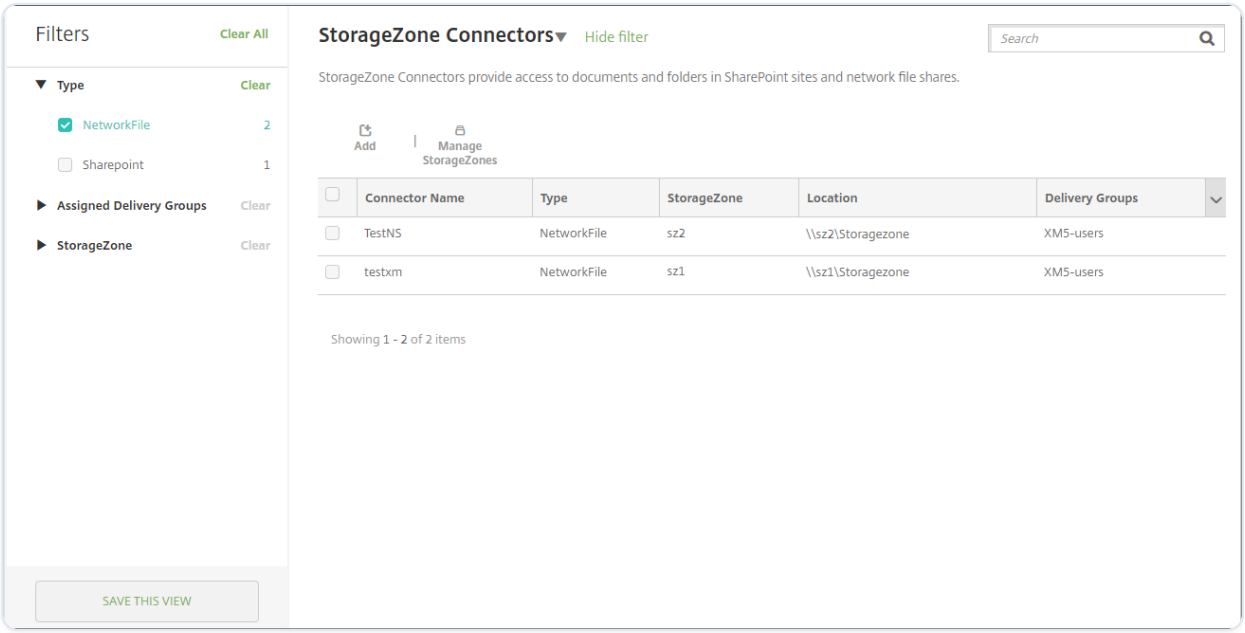
Filtrar a lista de conectores de zona de armazenamento

Você pode filtrar a lista de conectores de zona de armazenamento por tipo de conector, grupos de entrega atribuídos e zona de armazenamento.

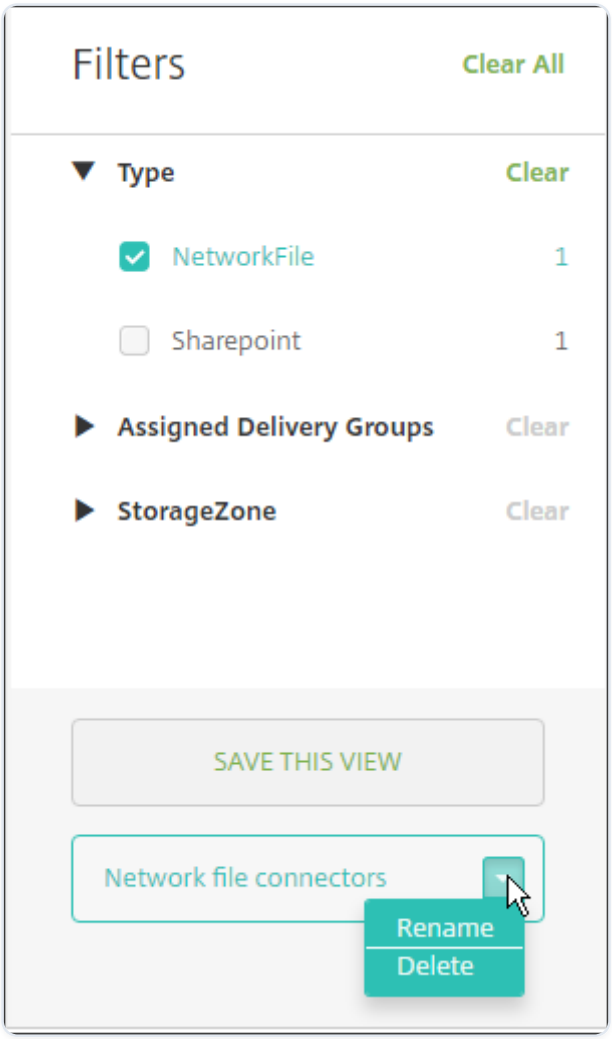
1. Vá para **Configurar > ShareFile** e clique em **Mostrar filtro**.



2. Expanda os títulos do filtro para fazer seleções. Para salvar um filtro, clique em **Salvar esta exibição**, digite o nome do filtro e clique em **Salvar**.



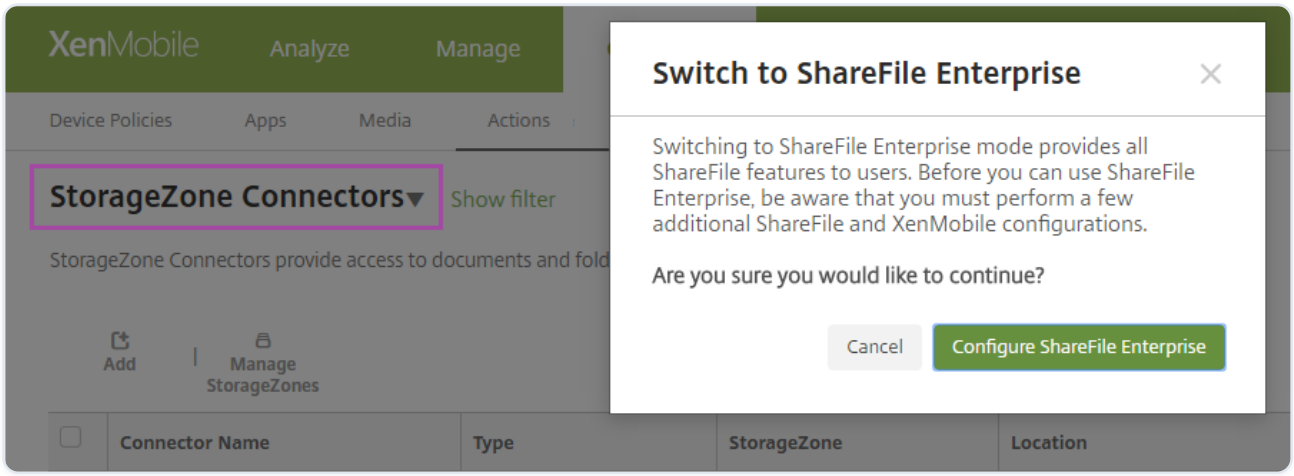
3. Para renomear ou excluir um filtro, clique no ícone de seta ao lado do nome do filtro.



Mudar para o Citrix Files

Após integrar os conectores de zona de armazenamento com o XenMobile, você pode posteriormente mudar para o conjunto completo de recursos Enterprise. O uso do conjunto de recursos do Citrix Files requer o XenMobile Advanced Edition (local) ou o Citrix Endpoint Management (nuvem). O XenMobile mantém suas configurações de integração de conector de zona de armazenamento existentes.

Vá para **Configurar > ShareFile**, clique no menu suspenso **Conectores de Zona de Armazenamento** e, em seguida, clique em **Configurar ShareFile Enterprise**.



Para obter informações sobre como configurar o Citrix Files, consulte SAML para logon único com Citrix Files.

SmartAccess para apps HDX™

Esse recurso permite controlar o acesso a apps HDX com base nas propriedades do dispositivo, propriedades do usuário de um dispositivo ou aplicativos instalados em um dispositivo. Você usa esse recurso definindo ações automatizadas para marcar o dispositivo como fora de conformidade para negar o acesso a esse dispositivo. Os apps HDX usados com esse recurso são configurados no Virtual Apps and Desktops usando uma política SmartAccess que nega acesso a dispositivos fora de conformidade. O XenMobile comunica o status do dispositivo ao StoreFront™ usando uma tag assinada e criptografada. O StoreFront então permite ou nega o acesso com base na política de controle de acesso do app.

Para usar esse recurso, sua implantação requer:

- Virtual Apps e Desktops 7.6
- StoreFront 3.7 ou 3.8
- XenMobile® Server configurado para agregar apps HDX de um servidor StoreFront
- XenMobile Server configurado com um certificado SAML para ser usado para assinar e criptografar tags. O mesmo certificado sem chave privada é carregado no servidor StoreFront.

Para começar a usar esse recurso:

- Configure o certificado do XenMobile Server para o armazenamento do StoreFront
- Configure pelo menos um grupo de entrega do Virtual Apps and Desktops com a política SmartAccess necessária
- Defina a ação automatizada no XenMobile

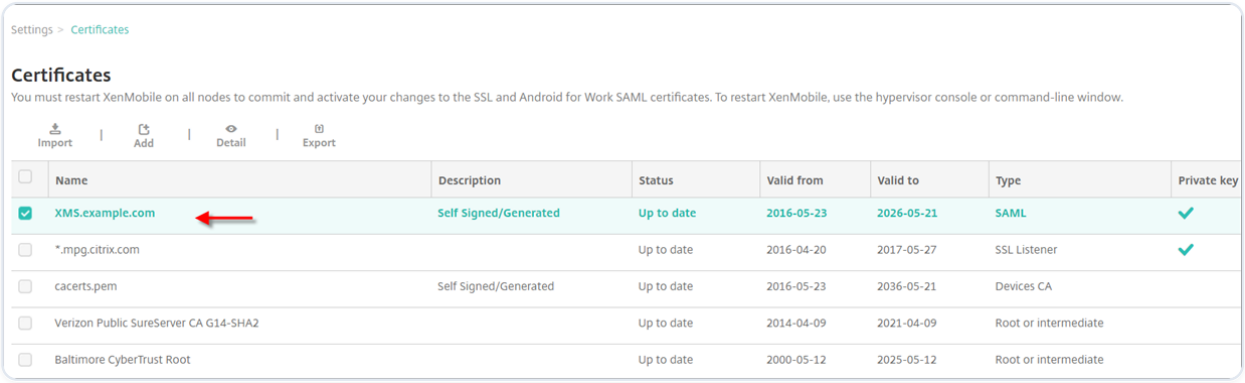
Exporte e configure o certificado do XenMobile Server e carregue-o para o armazenamento do StoreFront

O SmartAccess usa tags assinadas e criptografadas para se comunicar entre os servidores XenMobile e StoreFront. Para habilitar essa comunicação, você adiciona o certificado do XenMobile Server ao armazenamento do StoreFront.

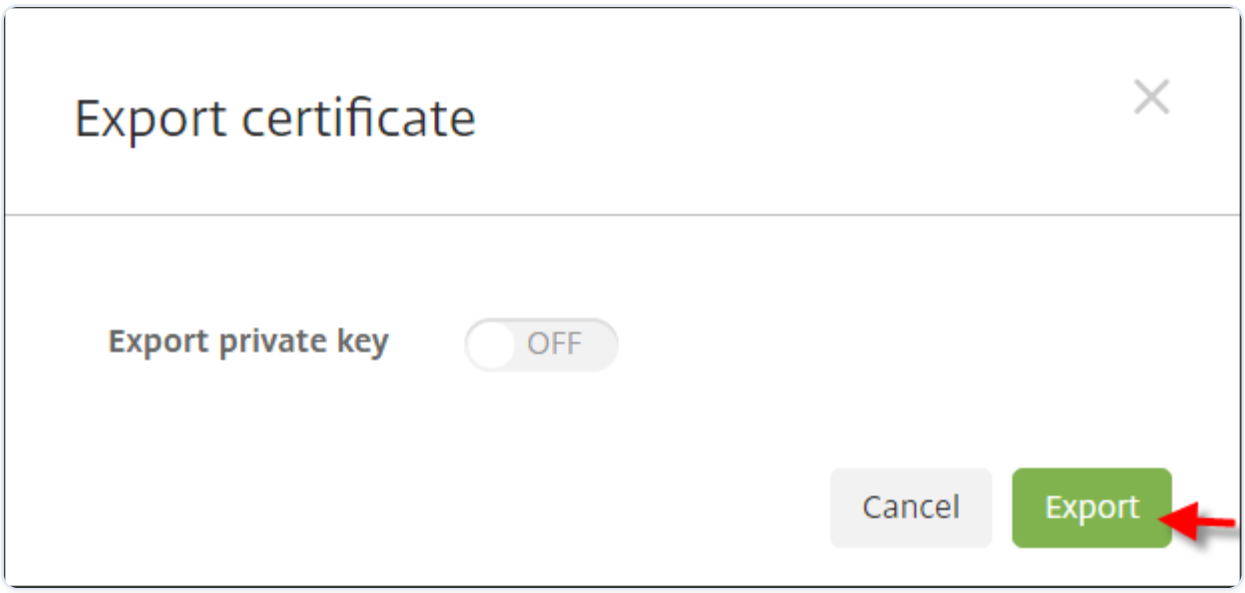
Para obter mais informações sobre a integração do StoreFront e do XenMobile quando o XenMobile está habilitado com autenticação baseada em domínio e certificado, consulte o Centro de Conhecimento de Suporte.

Exporte o certificado SAML do XenMobile Server

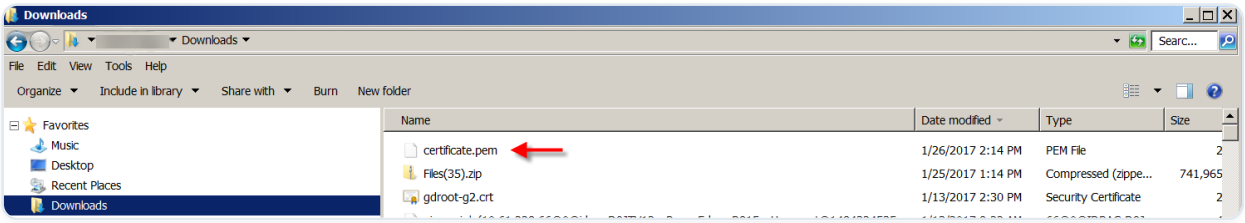
1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida. Clique em **Certificados**.
2. Localize o certificado SAML para o XenMobile Server.



3. Certifique-se de que **Exportar chave privada** esteja definido como **Desativado**. Clique em **Exportar** para exportar o certificado para o seu diretório de download.

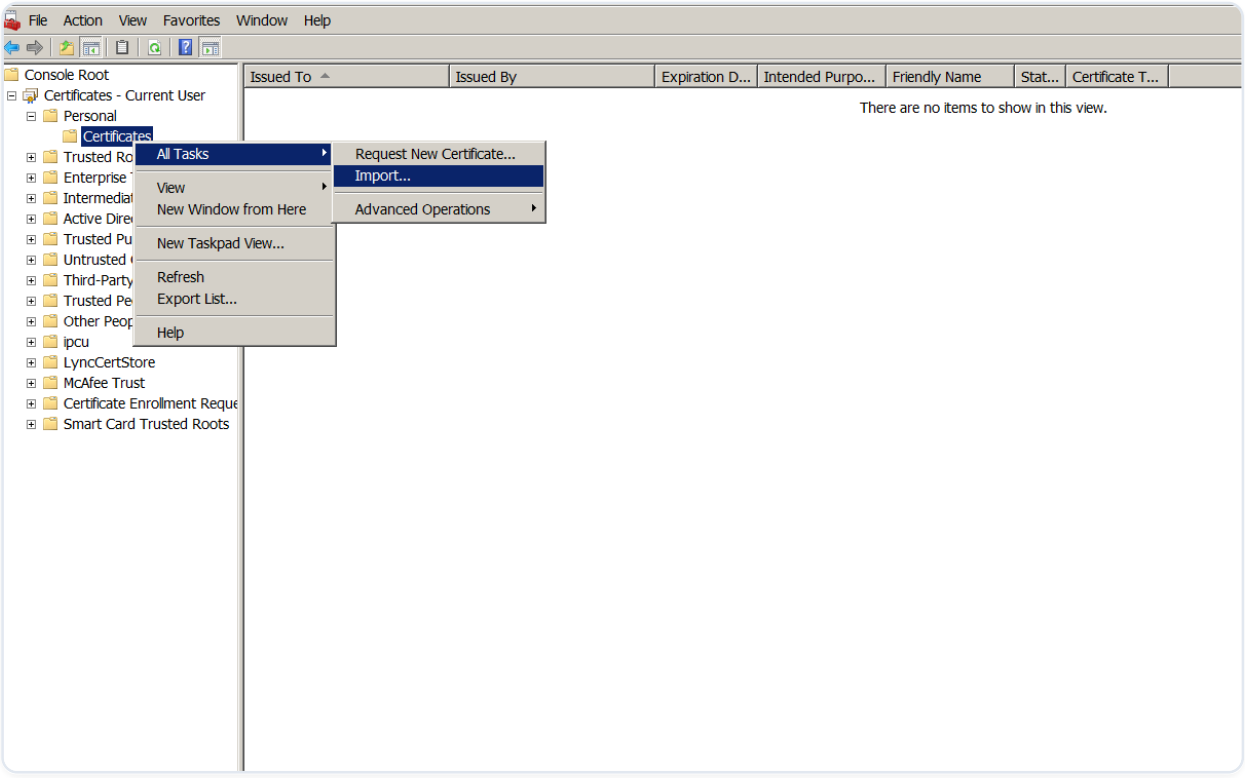


4. Localize o certificado no seu diretório de download. O certificado está no formato PEM.

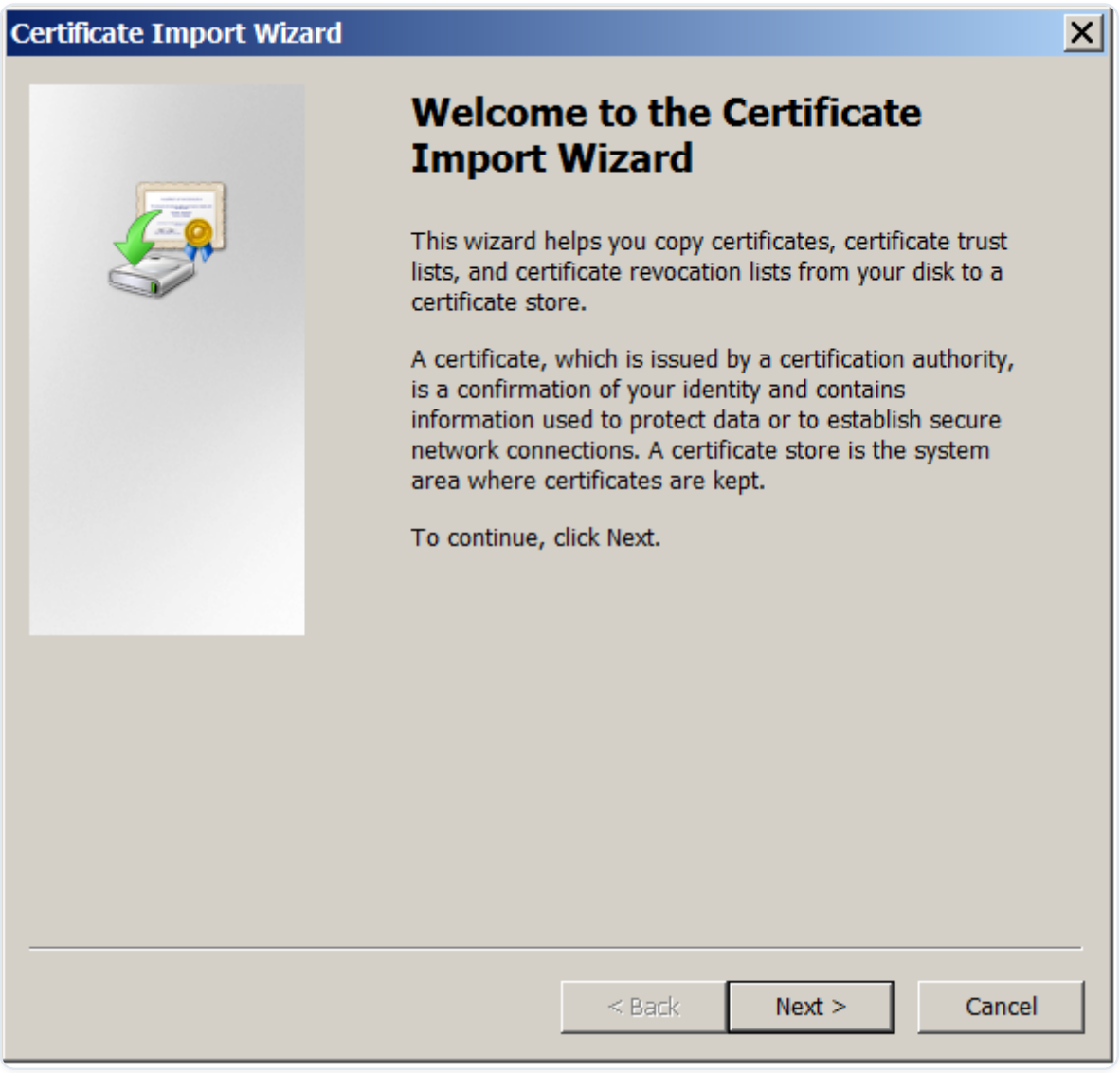


Converter o certificado de PEM para CER

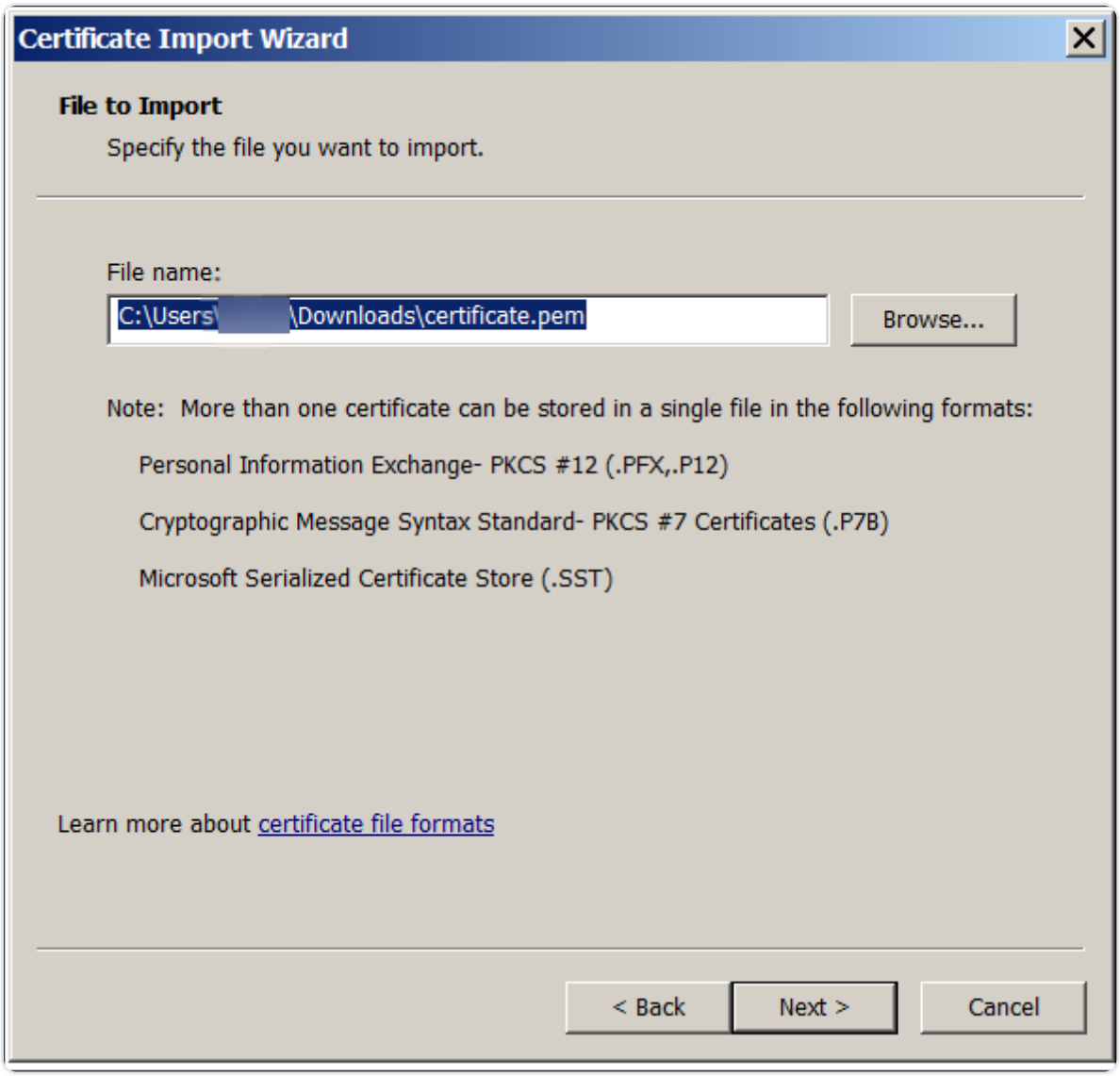
1. Abra o Microsoft Management Console (MMC) e clique com o botão direito em **Certificados > Todas as Tarefas > Importar**.



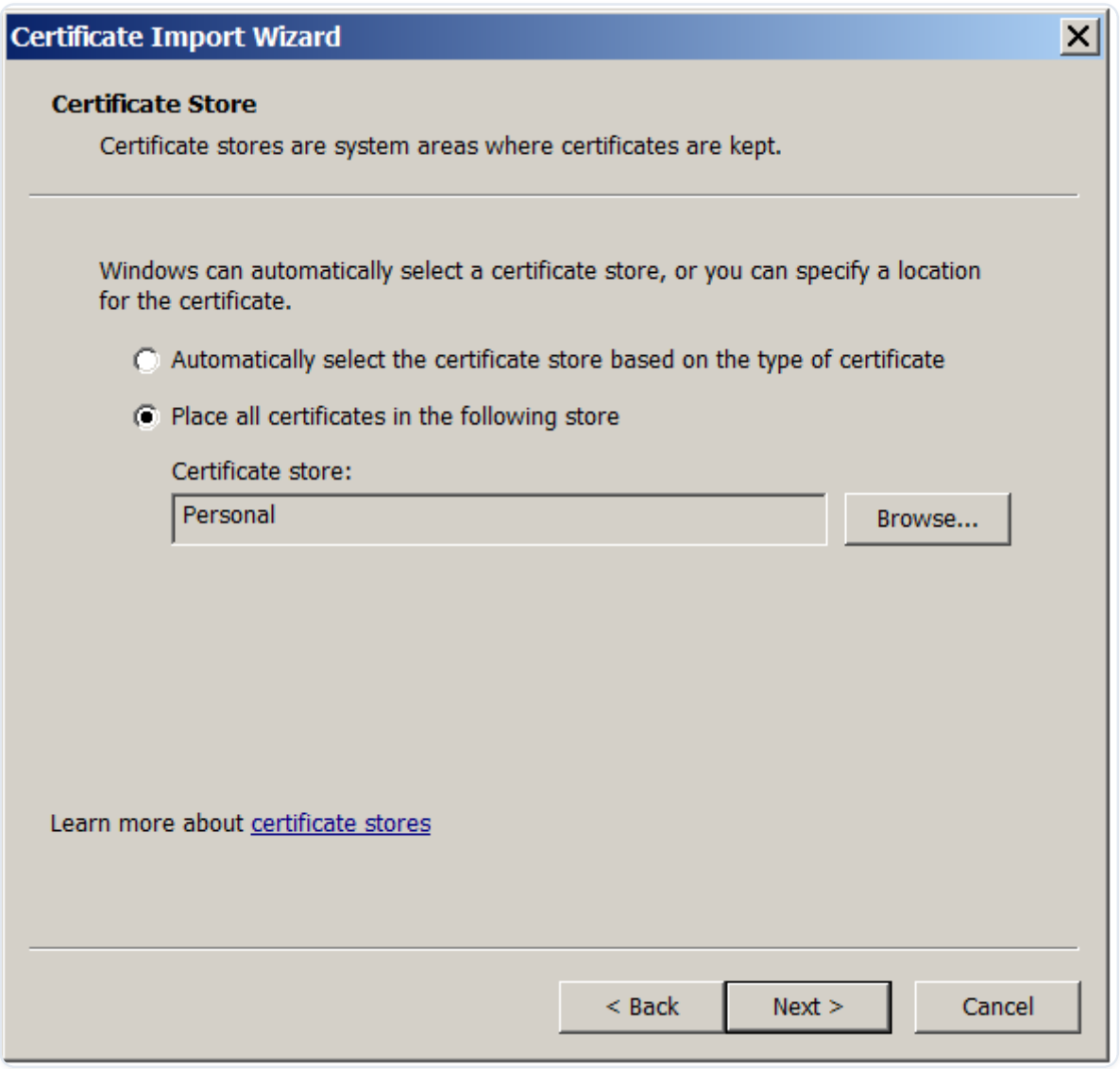
2. Quando o assistente de importação de certificado for exibido, clique em **Avançar**.



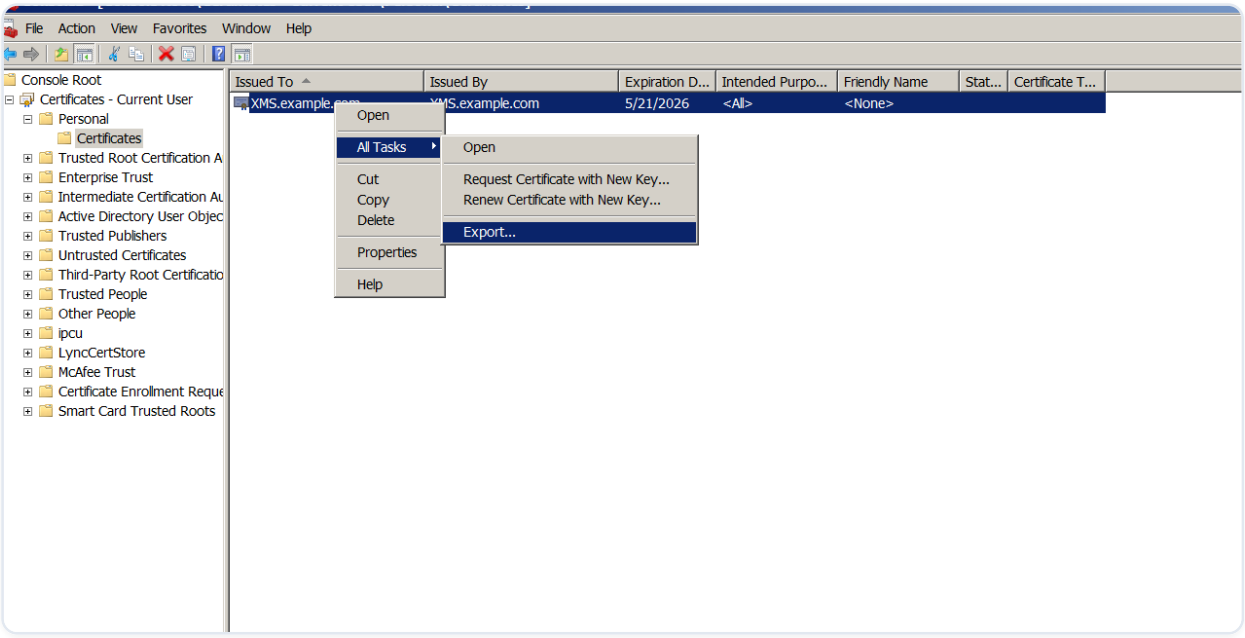
3. Procure o certificado no diretório de download.



4. Selecione **Colocar todos os certificados no seguinte repositório** e selecione **Pessoal** como o repositório de certificados. Clique em **Avançar**.



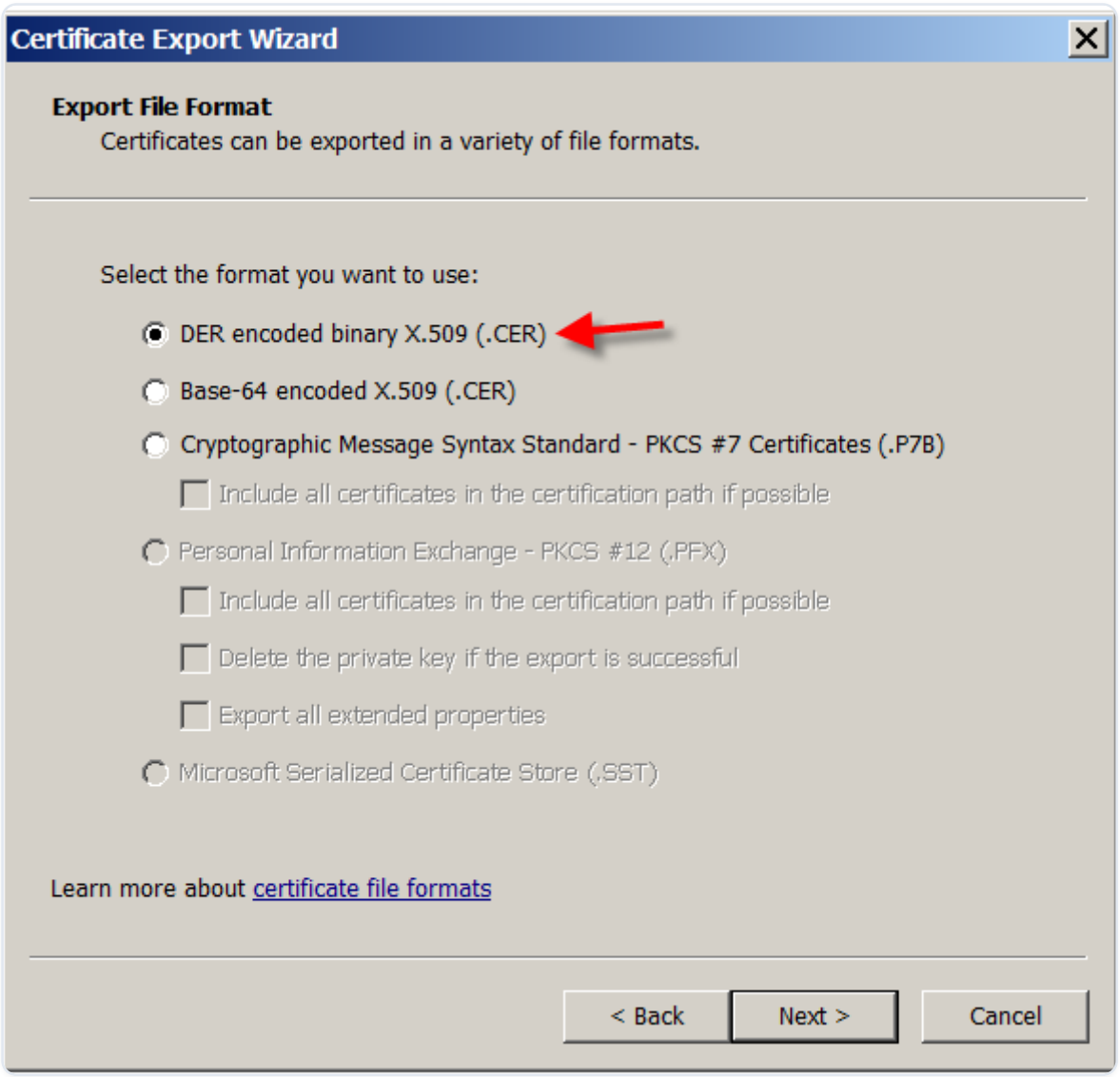
5. Revise suas seleções e clique em **Concluir**. Clique em **OK** para fechar a janela de confirmação.
6. No MMC, clique com o botão direito no certificado e então escolha **Todas as Tarefas > Exportar**.



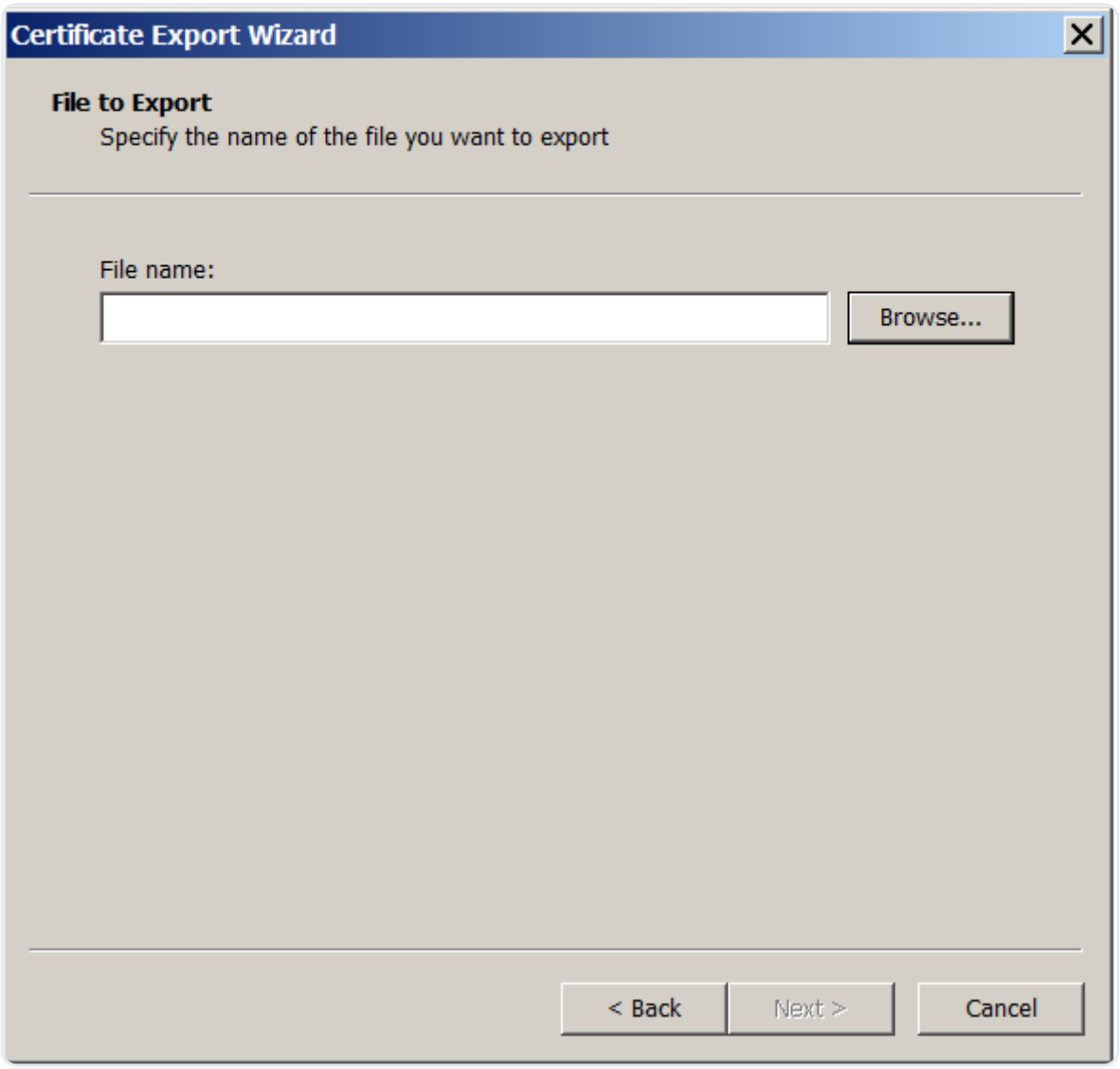
7. Quando o assistente de exportação de certificado aparecer, clique em **Avançar**.



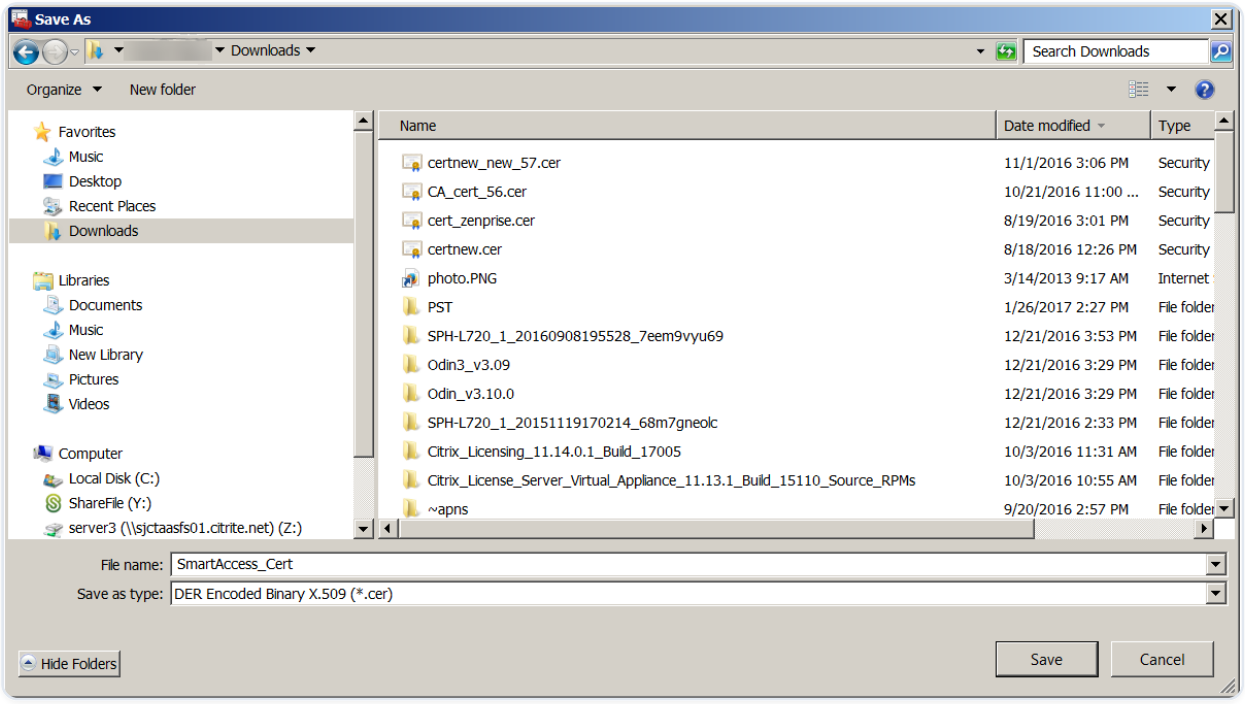
8. Escolha o formato **DER encoded binary X.509 (.CER)**. Clique em **Avançar**.



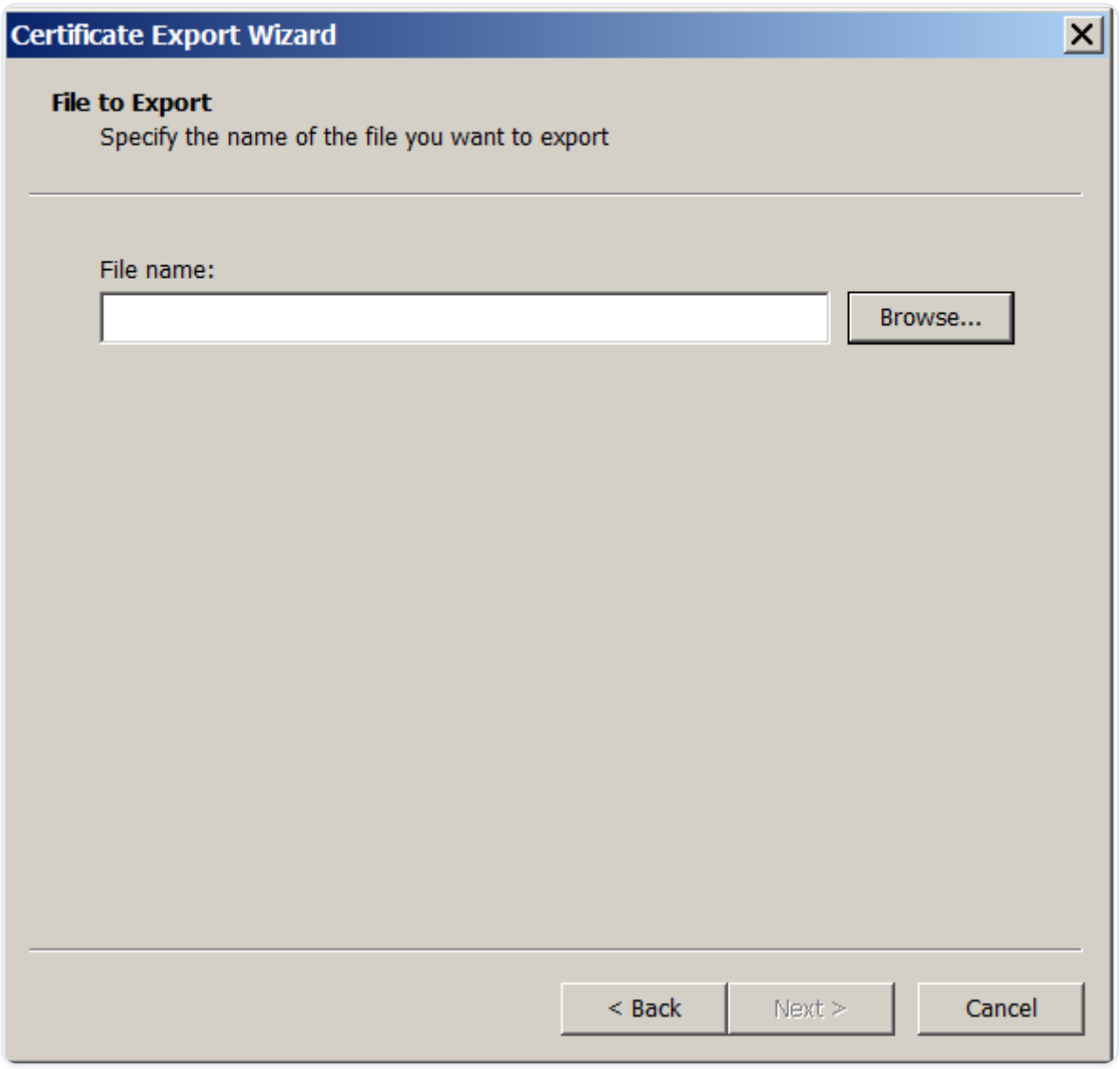
9. Navegue até o certificado. Digite um nome para o certificado e então clique em **Avançar**.



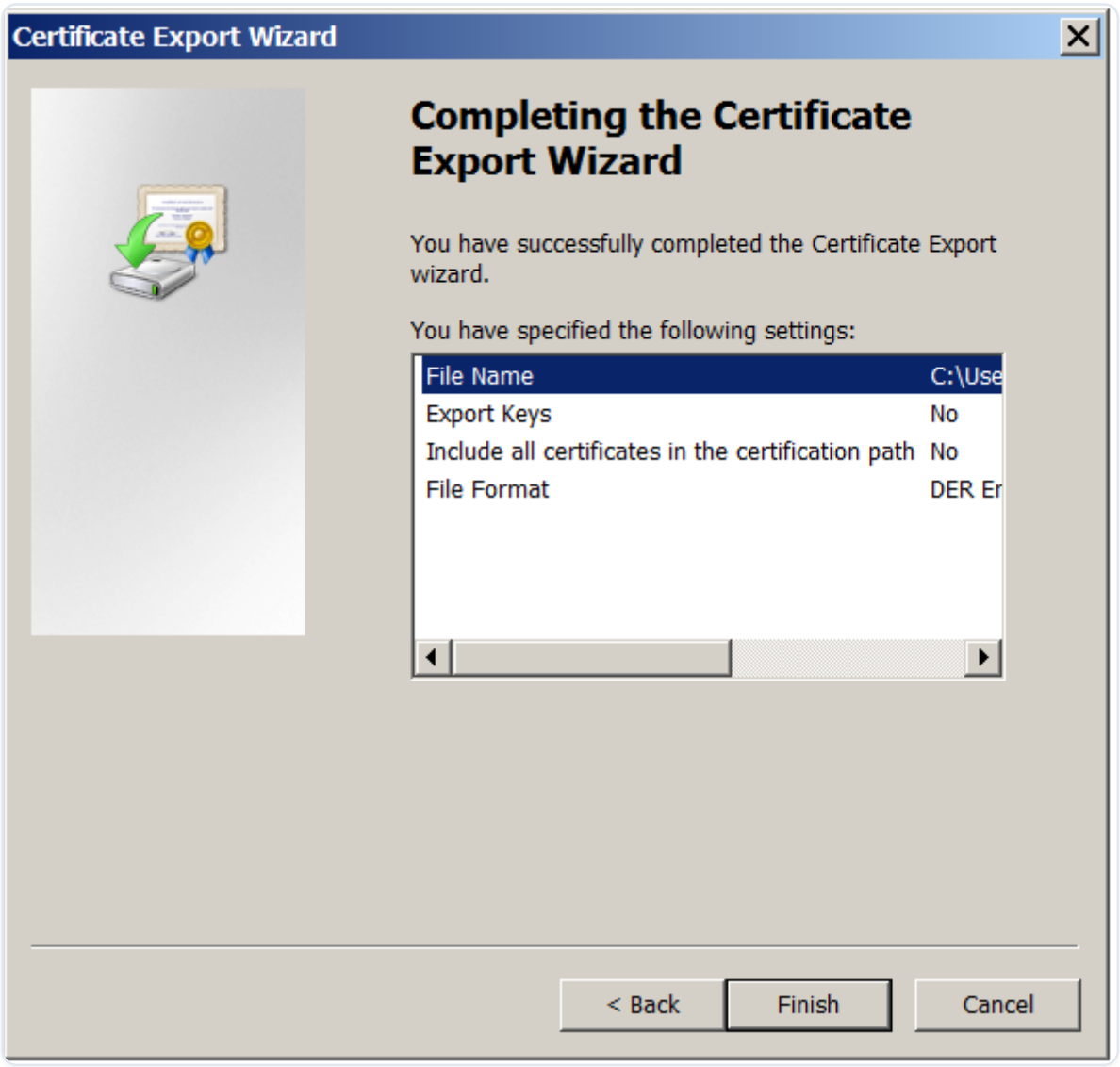
10. Salve o certificado.



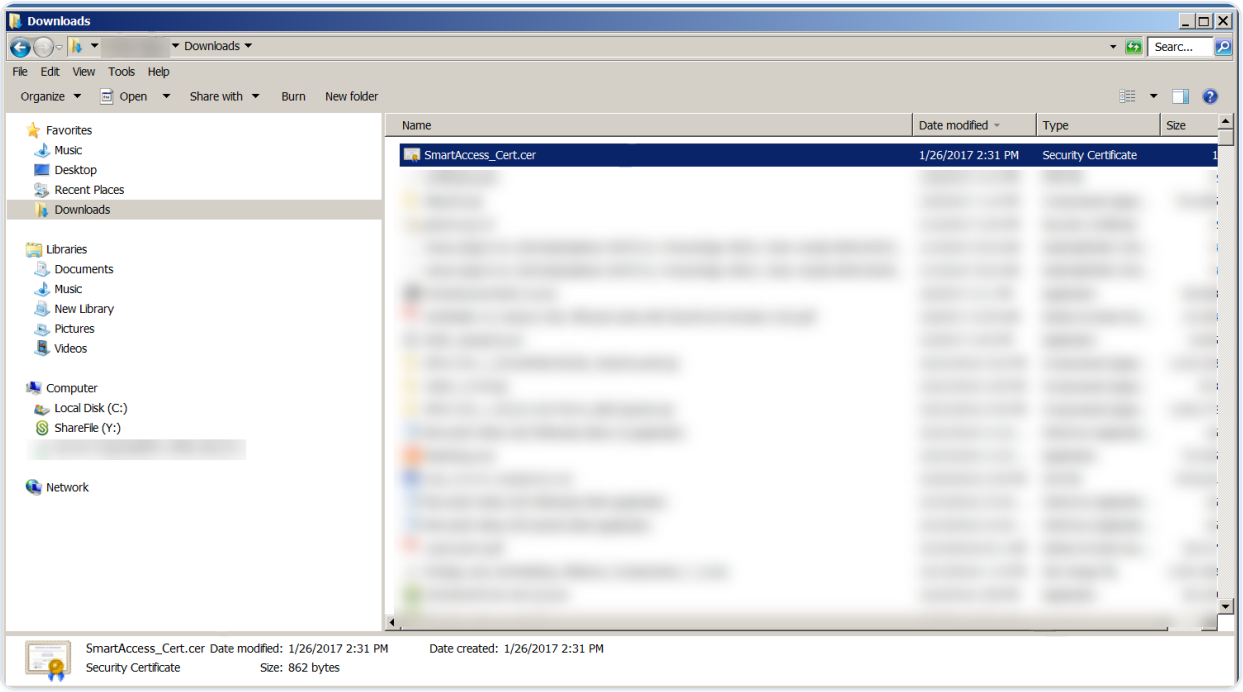
11. Navegue até o certificado e clique em **Avançar**.



12. Revise suas seleções e clique em **Concluir**. Clique em **OK** para fechar a janela de confirmação.

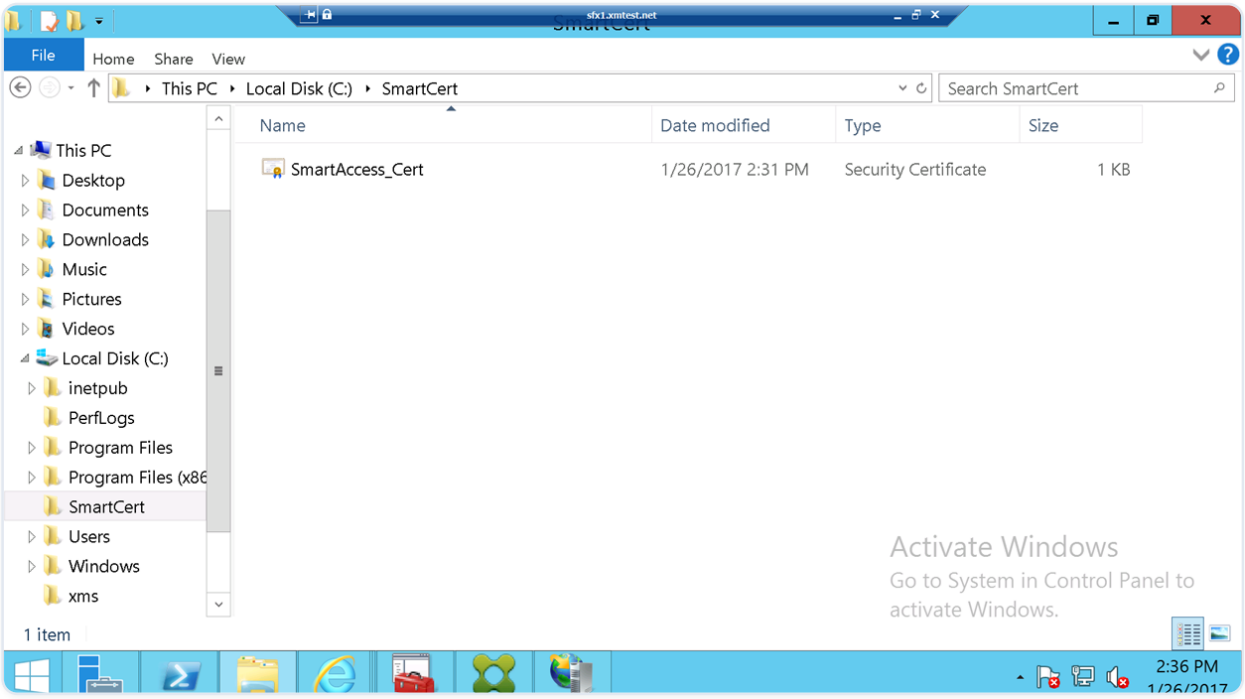


13. Localize o certificado em seu diretório de download. O certificado está no formato CER.



Copiar o certificado para o servidor StoreFront

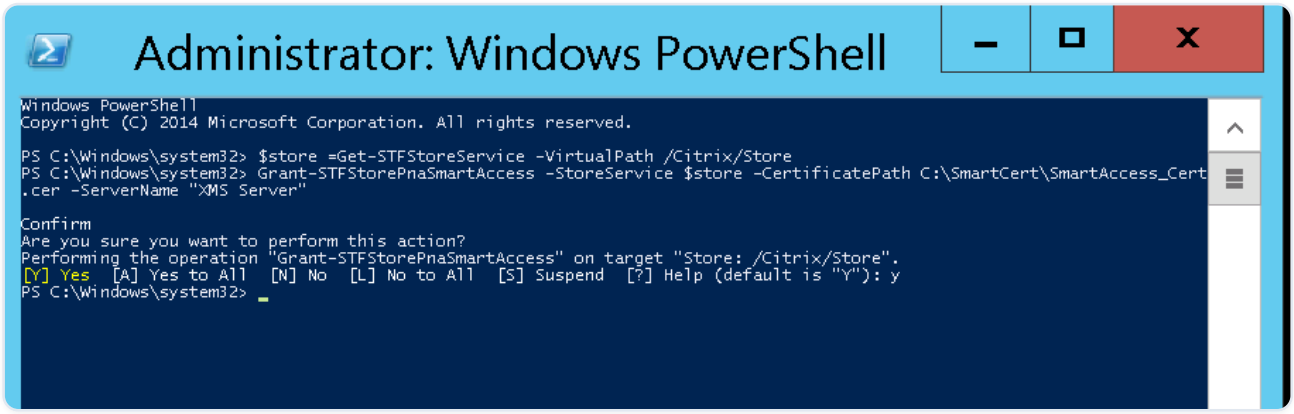
1. No servidor StoreFront, crie uma pasta chamada **SmartCert**.
2. Copie o certificado para a pasta **SmartCert**.



Configurar o certificado no armazenamento do StoreFront

No servidor StoreFront, execute este comando PowerShell para configurar o certificado convertido do XenMobile Server no armazenamento:

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```



Se houver certificados existentes no armazenamento do StoreFront, execute este comando PowerShell para revogá-los:

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```



Alternativamente, você pode executar qualquer um desses comandos PowerShell no servidor StoreFront para revogar certificados existentes no armazenamento do StoreFront:

- Revogar por nome:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server"
```

- Revogar por impressão digital:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “ReplaceWithThumbprint”
```

- Revogar por objeto de servidor:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    $access = Get-STFStorePnaSmartAccess –StoreService $store

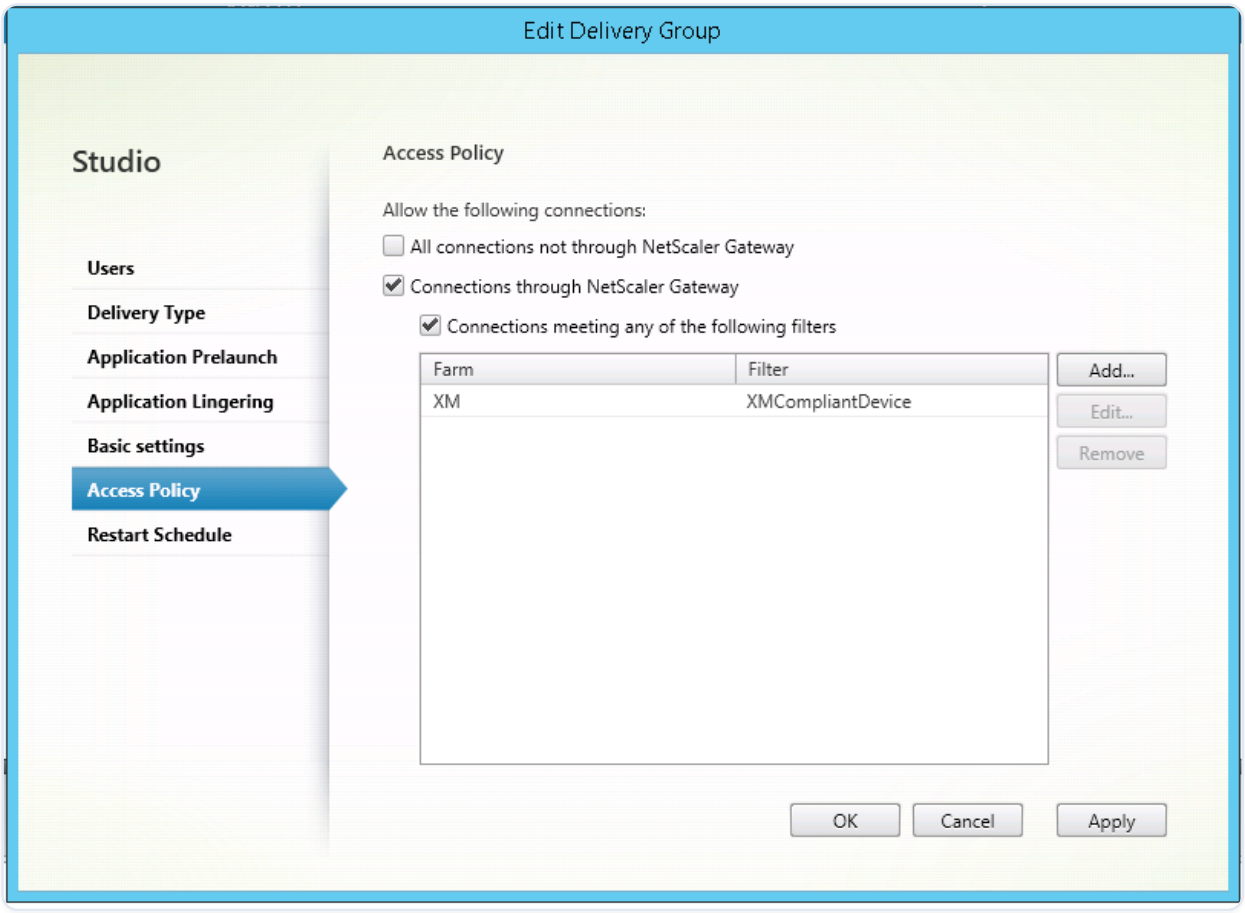


    Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

Configurar a política SmartAccess para Virtual Apps and Desktops

Para adicionar a política SmartAccess necessária ao grupo de entrega que entrega o aplicativo HDX:

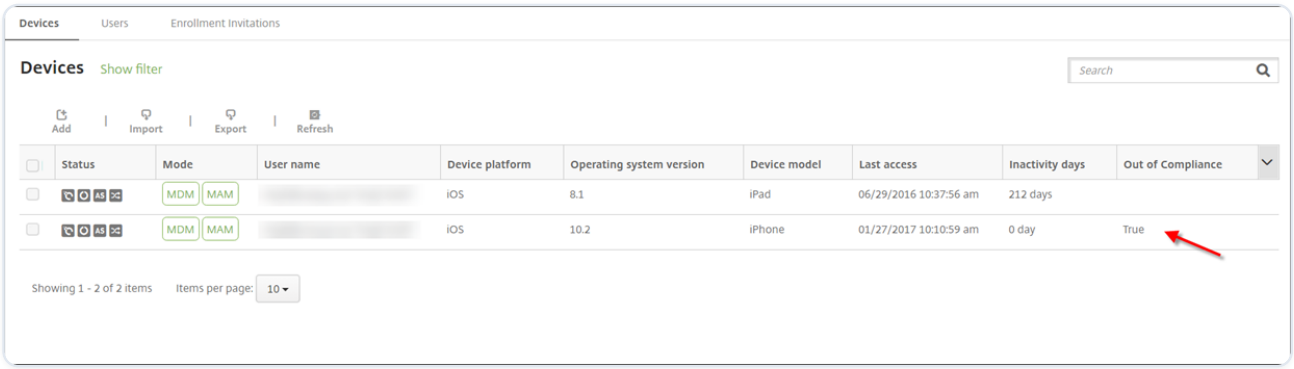
1. No servidor Virtual Apps and Desktops, abra o Citrix Studio.
2. Selecione **Grupos de Entrega** no painel de navegação do Studio.
3. Selecione um grupo que entrega o aplicativo ou aplicativos aos quais você deseja controlar o acesso. Em seguida, selecione **Editar Grupo de Entrega** no painel **Ações**.
4. Na página **Política de Acesso**, selecione **Conexões através do NetScaler® Gateway** e **Conexão que atenda a qualquer um dos seguintes**.
5. Clique em **Adicionar**.
6. Adicione uma política de acesso onde **Farm** é **XM** e **Filtro** é **XMCompliantDevice**.



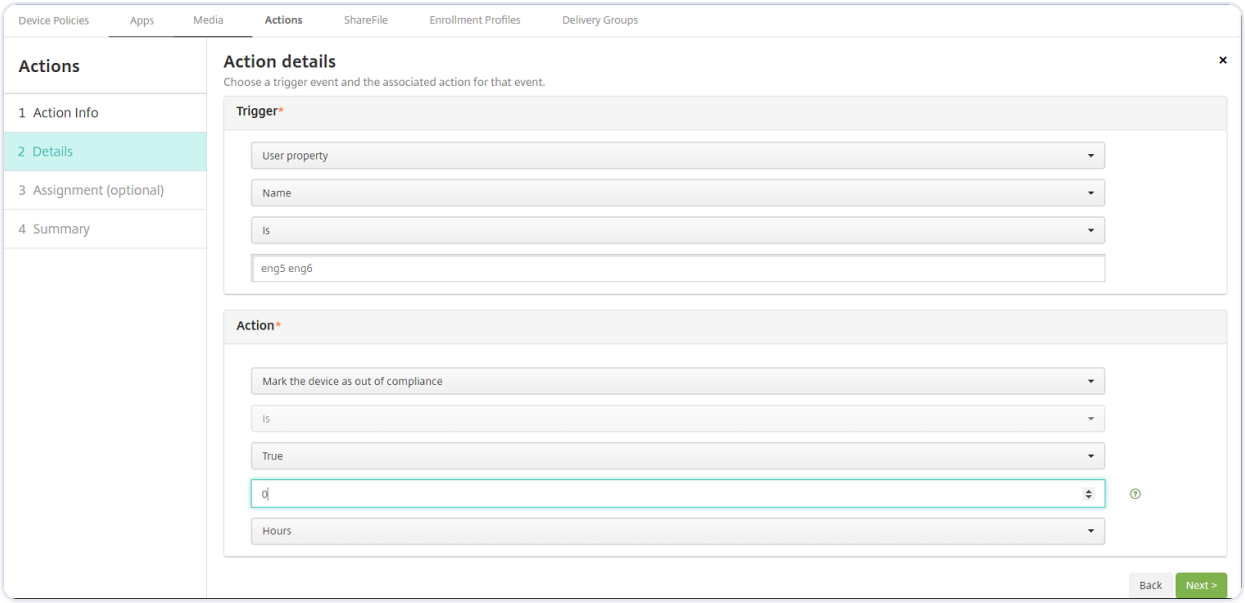
7. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Definir ações automatizadas no XenMobile

A política SmartAccess que você definiu no grupo de entrega para um aplicativo HDX nega o acesso a um dispositivo quando ele está fora de conformidade. Use ações automatizadas para marcar o dispositivo como fora de conformidade.



1. No console do XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações da Ação** é exibida.
3. Na página **Informações da Ação**, digite um nome e uma descrição para a ação.
4. Clique em **Avançar**. A página **Detalhes da ação** é exibida. No exemplo a seguir, um gatilho é criado que marca imediatamente os dispositivos como fora de conformidade se eles tiverem o nome da propriedade de usuário **eng5** ou **eng6**.



5. Na lista **Gatilho**, escolha **Propriedade do dispositivo**, **Propriedade do usuário** ou **Nome do aplicativo instalado**. O SmartAccess não oferece suporte a gatilhos de evento.
6. Na lista **Ação**:
   - Escolha **Marcar o dispositivo como fora de conformidade.**
   - Escolha **É**.

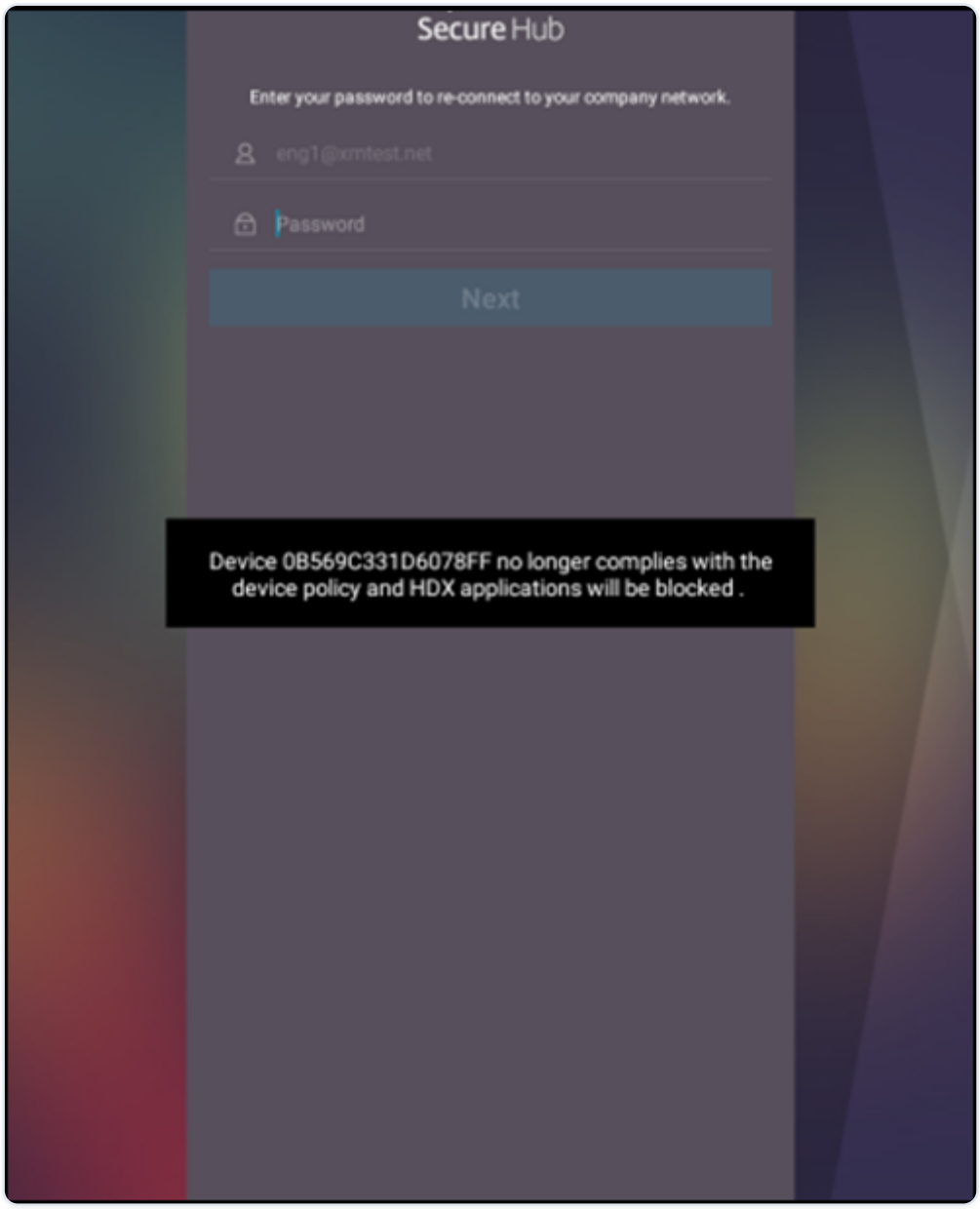
- Escolha **Verdadeiro**.
- Para definir a ação para marcar o dispositivo como fora de conformidade imediatamente quando a condição do gatilho for atendida, defina o período para **0**.

7. Escolha o grupo ou grupos de entrega do XenMobile aos quais aplicar esta ação.
8. Revise o resumo da ação.
9. Clique em **Avançar** e depois em **Salvar**.

Quando o dispositivo é marcado como fora de conformidade, os aplicativos HDX não aparecem mais na loja do Secure Hub. O usuário não está mais inscrito no aplicativo. Nenhuma notificação é enviada ao dispositivo e nada na loja do Secure Hub indica que os aplicativos HDX estavam disponíveis anteriormente.

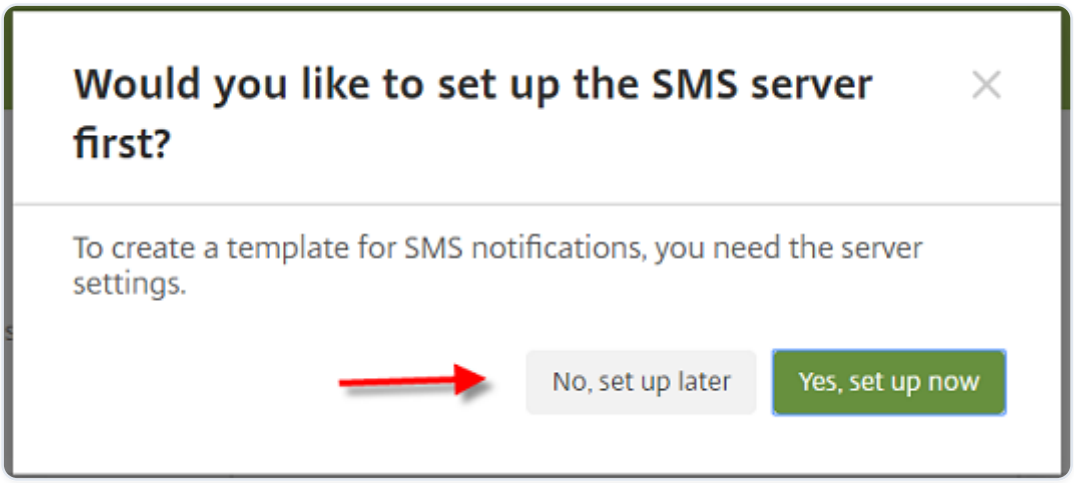
Se você quiser que os usuários sejam notificados quando um dispositivo for marcado como fora de conformidade, crie uma notificação e, em seguida, crie uma ação automatizada para enviar essa notificação.

Este exemplo cria e envia esta notificação quando um dispositivo é marcado como fora de conformidade: "O número de série ou número de telefone do dispositivo não está mais em conformidade com a política do dispositivo e os aplicativos HDX estão bloqueados."



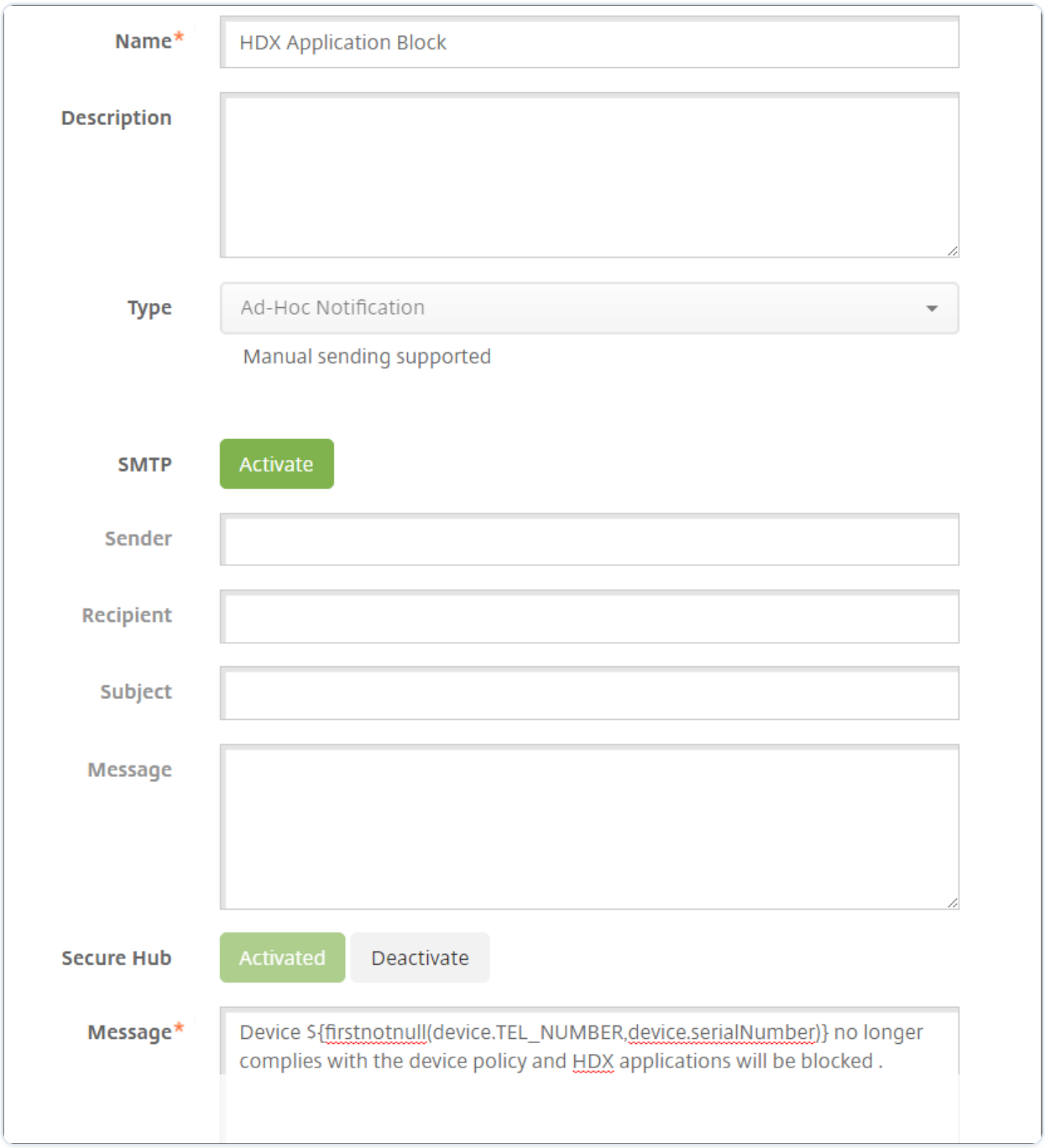
Crie a notificação que os usuários veem quando um dispositivo é marcado como fora de conformidade

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Modelos de Notificação**. A página **Modelos de Notificação** é exibida.
3. Clique em **Adicionar** para adicionar na página **Modelos de Notificação**.
4. Quando solicitado a configurar o servidor SMS primeiro, clique em **Não, configurar mais tarde**.



5. Configure estas configurações:

   - **Nome:** Bloqueio de Aplicativo HDX
   - **Descrição:** Notificação do agente quando um dispositivo está fora de conformidade
   - **Tipo:** Notificação Ad Hoc
   - **Secure Hub:** Ativado
   - **Mensagem:** O dispositivo ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} não está mais em conformidade com a política do dispositivo e os aplicativos HDX estão bloqueados.



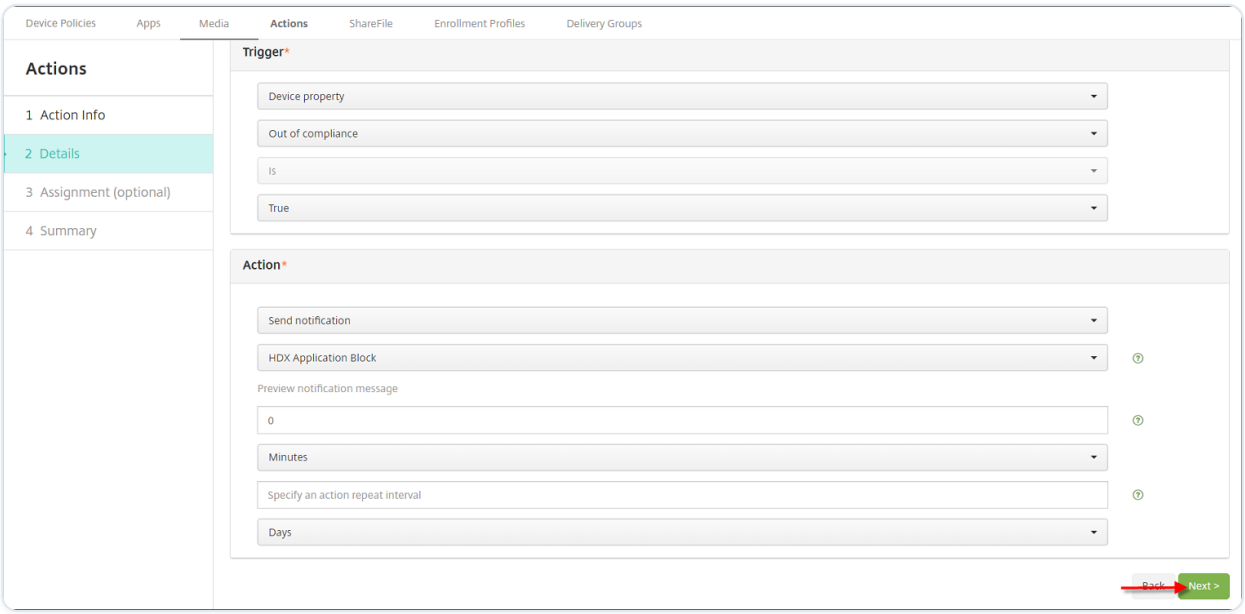
6. Clique em **Salvar**.

Crie a ação que envia a notificação quando um dispositivo é marcado como fora de conformidade

1. No console do XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações da Ação** é exibida.
3. Na página **Informações da Ação**, insira um nome e uma descrição para a ação:

   - **Nome:** Notificação de HDX bloqueado
   - **Descrição:** Notificação de HDX bloqueado porque o dispositivo está fora de conformidade

4. Clique em **Avançar**. A página **Detalhes da ação** é exibida.
5. Na lista **Gatilho**:
    - Escolha **Propriedade do dispositivo**.
    - Escolha **Fora de conformidade.**
    - Escolha **É**.
    - Escolha **Verdadeiro**.



6. Na lista **Ação**, especifique as ações que ocorrem quando o gatilho é atendido:
    - Escolha **Enviar notificação**
    - Escolha **Bloqueio de Aplicativo HDX, a notificação que você criou**.
    - Escolha **0**. Definir este valor como 0 faz com que a notificação seja enviada quando a condição de gatilho for atendida.
7. Selecione o grupo ou grupos de entrega do XenMobile aos quais aplicar esta ação. Neste exemplo, escolha **Todos os Usuários**.
8. Revise o resumo da ação.
9. Clique em **Avançar** e depois clique em **Salvar**.

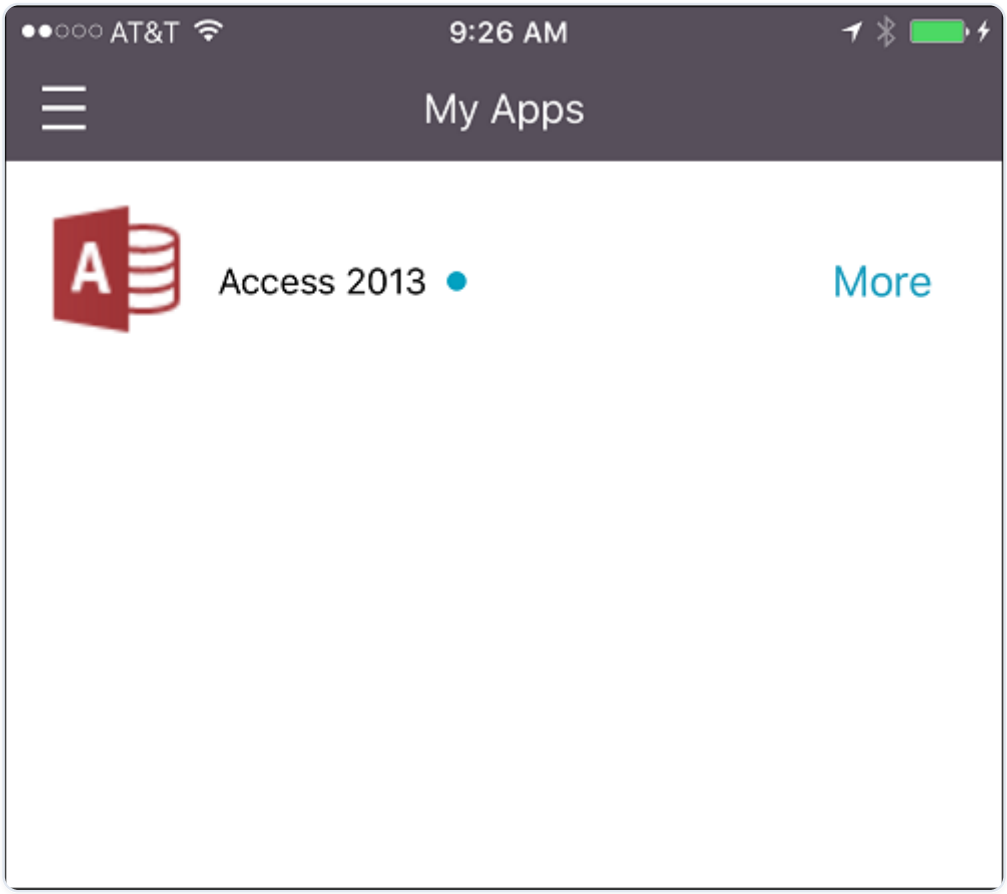
Para obter mais informações sobre como configurar ações automatizadas, consulte Ações automatizadas.

Como os usuários recuperam o acesso aos aplicativos HDX

Os usuários podem obter acesso aos aplicativos HDX novamente depois que o dispositivo for novamente colocado em conformidade:

1. No dispositivo, vá para a loja do Secure Hub para atualizar os aplicativos na loja.
2. Vá para o aplicativo e toque em **Adicionar** ao aplicativo.

Depois que o aplicativo é adicionado, ele aparece em Meus Aplicativos com um ponto azul ao lado, porque é um aplicativo recém-instalado.



Adicionar mídia

Você adiciona mídia ao XenMobile® para que possa implantá-la em dispositivos de usuário. Você pode usar o XenMobile para implantar Livros da Apple que você obtém por meio de compra por volume da Apple.

Depois de configurar uma conta de compra por volume no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura livros para implantação em dispositivos iOS, escolhendo grupos de entrega e especificando regras de implantação.

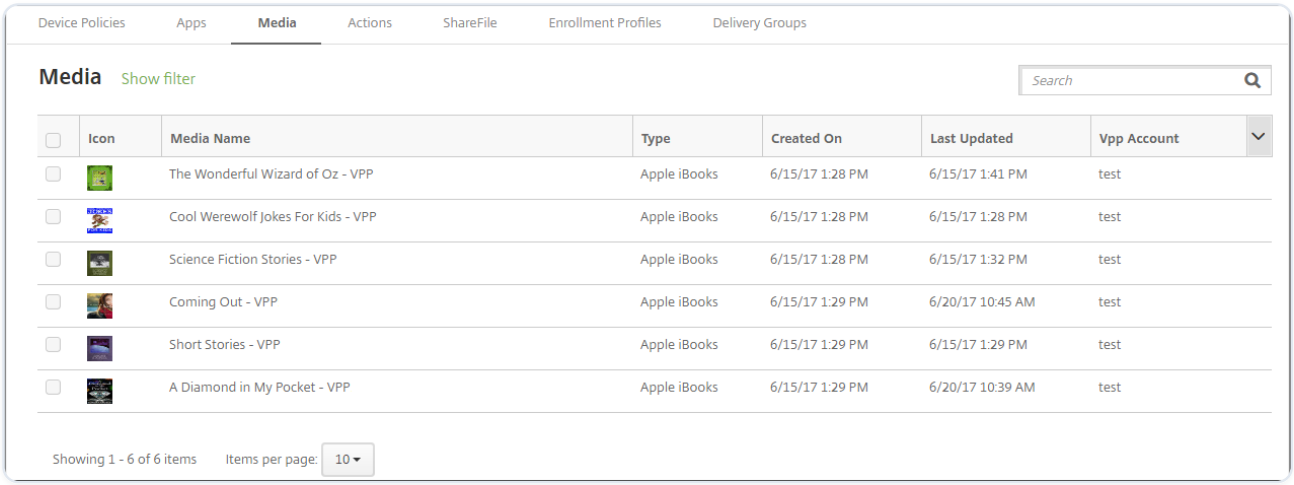
Na primeira vez que um usuário recebe um livro e aceita a licença de compra por volume, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple Book. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala livros como mídia obrigatória. Se um usuário excluir um livro instalado de seu dispositivo, o livro permanecerá no aplicativo Apple Book, pronto para download.

Pré-requisitos

- Dispositivos iOS
- Configure a compra por volume da Apple no XenMobile, conforme descrito em Compra por Volume da Apple.

Configurar livros

Os Livros da Apple obtidos por meio de compra por volume aparecem na página **Configurar > Mídia**.



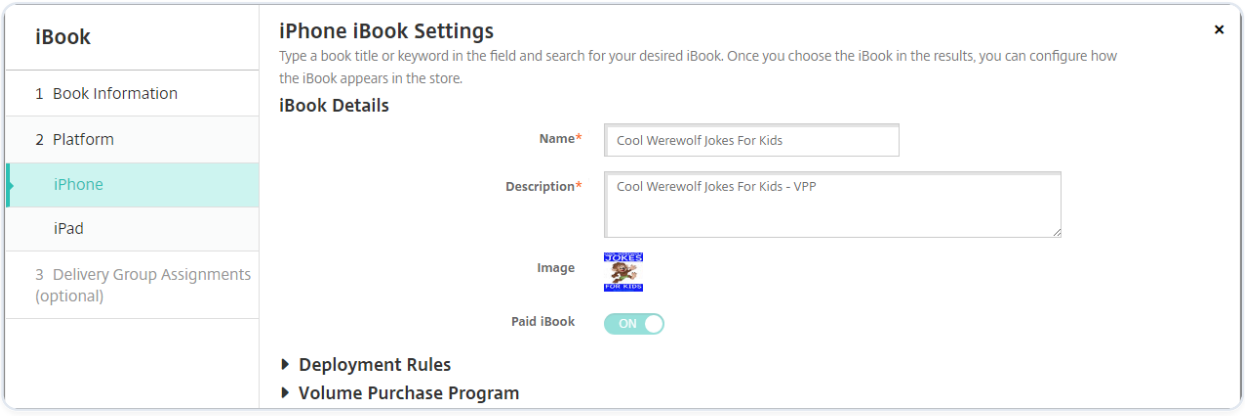
Para configurar um Livro da Apple para implantação

1. Em **Configurar > Mídia**, selecione um livro e clique em **Editar**. A página **Informações do Livro** é exibida.

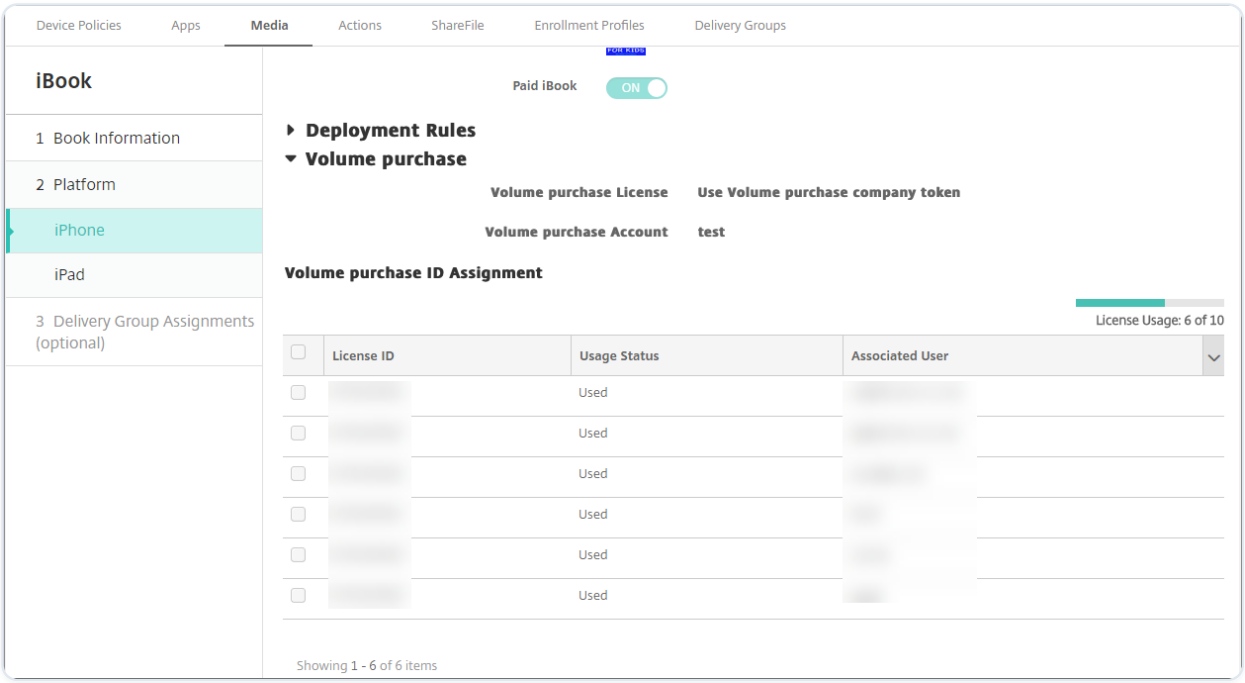


O **Nome** e a **Descrição** aparecem apenas no console e nos logs do XenMobile.

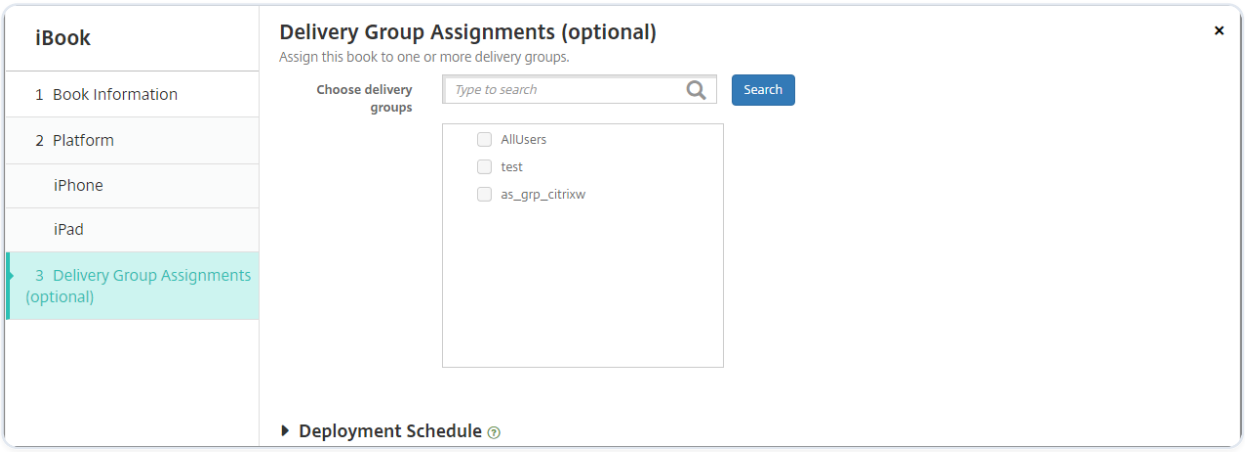
2. Nas páginas **Configurações do iBook para iPhone** e **Configurações do iBook para iPad**: Embora você possa opcionalmente alterar o nome e a descrição do livro, a Citrix® recomenda que você não altere essas configurações. A imagem é para sua informação e não é editável. **iBook Pago** indica que um livro foi comprado por meio de compra por volume da Apple.



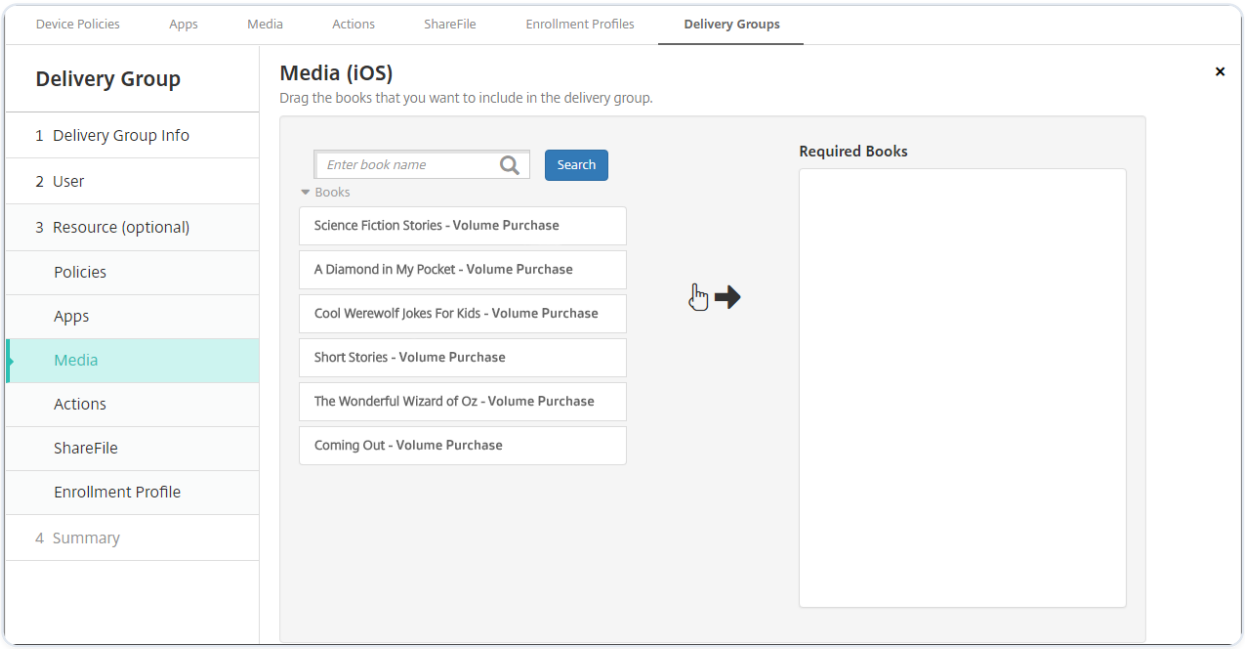
Você também pode especificar regras de implantação ou visualizar informações de compra por volume.



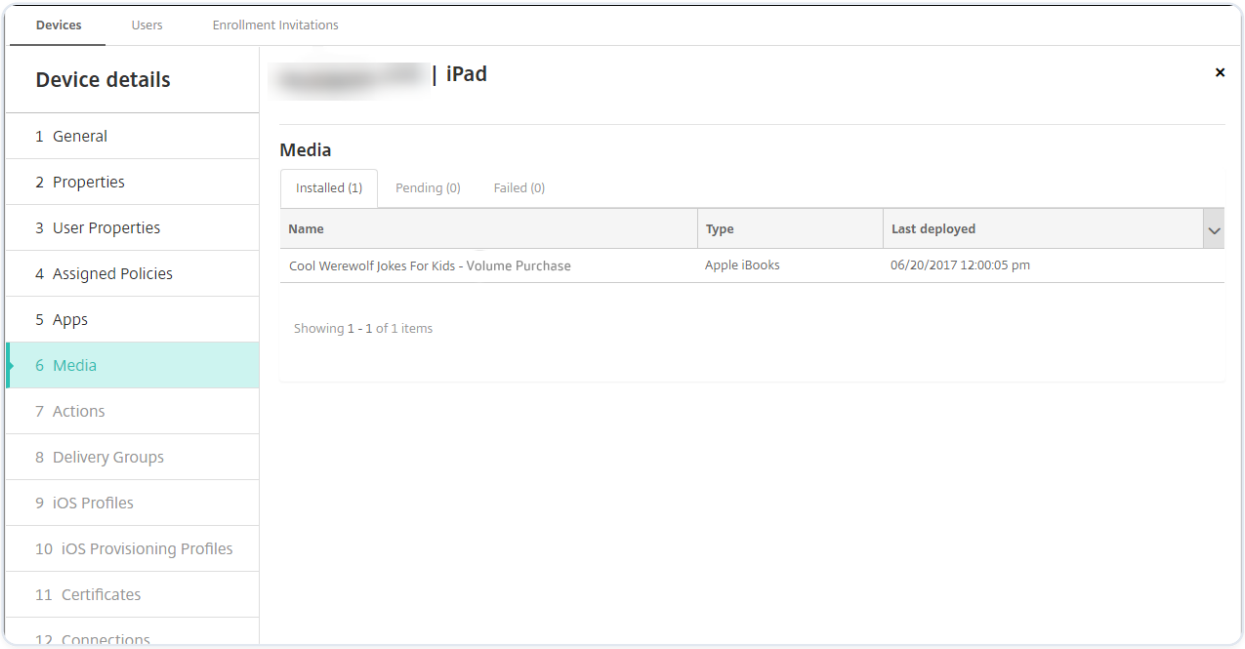
3. Opcionalmente, atribua o livro a grupos de entrega e defina um agendamento de implantação.



Você também pode atribuir livros a grupos de entrega na guia **Mídia** para **Configurar > Grupos de Entrega**. O XenMobile oferece suporte apenas à implantação de livros obrigatórios.



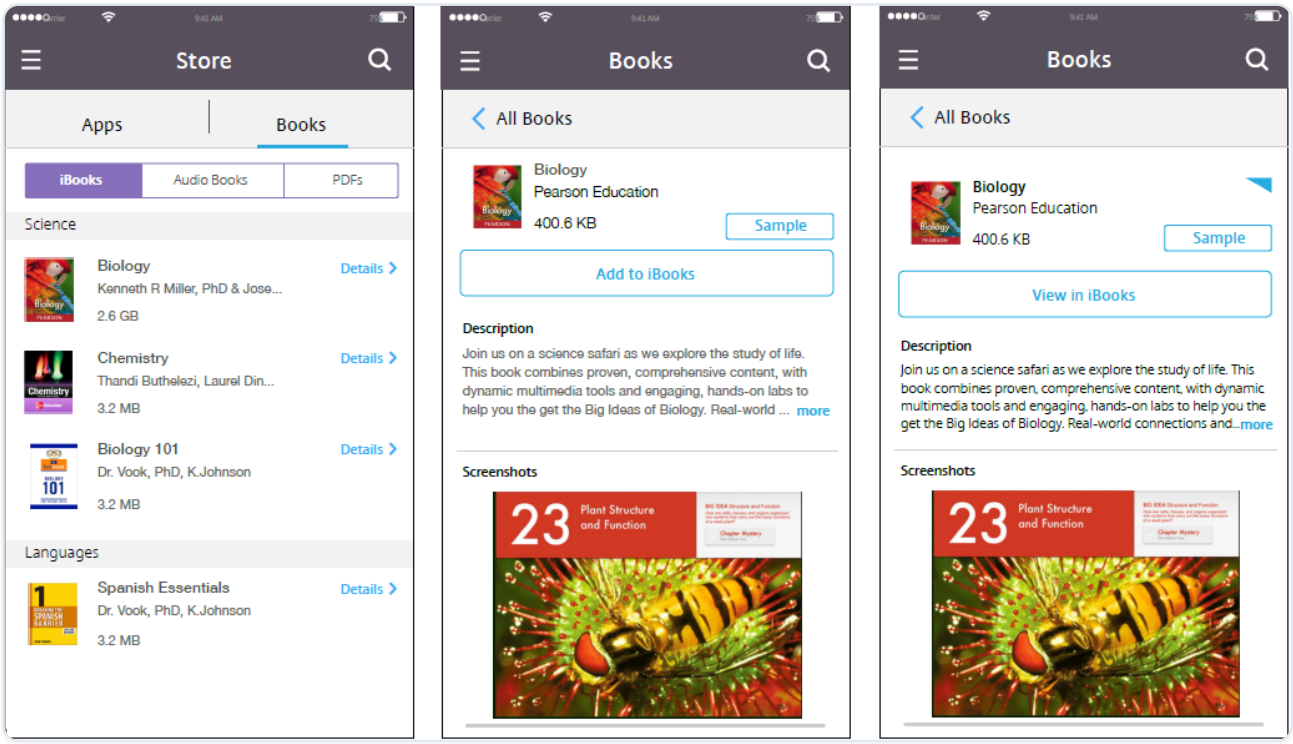
4. Use a guia **Mídia** para **Gerenciar > Dispositivos** para visualizar o status da implantação.



Observação:

Na página **Configurar > Mídia**, se você selecionar um livro e clicar em **Excluir**, o XenMobile removerá o livro da lista. No entanto, na próxima vez que o XenMobile sincronizar com a compra por volume da Apple, o livro reaparecerá na lista, a menos que tenha sido removido da compra por volume da Apple. Excluir um livro da lista não o remove do dispositivo.

Os livros aparecem nos dispositivos dos usuários conforme mostrado no exemplo a seguir.


Store
Apps
Books
iBooks
Audio Books
PDFs
Science
Biology
Kenneth R Miller, PhD & Jose...
2.6 GB
Details
Chemistry
Thandi Buthelezi, Laurel Din...
3.2 MB
Details
Biology 101
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Languages
Spanish Essentials
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
Add to iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world ... more
Screenshots
23
Plant Structure and Function
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
View in iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world connections and...more
Screenshots
23
Plant Structure and Function

Implantar recursos

A configuração e o gerenciamento de dispositivos geralmente envolvem a criação de recursos (políticas, aplicativos e mídia) e ações no console do XenMobile® e, em seguida, empacotá-los usando grupos de entrega. A ordem em que o XenMobile envia recursos e ações em um grupo de entrega para os dispositivos é chamada de ordem de implantação. Este artigo descreve como:

- Adicionar, gerenciar e implantar grupos de entrega
- Alterar a ordem de implantação de recursos e ações em grupos de entrega
- O XenMobile determina a ordem de implantação quando um usuário está em vários grupos de entrega que possuem políticas duplicadas ou conflitantes.

Os grupos de entrega especificam a categoria de usuários para cujos dispositivos você implanta combinações de políticas, aplicativos, mídia e ações. A inclusão em um grupo de entrega é tipicamente baseada em características do usuário, como empresa, país, departamento, endereço do escritório e cargo. Os grupos de entrega oferecem maior controle sobre quem recebe quais recursos e quando os recebe. Você pode implantar um grupo de entrega para todos ou para um grupo de usuários mais restrito.

Implantar em um grupo de entrega significa enviar uma notificação push para todos os usuários com dispositivos iOS e Windows compatíveis. Esses usuários devem pertencer ao grupo de entrega para se reconectarem ao XenMobile. Você pode reavaliar os dispositivos e implantar políticas, aplicativos, mídia e ações que fazem parte de um grupo de entrega.

Para usuários com dispositivos Android: Se já estiverem conectados, eles recebem os recursos imediatamente. Caso contrário, com base em sua política de agendamento, eles recebem os recursos na próxima vez que se conectarem.

O grupo de entrega padrão AllUsers é criado quando você instala e configura o XenMobile. Ele contém todos os usuários locais e usuários do Active Directory. Você não pode excluir o grupo AllUsers, mas pode desativá-lo quando não quiser enviar recursos para todos os usuários.

Ordem de implantação

A ordem de implantação é a sequência na qual o XenMobile envia recursos para os dispositivos. A ordem de implantação se aplica apenas a dispositivos em um grupo de entrega com um perfil de registro configurado para gerenciamento de dispositivos (MDM).

Ao determinar a ordem de implantação, o XenMobile aplica filtros e critérios de controle, como regras de implantação e agendamento de implantação, aos recursos. Os recursos incluem políticas, aplicativos, ações e grupos de entrega. Antes de adicionar grupos de entrega, considere como as informações nesta seção se relacionam com seus objetivos de implantação.

Aqui está um resumo dos principais conceitos relacionados à ordem de implantação:

- **Ordem de implantação:** A sequência na qual o XenMobile envia recursos (políticas, aplicativos e mídia) e ações para um dispositivo. A ordem de implantação para algumas políticas, como Termos e Condições e Inventário de Software, não tem efeito sobre outros recursos. A ordem em que as ações são implantadas não tem efeito sobre outros recursos. Portanto, sua posição é ignorada quando o XenMobile implanta os recursos.
- **Regras de implantação:** O XenMobile usa as regras de implantação que você especifica para as propriedades do dispositivo para filtrar políticas, aplicativos, mídia, ações e grupos de entrega. Por exemplo, uma regra de implantação pode especificar o envio do pacote de implantação quando um nome de domínio corresponde a um valor específico.
- **Agendamento de implantação:** O XenMobile usa o agendamento de implantação que você especifica para políticas, aplicativos, mídia e ações para controlar a implantação desses itens. Você pode especificar que uma implantação ocorra imediatamente, em uma data e hora específicas ou de acordo com as condições de implantação.

A tabela a seguir mostra os critérios de filtro e controle para os vários tipos de objeto e recurso. As regras de implantação são baseadas nas propriedades do dispositivo.

OBJETO/ RECURSO	PLATAFORMA DO DISPOSITIVO	REGRA DE IMPLANTAÇÃO	AGENDAMENTO DE IMPLANTAÇÃO	USUÁRIO/ GRUPOS
Política de dispositivo	S	S	S	-
Aplicativo	S	S	S	-
Mídia	S	S	S	-

OBJETO/ RECURSO	PLATAFORMA DO DISPOSITIVO	REGRA DE IMPLANTAÇÃO	AGENDAMENTO DE IMPLANTAÇÃO	USUÁRIO/ GRUPOS
Ação	-	S	S	-
Grupo de entrega	-	S	-	S

É provável que, em um ambiente típico, vários grupos de entrega sejam atribuídos a um único usuário, com os seguintes resultados possíveis:

- Objetos duplicados existem dentro dos grupos de entrega.
- Uma política específica é configurada de forma diferente em mais de um grupo de entrega atribuído a um usuário.

Quando qualquer uma dessas situações ocorre, o XenMobile calcula uma ordem de implantação para todos os objetos que ele deve entregar a um dispositivo ou sobre os quais deve agir. As etapas de cálculo são independentes da plataforma do dispositivo.

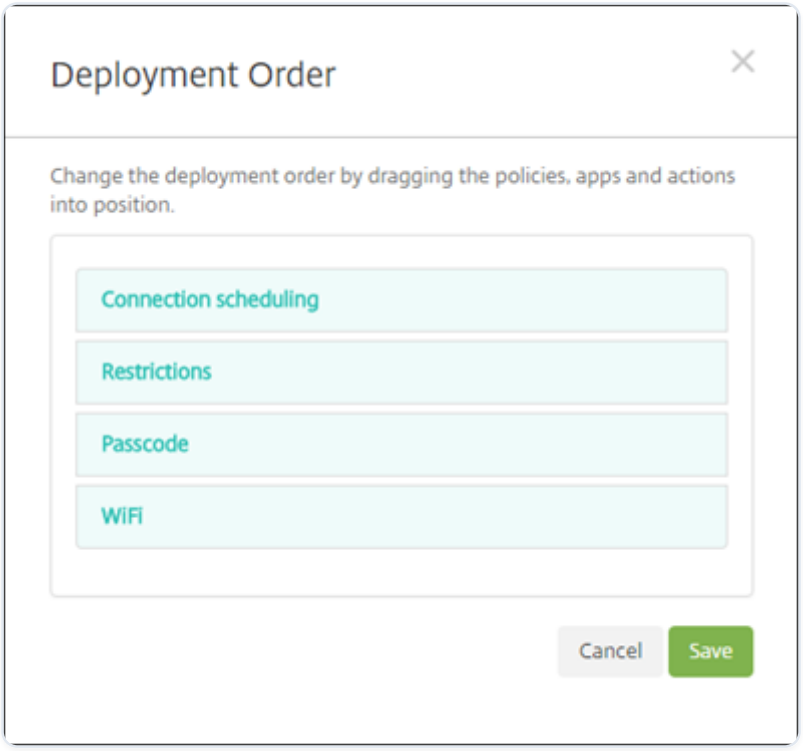
Etapas de cálculo

1. Determine todos os grupos de entrega para um usuário específico, com base nos filtros de usuários, grupos e regras de implantação.
2. Crie uma lista ordenada de todos os recursos (políticas, aplicativos, mídia e ações) dentro dos grupos de entrega selecionados. A lista é baseada nos filtros de plataforma do dispositivo, regras de implantação e agendamento de implantação. O algoritmo de ordenação é o seguinte:
    a. Coloque os recursos de grupos de entrega que possuem uma ordem de implantação definida pelo usuário antes dos recursos de grupos de entrega sem uma. A justificativa para este posicionamento é descrita após estas etapas.
    b. Como critério de desempate entre grupos de entrega, ordene os recursos dos grupos de entrega pelo nome do grupo de entrega. Por exemplo, coloque os recursos do grupo de entrega A antes dos recursos do grupo de entrega B.
    c. Durante a classificação, se uma ordem de implantação definida pelo usuário for especificada para os recursos de um grupo de entrega, mantenha essa ordem. Caso contrário, classifique os recursos dentro desse grupo de entrega pelo nome do recurso.
    d. Se o mesmo recurso aparecer mais de uma vez, remova o recurso duplicado.

Recursos que possuem uma ordem definida pelo usuário associada a eles são implantados antes dos recursos sem uma ordem definida pelo usuário. Um recurso pode existir em vários grupos de entrega atribuídos a um usuário. Conforme indicado nas etapas acima, o algoritmo de cálculo remove recursos redundantes e entrega apenas o primeiro recurso nesta lista. Ao remover recursos duplicados dessa forma, o XenMobile impõe a ordem definida pelo administrador do XenMobile.

Por exemplo, suponha que você tenha dois grupos de entrega da seguinte forma:

- Grupo de entrega, Gerentes de Conta 1: Com ordem **não especificada** para recursos. Contém as políticas **WiFi** e **Senha**.
- Grupo de entrega, Gerentes de Conta 2: Com ordem **especificada** para recursos. Contém as políticas **Agendamento de conexão**, **Restrições**, **Senha** e **WiFi**. Nesse caso, você deseja entregar a política de **Senha** antes da política de **WiFi**.



Se o algoritmo de cálculo ordenasse os grupos de implantação apenas por nome, o XenMobile executaria a implantação nesta ordem, começando com o grupo de entrega Gerentes de Conta 1: **WiFi**, **Senha**, **Agendamento de conexão** e **Restrições**. O XenMobile ignoraria **Senha** e **WiFi**, ambos duplicados, do grupo de entrega Gerentes de Conta 2.

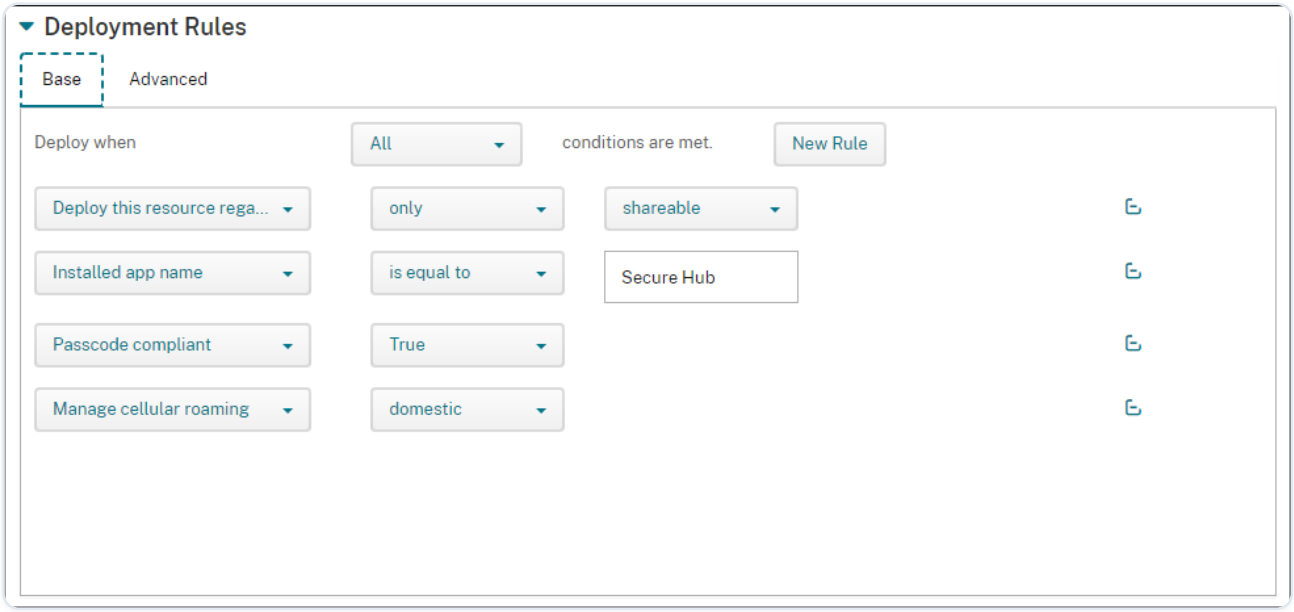
No entanto, o grupo Gerentes de Conta 2 tem uma ordem de implantação especificada pelo administrador. Portanto, o algoritmo de cálculo coloca os recursos do grupo de entrega Gerentes de Conta 2 mais acima na lista do que os recursos do outro grupo de entrega. Como resultado, o XenMobile implanta as políticas nesta ordem: **Agendamento de conexão**, **Restrições**, **Senha** e

WiFi. O XenMobile ignora as políticas **WiFi** e **Senha** do grupo de entrega Gerentes de Conta 1, porque são duplicadas. Esse algoritmo, portanto, respeita a ordem especificada pelo administrador do XenMobile.

Regras de implantação

Configure regras de implantação para entregar recursos somente quando condições específicas existirem. Você pode configurar regras de implantação básicas ou avançadas.

Ao adicionar uma regra de implantação usando o editor básico, primeiro selecione quando implantar o recurso.



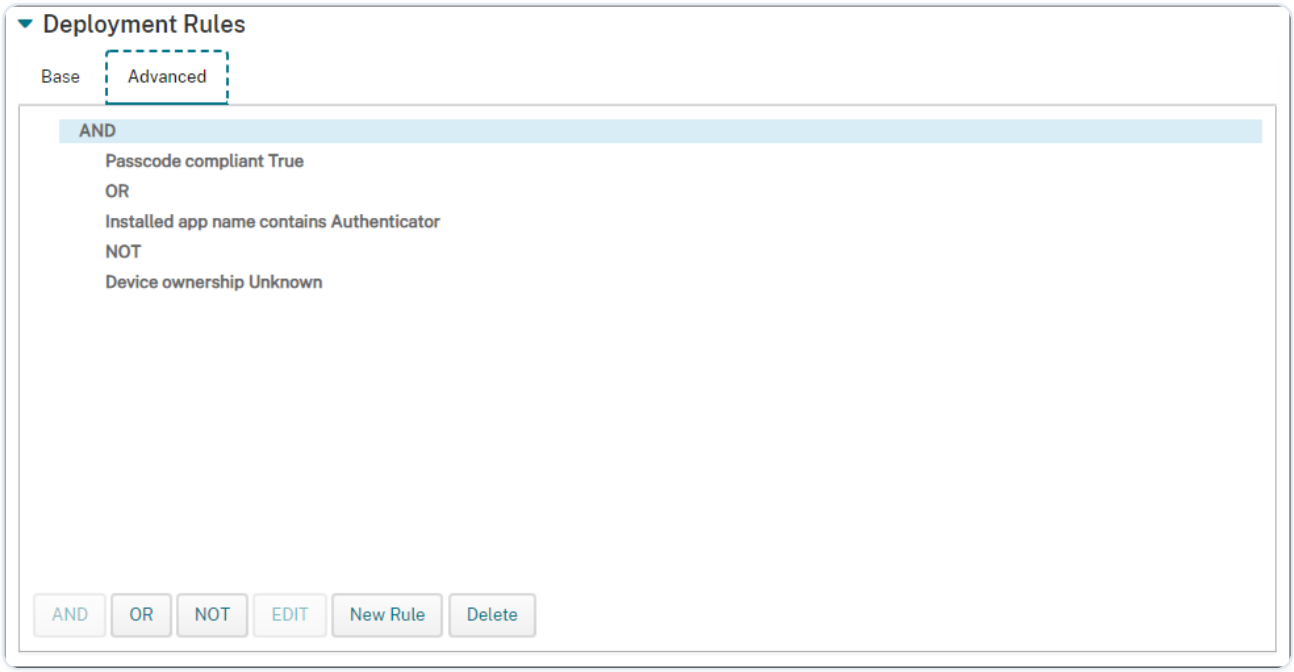
- **Todos:** Entregue o recurso quando o usuário ou dispositivo atender a todas as condições que você configurar.
- **Qualquer um:** Entregue o recurso quando o usuário ou dispositivo atender a pelo menos uma das condições que você configurar.

Clique em **Nova Regra** para adicionar uma condição. As regras variam com base no recurso que está sendo implantado e na plataforma para a qual você configura o recurso. Existem vários tipos de regras. Você pode optar por implantar o recurso:

- Somente quando a propriedade selecionada existir ou exceto quando a propriedade selecionada existir.
- Quando a propriedade corresponder exatamente ao texto que você digita, a propriedade contiver o texto que você digita ou a propriedade não corresponder ao texto que você digita.

- Quando o dispositivo ou usuário estiver em conformidade com a propriedade que você selecionar ou não estiver em conformidade com a propriedade que você selecionar.
- Quando as propriedades do dispositivo ou do usuário correspondem à condição que você seleciona em uma lista predefinida.

Use o editor avançado para criar regras de implantação mais complexas. Existem mais regras para selecionar e você pode combinar diferentes operadores de lógica booleana ao criar uma regra avançada.



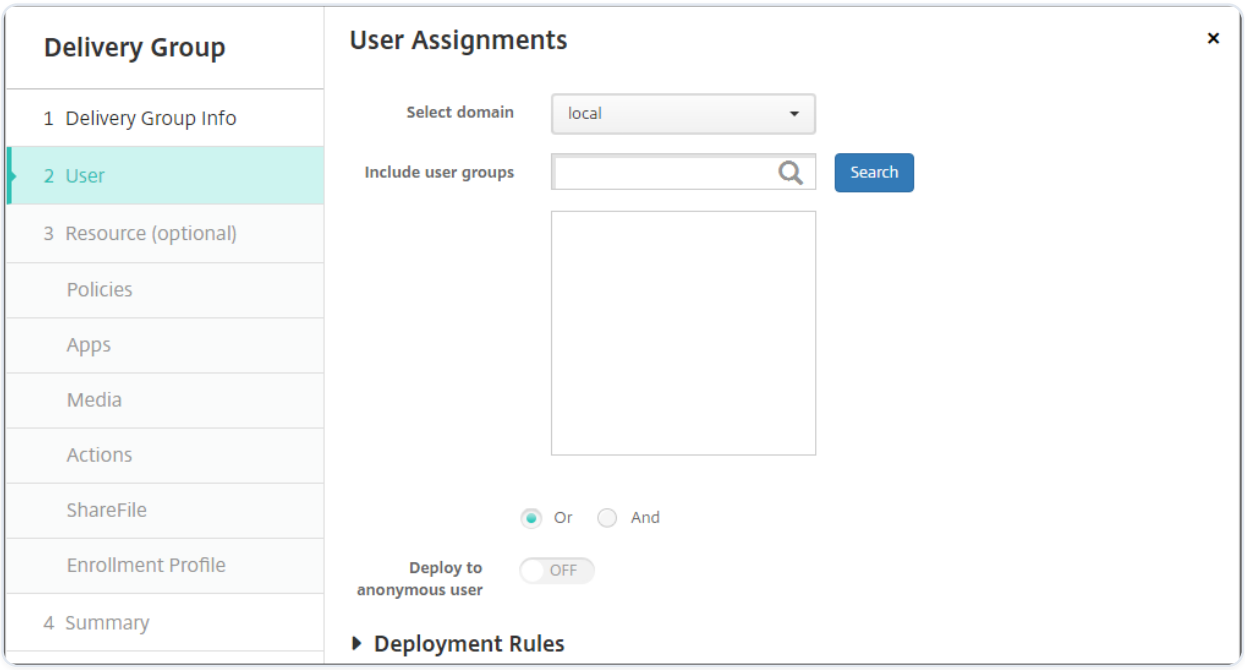
Para adicionar um grupo de entrega

A Citrix® recomenda criar grupos de entrega antes de criar políticas de dispositivo e perfis de registro.

1. No console, clique em **Configurar > Grupos de Entrega**.
2. Na página **Grupos de Entrega**, clique em **Adicionar**.
3. Na página **Informações do Grupo de Entrega**, digite um nome e uma descrição para o grupo de entrega e clique em **Avançar**.

   Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabetizada de grupos de entrega. Para obter mais informações, consulte Perfis de registro.

4. Na página **Atribuições de Usuário**, especifique como gerenciar as atribuições de usuário do grupo de entrega.



Importante:

Você não pode alterar a configuração **Gerenciar atribuições de usuário** depois que o grupo de usuários é criado.

- **Selecionar domínio:** Na lista, selecione o domínio do qual escolher os usuários.
- **Incluir grupos de usuários:** Faça um dos seguintes:
  - Na lista de grupos de usuários, clique nos grupos que deseja adicionar. Os grupos selecionados aparecem na lista **Grupos de usuários selecionados**.
  - Clique em **Pesquisar** para ver uma lista de todos os grupos de usuários no domínio selecionado.
  - Digite um nome de grupo completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar a lista de grupos de usuários.

  Para remover um grupo de usuários da lista **Grupos de usuários selecionados**, faça o seguinte:

  - Na lista **Grupos de usuários selecionados**, clique no **X** ao lado de cada um dos grupos que deseja remover.

    - Clique em **Pesquisar** para ver uma lista de todos os grupos de usuários no domínio selecionado. Role a lista e desmarque a caixa de seleção de cada um dos grupos que deseja remover.
    - Digite um nome de grupo completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar a lista de grupos de usuários. Role a lista e desmarque a caixa de seleção de cada um dos grupos que deseja remover.

- **Ou/E:** Selecione se os usuários podem estar em qualquer grupo (Ou) ou se eles devem estar em todos os grupos (E) para que o recurso seja implantado para eles.
- **Implantar para usuário anônimo:** Selecione se deseja implantar para usuários não autenticados no grupo de entrega. Usuários não autenticados são usuários que você não conseguiu autenticar, mas permitiu que seus dispositivos se conectassem ao XenMobile de qualquer forma.

5. Configure as regras de implantação.
6. Clique em **Avançar**. A página **Recursos do Grupo de Entrega** é exibida. Opcionalmente, você pode adicionar políticas, aplicativos ou ações para o grupo de entrega aqui. Para pular esta etapa, em **Grupo de Entrega**, clique em **Resumo** para ver um resumo da configuração do grupo de entrega.

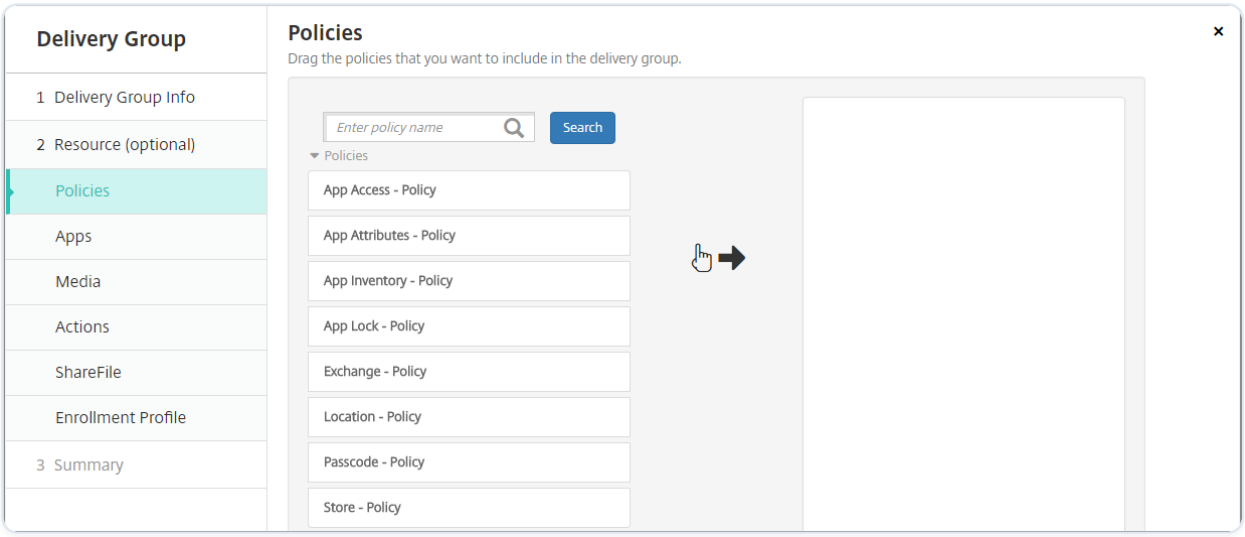
   Para pular um recurso, em **Recursos (opcional)**, clique no recurso que deseja adicionar e siga as etapas para esse recurso.

Para adicionar políticas

1. Para cada política que você deseja adicionar, faça o seguinte:

    - Role a lista de políticas disponíveis para encontrar a política que deseja adicionar.
    - Ou, para limitar a lista de políticas, digite um nome de política completo ou parcial na caixa de pesquisa e clique em **Pesquisar**.
    - Clique na política que você deseja adicionar e arraste-a para a caixa à direita.

   Para remover uma política, clique no **X** ao lado do nome da política na caixa à direita.



2. Clique em **Avançar**. A página **Aplicativos** é exibida.

Para adicionar aplicativos

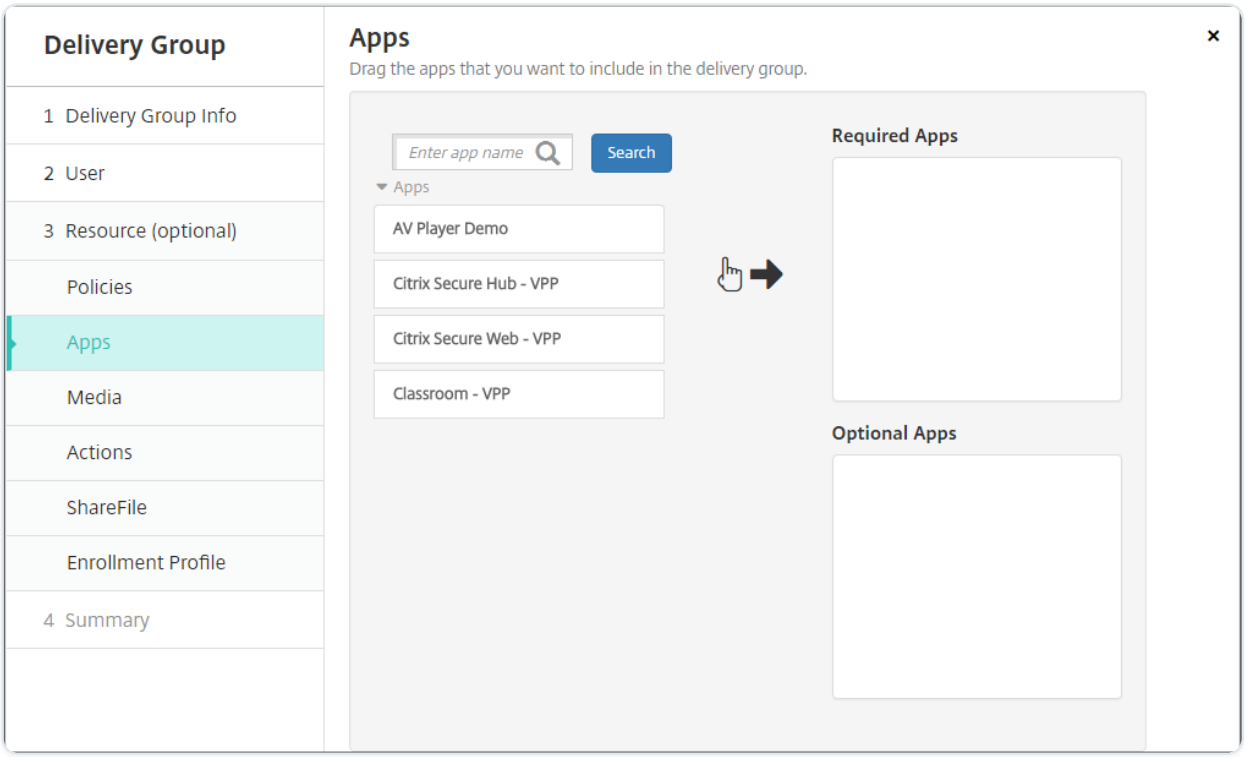
1. Para cada aplicativo que você deseja adicionar, faça o seguinte:

   - Role a lista de aplicativos disponíveis para encontrar o aplicativo que você deseja adicionar.
   - Ou, para limitar a lista de aplicativos, digite um nome de aplicativo completo ou parcial na caixa de pesquisa e clique em **Pesquisar**.
   - Clique no aplicativo que você deseja adicionar e arraste-o para a caixa **Aplicativos Obrigatórios** ou para a caixa **Aplicativos Opcionais**.

   Para aplicativos marcados como obrigatórios, os usuários podem receber atualizações prontamente em situações como:

   - Você carrega um novo aplicativo e o marca como obrigatório.
   - Você marca um aplicativo existente como obrigatório.
   - Quando um usuário exclui um aplicativo obrigatório.
   - Uma atualização do Secure Hub está disponível.

   Para obter informações sobre a implantação forçada de aplicativos obrigatórios, incluindo como habilitar o recurso, consulte Sobre aplicativos obrigatórios e opcionais.



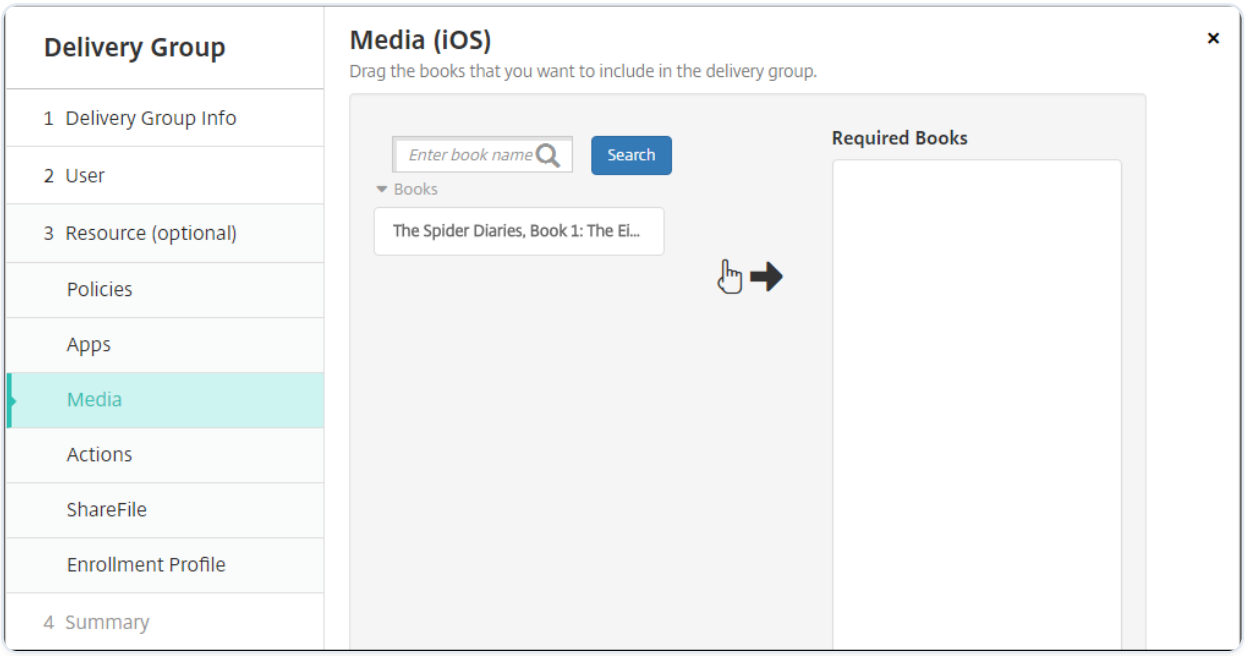
Para remover um aplicativo, clique no **X** ao lado do nome do aplicativo na caixa à direita.

2. Clique em **Avançar**. A página **Mídia** é exibida.

Para adicionar mídia

1. Para cada livro que você deseja adicionar, faça o seguinte:

    - Role a lista de livros disponíveis para encontrar o livro que você deseja adicionar.
    - Ou, para limitar a lista de livros, digite um nome de livro completo ou parcial na caixa de pesquisa e clique em **Pesquisar**.
    - Clique no livro que você deseja adicionar e arraste-o para a caixa **Livros Obrigatórios**.



Para livros marcados como obrigatórios, os usuários recebem atualizações prontamente em situações como:

- Você carrega um novo livro e o marca como obrigatório.
- Você marca um livro existente como obrigatório.
- Quando um usuário exclui um livro obrigatório.
- Uma atualização do Secure Hub está disponível.

Para remover um livro, clique no **X** ao lado do nome do livro na caixa à direita.

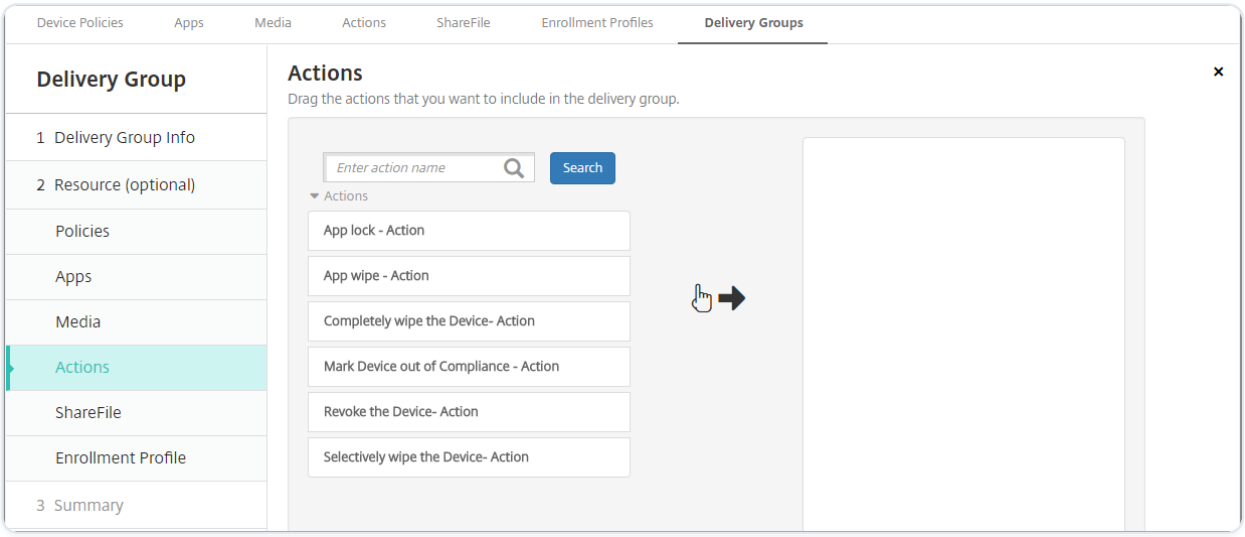
2. Clique em **Avançar**. A página **Ações** é exibida.

Para adicionar ações

1. Para cada ação que você deseja adicionar, faça o seguinte:

   - Role a lista de ações disponíveis para encontrar a ação que você deseja adicionar.
   - Ou, para limitar a lista de ações, digite um nome de ação completo ou parcial na caixa de pesquisa e clique em **Pesquisar**.
   - Clique na ação que você deseja adicionar e arraste-a para a caixa à direita.

   Para remover uma ação, clique no **X** ao lado do nome da ação na caixa à direita.

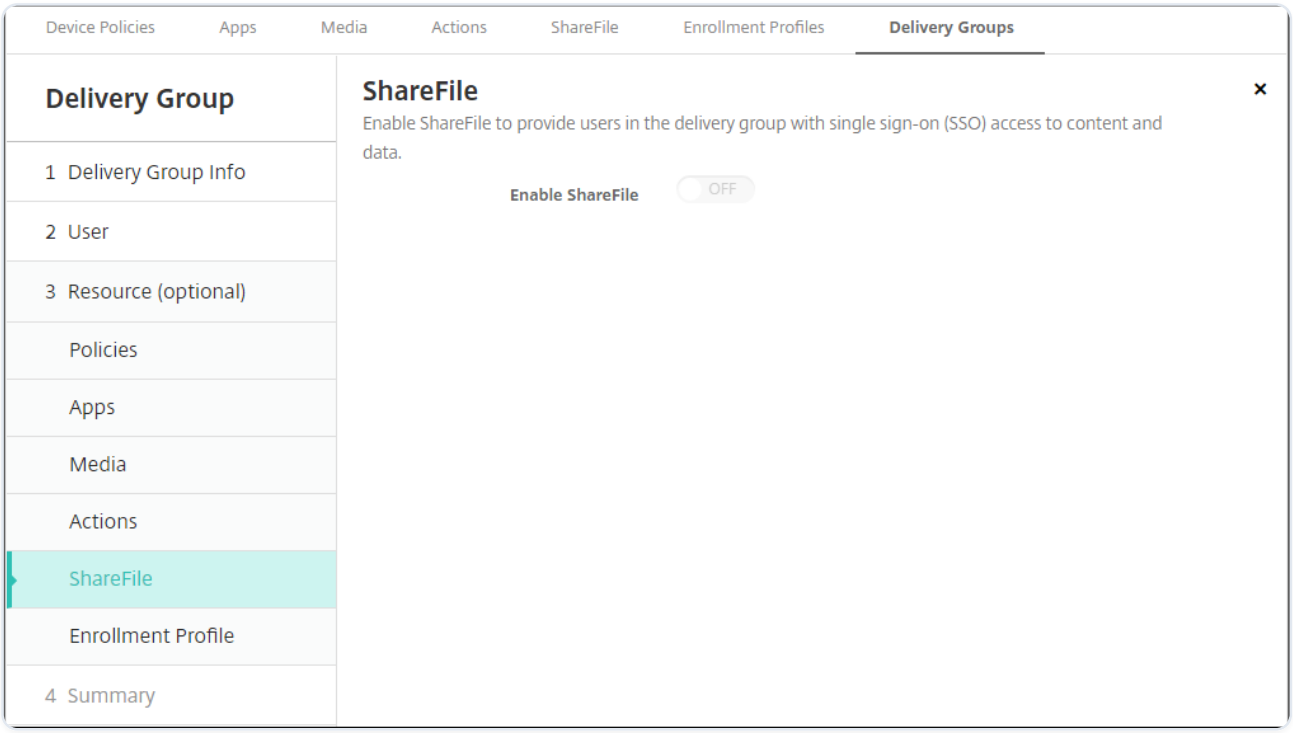


2. Clique em **Avançar**. A página **ShareFile** é exibida.

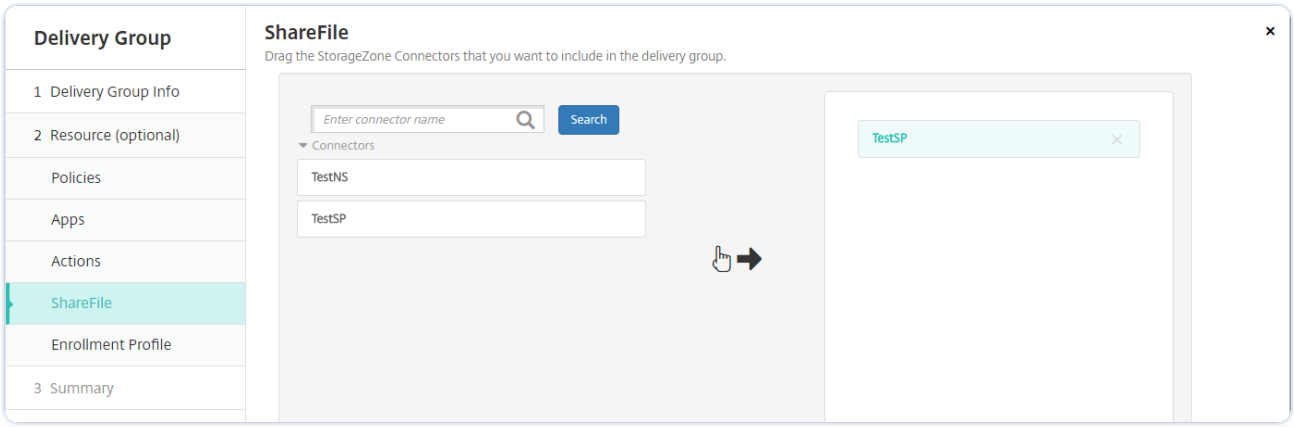
Para aplicar a configuração do ShareFile

A página ShareFile difere dependendo se você configurou o XenMobile (**Configurar > ShareFile**) para contas Enterprise ou para conectores de zona de armazenamento.

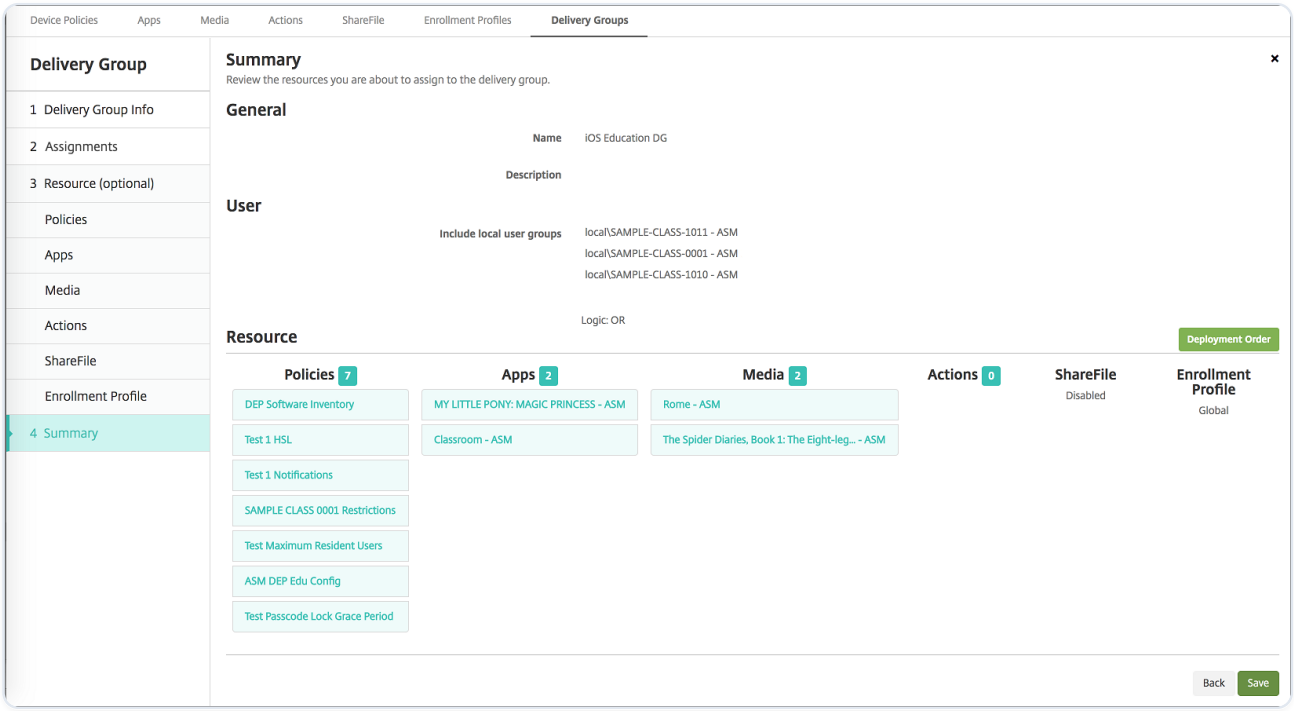
Se você configurou contas Enterprise para uso com o XenMobile: defina **Habilitar ShareFile** como **ATIVADO** para fornecer ao grupo de entrega acesso de logon único ao conteúdo e dados do ShareFile.



Se você configurou conectores de zona de armazenamento para uso com o XenMobile, selecione os conectores de zona de armazenamento a serem incluídos no grupo de entrega.

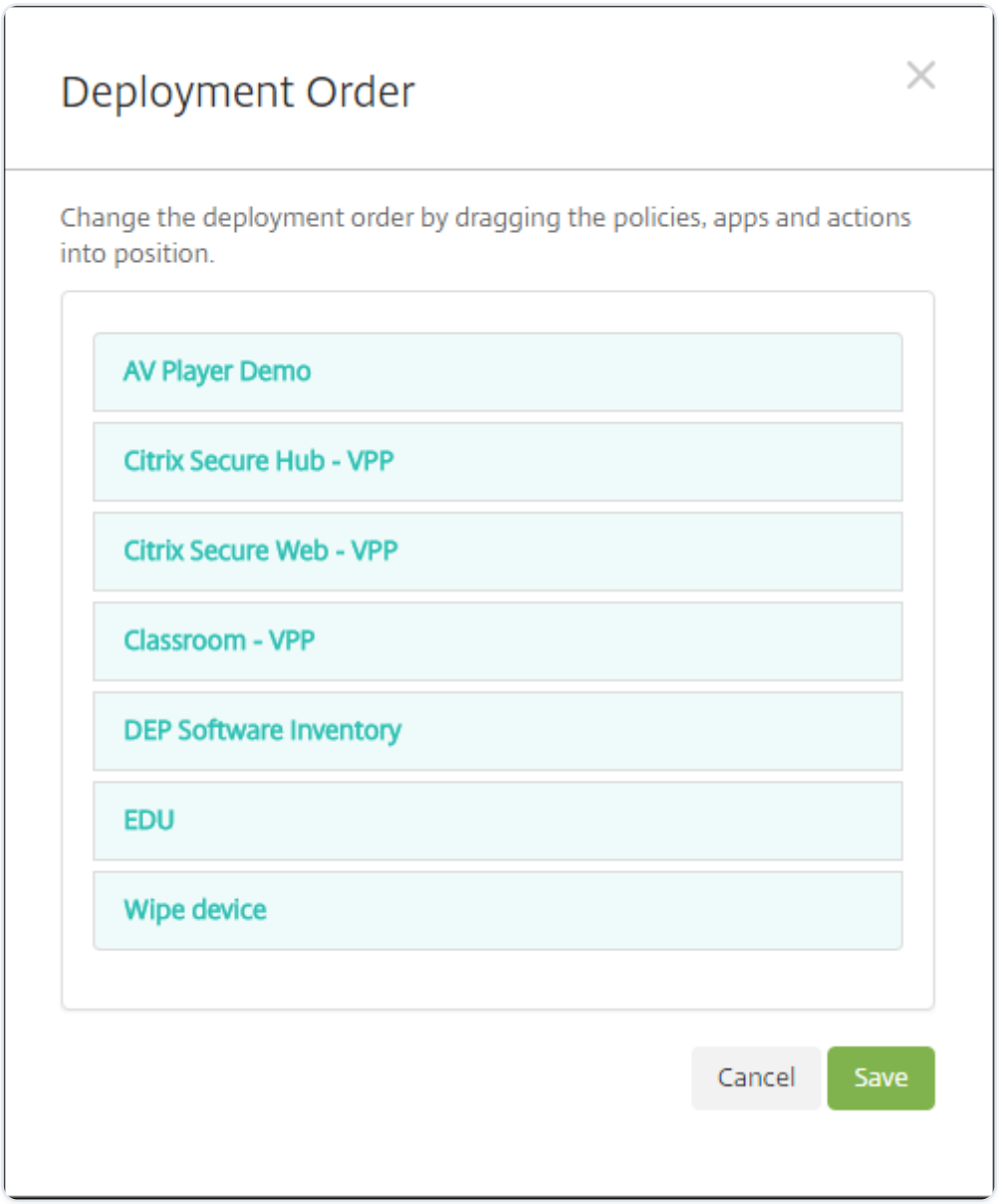


Para revisar as opções configuradas e alterar a ordem de implantação



Na página **Resumo**, você pode revisar as opções configuradas para o grupo de entrega e alterar a ordem de implantação dos recursos. A página Resumo mostra seus recursos por categoria. A página Resumo não reflete a ordem de implantação.

1. Clique em **Voltar** para retornar às páginas anteriores e fazer os ajustes necessários na configuração.
2. Clique em **Ordem de Implantação** para visualizar a ordem de implantação ou para reordená-la. A caixa de diálogo **Ordem de Implantação** é exibida.



3. Clique em um recurso e arraste-o para o local de onde você deseja que ele seja implantado. Depois de alterar a ordem de implantação, o XenMobile implanta os recursos na lista de cima para baixo.
4. Clique em **Salvar** para salvar a ordem de implantação.
5. Clique em **Salvar** para salvar o grupo de entrega.

Para editar um grupo de entrega

Você não pode alterar o nome de um grupo de entrega existente. Para atualizar outras configurações: Vá para **Configurar > Grupos de Entrega**, selecione o grupo que deseja editar e clique em **Editar**.

Para habilitar e desabilitar o grupo de entrega AllUsers

AllUsers é o único grupo de entrega que você pode habilitar ou desabilitar.

Na página **Grupos de Entrega**, escolha o grupo de entrega AllUsers selecionando a caixa de seleção ao lado de **AllUsers** ou clicando na linha que contém AllUsers. Em seguida, faça um dos seguintes:

- Clique em **Desativar** para desativar o grupo de entrega AllUsers. Este comando só está disponível se AllUsers estiver ativado (o padrão). **Desativado** aparece sob o cabeçalho **Desativado** na tabela de grupos de entrega.
- Clique em **Ativar** para ativar o grupo de entrega AllUsers. Este comando só está disponível se AllUsers estiver desativado. **Desativado** desaparece de debaixo do cabeçalho **Desativado** na tabela de grupos de entrega.

Para implantar em grupos de entrega

Implantar em um grupo de entrega significa enviar uma notificação push para todos os usuários com dispositivos tablet iOS e Windows. Esses usuários devem pertencer ao grupo de entrega para se reconectarem ao XenMobile. Dessa forma, você pode reavaliar os dispositivos e implantar aplicativos, políticas e ações.

Para usuários com dispositivos de outras plataformas: Se esses dispositivos já estiverem conectados ao XenMobile, eles receberão os recursos imediatamente. Caso contrário, com base em sua política de agendamento, eles receberão os recursos na próxima vez que se conectarem. Usuários na plataforma Android Enterprise recebem notificações do sistema de notificação Firebase Cloud Messaging e, em seguida, conectam-se ao XenMobile Server para recuperar recursos.

Para que os aplicativos atualizados apareçam na lista Disponíveis Atualizados na XenMobile Store em dispositivos Android: Primeiro, implante uma política de Inventário de Aplicativos nos dispositivos do usuário.

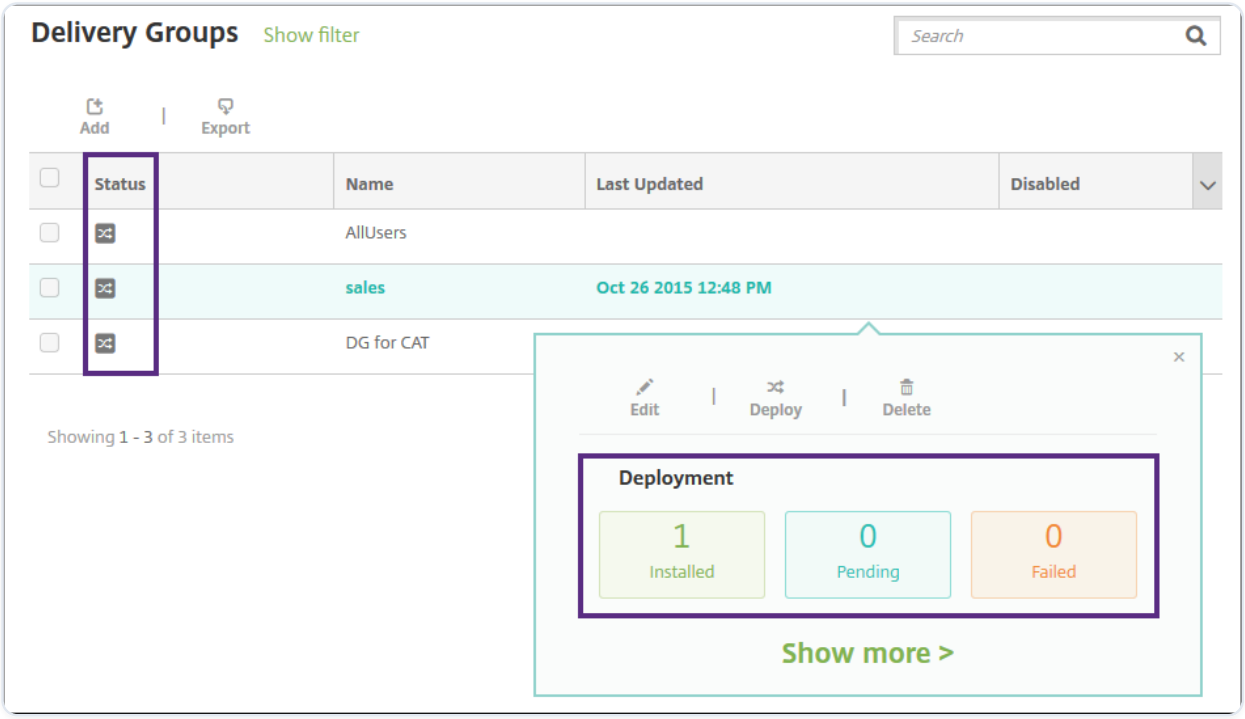
1. Na página **Grupos de Entrega**, faça uma das seguintes ações:
    - Para implantar em mais de um grupo de entrega por vez, selecione as caixas de seleção ao lado dos grupos que você deseja implantar.
    - Para implantar em um único grupo de entrega, selecione a caixa de seleção ao lado do nome ou clique na linha que contém o nome.
2. Clique em **Implantar**.

Dependendo de como você seleciona um único grupo de entrega, o comando **Implantar** aparece acima ou à direita do grupo de entrega.

Verifique se os grupos nos quais você deseja implantar aplicativos, políticas e ações estão listados e, em seguida, clique em **Implantar**. Os aplicativos, políticas e ações são implantados nos grupos selecionados com base na plataforma do dispositivo e na política de agendamento.

Você pode verificar o status da implantação na página **Grupos de Entrega** de uma destas maneiras:

- Observe o ícone de implantação sob o cabeçalho **Status** para o grupo de entrega, que indica qualquer falha de implantação.
- Clique na linha que contém o grupo de entrega para exibir uma sobreposição que indica implantações **Instaladas**, **Pendentes** e **Falhas**.



Para clonar um grupo de entrega

Clone um grupo de entrega quando quiser criar um grupo de entrega semelhante a um existente. Use o clone como ponto de partida para seu novo grupo de entrega. Em seguida, faça suas alterações no clone, como adicionar perfis de registro ou novos conjuntos de usuários do AD.

1. No console do XenMobile Server, clique em **Configurar** e, em seguida, selecione a guia **Grupos de Entrega**.

2. Na lista de grupos de entrega, selecione aquele que você deseja usar como base para o novo grupo.
3. Selecione **Clonar**.
4. Na caixa de diálogo **Clonar um Grupo de Entrega**, insira o nome do novo grupo e uma descrição (opcional).
5. Selecione **Clonar**.

Para excluir grupos de entrega

Você não pode excluir o grupo de entrega AllUsers, mas pode desativar o grupo quando não quiser enviar recursos para todos os usuários.

1. Na página **Grupos de Entrega**, faça uma das seguintes ações:
   - Para excluir mais de um grupo de entrega por vez, selecione as caixas de seleção ao lado dos grupos que deseja excluir.
   - Para excluir um único grupo de entrega, selecione a caixa de seleção ao lado do nome ou clique na linha que contém o nome.
2. Clique em **Excluir**. A caixa de diálogo **Excluir** é exibida.

   Dependendo de como você seleciona um único grupo de entrega, o comando **Excluir** aparece acima ou à direita do grupo de entrega.

   > **Importante:**
   >
   > Não é possível desfazer uma exclusão.

3. Clique em **Excluir**.

Para exportar a tabela Grupos de Entrega

1. Clique no botão **Exportar** acima da tabela **Grupos de Entrega**. O XenMobile extrai as informações da tabela **Grupos de Entrega** e as converte em um arquivo .csv.
2. Abra ou salve o arquivo .csv seguindo as etapas usuais do seu navegador. Você também pode cancelar a operação.

Macros

O XenMobile® fornece macros como uma forma de preencher dados de propriedades de usuário ou dispositivo no campo de texto dos seguintes itens:

- Políticas
- Notificações
- Modelos de registro
- Ações automatizadas
- Solicitações de assinatura de certificado do provedor de credenciais

O XenMobile substitui uma macro pelos valores de usuário ou sistema correspondentes. Por exemplo, você pode preencher previamente o valor da caixa de correio para um usuário em um único perfil do Exchange para milhares de usuários.

Sintaxe de macro

Uma macro pode ter a seguinte forma:

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

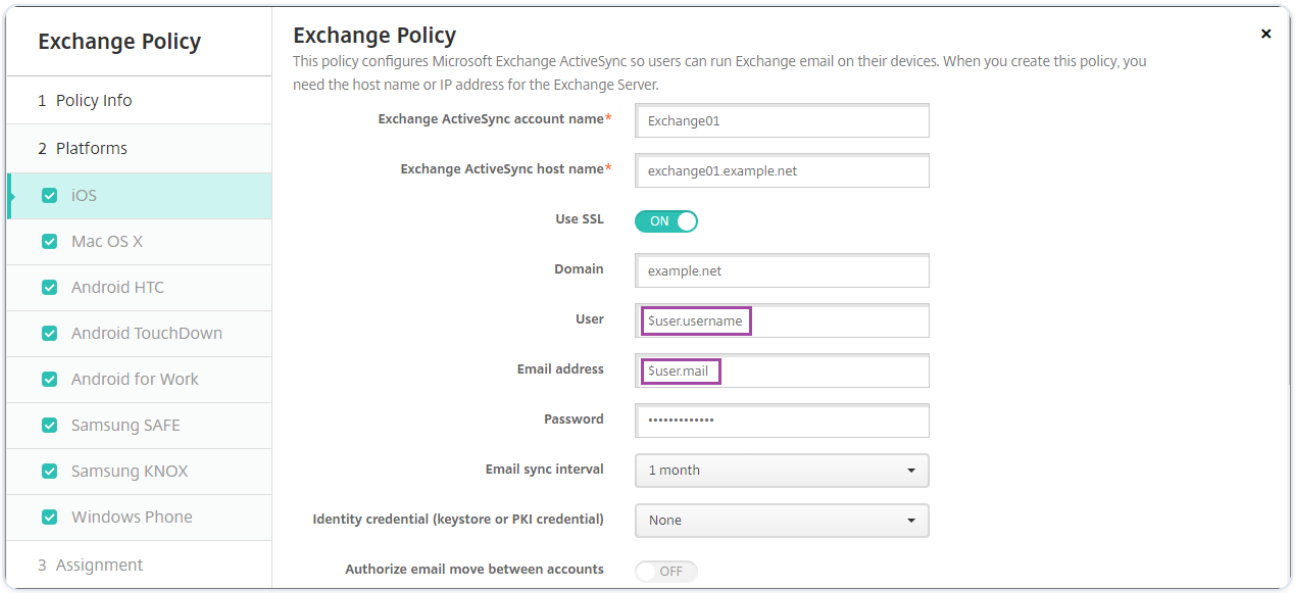
Inclua toda a sintaxe após o cifrão ($) entre chaves ({ }).

- Nomes de propriedade qualificados referenciam uma propriedade de usuário, uma propriedade de dispositivo ou uma propriedade personalizada.
- Nomes de propriedade qualificados consistem em um prefixo, seguido pelo nome real da propriedade.
- As propriedades do usuário assumem a forma `${user.[PROPERTYNAME] (prefix="user.")}`.
- As propriedades do dispositivo assumem a forma `${device.[PROPERTYNAME] (prefix="device.")}`.
- Os nomes das propriedades diferenciam maiúsculas de minúsculas.
- Uma função pode ser uma lista limitada ou um link para uma referência de terceiros que define funções. A macro a seguir para uma mensagem de notificação inclui a função **firstnotnull**.

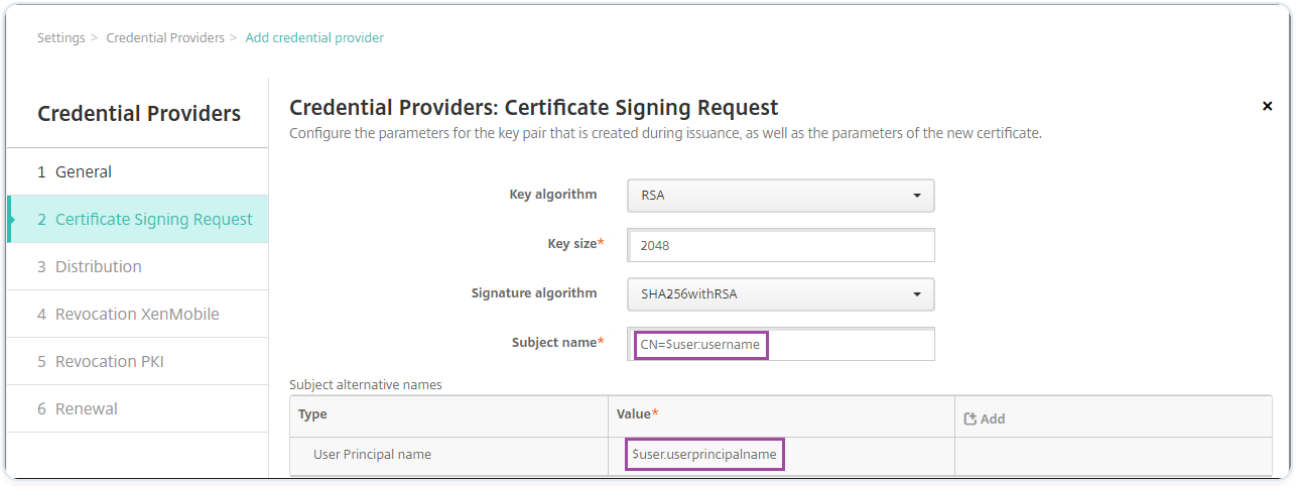
  Dispositivo `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` foi bloqueado…

- Para macros personalizadas (propriedades que você define), o prefixo é `${custom}`. Você pode omitir o prefixo.

Aqui está um exemplo de uma macro comumente usada `${user.username}` que preenche o valor do nome de usuário no campo de texto de uma política. Esta macro é útil para configurar perfis do Exchange ActiveSync e outros perfis usados por muitos usuários. O exemplo a seguir mostra como usar macros em uma política do Exchange. A macro para **Usuário** é **`${user.username}`**. A macro para **Endereço de e-mail** é **`${user.mail}`**.

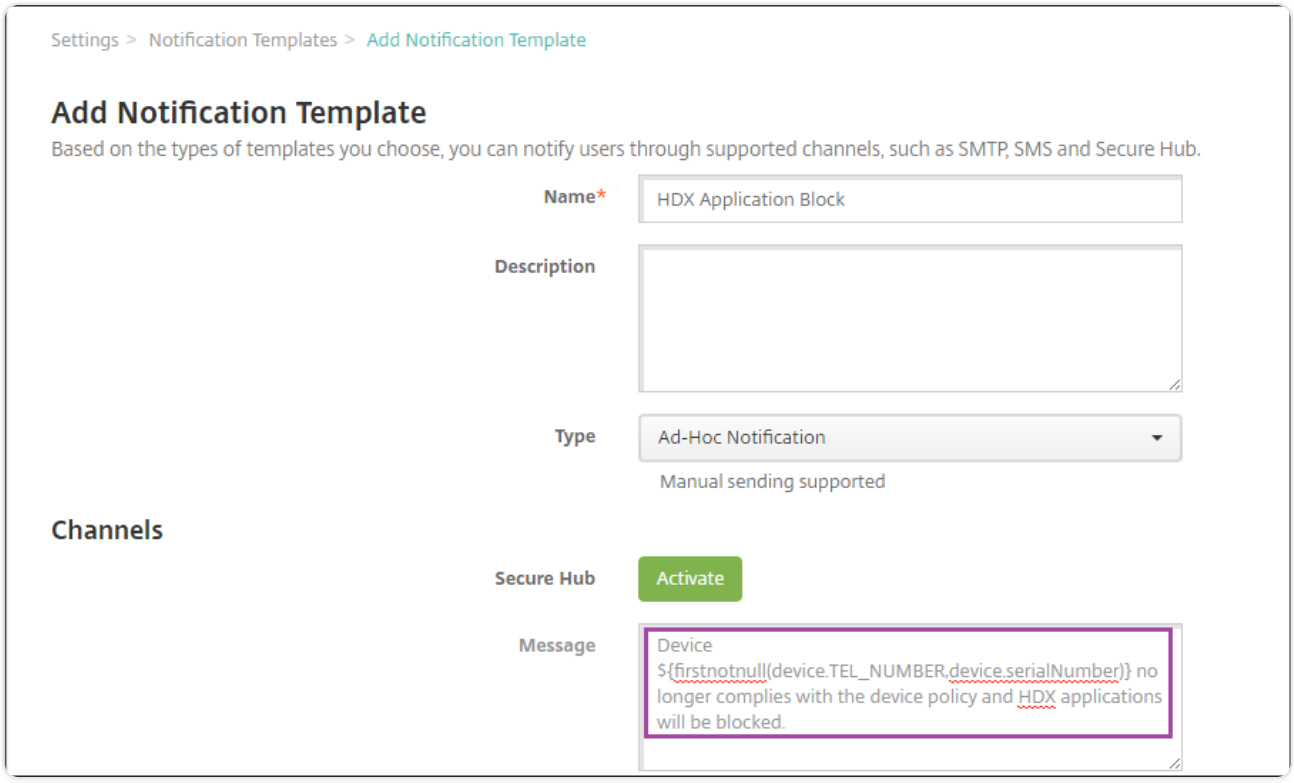


O exemplo a seguir mostra como usar macros para uma solicitação de assinatura de certificado. A macro para **Nome do assunto** é **`CN=$user.username`**. A macro para o **Valor** de um **Nome alternativo do assunto** é **`$user.userprincipalname`**.



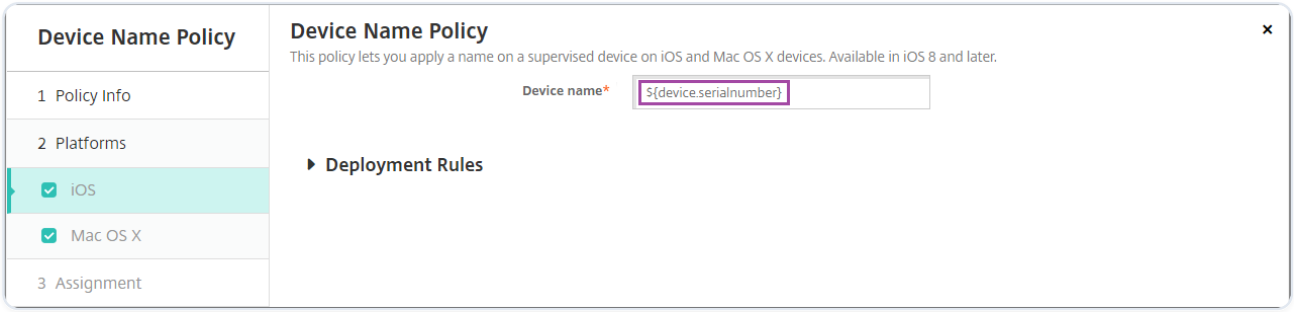
O exemplo a seguir mostra como usar macros em um modelo de notificação. O modelo de exemplo define a mensagem enviada a um usuário quando os aplicativos HDX™ são bloqueados devido a um dispositivo não compatível. A macro para a **Mensagem** é:

O dispositivo `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` não segue mais a política do dispositivo e os aplicativos HDX serão bloqueados.



Para mais exemplos de macros usadas em notificações, vá para **Configurações > Modelos de Notificação**, selecione um modelo predefinido e clique em **Editar**.

O exemplo a seguir mostra uma macro na política de dispositivo Nome do Dispositivo. Você pode digitar uma macro, uma combinação de macros ou uma combinação de macros e texto para nomear cada dispositivo de forma exclusiva. Por exemplo, use `${device.serialnumber}` para definir os nomes dos dispositivos como o número de série de cada dispositivo. Use `${device.serialnumber} ${ user.username }` para incluir o nome de usuário no nome do dispositivo. A política de dispositivo Nome do Dispositivo funciona em dispositivos iOS e macOS supervisionados.



Macros para modelos de notificação padrão

Você pode usar as seguintes macros nos modelos de notificação padrão:

- `${account.SUPPORT_EMAIL}`
- `${applicationName}`
- `${enrollment.andriod.agent.download.url}`
- `${enrollment.ios.agent.download.url}`
- `${enrollment.pin}`
- `${enrollment.url}`
- `${enrollment.urls}`
- `${enrollment.ios.url}`
- `${enrollment.macos.url}`
- `${enrollment.android.url}`
- `${enrollment.ios.platform}`
- `${enrollment.macos.platform}`
- `${enrollment.android.platform}`
- `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${outofcompliance.reason(smg_block)}`
- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`

> **Nota:**
>
> O console do XenMobile Server inclui os termos "lista negra" e "lista branca". Estamos alterando esses termos em uma próxima versão para "lista de bloqueio" e "lista de permissão".

- `${vpp.account}`
- `${vpp.appname}`
- `${vpp.url}`
- `${zdmserver.hostPath}/enroll`

Macros para políticas específicas

Para a política de dispositivo Nome do Dispositivo (para iOS e macOS), você pode usar estas macros para o **Nome do dispositivo**:

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`
- `${user.dnsroot}`

Para a política de dispositivo Webclip, você pode usar esta macro para a **URL**:

- `${webeas-url}`

Para a política de dispositivo Chave de Licença MDM Samsung, você pode usar esta macro para a **chave de licença ELM**:

- `${elm.license.key}`

Macros para obter propriedades de dispositivo integradas

NOME DE EXIBIÇÃO	MACROS
ID do Dispositivo	`$device.id`
GUID do Dispositivo	`$device.uniqueid`
IMEI do Dispositivo	`$device.imei`
Família do SO	`$device.OSFamily`
Número de Série	`$device.serialNumber`

Macros para todas as propriedades do dispositivo

A lista a seguir apresenta o nome de exibição, o elemento da Web e as Macros.

Conta Suspensa?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED}

Código de bypass de bloqueio de ativação

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE}

Bloqueio de ativação ativado

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED}

Conta iTunes ativa

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

Dispositivo ActiveSync conhecido pelo MSP

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP}

ID do ActiveSync

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID}

Administrador desativado

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED}

AIK Presente?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT}

API Amazon MDM disponível

- AMAZON_MDM
- ${device.AMAZON_MDM}

ID do Dispositivo Android Enterprise

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID}

Dispositivo Android Enterprise Habilitado?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE}

Tipo de Instalação do Android Enterprise

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE}

Status da Assinatura do Antispyware

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS}

Status do Antispyware

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS}

Status da Assinatura do Antivírus

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS}

Status do Antivírus

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS}

Código de bypass de bloqueio de ativação ASM DEP

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}

Chave de custódia DEP ASM

- DEP_ESCROW_KEY

- ${device.DEP_ESCROW_KEY}

Etiqueta de ativo

- ASSET_TAG
- ${device.ASSET_TAG}

Verificar automaticamente atualizações de software

- AutoCheckEnabled
- ${device.AutoCheckEnabled}

Baixar automaticamente atualizações de software em segundo plano

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled}

Instalar automaticamente atualizações de aplicativos

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled}

Instalar automaticamente atualizações do SO

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled}

Instalar automaticamente atualizações de segurança

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled}

Status da atualização automática

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS}

RAM disponível

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE}

Atualizações de software disponíveis

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}

Espaço de armazenamento disponível

- FREEDISK
- ${device.FREEDISK}

Bateria de backup

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT}

Versão do firmware da banda base

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION}

Carregamento da bateria

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS}

Carregamento da bateria

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING}

Bateria Restante

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING}

Duração da Bateria

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME}

Status da Bateria

- BATTERY_STATUS
- ${device.BATTERY_STATUS}

Dispositivo Bes conhecido por MS

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP}

PIN BES

- BES_PIN
- ${device.BES_PIN}

ID do agente do servidor BES

- AGENT_ID
- ${device.AGENT_ID}

Nome do servidor BES

- BES_SERVER
- ${device.BES_SERVER}

Versão do servidor BES

- BES_VERSION
- ${device.BES_VERSION}

Informações do BIOS

- BIOS_INFO
- ${device.BIOS_INFO}

Status do BitLocker

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS}

Endereço MAC Bluetooth

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC}

Depuração de Inicialização Ativada?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}

Versão da Lista de Revisão do Gerenciador de Inicialização

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}

Código da Operadora

- CARRIER_CODE
- ${device.CARRIER_CODE}

Versão das configurações da operadora

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION}

URL do Catálogo

- CatalogURL
- ${device.CatalogURL}

Altitude celular

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR}

Curso celular

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR}

Precisão horizontal celular

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}

Latitude celular

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR}

Longitude celular

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR}

Velocidade celular

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR}

Tecnologia celular

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY}

Carimbo de data/hora celular

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR}

Precisão vertical celular

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

Alterar Senha no Próximo Login?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

ID do dispositivo cliente

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID}

Backup em nuvem ativado

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED}

Integridade do Código Ativada?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}

Versão da Lista de Revogação de Integridade do Código

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}

Cor

- COLOR
- ${device.COLOR}

Velocidade do clock da CPU

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED}

Tipo de CPU

- CPU_TYPE
- ${device.CPU_TYPE}

Hora de Criação

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}

Atualizações de software críticas

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}

Rede da operadora atual

- CARRIER
- ${device.CARRIER}

Código de país móvel atual

- CURRENT_MCC
- ${device.CURRENT_MCC}

Código de rede móvel atual

- CURRENT_MNC

- ${device.CURRENT_MNC}

Roaming de dados permitido

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED}

Data do último backup do iCloud

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

Catálogo padrão

- IsDefaultCatalog
- ${device.IsDefaultCatalog}

Nome da conta DEP

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}

Política DEP

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY}

Perfil DEP atribuído

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME}

Perfil DEP enviado

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME}

Perfil DEP removido

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME}

Registro DEP por

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY}

Data de registro DEP

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE}

Descrição

- DESCRIPTION
- ${device.DESCRIPTION}

Identificador do dispositivo

- Activesyncid
- ${device.activesyncid}

Modelo do dispositivo

- SYSTEM_OEM
- ${device.SYSTEM_OEM}

Nome do dispositivo

- DEVICE_NAME
- ${device.DEVICE_NAME}

Tipo de dispositivo

- DEVICE_TYPE
- ${device.DEVICE_TYPE}

Não Perturbe ativado

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB}

Driver ELAM Carregado?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}

Conformidade de Criptografia

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE}

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE}

ID da Empresa

- ENTERPRISEID
- ${device.ENTERPRISEID}

Armazenamento externo 1: espaço disponível

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE}

Armazenamento externo 1: nome

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME}

Armazenamento externo 1: espaço total

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE}

Armazenamento externo 2: espaço disponível

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE}

Armazenamento externo 2: nome

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME}

Armazenamento externo 2: espaço total

- EXTERNAL_STORAGE2_TOTAL_SPACE

- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

Armazenamento externo criptografado

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION}

FileVault Ativado

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED}

Status do Firewall

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS}

Status do Firewall

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS}

Versão do firmware

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION}

Primeira sincronização

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC}

Alias do Diretório Google

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Sobrenome do Diretório Google

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Nome do Diretório Google

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

E-mail Principal do Diretório Google

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

ID de Usuário do Diretório Google

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

Altitude GPS

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS}

Curso GPS

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS}

Precisão horizontal do GPS

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}

Latitude GPS

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS}

Longitude GPS

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS}

Velocidade do GPS

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS}

Carimbo de data/hora do GPS

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS}

Precisão vertical do GPS

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS}

ID do Dispositivo de Hardware

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID}

Recursos de criptografia de hardware

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS}

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER}

Hash da conta da iTunes Store atualmente conectada

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH}

Rede da operadora de origem

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK}

Código de país móvel de origem

- SIM_MCC
- ${device.SIM_MCC}

Código de rede móvel de origem

- SIM_MNC

- ${device.SIM_MNC}

ICCID

- ICCID
- ${device.ICCID}

Identidade

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY}

Número IMEI/MEID

- IMEI
- ${device.IMEI}

IMSI

- SIM_ID
- ${device.SIM_ID}

Armazenamento interno criptografado

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION}

Localização IP

- IP_LOCATION
- ${device.IP_LOCATION}

Endereço IPV4

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4}

Endereço IPV6

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6}

Emitido Em

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT}

Com Jailbreak/Root

- ROOT_ACCESS
- ${device.ROOT_ACCESS}

Depuração de Kernel Ativada?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}

Modo quiosque

- IS_KIOSK
- ${device.IS_KIOSK}

Último endereço IP conhecido

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR}

Hora da última atualização da política

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME}

Data da última verificação

- PreviousScanDate
- ${device.PreviousScanDate}

Último resultado da verificação

- PreviousScanResult
- ${device.PreviousScanResult}

Últimas atualizações de software agendadas

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

Mensagem de falha das últimas atualizações de software agendadas

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

Status das últimas atualizações de software agendadas

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

Última sincronização

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC}

Serviço de localização ativado

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR}

Endereço MAC

- MAC_ADDRESS
- ${device.MAC_ADDRESS}

Conexão de Rede do Endereço MAC

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION}

Tipo de Endereço MAC

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE}

Configuração de Caixa de Correio

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}

Bateria principal

- MAIN_BATTERY_PERCENT

- ${device.MAIN_BATTERY_PERCENT}

Modo perdido do MDM ativado

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED}

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY}

MEID

- MEID
- ${device.MEID}

Número de telefone celular

- TEL_NUMBER
- ${device.TEL_NUMBER}

ID do Modelo

- MODEL_ID
- ${device.MODEL_ID}

Número do Modelo

- MODEL_NUMBER
- ${device.MODEL_NUMBER}

Tipo de Adaptador de Rede

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE}

Compilação do sistema operacional

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD}

Edição do Sistema Operacional

- OS_EDITION
- ${device.OS_EDITION}

Idioma do sistema operacional (localidade)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE}

Versão do sistema operacional

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION}

Endereço da organização

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS}

E-mail da organização

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL}

Magia da organização

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC}

Nome da organização

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME}

Número de telefone da organização

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE}

Fora de conformidade

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE}

Propriedade de

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED}

Senha em conformidade

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT}

Senha compatível com a configuração

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

Senha presente

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0}

Violação de perímetro

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH}

Verificação periódica

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck}

Ponto de Acesso Pessoal ativado

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED}

Código PIN para geocerca

- PIN_CODE_FOR_GEO_FENCE

- ${device.PIN_CODE_FOR_GEO_FENCE}

Plataforma

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

Nível da API da plataforma

- API_LEVEL
- ${device.API_LEVEL}

Nome da política

- POLICY_NAME
- ${device.POLICY_NAME}

Número de Telefone Principal

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER}

Operadora da SIM Principal

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

ICCID da SIM Principal

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID}

IMEI da SIM Principal

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI}

IMSI da SIM Principal

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI}

Roaming do SIM Primário

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING}

Conformidade de Roaming do SIM Primário

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE}

Nome do produto

- PRODUCT_NAME
- ${device.PRODUCT_NAME}

ID do Dispositivo do Editor

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID}

Contagem de Redefinições

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT}

Contagem de Reinicializações

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT}

Modo de Segurança Ativado?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE}

API Samsung KNOX disponível

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX}

Versão da API Samsung KNOX

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION}

Atestado Samsung KNOX

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED}

Data de atualização da atestação Samsung KNOX

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}

API Samsung SAFE disponível

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM}

Versão da API Samsung SAFE

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION}

Hash SBCP

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH}

Tela: altura

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT}

Tela: número de cores

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS}

Tela: tamanho

- SCREEN_SIZE
- ${device.SCREEN_SIZE}

Tela: largura

- SCREEN_WIDTH

- ${device.SCREEN_WIDTH}

Tela: resolução do eixo X

- SCREEN_XDPI
- ${device.SCREEN_XDPI}

Tela: resolução do eixo Y

- SCREEN_YDPI
- ${device.SCREEN_YDPI}

Número de Telefone Secundário

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER}

Operadora da SIM Secundária

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}

ICCID da SIM Secundária

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID}

IMEI da SIM Secundária

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI}

IMSI da SIM Secundária

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI}

Roaming do SIM Secundário

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING}

Conformidade de Roaming do SIM Secundário

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE}

Inicialização Segura Ativada?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}

Status da Inicialização Segura

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE}

SecureContainer Ativado

- DLP_ACTIVE
- ${device.DLP_ACTIVE}

Nível do patch de segurança

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL}

Número de série

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER}

Capaz de SMS

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE}

Supervisionado

- SUPERVISED
- ${device.SUPERVISED}

Motivo da Suspensão

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}

Status de Adulteração

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS}

Termos e Condições

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS}

Termos e Acordo Aceitos?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

Assinatura de Teste Habilitada?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

RAM Total

- MEMORY
- ${device.MEMORY}

Espaço total de armazenamento

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE}

Versão do TPM

- TPM_VERSION
- ${device.TPM_VERSION}

UDID

- UDID
- ${device.UDID}

Status do Controle de Conta de Usuário

- UAC_STATUS

- ${device.UAC_STATUS}

Agente de usuário

- USER_AGENT
- ${device.USER_AGENT}

Definido pelo usuário #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1}

Definido pelo usuário #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2}

Definido pelo usuário #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3}

Idioma do usuário (localidade)

- USER_LANGUAGE
- ${device.USER_LANGUAGE}

Fornecedor

- VENDOR
- ${device.VENDOR}

Capaz de voz

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE}

Roaming de voz permitido

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED}

VSM Ativado?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED}

Endereço MAC do WiFi

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY}

WinPE Ativado?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE}

Status de Notificação WNS

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS}

URL de Notificação WNS

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL}

Data de expiração da URL de Notificação WNS

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY}

ID do agente XenMobile

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID}

Revisão do agente XenMobile

- EW_REVISION
- ${device.EW_REVISION}

Versão do agente XenMobile

- EW_VERSION
- ${device.EW_VERSION}

API Zebra disponível

- ZEBRA_MDM
- ${device.ZEBRA_MDM}

Versão do Zebra MXMF

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION}

Versão do Patch Zebra

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Macros para obter propriedades de usuário integradas

NOME DE EXIBIÇÃO	MACROS
domainname (nome de domínio; domínio padrão)	`${user.domainname}`
loginname (nome de usuário mais nome de domínio)	`${user.loginname}`
username (nome de login menos o domínio, se houver)	`${user.username}`

Macros para todas as propriedades de usuário

NOME DE EXIBIÇÃO	ELEMENTO WEB	MACROS
Tentativas de logon com falha do Active Directory	erros_senha	`${user.badpwdcount}`
E-mail do usuário do ActiveSync	como e-mail do usuário	`${user.asuseremail}`

NOME DE EXIBIÇÃO	ELEMENTO WEB	MACROS
Fonte de dados ASM	como origem da pessoa	`${user.aspersonsource}`
Nome da conta DEP do ASM	como conta DEP	`${user.asmdepaccount}`
Apple ID gerenciado pelo ASM	como Apple ID gerenciado da pessoa	`${user.aspersonmanagedappleid}`
Tipo de senha do ASM	como tipo de senha da pessoa	`${user.aspersonpasscodetype}`
ID da pessoa ASM	ID da pessoa ASM	`${user.aspersonid}`
Status da pessoa ASM	Status da pessoa ASM	`${user.aspersonstatus}`
Título da pessoa ASM	Título da pessoa ASM	`${user.aspersontitle}`
ID exclusivo da pessoa ASM	ID exclusivo da pessoa ASM	`${user.aspersonuniqueid}`
ID do sistema de origem ASM	ID do sistema de origem da pessoa ASM	`${user.aspersonsourcesystemid}`
Nota do aluno ASM	grau da pessoa asm	`${user.aspersongrade}`
E-mail do usuário BES	e-mail do usuário bes	`${user.besuseremail}`
Empresa	empresa	`${user.company}`
Nome da empresa	nome da empresa	`${user.companyname}`
País	c	`${user.c}`
Departamento	departamento	`${user.department}`
Descrição	descrição	`${user.description}`
Usuário desabilitado	usuáriodesabilitado	`${user.disableduser}`

NOME DE EXIBIÇÃO	ELEMENTO WEB	MACROS
Nome de exibição	nomedeexibição	`${user.displayname}`
Nome diferenciado	nomediferenciado	`${user.distinguishedname}`
Nome de domínio	nome de domínio	`${user.domainname}`
E-mail	e-mail	`${user.mail}`
Primeiro nome	primeiro nome	`${user.givenname}`
Endereço residencial	endereço residencial	`${user.homestreetaddress}`
Cidade residencial	cidade residencial	`${user.homecity}`
País de origem	país de residência	`${user.homecountry}`
Fax residencial	fax residencial	`${user.homefax}`
Telefone residencial	telefone residencial	`${user.homephone}`
Estado/região de origem	estado de residência	`${user.homestate}`
CEP ou código postal residencial	CEP residencial	`${user.homezip}`
Telefone IP	telefone IP	`${user.ipphone}`
Inicial do meio	inicial do meio	`${user.middleinitial}`
Nome do meio	nome do meio	`${user.middlename}`
Celular	celular	`${user.mobile}`
Nome	cn	`${user.cn}`
Endereço do escritório	nome do escritório de entrega física	`${user.physicaldeliveryofficename}`

NOME DE EXIBIÇÃO	ELEMENTO WEB	MACROS
Cidade do escritório	l	`${user.l}`
Número de fax do escritório	número de fax	`${user.facsimiletelephonenumber}`
Estado/província do escritório	st	`${user.st}`
Endereço da rua do escritório	endereço do escritório	`${user.officestreetaddress}`
Número de telefone do escritório	número de telefone	`${user.telephonenumber}`
CEP ou código postal do escritório	código postal	`${user.postalcode}`
Caixa postal	caixa postal	`${user.postofficebox}`
Pager	Número de pager	`${user.pager}`
ID do grupo principal	ID do grupo primário	`${user.primarygroupid}`
Conta SAM	Nome da conta SAM	`${user.samaccountname}`
Endereço	Endereço	`${user.streetaddress}`
Sobrenome	sn	`${user.sn}`
Título	Título	`${user.title}`
Nome de logon do usuário	Nome principal do usuário	`${user.userprincipalname}`

Ações automatizadas

Você cria ações automatizadas no XenMobile® para programar uma reação a eventos, propriedades de usuário ou dispositivo, ou à existência de aplicativos em dispositivos de usuário. Ao criar uma ação automatizada, os gatilhos definidos para a ação determinam o que acontece no dispositivo do usuário quando ele está conectado ao XenMobile. Quando um evento é acionado, você pode enviar uma notificação ao usuário para corrigir um problema antes que uma ação mais séria seja tomada.

Os efeitos que você define para acontecer automaticamente variam do seguinte:

- Limpar o dispositivo total ou seletivamente.
- Definir o dispositivo como não conforme.
- Revogar o dispositivo.
- Enviar uma notificação ao usuário para corrigir um problema antes que uma ação mais severa seja tomada.

Você pode configurar ações de bloqueio de aplicativo e limpeza de aplicativo para o modo somente MAM.

> **Nota:**
>
> Antes de poder notificar os usuários, você deve configurar os servidores de notificação nas configurações do XenMobile para SMTP e SMS para que o XenMobile possa enviar as mensagens. Para obter informações, consulte Notificações. Além disso, configure quaisquer modelos de notificação que você planeja usar antes de prosseguir. Para obter detalhes, consulte Criar e atualizar modelos de notificação.

Exemplos de ações

Aqui estão alguns exemplos de uso de ações automatizadas:

Exemplo um

- Você deseja detectar um aplicativo que bloqueou anteriormente (por exemplo, “Words with Friends”). Você pode especificar um gatilho que define o dispositivo do usuário como não conforme após detectar o aplicativo “Words with Friends”. Ação então notifica os usuários de que eles devem remover o aplicativo para que o dispositivo volte a estar em conformidade. Você também pode definir um limite de tempo para quanto tempo esperar que os usuários cumpram. Após esse limite de tempo, uma ação definida ocorre, como a limpeza seletiva do dispositivo.

Exemplo dois

- Você deseja verificar se os clientes estão usando o firmware mais recente e bloquear o acesso aos recursos se os usuários precisarem atualizar seus dispositivos. Você pode especificar um gatilho que define o dispositivo do usuário como fora de conformidade quando um dispositivo do usuário não tem a versão mais recente. Você usa ações automatizadas para bloquear recursos e notificar os clientes.

Exemplo três

- Um dispositivo de usuário é colocado em um estado de não conformidade e o usuário então corrige o dispositivo. Você pode configurar uma política para implantar um pacote que redefine o dispositivo para um estado de conformidade.

Exemplo quatro

- Você deseja marcar dispositivos de usuário que estiveram inativos por um determinado período como fora de conformidade. Você pode criar uma ação automatizada para dispositivos inativos da seguinte forma:

  a. No console do XenMobile, vá para **Configurações > Controle de Acesso à Rede** e selecione **Dispositivos Inativos**. Para obter mais informações sobre a configuração **Dispositivos Inativos**, consulte Controle de Acesso à Rede.

  b. Siga as etapas para adicionar uma ação, conforme descrito em Adicionar e gerenciar ações. A única diferença é que você configura as configurações da seguinte forma na página **Detalhes da ação**:

     - **Gatilho**. Selecione **Propriedade do dispositivo**, **Fora de conformidade** e **Verdadeiro**.
     - **Ação**. Selecione **Enviar notificação** e selecione um modelo que você criou usando **Modelo de Notificação** em **Configurações**. Em seguida, defina o atraso em dias,

horas ou minutos antes de executar a ação. Defina o intervalo em que a ação se repete até que o usuário resolva o problema que a acionou.

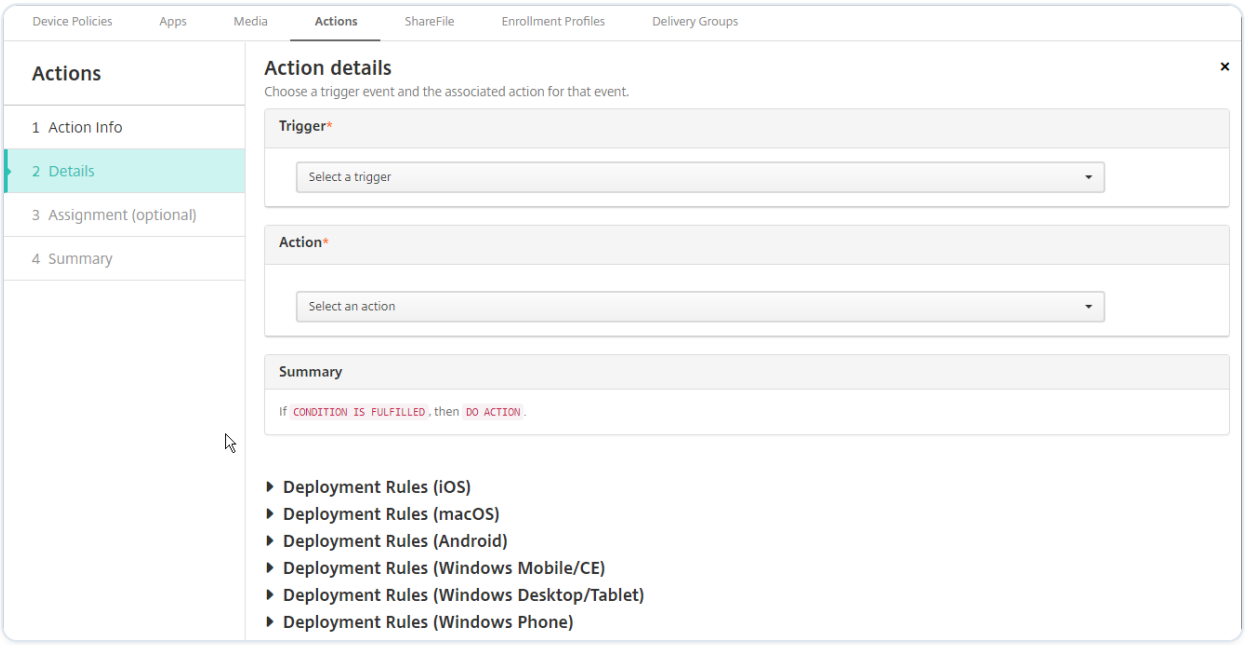
> **Dica:**
>
> Para excluir dispositivos inativos em massa, use a API Pública para Serviços REST. Primeiro, você obtém manualmente os IDs dos dispositivos inativos que deseja excluir e, em seguida, executa a API de exclusão para excluí-los em massa.

Adicionar e gerenciar ações

Para adicionar, editar e filtrar ações automatizadas:

1. No console do XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Na página **Ações**, faça um dos seguintes:
   - Clique em **Adicionar** para adicionar uma ação.
   - Selecione uma ação existente para editar ou excluir. Clique na opção que você deseja usar.
3. A página **Informações da Ação** é exibida.
4. Na página **Informações da Ação**, insira ou modifique as seguintes informações:
   - **Nome:** Digite um nome para identificar a ação. Este campo é obrigatório.
   - **Descrição:** Descreva o que a ação deve fazer.
5. Clique em **Avançar**. A página **Detalhes da ação** é exibida.

   O exemplo a seguir mostra como configurar um gatilho de **Evento**. Se você selecionar um gatilho diferente, as opções resultantes serão diferentes das mostradas aqui.



6. Na página **Detalhes da ação**, insira ou modifique as seguintes informações:

   Na lista **Gatilho**, clique no tipo de gatilho de evento para esta ação. O significado de cada gatilho é o seguinte:

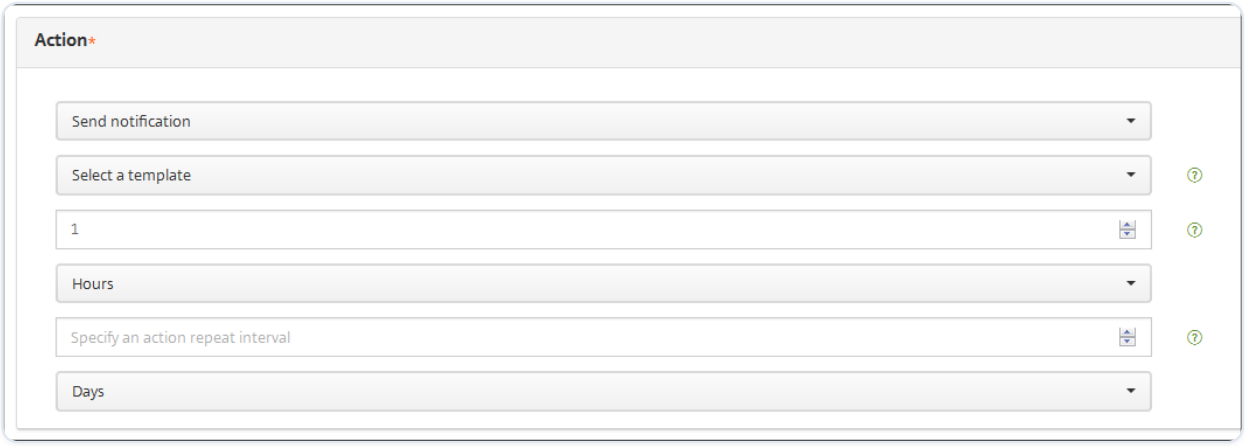
   - **Evento:** Reage a um evento predefinido.
   - **Propriedade do dispositivo:** Verifica um atributo do dispositivo em um dispositivo gerenciado por MDM e, em seguida, reage a ele. Para obter mais informações, consulte Nomes e valores de propriedades do dispositivo.
   - **Propriedade do usuário:** Reage a um atributo do usuário, geralmente do Active Directory.
   - **Nome do aplicativo instalado:** Reage à instalação de um aplicativo. Não se aplica ao modo somente MAM. Requer que a política de inventário de aplicativos esteja habilitada no dispositivo. A política de inventário de aplicativos é habilitada em todas as plataformas por padrão. Para obter detalhes, consulte Política de dispositivo de inventário de aplicativos.

7. Na próxima lista, clique na resposta ao gatilho.
8. Na lista **Ação**, clique na ação a ser executada quando o critério do gatilho for atendido. Exceto para **Enviar notificação**, você escolhe um período no qual os usuários podem resolver o problema que causou o gatilho. Se o problema não for resolvido dentro desse período, a ação selecionada será tomada. Para uma definição das ações, consulte Ações de segurança.

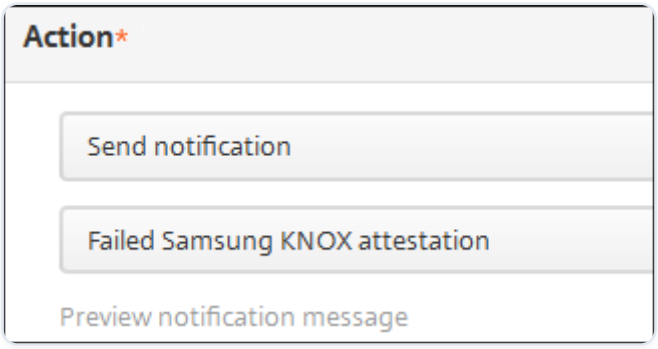
   Se você escolher **Enviar notificação**, use as seguintes etapas para enviar uma ação de notificação.
9. Na próxima lista, selecione o modelo a ser usado para a notificação. Os modelos de notificação relevantes para o evento selecionado aparecem, a menos que um modelo ainda

não exista para o tipo de notificação. Nesse caso, você será solicitado a configurar um modelo com a mensagem: Nenhum modelo para este tipo de evento. Crie um modelo usando **Modelo de Notificação** em **Configurações**.

Antes de poder notificar os usuários, você deve ter configurado servidores de notificação nas Configurações para SMTP e SMS para que o XenMobile possa enviar as mensagens, consulte Notificações. Além disso, configure quaisquer modelos de notificação que você planeja usar antes de prosseguir. Para obter detalhes sobre como configurar modelos de notificação, consulte Criar e atualizar modelos de notificação.



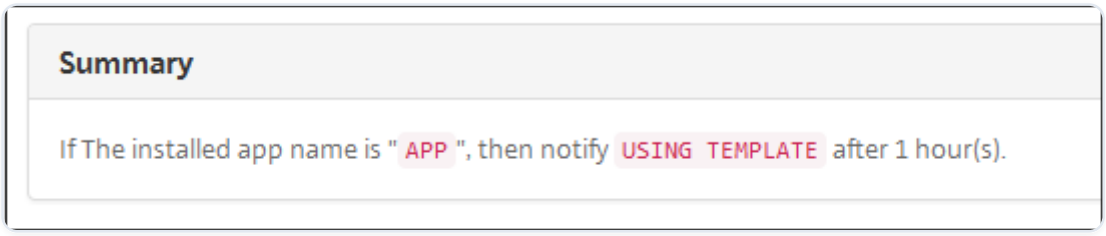
Depois de selecionar o modelo, você pode visualizar a notificação clicando em **Visualizar mensagem de notificação**.



10. Nos campos a seguir, defina o atraso em dias, horas ou minutos antes de executar a ação. Defina o intervalo no qual a ação se repete até que o usuário resolva o problema que a acionou.



11. Em **Resumo**, verifique se você criou a ação automatizada conforme o pretendido.



12. Depois de configurar os detalhes da ação, você pode configurar as regras de implantação para cada plataforma individualmente. Para fazer isso, conclua a etapa 13 para cada plataforma que você escolher.
13. Configure as regras de implantação. Para obter informações gerais sobre como configurar regras de implantação, consulte Implantar recursos.

    Para este exemplo:

    - A propriedade do dispositivo deve ser **BYOD**.
    - A criptografia local do dispositivo deve ser **Verdadeiro**.
    - O dispositivo deve estar em conformidade com o código de acesso.
    - O código de país móvel do dispositivo não pode ser apenas Andorra.

14. Quando terminar de configurar as regras de implantação da plataforma para a ação, clique em **Avançar**. A página **Atribuição de ações** é exibida, onde você atribui a ação a um ou mais grupos de entrega. Esta etapa é opcional.
15. Ao lado de **Escolher grupos de entrega**, digite para encontrar um grupo de entrega ou selecione grupos na lista. Os grupos selecionados aparecem na lista **Grupos de entrega para receber atribuição de aplicativo**.
16. Expanda o Agendamento de Implantação e, em seguida, configure as seguintes configurações:

    - Ao lado de **Implantar**, clique em **ATIVADO** para agendar a implantação ou clique em **DESATIVADO** para impedir a implantação. A opção padrão é definida como **ATIVADO**. Se você escolher **DESATIVADO**, nenhuma outra opção será necessária.
    - Ao lado de **Agendamento de implantação**, clique em **Agora** ou **Mais tarde**. A opção padrão é definida como **Agora**.
    - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora para a implantação.
    - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou clique em **Somente quando a implantação anterior falhou**. A opção padrão é definida como **Em cada conexão**.

- Ao lado de **Implantar para conexão sempre ativa**, clique em **ATIVADO** ou **DESATIVADO**. A opção padrão é definida como **DESATIVADO**.

  Esta opção se aplica quando você configurou a chave de implantação em segundo plano de agendamento em **Configurações > Propriedades do Servidor**. A opção sempre ativa não está disponível para dispositivos iOS.

O agendamento de implantação que você configura é o mesmo para todas as plataformas. Quaisquer alterações feitas se aplicam a todas as plataformas, exceto para **Implantar para conexão sempre ativa**, que não se aplica ao iOS.

17. Clique em **Avançar**. A página **Resumo** é exibida, onde você pode verificar a configuração da ação.
18. Clique em **Salvar** para salvar a ação.

Ações de bloqueio e limpeza de aplicativos para o modo somente MAM

Você pode limpar ou bloquear aplicativos em um dispositivo em resposta a todas as quatro categorias de gatilhos listadas no console do XenMobile: evento, propriedade do dispositivo, propriedade do usuário e nome do aplicativo instalado.

Para configurar uma limpeza ou bloqueio automático de aplicativo

1. No console do XenMobile, clique em **Configurar > Ações**.
2. Na página **Ações**, clique em **Adicionar**.
3. Na página **Informações da Ação**, insira um nome para a ação e uma descrição opcional.
4. Na página **Detalhes da Ação**, selecione o gatilho desejado.
5. Em **Ação**, selecione uma ação.

   Para esta etapa, tenha em mente as seguintes condições:

   Quando o tipo de gatilho é definido como **Evento** e o valor não é **Usuário desabilitado do Active Directory**, as ações de **Limpeza de aplicativo** e **Bloqueio de aplicativo** não aparecem.

   Quando o tipo de gatilho é definido como **Propriedade do dispositivo** e o valor é **Modo perdido do MDM ativado**, as seguintes ações não aparecem:

   - Limpar seletivamente o dispositivo

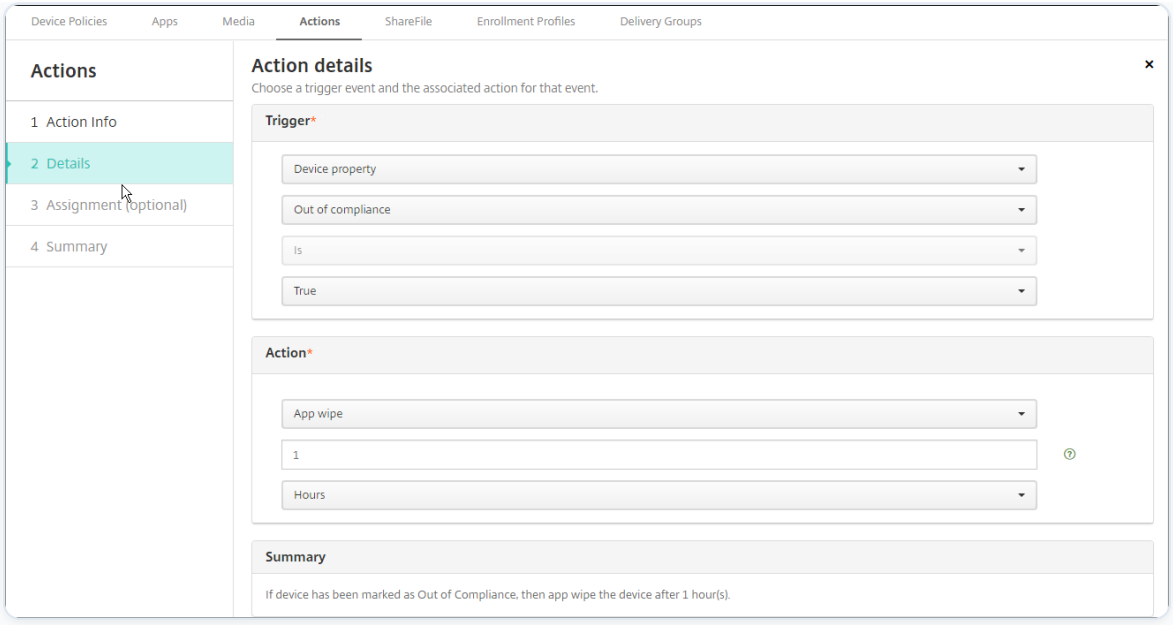
- Limpar completamente o dispositivo
- Revogar o dispositivo

Para cada opção, um atraso de 1 hora é definido automaticamente, mas você pode selecionar o período de atraso em minutos, horas ou dias. O objetivo do atraso é dar tempo aos usuários para corrigir um problema antes que a ação ocorra. Para obter mais informações sobre as ações de limpeza de aplicativo e bloqueio de aplicativo, consulte Ações de segurança.

Nota:

Se você definir o gatilho como **evento**, o intervalo de repetição será automaticamente de no mínimo 1 hora. O dispositivo deve realizar uma atualização das políticas para sincronizar com o servidor para que a notificação chegue. Normalmente, um dispositivo sincroniza com o servidor quando os usuários fazem login ou atualizam manualmente suas políticas através do Secure Hub.

Um atraso extra de aproximadamente 1 hora pode ocorrer antes que qualquer ação seja executada, para permitir que o banco de dados do Active Directory sincronize com o XenMobile.

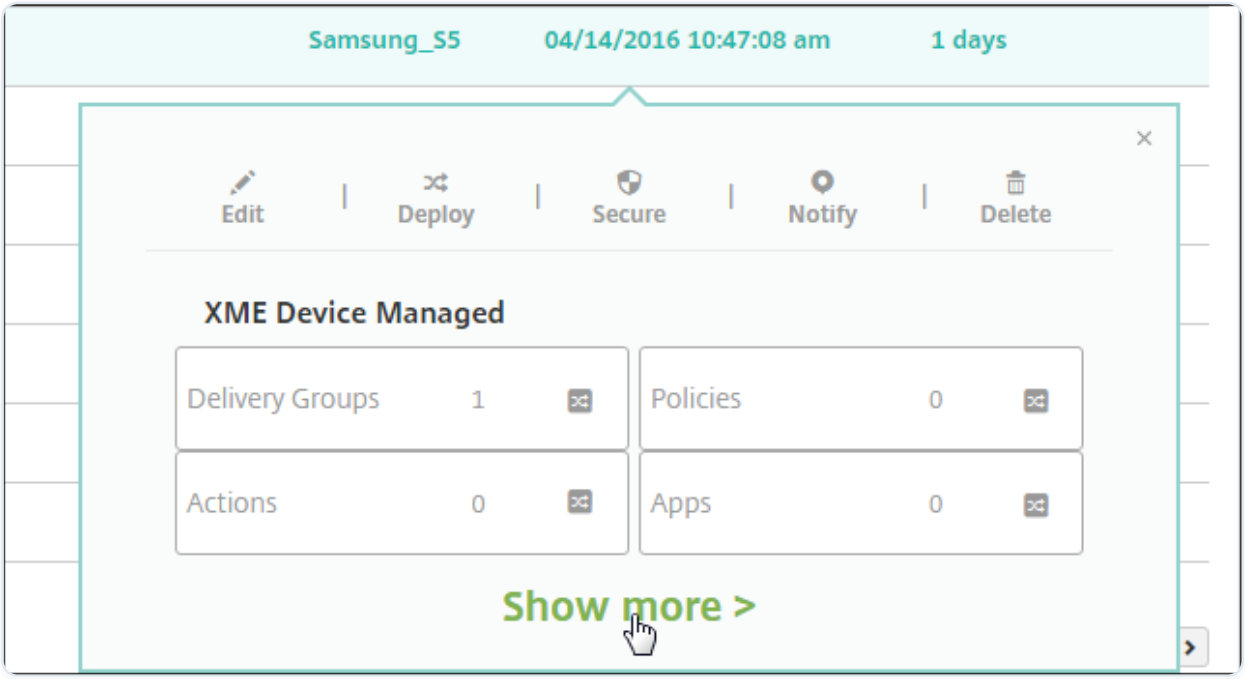


6. Configure as regras de implantação e clique em **Avançar**.
7. Configure as atribuições de grupo de entrega e um agendamento de implantação e clique em **Avançar**.

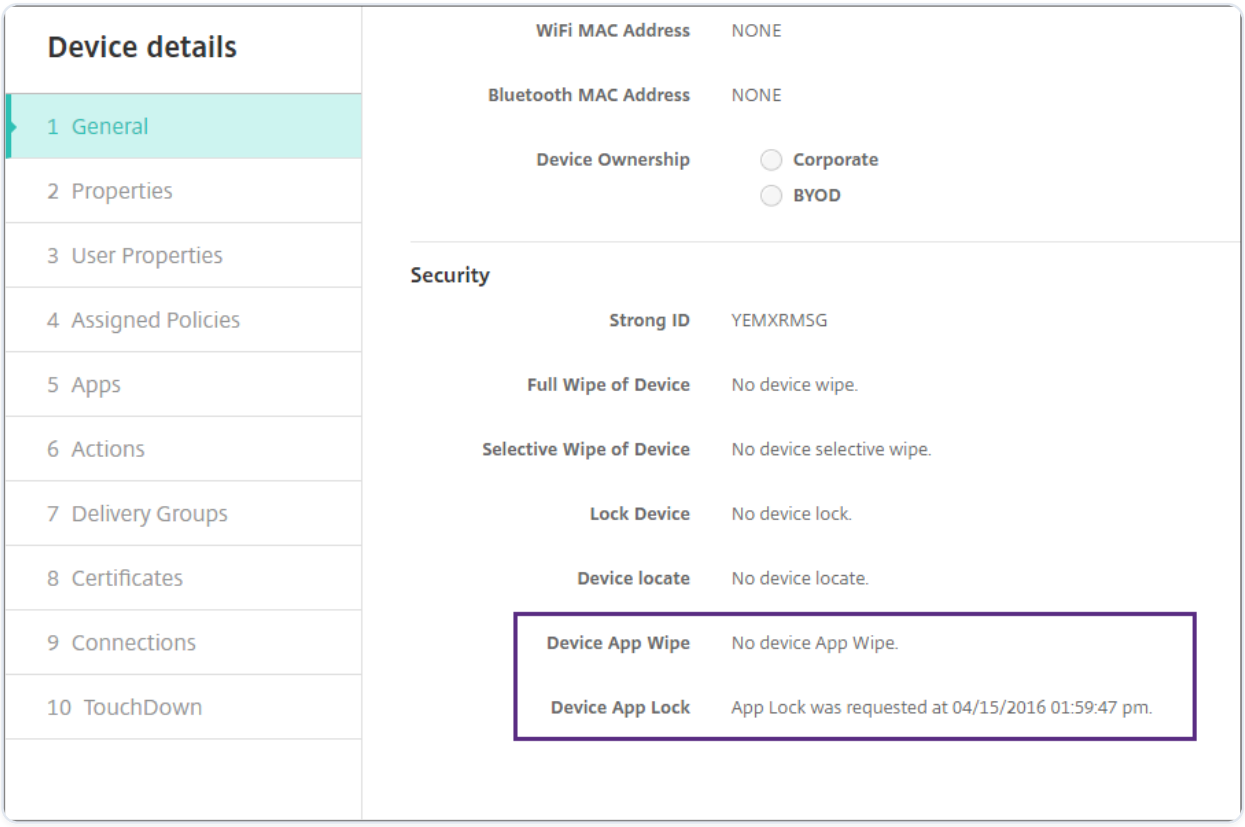
8. Clique em **Salvar**.

Para verificar o status de bloqueio ou limpeza de aplicativo

1. Vá para **Gerenciar > Dispositivos**, clique em um dispositivo e, em seguida, clique em **Mostrar mais**.



2. Role até **Limpeza de Aplicativo do Dispositivo** e **Bloqueio de Aplicativo do Dispositivo**.



Depois que um dispositivo é limpo, o usuário é solicitado a inserir um código PIN. Se o usuário esquecer o código, você pode consultá-lo nos Detalhes do Dispositivo.

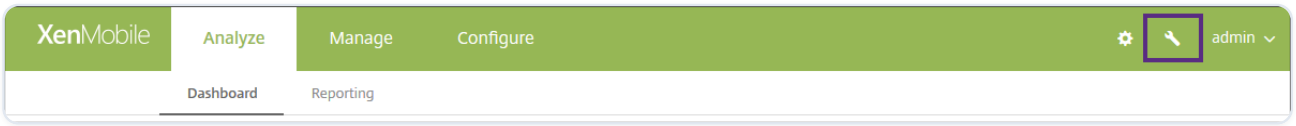


Monitoramento e suporte

Você pode usar o Painel do XenMobile® e a página de Suporte do XenMobile para monitorar e solucionar problemas do seu XenMobile Server. Use a página de Suporte do XenMobile para acessar informações e ferramentas relacionadas ao suporte.

Para um XenMobile Server local, você também pode executar ações a partir da CLI do XenMobile. Para obter detalhes, consulte Opções da interface de linha de comando.

No console do XenMobile, clique no ícone de chave inglesa no canto superior direito.

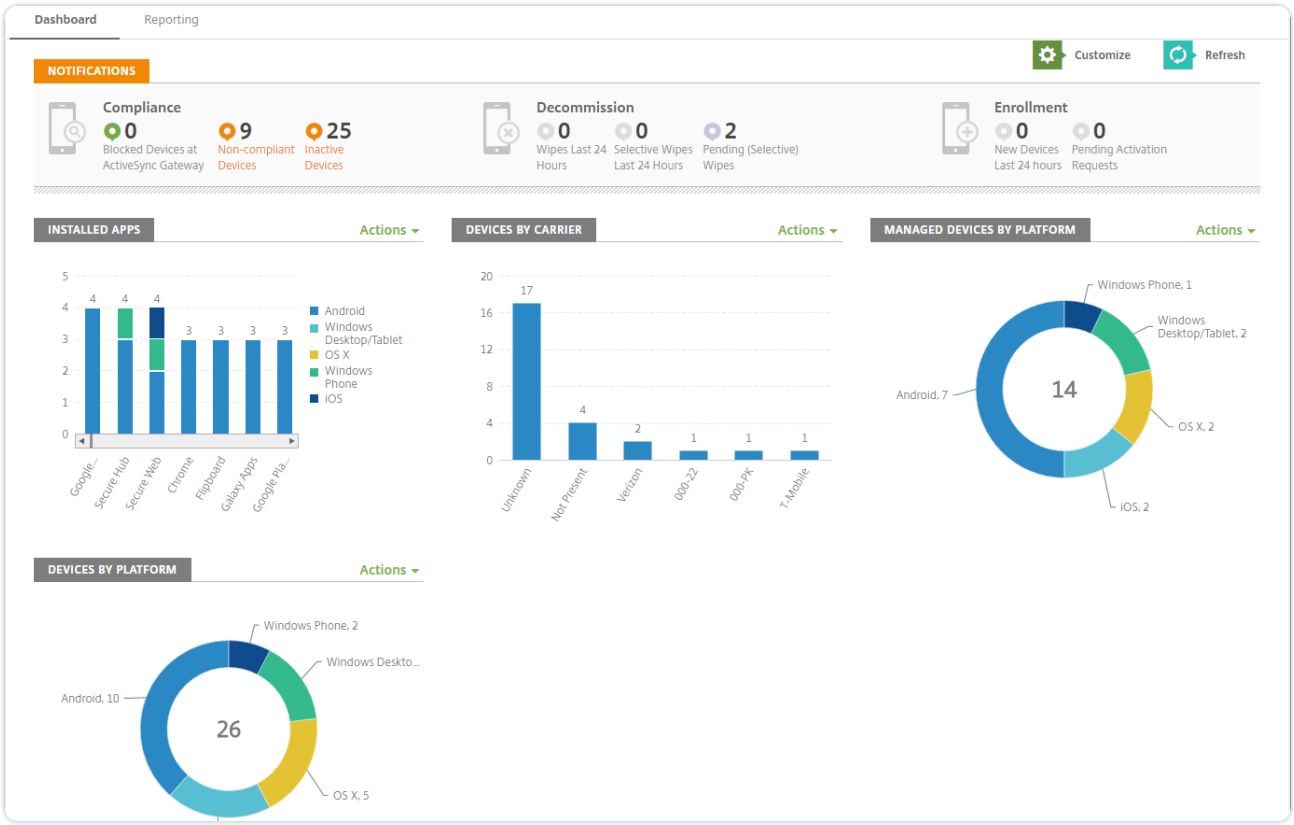


A página de Solução de Problemas e Suporte é exibida.

Use a página **Suporte** do XenMobile para:

- Acessar diagnósticos.
- Criar pacotes de suporte (somente instalações locais).
- Acessar links para a Documentação do Produto Citrix e o Centro de Conhecimento.
- Acessar operações de log.
- Usar opções de configuração avançadas.
- Acessar um conjunto de ferramentas e utilitários.

Você também pode visualizar informações rapidamente acessando o painel do console do XenMobile. Com essas informações, você pode ver problemas e sucessos rapidamente usando widgets.

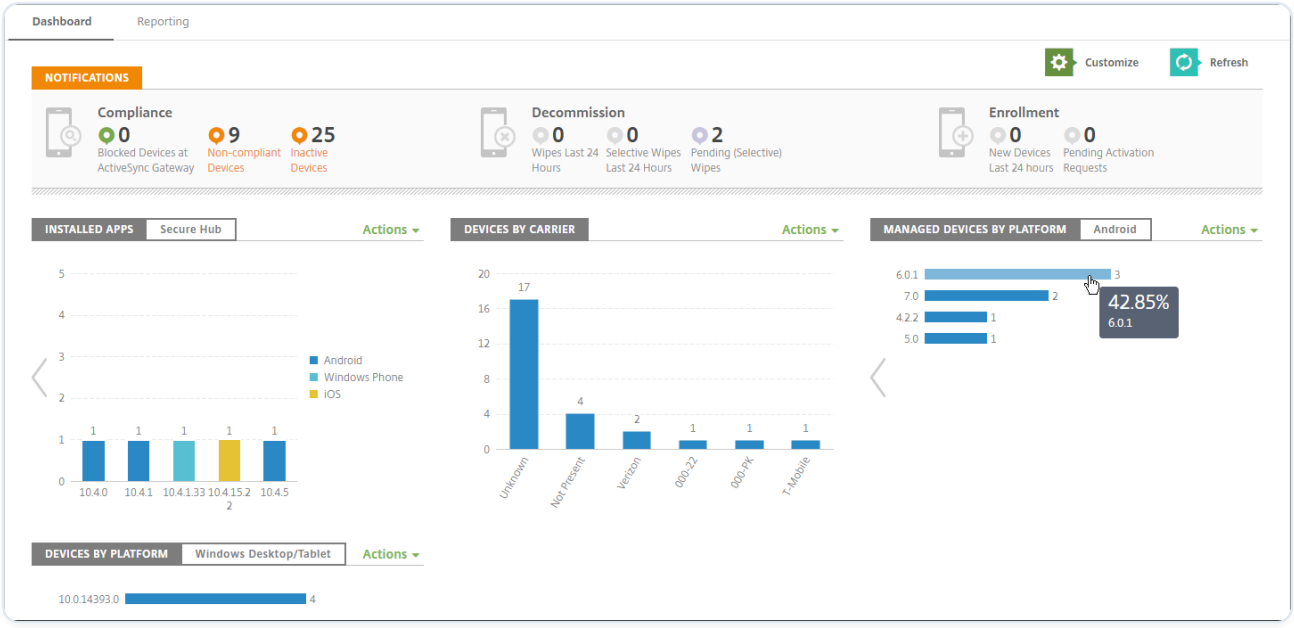


O painel é geralmente a página que aparece primeiro quando você faz logon no console do XenMobile. Para acessar o painel de qualquer outro lugar no console, clique em **Analisar**. Clique em **Personalizar** no painel para editar o layout da página e os widgets que aparecem.

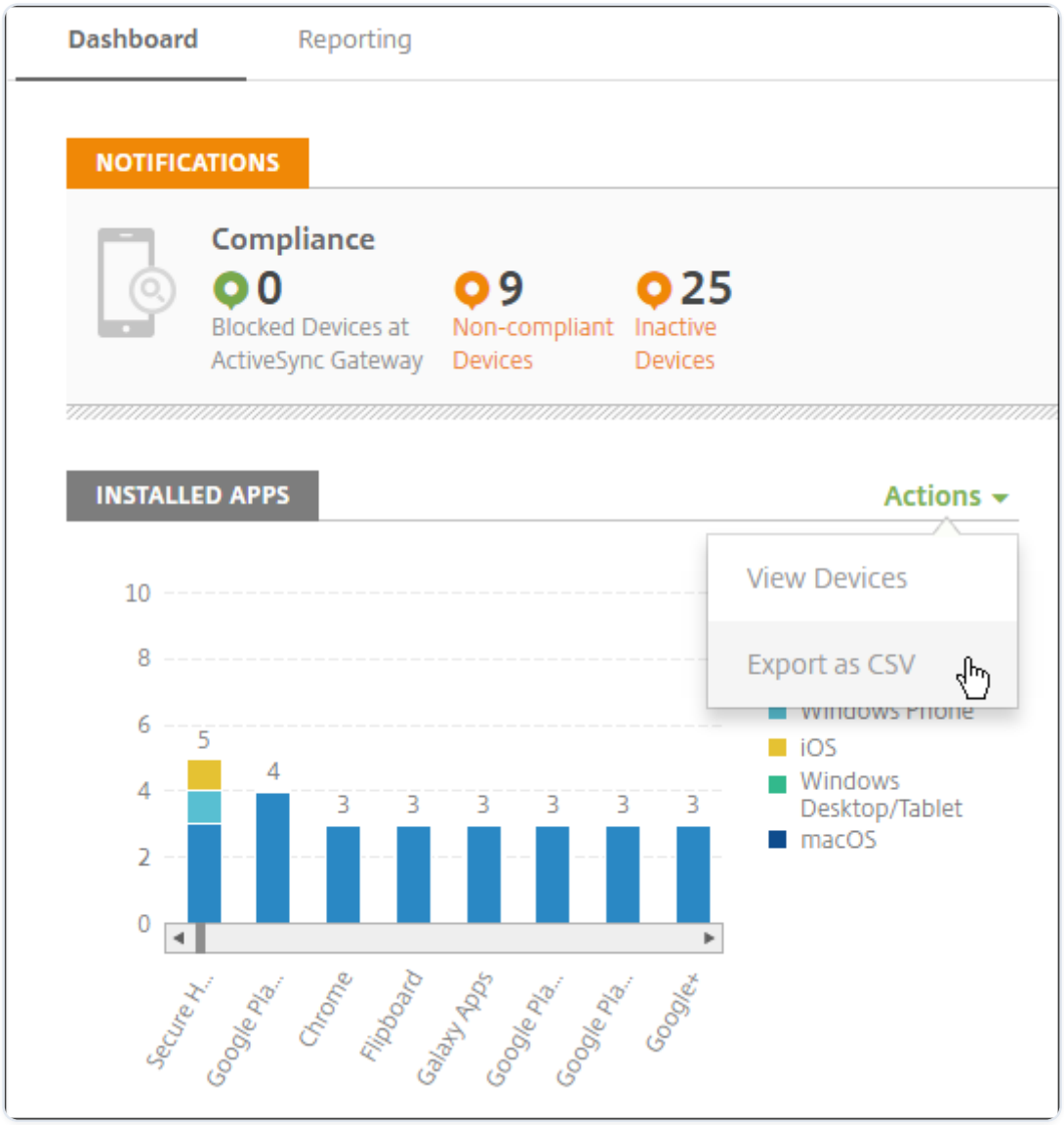
- **Meus Painéis:** Você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e visualizar cada um selecionando o painel salvo.
- **Estilo de Layout:** Nesta linha, você pode selecionar quantos widgets aparecem no seu painel e como os widgets são dispostos.
- **Seleção de Widget:** Você pode escolher quais informações aparecem no seu painel.
    - **Notificações:** Marque a caixa de seleção acima dos números à esquerda para adicionar uma barra de Notificações acima dos seus widgets. Esta barra mostra o número de dispositivos compatíveis, dispositivos inativos e dispositivos apagados ou registrados nas últimas 24 horas.
    - **Dispositivos por Plataforma:** Exibe o número de dispositivos gerenciados e não gerenciados por plataforma.
    - **Dispositivos por Operadora:** Exibe o número de dispositivos gerenciados e não gerenciados por operadora. Clique em cada barra para ver um detalhamento por plataforma.
    - **Dispositivos Gerenciados por Plataforma:** Exibe o número de dispositivos gerenciados por plataforma.

- **Dispositivos Não Gerenciados por Plataforma:** Exibe o número de dispositivos não gerenciados por plataforma. Os dispositivos que aparecem neste gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.
- **Dispositivos por Status do Gateway ActiveSync:** Exibe o número de dispositivos agrupados por status do Gateway ActiveSync. As informações mostram o status Bloqueado, Permitido ou Desconhecido. Você pode clicar em cada barra para detalhar os dados por plataforma.
- **Dispositivos por Propriedade:** Exibe o número de dispositivos agrupados por status de propriedade. As informações mostram o status de propriedade corporativa, de funcionário ou desconhecido.
- **Implantações de Grupo de Entrega com Falha:** Exibe o número total de implantações com falha por pacote. Apenas pacotes que tiveram implantações com falha aparecem.
- **Dispositivos por Motivo de Bloqueio:** Exibe o número de dispositivos bloqueados pelo ActiveSync
- **Aplicativos Instalados:** Digite um nome de aplicativo para um gráfico de informações do aplicativo.
- **Uso de Licença de Aplicativos de Compra por Volume:** Exibe estatísticas de uso de licença para aplicativos de compra por volume da Apple.

Com cada widget, você pode clicar nas partes individuais para detalhar e obter mais informações.



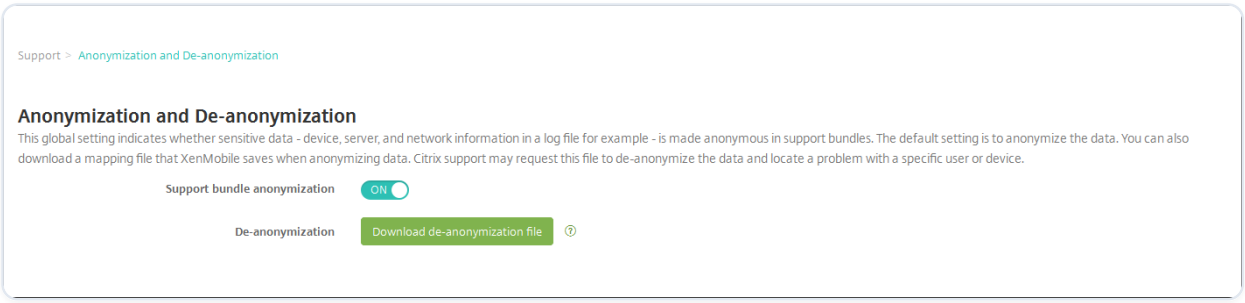
Você também pode exportar as informações como um arquivo .csv clicando no menu **Ação**.



Anonimizar dados em pacotes de suporte

Ao criar pacotes de suporte no XenMobile®, dados confidenciais de usuário, servidor e rede são anonimizados por padrão. Você pode alterar esse comportamento na página Anonimização e Desanonimização. Você também pode baixar um arquivo de mapeamento que o XenMobile salva ao anonimizar dados. O suporte da Citrix® pode solicitar este arquivo para desanonimizar os dados e localizar um problema com um usuário ou dispositivo específico.

1. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito. A página **Suporte** é exibida.
2. Na página **Suporte**, em **Avançado**, clique em **Anonimização e Desanonimização**. A página **Anonimização e Desanonimização** é exibida.



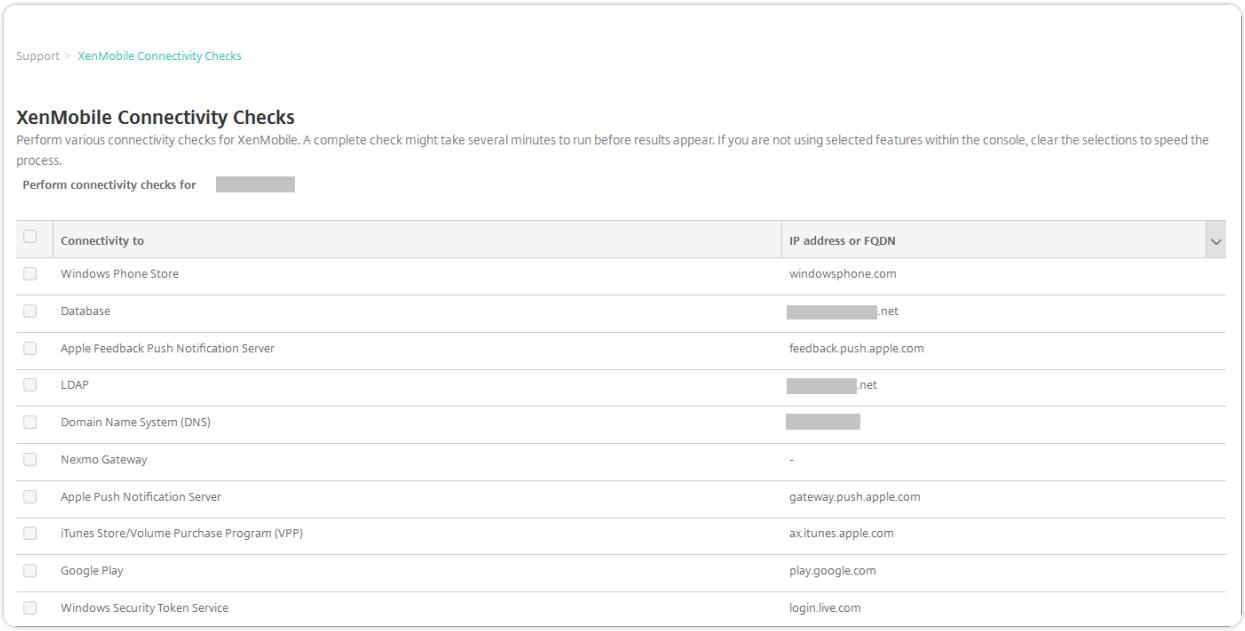
3. Em **Anonimização de pacote de suporte**, selecione se os dados são anonimizados. O padrão é **ATIVADO**.
4. Ao lado de **Desanonimização**, clique em **Baixar arquivo de desanonimização** para baixar o arquivo de mapeamento a ser enviado ao suporte da Citrix quando eles precisarem de informações específicas do dispositivo ou do usuário para diagnosticar um problema.

Verificações de conectividade

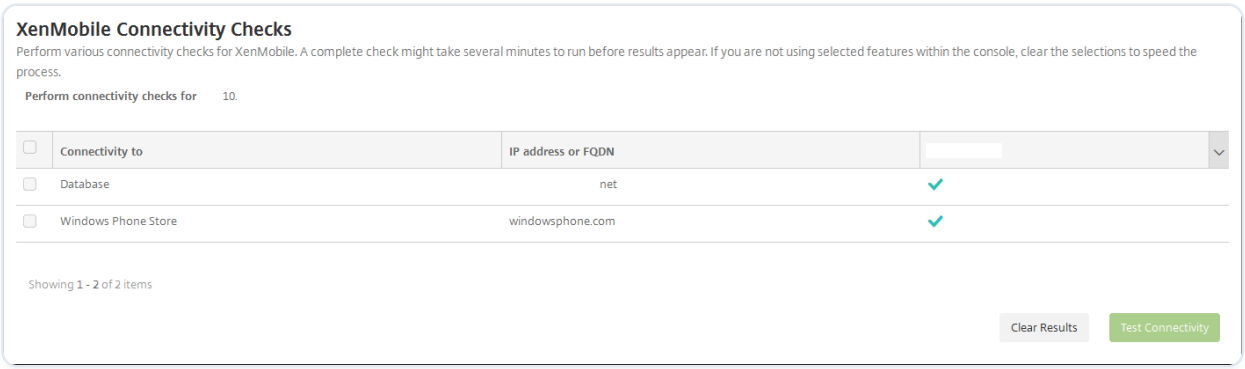
Na página **Suporte** do XenMobile®, você pode verificar a conexão do XenMobile com o Citrix Gateway e com outros servidores e locais.

Realizando verificações de conectividade do XenMobile

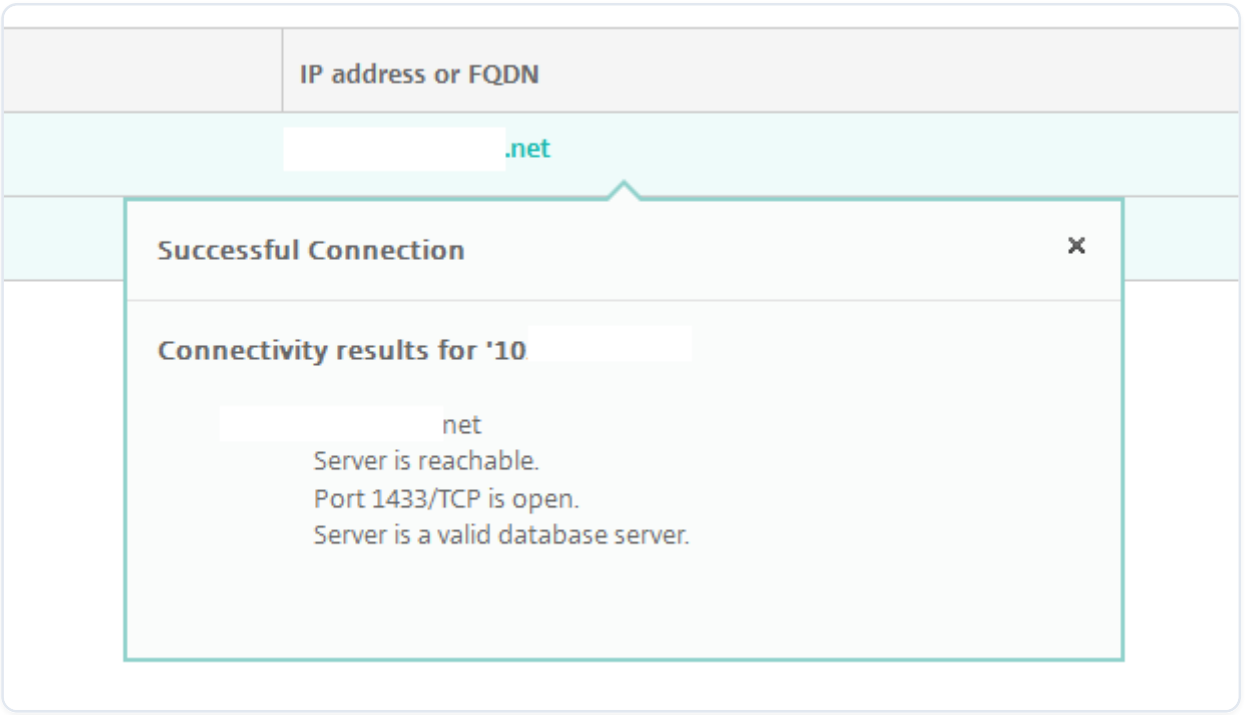
1. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito do console. A página **Suporte** é exibida.
2. Em **Diagnóstico**, clique em **Verificações de Conectividade do XenMobile**. A página **Verificações de Conectividade do XenMobile** é exibida. Se o seu ambiente XenMobile tiver nós em cluster, todos os nós serão exibidos.



3. Selecione os servidores que você deseja incluir no teste de conectividade e clique em **Testar Conectividade**. A página de resultados do teste é exibida.

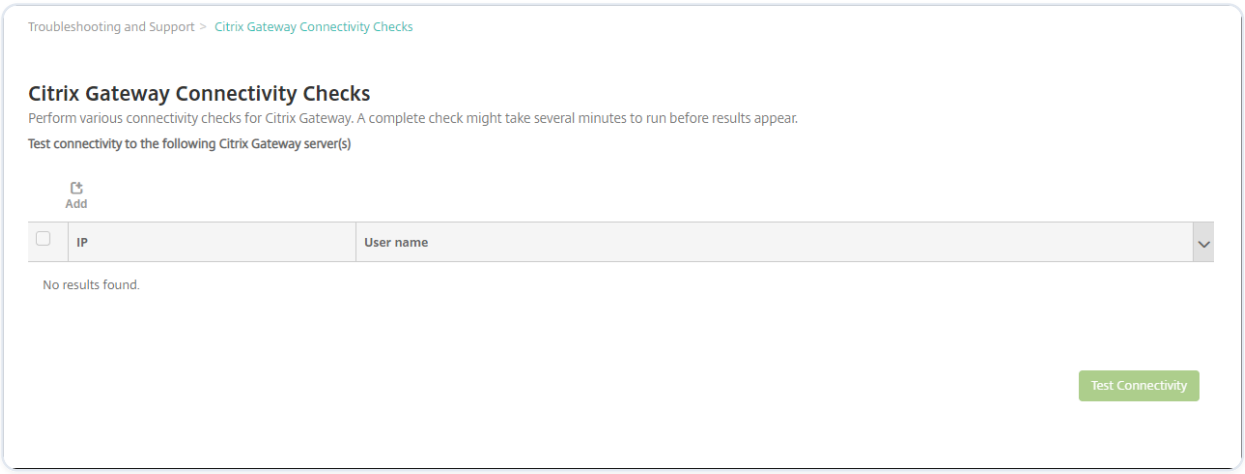


4. Selecione um servidor na tabela de resultados do teste para ver os resultados detalhados desse servidor.

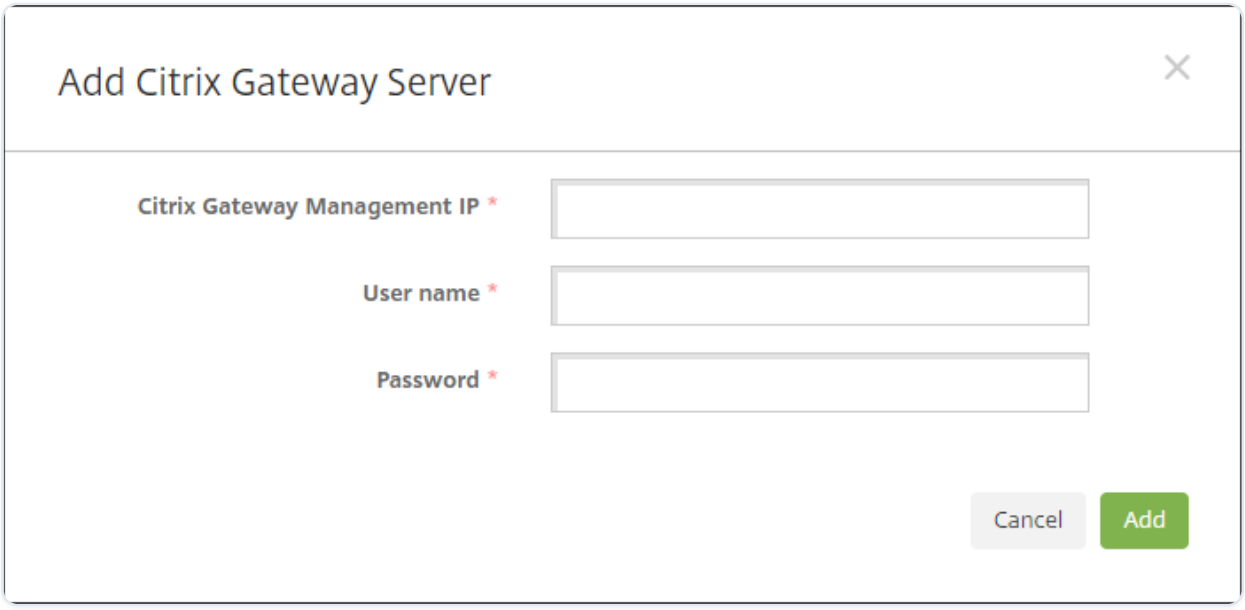


Realizando verificações de conectividade do Citrix Gateway

1. Na página **Suporte**, em **Diagnóstico**, clique em **Verificações de Conectividade do Citrix Gateway**. A página **Verificações de Conectividade do Citrix Gateway** é exibida. A tabela estará vazia se você não tiver adicionado nenhum servidor Citrix Gateway.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Servidor Citrix Gateway** é exibida.



3. Em **IP de Gerenciamento do Citrix Gateway**, digite o endereço IP de gerenciamento para o servidor que executa o Citrix Gateway que você deseja testar.

> **Observação:**
>
> Se você estiver realizando uma verificação de conectividade para um servidor Citrix Gateway que já foi adicionado anteriormente, o endereço IP é fornecido.

4. Digite suas credenciais de administrador para este Citrix Gateway.

> **Observação:**

> Se você estiver realizando uma verificação de conectividade para um servidor Citrix Gateway que já foi adicionado anteriormente, o nome de usuário é fornecido.

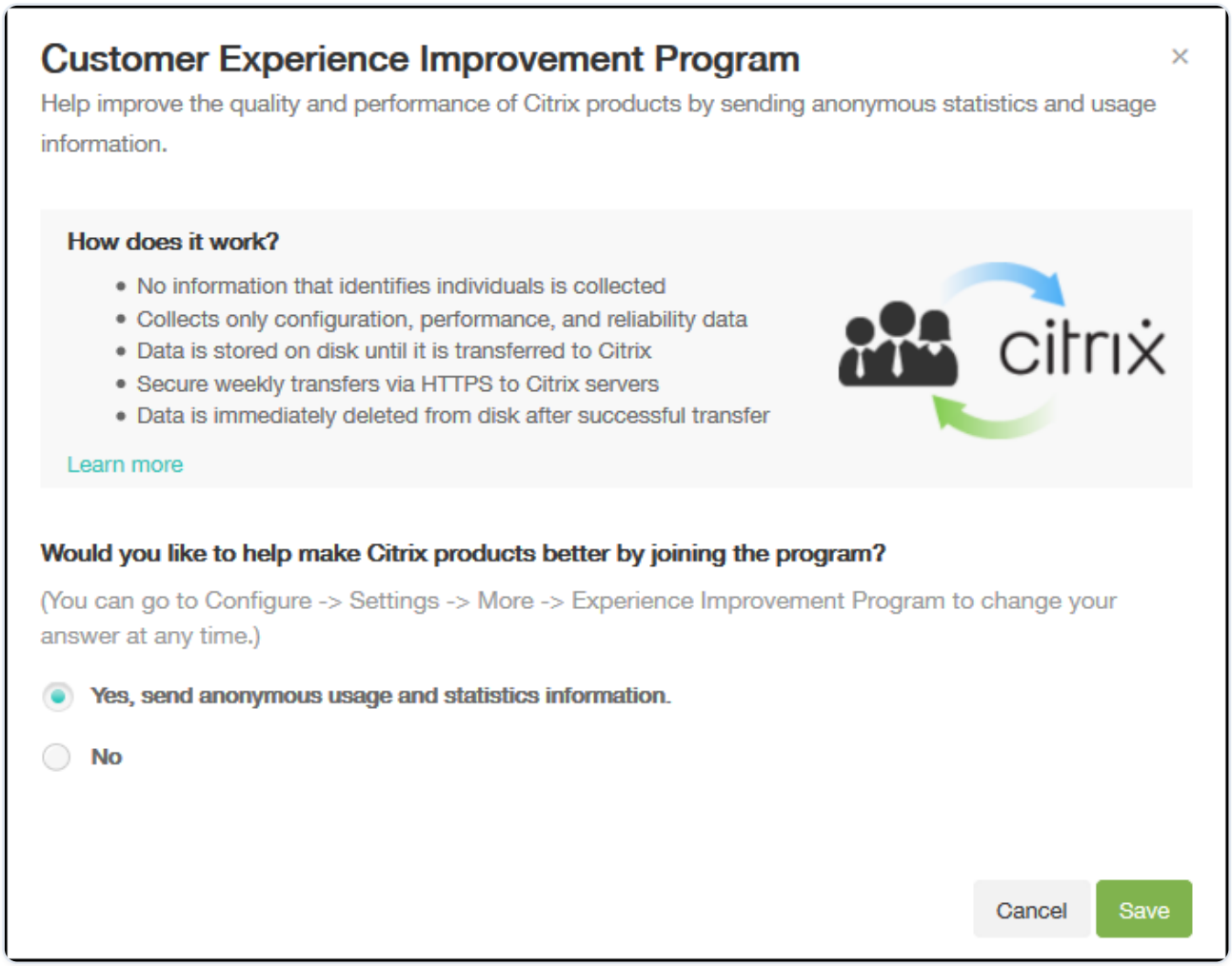
5. Clique em **Adicionar**. O Citrix Gateway é adicionado à tabela na página **Verificações de Conectividade do Citrix Gateway**.
6. Selecione o servidor Citrix Gateway e clique em **Testar Conectividade**. Os resultados aparecem em uma tabela de resultados de teste.
7. Selecione um servidor na tabela de resultados de teste para ver os resultados detalhados desse servidor.

Programa de Melhoria da Experiência do Cliente

O Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix coleta dados anônimos de configuração e uso do XenMobile e os envia automaticamente para a Citrix. Esses dados ajudam a Citrix a melhorar a qualidade, a confiabilidade e o desempenho do XenMobile. A participação no CEIP é voluntária. Ao instalar o XenMobile pela primeira vez ou ao instalar uma atualização, você pode participar do CEIP. Ao optar por participar, os dados são normalmente coletados semanalmente, e os dados de desempenho e uso são coletados a cada hora. Os dados são armazenados em disco e transferidos com segurança via HTTPS para a Citrix semanalmente. Você pode alterar sua participação no CEIP no console do XenMobile. Para obter mais informações sobre o CEIP, consulte Sobre o Programa de Melhoria da Experiência do Cliente (CEIP) da Citrix.

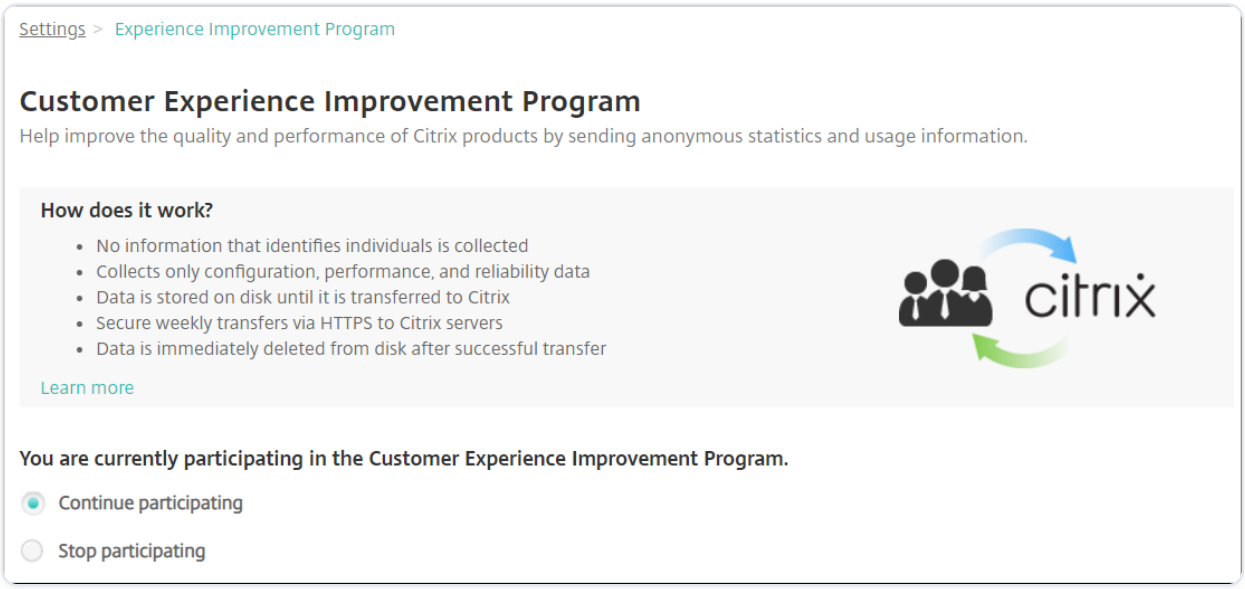
Escolhendo participar do CEIP

Na primeira vez que você instala o XenMobile® ou quando faz uma atualização, você vê a seguinte caixa de diálogo que o solicita a participar.



Alterando sua configuração de participação no CEIP

1. Para alterar sua configuração de participação no CEIP no console do XenMobile, clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações**.
2. Em **Servidor**, clique em **Programa de Melhoria da Experiência**. A página **Programa de Melhoria da Experiência do Cliente** é exibida. A página exata que você vê depende se você está participando atualmente do CEIP.

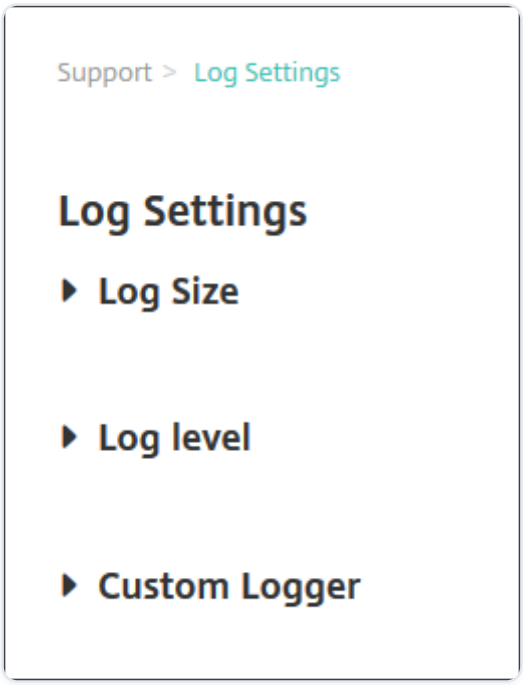


3. Se você estiver participando atualmente do CEIP e quiser parar, clique em **Parar de participar**.
4. Se você não estiver participando atualmente do CEIP e quiser começar, clique em **Começar a participar**.
5. Clique em **Salvar**.

Registros

Você pode configurar as definições de registro para personalizar a saída dos registros que o XenMobile® gera. Se você tiver servidores XenMobile em cluster ao configurar as definições de registro no console do XenMobile, essas definições serão compartilhadas com todos os outros servidores no cluster.

1. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito do console. A página **Suporte** é exibida.
2. Em **Operações de Registro**, clique em **Configurações de Registro**. A página **Configurações de Registro** é exibida.

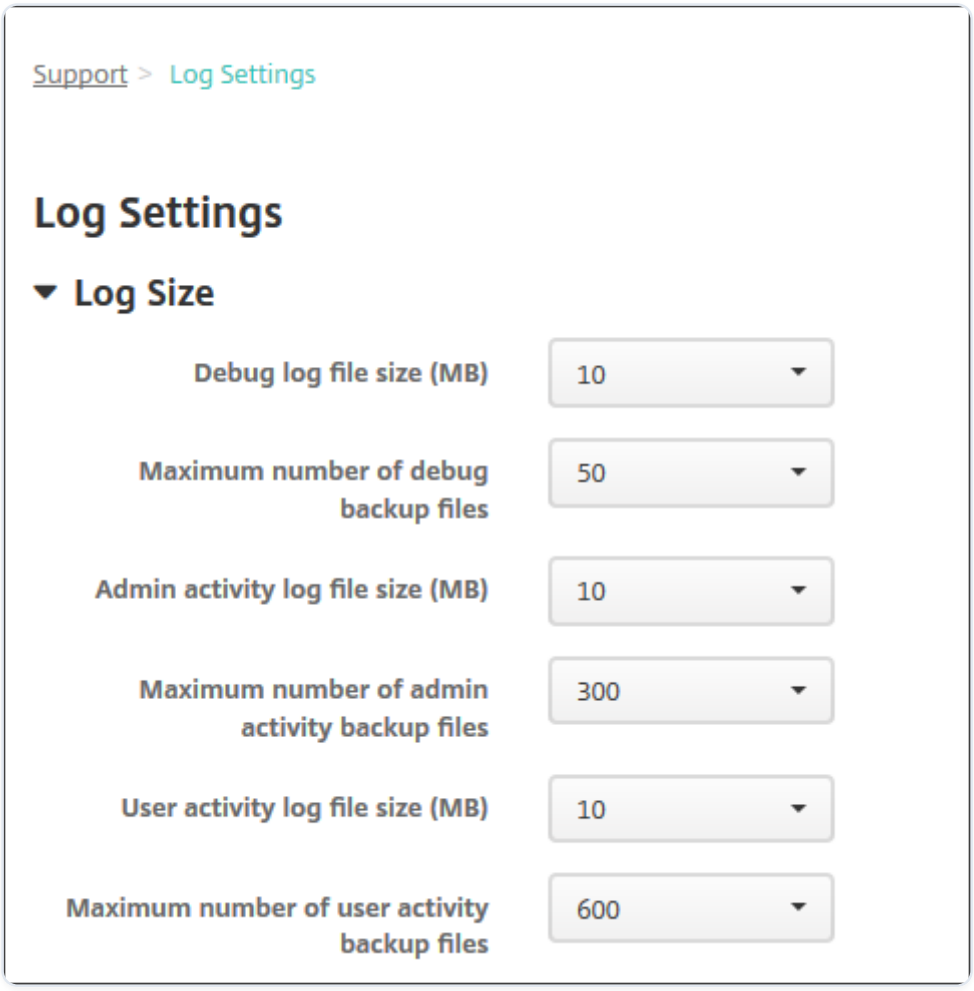


Na página **Configurações de Registro**, você pode acessar as seguintes opções:

- **Tamanho do Registro**. Use esta opção para controlar o tamanho do arquivo de registro e o número máximo de arquivos de backup de registro mantidos no banco de dados. O tamanho do registro se aplica a cada um dos registros suportados pelo XenMobile (registro de depuração, registro de atividade do administrador e registro de atividade do usuário).
- **Nível de registro**. Use esta opção para alterar o nível de registro ou para persistir as configurações.
- **Registrador Personalizado**. Use esta opção para criar um registrador personalizado; os registros personalizados exigem um nome de classe e o nível de registro.

Para configurar as opções de Tamanho do Registro

1. Na página **Configurações de Registro**, expanda **Tamanho do Registro**.



2. Configure estas definições:

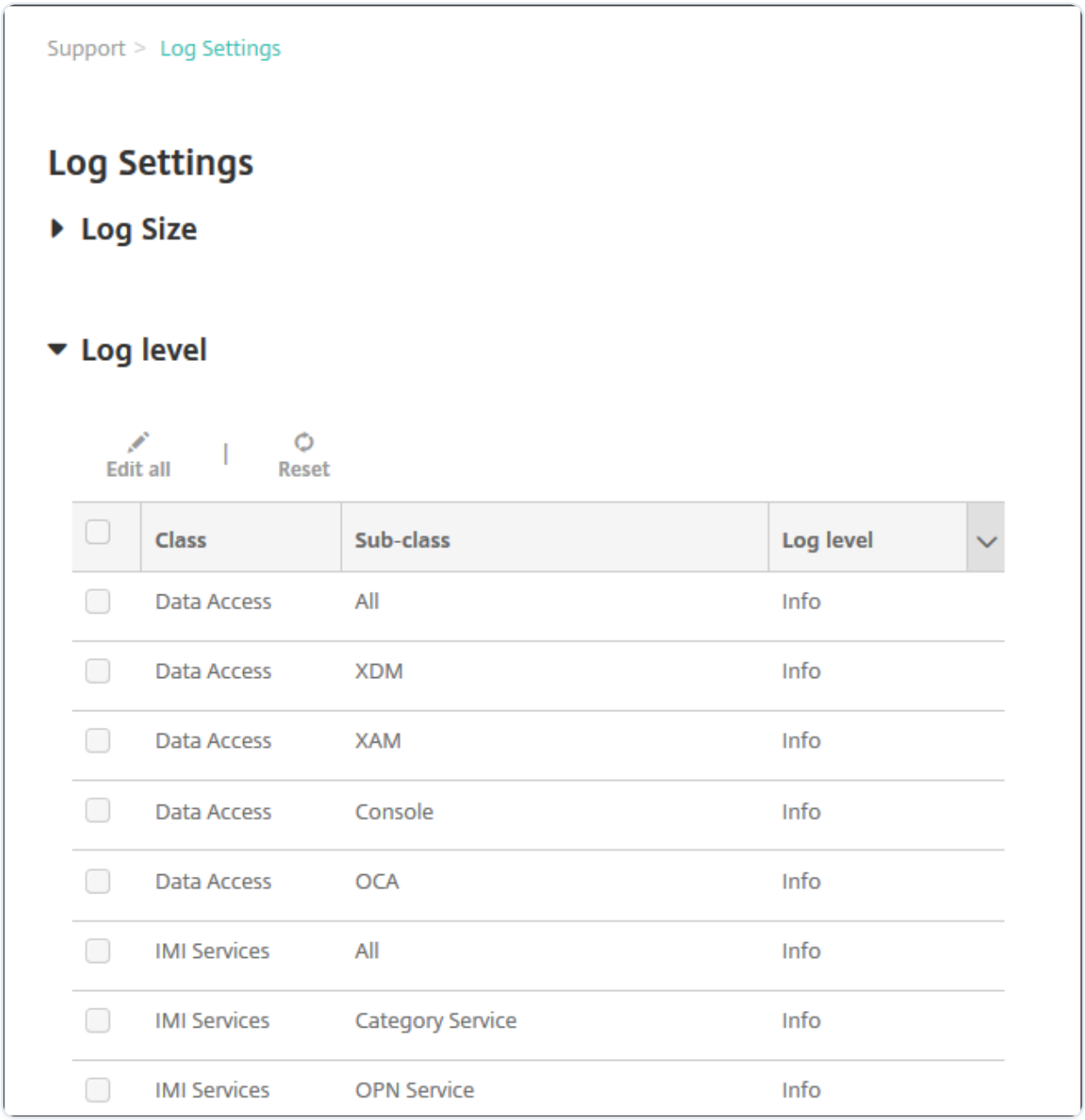
- **Tamanho do arquivo de registro de depuração (MB):** Na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de depuração. O tamanho do arquivo padrão é de **10 MB**.
- **Número máximo de arquivos de backup de depuração:** Na lista, clique no número máximo de arquivos de depuração mantidos pelo servidor. Por padrão, o XenMobile mantém 50 arquivos de backup no servidor.
- **Tamanho do arquivo de log de atividade do administrador (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividade do administrador. O tamanho de arquivo padrão é **10 MB**.
- **Número máximo de arquivos de backup de atividade do administrador:** Na lista, clique no número máximo de arquivos de atividade do administrador mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.
- **Tamanho do arquivo de log de atividade do usuário (MB):** Na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividade do usuário. O tamanho de arquivo padrão é **10 MB**.

- **Número máximo de arquivos de backup de atividade do usuário:** Na lista, clique no número máximo de arquivos de atividade do usuário mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.

Para configurar as opções de Nível de Log

O nível de log permite especificar o tipo de informação que o XenMobile coleta no log. Você pode definir o mesmo nível para todas as classes ou pode definir classes individuais para níveis específicos.

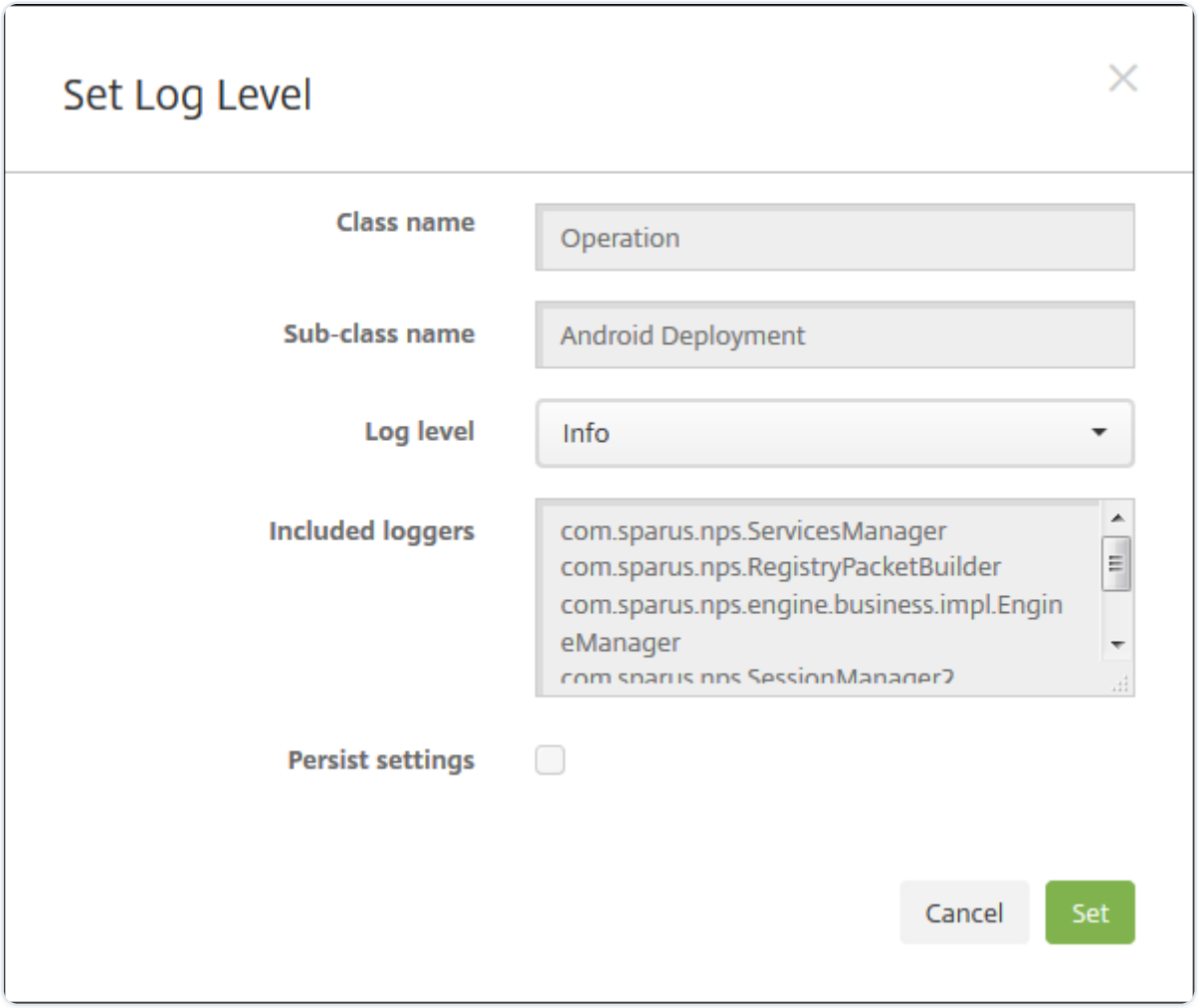
1. Na página **Configurações de Log**, expanda **Nível de log**. A tabela de todas as classes de log é exibida.



2. Faça um dos seguintes:

- Clique na caixa de seleção ao lado de uma Classe e, em seguida, clique em **Definir Nível** para alterar apenas o nível de log desta classe.
- Clique em **Editar** tudo para aplicar a alteração do nível de log a todas as classes na tabela.

A caixa de diálogo **Definir Nível de Log** é exibida, onde você pode definir o nível de log e selecionar se as configurações de nível de log devem persistir ao reiniciar o XenMobile Server.



- **Nome da Classe**: Este campo exibe **Todos** quando você está alterando o nível de log para todas as classes ou exibe o nome da classe individual. Não é editável.
- **Nome da Subclasse**: Este campo exibe **Todos** quando você está alterando o nível de log para todas as classes ou exibe o nome da subclasse individual. Não é editável.
- **Nível de log**: Na lista, clique em um nível de log. Os níveis de log suportados incluem:
  - Fatal
  - Erro
  - Aviso
  - Info

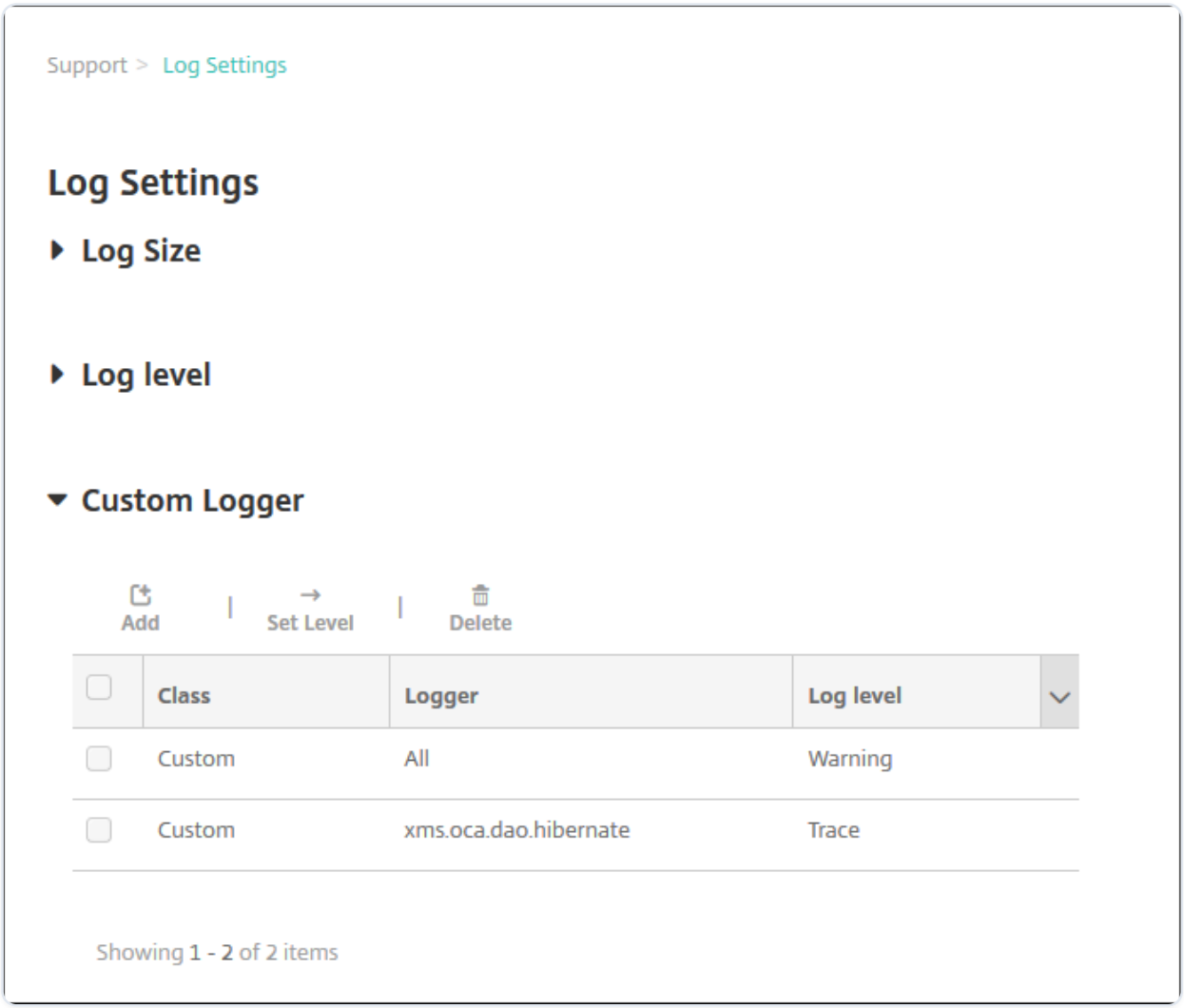
    - Debug
    - Trace
    - Desativado

- **Loggers Incluídos**: Este campo fica em branco quando você está alterando o nível de log para todas as classes ou exibe os loggers configurados atualmente para uma classe individual. Não é editável.
- **Manter configurações**: Se você quiser que as configurações de nível de log persistam quando você reiniciar o servidor, selecione esta caixa de seleção. Não selecionar esta caixa de seleção significa que as configurações de nível de log retornarão aos seus padrões quando você reiniciar o servidor.

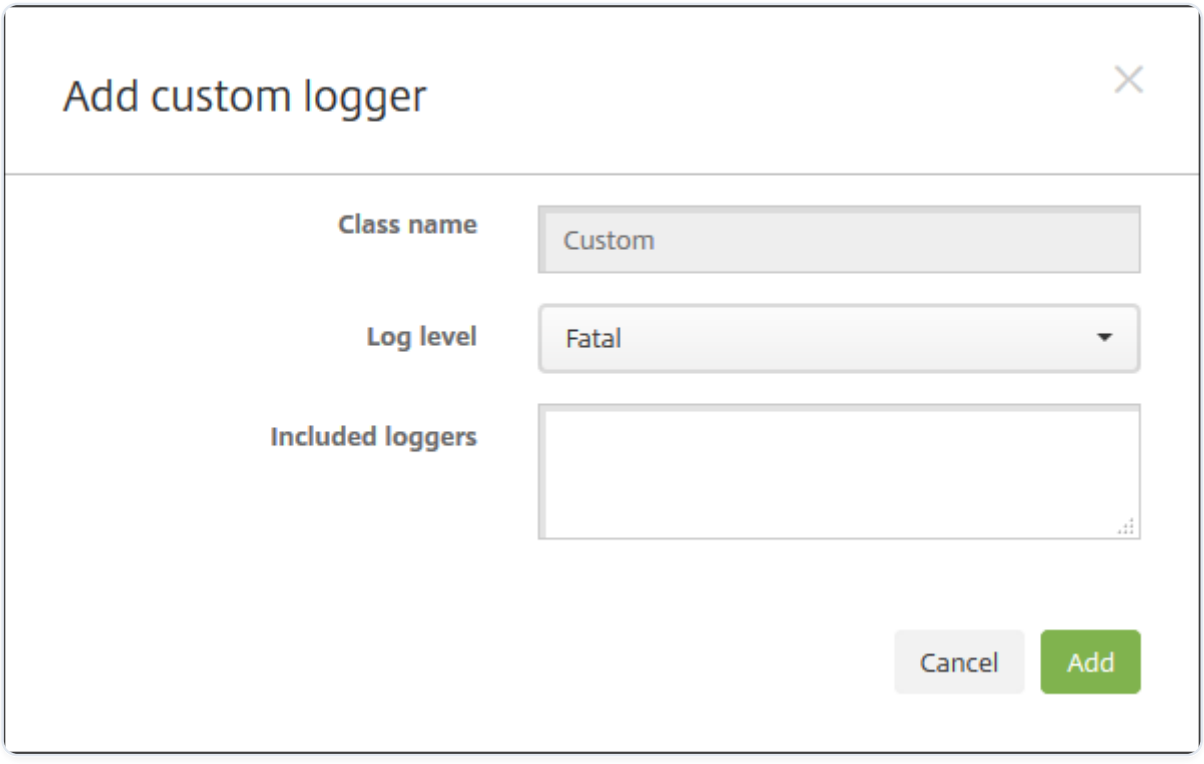
3. Clique em **Definir** para confirmar suas alterações.

Para adicionar um Logger Personalizado

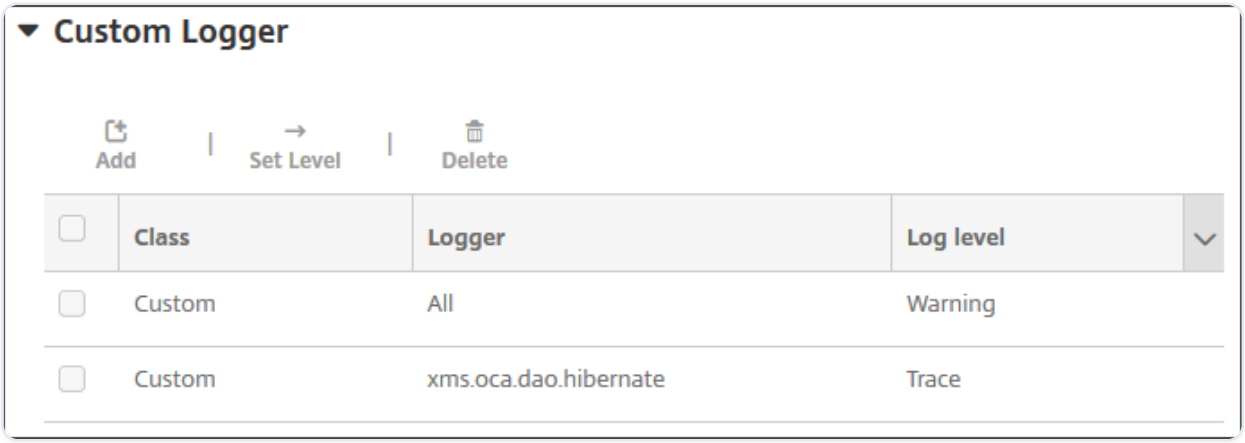
1. Na página **Configurações de Log**, expanda **Logger Personalizado**. A tabela **Logger Personalizado** é exibida. Se você não adicionou nenhum logger personalizado, a tabela estará inicialmente vazia.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar logger personalizado** é exibida.



3. Configure estas definições:
    - **Nome da Classe:** Este campo exibe **Personalizado**. Não é editável.
    - **Nível de log:** Na lista, clique em um nível de log. Os níveis de log suportados incluem:
        - Fatal
        - Erro
        - Aviso
        - Informação
        - Depuração
        - Rastreamento
        - Desativado
    - **Loggers Incluídos:** Digite os loggers específicos que você deseja incluir no logger personalizado ou deixe o campo em branco para incluir todos os loggers.
4. Clique em **Adicionar**. O logger personalizado é adicionado à tabela **Logger Personalizado**.



Para excluir um Logger Personalizado

1. Na página **Configurações de Log**, expanda **Registrador Personalizado**.
2. Selecione o registrador personalizado que você deseja excluir.
3. Clique em **Excluir**. Uma caixa de diálogo é exibida perguntando se você deseja excluir o registrador personalizado. Clique em **OK**.

> **Importante:**
>
> Você não pode desfazer esta operação.

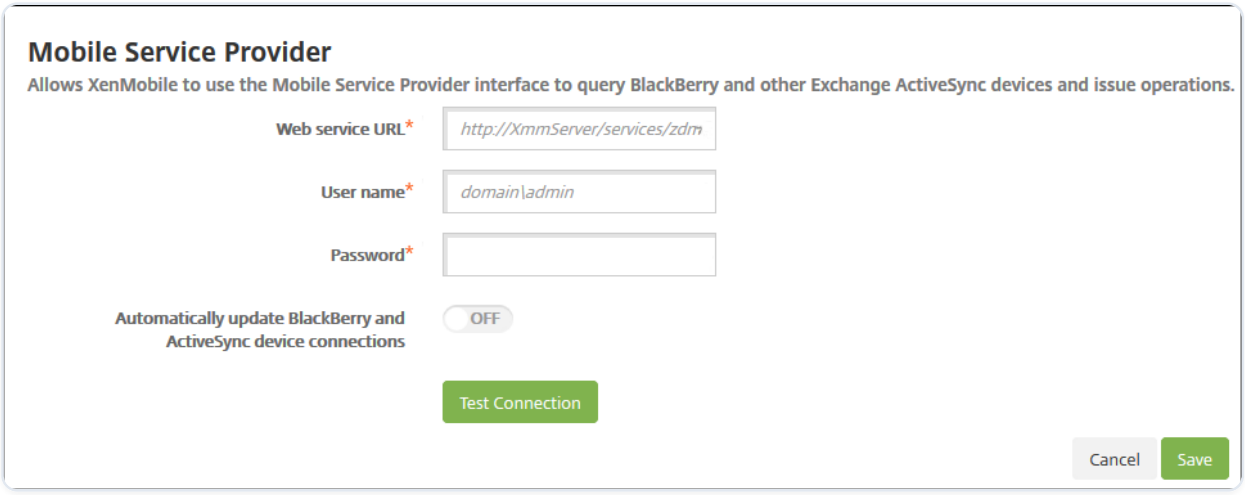
Provedor de Serviço Móvel

Você pode habilitar o XenMobile® para usar a interface do Provedor de Serviço Móvel para consultar dispositivos BlackBerry e Exchange ActiveSync e emitir operações.

Por exemplo, sua organização pode ter 1.000 usuários e cada usuário pode usar um ou mais dispositivos. Depois de comunicar a todos os usuários que eles devem registrar seus dispositivos no XenMobile para gerenciamento, o console do XenMobile indica o número de dispositivos que os usuários registram. Ao configurar esta definição, você pode determinar quantos dispositivos se conectam ao Exchange Server. Desta forma, você pode fazer o seguinte:

- Determinar se algum usuário ainda precisa registrar seus dispositivos.
- Emitir comandos para dispositivos de usuário que se conectam ao Exchange Server, como limpezas de dados.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Provedor de Serviço Móvel**. A página **Provedor de Serviço Móvel** é exibida.



3. Configure estas definições:

   - **URL do serviço Web:** Digite o URL do serviço Web; por exemplo, `https://<XmmServer>/services/xdmservice`
   - **Nome de usuário:** Digite o nome de usuário no formato domínio\\admin.
   - **Senha:** Digite a senha.

- **Atualizar automaticamente as conexões de dispositivos BlackBerry e ActiveSync:** Selecione se deseja atualizar automaticamente as conexões de dispositivos. O padrão é **DESATIVADO**.
- Clique em **Testar Conexão** para verificar a conectividade.

4. Clique em **Salvar**.

Relatórios

O XenMobile® fornece os seguintes relatórios predefinidos que permitem analisar suas implantações de aplicativos e dispositivos. Cada relatório aparece como uma tabela e um gráfico. Você pode classificar e filtrar as tabelas por coluna. Você pode selecionar elementos no gráfico para obter informações mais detalhadas.

- **Tentativas de Implantação Total de Aplicativos:** Lista os aplicativos implantados que os usuários tentaram instalar em seus dispositivos.
- **Aplicativos por Plataforma:** Lista aplicativos e versões de aplicativos por plataforma e versão do dispositivo.
- **Aplicativos por Tipo:** Lista aplicativos por versão, tipo e categoria.
- **Registro de Dispositivos:** Lista todos os dispositivos registrados.
- **Dispositivos e Aplicativos:** Lista os dispositivos que estão executando aplicativos gerenciados.
- **Dispositivos Inativos:** Uma lista de dispositivos que não tiveram nenhuma atividade pelo número de dias especificado pela propriedade do XenMobile Server device.inactivity.days.threshold.
- **Dispositivos com Jailbreak/Root:** Lista dispositivos iOS com jailbreak e dispositivos Android com root.
- **Termos e Condições:** Lista os usuários que aceitaram e recusaram os acordos de Termos e Condições. Você pode selecionar áreas do gráfico para visualizar mais detalhes.
- **Top 10 Aplicativos:** Implantação Falha - Lista até 10 aplicativos que falharam na implantação.
- **Aplicativos na Lista Negra por Dispositivo e Usuário:** Lista os aplicativos bloqueados que os usuários têm em seus dispositivos.

> **Nota:**

> O console do XenMobile Server inclui os termos "blacklist" e "whitelist". Estamos alterando esses termos em uma próxima versão para "block list" e "allow list".

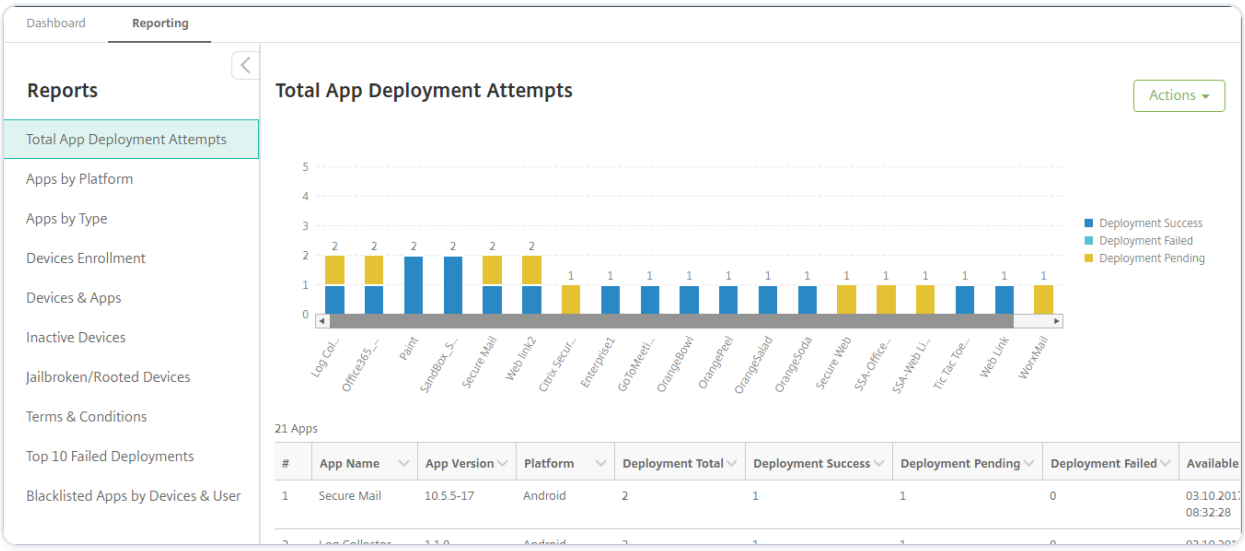
- **Dispositivos Não Conformantes:** Lista os dispositivos que não atendem aos critérios de conformidade, como se o dispositivo tem jailbreak, a versão do SO em execução e se o dispositivo possui uma senha.

Você pode exportar os dados de cada tabela no formato .csv, que pode ser aberto usando programas como o Microsoft Excel. Você pode exportar o gráfico de cada relatório no formato PDF.

- **100 principais aplicativos instalados:** Lista até os 100 principais aplicativos instalados para cada plataforma. Para obter mais informações, consulte Propriedades do servidor

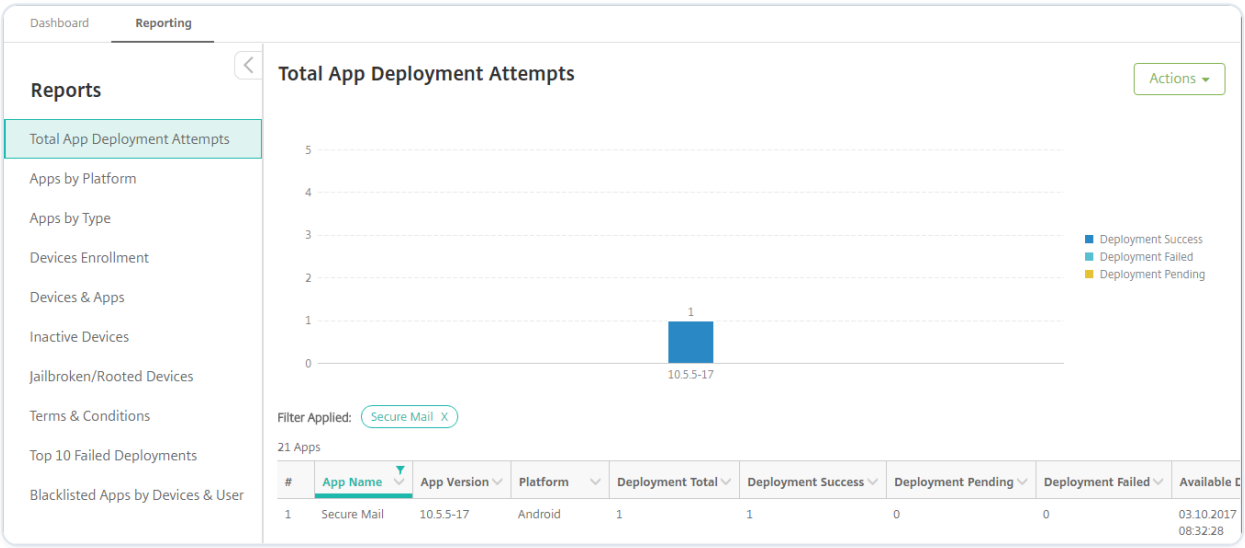
Para gerar um relatório

1. No console do XenMobile, clique em **Analisar > Relatórios**. A página **Relatórios** é exibida.
2. Clique no relatório que você deseja gerar.

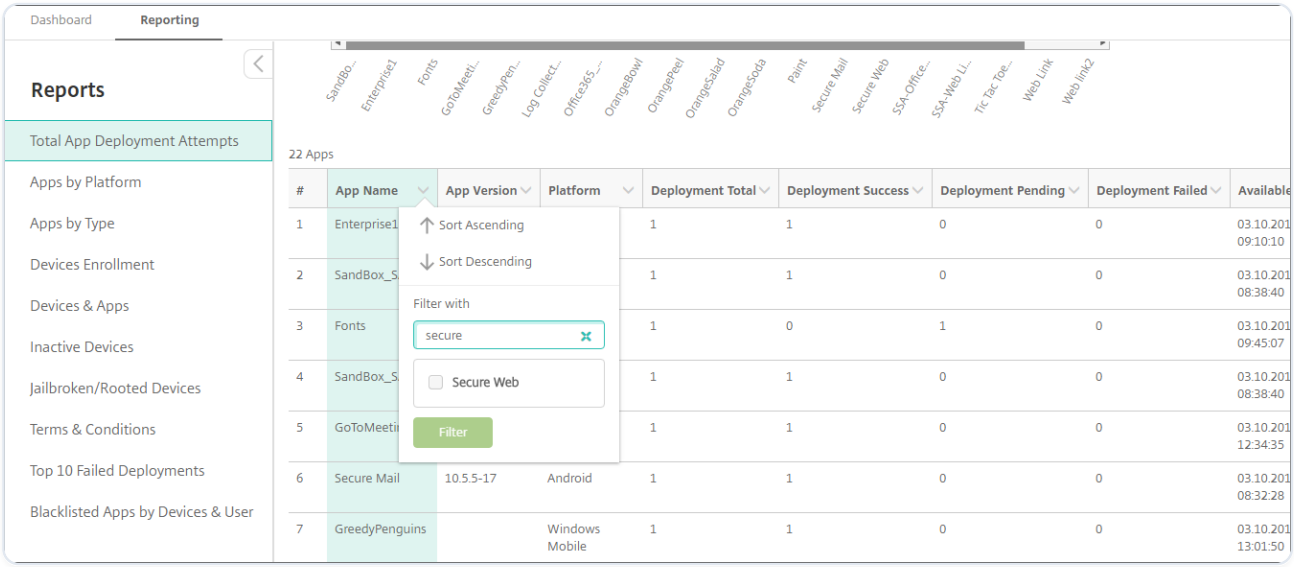


Para ver mais detalhes de um relatório

1. Clique nas áreas do gráfico para detalhar e ver informações mais detalhadas.

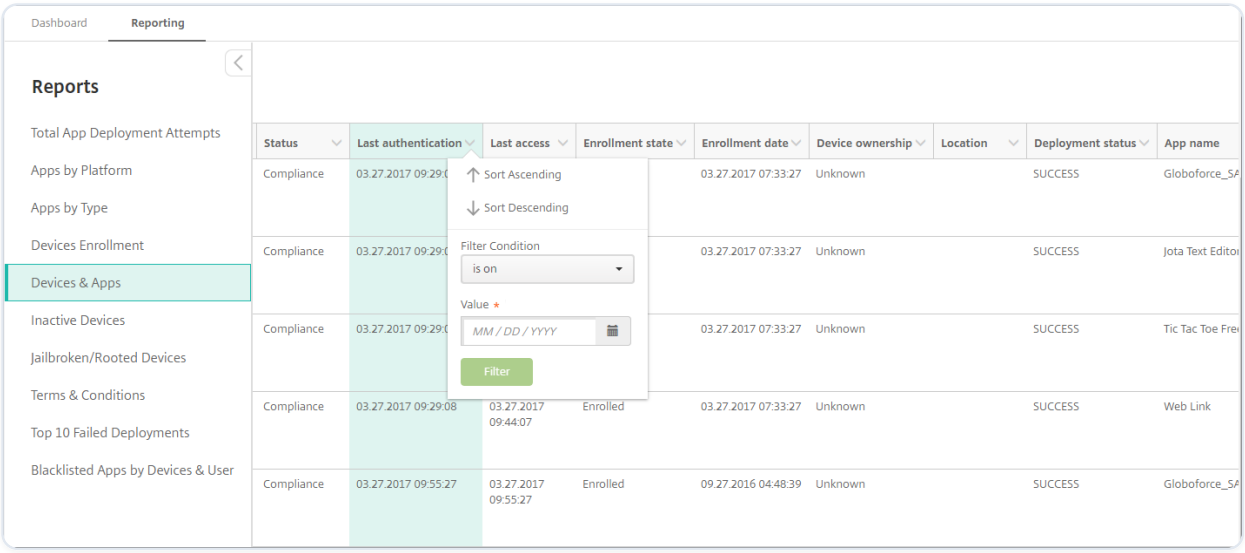


Para classificar, filtrar ou pesquisar uma coluna da tabela, clique no cabeçalho da coluna

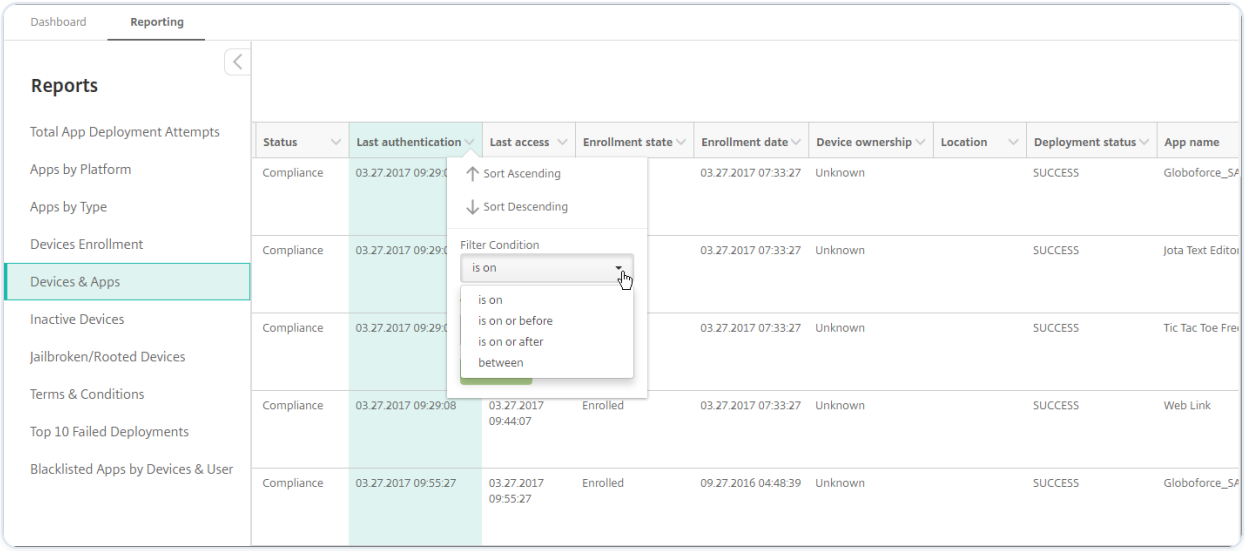


Para filtrar o relatório por data

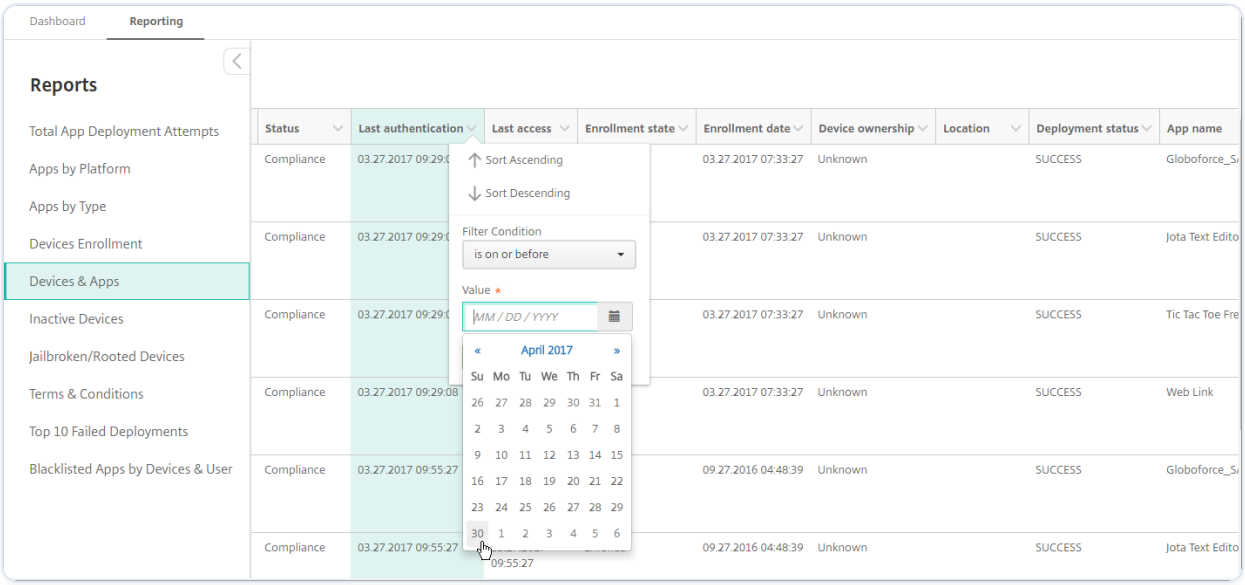
1. Clique em um cabeçalho de coluna para ver as configurações de filtro.



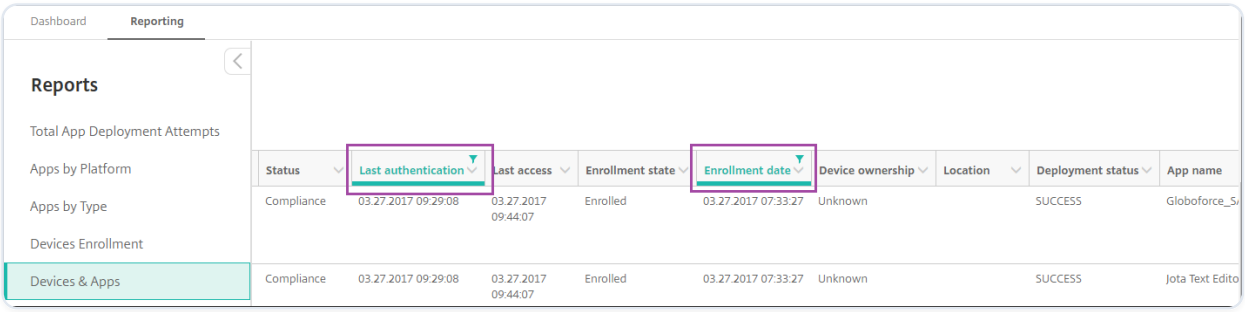
2. Em **Condição de Filtro**, escolha como você deseja restringir as datas relatadas.



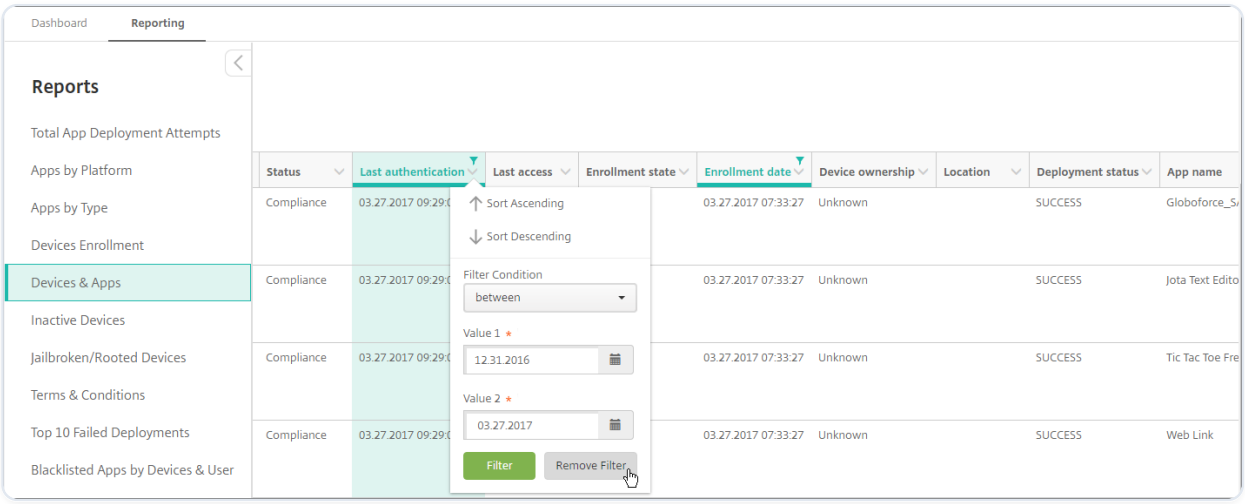
3. Use o seletor de data para especificar as datas.



4. Uma coluna com um filtro de data é exibida conforme o exemplo a seguir.

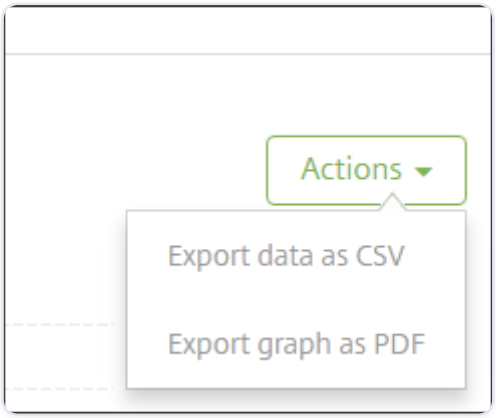


5. Para remover um filtro, clique no cabeçalho da coluna e, em seguida, clique em **Remover Filtro**



Para exportar um gráfico ou tabela

- Para exportar o gráfico no formato PDF, clique em **Ações** e depois em **Exportar gráfico como PDF**.
- Para exportar os dados da tabela no formato CSV, clique em **Ações** e depois em **Exportar dados como CVS**.



Importante:

> Embora seja possível usar o SQL Server para criar relatórios personalizados, a Citrix® não recomenda esse método. A Citrix não publica o esquema e pode alterá-lo sem aviso prévio. Se você decidir seguir esse método de relatório, certifique-se de que as consultas SQL sejam executadas usando uma conta somente leitura. Uma consulta com vários JOINs que leva algum tempo para ser executada afeta o desempenho do XenMobile Server durante esse período.

Monitoramento SNMP

Você pode habilitar o monitoramento SNMP no XenMobile Server para permitir que os sistemas de monitoramento consultem e obtenham informações sobre seus nós XenMobile. As consultas usam parâmetros como Carga do Processador, Carga Média, Uso da Memória e Conectividade. Para obter mais informações sobre SNMP v3, como especificações de autenticação e criptografia, consulte a documentação oficial do SNMP para RFC 3414.

> **Nota:**

> O monitoramento SNMP v3 é compatível com o XenMobile Server 10.8 e versões posteriores.

> Você pode usar vários aplicativos de monitoramento que suportam o monitoramento SNMP, como o SCOM. Para obter detalhes sobre como configurar o SCOM, consulte este artigo da Central de Conhecimento de Suporte da Citrix.

Pré-requisitos

Configure as seguintes portas TCP:

- **Porta 161 (UDP):** Usada para tráfego SNMP usando o protocolo UDP. A origem é o gerenciador SNMP e o destino é o XenMobile.
- **Porta 162 (UDP):** Usada para enviar alertas de trap SNMP do XenMobile para o gerenciador SNMP. A origem é o XenMobile e o destino é o Gerenciador SNMP.

Para obter mais informações sobre a configuração de portas do XenMobile, consulte Requisitos de porta.

Para ver um diagrama arquitetônico de uma implantação local do XenMobile que inclui SNMP, consulte Arquitetura de Referência para Implantações Locais.

As etapas gerais para configurar o SNMP são as seguintes.

1. **Adicionar usuários:** Os usuários herdam a permissão para receber traps e monitorar o XenMobile Server.
2. **Adicionar um Gerenciador SNMP para receber traps:** Traps são alertas que o XenMobile gera quando seu nó XenMobile excede o limite máximo definido pelo usuário.
3. **Configurar o gerenciador SNMP para interagir com o XenMobile:** O XenMobile Server usa certas bases de informações de gerenciamento (MIBs) para realizar operações. Você baixa as MIBs na página **Configurações > Configuração SNMP** no console do XenMobile. Em seguida, você importa as MIBs para o gerenciador SNMP usando um importador de MIB.

   > **Nota:**
   >
   > Cada gerenciador SNMP tem seu próprio importador MIB.

4. **Habilitar traps:** Você habilita traps no console do XenMobile e define os intervalos e limites com base no seu ambiente.
5. **Visualizar traps no gerenciador SNMP de terceiros:** Para visualizar traps, verifique o gerenciador SNMP. Em alguns gerenciadores, no entanto, você pode configurar as definições para habilitar notificações fora do gerenciador. Você pode configurar as notificações para aparecer, por exemplo, em e-mail.

Você pode gerar os seguintes traps do XenMobile.

Nome do trap: Carga do processador

- **ID do objeto de monitoramento (OID):** .1.3.6.1.2.1.25.3.3.1.2
- **Descrição:** Monitora a carga da CPU do sistema para o intervalo definido pelo usuário. Se a carga exceder o valor limite personalizado, o XenMobile gera o trap SNMP.

Nome do trap: Carga média por um minuto

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.2021.10.1.5.1
- **Descrição:** Monitora a carga média do sistema durante um período de um minuto para o intervalo definido pelo usuário. Se a carga média exceder o valor limite personalizado, o XenMobile gera o trap SNMP.

Nome do trap: Carga média por cinco minutos

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.2021.10.1.5.2
- **Descrição:** Monitora a carga média do sistema durante um período de cinco minutos para o intervalo definido pelo usuário. Se a carga média exceder o valor limite personalizado, o XenMobile gera o trap SNMP.

Nome do trap: Carga média por 15 minutos

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.2021.10.1.5.3
- **Descrição:** Monitora a carga média do sistema durante um período de 15 minutos para cada intervalo definido pelo usuário. Se a carga média exceder o valor limite personalizado, o XenMobile gera a trap SNMP.

Nome da trap: Memória total disponível

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.2021.4.11
- **Descrição:** Monitora a memória disponível para cada intervalo definido pelo usuário. Se a memória disponível cair abaixo do valor limite personalizado, o XenMobile gera a trap SNMP. Observação: A memória total disponível inclui RAM e memória de troca (memória virtual). Para recuperar a memória de troca total, você pode consultar usando o OID SNMP .1.3.6.1.4.1.2021.4.3. Para recuperar a memória de troca disponível, você pode consultar usando o OID SNMP .1.3.6.1.4.1.2021.4.4

Nome da trap: Armazenamento em disco total usado

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.2021.9.1.9.1
- **Descrição:** Monitora o armazenamento em disco do sistema para cada intervalo definido pelo usuário. Se o armazenamento em disco exceder o valor limite personalizado, o XenMobile gera a trap SNMP.

Nome da trap: Uso da memória heap Java

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Descrição:** Monitora o uso da memória heap da máquina virtual Java (JVM) do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor limite personalizado, o XenMobile gera a trap SNMP.

Nome da trap: Uso do metaspace Java

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.2.5.0

- **Descrição:** Monitora o uso do metaspace Java do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor limite, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade LDAP

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Descrição:** Monitora a conectividade entre o servidor LDAP e o nó XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade DNS

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Descrição:** Monitora a conectividade entre o servidor DNS e o nó XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor Google Store

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Descrição:** Monitora a conectividade entre o servidor Google Store e o nó XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade da Windows Tab Store

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **Descrição:** Monitora a conectividade entre o servidor Tab Store e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor de token de segurança do Windows

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Descrição:** Monitora a conectividade entre o servidor de token de segurança do Windows e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor de notificação do Windows

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Descrição:** Monitora a conectividade entre o servidor de Notificação do Windows e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor Apple Push Notification (APNs)

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Descrição:** Monitora a conectividade entre os APNs e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor Apple Feedback

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Descrição:** Monitora a conectividade entre o servidor Apple Feedback e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor Apple Store

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Descrição:** Monitora a conectividade entre o servidor Apple Store e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do banco de dados do XenMobile

- **ID do objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **Descrição:** Monitora a conectividade entre o Banco de Dados do XenMobile e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do servidor Firebase Cloud Messaging

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **Descrição:** Monitora a conectividade entre o servidor Firebase Cloud Messaging e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do Citrix License Server

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Descrição:** Monitora a conectividade entre o Citrix License Server e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do Citrix Gateway

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0

- **Descrição:** Monitora a conectividade entre o Citrix Gateway e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade inter-nós do XenMobile

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Descrição:** Monitora a conectividade entre os nós do cluster XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

Nome da trap: Conectividade do serviço de nó Tomcat do XenMobile

- **ID de objeto de monitoramento (OID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Descrição:** Monitora a conectividade entre o serviço de nó Tomcat do XenMobile e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a trap SNMP.

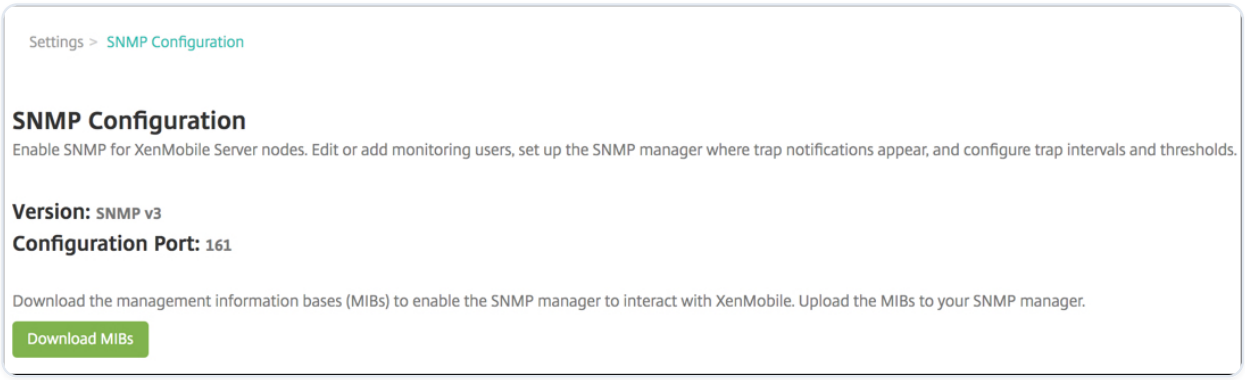
Para o melhor desempenho do servidor ao configurar os limites de SNMP, leve em consideração os seguintes fatores:

- Frequência das chamadas
- Dados de trap a serem coletados e as verificações de limite
- O mecanismo de comunicação entre nós
- Frequência das verificações de conectividade
- Tempos limite em qualquer falha durante as verificações

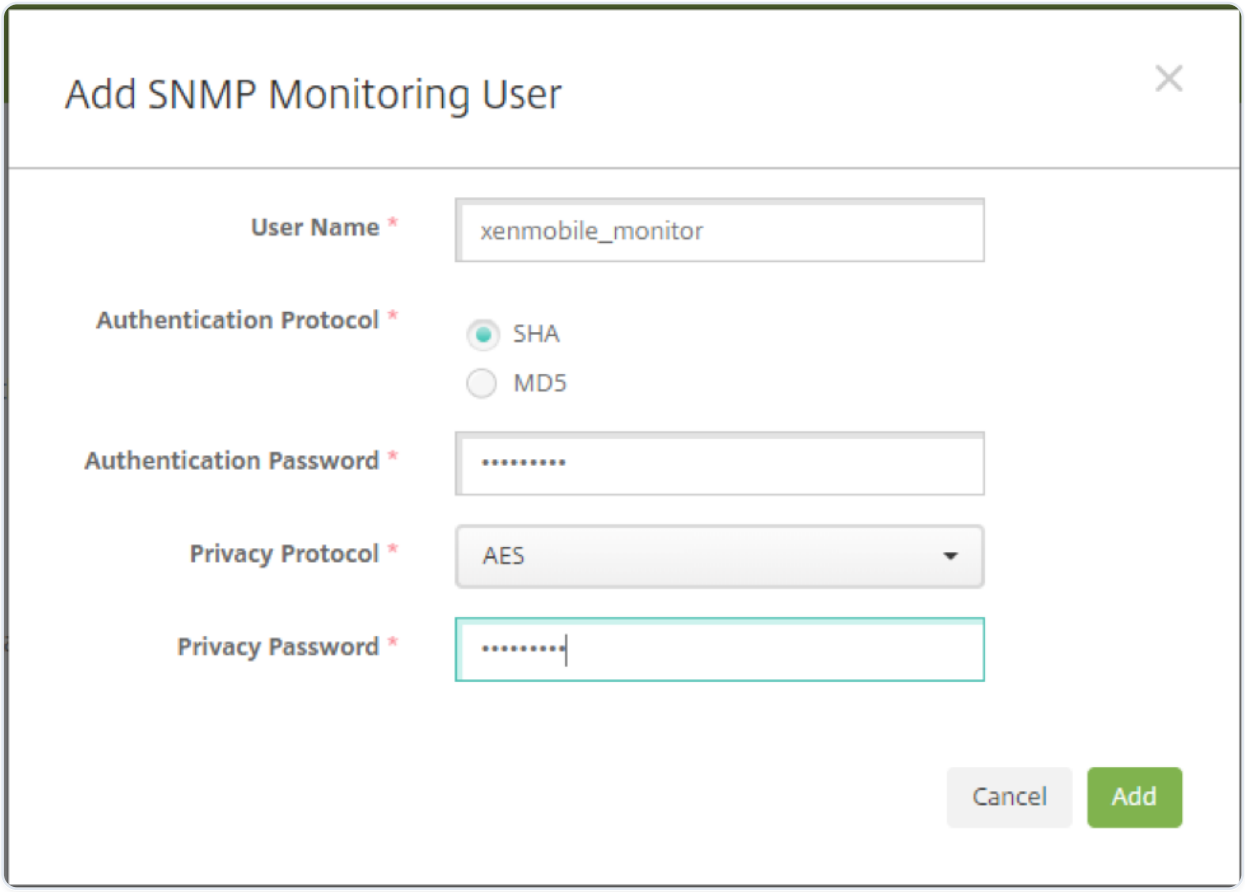
Para adicionar usuários SNMP

Os usuários SNMP interagem com os gerentes SNMP e recebem traps.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Monitoramento**, clique em **Configuração SNMP**. A página **Configuração SNMP** é exibida.



3. Em **Usuários de Monitoramento SNMP**, clique em **Adicionar**.
4. Na caixa de diálogo **Adicionar Usuário de Monitoramento SNMP**, configure as seguintes definições:



Nome de Usuário: O nome de usuário usado para fazer logon no gerente SNMP. Embora você possa usar caracteres alfanuméricos, sublinhado e hífens, você não pode usar espaços e outros caracteres especiais para seu nome de usuário.

> **Nota:**
>
> Você não pode adicionar o nome de usuário "xmsmonitor" porque o XenMobile reserva o nome para uso interno.

Protocolo de Autenticação:

- **SHA** (Recomendado)
- **MD5**

Senha de Autenticação: Digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

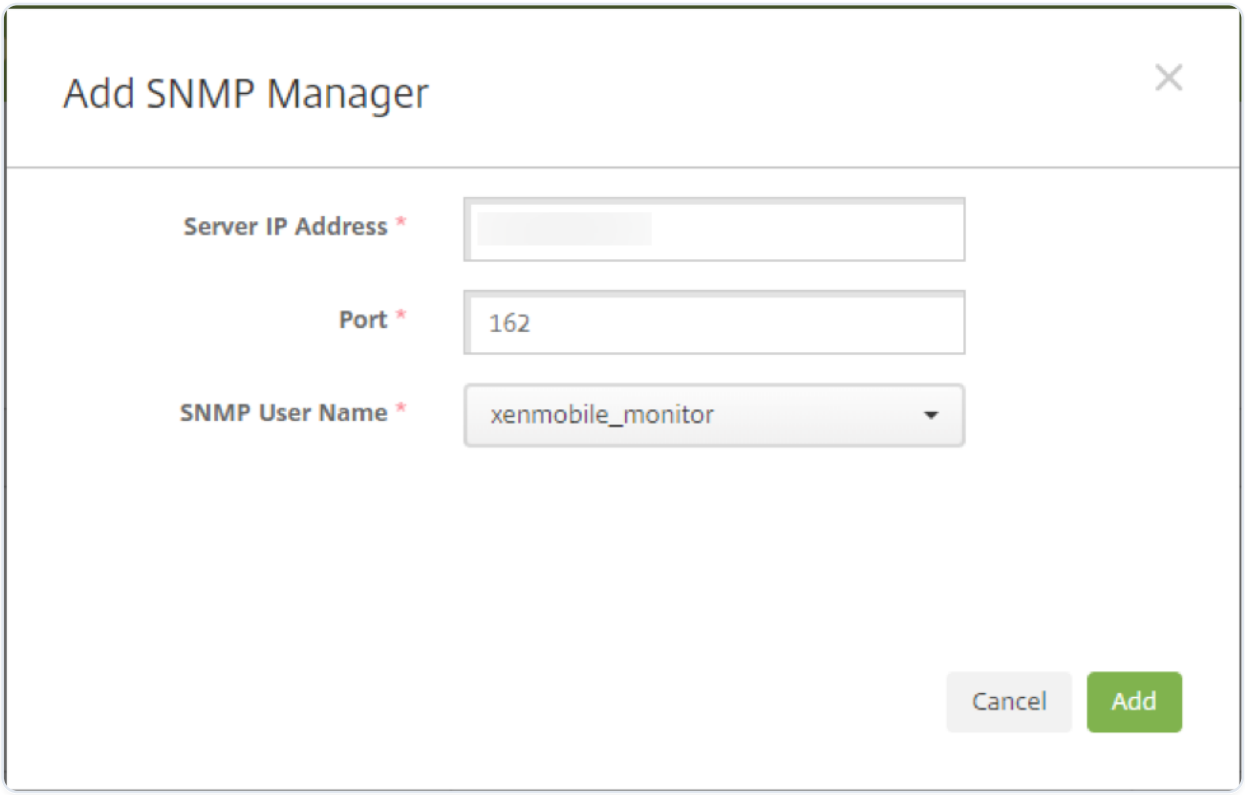
Protocolo de Privacidade:

- **DES**
- **AES 128** (Recomendado)

Senha de Privacidade: Digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

Para adicionar um gerenciador SNMP

1. Em **Gerenciadores SNMP**, clique em **Adicionar**.
2. Na caixa de diálogo **Adicionar Gerenciador SNMP**, configure as seguintes definições:



Endereço IP do Servidor: Digite o endereço IP do gerenciador SNMP.

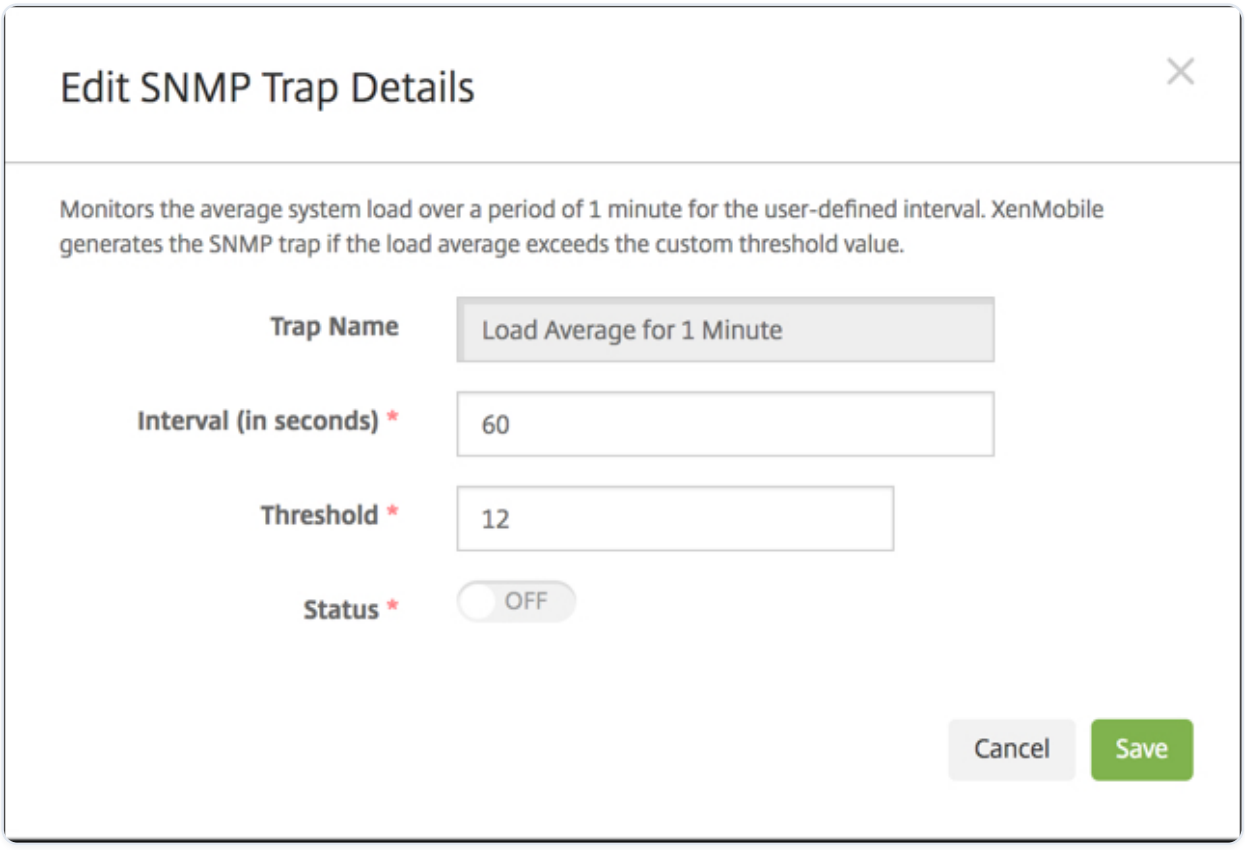
Porta: Altere o número da porta, se necessário. O padrão é 162.

Nome de Usuário SNMP: Selecione o nome de um usuário com acesso ao gerenciador.

Para habilitar e configurar traps SNMP

Para ajudar a determinar as configurações de trap apropriadas para seu ambiente, consulte Escalabilidade e desempenho. Por exemplo, para monitorar a Média de Carga do XenMobile por um minuto, você pode habilitar a Média de Carga por 1 Minuto e fornecer um valor de limite. Se a Média de Carga do Servidor XenMobile por 1 Minuto exceder o limite especificado, você receberá um trap nos gerenciadores SNMP configurados.

1. Para habilitar traps individuais, faça um dos seguintes:
   - Selecione a caixa de seleção ao lado do parâmetro e, em seguida, clique em **Habilitar**.
   - Para habilitar todos os traps na lista, selecione a caixa de seleção na parte superior e, em seguida, clique em **Habilitar**.
2. Para editar um trap, selecione o parâmetro e, em seguida, clique em **Editar**.
3. Na caixa de diálogo **Editar Detalhes do Trap SNMP**, você pode editar os valores de limite para traps individuais.



Nome do Trap: O nome do trap. Você não pode editar este campo.

Intervalo (em segundos): O intervalo permitido é de 60 a 86400 (24 horas).

Limite: Você pode alterar o limite apenas para os seguintes traps:

- Carga do Processador
- Média de Carga por 1 Minuto
- Média de Carga por 5 Minutos
- Carga Média por 15 Minutos
- Memória Total Disponível
- Armazenamento em Disco Total Usado
- Uso da Memória Heap do Java
- Uso do Metaspace do Java

Status: Selecione **ATIVADO** para habilitar o monitoramento SNMP para a trap. Selecione **DESATIVADO** para desabilitar o monitoramento.

Para obter informações mais úteis sobre o monitoramento do XenMobile usando SNMP, consulte esta publicação do blog.

Pacotes de suporte

Para relatar um problema à Citrix ou solucionar um problema, crie um pacote de suporte. Em seguida, carregue o pacote de suporte para o Citrix Insight Services (CIS).

Por padrão, um pacote de suporte inclui um máximo de 100 arquivos de backup dos seguintes arquivos. O tamanho de arquivo padrão para esses arquivos é de 10 MB.

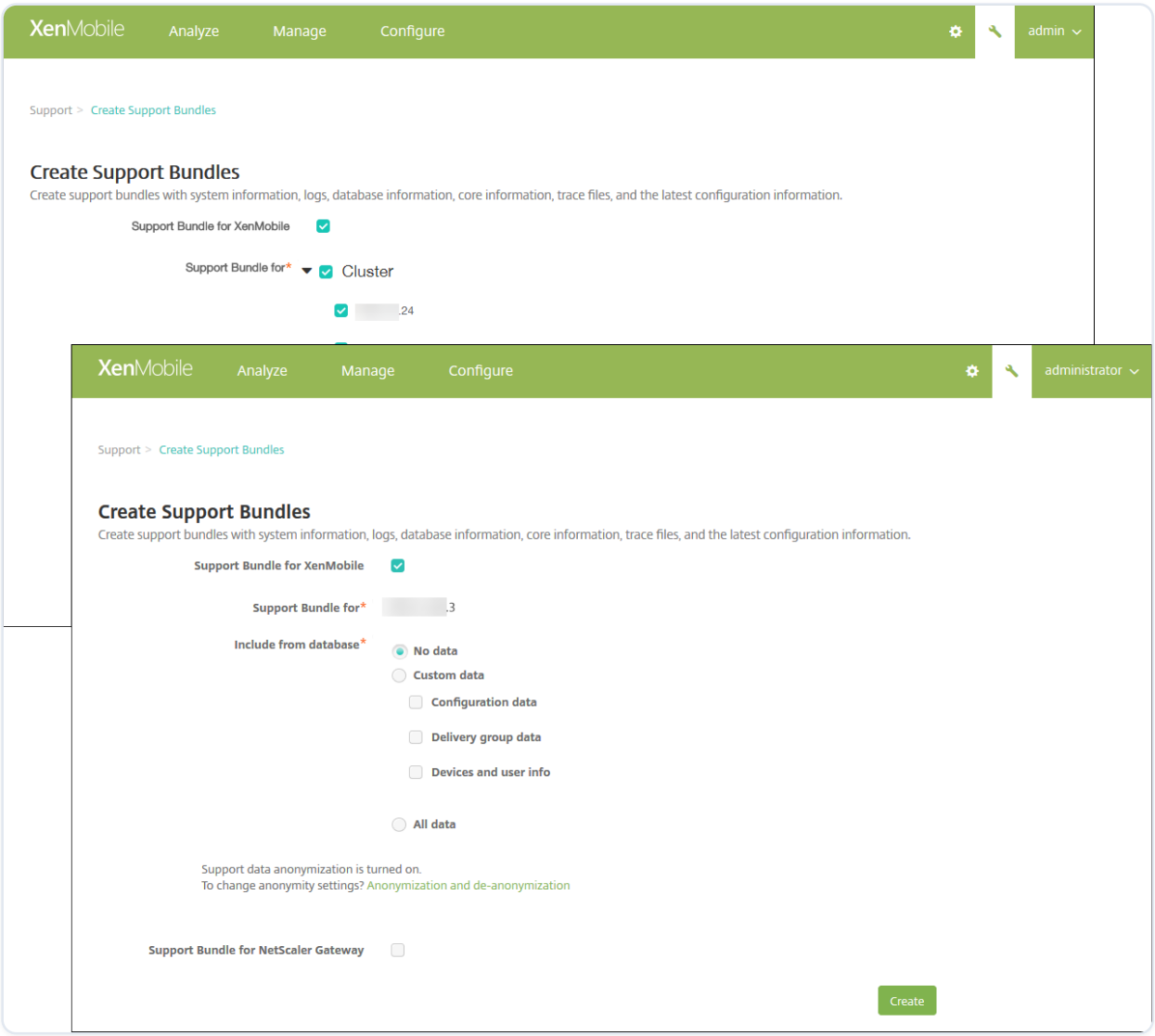
- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Quando o pacote de suporte inclui 100 arquivos de log de cada uma dessas categorias, o arquivo de log é substituído. Se você configurar um número máximo menor de arquivos de log, o XenMobile® excluirá imediatamente os arquivos de log extras para esse nó. Para configurar o número de arquivos de log, vá para **Solução de problemas e suporte > Configurações de log**.

Para criar um pacote de suporte:

1. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito. A página **Suporte** é exibida.

2. Na página **Suporte**, clique em **Criar pacotes de suporte**. A página **Criar pacotes de suporte** é exibida. Se o seu ambiente XenMobile tiver nós em cluster, todos os nós serão mostrados.



3. Certifique-se de que a caixa de seleção **Pacote de suporte para XenMobile** esteja selecionada.
4. Se o seu ambiente XenMobile tiver nós em cluster, em **Pacote de suporte para**, você poderá selecionar todos os nós ou qualquer combinação de nós dos quais extrair dados.
5. Em **Incluir do banco de dados**, faça um dos seguintes:

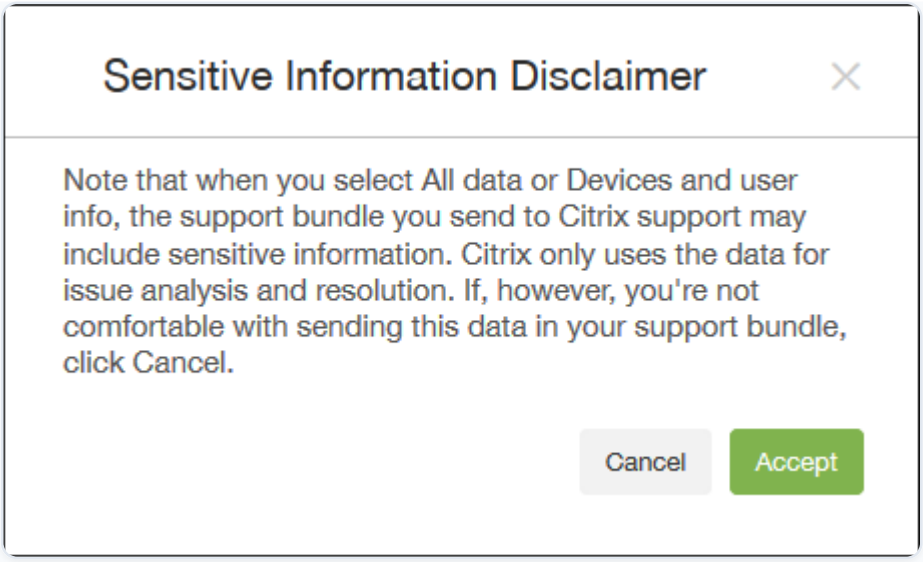
   - Clique em **Nenhum dado**.
   - Clique em **Dados personalizados**. Por padrão, todas essas opções são selecionadas.

     - **Dados de configuração:** Inclui configurações de certificado e políticas do gerenciador de dispositivos.
     - **Dados do grupo de entrega:** Inclui informações do grupo de entrega de aplicativos contendo tipos de aplicativos e detalhes da política de entrega de aplicativos.

- **Informações de dispositivos e usuários:** Inclui políticas de dispositivo, aplicativos, ações e grupos de entrega.

- Clique em **Todos os dados**.

> **Observação:**
>
> Se você escolher **Informações de dispositivos e usuários** ou **Todos os dados**, e este for o primeiro pacote de suporte que você criou, a caixa de diálogo **Aviso de Isenção de Responsabilidade de Informações Confidenciais** será exibida. Leia o aviso de isenção de responsabilidade e clique em **Aceitar** ou **Cancelar**. Se você clicar em **Cancelar**, o pacote de suporte não poderá ser carregado para a Citrix. Se você clicar em **Aceitar**, poderá carregar o pacote de suporte para a Citrix e não verá o aviso de isenção de responsabilidade na próxima vez que criar um pacote de suporte que inclua dados de dispositivo ou usuário.

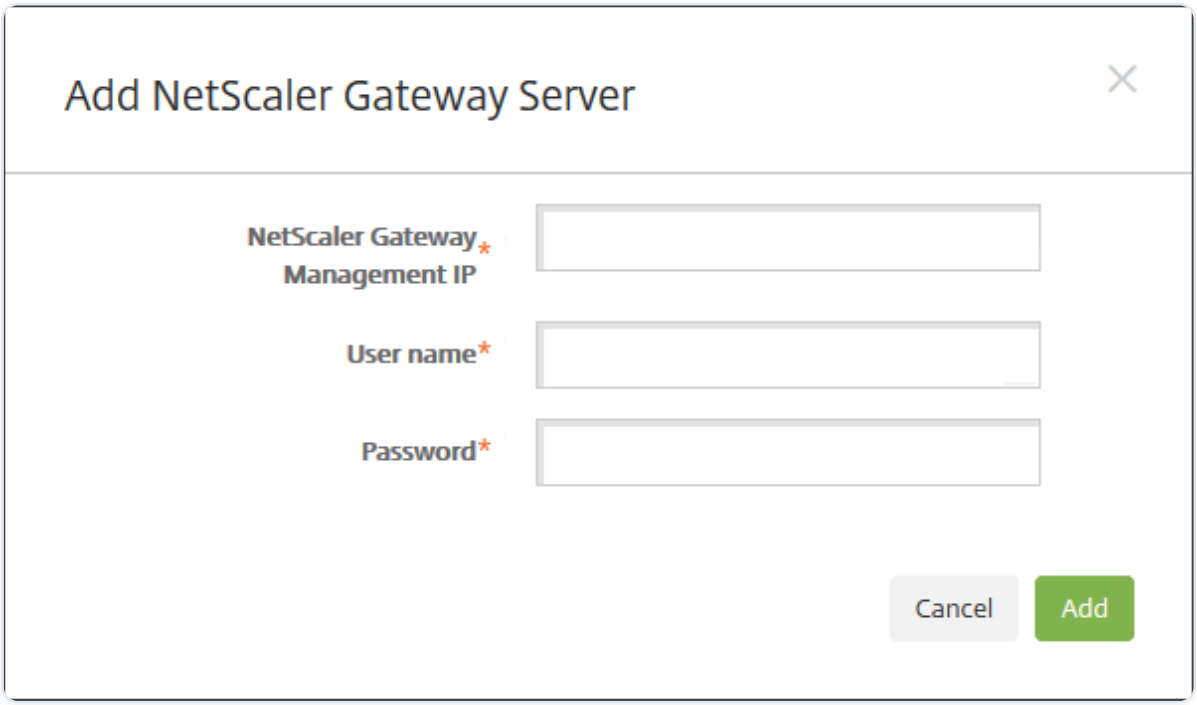


6. A opção **A anonimização de dados de suporte está ativada**, indica que a configuração padrão é anonimizar os dados. A anonimização de dados significa que dados confidenciais de usuário, servidor e rede são tornados anônimos em pacotes de suporte.

   Para alterar essa configuração, clique em **Anonimização e desanonimização**. Para obter mais informações sobre a anonimização de dados, consulte Anonimizando dados em pacotes de suporte.

7. Para incluir pacotes de suporte do Citrix Gateway: Selecione a caixa de seleção **Pacote de Suporte para Citrix Gateway** e faça o seguinte:

a. Clique em **Adicionar**. A caixa de diálogo **Adicionar Servidor Citrix Gateway** será exibida.



b. Em **IP de Gerenciamento do Citrix Gateway**, digite o endereço IP de gerenciamento do Citrix ADC para o Citrix Gateway do qual você deseja extrair os dados do pacote de suporte.

> **Observação:**
>
> Se você estiver criando um pacote de um servidor Citrix Gateway que já foi adicionado, o endereço IP é fornecido.

c. Em **Nome de usuário** e **Senha**, digite as credenciais de usuário necessárias para acessar o servidor que executa o Citrix Gateway.

> **Observação:**
>
> Se você estiver criando um pacote de um servidor Citrix Gateway que já foi adicionado, o nome de usuário é fornecido.

8. Clique em **Adicionar**. O novo pacote de suporte do Citrix Gateway é adicionado à tabela.
9. Repita a Etapa 7 para adicionar mais pacotes de suporte do Citrix Gateway.

10. Clique em **Criar**. O pacote de suporte é criado e dois novos botões **Carregar para CIS** e **Baixar para Cliente** aparecem.

Carregando Pacotes de Suporte para o Citrix Insight Services

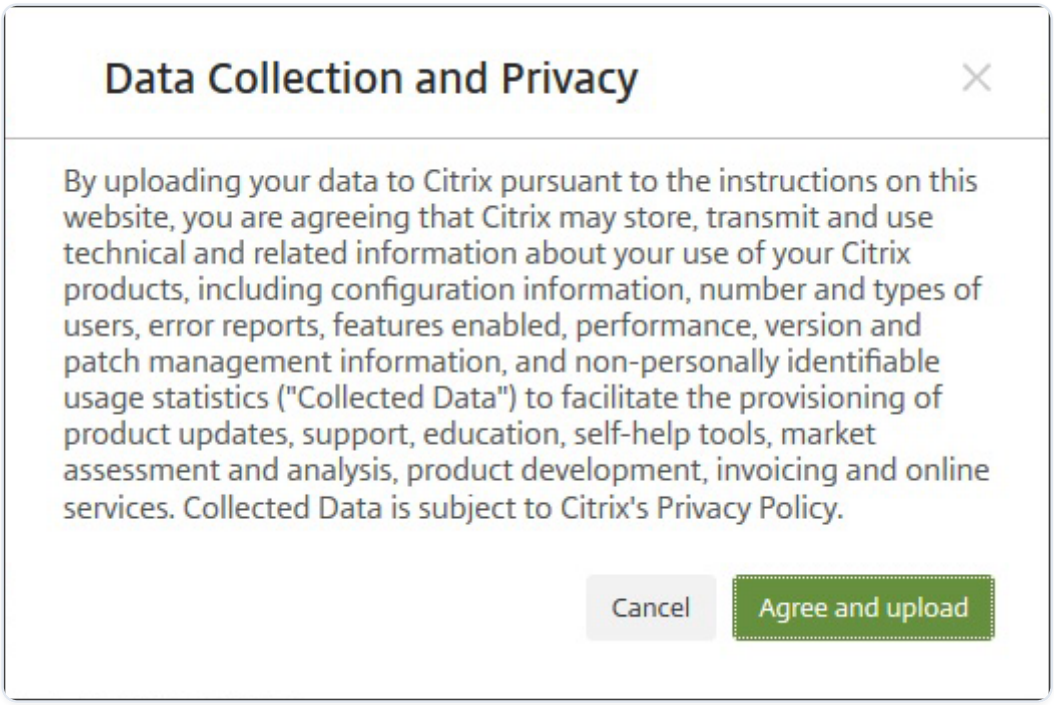
Após criar um pacote de suporte, você pode carregar o pacote para o Citrix Insight Services (CIS) ou baixar o pacote para o seu computador.

O carregamento do XenMobile para o CIS é feito por meio de uma conexão SSL de saída. Abra a porta 443 para o endereço IP do servidor CIS (52.88.24.76, 52.88.118.220, 52.11.72.119). Se você tiver um proxy para tráfego HTTPS, verifique se o proxy pode alcançar o endereço IP do servidor CIS.

Estas etapas mostram como carregar o pacote para o CIS. Você precisa de um ID e senha do My Citrix para carregar para o CIS.

1. Na página **Criar Pacotes de Suporte**, clique em **Carregar para CIS**. A caixa de diálogo **Carregar para Citrix Insight Services (CIS)** é exibida.
2. Em **Nome de Usuário**, digite seu ID do My Citrix.
3. Em **Senha**, digite sua senha do My Citrix.
4. Se você deseja conectar este pacote a um número de solicitação de serviço existente, selecione a caixa de seleção **Associar com SR#** e, nos dois novos campos que aparecerem, faça o seguinte:
   - Em **SR#**, digite o número de solicitação de serviço de oito dígitos ao qual você deseja associar este pacote.
   - Em **Descrição do SR**, digite uma descrição do SR.
5. Clique em **Carregar**.

   Se esta for a primeira vez que você carrega um pacote de suporte para o CIS, e você não criou uma conta no CIS por meio de outro produto e aceitou o contrato de Coleta de Dados e Privacidade, a seguinte caixa de diálogo aparecerá; você deve aceitar o contrato antes que o carregamento possa começar. Se você tiver uma conta no CIS e já tiver aceitado o contrato, o pacote de suporte será carregado imediatamente.



6. Leia o contrato e clique em **Concordar e carregar**. O pacote de suporte é carregado.

Baixando pacotes de suporte para o seu computador

Depois de criar um pacote de suporte, você pode carregá-lo para o CIS ou baixá-lo para o seu computador. Se você quiser solucionar o problema por conta própria, baixe o pacote de suporte para o seu computador.

Na página **Criar Pacotes de Suporte**, clique em **Baixar para Cliente**. O pacote é baixado para o seu computador.

O pacote de suporte possui arquivos de valor analítico variável. Consulte a tabela a seguir para obter uma lista de arquivos e seu valor analítico.

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
DbDump.json	Despejo de Banco de Dados JSON	Informações de Usuários/ Dispositivos/ Aplicativos	Alta
Garbage.html	Arquivo HTML	Coletor de lixo Java	Baixa
MemoryInfo.html	Arquivo HTML	Uso de memória - uso de memória relacionado ao Java	Alta

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
MultiNodeClusterInfo.html	Arquivo HTML	Configuração do cluster	Alta
Patches.html	Arquivo HTML	Informações de patch. Melhor para xmspatches.txt	Alta
pg_dump0.sql	Dump PG	Dump da instância padrão do Postgres	Média
rt_db/*	Cópia do BD (redundante, esta é uma representação binária de pg_dump0.sql)		N/A
sas_config/c3p0.properties	Arquivo de propriedades	Propriedades de configuração do BD C3P0	Médio
sas_config/catalina.policy	arquivo de política	Políticas do Servidor Web Catalina - Os arquivos não mudam	Baixo
sas_config/catalina.properties	Arquivo de propriedades	Propriedades do Servidor Web Catalina - Os arquivos não mudam	Baixo
sas_config/ew-config.properties	Arquivo de propriedades	Informações sobre a configuração do servidor XM	Alto
sas_config/ew-config-reloadable.properties	Arquivo de propriedades	Informações do modelo de segurança	Alta
sas_config/hazelcast.xml	Arquivo XML	Logs do Hazelcast - Não creio que seriam de muita utilidade.	Baixa

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
sas_config/pki.xml	Arquivo XML	Poderia ser usado para determinar se um servidor PKI de terceiros está em uso.	Alta
sas_config/ push_services.xml	Arquivo XML	Serviços de Push - Os arquivos não mudam	Baixa
sas_config/ server.xml	Arquivo XML	Informações de cifra aqui - Relacionado à segurança	Alta
sas_config/ sftu_config/ AppC.properties	Arquivo de propriedades	Propriedades do AppC - Os arquivos não mudam	Baixa
sas_config/ sftu_config/ catalina.policy	Arquivo de política	Políticas do Catalina - Os arquivos não mudam	Baixa
sas_config/ sftu_config/ catalina.properties	Arquivo de propriedades	Propriedades do Catalina - Os arquivos não mudam	Baixa
sas_config/ sftu_config/ logging.properties	Arquivo de propriedades	Propriedades de registro - Os arquivos não mudam	Baixo
sas_config/ sftu_config/ server.xml	Arquivo XML	Informações de cifra aqui - Relacionado à segurança	Alto
sas_config/ sftu_config/ server_migration.xml	Arquivo XML	Informações de migração	Alto
sas_config/ sftu_config/ server_sftu.xml	Arquivo XML	Configurações do usuário iniciante	Alto

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
sas_config/sftu_config/tomcat-users.xml	Arquivo XML	Usuários TomCat - Os arquivos não mudam	Baixo
sas_config/sftu_config/web.xml	Arquivo XML	Web - Os arquivos não mudam	Baixo
sas_config/sftu.properties	Arquivo de propriedades	Propriedades de configuração SFTU	Alto
sas_config/variables.xml	Arquivo XML	Variáveis - Arquivos não mudam	Baixo
sas_config/web.xml	Arquivo XML	Informações relacionadas ao servidor web	Médio
sas_log/AdminAuditLogFile.log	Arquivo de Log do Linux	Quaisquer alterações de configuração	Alto
sas_log/create_sb_output.sh	Arquivo de Log do Linux	Saída do comando de geração de suporte	Baixo
sas_log/DebugLogFile.log	Arquivo de Log do Linux	Log de todos os recursos	Alta
sas_log/HibernateStats.log	Arquivo de Log do Linux	Log de estatísticas do Hibernate	Baixa
sas_log/kafka-consumer.log	Arquivo de Log do Linux	Log do Kafka	Baixa
sas_log/kafka-server.log	Arquivo de Log do Linux	Log do Kafka	Baixa
sas_log/kafka-topics.log	Arquivo de Log do Linux	Log do Kafka	Baixo

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
sas_log/LPE.log	Arquivo de Log do Linux	Log LPE	Baixo
sas_log/migration.log	Arquivo de Log do Linux	Saída do processo de migração	Médio
sas_log/PlatformAuditLogFile.log	Arquivo de Log do Linux	Informações de nível de auditoria de backend	Alta
sas_log/PlatformDebugLogFile.txt	Arquivo de texto	Logs relacionados ao servidor de backend	Alta
sas_log/postgres.log	Arquivo de log do Linux	Logs do PostGres	Média
sas_log/SFTU.log	Arquivo de log do Linux	Log do SFTU	Média
sas_log/tc1/catalina.log	Arquivo de log do Linux	Log do Catalina	Baixo
sas_log/tc1/console	Arquivo de Log do Linux	Console	Baixo
sas_log/tc1/host-manager.log	Arquivo de Log do Linux	Gerenciador de Host	Baixo
sas_log/tc1/localhost.log	Arquivo de Log do Linux	LocalHost	Baixo
sas_log/updates.log	Arquivo de Log do Linux	Saída do processo de aplicação de patches	Médio
sas_log/UserAuditLogFile.log	Arquivo de Log do Linux	Ações do usuário	Alto
sas_log/zookeeper.txt	Arquivo de texto	Log do Zookeeper	Baixo

NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
snmp/snmpd_etc_netsnmp.conf	Arquivo de propriedades	Propriedades de configuração SNMP	Baixo
snmp/snmpd_privileges.conf	Arquivo de propriedades	Propriedades de configuração SNMP	Baixo
sys_info/arp_entries.txt	Arquivo de texto	Entradas ARP no servidor XMS	Médio
sys_info/chrony.txt	Arquivo de texto	Log do Chrony	Baixo
sys_info/diskspace_usage.txt	Arquivo de texto	Uso do espaço em disco	Alto
sys_info/firewall_rules.txt	Arquivo de texto	Regras de firewall definidas no XMS	Médio
sys_info/interface_config.txt	Arquivo de texto	Saída de comando do sistema	Médio
sys_info/net_connections.txt	Arquivo de texto	Saída de comando do sistema	Médio
sys_info/root_account_info.txt	Arquivo de texto	Saída de comando do sistema	Médio
sys_info/routing_table.txt	Arquivo de texto	Alto valor	Alto
sys_info/running_process.txt	Arquivo de texto	Alto valor	Alto
sys_info/top.txt	Arquivo de texto	Saída de comando do sistema	Médio
ThreadDump.html	Arquivo HTML	Não é mais usado.	Baixo
ThreadDumpV2.html	Arquivo HTML	Rastreamentos de pilha de threads etc.	Médio

XENMOBILE® SERVER

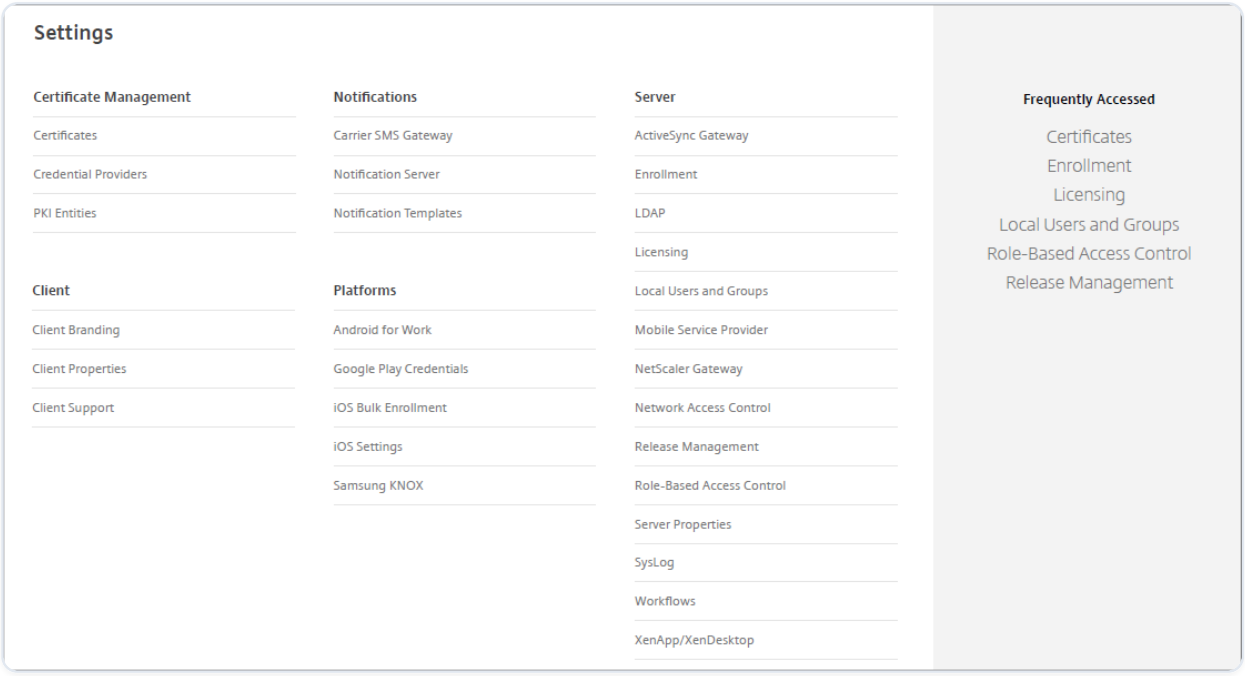
NOME DO ARQUIVO	TIPO	DESCRIÇÃO	VALOR
var_log/auth.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/boot.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/btmp	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/daemon.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/kern.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/lastlog	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/mail.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/sys.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/user.log	Arquivo de Log do Linux	Log de Nível de SO	Médio
var_log/wtmp	Arquivo de Log do Linux	Log de nível de SO	Médio
version.txt	arquivo de texto	Versão do servidor XM	Médio
XENMOBILE-`<IP Address>`-ConnectivityCheckResults.xml	arquivo XML	Resultados da Verificação de Conectividade no servidor XMS	Médio
xmspatches.txt	Arquivo de texto	Informações do patch.	Alto

Opções de suporte e Suporte Remoto

Você pode fornecer um endereço de e-mail para os usuários entrarem em contato com a equipe de suporte. Quando os usuários solicitam assistência de seus dispositivos, eles veem o endereço de e-mail.

Você também pode configurar como os usuários enviam logs para o suporte técnico de seus dispositivos. Você pode configurar os logs para serem enviados diretamente ou por e-mail.

1. No console do XenMobile®, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.



2. Em **Cliente**, clique em **Suporte ao Cliente**. A página **Suporte ao Cliente** é exibida.
3. Configure as seguintes configurações:

   - **E-mail de suporte (suporte técnico de TI):** Digite o endereço de e-mail para o contato do seu suporte técnico de TI.
   - **Enviar logs do dispositivo para o suporte técnico de TI:** Selecione se os logs do dispositivo são enviados **diretamente** ou **por e-mail**. O padrão é **por e-mail**.
     - Quando você habilita **diretamente**, as configurações para Armazenar logs no ShareFile (agora chamado ShareFile) aparecem. Se você habilitar Armazenar logs no ShareFile, os logs serão enviados diretamente para o Citrix Files. Caso contrário, os logs são enviados para o XenMobile e, em seguida, enviados por e-mail para o suporte técnico. Além disso, a opção **Se o envio direto falhar, use e-mail** aparece, que é habilitada por padrão. Você pode desabilitar esta opção quando não quiser usar o e-mail do

cliente para enviar os logs para um problema de servidor. No entanto, se você desabilitar esta opção e ocorrer um problema de servidor, os logs não serão enviados.

- Quando você habilita **por e-mail**, o e-mail do cliente é sempre usado para enviar os logs.

4. Clique em **Salvar**.

Suporte Remoto

> **Nota:**

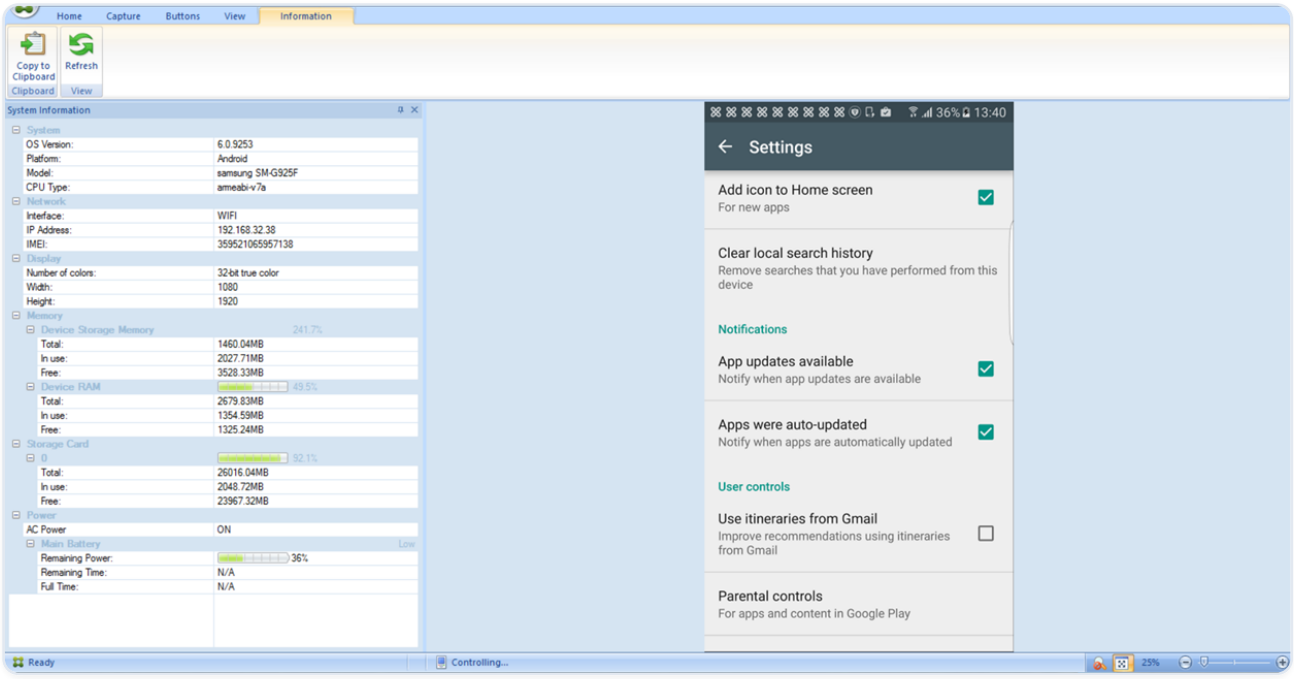
> O Suporte Remoto não está mais disponível para novos clientes a partir de January 1, 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá aprimoramentos ou correções.

> Para implantações locais do XenMobile Server: O suporte remoto permite que os representantes do seu help desk assumam o controle remoto de dispositivos móveis Android gerenciados. A transmissão de tela é suportada apenas em dispositivos Samsung Knox.

O suporte remoto não está disponível para implantações locais em cluster do XenMobile Server.

Durante uma sessão de controle remoto:

- Os usuários veem em seu dispositivo móvel um ícone indicando que uma sessão de controle remoto está ativa.
- Os usuários do Suporte Remoto veem a janela do aplicativo Suporte Remoto e uma janela de Controle Remoto que mostra uma renderização do dispositivo controlado.



Ao usar o Suporte Remoto, você pode fazer o seguinte:

- Fazer login remotamente em um dispositivo de usuário e controlar a tela. Os usuários podem observar você navegar na tela deles, o que também pode ser útil para fins de treinamento.
- navegar e reparar um dispositivo remoto em tempo real. Você pode alterar configurações, solucionar problemas do sistema operacional e desativar ou interromper aplicativos ou processos problemáticos.
- Isolar e conter ameaças antes que se espalhem para outros dispositivos móveis, desativando remotamente o acesso à rede, interrompendo processos maliciosos e removendo aplicativos ou malware.
- Ativar remotamente o toque do dispositivo e ligar para o telefone, para ajudar o usuário a localizar o dispositivo. Quando um usuário não consegue encontrar o dispositivo, você pode limpá-lo para garantir que seus dados confidenciais não sejam comprometidos.

O Suporte Remoto também permite que a equipe de suporte:

- Exibir uma lista de todos os dispositivos conectados em uma ou mais instâncias do XenMobile.
- Exibir informações do sistema, incluindo modelo do dispositivo, nível do sistema operacional, International Mobile Station Equipment Identity (IMEI), número de série, status da memória e bateria, e conectividade.
- Exibir os usuários e grupos do XenMobile.
- Executar o gerenciador de tarefas do dispositivo onde você pode exibir processos ativos, encerrar processos ativos e reiniciar o dispositivo móvel.

- Executar transferência remota de arquivos que inclui transferência bidirecional de arquivos entre dispositivos móveis e um servidor de arquivos central.
- Baixar e instalar programas de software em lote para um ou mais dispositivos móveis.
- Configurar as configurações de chave de registro remoto no dispositivo.
- Otimizar o tempo de resposta em redes celulares de baixa largura de banda usando o controle remoto da tela do dispositivo em tempo real.
- Exibir a interface do dispositivo para a maioria das marcas e modelos de dispositivos móveis. Exibir um editor de interface para adicionar novos modelos de dispositivos e mapear teclas físicas.
- Habilitar captura de tela do dispositivo, gravação e reprodução com a capacidade de capturar uma sequência de interações no dispositivo que cria um arquivo AVI de vídeo.
- Realizar reuniões ao vivo usando um quadro branco compartilhado, comunicações de voz baseadas em VoIP e bate-papo entre usuários móveis e pessoal de suporte.

Requisitos do Sistema de Suporte Remoto

O software de Suporte Remoto é instalado em computadores baseados em Windows que atendem aos seguintes requisitos. Para requisitos de porta, consulte Requisitos de Porta.

Plataformas suportadas:

- Intel Xeon/Pentium 4 -1 GHz mínimo Classe Workstation
- 512 MB de RAM mínimo
- 100 MB de espaço livre em disco mínimo

Sistemas operacionais suportados:

- Microsoft Windows 2003 Server Standard Edition ou Enterprise Edition SP1 ou posterior
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 ou posterior
- Microsoft Windows Vista SP1 ou posterior
- Microsoft Windows 10 ou Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

Para instalar o Remote Support a partir da linha de comando

Execute o seguinte comando:

```
*RemoteSupport*.exe /S
```

RemoteSupport é o nome do programa de instalação. Por exemplo:

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

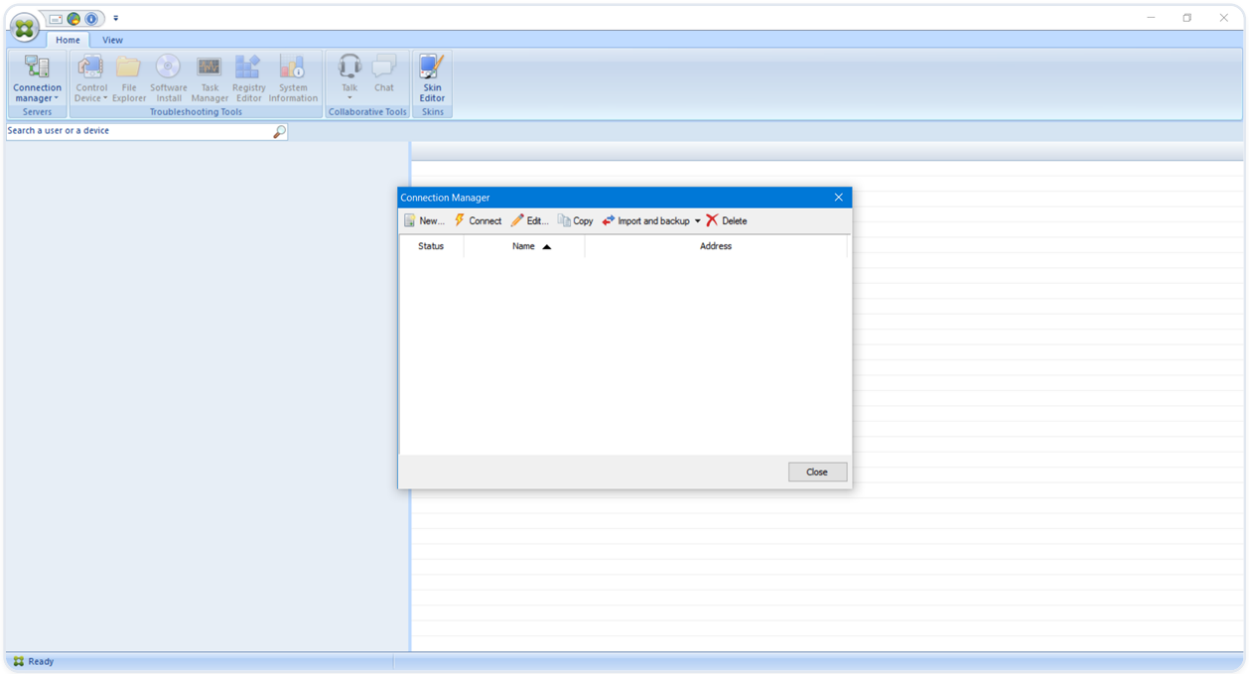
Você pode usar as seguintes variáveis ao instalar o software Remote Support:

- /S: para instalar o software Remote Support silenciosamente com os parâmetros padrão.
- /D=dir: para especificar um diretório de instalação personalizado.

Para conectar o Remote Support ao XenMobile

Para estabelecer conexões de suporte remoto com dispositivos gerenciados, você deve adicionar uma conexão do Remote Support a um ou mais XenMobile Servers que gerenciam os dispositivos. Essa conexão é executada por meio de um túnel de aplicativo que você define na política Tunnel MDM, uma política de dispositivo para dispositivos Android. Defina o túnel de aplicativo antes de conectar o Remote Support ao XenMobile. Para obter detalhes, consulte Políticas de dispositivo de tunelamento de aplicativo.

1. Inicie o software de Suporte Remoto e use suas credenciais do XenMobile para fazer login.
2. Em **Gerenciador de Conexões**, clique em **Novo**.



3. Na caixa de diálogo **Configuração da Conexão**, na guia **Servidor**, digite os seguintes valores:

a. Em **Nome da configuração**, digite um nome para a entrada de configuração.

b. Em **Endereço IP ou nome do servidor**, digite o endereço IP ou o nome DNS do XenMobile Server.

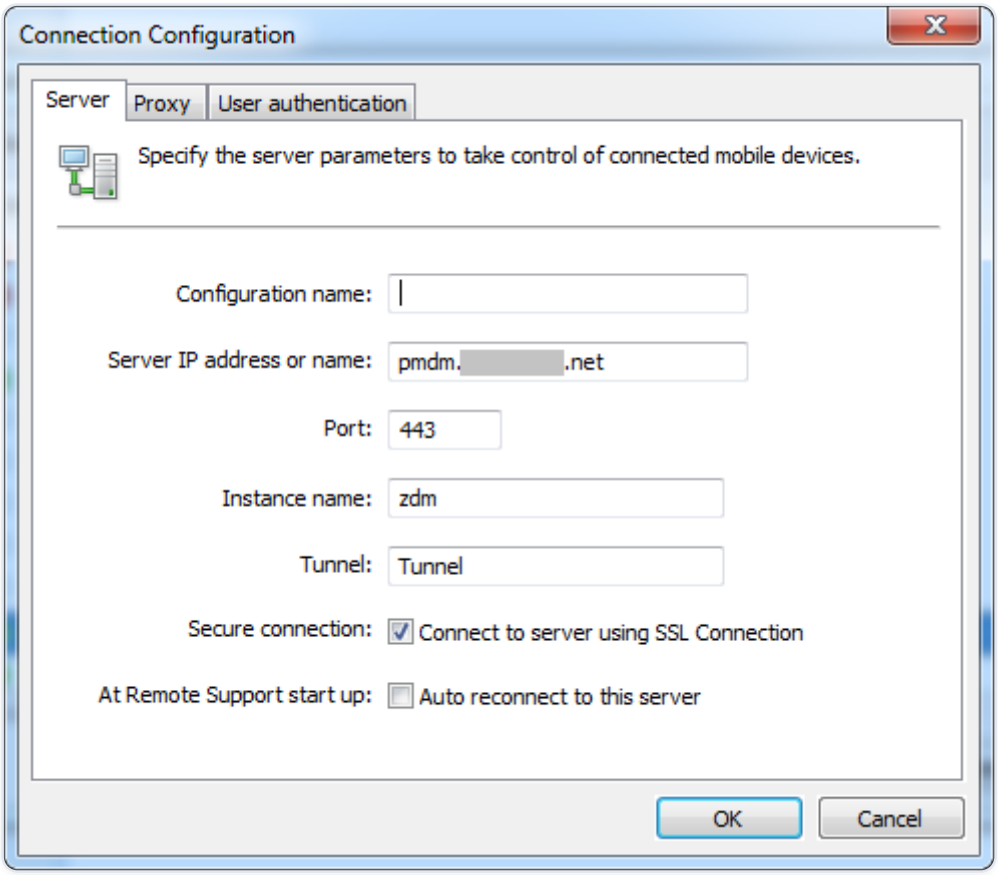
c. Em **Porta**, digite um número de porta TCP, conforme definido na configuração do XenMobile Server.

d. Em **Nome da instância**, quando o XenMobile faz parte de uma implantação multilocatário, digite um nome de instância.

e. Em **Túnel**, digite o nome da política de Túnel.

f. Selecione a caixa de seleção **Conectar ao servidor usando Conexão SSL**.

g. Selecione a caixa de seleção **Reconectar automaticamente a este servidor** para conectar-se ao XenMobile Server configurado toda vez que o aplicativo de Suporte Remoto for iniciado.



4. Na guia **Proxy**, selecione **Usar um servidor proxy http** e, em seguida, digite as seguintes informações:

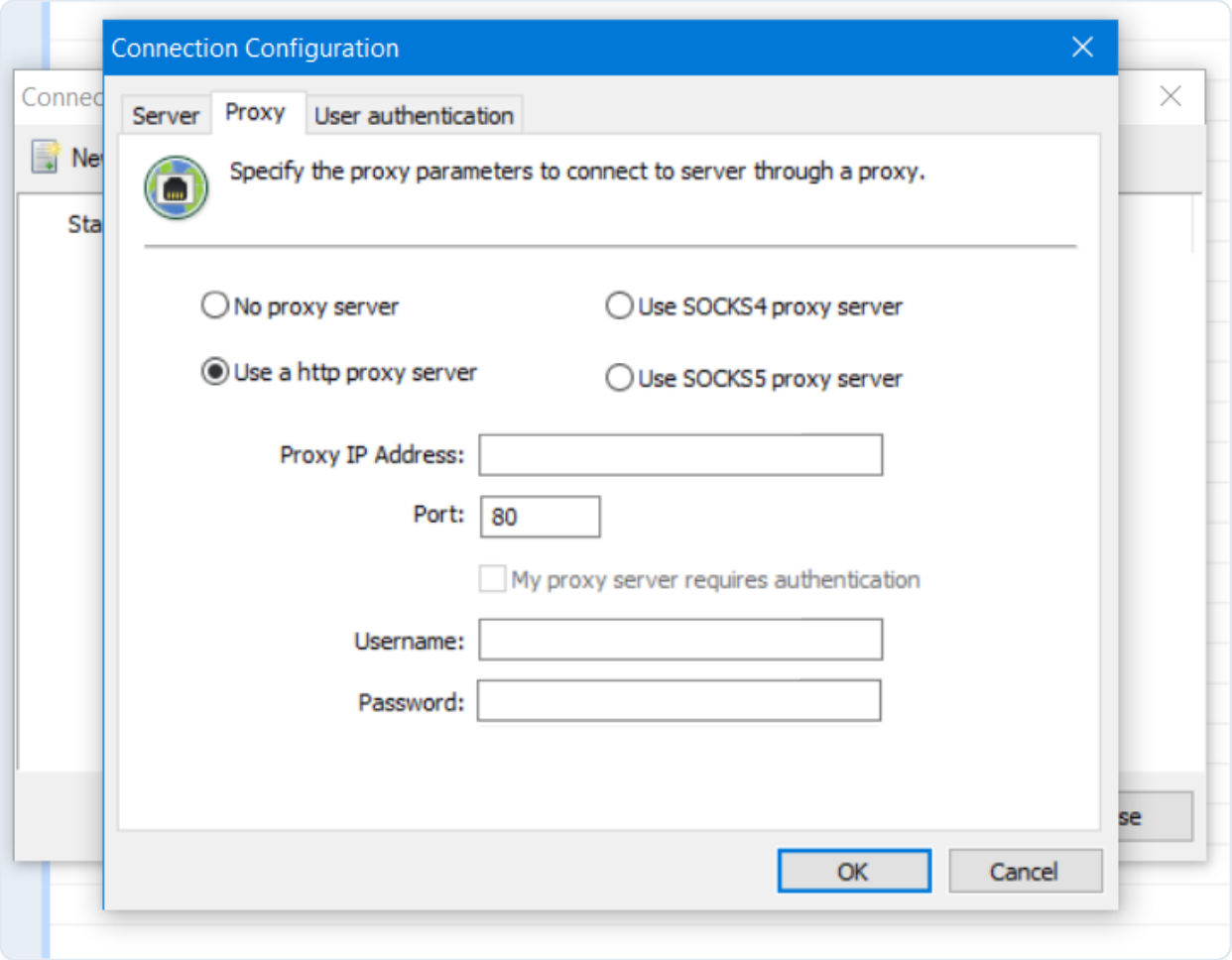
a. Em **Endereço IP do Proxy**, digite o endereço IP do servidor proxy.

b. Em **Porta**, digite um número de porta TCP usado pelo proxy.

c. Selecione a caixa de seleção **Meu servidor proxy requer autenticação** quando o servidor proxy exigir autenticação para permitir o tráfego.

d. Em **Nome de usuário**, digite o nome de usuário a ser autenticado no servidor proxy.

e. Em **Senha**, digite a senha a ser autenticada no servidor proxy.



5. Na guia **Autenticação do usuário**, selecione a caixa de seleção **Lembrar meu login e senha** e insira as credenciais.
6. Clique em **OK**.

Para se conectar ao XenMobile, clique duas vezes na conexão que você criou e, em seguida, insira o nome de usuário e a senha que você configurou para a conexão.

Para habilitar o suporte remoto para dispositivos Samsung Knox

Você cria uma política de Suporte Remoto no XenMobile para conceder acesso remoto a dispositivos Samsung Knox. Você pode configurar dois tipos de suporte:

- **Básico:** Permite visualizar informações de diagnóstico sobre o dispositivo. Por exemplo, informações do sistema, processos em execução, gerenciador de tarefas (uso de memória e CPU) e conteúdo da pasta de software instalado.

- **Premium:** Permite controlar remotamente a tela do dispositivo. Por exemplo, controlar as cores da janela, estabelecer uma sessão VoIP entre o suporte técnico e o usuário, e estabelecer uma sessão de chat entre o suporte técnico e o usuário.

  O suporte Premium exige que você configure a política de dispositivo Chave de Licença MDM Samsung no console do XenMobile. Ao configurar esta política, selecione apenas a plataforma **Samsung KNOX**. Para a plataforma Samsung SAFE, a chave ELM é implantada automaticamente em dispositivos Samsung quando eles se registram no XenMobile. Portanto, não selecione a plataforma Samsung SAFE para esta política. Para obter detalhes, consulte Chave de licença MDM Samsung.

Para obter informações sobre como configurar a Política de Suporte Remoto, consulte Política de dispositivo de suporte remoto.

Para usar uma sessão de Suporte Remoto

Depois de iniciar o Suporte Remoto, o lado esquerdo da janela do aplicativo Suporte Remoto apresenta os grupos de usuários do XenMobile conforme você os definiu no console do XenMobile. Por padrão, apenas os grupos que têm usuários atualmente conectados aparecem. Você pode ver o dispositivo de cada usuário ao lado da entrada do usuário.

1. Para ver todos os usuários, expanda cada grupo da coluna esquerda. Os usuários atualmente conectados ao XenMobile Server são indicados com um ícone verde.
2. Para exibir todos os usuários, incluindo aqueles que não estão conectados no momento, clique em **Exibir** e selecione **Dispositivos não conectados**. Usuários não conectados aparecem sem o pequeno ícone verde.

Dispositivos conectados ao XenMobile Server, mas não atribuídos a um usuário, aparecem no modo Anônimo. (A string **Anônimo** aparece na lista.) Você pode controlar esses dispositivos assim como o dispositivo de um usuário logado.

Para controlar um dispositivo, selecione o dispositivo clicando em sua linha e, em seguida, clicando em **Controlar Dispositivo**. Uma renderização do dispositivo aparece na janela de Controle Remoto. Você pode interagir com um dispositivo controlado das seguintes maneiras:

- Controle a tela do dispositivo, incluindo o controle com cores, na janela principal ou em uma janela separada e flutuante.
- Estabeleça uma sessão VoIP entre o suporte técnico e o usuário. Configure as configurações de VoIP.
- Estabeleça uma sessão de chat com o usuário.

- Acesse o gerenciador de tarefas do dispositivo, para gerenciar itens como uso de memória, uso de CPU e aplicativos em execução.
- Explore os diretórios locais do dispositivo móvel. Transfira arquivos.
- Exiba informações do sistema do dispositivo e todo o software instalado.
- Atualize o status da conexão do dispositivo móvel com o XenMobile Server.

Syslog

Você pode configurar o XenMobile® Server (somente no local) para enviar arquivos de log para um servidor de log do sistema (syslog). Você precisa do nome do host ou do endereço IP do servidor.

Syslog é um protocolo de registro padrão com dois componentes: um módulo de auditoria (que é executado no dispositivo) e um servidor, que pode ser executado em um sistema remoto. O protocolo Syslog usa o protocolo de datagrama de usuário (UDP) para transferência de dados. Eventos de administrador e eventos de usuário são registrados.

Você pode configurar o servidor para coletar os seguintes tipos de informações:

- Logs do sistema que contêm um registro das ações realizadas pelo XenMobile.
- Logs de auditoria que contêm um registro cronológico das atividades do sistema para o XenMobile.

As informações de log que um servidor syslog coleta de um dispositivo são armazenadas em um arquivo de log na forma de mensagens. Essas mensagens geralmente contêm as seguintes informações:

- O endereço IP do dispositivo que gerou a mensagem de log
- Um carimbo de data/hora
- O tipo de mensagem
- O nível de log associado a um evento (Crítico, Erro, Aviso, Alerta, Informativo, Depuração, Alerta ou Emergência)
- As informações da mensagem

O XenMobile usa o appender syslog log4j para enviar mensagens syslog formatadas em RFC5424. Os dados da mensagem syslog são texto simples sem formato específico.

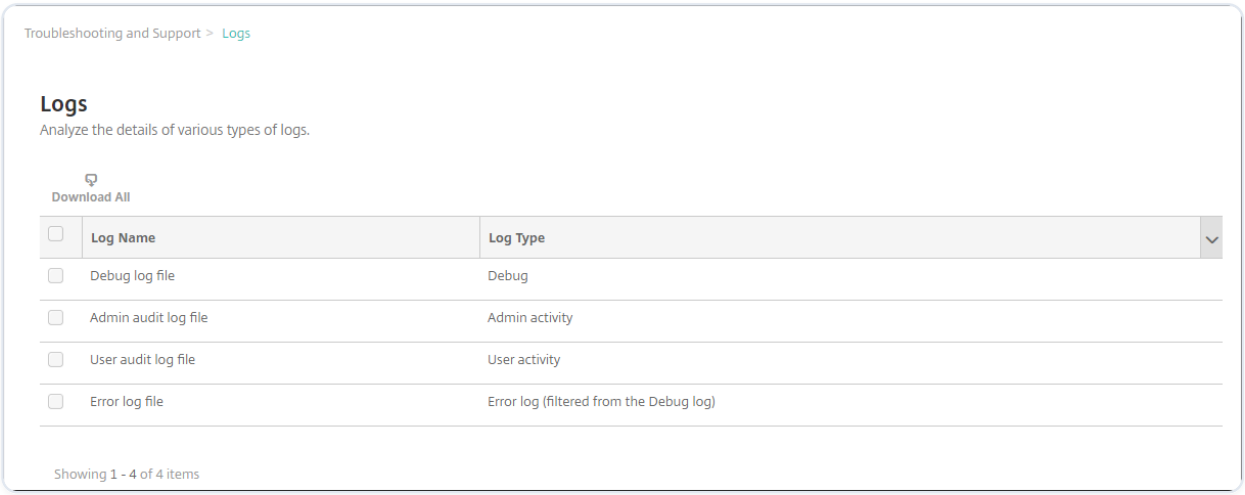
Você pode usar essas informações para analisar a origem do alerta e tomar medidas corretivas, se necessário.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Syslog**. A página **Syslog** é exibida.
3. Configure estas definições:
   - **Servidor:** Digite o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do seu servidor syslog.
   - **Porta:** Digite o número da porta. Por padrão, a porta é definida como 514.
   - **Informações para registrar:** Selecione ou desmarque **Logs do sistema** e **Auditoria**.
     - Os logs do sistema contêm ações realizadas pelo XenMobile.
     - Os logs de auditoria contêm um registro cronológico das atividades do sistema para o XenMobile.
     - Logs de depuração para XenMobile.
4. Clique em **Salvar**.

Visualizar arquivos de log no XenMobile®

Visualize, manipule e baixe logs para ajudar no gerenciamento com o XenMobile.

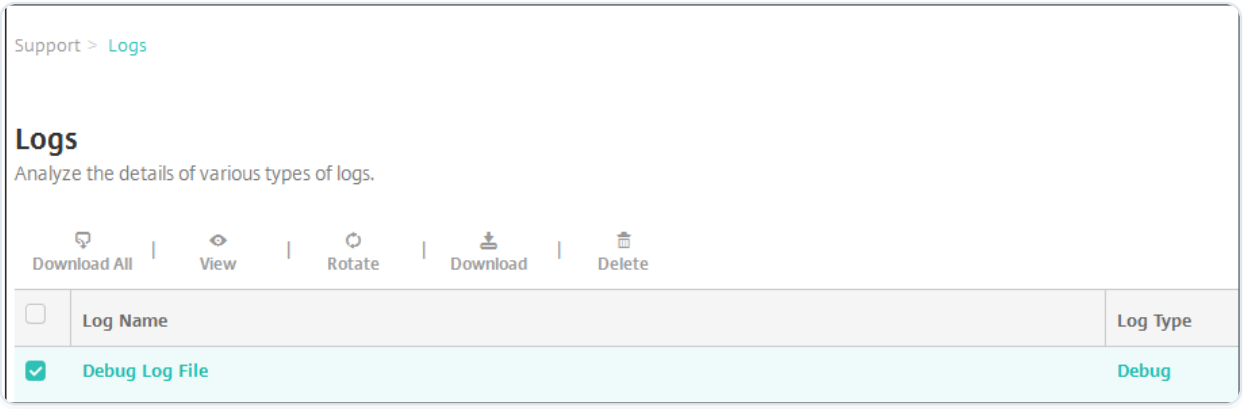
1. No console do XenMobile, clique no ícone de chave inglesa no canto superior direito do console. A página **Suporte** é aberta.
2. Em **Operações de Log**, clique em **Logs**. A página **Logs** é exibida. Os logs individuais aparecem em uma tabela.



3. Selecione o log que você deseja visualizar:

- Os arquivos de log de depuração contêm informações úteis para o Suporte Citrix, como mensagens de erro e ações relacionadas ao servidor.
- Os arquivos de log de auditoria do administrador contêm informações de auditoria sobre a atividade no console do XenMobile.
- Os arquivos de log de auditoria do usuário contêm informações relacionadas aos usuários configurados.
- Os arquivos de log de erro contêm apenas mensagens de erro filtradas do log de depuração.

4. Use as ações na parte superior da tabela para baixar todos, visualizar, girar, baixar um único log ou excluir o log selecionado.



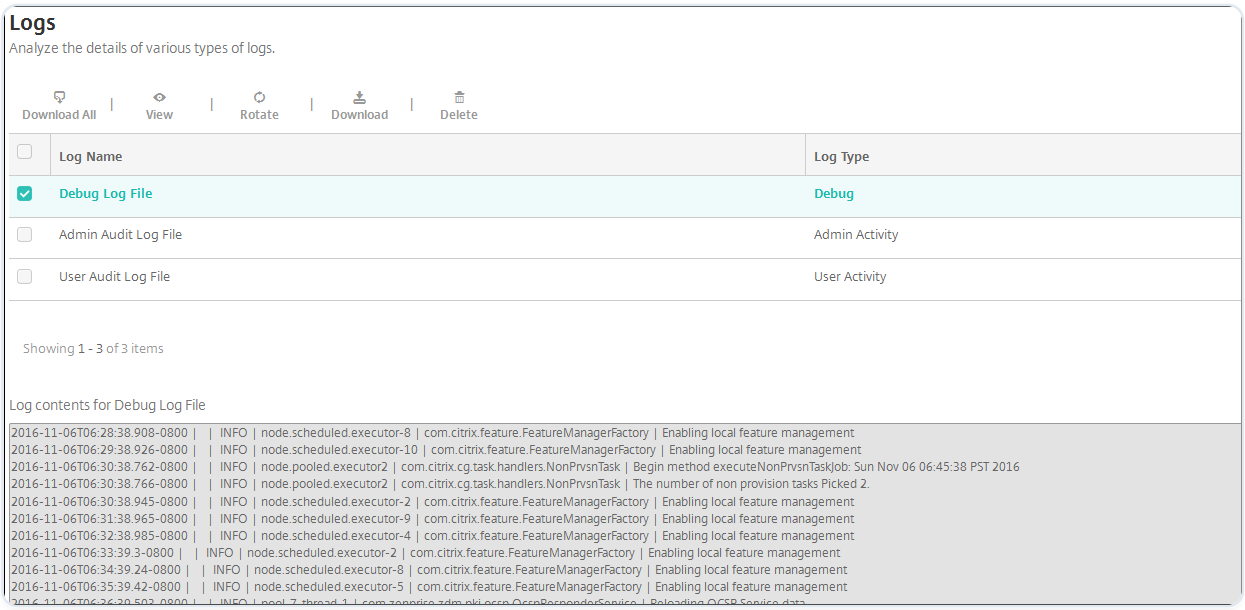
Nota:

- Se você selecionar mais de um arquivo de log, apenas **Baixar Tudo** e **Girar** estarão disponíveis.
- Se você tiver servidores XenMobile em cluster, poderá visualizar apenas os logs do servidor ao qual está conectado. Para ver os logs de outros servidores, use uma das opções de download.

5. Faça um dos seguintes:

- **Baixar Tudo:** O console baixa todos os logs presentes no sistema (incluindo depuração, auditoria de administrador, auditoria de usuário, logs do servidor e assim por diante).
- **Visualizar:** Mostra o conteúdo do log selecionado abaixo da tabela.

- **Rotacionar:** Arquiva o arquivo de log atual e cria um arquivo para capturar entradas de log. Uma caixa de diálogo aparece ao arquivar um arquivo de log; clique em Rotacionar para continuar.
- **Baixar:** O console baixa apenas o tipo de arquivo de log único selecionado. Ele também baixa quaisquer logs arquivados para o mesmo tipo.
- **Excluir:** Remove permanentemente os arquivos de log selecionados.



Elementos de dados de telemetria do XenMobile® Server

Configuração do XenMobile Server

Cabeçalho do evento

CHAVE	DESCRIÇÃO	EXEMPLOS
versão	Indica a versão do cabeçalho.	1
id	Indica o ID exclusivo do evento (GUID).	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
tipo	Indica o nome do tipo de evento.	SYSTEM_CONFIGURATION
st	Indica o carimbo de data/hora formatado em UTC.	2011-08-12T20:17:46.384Z

CHAVE	DESCRIÇÃO	EXEMPLOS
produção	Indica o nome do produto.	XenMobile.OnPrem
prodVer	Indica a versão do produto.	10.16.0.10123

Payload do evento

CHAVE	DESCRIÇÃO	EXEMPLOS
versão	Indica o número da versão do payload de configuração do XenMobile Server.	1.1
xmsVer	Indica o número da versão do XenMobile Server.	10.16.0.48
xmsrpVer	Indica o número da versão do patch cumulativo do XenMobile Server.	10.16.0.10323
dbType	Indica o tipo de banco de dados do XenMobile Server.	MSSQL
dbVer	Indica o número da versão do banco de dados do XenMobile Server.	Microsoft SQL Server 2019 (RTM-CU8) (KB4577194) - 15.0.4073.23 (X64) Sep 23 2020 16:03:08 Copyright (C) 2019 Microsoft Corporation Standard Edition (64-bit) on Windows Server 2016 Standard 10.0 X64 (Build 14393:) (Hypervisor)

CHAVE	DESCRIÇÃO	EXEMPLOS
hostType	Indica o tipo de hipervisor do XenMobile Server.	OnPrem - XenServer®
instanceName	Indica o nome da instância do XenMobile Server.	O /zdm
licenseType	Indica o tipo de licença ativada do XenMobile Server.	CXM_ENTU_UD
sp	Indica todas as propriedades do servidor a serem coletadas.	sp: {afw_restriction_v2: verdadeiro device_page_enhancement_new: verdadeiro multimode: verdadeiro http2_alternate_port: falso playemmapi_update: verdadeiro afw_efota: verdadeiro password_strength: verdadeiro modo: ENT wsdl: falso afw_restriction_cope: verdadeiro

CHAVE	DESCRIÇÃO	EXEMPLOS
		playemmapi: verdadeiro mac_app_push: verdadeiro ga: verdadeiro zdm_pki: verdadeiro tiffany: falso ios_mdm: verdadeiro nac_mail: falso console_ceip: verdadeiro ssl_sign: verdadeiro wip: verdadeiro zebra: verdadeiro apple_apns_http2: verdadeiro afw_hide_vpn_always_on: verdadeiro force_push_apps: verdadeiro ftu: falso afw_vpn_always_on_lockdown: verdadeiro mfa: verdadeiro

CHAVE	DESCRIÇÃO	EXEMPLOS
		mobile_service_provider: verdadeiro afw_network_domain: verdadeiro deprecate_sms: verdadeiro cert_self_signed: verdadeiro ios_http2_pushtype_bg: falso device_update_awapppushtask: verdadeiro android.deprecate.policy: verdadeiro device_page_enhancement: verdadeiro macos_http2_pushtype_bg: falso edu_shared_ipad: verdadeiro licença de sincronização: falso force_push_apps_flag: verdadeiro shp: falso wsapi: falso

CHAVE	DESCRIÇÃO	EXEMPLOS
		aw_dg_performance: verdadeiro apple_profile_renew: verdadeiro afw_priority_update_apps: verdadeiro esim: verdadeiro wpcod: verdadeiro knox: verdadeiro device_report: verdadeiro ios_app_update: true mspki_revert: verdadeiro}

CHAVE	DESCRIÇÃO	EXEMPLOS
cp	Indica todas as propriedades do cliente a serem coletadas.	cp: {PASSCODE_STRENGTH: Medium ENABLE_WORXHOME_CEIP: falso ENABLE_FIPS_MODE: falso DEVICE_LOGS_TO_IT_HELP_DESK: falso ENABLE_WORXHOME_GA: verdadeiro ENCRYPT_SECRETS_USING_PASSCODE: falso ENABLE_PASSCODE_AUTH: falso Usar e-mail em caso de falha: true PASSCODE_TYPE: Numeric CONTAINER_SELF_DESTRUCT_PERIOD: 0 PASSCODE_MIN_LENGTH: 6

CHAVE	DESCRIÇÃO	EXEMPLOS
		Habilitar relatório de falhas: true PASSCODE_EXPIRY: 90 INACTIVITY_TIMER: 15 Habilitar cache de senha: falso PASSCODE_MAX_ATTEMPTS: 15 PASSCODE_HISTORY: 5 DESABILITAR_LOGGING: falso HABILITAR_AUTENTICACAO_TOUCH_ID: falso HABILITAR_VERIFICACAO_BEACON: falso}
enrolledDevices	Indica a contagem de dispositivos registrados.	enrolledDevices: {ANDROID:1,iOS:2, MACOSX:1}
nome de domínio totalmente qualificado	Indica o FQDN público do cliente.	zl225.xmqa.cloud.com
ladpAuthType	Indica o tipo de autenticação LDAP.	Domínio

CHAVE	DESCRIÇÃO	EXEMPLOS
nodeCount	Indica a contagem de nós em um cluster.	4
managedApps	Indica o número de aplicativos gerenciados pelo XenMobile Server.	1000
usersUsingMicroVPN	Indica o número de usuários de MicroVPN.	9999
isIntuneIntegrated	Indica se o Intune está integrado ao XenMobile Server.	verdadeiro
configuratedPolicies	Indica o número de políticas configuradas pelo XenMobile Server.	7777

Uso do XenMobile Server

Cabeçalho do evento

CHAVE	DESCRIÇÃO	EXEMPLOS
Versão	Indica a versão do cabeçalho.	1
id	Indica um ID de evento exclusivo (GUID).	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
Tipo	Indica o nome do tipo de evento.	DEVICE_CHECKIN
st	Indica o carimbo de data/hora formatado em UTC.	2011-08-12T20:17:46.384Z

CHAVE	DESCRIÇÃO	EXEMPLOS
produto	Indica o nome do produto.	XenMobile.OnPrem
prodVer	Indica a versão do produto.	10.16.0.10123
usuário	Indica as informações do usuário. Para um usuário local, não há sid no payload. **Os valores são embaralhados.**	**Usuário AD** usuário: { upn: C982F651A44B3F7 **(sempre embaralhado)** domain: C982F651A44B3F7 **(sempre embaralhado)** email: C982F651A44B3F7 **(sempre embaralhado)** sid: C982F651A44B3F7 **(sempre embaralhado)**} **Usuário local**
		usuário: { upn: C982F651A44B3F7 **(sempre embaralhado)** sAMAccountName: C982F651A44B3F7

CHAVE	DESCRIÇÃO	EXEMPLOS
		(sempre embaralhado)}

Payload do evento

CHAVE	DESCRIÇÃO	EXEMPLOS
versão	Indica o número da versão do payload de Uso do XenMobile Server.	1.1
deviceType	Indica o tipo do dispositivo.	iPhone
hostName	Indica o fqdn do cliente para implantação On-premises.	test.xmqa.cloud.com
platformInfo	Indica a plataforma do dispositivo.	iPhone - iPhone
jailBroken	Esta chave está disponível apenas se o dispositivo for **JAILBROKEN** ou **ROOT**. Se a tag estiver ausente, o dispositivo não está Jailbroken ou rooteado.	sim ou não
serialNum	Indica o número de série do dispositivo, com hash por padrão.	KsPRhShj0h9IhbVkFEU7ZQ==
os	Indica o tipo de SO do dispositivo.	iOS
managementMode	Indica o modo de gerenciamento do dispositivo.	mdm ou mam ou xme ou não gerenciado
deviceId	Indica o ID exclusivo interno do dispositivo.	41CC018E-7CC0-4697-B07E-1E8CCEF7F592
supervisionado	Indica se o dispositivo é supervisionado ou não.	sim ou não

CHAVE	DESCRIÇÃO	EXEMPLOS
osVersion	Indica o número da versão do SO do dispositivo.	16.4.1 (a)
IMEI	Indica o número IMEI do dispositivo, se disponível, com hash por padrão.	6M6iBmcsokQxPQyeVwiaQQ==
deviceModel	Indica o modelo do dispositivo.	iPhone
lastActivity	Indica o carimbo de data/hora da última atividade do dispositivo.	2024-03-29 14:17:14.277
corporateOwned	Indica se o dispositivo pertence à empresa ou não.	não
enabledFeatures	Indica a habilitação de múltiplos recursos.	1
ID do evento de política mais recente	Indica o ID de Ambiente Exclusivo que pode ser usado para identificar um site XMS exclusivo.	95ba4968cfaf069c20949d76473ecd4f3994f556d0fef7f2fa11912731d720bf Ou em branco se o LAS não estiver disponível

APIs REST

> **Nota:**
>
> Este artigo aborda as APIs REST para o XenMobile Server. Para as APIs REST para Endpoint Management, consulte APIs REST.

> Com a API REST do XenMobile®, você pode chamar serviços expostos através do console do XenMobile. Você pode chamar serviços REST usando qualquer cliente REST. A API não exige que você faça login no console do XenMobile para chamar os serviços.

Para o conjunto completo atual de APIs disponíveis, baixe o PDF API Pública para Serviços REST.

Permissões necessárias para acessar a API REST

O acesso à API REST requer uma das seguintes permissões:

- Permissão de acesso à API pública definida como parte da configuração de acesso baseado em função. Para obter informações, consulte Configurando funções com RBAC.
- Permissão de superusuário

Para invocar serviços da API REST

Você pode invocar serviços da API REST usando o cliente REST ou comandos cURL. Os exemplos a seguir usam o cliente Advanced REST para Chrome.

> **Nota:**
>
> Nos exemplos a seguir, altere o nome do host e o número da porta para corresponder ao seu ambiente.

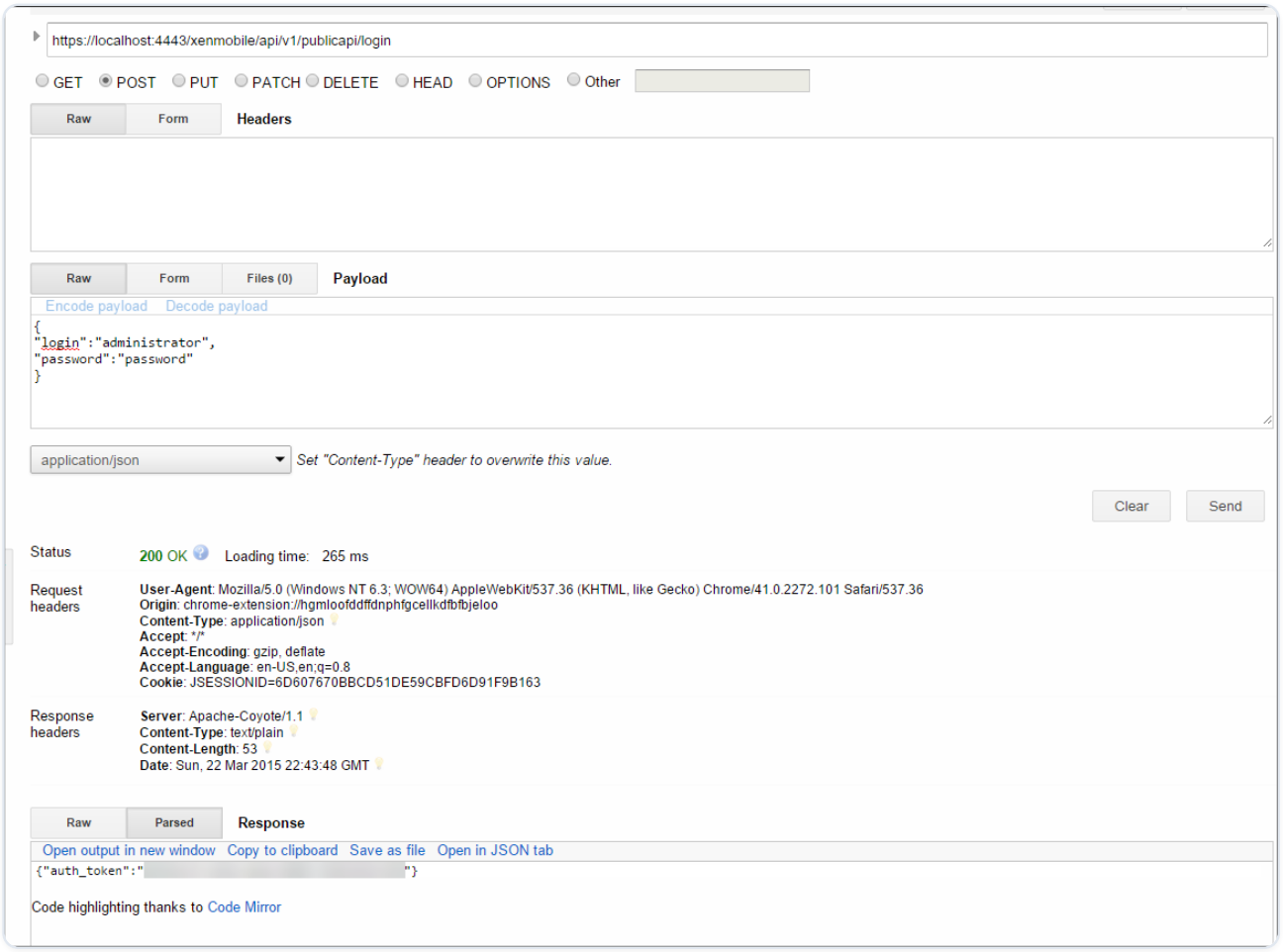
Fazer login

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Solicitação: `{ "login":"administrator", "password":"password" }`

Tipo de método: POST

Tipo de conteúdo: application/json



Informações relacionadas

- XenMobile REST API

Conector do Endpoint Management para Exchange ActiveSync

O XenMobile Mail Manager agora é um conector do Endpoint Management para Exchange ActiveSync. Para obter mais detalhes sobre o portfólio unificado da Citrix, consulte o guia de produtos da Citrix.

O conector estende os recursos do XenMobile® das seguintes maneiras:

- Controle de Acesso Dinâmico para dispositivos Exchange Active Sync (EAS). Os dispositivos EAS podem ter o acesso aos serviços do Exchange permitido ou bloqueado automaticamente.
- A capacidade do XenMobile de acessar informações de parceria de dispositivos EAS fornecidas pelo Exchange.
- A capacidade do XenMobile de apagar um dispositivo móvel com base no status do EAS.
- A capacidade do XenMobile de acessar informações sobre dispositivos Blackberry e de realizar operações de controle como Limpar e Redefinir Senha.

Para apagar um dispositivo com base no status do EAS, configure uma ação automatizada com um gatilho do ActiveSync. Consulte Ações Automatizadas.

Para baixar o conector do Endpoint Management para Exchange ActiveSync:

1. Vá para `<https://www.citrix.com/downloads>`.
2. navegar para **Citrix Endpoint Management™ (e Citrix XenMobile Server) > XenMobile Server (local) > Product Software > XenMobile Server 10 > Server Components**.
3. No bloco **Citrix Endpoint Management connector for Exchange ActiveSync**, clique em **Baixar Arquivo**.

> **Importante:**

> A partir de outubro de 2022, os conectores do Endpoint Management e do Citrix Gateway para Exchange ActiveSync não oferecerão mais suporte ao Exchange Online, dadas as

> alterações de autenticação anunciadas pela Microsoft aqui. O conector do Endpoint Management para Exchange continua a funcionar com o Microsoft Exchange Server (local).

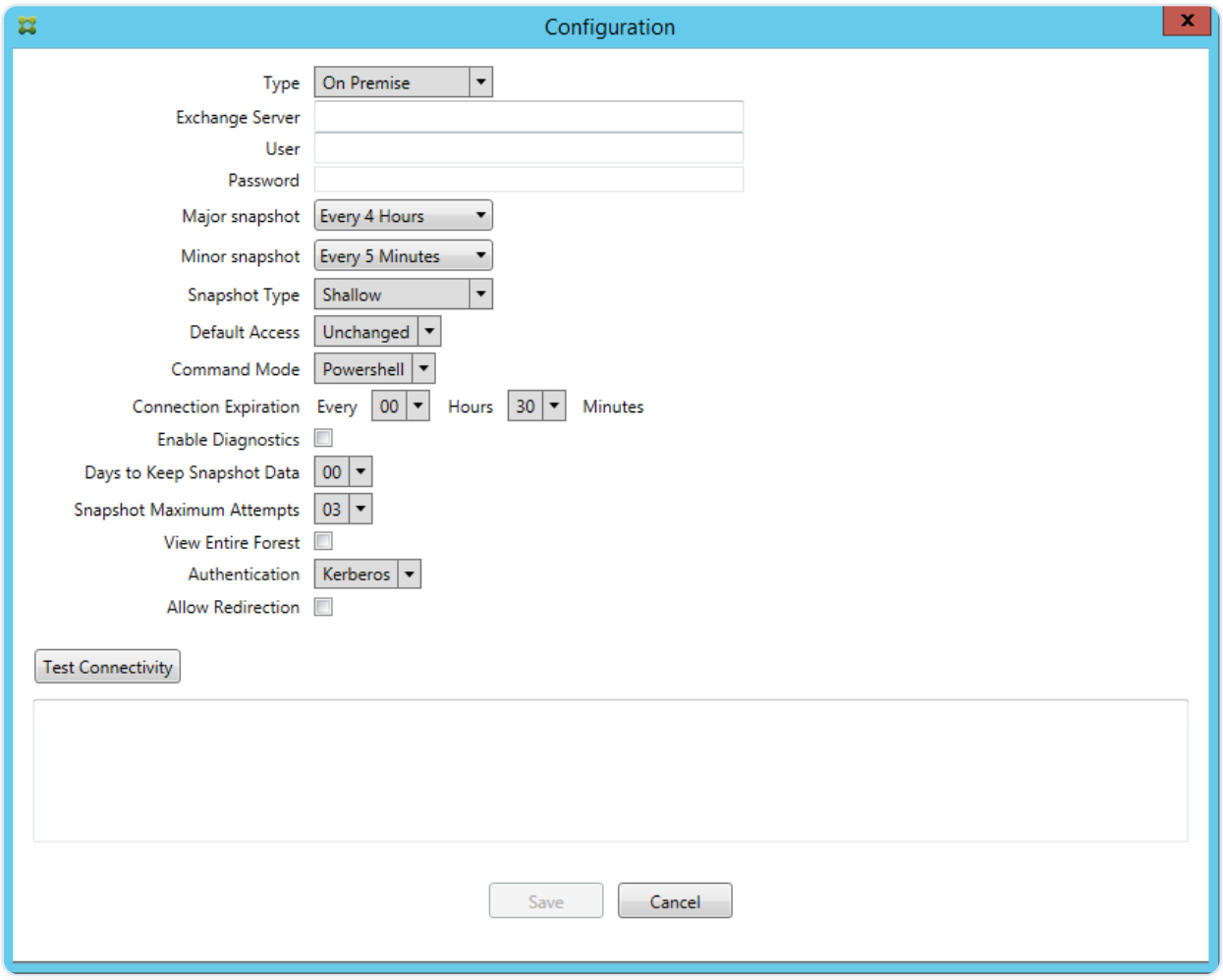
Novidades

As seções a seguir listam as novidades no conector do Endpoint Management para Exchange ActiveSync, anteriormente XenMobile Mail Manager.

Novidades na versão 10.1.10

Os seguintes problemas foram corrigidos na versão 10.1.10:

- Clientes que enfrentam problemas frequentes de rede podem não conseguir concluir um Snapshot dentro das três tentativas fornecidas anteriormente. Com esta versão, um administrador pode configurar o número máximo de tentativas (1-10). Esta correção permite que um snapshot sofra várias interrupções na comunicação sem abandonar completamente o processo de snapshot.



- Em versões anteriores, o tipo Snapshot não aparecia na lista de Configurações do Exchange. Agora, o tipo de snapshot aparece.
- A exceção PSRemotingTransport relatada pelo PowerShell indica que a sessão para o Exchange não é mais viável. O status é adicionado à lista de Erros Críticos no arquivo de configuração por padrão. Ao fazer isso, quando a PSRemotingTransportException é detectada, a conexão é marcada como em Erro para descarte posterior. A próxima comunicação usa uma conexão válida ou cria uma conexão.
- Quando uma alteração de configuração é salva, é possível que nem todos os componentes internos configurados anteriormente tenham sido descartados corretamente antes de carregar a nova configuração. Este problema pode levar a um comportamento imprevisível. O comportamento depende da alteração específica e se a alteração entrou em conflito com a configuração anterior. Nesta versão, todos os componentes internos são descartados antes de carregar a nova configuração.

Novidades em versões anteriores

A seção a seguir lista os recursos e problemas corrigidos em versões anteriores do conector do Endpoint Management para Exchange ActiveSync.

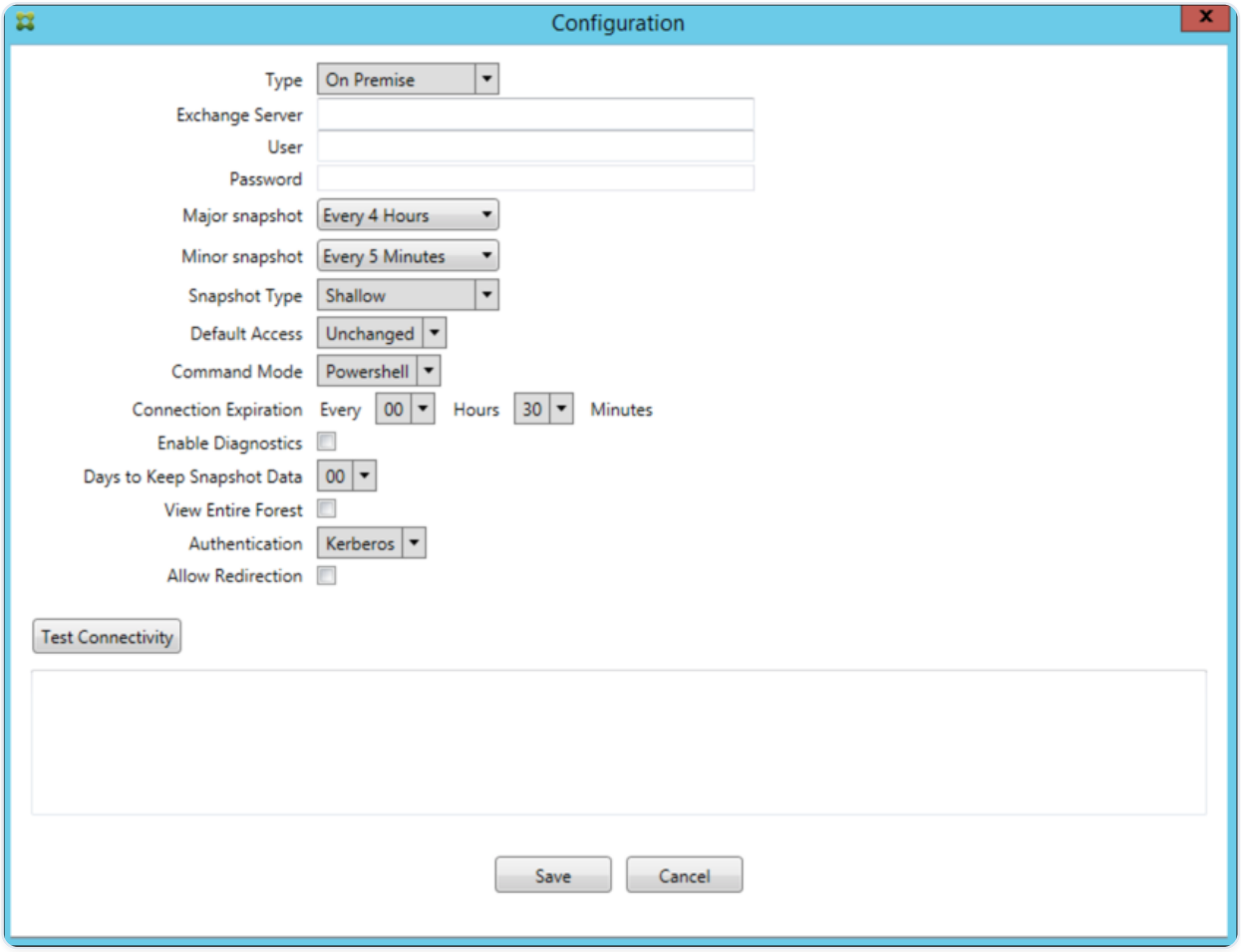
Novidades na versão 10.1.9

Os seguintes problemas foram corrigidos na versão 10.1.9:

- As alterações de configuração agora são tratadas de forma mais consistente. Quando o serviço detecta uma alteração na configuração, cada subsistema interno é interrompido, o que significa que qualquer processamento ativo ou agendado é interrompido. Em seguida, a nova configuração é carregada e os subsistemas são iniciados novamente, o que significa que todos os agendamentos e outras infraestruturas internas são restabelecidos com novas configurações. Este problema corrige um problema conhecido na versão 10.1.8.
- Durante uma atualização, a configuração do banco de dados existente não foi mesclada no novo arquivo de configuração. A configuração do banco de dados agora é mesclada no arquivo de configuração atualizado.
- Nos arquivos de diagnóstico relacionados ao snapshot, os cabeçalhos das colunas estavam faltando. Os cabeçalhos foram restaurados.
- Ao atualizar de uma versão anterior, a seção de padrões do arquivo de configuração estava sendo sobrescrita pela seção análoga do arquivo de configuração em uso. Este problema impedia que adições ou melhorias à seção de padrões fossem carregadas pelo serviço após a

atualização. A partir desta versão, a seção de padrões sempre reflete a configuração mais recente.

- Os administradores não podem mais acessar certas opções pressionando Shift ao executar o aplicativo. Essas opções estavam anteriormente disponíveis com permissão da Citrix. Algumas opções agora estão totalmente disponíveis, como Permitir Redirecionamento, e outras, como Detecção de Travamento e Correção de Contagem, foram descontinuadas.



Novidades na versão 10.1.8

Os seguintes problemas foram corrigidos na versão 10.1.8:

- É possível que o Exchange limite o conector do Citrix Endpoint Management para o serviço Exchange ActiveSync de emitir comandos com muita frequência. Isso é comum em conexões com o Office 365. O efeito da limitação exige que o serviço pause por um período especificado antes de enviar o próximo comando. O console de Configuração agora mostra a quantidade de tempo restante na pausa.
- Quando modificações são feitas nas seções "Watchdog" ou "SpecialistsDefaults" do arquivo de configuração (config.xml), as alterações não são refletidas no arquivo de configuração após

uma atualização. Com esta versão, as modificações são mescladas corretamente no novo arquivo de configuração.

- Mais detalhes foram adicionados aos dados analíticos enviados ao Google Analytics, especialmente em relação aos snapshots.
- O recurso de teste de conectividade do Exchange tentaria inicializar a conexão apenas uma vez. Como as conexões do Office 365 podem ser limitadas, era possível que um teste de conectividade parecesse falhar quando limitado. O conector do Citrix Endpoint Management para Exchange ActiveSync agora tenta iniciar uma conexão até três vezes.
- Para aplicar políticas no Exchange, o conector do Citrix Endpoint Management para Exchange ActiveSync deve compilar um comando **Set-CASMailbox** que inclua todos os dispositivos pertinentes para cada caixa de correio, em duas listas: permitir e bloquear. Se um dispositivo não estiver incluído em nenhuma das listas, o Exchange retorna ao seu estado de acesso padrão. Se esse estado de acesso padrão for diferente do estado desejado para um dispositivo, esse dispositivo ficará fora de conformidade. Consequentemente, um usuário pode perder o acesso ao seu e-mail se o estado de acesso padrão do Exchange for bloqueado e deveria ser permitido. Ou, um usuário cujo acesso ao e-mail deveria ser bloqueado pode ter o acesso concedido. O conector do Citrix Endpoint Management para Exchange ActiveSync agora garante que todos os dispositivos com um estado desejado válido sejam incluídos em cada comando **Set-CasMailbox**.

O seguinte problema é conhecido na versão 10.1.8:

Se um administrador fizer uma alteração no aplicativo Configurar que modifique os dados de configuração, enquanto o serviço estiver executando operações de longa duração, como um snapshot ou avaliação de política, o serviço poderá entrar em um estado indeterminado. Um possível sintoma pode ser que as alterações de política não sejam processadas ou que os snapshots não sejam iniciados. Para retornar o serviço a um estado de funcionamento, o serviço deve ser reiniciado. Pode ser necessário usar o gerenciador de Serviços do Windows para encerrar o processo do serviço antes de iniciá-lo.

Novidades na versão 10.1.7

- O XenMobile Mail Manager agora é um conector do Endpoint Management para Exchange ActiveSync.
- Descontinuamos a opção **Disable Pipelining** na caixa de diálogo de configuração do Exchange. Você pode obter a mesma funcionalidade configurando várias etapas para cada comando no arquivo config.xml.

Os seguintes problemas foram corrigidos na versão 10.1.7:

- Na janela Histórico de Instantâneos, as mensagens de erro podem ser exibidas com pouco contexto. Agora, as mensagens de erro são prefixadas com o contexto de onde ocorreram.
- A DLL XmmGoogleAnalytics não tinha a versão de arquivo correspondente para o lançamento.
- Para melhorar o diagnóstico, recentemente alteramos o formato da string para uma lista de IDs de dispositivo usadas para definir o estado Permitido/Bloqueado de uma caixa de correio. No entanto, a especificação de muitos dispositivos excedeu o tamanho máximo da string. Agora, usamos uma estrutura de dados de array interna. Essa estrutura não tem limite de tamanho e também formata os dados de forma apropriada para fins de diagnóstico.
- Quando políticas de dispositivo que não estão sincronizadas com o Exchange são detectadas, seus comandos podem incluir dispositivos que não pertencem à caixa de correio relevante. O conector do Endpoint Management para Exchange ActiveSync agora garante que os comandos para o Exchange representem apenas dispositivos que pertencem às suas respectivas caixas de correio.
- Em alguns ambientes, um assembly da Microsoft não está disponível. O assembly necessário agora é explicitamente instalado com o aplicativo.
- Se os Nomes Distintos para dispositivos ou caixas de correio tiverem espaços entre o nome do atributo e o sinal de igual, e/ou espaços após o sinal de igual e antes do valor, o conector do Endpoint Management para Exchange ActiveSync pode não corresponder corretamente um dispositivo à sua caixa de correio e vice-versa. O resultado pode ser que alguns dispositivos e/ou caixas de correio sejam rejeitados durante a reconciliação do instantâneo.

> **Nota:**
>
> As seções a seguir se referem ao conector do Endpoint Management para Exchange ActiveSync pelo seu nome anterior, XenMobile Mail Manager. O nome mudou a partir da versão 10.1.7.

Atualização na versão 10.1.6.20

Uma atualização para 10.1.6 contém a seguinte correção na versão 10.1.6.20:

- Quando políticas de dispositivo que não estão sincronizadas com o Exchange são detectadas, seus comandos podem incluir dispositivos que não pertencem à caixa de correio relevante. O

XenMobile Mail Manager agora garante que os comandos para o Exchange representem apenas dispositivos que pertencem às suas respectivas caixas de correio.

Novidades na versão 10.1.6

O XenMobile Mail Manager versão 10.1.6 contém os seguintes problemas corrigidos e aprimoramentos:

- A janela de histórico de instantâneos, às vezes, entra em um estado em que não está mais sendo atualizada. O mecanismo de atualização das janelas foi aprimorado para atualizar de forma mais confiável.
- Dois modos e caminhos de código separados eram usados para instantâneos particionados e não particionados. Como os instantâneos não particionados são equivalentes a instantâneos particionados com uma configuração usando uma única partição "*", o modo de instantâneo não particionado foi eliminado. O modo de instantâneo padrão agora é instantâneos particionados com 36 partições (0–9, A–Z).
- Na janela Histórico de Instantâneos, as mensagens de erro são sobrescritas pelas mensagens de status. Agora, o XenMobile Mail Manager fornece dois campos separados para que os usuários possam visualizar o status e os erros simultaneamente.
- Ao conectar-se ao Exchange Online (Office 365), as consultas relacionadas a instantâneos podem resultar em um conjunto de dados truncado. Esse problema pode ocorrer quando o XenMobile Mail Manager executa um script pipeline de múltiplos comandos. O comando upstream não consegue passar os dados rapidamente o suficiente para o comando downstream, que então conclui o trabalho prematuramente. Dados incompletos ocorrem como resultado. O XenMobile Mail Manager agora pode imitar o próprio pipeline e esperar até que o comando upstream seja concluído antes de invocar o comando downstream. Essa alteração deve resultar no processamento e captura de todos os dados.
- Se ocorrer um erro não resolúvel em um comando de atualização de política para o Exchange, o mesmo comando é retornado à fila de trabalho repetidamente por um longo período. Essa situação resultou no envio do comando ao Exchange muitas vezes. Nesta versão do XenMobile Mail Manager, um comando que resulta em erro é retornado à fila de trabalho apenas um número discreto de vezes.
- Se uma atualização de política para uma caixa de correio específica envolvesse a permissão ou o bloqueio de todos os dispositivos: O comando **Set-CASMailbox** emitido falharia devido à lista vazia ser convertida em uma string vazia em vez de um **NULL**. Os dados corretos agora são enviados.

- Ao processar um novo dispositivo, o Exchange pode retornar o estado como "DeviceDiscovery" por um tempo (geralmente 15 minutos). O XenMobile Mail Manager não estava lidando especificamente com esse estado. O XenMobile Mail Manager agora lida com o estado. Na guia Monitor da interface do usuário, os usuários podem filtrar por dispositivos neste estado.
- O XenMobile Mail Manager não verificava a capacidade de gravar no banco de dados do XenMobile Mail Manager. Consequentemente, se as permissões fossem restritas, o comportamento não poderia ser previsto. O XenMobile Mail Manager agora captura e valida as permissões necessárias do banco de dados. O XenMobile Mail Manager indica permissões reduzidas ao testar a conexão (mensagem exibida) ou no indicador do Banco de Dados (passe o mouse para ver a mensagem) na parte inferior da janela principal de Configuração.
- Dependendo da carga de trabalho atual, quando solicitado, o serviço XenMobile Mail Manager pode não parar prontamente. Portanto, o serviço parece estar em um estado sem resposta. As melhorias permitem que as tarefas em andamento sejam interrompidas, resultando em um desligamento mais elegante.

Novidades na versão 10.1.5

A versão 10.1.5 do XenMobile Mail Manager contém os seguintes problemas corrigidos:

- Quando o Exchange está aplicando limitação (throttling) à atividade do XenMobile Mail Manager, não há indicação (fora dos logs) de que a limitação está ocorrendo. Com esta versão, um usuário pode passar o mouse sobre o instantâneo ativo e um estado de "limitação" aparece. Além disso, enquanto o XenMobile Mail Manager está sendo limitado, o início de um instantâneo principal é proibido até que o Exchange suspenda o embargo de limitação.
- Se o XenMobile Mail Manager estiver sendo limitado pelo Exchange durante um instantâneo principal: É possível que um tempo insuficiente seja permitido para decorrer antes de executar a próxima tentativa de um instantâneo. Esse problema resulta em mais limitação e um instantâneo com falha. O XenMobile Mail Manager agora aguarda um mínimo do tempo que o Exchange especifica para aguardar entre as tentativas de instantâneo.
- Quando o diagnóstico está ativado, o arquivo de comandos mostra comandos **Set-CasMailbox** que têm hífens ausentes antes de cada nome de propriedade. Esse problema ocorre apenas na formatação do arquivo de diagnóstico e não no comando real para o Exchange. O hífen ausente impede que um usuário recorte o comando e o cole diretamente em um prompt do PowerShell para teste ou validação. Os hífens foram adicionados.
- Se uma identidade de caixa de correio for do formato "sobrenome, nome", o Exchange adiciona uma barra invertida antes da vírgula ao retornar dados de uma consulta. Essa barra

invertida deve ser removida quando o XenMobile Mail Manager usa a identidade para consultar mais dados.

Limitações conhecidas

> **Nota:**

> A seguinte limitação foi resolvida na versão 10.1.6.

> O XenMobile Mail Manager possui uma limitação conhecida que pode fazer com que os comandos para o Exchange falhem. Para aplicar alterações de política ao Exchange, um comando **Set_CASMailbox** é emitido pelo XenMobile Mail Manager. Este comando pode receber duas listas de dispositivos: uma para Permitir e outra para Bloquear. O comando é aplicado aos dispositivos associados a uma caixa de correio.

Essas listas são limitadas a 256 caracteres cada pela API da Microsoft. Se uma dessas listas exceder a limitação, o comando falha completamente, impedindo que todas as políticas para esses dispositivos da caixa de correio sejam definidas. O erro relatado, que aparecerá nos logs do XenMobile Mail Manager, seria semelhante ao seguinte. O exemplo é para a lista bloqueada.

“Mensagem:'Não é possível vincular o parâmetro 'ActiveSyncBlockedDeviceIDs' ao destino. Exceção ao definir "ActiveSyncBlockedDeviceIDs": "O comprimento da propriedade é muito longo. O comprimento máximo é 256 e o comprimento do valor fornecido é…”

Os comprimentos dos IDs de dispositivo podem variar, mas uma boa diretriz é que cerca de 10 ou mais dispositivos Permitidos ou Bloqueados simultaneamente podem exceder o limite. Embora ter tantos dispositivos associados a uma caixa de correio específica seja raro, é uma possibilidade. Até que o XenMobile Mail Manager seja aprimorado para manipular tal cenário, recomendamos que você limite o número de dispositivos associados a um usuário e caixa de correio a 10 ou menos.

Novidades na versão 10.1.4

A versão 10.1.4 do XenMobile Mail Manager contém os seguintes problemas corrigidos:

- Devido à sua segurança enfraquecida, o TLS 1.0 está sendo descontinuado pelo PCI Council. O suporte para TLS 1.1 e 1.2 foi adicionado ao XenMobile Mail Manager.
- O XenMobile Mail Manager inclui um novo arquivo de diagnóstico. Quando **Enable Diagnostics** é selecionado na especificação do Exchange, um novo arquivo Snapshot History

é gerado. A cada tentativa de snapshot, uma linha é adicionada ao arquivo com os resultados do snapshot.

- No arquivo de diagnóstico de Comandos, a lista de dispositivos permitidos ou bloqueados não aparecia para o comando **Set-CASMailbox**. Em vez disso, o nome da classe interna era exibido no arquivo para os argumentos relacionados. O XenMobile Mail Manager agora mostra a lista de deviceIDs como uma lista separada por vírgulas.
- Quando uma tentativa de adquirir uma conexão com o Exchange falha devido a uma especificação incorreta: A mensagem de erro é substituída por uma mensagem incorreta: "Todas as conexões em uso". Mensagens mais descritivas agora aparecem, como "Todas as conexões estão inoperáveis", "O pool de conexões está vazio", "Todas as conexões estão limitadas" e "Nenhuma conexão disponível".
- Às vezes, os comandos Permitir/Bloquear/Limpar são enfileirados no cache interno do XenMobile Mail Manager várias vezes. Esse problema causa um atraso no envio do comando para o Exchange. O XenMobile Mail Manager agora enfileira apenas uma instância de cada comando.

Novidades na versão 10.1.3

- **Suporte ao Google Analytics:** Queremos saber como você usa o XenMobile Mail Manager para que possamos focar em onde podemos melhorar o produto.
- **Configuração para habilitar diagnósticos:** Uma caixa de seleção **Enable Diagnostic** aparece no console de Configuração na caixa de diálogo **Configuration**.

Imagem do conector do Endpoint Management para Exchange ActiveSync(/en-us/xenmobile/server/media/mail-manager-diagnostics-checkbox.png)

Problemas corrigidos na versão 10.1.3

- Na janela **Histórico de Instantâneos**, as dicas de ferramentas que mostram o estado atual do instantâneo não refletem o estado real. Ocasionalmente, o XenMobile Mail Manager não consegue gravar no arquivo de diagnóstico de Comandos. Quando isso ocorre, o histórico de comandos não é registrado na íntegra.
- Quando ocorre um erro com uma conexão, a conexão pode não ser marcada como "com erro". Como resultado, um comando subsequente pode tentar usar a conexão e causar outro erro.
- Quando ocorre a limitação de recursos do Exchange Server, uma exceção pode ser lançada na rotina de Verificação de Integridade. Como resultado, as conexões que apresentaram um

erro ou expiraram podem não ser limpas. Além disso, o XenMobile Mail Manager pode não criar conexões até que o tempo de limitação expire.

- Quando o número máximo de sessões para o Exchange é excedido, o XenMobile Mail Manager relata o erro "Falha na Captura do Dispositivo", o que não é uma mensagem precisa. Em vez disso, a mensagem deve indicar que as duas sessões que o XenMobile Mail Manager normalmente usa para a comunicação com o Exchange estão em uso.

O que há de novo na versão 10.1.2

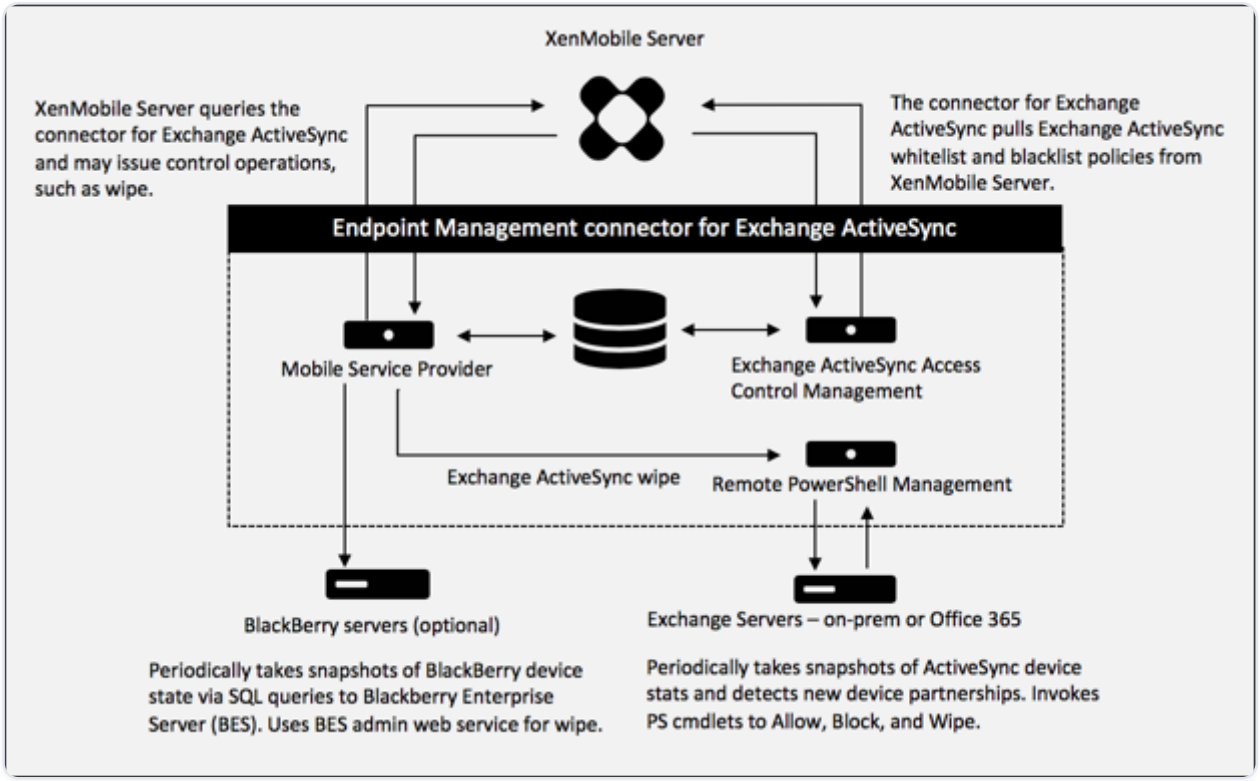
- **Conexão aprimorada com o Exchange**: O XenMobile Mail Manager usa sessões do PowerShell para se comunicar com o Exchange. Uma sessão do PowerShell, especialmente ao lidar com o Office 365, pode se tornar instável após um tempo, impedindo que comandos subsequentes sejam bem-sucedidos. O XenMobile Mail Manager agora pode definir um período de expiração para as conexões. Quando a conexão atinge seu tempo de expiração, o XenMobile Mail Manager encerra a sessão do PowerShell de forma elegante e cria uma nova sessão. Ao fazer isso, a sessão do PowerShell tem menos probabilidade de se tornar instável, reduzindo significativamente a chance de falha de instantâneo.
- **Fluxo de trabalho de instantâneo aprimorado**: Instantâneos importantes são uma operação demorada e intensiva em termos de processo. Se ocorrer um erro durante um instantâneo, o XenMobile Mail Manager agora tenta várias vezes (até três) para concluir um instantâneo. As tentativas subsequentes não começam do início. O XenMobile Mail Manager continua de onde parou. Esse aprimoramento melhora a taxa de sucesso dos instantâneos em geral, permitindo que erros transitórios passem enquanto um instantâneo ainda está em andamento.
- **Diagnóstico aprimorado**: A solução de problemas de operações de instantâneo agora é mais fácil com três novos arquivos de diagnóstico gerados opcionalmente durante um instantâneo. Esses arquivos ajudam a identificar problemas de comando do PowerShell, caixas de correio com informações ausentes e dispositivos que não podem ser relacionados a uma caixa de correio. Um administrador pode usar esses arquivos para identificar dados que podem não estar corretos no Exchange.
- **Uso de memória aprimorado**: O XenMobile Mail Manager agora é mais eficiente no uso da memória. Os administradores podem agendar o XenMobile Mail Manager para reiniciar automaticamente, a fim de fornecer um sistema limpo.
- **Pré-requisito do Microsoft .NET Framework 4.6**: O pré-requisito para o Microsoft .NET Framework agora é a versão 4.6.

Problemas corrigidos

- Erro de solicitação de credenciais: A instabilidade da sessão do Office 365 frequentemente causava esse erro. O aprimoramento da Conexão Aprimorada com o Exchange resolve o problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Imprecisões na contagem de caixas de correio e dispositivos: O XenMobile Mail Manager possui um algoritmo aprimorado de associação de Caixa de Correio a Dispositivo. O recurso de Diagnóstico Aprimorado ajuda na identificação de caixas de correio e dispositivos que o XenMobile Mail Manager considera não estarem dentro de sua esfera de responsabilidade. (XMHELP-623)
- Comandos de Permitir/Bloquear/Limpar não sendo reconhecidos: Um bug foi corrigido onde, às vezes, os comandos de permitir/bloquear/limpar do XenMobile Mail Manager não eram reconhecidos. (XMHELP-489)
- Gerenciamento de memória: Melhor gerenciamento e mitigação de memória. (XMHELP-419)

Arquitetura

A figura a seguir mostra os principais componentes do conector do Endpoint Management para Exchange ActiveSync. Para um diagrama de arquitetura de referência detalhado, consulte Arquitetura.



Os três principais componentes são:

- **Gerenciamento de Controle de Acesso do Exchange ActiveSync:** Comunica-se com o XenMobile para recuperar uma política do Exchange ActiveSync do XenMobile e mescla essa política com qualquer política definida localmente para determinar os dispositivos do Exchange ActiveSync que devem ter acesso permitido ou negado ao Exchange. A política local permite estender as regras da política para permitir o controle de acesso por Grupo do Active Directory, Usuário, Tipo de Dispositivo ou Agente de Usuário do Dispositivo (geralmente a versão da plataforma móvel).
- **Gerenciamento Remoto do PowerShell:** Responsável por agendar e invocar comandos remotos do PowerShell para implementar a política compilada pelo Gerenciamento de Controle de Acesso do Exchange ActiveSync. Periodicamente, tira um instantâneo do banco de dados do Exchange ActiveSync para detectar dispositivos Exchange ActiveSync novos ou alterados.
- **Provedor de Serviços Móveis:** Fornece uma interface de serviço web para que o XenMobile possa consultar o Exchange ActiveSync, consultar dispositivos Blackberry e emitir operações de controle, como Limpar, contra dispositivos ActiveSync e Blackberry.

Requisitos do sistema e pré-requisitos

Os seguintes requisitos mínimos de sistema são necessários para usar o conector do Endpoint Management para Exchange ActiveSync:

- Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Deve ser um servidor baseado em inglês. O suporte para Windows Server 2008 R2 Service Pack 1 termina em January 14, 2020 e o suporte para Windows Server 2012 R2 termina em October 10, 2023.
- Microsoft SQL Server 2016 Service Pack 2 ou SQL Server 2014 Service Pack 3.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, versão 5 (opcional).

Versões mínimas compatíveis do Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013 (o suporte termina em April 11, 2023)
- Exchange Server 2010 Service Pack 3 (o suporte termina em January 14, 2020)

Pré-requisitos

- O Windows Management Framework deve ser instalado.
    - PowerShell V5, V4 e V3
- A política de execução do PowerShell deve ser definida como RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- A porta TCP 80 deve estar aberta entre o computador que executa o conector do Endpoint Management para Exchange ActiveSync e o Exchange Server remoto.
- **Clientes de e-mail de dispositivo**: Nem todos os clientes de e-mail retornam consistentemente o mesmo ID do ActiveSync para um dispositivo. Como o conector do Endpoint Management para Exchange ActiveSync espera um ID do ActiveSync exclusivo para cada dispositivo, apenas os clientes de e-mail que geram consistentemente os mesmos IDs do ActiveSync exclusivos para cada dispositivo são compatíveis. Esses clientes de e-mail foram testados pela Citrix e funcionaram sem erros:
    - Cliente de e-mail nativo da Samsung
    - Cliente de e-mail nativo do iOS
- **Exchange**: Os requisitos para o computador local que executa o Exchange são os seguintes:

  As credenciais especificadas na interface do usuário de configuração do Exchange devem ser capazes de se conectar ao Exchange Server e ter acesso total para executar os seguintes cmdlets do PowerShell específicos do Exchange.
    - **Para Exchange Server 2010 SP2:**
        - Get-CASMailbox
        - Set-CASMailbox
        - Get-Mailbox
        - Get-ActiveSyncDevice
        - Get-ActiveSyncDeviceStatistics
        - Clear-ActiveSyncDevice
        - Get-ExchangeServer
        - Get-ManagementRole
        - Get-ManagementRoleAssignment
    - **Para Exchange Server 2013 e Exchange Server 2016:**

- Get-CASMailbox
- Set-CASMailbox
- Get-Mailbox
- Get-MobileDevice
- Get-MobileDeviceStatistics
- Clear-MobileDevice
- Get-ExchangeServer
- Get-ManagementRole
- Get-ManagementRoleAssignment

- Se o conector do Endpoint Management para Exchange ActiveSync estiver configurado para visualizar a floresta inteira, a permissão deve ter sido concedida para executar: **Set-AdServerSettings -ViewEntireForest $true**
- As credenciais fornecidas devem ter recebido o direito de se conectar ao Exchange Server via Shell remoto. Por padrão, o usuário que instalou o Exchange tem esse direito.
- Para estabelecer uma conexão remota e executar comandos remotos, as credenciais devem corresponder a um usuário que seja administrador na máquina remota. Você pode usar Set-PSSessionConfiguration para eliminar o requisito administrativo, mas a discussão desse comando está além do escopo deste documento. Para obter mais informações, consulte o artigo da Microsoft About Session Configurations.
- O Exchange Server deve ser configurado para suportar solicitações remotas do PowerShell via HTTP. Normalmente, um administrador executando o seguinte comando do PowerShell no Exchange Server é tudo o que é necessário: WinRM QuickConfig.
- O Exchange possui muitas políticas de limitação. Uma das políticas controla quantas conexões PowerShell simultâneas são permitidas por usuário. O número padrão de conexões simultâneas permitidas para um usuário é 18 no Exchange 2010. Quando o limite de conexão é atingido, o conector do Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo de conexões simultâneas permitidas via PowerShell que estão além do escopo desta documentação. Se estiver interessado, investigue as políticas de limitação do Exchange relacionadas ao gerenciamento remoto com PowerShell.

Requisitos para o Office 365 Exchange

- **Permissões:** As credenciais especificadas na interface do usuário de Configuração do Exchange devem ser capazes de se conectar ao Office 365 e ter acesso total para executar os seguintes cmdlets do PowerShell específicos do Exchange:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Privilégios:** As credenciais fornecidas devem ter recebido o direito de se conectar ao servidor do Office 365 via Shell remoto. Por padrão, o administrador online do Office 365 possui os privilégios necessários.
- **Políticas de limitação:** O Exchange possui muitas políticas de limitação. Uma das políticas controla quantas conexões PowerShell simultâneas são permitidas por usuário. O número padrão de conexões simultâneas permitidas para um usuário é três no Office 365. Quando o limite de conexão é atingido, o conector do Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo de conexões simultâneas permitidas via PowerShell que estão além do escopo desta documentação. Se estiver interessado, investigue as políticas de limitação do Exchange relacionadas ao gerenciamento remoto com PowerShell.

Instalar e configurar

1. Clique no arquivo XmmSetup.msi e siga as instruções do instalador para instalar o conector do Endpoint Management para Exchange ActiveSync.
2. Deixe **Iniciar o utilitário de configuração** selecionado na última tela do assistente de instalação. Ou, no menu **Iniciar**, abra o conector do Endpoint Management para Exchange ActiveSync.
3. Configure as seguintes propriedades do banco de dados:

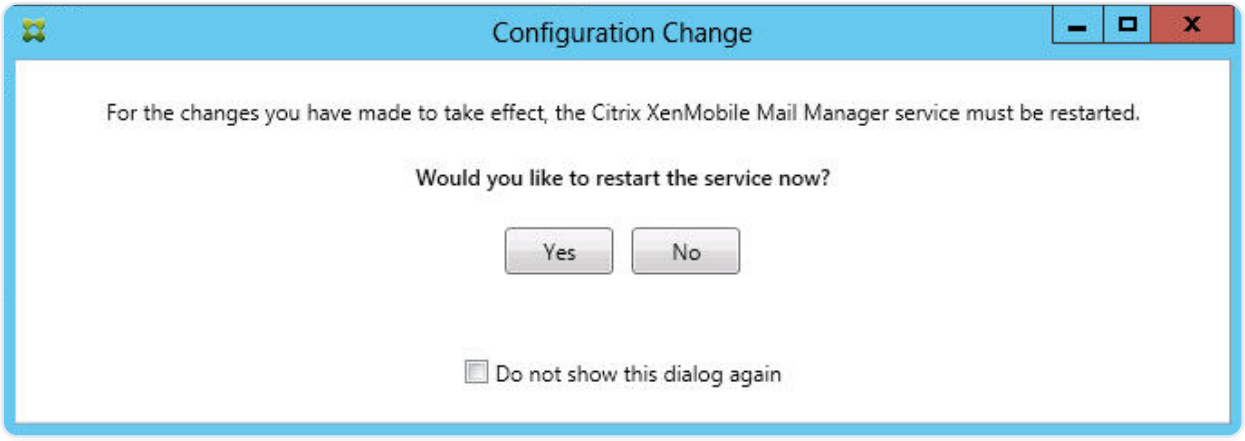
- Selecione a guia **Configurar > Banco de Dados**.
- Insira o nome do SQL Server (o padrão é localhost).
- Mantenha o banco de dados como o padrão **CitrixXmm**.

4. Selecione um dos seguintes modos de autenticação usados para SQL:

   - **SQL:** Insira o nome de usuário e a senha de um usuário SQL válido.
   - **Windows Integrado:** Se você selecionar esta opção, as credenciais de logon do serviço do conector do Endpoint Management para Exchange ActiveSync devem ser alteradas para uma conta do Windows que tenha permissões para acessar o SQL Server. Para fazer isso, abra o **Painel de Controle > Ferramentas Administrativas > Serviços**, clique com o botão direito do mouse na entrada do serviço do conector do Endpoint Management para Exchange ActiveSync e, em seguida, clique na guia **Fazer Logon**.

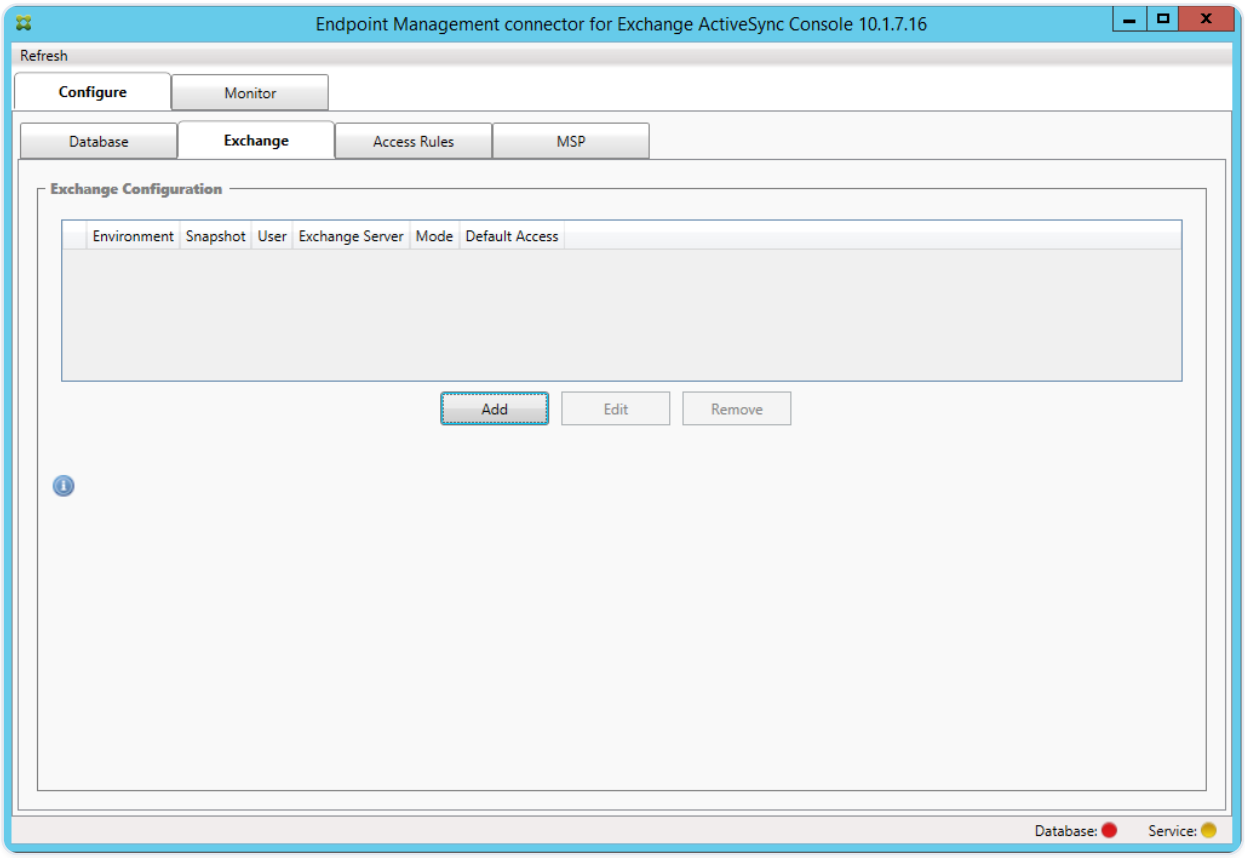
   Se o Windows Integrado também for escolhido para a conexão do banco de dados BlackBerry, a conta do Windows especificada aqui também deverá ter acesso ao banco de dados BlackBerry.

5. Clique em **Testar Conectividade** para verificar se uma conexão pode ser feita com o SQL Server e, em seguida, clique em **Salvar**.
6. Uma mensagem solicita que você reinicie o serviço. Clique em **Sim**.



7. Configure um ou mais Servidores Exchange:

   - Se estiver gerenciando um único ambiente Exchange, especifique apenas um servidor. Se estiver gerenciando vários ambientes Exchange, especifique um único Servidor Exchange para cada ambiente Exchange.
   - Clique na guia **Configurar > Exchange** e, em seguida, clique em **Adicionar**.



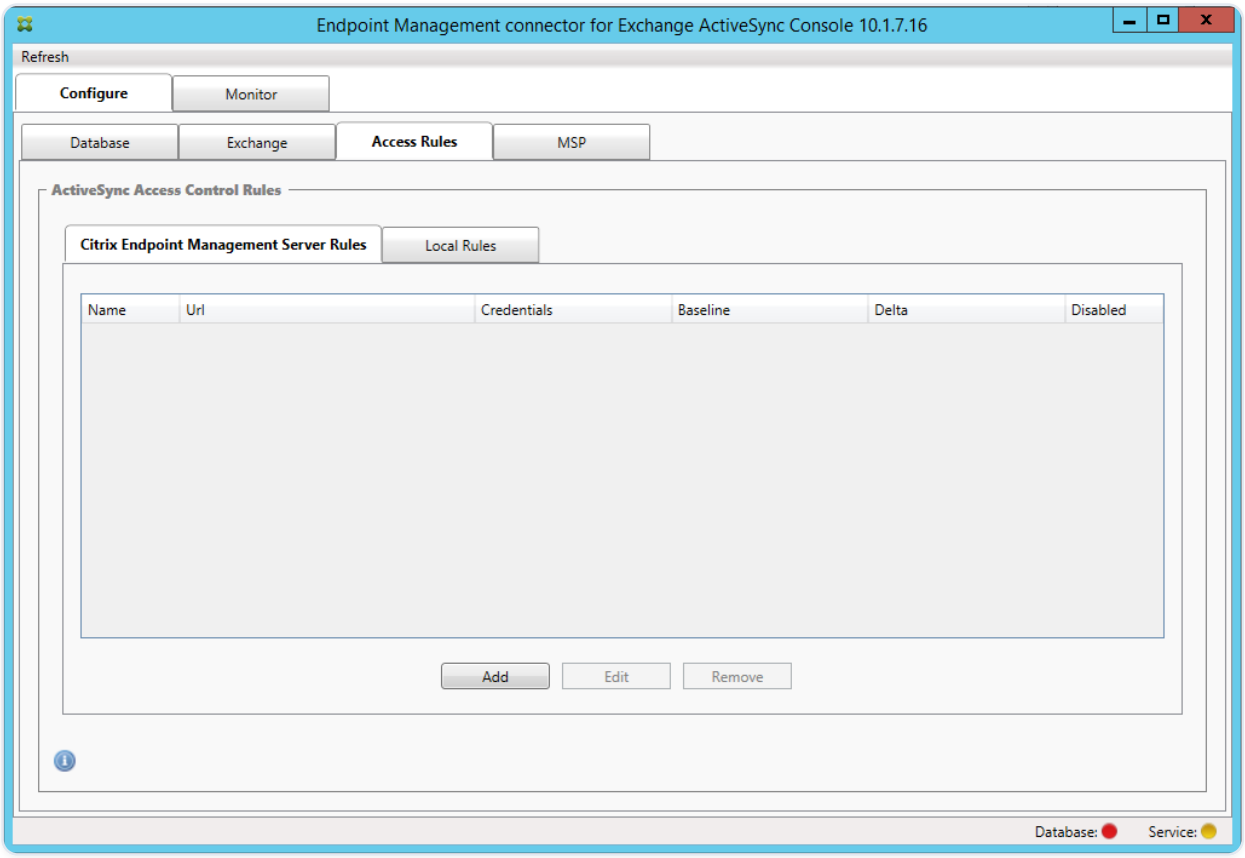
8. Selecione o tipo de ambiente do Servidor Exchange: **Local** ou **Office 365**.

   - Se você selecionar **Local**, insira o nome do Servidor Exchange a ser usado para comandos do PowerShell Remoto.
   - Insira o **nome de usuário** de uma identidade do Windows que tenha os direitos apropriados no Servidor Exchange, conforme especificado na seção Requisitos, e, em seguida, insira a **Senha** para o usuário.
   - Selecione o agendamento para executar snapshots principais. Um snapshot principal detecta cada parceria do Exchange ActiveSync.
   - Selecione o agendamento para executar instantâneos Menores. Um instantâneo menor detecta parcerias do Exchange ActiveSync recém-criadas.
   - Selecione o Tipo de Instantâneo: **Profundo** ou **Superficial**. Instantâneos superficiais são geralmente muito mais rápidos e suficientes para executar todas as funções de Controle de Acesso do Exchange ActiveSync do conector do Endpoint Management para Exchange ActiveSync. Instantâneos profundos podem demorar mais e são necessários apenas se o Provedor de Serviços Móveis estiver habilitado para ActiveSync. Esta opção permite que o XenMobile consulte dispositivos não gerenciados.
   - Selecione o Acesso Padrão: **Permitir**, **Bloquear** ou **Inalterado**. Essa configuração controla como todos os dispositivos, exceto aqueles identificados por regras explícitas do XenMobile ou Locais, são tratados. Se você selecionar **Permitir**, o acesso do ActiveSync a

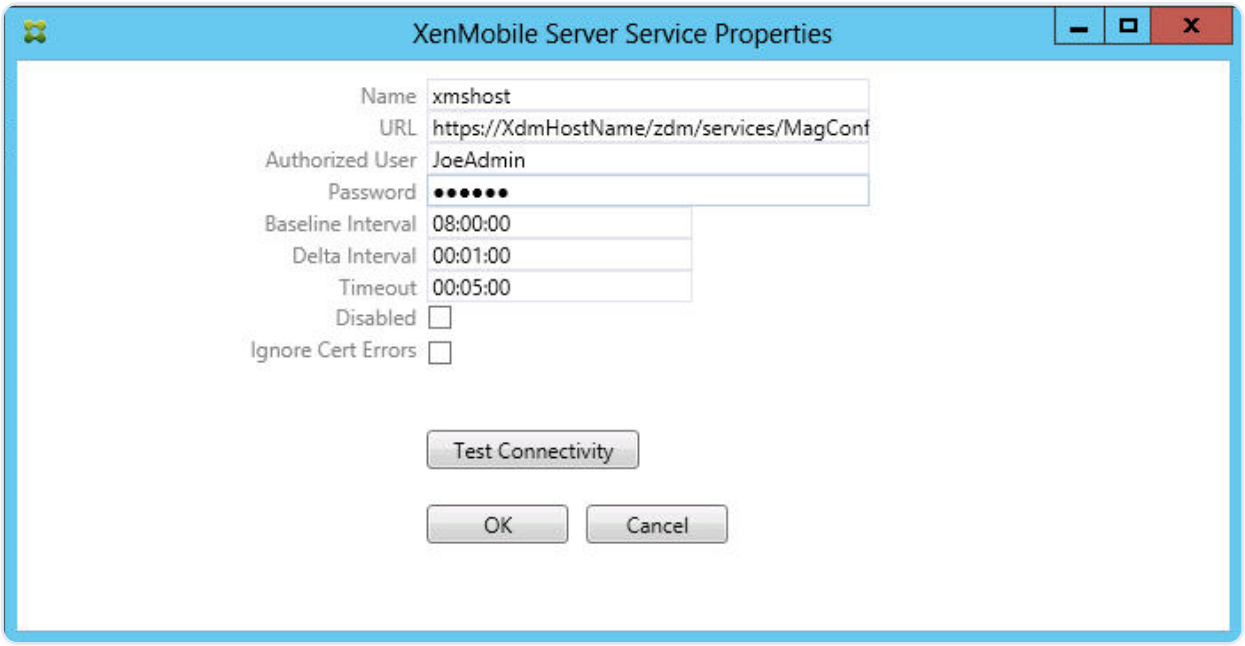
todos esses dispositivos será permitido. Se você selecionar **Bloquear**, o acesso será negado. Se você selecionar **Inalterado**, nenhuma alteração será feita.

- Selecione o Modo de Comando do ActiveSync: **PowerShell** ou **Simulação**.
- No modo **PowerShell**, o conector do Endpoint Management para Exchange ActiveSync emite comandos PowerShell para implementar o controle de acesso desejado. No modo de Simulação, o conector do Endpoint Management para Exchange ActiveSync não emite comandos PowerShell, mas registra o comando pretendido e os resultados pretendidos no banco de dados. No modo de Simulação, o usuário pode então usar a guia **Monitor** para ver o que teria acontecido se o modo PowerShell estivesse habilitado.
- Em **Expiração da Conexão**, defina as horas e minutos para a vida útil de uma conexão. Quando uma conexão atinge a idade especificada, ela é marcada como expirada, para que nunca mais seja usada. Quando a conexão expirada não é mais usada, o conector do Endpoint Management para Exchange ActiveSync encerra a conexão de forma elegante. Quando uma conexão é necessária novamente, uma nova conexão é inicializada se nenhuma estiver disponível. Se nada for especificado, o padrão de 30 minutos é usado.
- Selecione **Visualizar Floresta Inteira** para configurar o conector do Endpoint Management para Exchange ActiveSync para visualizar toda a floresta do Active Directory no ambiente Exchange.
- Selecione o protocolo de autenticação: **Kerberos** ou **Básico**. O conector do Endpoint Management para Exchange ActiveSync oferece suporte à autenticação Básica para implantações locais. Isso permite que o conector do Endpoint Management para Exchange ActiveSync seja usado quando o servidor do conector do Endpoint Management para Exchange ActiveSync não for membro do domínio em que o servidor Exchange reside.
- Clique em **Testar Conectividade** para verificar se uma conexão pode ser feita com o Servidor Exchange e, em seguida, clique em **Salvar**.
- Uma mensagem solicita que você reinicie o serviço. Clique em **Sim**.

9. Configure as regras de acesso: Selecione a guia **Configurar > Regras de Acesso**, clique na guia **Regras XMS** e, em seguida, clique em **Adicionar**.



10. Na página **Propriedades do Serviço do servidor XenMobile**, modifique a string de URL para apontar para o Servidor XenMobile. Por exemplo, se o nome da instância for **zdm**, insira `https://<XdmHostName>/zdm/services/MagConfigService`. No exemplo, substitua **XdmHostName** pelo endereço IP ou DNS do Servidor XenMobile.

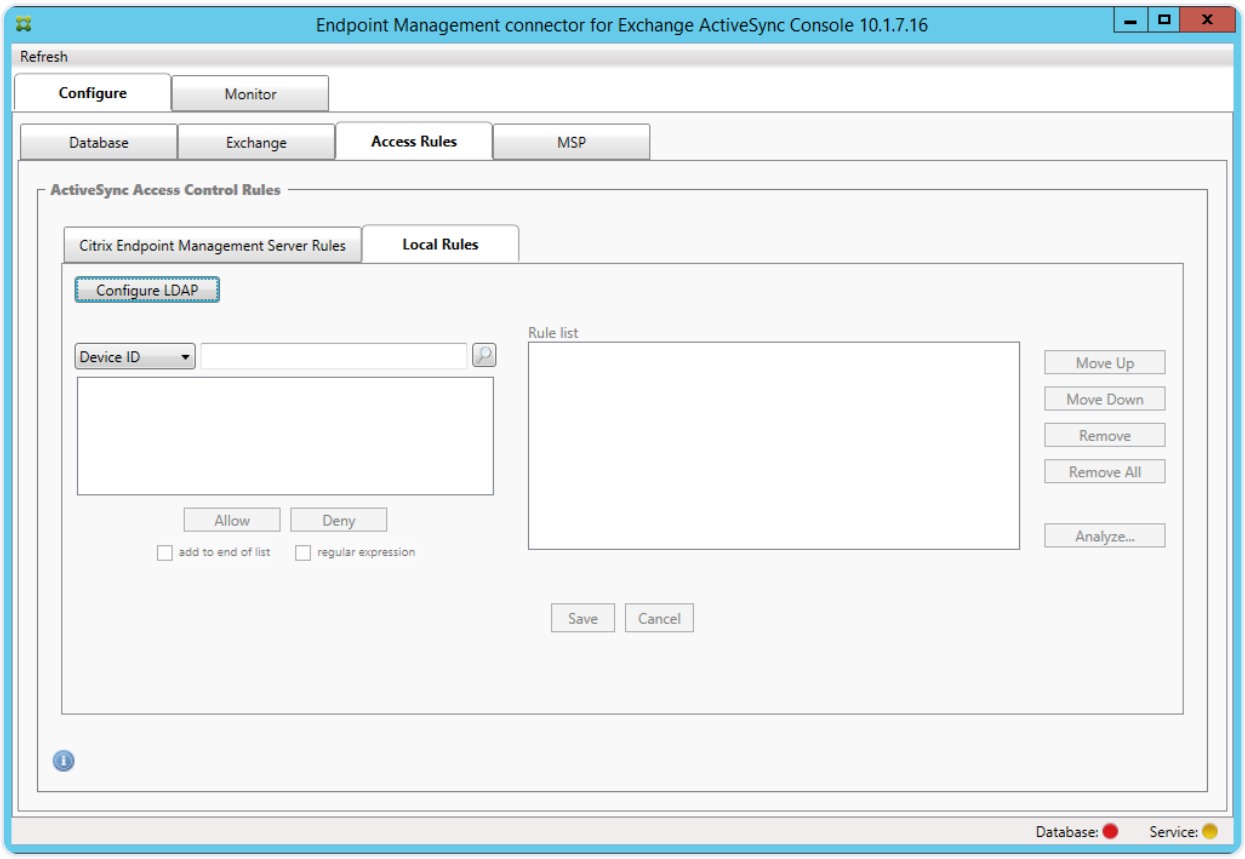


- Insira um usuário autorizado do servidor.
- Insira a senha do usuário.

- Mantenha os valores padrão para **Intervalo de Linha de Base**, **Intervalo Delta** e **Tempo Limite**.
- Clique em **Testar Conectividade** para verificar a conexão com o servidor e, em seguida, clique em **OK**.

Se a caixa de seleção **Desabilitado** estiver marcada, o XenMobile Mail Service não coletará políticas do XenMobile.

11. Clique na guia **Regras Locais**.



- Você pode adicionar regras locais com base no ID do Dispositivo ActiveSync, Tipo de Dispositivo, Grupo AD, Usuário ou UserAgent do dispositivo. Na lista, selecione o tipo apropriado.
- Insira texto ou fragmentos de texto na caixa de texto. Opcionalmente, clique no botão de consulta para visualizar as entidades que correspondem ao fragmento.

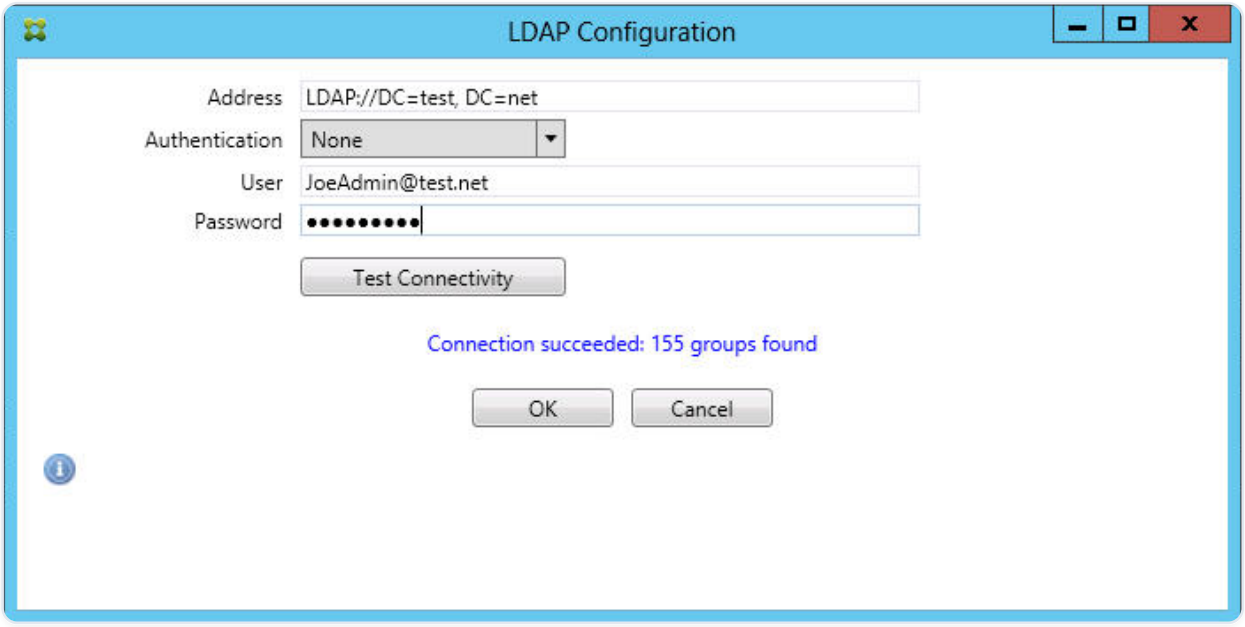
Para todos os tipos, exceto Grupo, o sistema depende dos dispositivos que foram encontrados em um instantâneo. Portanto, se você está apenas começando e ainda não concluiu um instantâneo, nenhuma entidade estará disponível.

- Selecione um valor de texto e clique em **Permitir** ou **Negar** para adicioná-lo ao painel **Lista de Regras** no lado direito. Você pode alterar a ordem das regras ou removê-las

usando os botões à direita do painel **Lista de Regras**. A ordem é importante porque, para um determinado usuário e dispositivo, as regras são avaliadas na ordem mostrada e uma correspondência em uma regra superior (mais próxima do topo) faz com que as regras subsequentes não tenham efeito. Por exemplo, se você tiver uma regra que permite todos os dispositivos iPad e uma regra subsequente que bloqueia o usuário Matt, o iPad de Matt ainda será permitido porque a regra do iPad tem uma prioridade efetiva maior do que a regra do Matt.

- Para realizar uma análise das regras dentro da lista de regras para encontrar quaisquer substituições, conflitos ou construções suplementares potenciais, clique em **Analisar** e, em seguida, clique em **Salvar**.

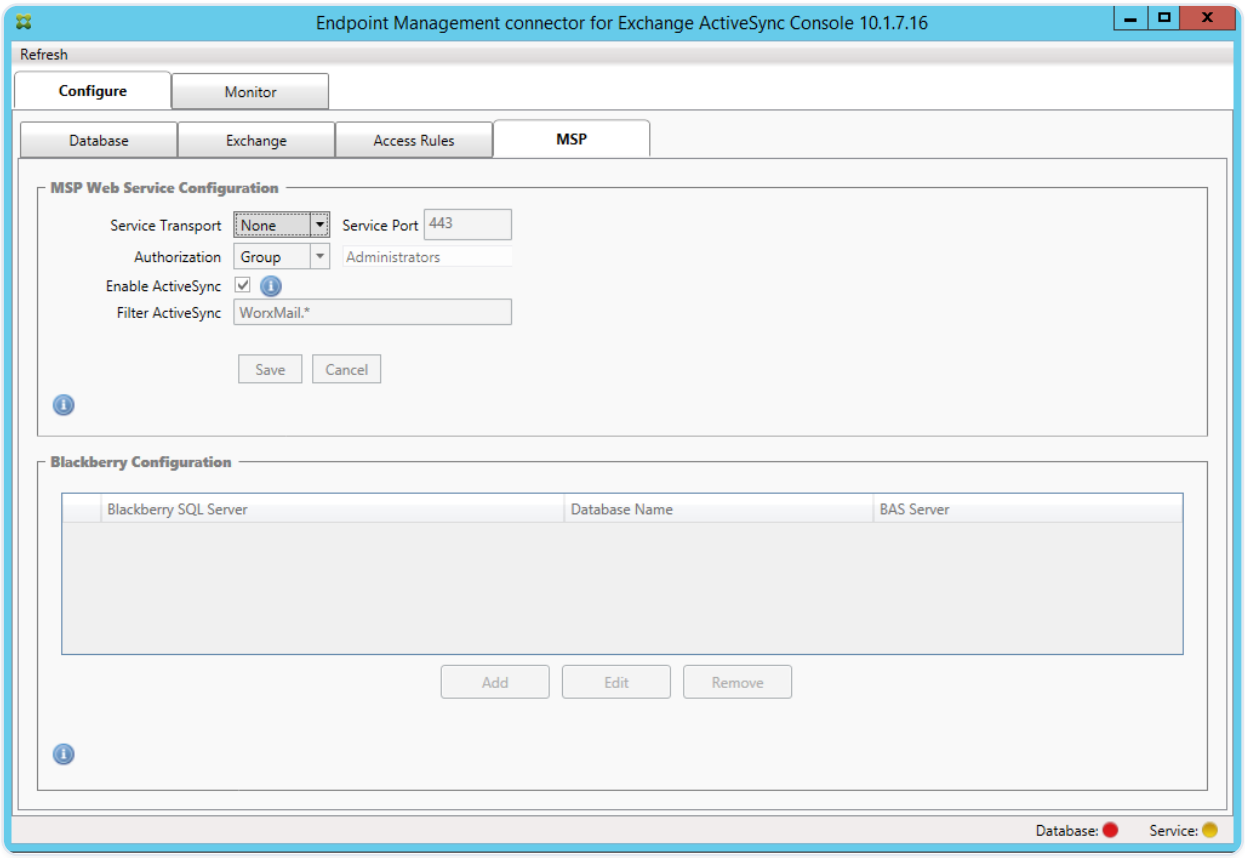
12. Se você quiser construir regras locais que operam em Grupos do Active Directory, clique em **Configurar LDAP** e, em seguida, configure as propriedades de conexão LDAP.



13. Configure o Provedor de Serviços Móveis.

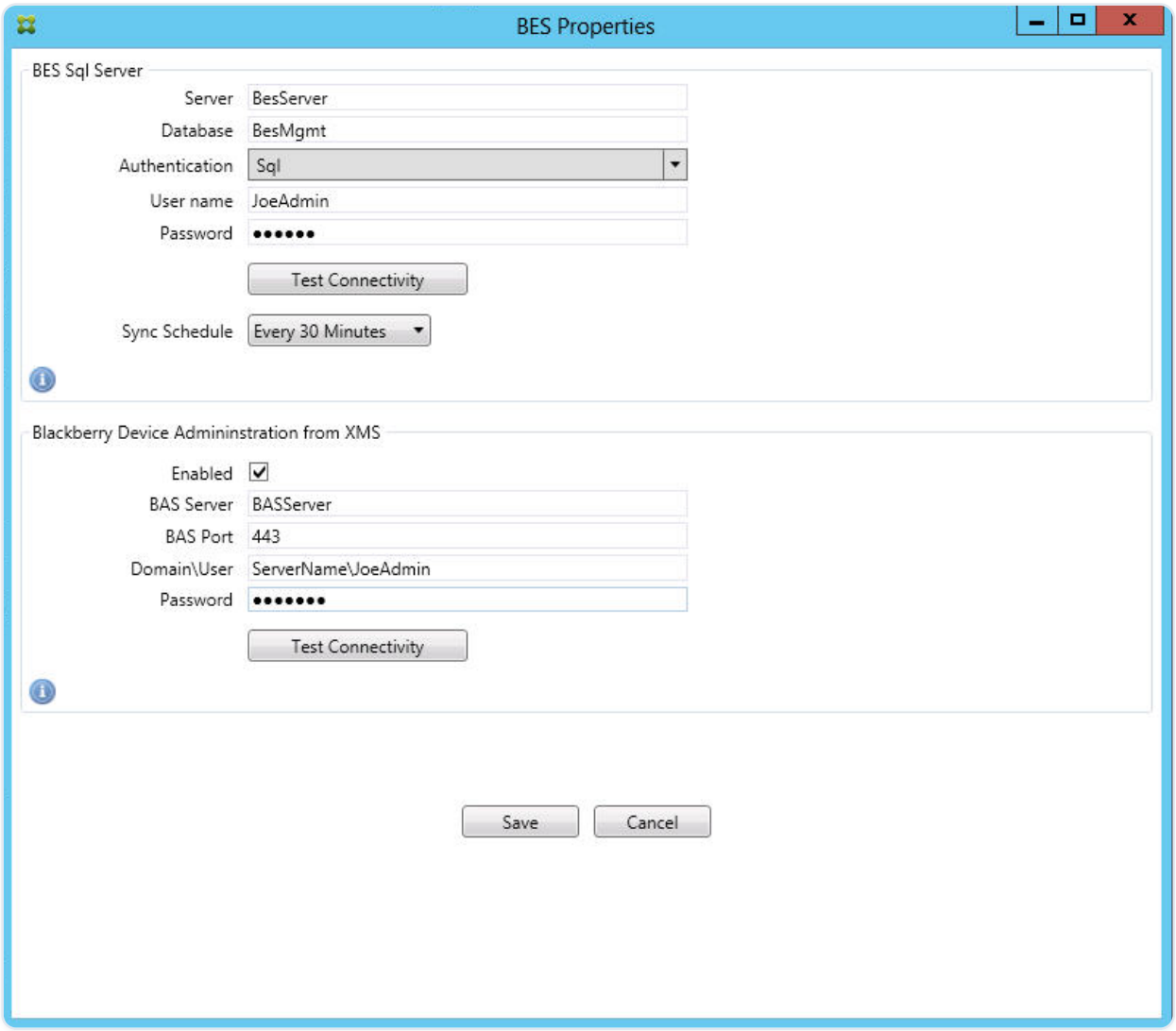
O Provedor de Serviços Móveis é opcional. Essa configuração é necessária apenas se o XenMobile também estiver configurado para usar a interface do Provedor de Serviços Móveis para consultar dispositivos não gerenciados.

- Clique na guia **Configure > MSP**.



- Defina o tipo de transporte de serviço como **HTTP** ou **HTTPS** para o serviço do Provedor de Serviços Móveis.
- Defina a **porta de serviço** (geralmente 80 ou 443) para o serviço do Provedor de Serviços Móveis. Se você usar a porta 443, a porta exigirá um certificado SSL vinculado a ela no IIS.
- Defina o **Grupo de Autorização** ou **Usuário**. Isso define o usuário ou conjunto de usuários que poderão se conectar ao serviço do Provedor de Serviços Móveis a partir do XenMobile.
- Defina se as consultas do ActiveSync estão ativadas ou não. Se as consultas do ActiveSync estiverem ativadas para o XenMobile Server, o tipo de Snapshot para um ou mais Exchange Servers deve ser definido como **Deep**. Essa configuração pode ter custos de desempenho significativos para a criação de snapshots.
- Por padrão, os dispositivos ActiveSync que correspondem à expressão regular WorxMail.* não serão enviados para o XenMobile. Para alterar esse comportamento, modifique o campo **Filtrar ActiveSync** conforme necessário. Em branco significa que todos os dispositivos são encaminhados para o XenMobile.
- Clique em **Salvar**.

14. Opcionalmente, configure uma ou mais instâncias do BlackBerry Enterprise Server (BES): Clique em **Adicionar** e, em seguida, insira o nome do servidor do BES SQL Server.



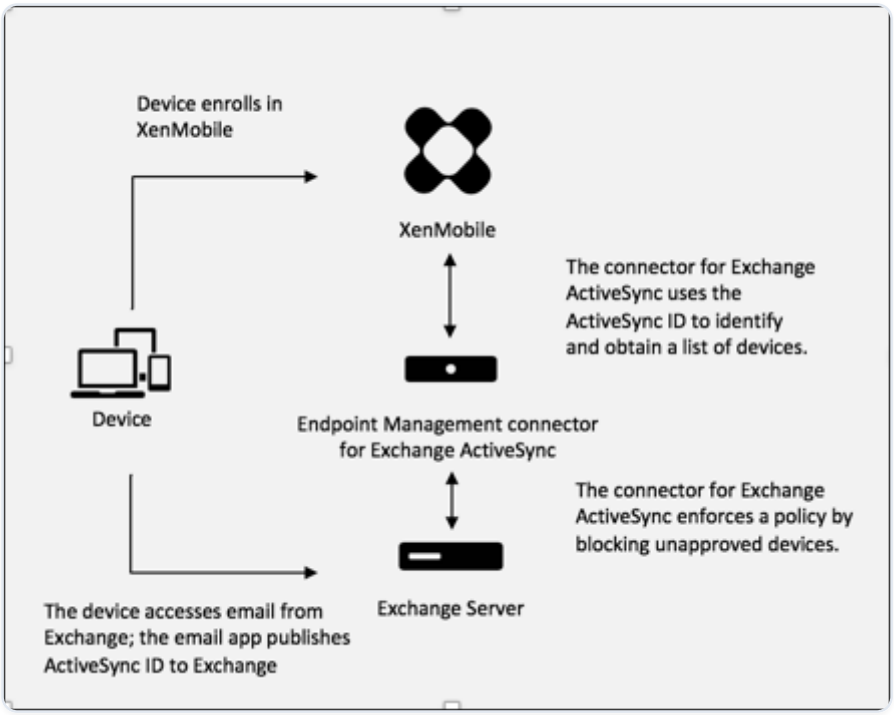
- Insira o nome do banco de dados de gerenciamento do BES.
- Selecione o modo de **Autenticação**. Se você selecionar a autenticação Integrada do Windows, a conta de usuário do serviço do conector do Endpoint Management para Exchange ActiveSync é a conta usada para se conectar ao BES SQL Server. Se você também escolher Integrada do Windows para a conexão do banco de dados do conector do Endpoint Management para Exchange ActiveSync, a conta do Windows especificada aqui também deverá ter acesso ao banco de dados do conector do Endpoint Management para Exchange ActiveSync.
- Se você selecionar a **autenticação SQL**, insira o nome de usuário e a senha.
- Defina o **Agendamento de Sincronização**. Este é o agendamento usado para se conectar ao BES SQL Server e verificar se há atualizações de dispositivos.
- Clique em **Testar Conectividade** para verificar a conectividade com o SQL Server. Se você selecionar Integrado do Windows, este teste usará o usuário atualmente logado e não o usuário do serviço do conector do Endpoint Management para Exchange ActiveSync e, portanto, não testará com precisão a autenticação SQL.

- Para oferecer suporte a Wipe e ResetPassword remotos de dispositivos BlackBerry do XenMobile, selecione a caixa de seleção **Enabled**.
- Insira o nome de domínio totalmente qualificado (FQDN) do BES.
- Insira a porta BES usada para o serviço web de administração.
- Insira o usuário totalmente qualificado e a senha exigidos pelo serviço BES.
- Clique em **Testar Conectividade** para testar a conexão com o BES.
- Clique em **Salvar**.

Aplicar políticas de e-mail com IDs do ActiveSync

Sua política de e-mail corporativo pode ditar que certos dispositivos não são aprovados para uso de e-mail corporativo. Para seguir esta política, você deseja garantir que os funcionários não possam acessar o e-mail corporativo a partir de tais dispositivos. O conector do Endpoint Management para Exchange ActiveSync e o XenMobile trabalham juntos para aplicar tal política de e-mail. O XenMobile define a política para acesso ao e-mail corporativo e, quando um dispositivo não aprovado se registra no XenMobile, o conector do Endpoint Management para Exchange ActiveSync aplica a política.

O cliente de e-mail em um dispositivo se anuncia ao Exchange Server (ou Office 365) usando o ID do dispositivo, também conhecido como ID do ActiveSync, que é usado para identificar o dispositivo. O Secure Hub obtém um identificador semelhante e o envia ao XenMobile quando o dispositivo é registrado. Ao comparar os dois IDs de dispositivo, o conector do Endpoint Management para Exchange ActiveSync pode determinar se um dispositivo específico deve ter acesso ao e-mail corporativo. A figura a seguir ilustra este conceito:



Se o XenMobile enviar ao conector do Endpoint Management para Exchange ActiveSync um ID do ActiveSync que seja diferente do ID que o dispositivo publica para o Exchange, o conector do Endpoint Management para Exchange ActiveSync não poderá indicar ao Exchange o que fazer com o dispositivo.

A correspondência de IDs do ActiveSync funciona de forma confiável na maioria das plataformas. No entanto, a Citrix descobriu que, em algumas implementações do Android, o ID do ActiveSync do dispositivo é diferente do ID que o cliente de e-mail anuncia ao Exchange. Para mitigar esse problema, você pode fazer o seguinte:

- Na plataforma Samsung SAFE, envie a configuração do ActiveSync do dispositivo a partir do XenMobile.

Para garantir que sua política de acesso ao e-mail corporativo seja aplicada corretamente, você pode adotar uma postura de segurança defensiva e configurar o conector do Endpoint Management para Exchange ActiveSync para bloquear e-mails definindo a política estática como Negar por padrão. Isso significa que, se um funcionário configurar um cliente de e-mail em um dispositivo Android e se a detecção do ID do ActiveSync não funcionar corretamente, o funcionário terá o acesso ao e-mail corporativo negado.

Regras de controle de acesso

O conector do Endpoint Management para Exchange ActiveSync oferece uma abordagem baseada em regras para configurar dinamicamente o controle de acesso para dispositivos Exchange ActiveSync. Uma regra de controle de acesso do conector do Endpoint Management

para Exchange ActiveSync consiste em duas partes: uma expressão de correspondência e um estado de acesso desejado (Permitir ou Bloquear). Uma regra pode ser avaliada em relação a um determinado dispositivo Exchange ActiveSync para determinar se a regra se aplica ou corresponde ao dispositivo. Existem vários tipos de expressões de correspondência; por exemplo, uma regra pode corresponder a todos os dispositivos de um determinado Tipo de Dispositivo, ou a um ID de dispositivo Exchange ActiveSync específico, ou a todos os dispositivos de um usuário específico, e assim por diante.

A qualquer momento durante a adição, remoção e reorganização das regras na lista de regras, clicar no botão **Cancelar** reverte a lista de regras para o estado em que estava quando foi aberta pela primeira vez. A menos que você clique em **Salvar**, quaisquer alterações feitas nesta janela serão perdidas se você fechar a ferramenta Configurar.

O conector do Endpoint Management para Exchange ActiveSync possui três tipos de regras: regras locais, regras do XenMobile Server (também conhecidas como regras XDM) e a regra de acesso padrão.

Regras locais: As regras locais têm a prioridade mais alta: se um dispositivo for correspondido por uma regra local, a avaliação da regra é interrompida. Nem as regras do XenMobile Server nem as regras de acesso padrão serão consultadas. As regras locais são configuradas localmente para o conector do Endpoint Management para Exchange ActiveSync através da guia **Configurar > Regras de Acesso > Regras Locais**. A correspondência de suporte é baseada na associação de um usuário a um determinado grupo do Active Directory. A correspondência de suporte é baseada em expressões regulares para os seguintes campos:

- ID do Dispositivo Active Sync
- Tipo de Dispositivo ActiveSync
- Nome Principal do Usuário (UPN)
- Agente de Usuário ActiveSync (geralmente a plataforma do dispositivo ou cliente de e-mail)

Desde que um snapshot principal tenha sido concluído e encontrado dispositivos, você deve ser capaz de adicionar uma regra normal ou de expressão regular. Se um snapshot principal não tiver sido concluído, você só poderá adicionar regras de expressão regular.

Regras do servidor XenMobile: As regras do XenMobile Server são referências a um XenMobile Server externo que fornece regras sobre dispositivos gerenciados. O XenMobile Server pode ser configurado com suas próprias regras de alto nível que identificam os dispositivos a serem permitidos ou bloqueados com base em propriedades conhecidas pelo XenMobile, como se o dispositivo está com jailbreak ou se contém aplicativos proibidos. O XenMobile avalia as regras de

alto nível e produz um conjunto de IDs de Dispositivo ActiveSync permitidos ou bloqueados, que são então entregues ao conector do Endpoint Management para Exchange ActiveSync.

Regra de acesso padrão: A regra de acesso padrão é única, pois pode potencialmente corresponder a todos os dispositivos e é sempre avaliada por último. Esta regra é a regra de captura geral, o que significa que se um determinado dispositivo não corresponder a uma regra local ou do XenMobile Server, o estado de acesso desejado do dispositivo é determinado pelo estado de acesso desejado da regra de acesso padrão.

- **Acesso Padrão – Permitir:** Qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será permitido.
- **Acesso Padrão – Bloquear:** Qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será bloqueado.
- **Acesso Padrão - Inalterado:** Qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server não terá seu estado de acesso modificado de forma alguma pelo conector do Endpoint Management para Exchange ActiveSync. Se um dispositivo tiver sido colocado no modo de Quarentena pelo Exchange, nenhuma ação será tomada. Por exemplo, a única maneira de remover um dispositivo do modo de Quarentena é ter uma regra Local ou XDM explícita que substitua a quarentena.

Sobre as avaliações de regras

Para cada dispositivo que o Exchange relata ao conector do Endpoint Management para Exchange ActiveSync, as regras são avaliadas em sequência, da prioridade mais alta para a mais baixa, da seguinte forma:

- Regras locais
- Regras do XenMobile Server
- Regra de acesso padrão

Quando uma correspondência é encontrada, a avaliação para. Por exemplo, se uma regra local corresponder a um determinado dispositivo, o dispositivo não será avaliado em relação a nenhuma das regras do XenMobile Server ou à regra de acesso padrão. Isso também é válido para um determinado tipo de regra. Por exemplo, se houver mais de uma correspondência para um determinado dispositivo na lista de regras locais, quando a primeira correspondência for encontrada, a avaliação para.

O conector do Endpoint Management para Exchange ActiveSync reavalia o conjunto de regras atualmente definido quando as propriedades do dispositivo mudam, ou quando os dispositivos são

adicionados ou removidos, ou quando as próprias regras mudam. Os snapshots principais capturam as alterações e remoções de propriedades do dispositivo em intervalos configuráveis. Os snapshots secundários capturam novos dispositivos em intervalos configuráveis.

O Exchange ActiveSync também possui regras que governam o acesso. É importante entender como essas regras funcionam no contexto do conector do Endpoint Management para Exchange ActiveSync. O Exchange pode ser configurado com três níveis de regras: isenções pessoais, regras de dispositivo e configurações da organização. O conector do Endpoint Management para Exchange ActiveSync automatiza o controle de acesso emitindo programaticamente solicitações do Remote PowerShell para afetar as listas de isenções pessoais. Estas são listas de IDs de dispositivo do Exchange ActiveSync permitidos ou bloqueados associados a uma determinada caixa de correio. Quando implantado, o conector do Endpoint Management para Exchange ActiveSync efetivamente assume o gerenciamento da capacidade de listas de isenção dentro do Exchange. Para obter detalhes, consulte o artigo da Microsoft, Controlling Device Access.

A análise é útil em situações em que várias regras para o mesmo campo foram definidas. Você pode solucionar problemas de relacionamento entre as regras. Você realiza a análise da perspectiva dos campos da regra. Por exemplo, as regras são analisadas em grupos com base no campo que está sendo correspondido, como ID do dispositivo ActiveSync, tipo de dispositivo ActiveSync, Usuário, Agente do Usuário.

Terminologia da regra

- **Regra de substituição:** Uma substituição ocorre quando mais de uma única regra pode ser aplicada ao mesmo dispositivo. Como as regras são avaliadas por prioridade na lista, as instâncias de regras posteriores que poderiam ser aplicadas podem nunca ser avaliadas.
- **Regra conflitante:** Um conflito ocorre quando mais de uma única regra pode ser aplicada ao mesmo dispositivo, mas o acesso (Permitir/Bloquear) não corresponde. Se as regras conflitantes não forem regras de expressão regular, um conflito sempre conota implicitamente uma substituição.
- **Regra suplementar:** Um suplemento ocorre quando mais de uma regra é uma regra de expressão regular e, portanto, pode haver a necessidade de garantir que as duas (ou mais) expressões regulares possam ser combinadas em uma única regra de expressão regular, ou não estejam duplicando a funcionalidade. Uma regra suplementar também pode entrar em conflito em seu acesso (Permitir/Bloquear).
- **Regra primária:** A regra primária é a regra que foi clicada dentro da caixa de diálogo. A regra é indicada visualmente por uma linha de borda sólida que a circunda. A regra também terá uma ou duas setas verdes apontando para cima ou para baixo. Se uma seta apontar para

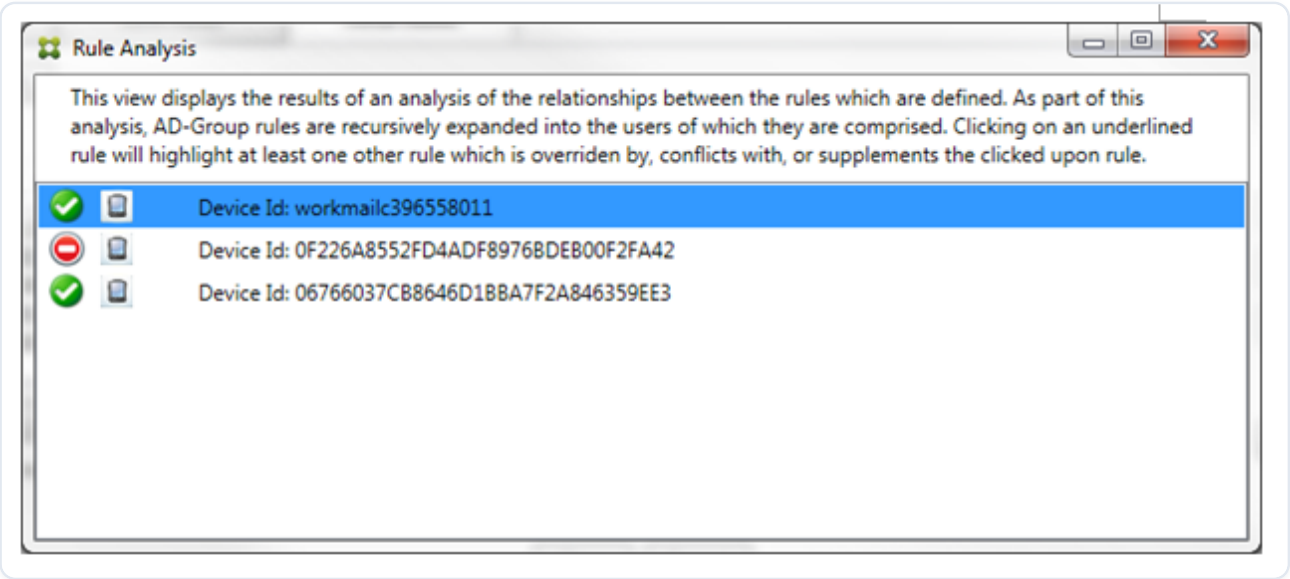
cima, a seta indica que existem regras auxiliares que precedem a regra primária. Se uma seta apontar para baixo, isso indica que existem regras auxiliares que vêm depois da regra primária. Apenas uma única regra primária pode estar ativa a qualquer momento.

- **Regra auxiliar:** Uma regra auxiliar está relacionada de alguma forma à regra primária, seja por meio de substituição, conflito ou relacionamento suplementar. As regras são indicadas visualmente por uma borda tracejada que as circunda. Para cada regra primária, pode haver de uma a muitas regras auxiliares. Ao clicar em qualquer entrada sublinhada, a regra ou regras auxiliares que são destacadas são sempre da perspectiva da regra primária. Por exemplo, a regra auxiliar é substituída pela regra primária, e/ou a regra auxiliar entrará em conflito em seu acesso com a regra primária, e/ou a regra auxiliar suplementará a regra primária.

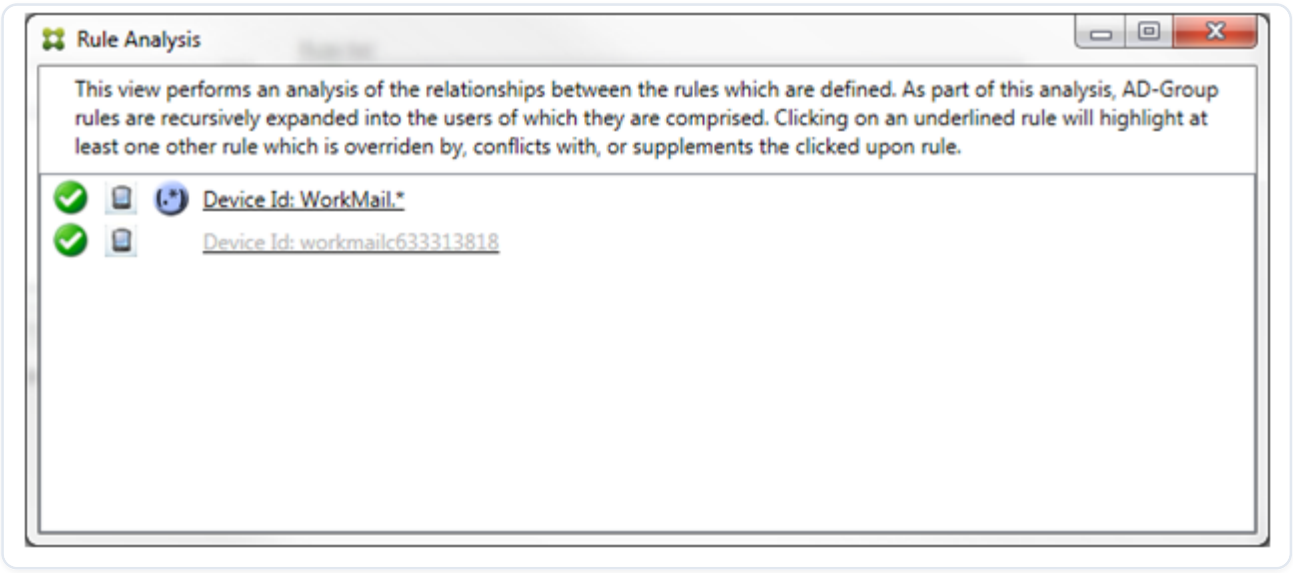
Como os tipos de regras aparecem na caixa de diálogo Análise de Regras

Quando não há conflitos, substituições ou complementos, a caixa de diálogo Análise de Regras não tem entradas sublinhadas. Clicar em qualquer um dos itens não tem impacto; por exemplo, visuais normais de itens selecionados ocorrem.

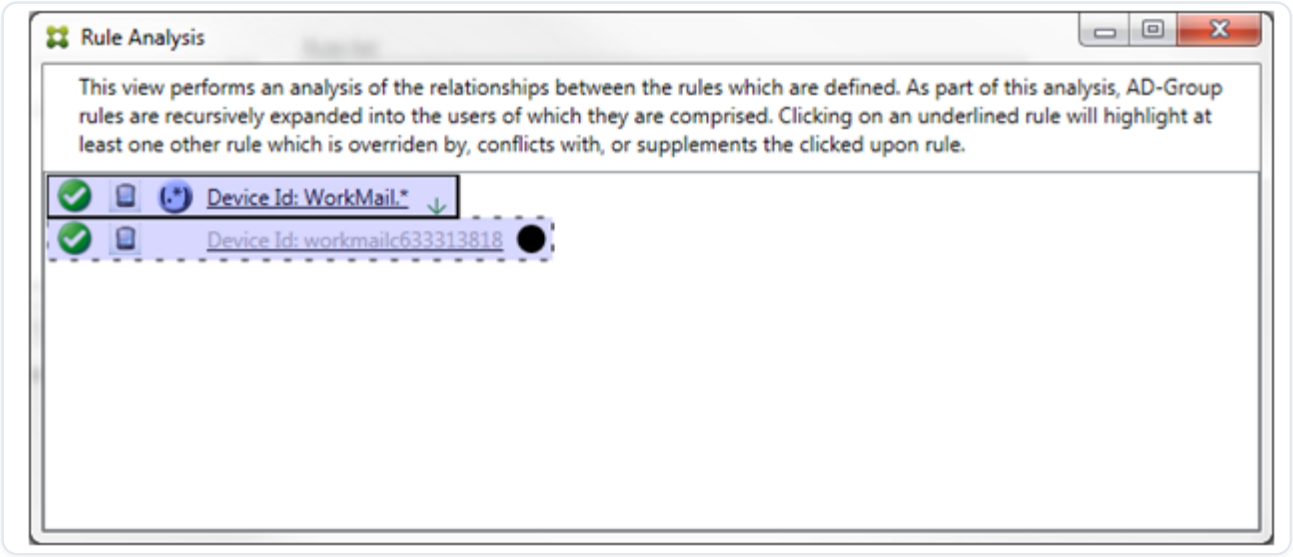
A janela Análise de Regras tem uma caixa de seleção que, quando selecionada, exibe apenas as regras que são conflitos, substituições, redundâncias ou complementos.



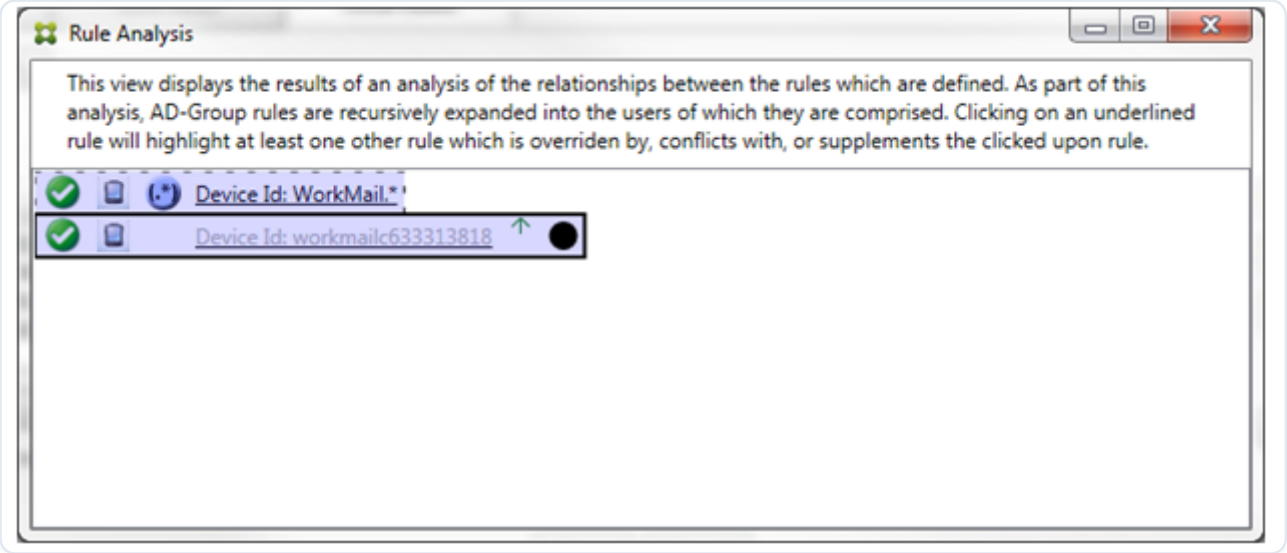
Quando ocorre uma substituição, pelo menos duas regras serão sublinhadas: a regra primária e a regra ou regras auxiliares. Pelo menos uma regra auxiliar aparece em uma fonte mais clara para indicar que a regra foi substituída por uma regra de prioridade mais alta. Você pode clicar na regra substituída para descobrir qual regra ou regras a substituíram. Sempre que uma regra substituída for destacada, seja porque a regra é a primária ou a auxiliar, um círculo preto aparece ao lado dela como uma indicação visual adicional de que a regra está inativa. Por exemplo, antes de clicar na regra, a caixa de diálogo aparece da seguinte forma:



Ao clicar na regra de maior prioridade, a caixa de diálogo aparece da seguinte forma:

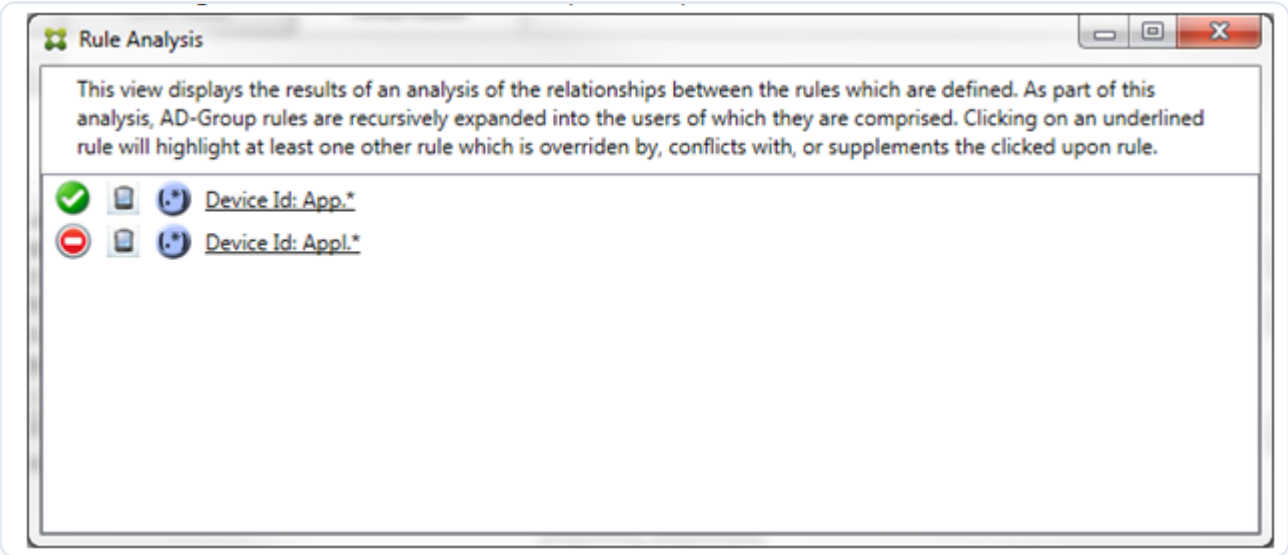


Neste exemplo, a regra de expressão regular `WorkMail.*` é a regra primária (indicada pela borda sólida) e a regra normal `workmailc633313818` é uma regra auxiliar (indicada pela borda tracejada). O ponto preto ao lado da regra auxiliar é uma pista visual que indica ainda que a regra está inativa (nunca será avaliada) devido à regra de expressão regular de maior prioridade que a precede. Depois de clicar na regra substituída, a caixa de diálogo aparece da seguinte forma:



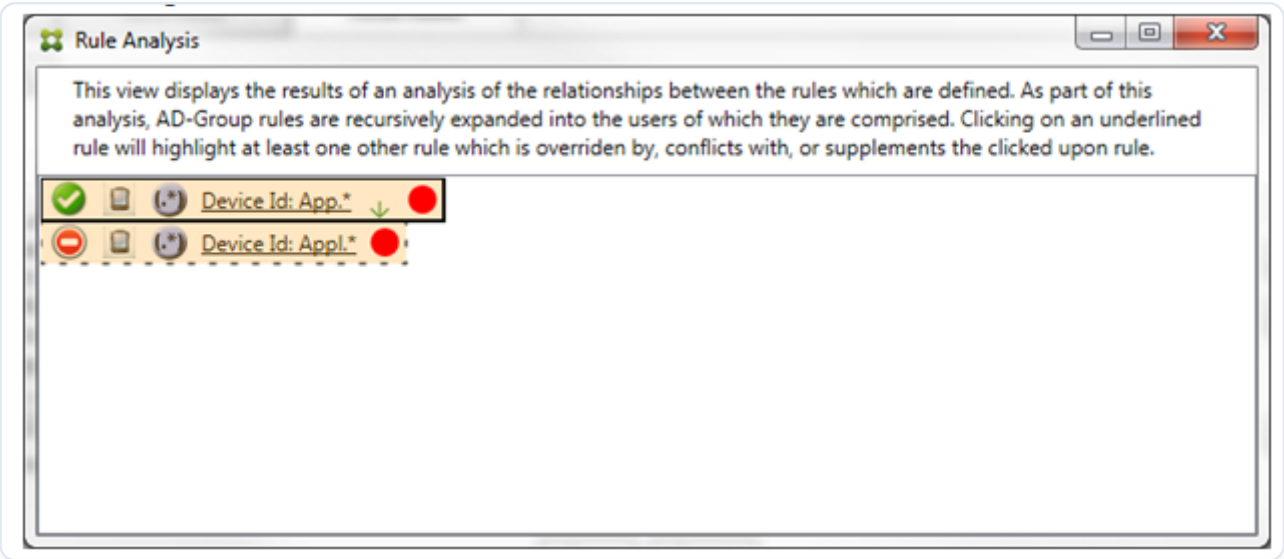
No exemplo anterior, a regra de expressão regular `WorkMail.*` é a regra auxiliar (indicada pela borda tracejada) e a regra normal `workmailc633313818` é uma regra primária (indicada pela borda sólida). Para este exemplo simples, não há muita diferença. Para um exemplo mais complicado, consulte o exemplo de expressão complexa mais adiante neste tópico. Em um cenário com muitas regras definidas, clicar na regra substituída identificaria rapidamente qual regra ou regras a substituíram.

Quando ocorre um conflito, pelo menos duas regras serão sublinhadas: a regra primária e a regra ou regras auxiliares. As regras em conflito são indicadas por um ponto vermelho. Regras que só conflitam entre si só são possíveis com duas ou mais regras de expressão regular definidas. Em todos os outros cenários de conflito, haverá não apenas um conflito, mas também uma substituição em jogo. Antes de clicar em qualquer uma das regras em um exemplo simples, a caixa de diálogo aparece da seguinte forma:



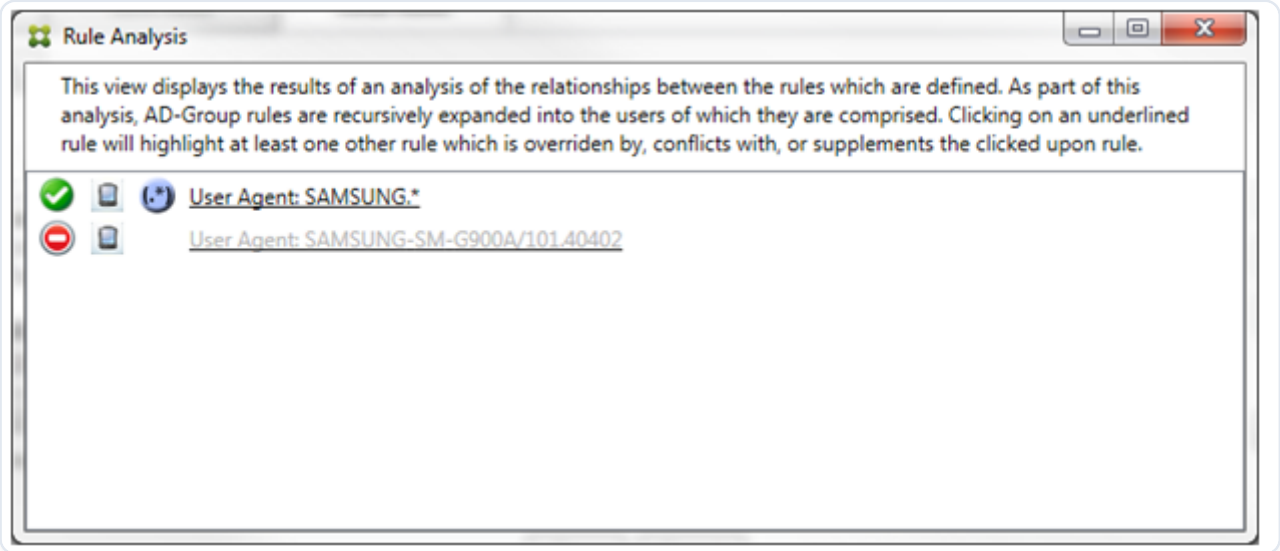
Ao inspecionar as duas regras de expressão regular, é evidente que a primeira regra permite todos os dispositivos com um ID de dispositivo que contém "App" e que a segunda regra nega

todos os dispositivos com um ID de dispositivo que contém "Appl". Além disso, embora a segunda regra negue todos os dispositivos com um ID de dispositivo que contém "Appl", nenhum dispositivo que corresponda aos critérios será negado devido à maior precedência da regra de permissão. Depois de clicar na primeira regra, a caixa de diálogo aparece da seguinte forma:



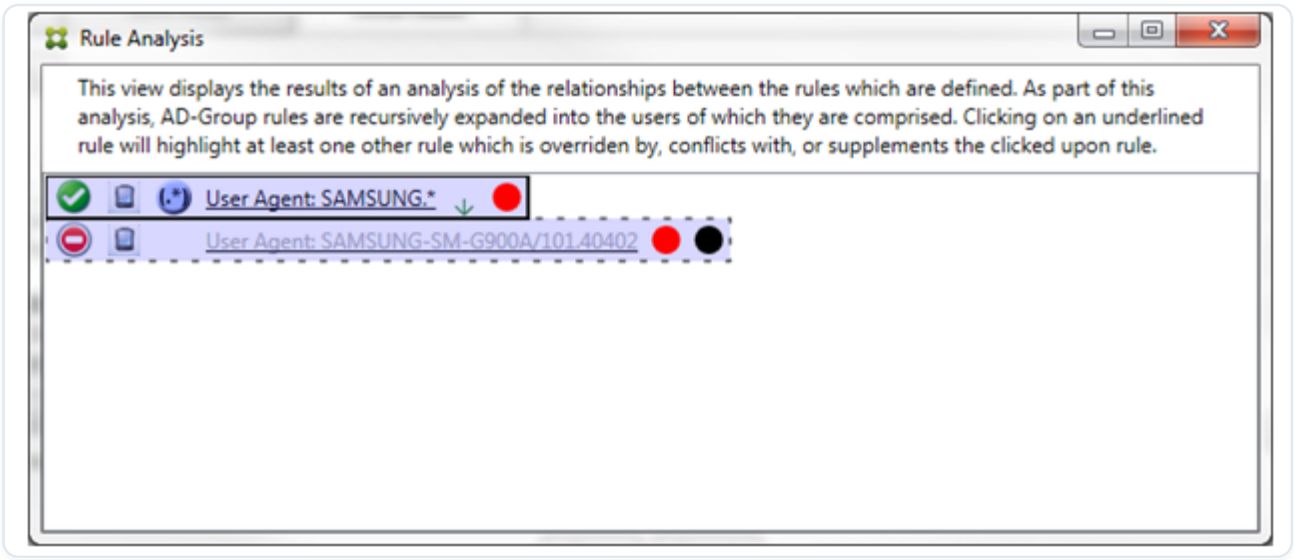
No cenário anterior, tanto a regra primária (regra de expressão regular `App.*`) quanto a regra auxiliar (regra de expressão regular `Appl.*`) são destacadas em amarelo. Este é simplesmente um aviso visual para alertá-lo para o fato de que você aplicou mais de uma única regra de expressão regular a um único campo correspondente, o que pode significar um problema de redundância ou algo mais sério.

Em um cenário com conflito e substituição, tanto a regra primária (regra de expressão regular `App.*`) quanto a regra auxiliar (regra de expressão regular `Appl.*`) são destacadas em amarelo. Isso é simplesmente um aviso visual para alertá-lo sobre o fato de que você aplicou mais de uma única regra de expressão regular a um único campo correspondente, o que pode significar um problema de redundância ou algo mais sério.



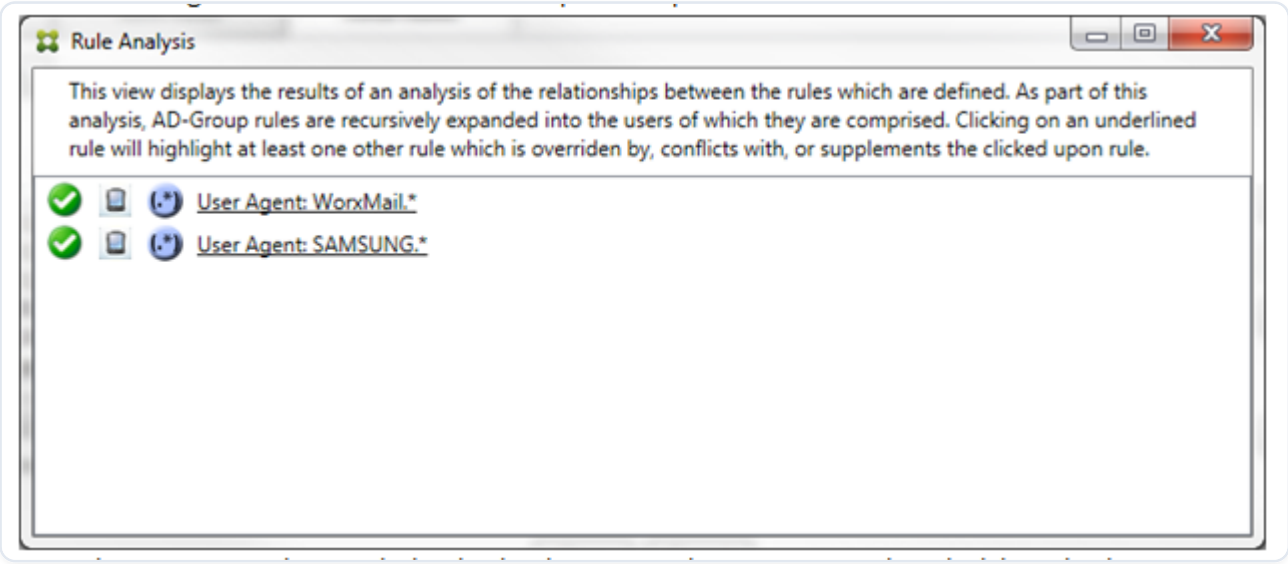
É fácil ver no exemplo anterior que a primeira regra (regra de expressão regular `SAMSUNG.*`) não apenas substitui a próxima regra (regra normal `SAMSUNG-SM-G900A/101.40402`), mas que as duas regras diferem em seu acesso (a primária especifica Permitir, a auxiliar especifica Bloquear). A segunda regra (regra normal `SAMSUNG-SM-G900A/101.40402`) é exibida em texto mais claro para indicar que foi substituída e, portanto, está inativa.

Após clicar na regra de expressão regular, a caixa de diálogo aparece da seguinte forma:

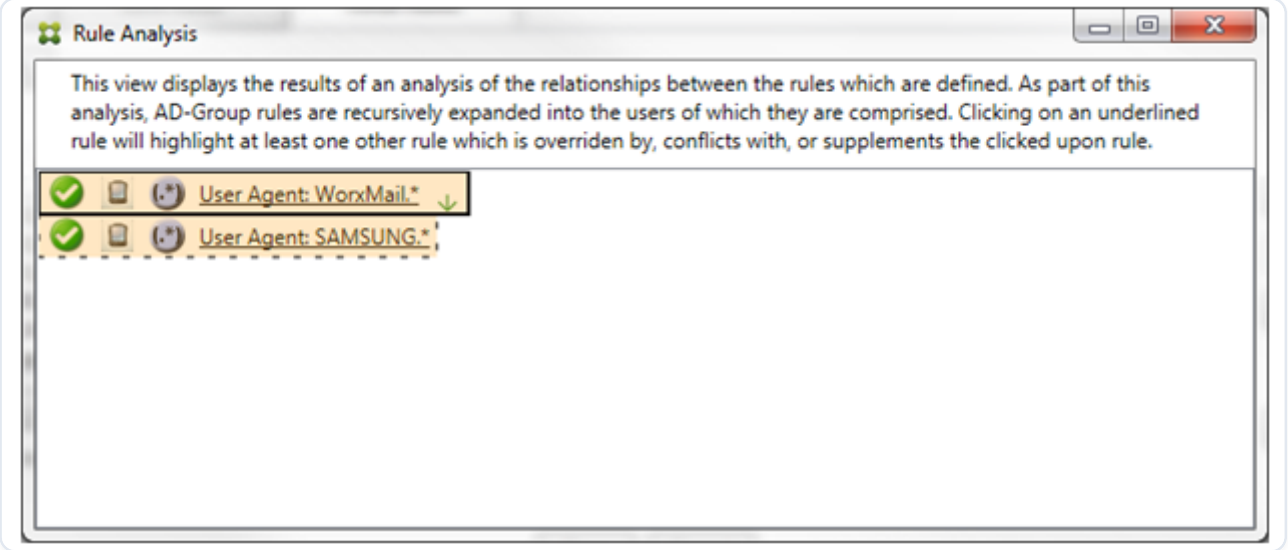


A regra primária (regra de expressão regular `SAMSUNG.*`) é seguida por um ponto vermelho para indicar que seu estado de acesso conflita com uma ou mais regras auxiliares. A regra auxiliar (regra normal `SAMSUNG-SM-G900A/101.40402`) é seguida por um ponto vermelho para indicar que seu estado de acesso conflita com a regra primária. Essa regra também é seguida por um ponto preto para indicar que foi substituída e, portanto, está inativa.

Pelo menos duas regras serão sublinhadas: a regra primária e a(s) regra(s) auxiliar(es). Regras que apenas se complementam envolverão apenas regras de expressão regular. Quando as regras se complementam, elas são indicadas com uma sobreposição amarela. Antes de clicar em qualquer uma das regras, em um exemplo simples, a caixa de diálogo aparece da seguinte forma:



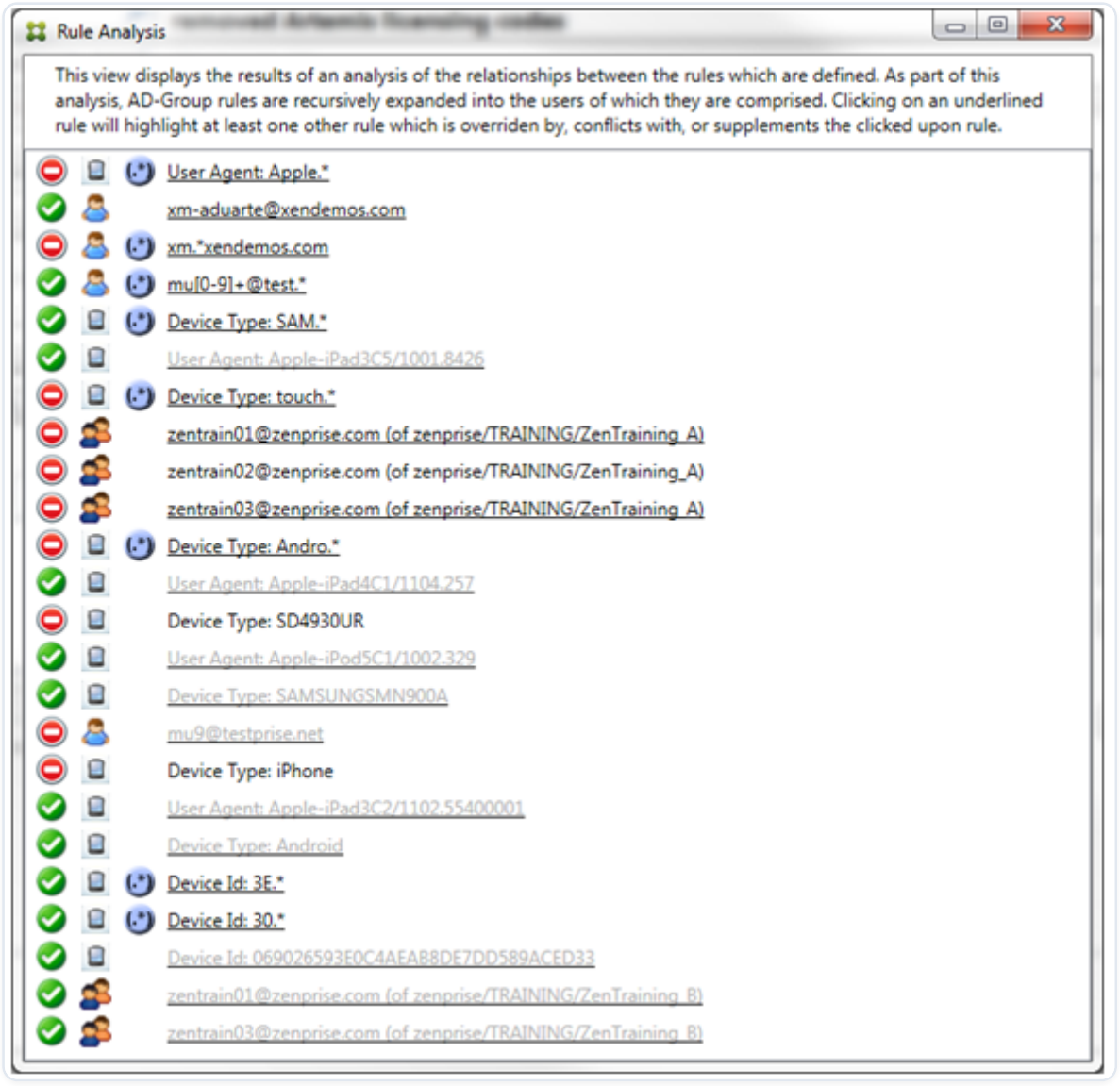
A inspeção visual revela facilmente que ambas as regras são regras de expressão regular que foram aplicadas ao campo ID do dispositivo ActiveSync no conector do Endpoint Management para Exchange ActiveSync. Após clicar na primeira regra, a caixa de diálogo se parece com o seguinte:



A regra primária (regra de expressão regular `WorkMail.*`) é destacada com uma sobreposição amarela para indicar que existe pelo menos mais uma regra auxiliar que é uma expressão regular. A regra auxiliar (regra de expressão regular `SAMSUNG.*`) é destacada com uma sobreposição amarela para indicar que tanto ela quanto a regra primária são regras de expressão regular sendo aplicadas ao mesmo campo dentro do conector do Endpoint Management para Exchange ActiveSync. Neste caso, esse campo é o ID do dispositivo ActiveSync. As expressões regulares podem ou não se sobrepor. Cabe a você decidir se suas expressões regulares estão corretamente elaboradas.

Exemplo de uma expressão complexa

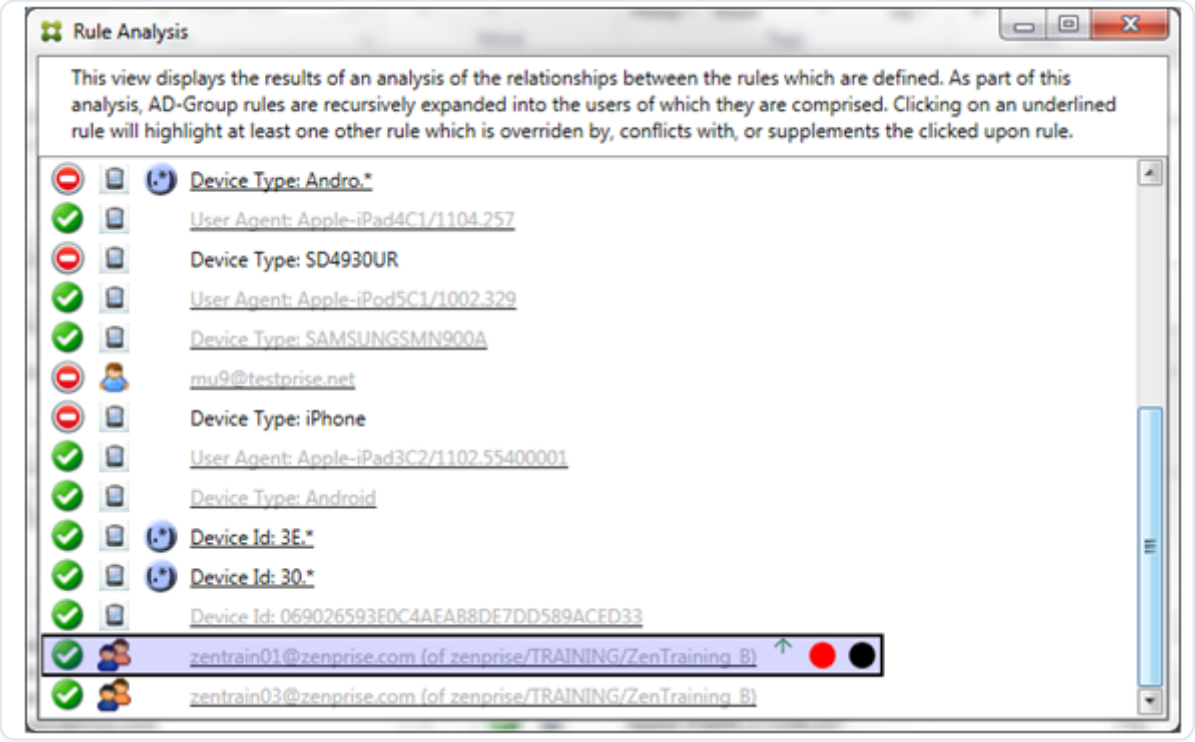
Muitas substituições, conflitos ou complementos potenciais podem ocorrer, tornando impossível dar um exemplo de todos os cenários possíveis. O exemplo a seguir discute o que não fazer, ao mesmo tempo em que serve para ilustrar todo o poder da construção visual de análise de regras. A maioria dos itens está sublinhada na figura a seguir. Muitos dos itens são renderizados em uma fonte mais clara, o que indica que a regra em questão foi substituída por uma regra de prioridade mais alta de alguma forma. Várias regras de expressão regular também estão incluídas na lista, conforme indicado pelo ícone (.*).



Como analisar uma substituição

Para ver qual regra ou regras substituíram uma regra específica, clique na regra.

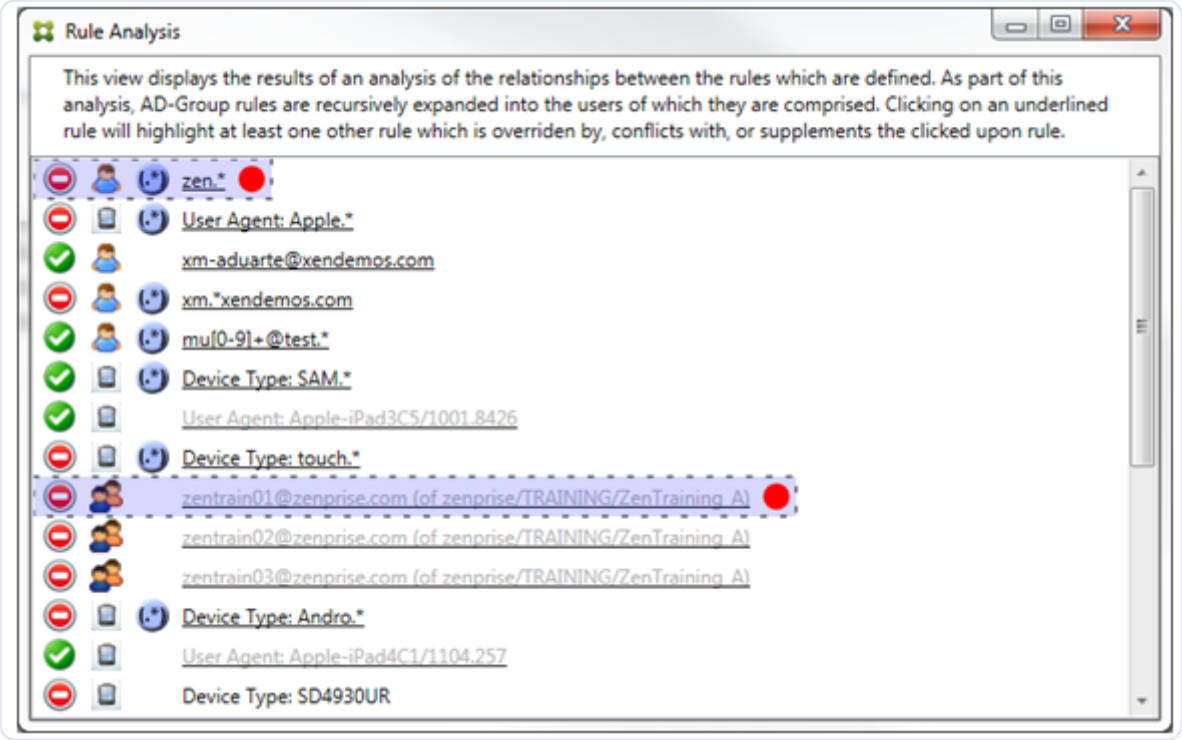
Exemplo 1: Este exemplo examina por que `zentrain01@zenprise.com` foi substituído.



A regra primária (regra de Grupo AD `zenprise/TRAINING/ZenTraining B`, da qual `zentrain01@zenprise.com` é membro) tem as seguintes características:

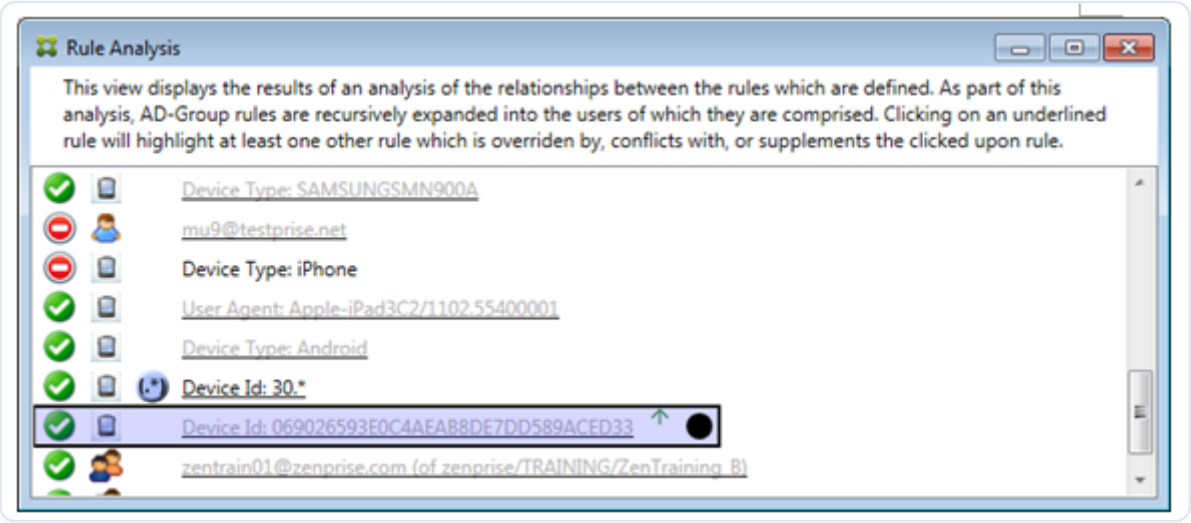
- É destacada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra ou regras auxiliares devem ser encontradas acima dela).
- É seguida por um círculo vermelho e um círculo preto para indicar, respectivamente, que uma ou mais regras auxiliares entram em conflito com seu acesso e que a regra primária foi substituída e, portanto, está inativa.

Ao rolar para cima, você verá o seguinte:



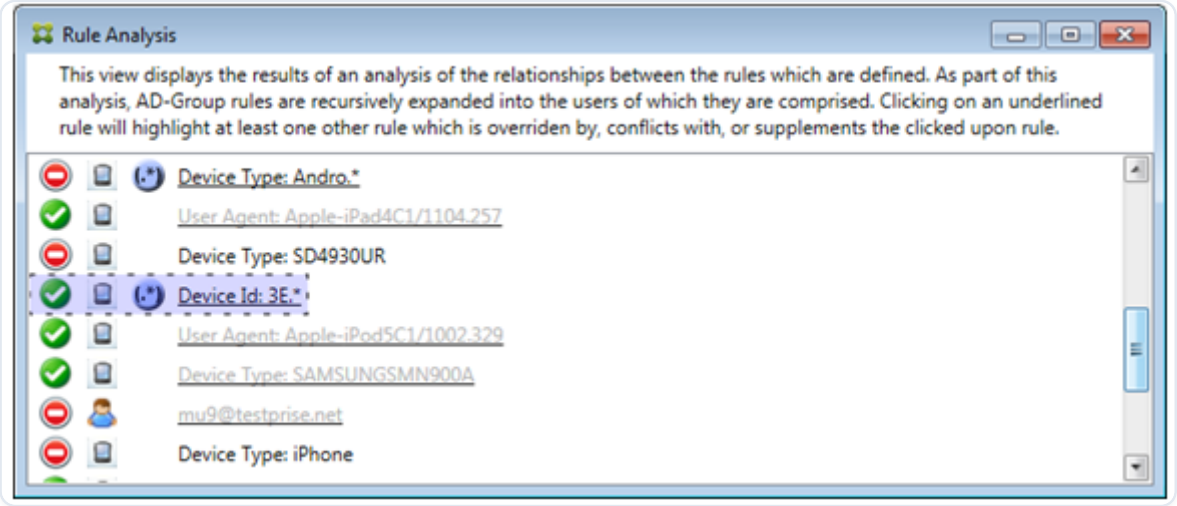
Neste caso, existem duas regras auxiliares que substituem a regra primária: a regra de expressão regular `zen.*` e a regra normal `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). No caso da última regra auxiliar, o que ocorreu é que a regra de Grupo do Active Directory `ZenTraining A` contém o usuário `zentrain01@zenprise.com`, e a regra de Grupo do Active Directory `ZenTraining B` também contém o usuário `zentrain01@zenprise.com`. No entanto, como a regra auxiliar tem uma precedência maior do que a regra primária, a regra primária foi substituída. O acesso da regra primária é Permitir, e como o acesso de ambas as regras auxiliares é Bloquear, todas são seguidas por um círculo vermelho para indicar ainda mais um conflito de acesso.

Exemplo 2: Este exemplo mostra por que o dispositivo com um ID de dispositivo ActiveSync de `069026593E0C4AEAB8DE7DD589ACED33` foi substituído:



A regra primária (regra de ID de dispositivo normal `069026593E0C4AEAB8DE7DD589ACED33`) tem as seguintes características:

- É destacada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra auxiliar deve ser encontrada acima dela).
- É seguido por um círculo preto para indicar que uma regra auxiliar substituiu a regra primária e, portanto, está inativa.



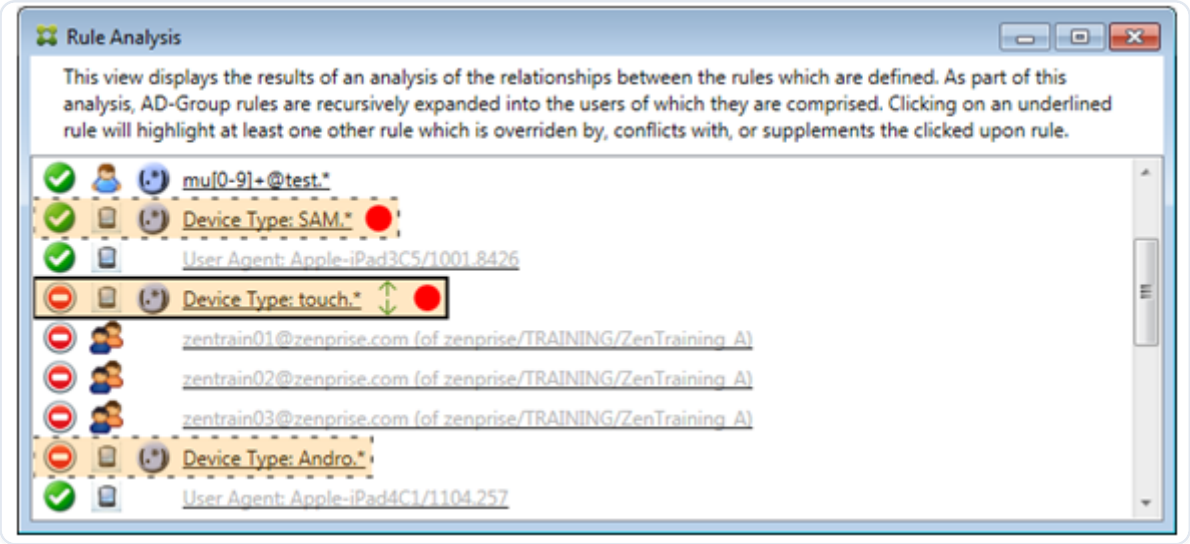
Neste caso, uma única regra auxiliar substitui a regra primária: A regra de ID de dispositivo ActiveSync de expressão regular é `3E.*` Como a expressão regular `3E.*` corresponderia a `069026593E0C4AEAB8DE7DD589ACED33`, a regra primária nunca será avaliada.

Como analisar um suplemento e conflito

Neste caso, a regra primária é a regra de tipo de dispositivo ActiveSync de expressão regular `touch.*` As características são as seguintes:

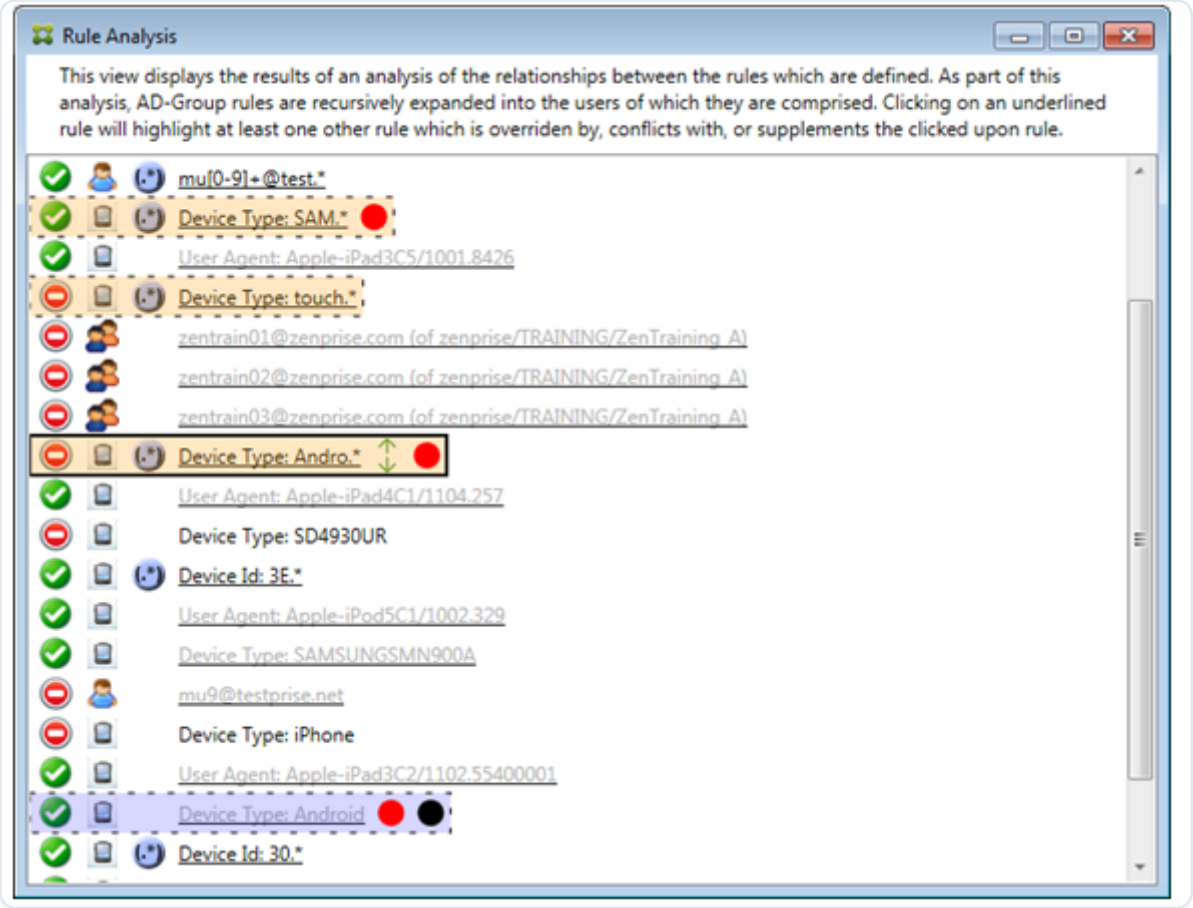
- É indicado por uma borda sólida com uma sobreposição amarela como um aviso de que há mais de uma regra de expressão regular operando contra um campo de regra específico, neste caso, o tipo de dispositivo ActiveSync.
- Duas setas apontam para cima e para baixo, respectivamente, indicando que há pelo menos uma regra auxiliar com prioridade mais alta e pelo menos uma regra auxiliar com prioridade mais baixa.
- O círculo vermelho ao lado indica que pelo menos uma regra auxiliar tem seu acesso definido como Permitir, o que entra em conflito com o acesso da regra primária de Bloquear.
- Existem duas regras auxiliares: a regra de tipo de dispositivo ActiveSync de expressão regular `SAM.*` e a regra de tipo de dispositivo ActiveSync de expressão regular `Andro.*`.

- Ambas as regras auxiliares são delimitadas por traços para indicar que são auxiliares.
- Ambas as regras auxiliares são sobrepostas com amarelo para indicar que também são aplicadas ao campo de regra do tipo de dispositivo ActiveSync.
- Você deve garantir, em tais cenários, que suas regras de expressão regular não sejam redundantes.



Como analisar as regras mais a fundo

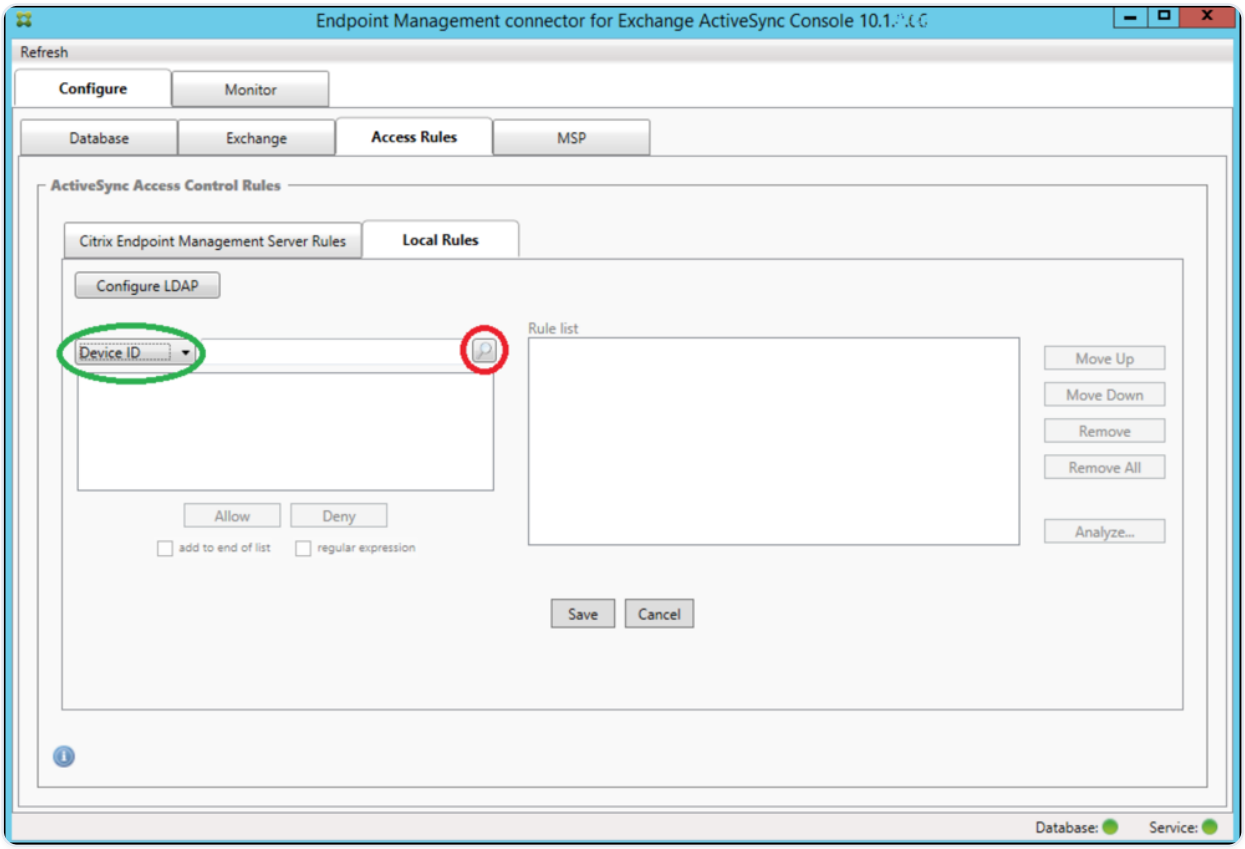
Este exemplo explora como os relacionamentos de regras são sempre da perspectiva da regra primária. O exemplo anterior mostrou como um clique na regra de expressão regular aplicada ao campo de regra do tipo de dispositivo com um valor de `touch.*`. Clicar na regra auxiliar `Andro.*` mostra que um conjunto diferente de regras auxiliares é destacado.



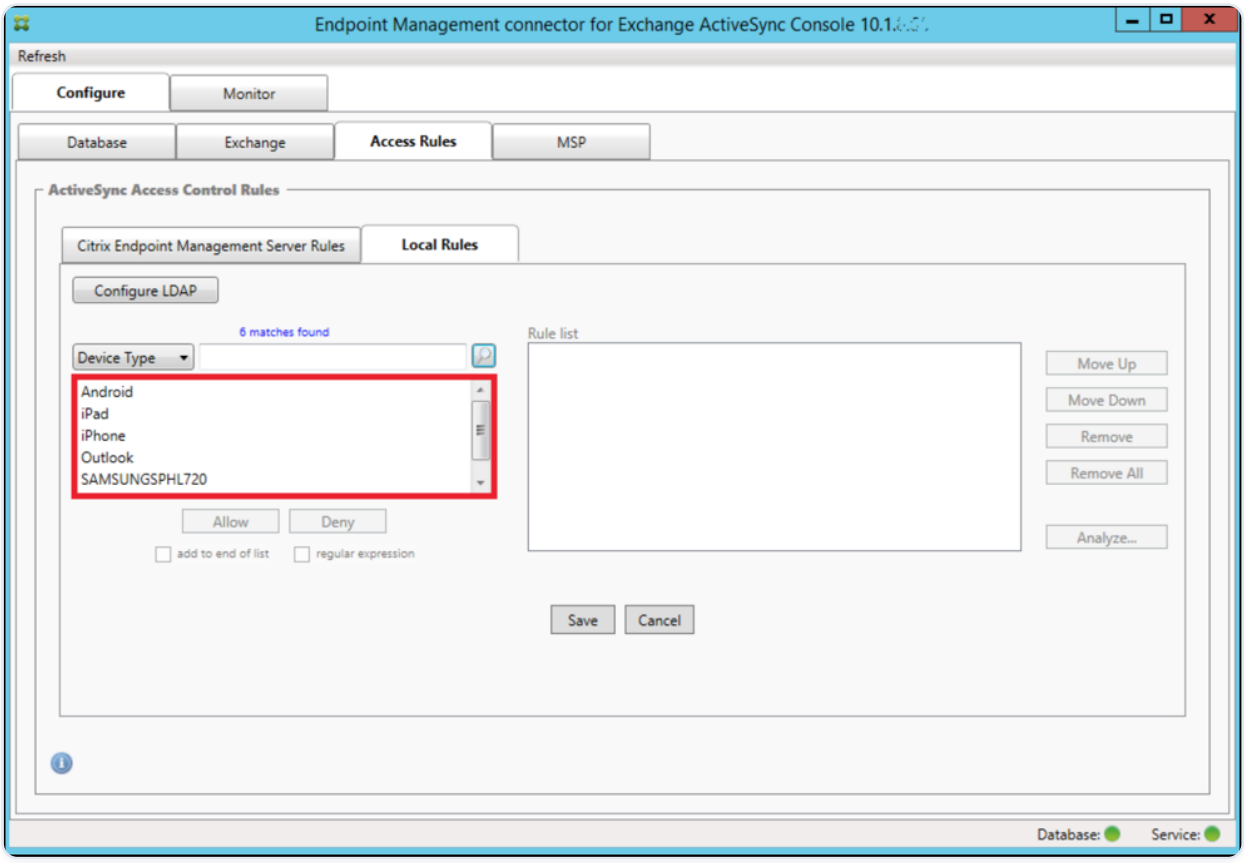
O exemplo mostra uma regra substituída que está incluída no relacionamento da regra. Esta regra é a regra normal de tipo de dispositivo ActiveSync `Android`, que é substituída (indicado pela fonte mais clara e pelo círculo preto ao lado dela) e também entra em conflito em seu acesso com a regra primária de expressão regular de tipo de dispositivo ActiveSync `Andro.*`. Essa regra era anteriormente uma regra auxiliar antes de ser clicada. No exemplo anterior, a regra normal de tipo de dispositivo ActiveSync `Android` não foi exibida como uma regra auxiliar porque, da perspectiva da então regra primária (a regra de expressão regular de tipo de dispositivo ActiveSync `touch.*`), ela não estava relacionada a ela.

Para configurar uma regra local de expressão normal

1. Clique na guia **Regras de Acesso**.



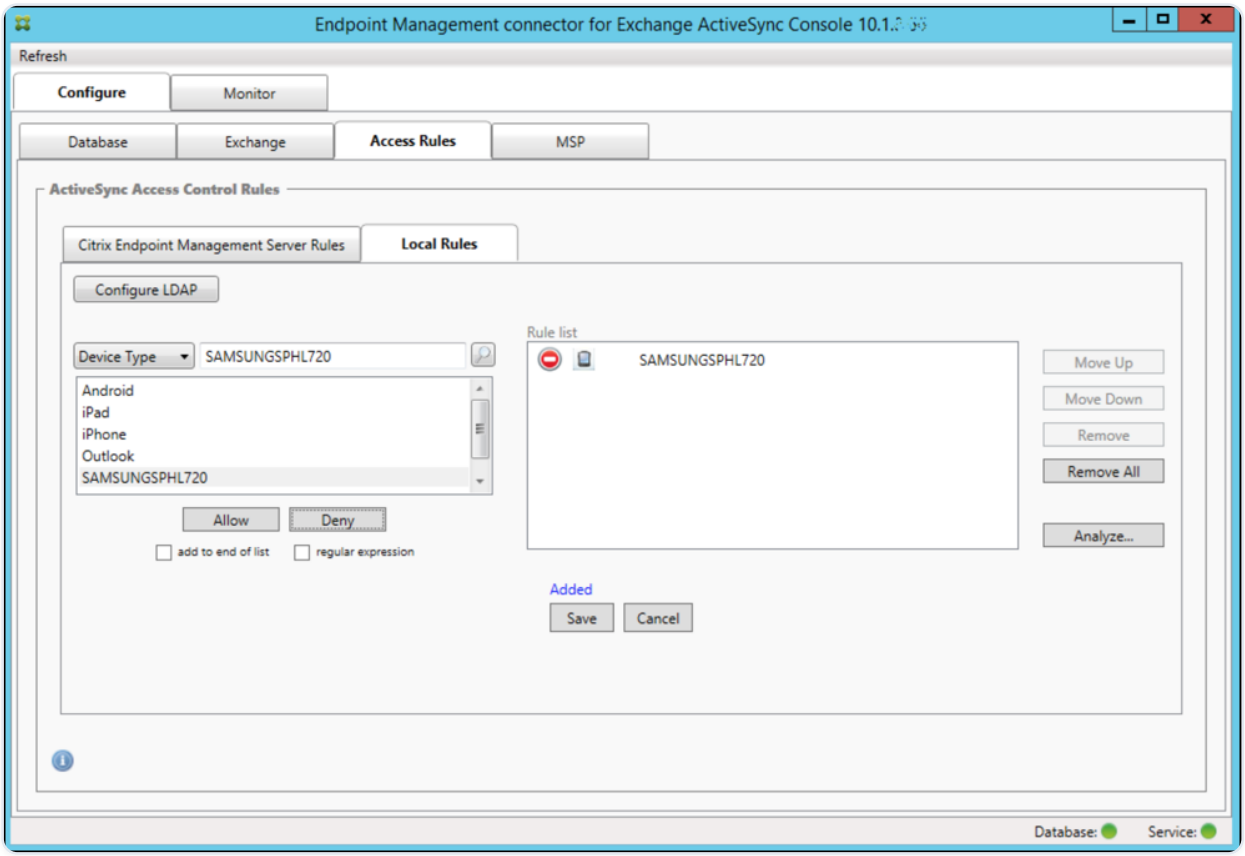
2. Na lista **ID do Dispositivo**, selecione o campo para o qual você deseja criar uma Regra Local.
3. Clique no ícone da lupa para exibir todas as correspondências exclusivas para o campo escolhido. Neste exemplo, o campo **Tipo de Dispositivo** foi escolhido e as opções são mostradas abaixo na caixa de listagem.



4. Clique em um dos itens na caixa de listagem de resultados e, em seguida, clique em uma das seguintes opções:

   - **Permitir** significa que o Exchange será configurado para permitir o tráfego do ActiveSync para todos os dispositivos correspondentes.
   - **Negar** significa que o Exchange será configurado para negar o tráfego do ActiveSync para todos os dispositivos correspondentes.

   Neste exemplo, todos os dispositivos que têm um tipo de dispositivo SamsungSPhl720 têm o acesso negado.



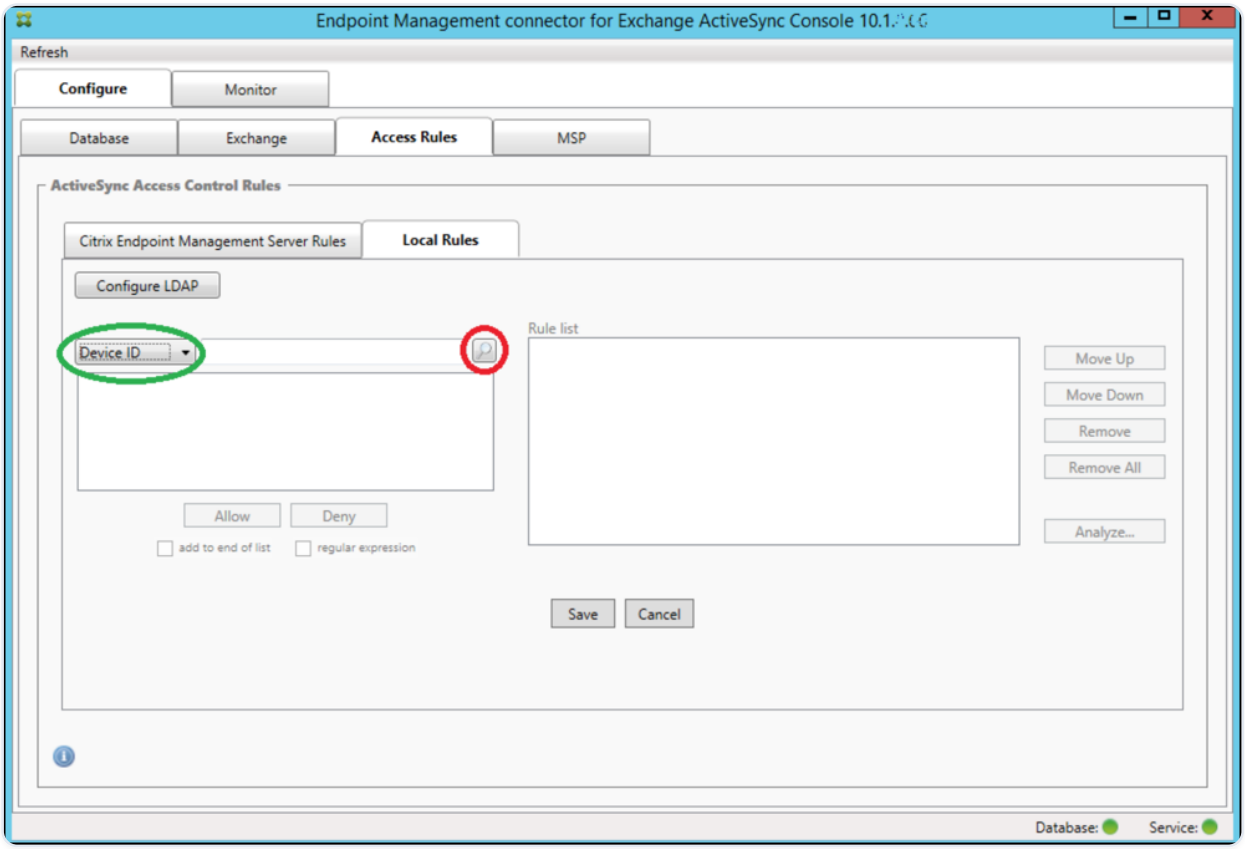
Para adicionar uma expressão regular

As regras locais de expressão regular podem ser distinguidas pelo ícone que aparece ao lado delas -  .

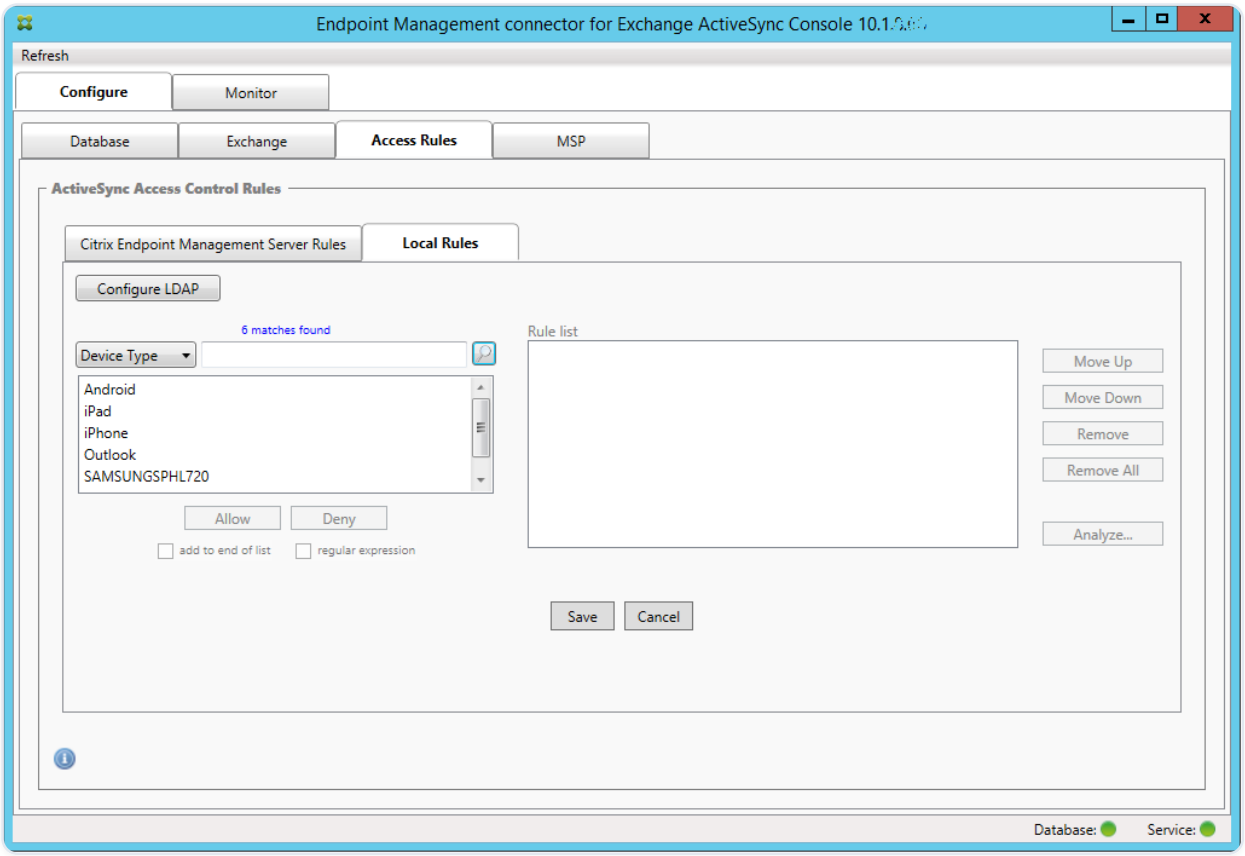
Para adicionar uma regra de expressão regular, você pode construir uma regra de expressão regular a partir de um valor existente na lista de resultados para um determinado campo (desde que um snapshot principal tenha sido concluído), ou você pode simplesmente digitar a expressão regular que deseja.

Para construir uma expressão regular a partir de um valor de campo existente

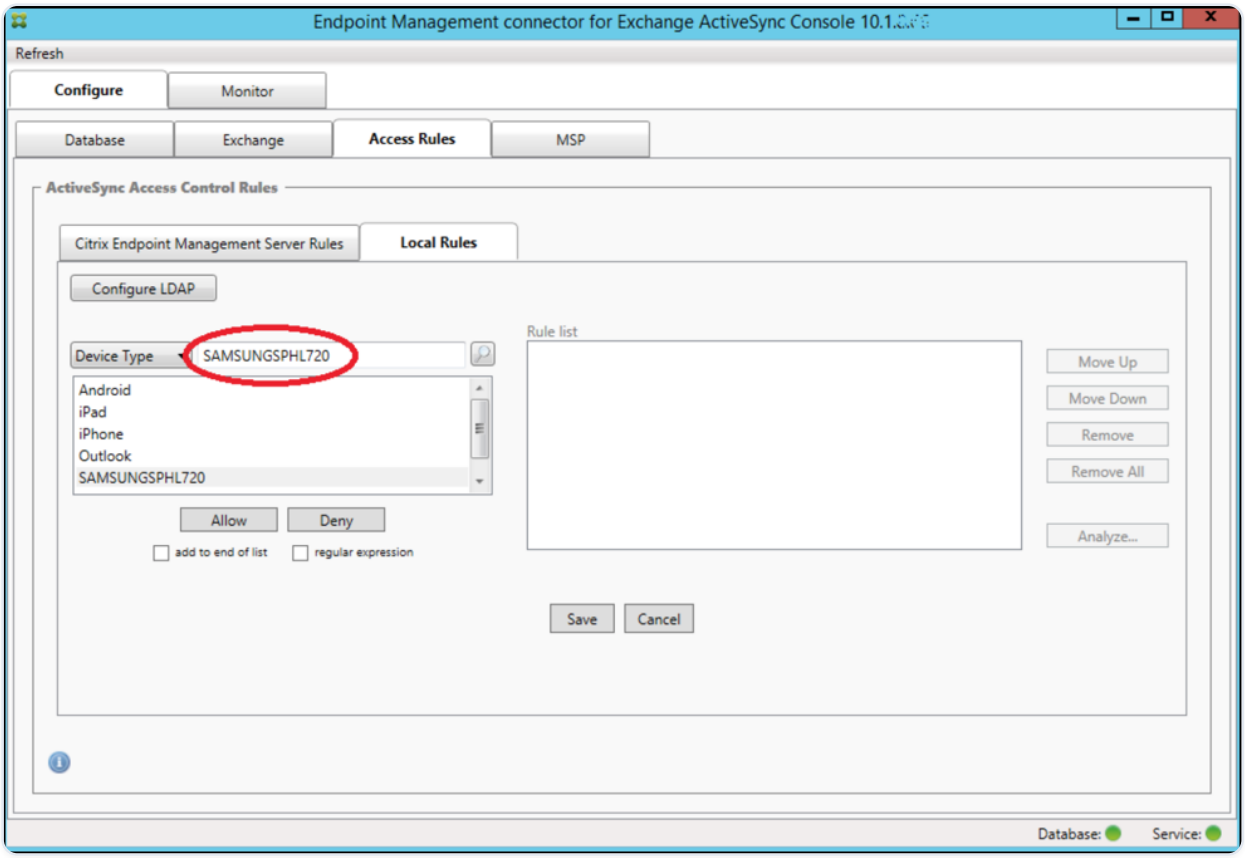
1. Clique na guia **Regras de Acesso**.



2. Na lista **ID do Dispositivo**, selecione o campo para o qual você deseja criar uma Regra Local de expressão regular.
3. Clique no ícone da lupa para exibir todas as correspondências exclusivas para o campo escolhido. Neste exemplo, o campo **Tipo de Dispositivo** foi escolhido e as opções são mostradas abaixo na caixa de listagem.



4. Clique em um dos itens na lista de resultados. Neste exemplo, **SAMSUNGSPHL720** foi selecionado e aparece na caixa de texto ao lado de **Tipo de Dispositivo**.



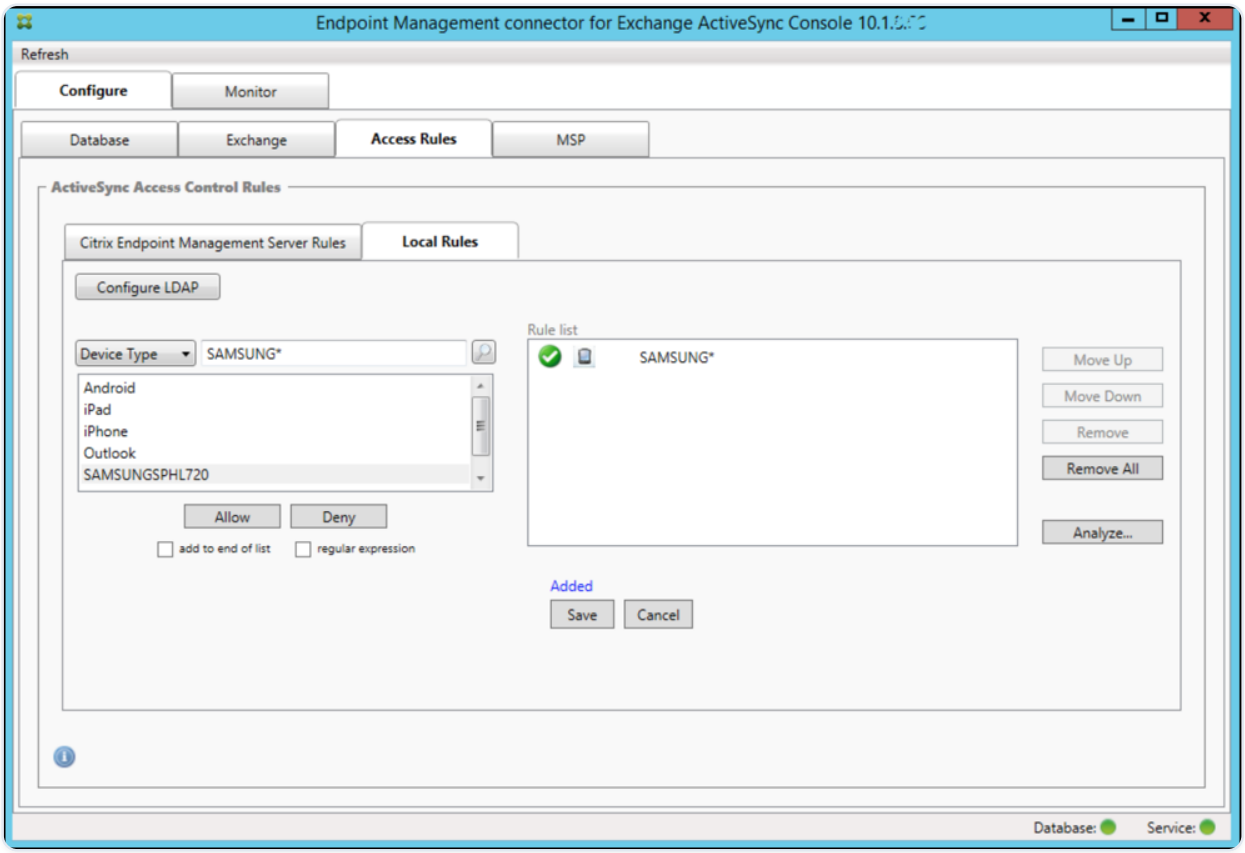
5. Para permitir todos os tipos de dispositivo que contêm "Samsung" em seu valor de tipo de dispositivo, adicione uma regra de expressão regular seguindo estas etapas:

   a. Clique dentro da caixa de texto do item selecionado.

   b. Altere o texto de **SAMSUNGSPHL720** para **SAMSUNG.***.

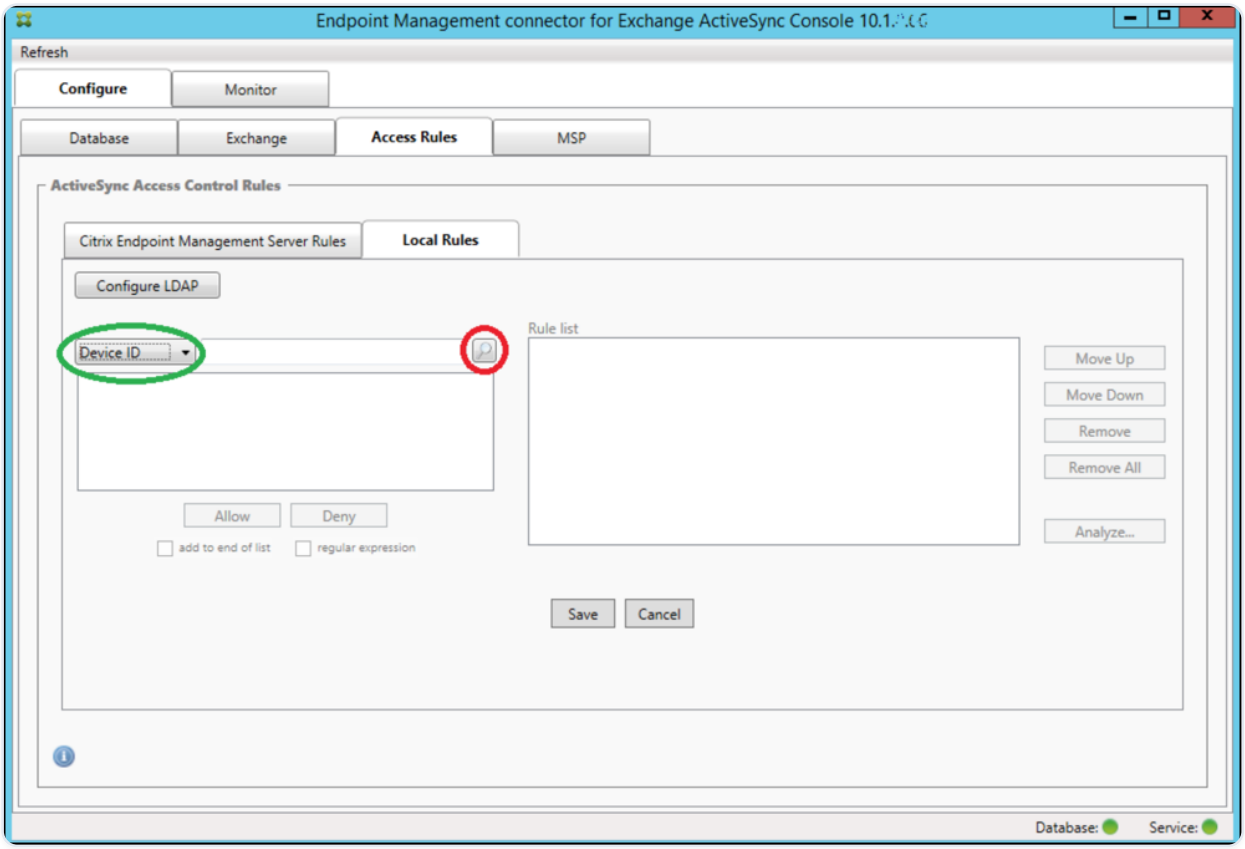
   c. Certifique-se de que a caixa de seleção da expressão regular esteja marcada.

   d. Clique em **Permitir**.

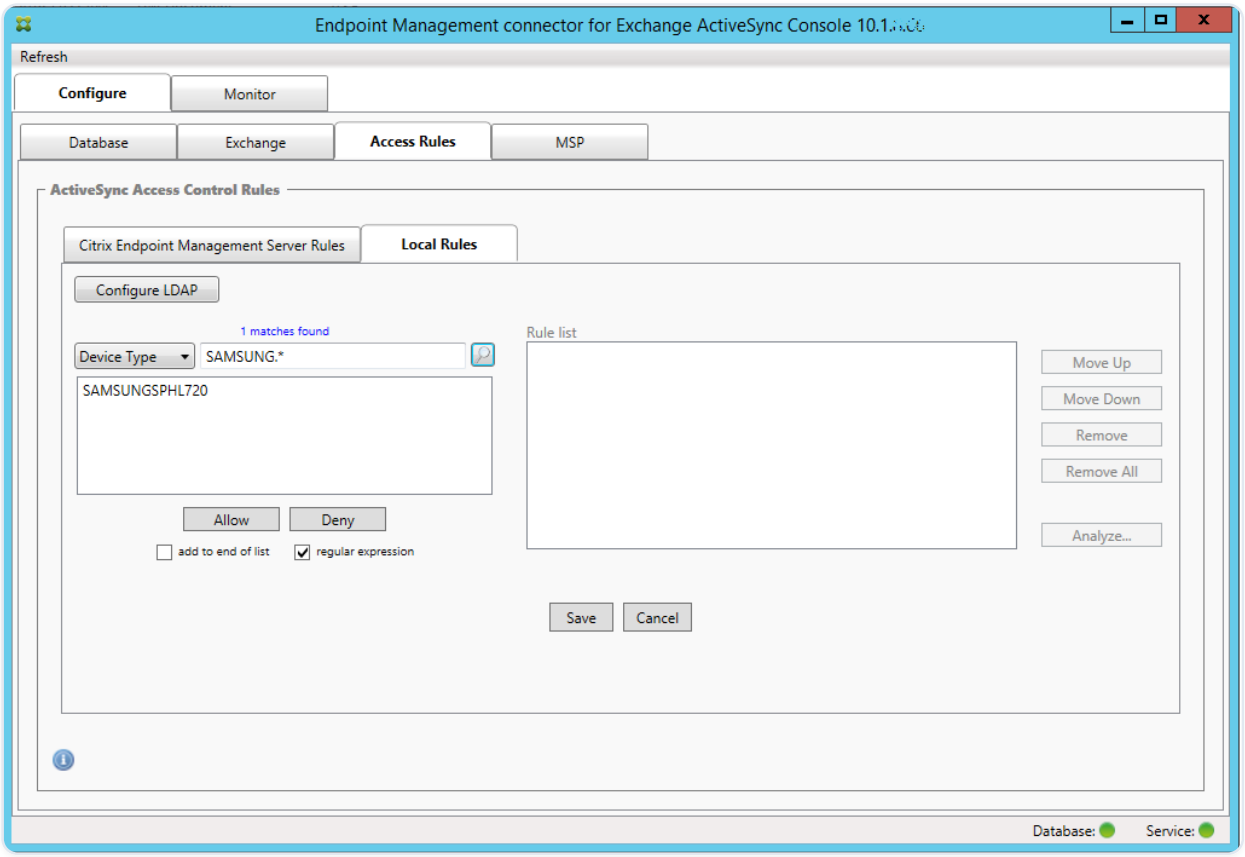


Para criar uma regra de acesso

1. Clique na guia **Regras Locais**.
2. Para inserir a expressão regular, você deve usar tanto a lista de ID do Dispositivo quanto a caixa de texto do item selecionado.



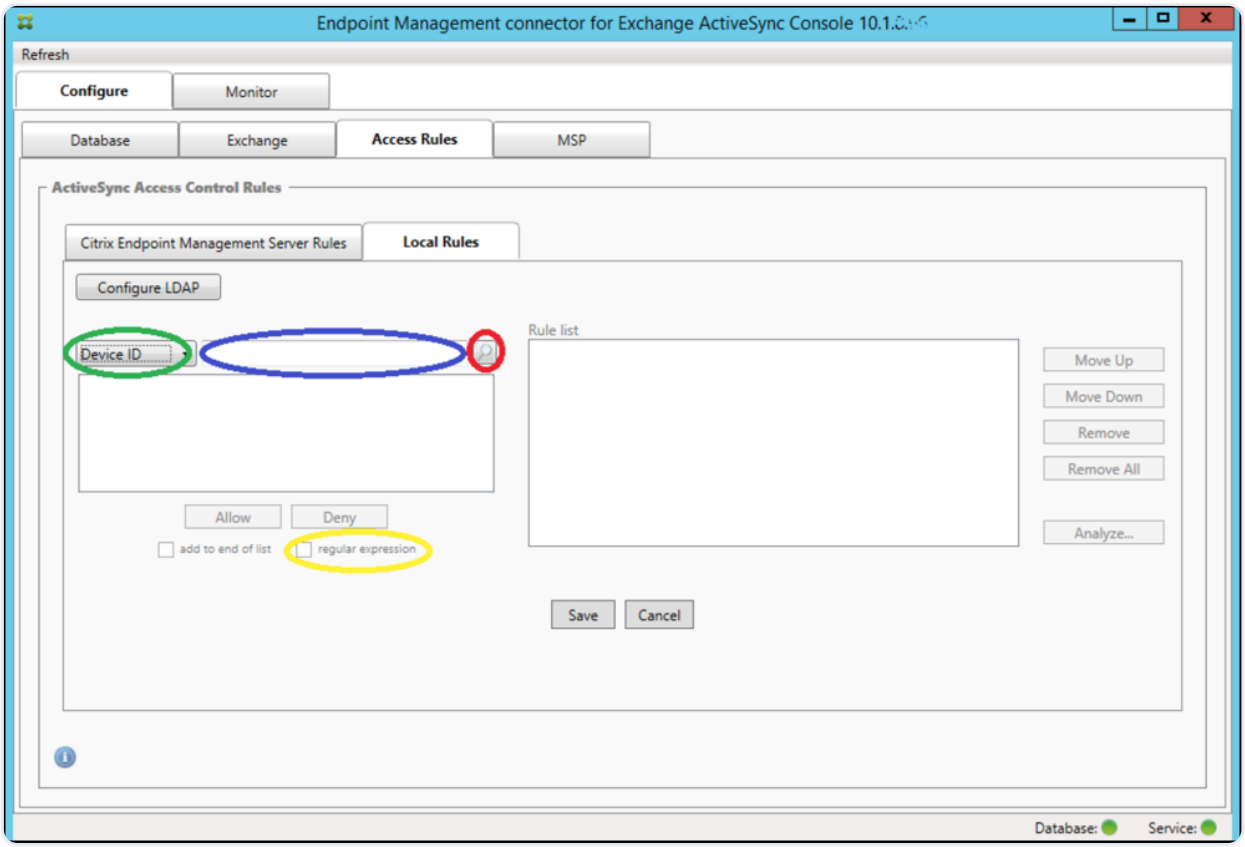
3. Selecione o campo com o qual você deseja fazer a correspondência. Este exemplo usa Tipo de Dispositivo.
4. Digite a expressão regular. Este exemplo usa `samsung.*`.
5. Certifique-se de que a caixa de seleção da expressão regular esteja marcada e, em seguida, clique em **Permitir** ou **Negar**. Neste exemplo, a escolha é **Permitir**. O resultado final é o seguinte:



Para encontrar dispositivos

Ao selecionar a caixa de seleção da expressão regular, você pode executar pesquisas por dispositivos específicos que correspondam à expressão fornecida. Este recurso está disponível apenas se um snapshot principal tiver sido concluído com sucesso. Você pode usar este recurso mesmo que não haja planos de usar regras de expressão regular. Por exemplo, suponha que você queira encontrar todos os dispositivos que contenham o texto "workmail" em seu ID de dispositivo ActiveSync. Para fazer isso, siga este procedimento.

1. Clique na guia **Regras de Acesso**.
2. Certifique-se de que o seletor de campo de correspondência de dispositivo esteja definido como ID do Dispositivo (o padrão).



3. Clique dentro da caixa de texto do item selecionado (conforme mostrado em azul na figura anterior) e, em seguida, digite `workmail.*`.
4. Certifique-se de que a caixa de seleção da expressão regular esteja marcada e, em seguida, clique no ícone da lupa para exibir as correspondências, conforme mostrado na figura a seguir.

   Imagem da página do console do conector do Endpoint Management para Exchange ActiveSync(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-localrules-regex.png)

Para adicionar um usuário, dispositivo ou tipo de dispositivo individual a uma regra estática

Você pode adicionar regras estáticas com base no usuário, ID do dispositivo ou tipo de dispositivo na guia **Dispositivos ActiveSync**.

1. Clique na guia **Dispositivos ActiveSync**.
2. Na lista, clique com o botão direito do mouse em um usuário, dispositivo ou tipo de dispositivo e selecione se deseja permitir ou negar sua seleção.

   A imagem a seguir mostra a opção Permitir/Negar quando user1 é selecionado.

Imagem da página do console do conector do Endpoint Management para Exchange ActiveSync(/en-us/xenmobile/server/media/connector-exchangeactivesync-devices-allowdeny.png)

Monitoramento de dispositivos

A guia **Monitor** no conector do Endpoint Management para Exchange ActiveSync permite navegar pelos dispositivos Exchange ActiveSync e BlackBerry que foram detectados e pelo histórico de comandos automatizados do PowerShell que foram emitidos. A guia **Monitor** possui as três guias a seguir:

- **Dispositivos ActiveSync**:
  - Você pode exportar as parcerias de dispositivos ActiveSync exibidas clicando no botão **Exportar**.
  - Você pode adicionar regras Locais (estáticas) clicando com o botão direito do mouse nas colunas **Usuário**, **ID do Dispositivo** ou **Tipo** e selecionando o tipo de regra de permissão ou bloqueio apropriado.
  - Para recolher uma linha expandida, Ctrl-clique na linha expandida.
- **Dispositivos Blackberry**
- **Histórico de Automação**

A guia **Configurar** mostra o histórico de todos os instantâneos. O histórico de instantâneos mostra quando o instantâneo foi feito, quanto tempo levou, quantos dispositivos foram detectados e quaisquer erros que ocorreram:

- Na guia **Exchange**, clique no ícone Informações para o Exchange Server desejado.
- Na guia **MSP**, clique no ícone Informações para o BlackBerry Server desejado.

Solução de problemas e diagnósticos

O conector do Endpoint Management para Exchange ActiveSync registra erros e outras informações operacionais em seu arquivo de log: *Install Folder*\log\XmmWindowsService.log. O conector do Endpoint Management para Exchange ActiveSync também registra eventos significativos no Log de Eventos do Windows.

Para alterar o nível de log

O conector do Endpoint Management para Exchange ActiveSync inclui os seguintes níveis de log: Error, Info, Warn, Debug e Trace.

> **Nota:**
>
> Cada nível sucessivo gera mais detalhes (mais dados). Por exemplo, o nível Error fornece o mínimo de detalhes, enquanto o nível Trace fornece o máximo de detalhes.

Para alterar o nível de log, faça o seguinte:

1. Em C:\Program Files\Citrix\Citrix Endpoint Management connector, abra o arquivo nlog.config.
2. Na seção `<rules>`, altere o parâmetro *minilevel* para o nível de log de sua preferência. Por exemplo:

```
    <rules>



    <logger name="*" writeTo="file" minlevel="Debug" />



    </rules>
```

3. Salve o arquivo.

   As alterações entram em vigor imediatamente. Você não precisa reiniciar o conector para Exchange ActiveSync.

Erros comuns

A lista a seguir inclui erros comuns:

- O serviço do conector do Endpoint Management para Exchange ActiveSync não inicia

  Verifique o arquivo de log e o Log de Eventos do Windows em busca de erros. As causas típicas são as seguintes:

- O conector do Endpoint Management para o serviço Exchange ActiveSync não consegue acessar o SQL Server. Isso pode ser causado pelos seguintes problemas:
  - O serviço do SQL Server não está em execução.
  - Falha na autenticação.

  Se a autenticação integrada do Windows estiver configurada, a conta de usuário do conector do Endpoint Management para o serviço Exchange ActiveSync deve ser um logon SQL permitido. A conta do conector do Endpoint Management para o serviço Exchange ActiveSync assume como padrão o Sistema Local, mas pode ser alterada para qualquer conta que tenha privilégios de administrador local. Se a autenticação SQL estiver configurada, o logon SQL deve ser configurado corretamente no SQL.
- A porta configurada para o Provedor de Serviços Móveis (MSP) não está disponível. Uma porta de escuta deve ser selecionada que não esteja sendo usada por outro processo no sistema.

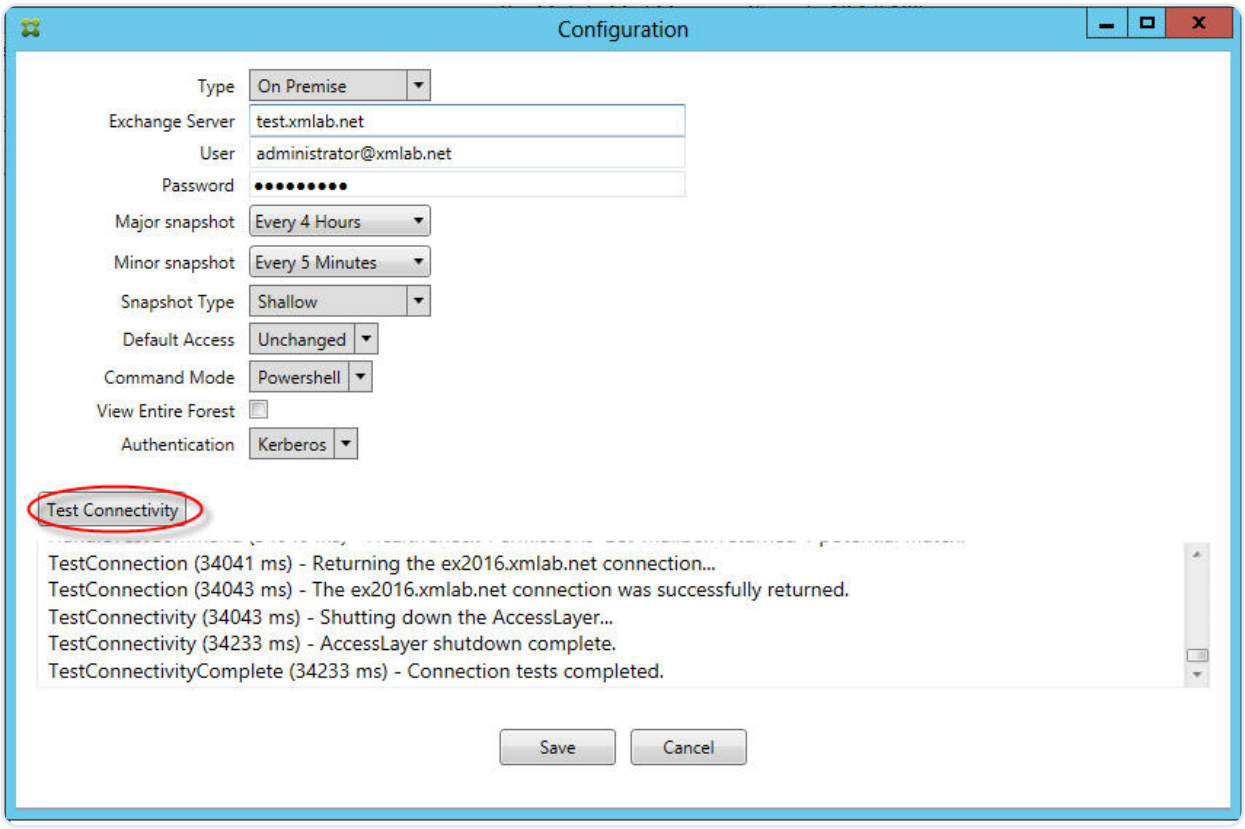
- O XenMobile não consegue se conectar ao MSP

  Verifique se a porta de serviço e o transporte do MSP estão configurados corretamente na guia **Configurar > MSP** do console do conector do Endpoint Management para Exchange ActiveSync. Verifique se o Grupo de Autorização ou Usuário está definido corretamente.

  Se o HTTPS estiver configurado, um certificado de servidor SSL válido deve ser instalado. Se o IIS estiver instalado, o Gerenciador do IIS pode ser usado para instalar o certificado. Se o IIS não estiver instalado, consulte Como configurar uma porta com um certificado SSL para obter detalhes sobre a instalação de certificados.

  O conector do Endpoint Management para Exchange ActiveSync contém um programa utilitário para testar a conectividade com o serviço MSP. Execute o programa *InstallFolder*\MspTestServiceClient.exe e defina o URL e as credenciais para um URL e credenciais que estejam configurados no XenMobile e, em seguida, clique em **Testar Conectividade**. Isso simula as solicitações de serviço web que o XenMobile Server emite. Se o HTTPS estiver configurado, você deve especificar o nome do host real do servidor (o nome especificado no certificado SSL).

  Ao usar **Testar Conectividade**, certifique-se de ter pelo menos um registro ActiveSyncDevice ou o teste pode falhar.



Ferramentas de solução de problemas

Um conjunto de utilitários PowerShell para solução de problemas está disponível na pasta **Support\PowerShell**.

Uma ferramenta de solução de problemas executa uma análise aprofundada de caixas de correio e dispositivos de usuário, detectando condições de erro e áreas potenciais de falha, e uma análise aprofundada de RBAC de usuários. Ela pode salvar a saída bruta de todos os cmdlets em um arquivo de texto.

Conector Citrix Gateway™ para Exchange ActiveSync

O Conector XenMobile Citrix ADC agora é um conector Citrix Gateway para Exchange ActiveSync. Para mais detalhes sobre o portfólio unificado da Citrix, consulte o guia de produtos Citrix.

O conector para Exchange ActiveSync fornece um serviço de autorização em nível de dispositivo para clientes ActiveSync ao Citrix ADC, que atua como um proxy reverso para o protocolo Exchange ActiveSync. A autorização é controlada por uma combinação de políticas que você define no XenMobile® e por regras definidas localmente pelo conector Citrix Gateway para Exchange ActiveSync.

Para mais informações, consulte ActiveSync Gateway.

Para um diagrama de arquitetura de referência detalhado, consulte Arquitetura.

A versão atual do conector Citrix Gateway para Exchange ActiveSync é a 8.5.2.

> **Importante:**
>
> A partir de outubro de 2022, os conectores Endpoint Management e Citrix Gateway para Exchange ActiveSync não oferecem mais suporte ao Exchange Online, dadas as alterações de autenticação anunciadas pela Microsoft aqui. O conector Endpoint Management para Exchange continua a funcionar com o Microsoft Exchange Server (local).

Novidades

As seções a seguir listam as novidades nas versões atual e anteriores do conector Citrix Gateway para Exchange ActiveSync, anteriormente Conector XenMobile Citrix ADC.

Novidades na versão 8.5.3

- Esta versão adiciona suporte para os protocolos ActiveSync 16.0 e 16.1.

- Mais detalhes foram adicionados aos dados analíticos enviados ao Google Analytics, especialmente em relação aos snapshots.

Novidades na versão 8.5.2

- O Conector XenMobile Citrix ADC agora é um conector Citrix Gateway para Exchange ActiveSync.

Os seguintes problemas foram corrigidos nesta versão:

- Se mais de um critério for usado na definição de uma regra de política e se um dos critérios envolver o ID do usuário, o seguinte problema pode ocorrer: Se um usuário tiver mais aliases, os aliases também não serão verificados ao aplicar a regra.

> **Nota:**
>
> A seção Novidades a seguir se refere ao conector do Citrix Gateway para Exchange ActiveSync pelo seu nome anterior de Conector XenMobile Citrix ADC. O nome mudou a partir da versão 8.5.2.

Novidades na versão 8.5.1.11

- **Alteração nos requisitos do sistema:** A versão atual do Conector Citrix ADC requer o Microsoft .NET Framework 4.5.
- **Suporte ao Google Analytics:** Queremos saber como você usa um Conector XenMobile Citrix ADC para que possamos focar em onde podemos melhorar o produto.
- **Suporte para TLS 1.1 e 1.2:** Devido à sua segurança enfraquecida, o TLS 1.0 está sendo descontinuado pelo PCI Council. O suporte para TLS 1.1 e 1.2 foi adicionado ao Conector XenMobile Citrix ADC.

Monitorando o conector do Citrix Gateway para Exchange ActiveSync

O utilitário de configuração do conector do Citrix Gateway para Exchange ActiveSync fornece registro detalhado que você pode usar para visualizar todo o tráfego que passa pelo seu Exchange Server e que é permitido ou bloqueado pelo Secure Mobile Gateway.

Use a guia **Log** para visualizar o histórico das solicitações do ActiveSync encaminhadas ao conector para Exchange ActiveSync pelo Citrix ADC para autorização.

Além disso, para garantir que o conector do Citrix Gateway para o serviço web do Exchange ActiveSync esteja em execução, carregue a seguinte URL em um navegador no servidor do conector `https://<host:port>/services/ActiveSync/Version`. Se a URL retornar a versão do produto como uma string, o serviço web estará responsivo.

Para simular o tráfego do ActiveSync com o conector do Citrix Gateway para Exchange ActiveSync

Você pode usar o conector do Citrix Gateway para Exchange ActiveSync para simular como o tráfego do ActiveSync se comporta com suas políticas. No utilitário de configuração do conector, selecione a guia **Simulador**. Os resultados mostram como suas políticas se aplicam de acordo com as regras que você configurou.

Escolhendo filtros para o conector do Citrix Gateway para Exchange ActiveSync

Os filtros do conector do Citrix Gateway para Exchange ActiveSync funcionam analisando um dispositivo em busca de uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, ele será colocado em uma Lista de Dispositivos. Esta Lista de Dispositivos não é uma lista de permissão nem uma lista de bloqueio. É uma lista de dispositivos que atendem aos critérios definidos. Os seguintes filtros estão disponíveis para o conector no XenMobile. As duas opções para cada filtro são **Permitir** ou **Negar**.

- **Dispositivos Anônimos:** Permite ou nega dispositivos que estão registrados no XenMobile, mas a identidade do usuário é desconhecida. Por exemplo, pode ser um usuário que foi registrado, mas a senha do Active Directory do usuário expirou, ou um usuário que se registrou com credenciais desconhecidas.
- **Atestado Samsung KNOX falhou:** Os dispositivos Samsung possuem funcionalidades de segurança e diagnóstico. Este filtro fornece a confirmação de que o dispositivo está configurado para KNOX. Para obter detalhes, consulte Samsung Knox.
- **Aplicativos Proibidos:** Permite ou nega dispositivos com base na Lista de Dispositivos definida por políticas de lista de bloqueio e na presença de aplicativos bloqueados.
- **Permitir/Negar Implícito:** Cria uma Lista de Dispositivos de todos os dispositivos que não atendem a nenhum dos outros critérios de regra de filtro e permite ou nega com base nessa lista. A opção Permitir/Negar Implícito garante que o status do conector do Citrix Gateway para Exchange ActiveSync na guia Dispositivos esteja ativado e mostre o status do conector para seus dispositivos. A opção Permitir/Negar Implícito também controla todos os outros filtros do

conector que não foram selecionados. Por exemplo, o conector nega aplicativos bloqueados, mas permite todos os outros filtros porque a opção Permitir/Negar Implícito está definida como **Permitir**.

- **Dispositivos inativos:** Cria uma Lista de Dispositivos de dispositivos que não se comunicaram com o XenMobile dentro de um tempo especificado. Esses dispositivos são considerados inativos. O filtro permite ou nega os dispositivos de acordo.
- **Aplicativos obrigatórios ausentes:** Quando um usuário se registra, ele recebe uma lista de aplicativos obrigatórios que devem ser instalados. O filtro de aplicativos obrigatórios ausentes indica que um ou mais dos aplicativos não estão mais presentes; por exemplo, o usuário excluiu um ou mais aplicativos.
- **Aplicativos Não Sugeridos:** Quando um usuário se registra, ele recebe uma lista dos aplicativos que deve instalar. O filtro de aplicativos não sugeridos verifica o dispositivo em busca de aplicativos que não estão nessa lista.
- **Senha não compatível:** Cria uma Lista de Dispositivos de todos os dispositivos que não possuem uma senha no dispositivo.
- **Dispositivos Fora de Conformidade:** Permite negar ou permitir dispositivos que atendem aos seus próprios critérios internos de conformidade de TI. A conformidade é uma configuração arbitrária definida pela propriedade do dispositivo chamada Fora de Conformidade, que é um sinalizador booleano que pode ser **Verdadeiro** ou **Falso**. (Você pode criar esta propriedade manualmente e definir o valor, ou pode usar Ações Automatizadas para criar esta propriedade em um dispositivo se o dispositivo atender ou não a critérios específicos.)
    - **Fora de Conformidade = Verdadeiro**. Se um dispositivo não atender aos padrões de conformidade e definições de política estabelecidos pelo seu departamento de TI, o dispositivo estará fora de conformidade.
    - **Fora de Conformidade = Falso.** Se um dispositivo atender aos padrões de conformidade e definições de política estabelecidos pelo seu departamento de TI, o dispositivo estará em conformidade.
- **Status Revogado:** Cria uma Lista de Dispositivos de todos os dispositivos revogados e permite ou nega com base no status revogado.
- **Dispositivos Android com Root/iOS com Jailbreak**. Cria uma Lista de Dispositivos de todos os dispositivos sinalizados como com root e permite ou nega com base no status de root.

- **Dispositivos Não Gerenciados**. Cria uma Lista de Dispositivos de todos os dispositivos no banco de dados do XenMobile. O Mobile Application Gateway deve ser implantado no Modo de Bloqueio.

Para configurar uma conexão com o conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o XenMobile e outros provedores de configuração remota por meio de serviços web seguros.

1. No utilitário de configuração do conector, clique na guia **Config Providers** e, em seguida, clique em **Add**.
2. Na caixa de diálogo **Config Providers**, em **Name**, insira um nome de usuário que tenha privilégios administrativos e seja usado para autorização HTTP básica com o XenMobile Server.
3. Em **Url**, insira o endereço web do GCS do XenMobile, tipicamente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.
4. Em **Password**, insira a senha que é usada para autorização HTTP básica com o XenMobile Server.
5. Em **Managing Host**, insira o nome do servidor do conector.
6. Em **Baseline Interval**, especifique um período de tempo para quando um novo conjunto de regras dinâmicas atualizado é extraído do Device Manager.
7. Em **Delta interval**, especifique um período de tempo para quando uma atualização de regras dinâmicas é extraída.
8. Em **Request Timeout**, especifique o intervalo de tempo limite da solicitação do servidor.
9. Em **Config Provider**, selecione se a instância do servidor do provedor de configuração está fornecendo a configuração da política.
10. Em **Events Enabled**, habilite esta opção se você quiser que o conector notifique o XenMobile quando um dispositivo for bloqueado. Esta opção é necessária se você estiver usando as regras do conector em qualquer uma das suas Ações Automatizadas do XenMobile.
11. Clique em **Save** e, em seguida, clique em **Test Connectivity** para testar a conectividade do gateway com o provedor de configuração. Se a conexão falhar, verifique se as configurações do firewall local permitem a conexão ou entre em contato com o administrador.

12. Quando a conexão for bem-sucedida, desmarque a caixa de seleção **Disabled** e, em seguida, clique em **Save**.

Ao adicionar um novo provedor de configuração, o conector Citrix Gateway para Exchange ActiveSync cria automaticamente uma ou mais políticas associadas ao provedor. Essas políticas são definidas por uma definição de modelo contida em `config\policyTemplates.xml` na seção NewPolicyTemplate. Para cada elemento Policy definido nesta seção, uma nova política é criada.

O operador pode adicionar, remover ou modificar elementos de política se o seguinte for verdadeiro: O elemento de política está em conformidade com a definição do esquema e as cadeias de caracteres de substituição padrão (entre chaves) não são modificadas. Em seguida, adicione novos grupos para o provedor e atualize a política para incluir os novos grupos.

Para importar uma política do XenMobile

1. No utilitário de configuração do Citrix Gateway connector para Exchange ActiveSync, clique na guia **Config Providers** e, em seguida, clique em **Add**.
2. Na caixa de diálogo **Config Providers**, em **Name**, insira um nome de usuário que é usado para autorização HTTP básica com o XenMobile Server e que tem privilégios administrativos.
3. Em **Url**, insira o endereço da web do XenMobile Gateway Configuration Service (GCS), normalmente no formato `https://<xdmHost>/xdm/services/<MagConfigService>`. O nome MagConfigService diferencia maiúsculas de minúsculas.
4. Em **Password**, insira a senha que é usada para autorização HTTP básica com o XenMobile Server.
5. Clique em **Test Connectivity** para testar a conectividade do gateway com o provedor de configuração. Se a conexão falhar, verifique se as configurações do firewall local permitem a conexão ou consulte seu administrador.
6. Quando uma conexão for estabelecida com sucesso, desmarque a caixa de seleção **Disabled** e, em seguida, clique em **Save**.
7. Em **Managing Host**, deixe o nome DNS padrão do computador host local. Essa configuração era usada para coordenar a comunicação com o XenMobile quando vários servidores Forefront Threat Management Gateway (TMG) são configurados em um array.

   Depois de salvar as configurações, abra o GCS.

Configurando o modo de política do Citrix Gateway connector para Exchange ActiveSync

O Citrix Gateway connector para Exchange ActiveSync pode ser executado nos seis modos a seguir:

- **Allow All**. Este modo de política concede acesso a todo o tráfego que passa pelo conector. Nenhuma outra regra de filtragem é usada.
- **Deny All**. Este modo de política bloqueia o acesso a todo o tráfego que passa pelo conector. Nenhuma outra regra de filtragem é usada.
- **Static Rules: Block Mode**. Este modo de política executa regras estáticas com uma instrução implícita de negação ou bloqueio no final. O conector bloqueia dispositivos que não são permitidos ou autorizados por meio de outras regras de filtro.
- **Regras Estáticas: Modo de Permissão**. Este modo de política executa regras estáticas com uma declaração implícita de permissão ou autorização no final. Dispositivos que não são bloqueados ou negados por outras regras de filtro são permitidos através do conector.
- **Regras Estáticas + ZDM**: Modo de Bloqueio. Este modo de política executa primeiro as regras estáticas, seguidas pelas regras dinâmicas do XenMobile com uma declaração implícita de negação ou bloqueio no final. Os dispositivos são permitidos ou negados com base em filtros definidos e regras do Gerenciador de Dispositivos. Quaisquer dispositivos que não correspondam aos filtros e regras definidos são bloqueados.
- **Regras Estáticas + ZDM**: Modo de Permissão. Este modo de política executa primeiro as regras estáticas, seguidas pelas regras dinâmicas do XenMobile com uma declaração implícita de permissão ou autorização no final. Os dispositivos são permitidos ou negados com base em filtros definidos e regras do XenMobile. Quaisquer dispositivos que não correspondam aos filtros e regras definidos são permitidos.

O conector Citrix Gateway para Exchange ActiveSync permite ou bloqueia regras dinâmicas com base em IDs ActiveSync exclusivos para dispositivos móveis iOS e baseados em Windows recebidos do XenMobile. Dispositivos Android diferem em seu comportamento com base no fabricante e alguns não expõem facilmente um ID ActiveSync exclusivo. Para compensar, o XenMobile envia informações de ID de usuário para dispositivos Android para tomar uma decisão de permissão ou bloqueio. Como resultado, se um usuário tiver apenas um dispositivo Android, as permissões e bloqueios funcionam normalmente. Se o usuário tiver vários dispositivos Android, todos os dispositivos são permitidos porque os dispositivos Android não podem ser diferenciados. Você pode configurar o gateway para bloquear estaticamente esses dispositivos por ActiveSyncID,

se forem conhecidos. Você também pode configurar o gateway para bloquear com base no tipo de dispositivo ou agente de usuário.

Para especificar o modo de política, no utilitário de Configuração do Controlador SMG, faça o seguinte:

1. Clique na guia **Filtros de Caminho** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Propriedades do Caminho**, selecione um modo de política na lista **Política** e, em seguida, clique em **Salvar**.

Você pode revisar as regras na guia **Políticas** do utilitário de configuração. As regras são processadas no conector Citrix Gateway para Exchange ActiveSync de cima para baixo. As políticas de Permissão são exibidas com uma marca de seleção verde. As políticas de Negação são mostradas como um círculo vermelho com uma linha no meio. Para atualizar a tela e ver as regras mais recentes, clique em **Atualizar**. Você também pode modificar a ordem das regras no arquivo config.xml.

Para testar as regras, clique na guia **Simulador**. Especifique valores nos campos. Estes também podem ser obtidos dos logs. Uma mensagem de resultado aparece especificando Permitir ou Bloquear.

Para configurar regras estáticas

Insira regras estáticas com valores que a filtragem ISAPI das solicitações HTTP de conexão ActiveSync lê. As regras estáticas permitem que o conector Citrix Gateway para Exchange ActiveSync permita ou bloqueie o tráfego pelos seguintes critérios:

- **Usuário:** O conector Citrix Gateway para Exchange ActiveSync usa o valor de usuário autorizado e a estrutura de nome que foram capturados durante o registro do dispositivo. Isso é comumente encontrado como domínio\nome de usuário, conforme referenciado pelo servidor que executa o XenMobile conectado ao Active Directory via LDAP. A guia **Log** dentro do utilitário de configuração do conector mostra os valores que são passados através do conector. Os valores são passados se a estrutura do valor precisar ser determinada ou for diferente.
- **ID do Dispositivo (ActiveSyncID):** Também conhecido como o ActiveSyncID do dispositivo conectado. Este valor é comumente encontrado na página de propriedades específicas do dispositivo no console do XenMobile. Este valor também pode ser verificado na guia Log no utilitário de configuração do conector.
- **Tipo de Dispositivo:** O conector pode determinar se um dispositivo é um iPhone, iPad ou outro tipo de dispositivo e pode permitir ou bloquear com base nesse critério. Assim como

outros valores, o utilitário de configuração do conector pode revelar todos os tipos de dispositivos conectados que estão sendo processados para a conexão ActiveSync.

- **Agente de Usuário:** Contém informações sobre o cliente ActiveSync que é usado. Geralmente, o valor especificado corresponde a uma compilação e versão específicas do sistema operacional para a plataforma de dispositivo móvel.

O utilitário de configuração do conector em execução no servidor sempre gerencia as regras estáticas.

1. No utilitário de configuração do controlador SMG, clique na guia **Static Rules** e depois em **Add**.
2. Na caixa de diálogo **Static Rule Properties**, especifique os valores que você deseja usar como critérios. Por exemplo, você pode inserir um usuário para permitir o acesso digitando o nome de usuário (por exemplo, AllowedUser) e, em seguida, desmarcando a caixa de seleção **Disabled**.
3. Clique em **Save**.

   A regra estática está agora em vigor. Além disso, você pode usar expressões regulares para definir valores, mas deve habilitar o modo de processamento de regras no arquivo config.xml.

Para configurar regras dinâmicas

As políticas e propriedades do dispositivo no XenMobile definem regras dinâmicas e podem acionar um filtro dinâmico do Citrix Gateway connector para o Exchange ActiveSync. Os gatilhos são baseados na presença de uma violação de política ou configuração de propriedade. Os filtros do conector funcionam analisando um dispositivo em busca de uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, ele será colocado em uma Lista de Dispositivos. Esta Lista de Dispositivos não é uma lista de permissões ou uma lista de bloqueios. É uma lista de dispositivos que atendem aos critérios definidos. As seguintes opções de configuração permitem definir se você deseja permitir ou negar os dispositivos na Lista de Dispositivos usando o conector.

> **Nota:**
>
> Você deve usar o console do XenMobile para configurar regras dinâmicas.

1. No console do XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.

2. Em **Server**, clique em **ActiveSync Gateway**. A página ActiveSync Gateway é exibida.
3. Em **Activate the following rules**, selecione uma ou mais regras que você deseja ativar.
4. Somente no Android, em **Send Android domain users to ActiveSync Gateway**, clique em **YES** para garantir que o XenMobile envie informações do dispositivo Android para o Secure Mobile Gateway.

   Quando esta opção está habilitada, o XenMobile envia informações do dispositivo Android para o Citrix Gateway connector para Exchange ActiveSync quando o XenMobile não possui o identificador ActiveSync para o usuário do dispositivo Android.

Para configurar políticas personalizadas editando o arquivo XML do Citrix Gateway connector para Exchange ActiveSync

Você pode visualizar as políticas básicas na configuração padrão na guia **Políticas** do utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync. Se você quiser criar políticas personalizadas, pode editar o arquivo de configuração XML do conector (config\config.xml).

1. Encontre a seção **PolicyList** no arquivo e adicione um novo elemento **Policy**.
2. Se um novo grupo também for necessário, como outro grupo estático ou um grupo para suportar outro GCP, adicione o novo elemento **Group** à seção **GroupList**.
3. Opcionalmente, você pode alterar a ordem dos grupos dentro de uma política existente reorganizando os elementos **GroupRef**.

Configurando o arquivo XML do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync usa um arquivo de configuração XML para ditar as ações do conector. Entre outras entradas, o arquivo especifica os arquivos de grupo e as ações associadas que o filtro executa ao avaliar as solicitações HTTP. Por padrão, o arquivo é nomeado config.xml e pode ser encontrado no seguinte local: ..\Program Files\Citrix\XenMobile Citrix ADC Connector\config\.

Nós GroupRef

Os nós GroupRef definem os nomes de grupo lógicos. Os padrões são AllowGroup e DenyGroup.

> **Nota:**
>
> A ordem dos nós GroupRef, conforme aparecem no nó GroupRefList, é significativa.

> O valor de ID de um nó GroupRef identifica um contêiner lógico ou uma coleção de membros que são usados para corresponder a contas de usuário ou dispositivos específicos. Os atributos de ação especificam como o filtro trata um membro que corresponde a uma regra na coleção. Por exemplo, uma conta de usuário ou dispositivo que corresponde a uma regra no conjunto AllowGroup será "aprovada". Ser aprovado significa ter permissão para acessar o Exchange CAS. Uma conta de usuário ou dispositivo que corresponde a uma regra no conjunto DenyGroup é "rejeitada". Rejeitado significa não ter permissão para acessar o Exchange CAS.

Quando uma conta/dispositivo de usuário específica ou uma combinação atende às regras em ambos os grupos, uma convenção de precedência é usada para direcionar o resultado da solicitação. A precedência é incorporada na ordem dos nós GroupRef no arquivo config.xml de cima para baixo. Os nós GroupRef são classificados em ordem de prioridade. As regras para uma determinada condição no grupo Permitir sempre terão precedência sobre as regras para a mesma condição no grupo Negar.

Nós de Grupo

Além disso, o config.xml define nós de Grupo. Esses nós vinculam os contêineres lógicos AllowGroup e DenyGroup a arquivos XML externos. As entradas armazenadas nos arquivos externos formam a base das regras de filtro.

> **Nota:**
>
> Nesta versão, apenas arquivos XML externos são suportados.

> A instalação padrão implementa dois arquivos XML na configuração: allow.xml e deny.xml.

Configurando o conector Citrix Gateway para Exchange ActiveSync

Você pode configurar o conector Citrix Gateway para Exchange ActiveSync para bloquear ou permitir seletivamente solicitações do ActiveSync com base nas seguintes propriedades: **ID do Serviço Active Sync**, **Tipo de dispositivo**, **Agente do usuário** (sistema operacional do dispositivo), **Usuário autorizado** e **Comando ActiveSync**.

A configuração padrão suporta uma combinação de grupos estáticos e dinâmicos. Você mantém grupos estáticos usando o utilitário de Configuração do Controlador SMG. Os grupos estáticos podem consistir em categorias conhecidas de dispositivos, como todos os dispositivos que usam um determinado agente do usuário.

Uma fonte externa chamada Provedor de Configuração de Gateway mantém grupos dinâmicos. O conector Citrix Gateway para Exchange ActiveSync conecta os grupos periodicamente. O XenMobile pode exportar grupos de dispositivos e usuários permitidos e bloqueados para o conector.

Os grupos dinâmicos são mantidos por uma fonte externa chamada Provedor de Configuração de Gateway e coletados pelo conector Citrix Gateway para Exchange ActiveSync periodicamente. O XenMobile pode exportar grupos de dispositivos e usuários permitidos e bloqueados para o conector.

Uma política é uma lista ordenada de grupos em que cada grupo tem uma ação associada (permitir ou bloquear) e uma lista de membros do grupo. Uma política pode ter qualquer número de grupos. A ordem dos grupos dentro de uma política é importante porque, quando uma correspondência é encontrada, a ação do grupo é executada e os grupos subsequentes não são avaliados.

Um membro define uma forma de corresponder às propriedades de uma solicitação. Ele pode corresponder a uma única propriedade, como ID do dispositivo, ou a várias propriedades, como tipo de dispositivo e agente do usuário.

Escolhendo um modelo de segurança para o conector Citrix Gateway para Exchange ActiveSync

Estabelecer um modelo de segurança é essencial para uma implantação bem-sucedida de dispositivos móveis para organizações de qualquer tamanho. É comum usar controle de rede protegido ou em quarentena para permitir o acesso a um usuário, computador ou dispositivo por padrão. Essa prática nem sempre é ideal. Cada organização que gerencia a segurança de TI pode ter uma abordagem ligeiramente diferente ou personalizada para a segurança de dispositivos móveis.

A mesma lógica se aplica à segurança de dispositivos móveis. Usar um modelo permissivo é uma escolha fraca devido à infinidade de dispositivos e tipos de dispositivos móveis, dispositivos móveis por usuário e plataformas e aplicativos de sistema operacional disponíveis. Na maioria das organizações, o modelo restritivo é a escolha mais lógica.

Os cenários de configuração que o Citrix permite para integrar o conector Citrix Gateway para Exchange ActiveSync com o XenMobile são os seguintes:

Modelo Permissivo (Modo de Permissão)

O modelo de segurança permissivo opera sob a premissa de que tudo é permitido ou tem acesso concedido por padrão. Somente por meio de regras e filtragem algo é bloqueado e uma restrição é aplicada. O modelo de segurança permissivo é bom para organizações que têm uma preocupação de segurança relativamente frouxa em relação a dispositivos móveis. O modelo aplica controles restritivos apenas para negar acesso quando apropriado (quando uma regra de política falha).

Modelo Restritivo (Modo de Bloqueio)

O modelo de segurança restritivo baseia-se na premissa de que nada é permitido ou tem acesso concedido por padrão. Tudo o que passa pelo ponto de verificação de segurança é filtrado e inspecionado, e o acesso é negado a menos que as regras que permitem o acesso sejam aprovadas. O modelo de segurança restritivo é bom para organizações que têm um critério de segurança relativamente rigoroso sobre dispositivos móveis. O modo só concede acesso para uso e funcionalidade com os serviços de rede quando todas as regras para permitir o acesso foram aprovadas.

Gerenciando o conector do Citrix Gateway para Exchange ActiveSync

Você pode usar o conector do Citrix Gateway para Exchange ActiveSync para criar regras de controle de acesso. As regras permitem ou bloqueiam o acesso a solicitações de conexão do ActiveSync de dispositivos gerenciados. O acesso é baseado no status do dispositivo, listas de permissão ou bloqueio de aplicativos e outras condições de conformidade.

Ao usar o conector do Citrix Gateway para o utilitário de configuração do Exchange ActiveSync, você pode criar regras dinâmicas e estáticas que impõem políticas de e-mail corporativas, permitindo bloquear usuários que estão em violação dos padrões de conformidade. Você também pode configurar a criptografia de anexos de e-mail, para que todos os anexos que passam pelo seu Exchange Server para dispositivos gerenciados sejam criptografados e visíveis apenas em dispositivos gerenciados por usuários autorizados.

Para desinstalar o conector do Citrix Gateway para Exchange ActiveSync

1. Execute XncInstaller.exe com uma conta de administrador.
2. Siga as instruções na tela para concluir a desinstalação.

Para instalar, atualizar ou desinstalar o conector do Citrix Gateway para Exchange ActiveSync

1. Execute XncInstaller.exe com uma conta de administrador para instalar o conector ou permitir a atualização ou remoção de um conector existente.
2. Siga as instruções na tela para concluir a instalação, atualização ou desinstalação.

Após instalar o conector, você deve reiniciar manualmente o serviço de configuração do XenMobile e o serviço de notificação.

Instalando o conector do Citrix Gateway para Exchange ActiveSync

Você instala o conector do Citrix Gateway para Exchange ActiveSync em seu próprio Windows Server.

A carga da CPU que o conector impõe a um servidor depende de quantos dispositivos são gerenciados. Para um grande número de dispositivos (mais de 50.000), pode ser necessário provisionar mais de um núcleo se você não tiver um ambiente em cluster. O consumo de memória do conector não é significativo o suficiente para justificar mais memória.

Requisitos de sistema do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o Citrix ADC por meio de uma ponte SSL configurada no dispositivo Citrix ADC. A ponte permite que o dispositivo faça a ponte de todo o tráfego seguro diretamente para o XenMobile. O conector requer a seguinte configuração mínima de sistema:

COMPONENTE	REQUISITO
Computador e processador	Processador Pentium III de 733 MHz ou superior. Processador Pentium III de 2,0 GHz ou superior (recomendado)
Citrix ADC	Dispositivo Citrix ADC com versão de software 10
Memória	1 GB

COMPONENTE	REQUISITO
Disco rígido	Partição local formatada em NTFS com 150 MB de espaço disponível em disco rígido
Sistema operacional	Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Deve ser um servidor baseado em inglês. O suporte para Windows Server 2008 R2 Service Pack 1 termina em January 14, 2020 e o suporte para Windows Server 2012 R2 termina em October 10, 2023.
Outros dispositivos	Adaptador de rede compatível com o sistema operacional host para comunicação com a rede interna
Microsoft .NET Framework	A versão 8.5.1.11 requer o Microsoft .NET Framework 4.5.
Monitor	Monitor VGA ou de resolução superior

O computador host para o conector Citrix Gateway para Exchange ActiveSync requer o seguinte espaço mínimo disponível em disco rígido:

- **Aplicativo:** 10–15 MB (100 MB recomendado)
- **Registro:** 1 GB (20 GB recomendado)

Para obter informações sobre o suporte de plataforma para o conector Citrix Gateway para Exchange ActiveSync, consulte Sistemas operacionais de dispositivos compatíveis.

Clientes de e-mail de dispositivo

Nem todos os clientes de e-mail retornam consistentemente o mesmo ID do ActiveSync para um dispositivo. Como o conector Citrix Gateway para Exchange ActiveSync espera um ID do ActiveSync exclusivo para cada dispositivo, o seguinte é verdadeiro: Somente clientes de e-mail que geram consistentemente os mesmos IDs do ActiveSync exclusivos para cada dispositivo são suportados. A Citrix testou esses clientes de e-mail e eles funcionaram sem erros:

- Cliente de e-mail nativo da Samsung
- Cliente de e-mail nativo do iOS

Implantação do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync permite que você use o Citrix ADC para proxy e balanceamento de carga da comunicação do XenMobile Server com dispositivos gerenciados pelo XenMobile. O conector se comunica periodicamente com o XenMobile para sincronizar políticas. O conector e o XenMobile podem ser agrupados juntos ou independentemente, e podem ser balanceados por carga pelo Citrix ADC.

Componentes do conector do Citrix Gateway para Exchange ActiveSync

- **Serviço do conector do Citrix Gateway para Exchange ActiveSync:** Este serviço fornece uma interface de serviço web REST que pode ser invocada pelo Citrix ADC para determinar se uma solicitação ActiveSync de um dispositivo é autorizada.
- **Serviço de configuração do XenMobile:** Este serviço se comunica com o XenMobile para sincronizar as alterações de política do XenMobile com o conector.
- **Serviço de notificação do XenMobile:** Este serviço envia notificações de acesso não autorizado de dispositivos ao XenMobile. Dessa forma, o XenMobile pode tomar as medidas apropriadas, como notificar o usuário sobre o motivo pelo qual o dispositivo foi bloqueado.
- **Utilitário de configuração do conector do Citrix Gateway para Exchange ActiveSync:** Este aplicativo permite que o administrador configure e monitore o conector.

Para configurar endereços de escuta para o conector do Citrix Gateway para Exchange ActiveSync

Para que o conector do Citrix Gateway para Exchange ActiveSync receba solicitações do Citrix ADC para autorizar o tráfego do ActiveSync, faça o seguinte. Especifique a porta na qual o conector escuta as chamadas de serviço web do Citrix ADC.

1. No menu **Iniciar**, selecione o utilitário de configuração do conector do Citrix Gateway para Exchange ActiveSync.
2. Clique na guia **Serviço Web** e digite os endereços de escuta para o serviço web do conector. Você pode selecionar **HTTP** ou **HTTPS** ou ambos. Se o conector for corresidente com o XenMobile (instalado no mesmo servidor), selecione valores de porta que não entrem em conflito com o XenMobile.
3. Depois que os valores forem configurados, clique em **Salvar** e, em seguida, clique em **Iniciar Serviço** para iniciar o serviço web.

Para configurar políticas de controle de acesso de dispositivos no conector do Citrix Gateway para Exchange ActiveSync

Para configurar a política de controle de acesso que você deseja aplicar aos seus dispositivos gerenciados, faça o seguinte:

1. No utilitário de configuração do conector do Citrix Gateway para Exchange ActiveSync, clique na guia **Filtros de Caminho**.
2. Selecione a primeira linha, **Microsoft-Server-ActiveSync é para ActiveSync** e clique em **Editar**.
3. Na lista **Política**, selecione a política desejada. Para uma política que inclua políticas do XenMobile, selecione **Estático + ZDM: Modo Permitir ou Estático + ZDM: Modo Bloquear**. Essas políticas combinam regras locais (ou estáticas) com as regras do XenMobile. O Modo Permitir significa que todos os dispositivos não explicitamente identificados pelas regras têm acesso permitido ao ActiveSync. O Modo Bloquear significa que esses dispositivos são bloqueados.
4. Depois de definir as políticas, clique em **Salvar**.

Para configurar a comunicação com o XenMobile

Especifique o nome e as propriedades do XenMobile Server (também conhecido como Provedor de Configuração) que você deseja usar com o conector do Citrix Gateway para Exchange ActiveSync e Citrix ADC.

> **Nota:**
>
> Esta tarefa pressupõe que você já tenha instalado e configurado o XenMobile.

1. No utilitário de configuração do conector do Citrix Gateway para Exchange ActiveSync, clique na guia **Provedores de Configuração** e, em seguida, clique em **Adicionar**.
2. Insira o nome e o URL do XenMobile Server que você está usando nesta implantação. Se você tiver vários XenMobile Servers implantados em uma implantação multilocatário, esse nome deverá ser exclusivo para cada instância de servidor. Por exemplo, para **Nome**, você pode digitar **XMS**.

3. Em **URL**, insira o endereço da Web do Provedor de Configuração Global (GCP) do XenMobile, geralmente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.
4. Em **Senha**, insira a senha usada para autorização HTTP básica com o servidor web do XenMobile.
5. Em **Host de Gerenciamento**, insira o nome do servidor onde você instalou o conector do Citrix Gateway para Exchange ActiveSync.
6. Em **Intervalo de Linha de Base**, especifique um período para quando um novo conjunto de regras dinâmicas atualizado é extraído do XenMobile.
7. Em **Tempo Limite da Solicitação**, especifique o intervalo de tempo limite da solicitação do servidor.
8. Em **Provedor de Configuração**, selecione se a instância do servidor do provedor de configuração está fornecendo a configuração da política.
9. Em **Eventos Habilitados**, ative esta opção se desejar que o Secure Mobile Gateway notifique o XenMobile quando um dispositivo for bloqueado. Esta opção é necessária se você estiver usando regras do Secure Mobile Gateway em qualquer uma de suas Ações Automatizadas do Gerenciador de Dispositivos.
10. Após configurar o servidor, clique em **Testar Conectividade** para testar a conexão com o XenMobile.
11. Quando a conectividade for estabelecida, clique em **Salvar**.

Implantando o Citrix Gateway connector para Exchange ActiveSync para redundância e escalabilidade

Se você quiser escalar sua implantação do Citrix Gateway connector para Exchange ActiveSync e XenMobile, você pode instalar instâncias do conector em vários servidores Windows, todos apontando para a mesma instância do XenMobile, e então você pode usar o Citrix ADC para balancear a carga dos servidores.

Existem dois modos para a configuração do Citrix Gateway connector para Exchange ActiveSync:

- No modo não compartilhado, cada instância do Citrix Gateway connector para Exchange ActiveSync se comunica com um XenMobile Server e mantém sua própria cópia privada da política resultante. Por exemplo, se você tivesse um cluster de XenMobile Servers, você poderia executar uma instância do conector em cada XenMobile Server e o conector obteria políticas da instância local do XenMobile.

- No modo compartilhado, um nó do conector é escolhido como o nó primário e ele se comunica com o XenMobile. A configuração resultante é compartilhada entre os outros nós por meio de um compartilhamento de rede do Windows ou por replicação do Windows (ou de terceiros).

Toda a configuração do conector está em uma única pasta (consistindo em alguns arquivos XML). O processo do conector detecta alterações em qualquer arquivo nesta pasta e recarrega automaticamente a configuração. Não há failover para o nó primário no modo compartilhado. Mas o sistema pode tolerar que o servidor primário fique inativo por alguns minutos (por exemplo, para reiniciar) porque a última configuração boa conhecida é armazenada em cache no processo do conector.

Conceitos Avançados

> **Nota:**
>
> Este artigo aborda conceitos avançados para o XenMobile Server. Para informações avançadas sobre o Citrix Endpoint Management, consulte Conceitos avançados.

> Os artigos de Conceitos Avançados do XenMobile® oferecem um aprofundamento na documentação do produto sobre o XenMobile. O objetivo é ajudar a reduzir o tempo de implantação por meio de técnicas especializadas. Os artigos podem citar os especialistas técnicos que elaboraram o conteúdo.

Para pontos de decisão, recomendações, perguntas comuns e casos de uso para seu ambiente XenMobile de ponta a ponta, consulte o Manual de Implantação do XenMobile nesta seção.

Para fóruns de suporte da comunidade sobre XenMobile, consulte Discussões Citrix.

Interação do XenMobile® local com o Active Directory

Este artigo explica a interação entre o XenMobile Server e o Active Directory. O XenMobile Server interage com o Active Directory tanto de forma direta (inline) quanto em segundo plano. As seções a seguir fornecem mais informações sobre as operações diretas e em segundo plano que envolvem a interação com o Active Directory.

> **Nota:**
>
> Este artigo é uma visão geral da interação e não aborda os detalhes granulares. Para obter mais informações sobre como configurar o Active Directory e o LDAP no console do XenMobile, consulte Autenticação de domínio ou domínio mais token de segurança.

Interações diretas

O XenMobile Server se comunica com o Active Directory usando as configurações LDAP que um administrador configura. As configurações recuperam informações sobre usuários e grupos. A seguir estão as operações que resultam na interação entre o XenMobile Server e o Active Directory.

1. **Configuração LDAP.** A própria configuração do Active Directory resulta em uma interação com o Active Directory. O XenMobile Server tenta validar as informações autenticando-as com o Active Directory. O servidor faz isso usando o protocolo de internet, a porta e as credenciais da conta de serviço fornecidos. Uma vinculação bem-sucedida indica que a conexão está configurada corretamente.
2. **Interações baseadas em grupo.**

    a. Pesquisa por um ou mais grupos durante a criação da definição de Controle de Acesso Baseado em Função (RBAC) e de grupo de entrega. O administrador do XenMobile Server insere uma string de texto de pesquisa no console do XenMobile. O XenMobile Server pesquisa o domínio selecionado por todos os grupos que contêm a substring fornecida. Em seguida, o XenMobile Server recupera os atributos objectGUID, sAMAccountName e Distinguished Name dos grupos identificados na pesquisa.

    > **Nota:**
    >
    > Esta informação não é armazenada no banco de dados do XenMobile Server.

    b. Adição ou atualização da definição de RBAC e grupo de implantação. O administrador do XenMobile Server seleciona os grupos do Active Directory de interesse com base na pesquisa anterior e os inclui na definição do grupo de implantação. O XenMobile Server pesquisa o grupo específico um por um no Active Directory. O XenMobile Server pesquisa o atributo objectGUID e recupera atributos selecionados, incluindo informações de associação. As informações de associação de grupo ajudam a determinar a associação entre o grupo recuperado e os usuários ou grupos existentes no banco de dados do XenMobile Server. Alterações na associação de grupo resultam na derivação de RBAC e grupo de implantação para os membros usuários afetados, o que resulta em direitos de usuário.

    > **Nota:**

> Alterações na definição do grupo de implantação podem levar a mudanças nos direitos de aplicativos ou políticas para os usuários afetados.

c. **Convites de PIN único (OTP)**. O administrador do XenMobile Server seleciona um grupo da lista de grupos do Active Directory presentes no banco de dados do XenMobile Server. Para este grupo, todos os usuários, diretos e indiretos, são recuperados do Active Directory. Os convites OTP são enviados aos usuários identificados na etapa anterior.

> **Nota:**
>
> As três interações anteriores implicam que as interações baseadas em grupo são acionadas com base nas alterações de configuração do XenMobile Server. Quando não há alterações na configuração, as interações implicam que não há interações com o Active Directory. Elas também implicam que não há necessidade de trabalhos em segundo plano para capturar o lado do grupo das alterações periodicamente.

3. **Interação baseada no usuário**

a. **Autenticação do usuário:** O fluxo de trabalho de autenticação do usuário resulta em duas interações com o Active Directory:

- Usado para autenticar o usuário com as credenciais fornecidas.
- Adicionar ou atualizar atributos de usuário selecionados no banco de dados do XenMobile Server, incluindo objectGUID, Distinguished Name, sAMAccountName e associação direta a grupos. Alterações na associação a grupos resultam na reavaliação dos direitos de aplicativo, política e acesso.

O usuário pode autenticar tanto do dispositivo quanto do console do XenMobile Server. Em ambos os cenários, a interação com o Active Directory adere ao mesmo comportamento.

b. **Acesso e atualização da App Store:** Uma atualização da loja resulta em uma atualização dos atributos do usuário, incluindo associações diretas a grupos. Esta ação permite uma reavaliação dos direitos do usuário.

c. **Check-ins de dispositivo:** Os administradores podem configurar no console do XenMobile os check-ins de dispositivo periodicamente. Cada vez que um dispositivo é verificado, os atributos de usuário correspondentes são atualizados, incluindo associações diretas a grupos. Esses check-ins permitem uma reavaliação dos direitos do usuário.

d. **Convites OTP por Grupo:** O administrador do XenMobile Server seleciona um grupo da lista de grupos do Active Directory presentes no banco de dados do XenMobile Server. Os membros do usuário, tanto diretos quanto indiretos (devido ao aninhamento), são recuperados do Active Directory e salvos no banco de dados do XenMobile Server. Os convites OTP são enviados aos membros do usuário identificados na etapa anterior.

e. **Convites OTP por usuário:** O administrador insere uma string de texto de pesquisa no console do XenMobile. O XenMobile Server consulta o Active Directory e retorna os registros de usuário que correspondem à string de texto inserida. O administrador então seleciona o usuário para enviar o convite OTP. O XenMobile Server recupera os detalhes do usuário do Active Directory e atualiza os mesmos detalhes no banco de dados antes de enviar o convite ao usuário.

Interações em segundo plano

Uma conclusão da comunicação em linha com o Active Directory é que as interações baseadas em grupo são acionadas mediante alterações selecionadas na configuração do XenMobile Server. Quando não há alterações na configuração, isso implica que não há interações com o Active Directory para grupos.

Essa interação requer trabalhos em segundo plano que sincronizam periodicamente com o Active Directory e atualizam as alterações relevantes para os grupos interessados.

A seguir estão os trabalhos em segundo plano que interagem com o Active Directory.

1. **Trabalho de sincronização de grupo**. O objetivo deste trabalho é consultar o Active Directory, um grupo por vez, sobre grupos de interesse para alterações nos atributos de nome distinto ou sAMAccountName. A consulta de pesquisa ao Active Directory usa o objectGUID do grupo de interesse para obter os valores atuais dos atributos de nome distinto e sAMAccountName. As alterações nos valores de nome distinto ou sAMAccountName para grupos de interesse são atualizadas no banco de dados.

   > **Nota:**
   >
   > Este trabalho não atualiza as informações de associação de usuário a grupo.

2. **Trabalho de sincronização de grupo aninhado**. Este trabalho atualiza as alterações na hierarquia de aninhamento de grupos de interesse. O XenMobile Server permite que membros diretos e indiretos de um grupo de interesse obtenham direitos. A associação direta dos

usuários é atualizada durante as interações em linha baseadas no usuário. Executado em segundo plano, este trabalho rastreia as associações indiretas. Associações indiretas ocorrem quando um usuário é membro de um grupo que é membro de um grupo de interesse.

Este trabalho coleta a lista de grupos do Active Directory do banco de dados do XenMobile Server. Esses grupos fazem parte do grupo de implantação ou da definição de RBAC. Para cada grupo nesta lista, o XenMobile Server obtém os membros do grupo. Os membros de um grupo são uma lista de nomes distintos que representam usuários e grupos.

O XenMobile Server faz outra consulta ao Active Directory para obter apenas os membros usuários do grupo de interesse. A diferença entre as duas listas fornece apenas os membros do grupo para o grupo de interesse. As alterações nos grupos de membros são atualizadas no banco de dados. O mesmo processo é repetido para todos os grupos na hierarquia.

As alterações no aninhamento resultam no processamento dos usuários afetados para alterações de direitos.

3. **Verificação de usuário desabilitado**. Este trabalho é executado apenas quando o administrador do XenMobile cria uma ação para verificar usuários desabilitados. O trabalho é executado no escopo de um trabalho de sincronização de grupo. O trabalho consulta o Active Directory para verificar o status de desabilitação de usuários de interesse, um usuário por vez.

FAQ

Qual é a frequência de execução dos trabalhos em segundo plano, por padrão?

- Os trabalhos de sincronização de grupo são executados a cada cinco horas, a partir das 02:00, horário local.
- Os trabalhos de sincronização de grupo aninhado são executados uma vez por dia à meia-noite, horário local.

Por que um trabalho de sincronização de grupo é necessário?

- O atributo **memberOf** de um registro de usuário no Active Directory fornece a lista de grupos dos quais o usuário é membro direto. Se um grupo se move de uma OU para outra, o atributo **memberOf** reflete o valor mais recente do nome distinto. O banco de dados do XenMobile Server também possui o último valor atualizado. Qualquer incompatibilidade nos nomes distintos do grupo pode resultar na perda de acesso do usuário ao grupo de implantação. O usuário também pode perder os aplicativos e políticas associados a esse grupo de implantação.

- O trabalho em segundo plano mantém o atributo de nome distinto do grupo atualizado no banco de dados do XenMobile Server para garantir que os usuários tenham acesso aos seus direitos.
- Os trabalhos de sincronização são agendados a cada cinco horas porque se assume que as alterações de grupo dentro do Active Directory são incomuns.

Um trabalho de sincronização de grupo pode ser desativado?

- Você pode desativar trabalhos quando souber que os grupos de interesse não mudam de uma OU para outra.

Por que um trabalho em segundo plano de processamento de grupo aninhado é necessário?

- Alterações no aninhamento de grupos no Active Directory não são uma ocorrência diária. Alterações na hierarquia de aninhamento de grupos de interesse resultam em alterações nos direitos dos usuários afetados. Quando um grupo é adicionado à hierarquia, seus usuários membros tornam-se elegíveis para as respectivas funções. Quando um grupo sai do aninhamento, os usuários membros do grupo podem perder o acesso aos direitos baseados em função.
- As alterações de aninhamento não são capturadas durante a atualização do usuário. Como as alterações de aninhamento não podem ser sob demanda, as alterações são capturadas por meio de um trabalho em segundo plano.
- As alterações de aninhamento são consideradas incomuns e, portanto, o trabalho em segundo plano é executado uma vez por dia para verificar se há alguma alteração.

Um trabalho de processamento de grupo aninhado pode ser desativado?

- Você pode desativar trabalhos quando souber que as alterações de aninhamento não ocorrem em grupos de interesse.

Implantação do XenMobile®

Há muito a considerar ao planejar uma implantação do XenMobile:

- Quais dispositivos escolher?
- Como gerenciar os dispositivos?
- Como garantir que sua rede permaneça segura enquanto ainda oferece uma ótima experiência do usuário?
- Qual hardware você precisa e como solucionar problemas?

Os artigos nesta seção visam ajudar a responder a essas perguntas. Estão incluídos casos de uso e recomendações sobre tópicos que abrangem suas preocupações de implantação.

Tenha em mente que uma diretriz ou recomendação pode não se aplicar a todos os ambientes ou casos de uso. Certifique-se de configurar um ambiente de teste antes de entrar em produção com uma implantação do XenMobile.

Os artigos nesta seção abrangem estas áreas:

- **Avaliar:** Casos de uso comuns e perguntas a serem consideradas ao planejar sua implantação.
- **Projetar e Configurar:** Recomendações para projetar e configurar seu ambiente
- **Operar e Monitorar:** Garantindo a operação tranquila do seu ambiente em execução.

Avaliar

Como em qualquer implantação, avaliar suas necessidades é a principal prioridade. Qual é a sua principal necessidade para o XenMobile? Você precisa gerenciar todos os dispositivos em seu ambiente ou apenas os aplicativos? Talvez você precise gerenciar ambos. Quão seguro você precisa que seu ambiente XenMobile seja? Vamos analisar casos de uso comuns e perguntas para você considerar ao planejar sua implantação.

- Modos de gerenciamento
- Requisitos do dispositivo
- Segurança e experiência do usuário
- Aplicativos
- Comunidades de usuários
- Estratégia de e-mail
- Integração do XenMobile
- Requisitos de vários sites

Projetar e configurar

Depois de terminar de avaliar suas necessidades de implantação, você pode determinar o design e a configuração do seu ambiente. Algumas coisas que você precisa planejar:

- Escolher o hardware para seu servidor
- Configurar políticas para aplicativos e dispositivos

- Registrar usuários

Esta seção inclui casos de uso e recomendações para cada um desses cenários e muito mais.

- Integração com Citrix ADC e Citrix Gateway
- Considerações de SSO e proxy para aplicativos MDX
- Autenticação
- Arquitetura de referência para implantações locais
- Propriedades do servidor
- Políticas de dispositivo e aplicativo
- Opções de registro de usuário
- Ajustando as operações do XenMobile

Operar e monitorar

Depois que seu ambiente XenMobile estiver funcionando, você desejará monitorá-lo para garantir uma operação tranquila. A seção de monitoramento aborda o seguinte:

- Onde você pode encontrar os vários logs e mensagens que o XenMobile e seus componentes geram
- Como ler esses logs

Esta seção também inclui várias etapas comuns de solução de problemas que você pode seguir para reduzir o tempo de feedback do suporte ao cliente.

- Provisionamento e desprovisionamento de aplicativos
- Operações baseadas em painel
- Controle de Acesso Baseado em Função e suporte XenMobile
- Monitoramento de sistemas
- Recuperação de desastres
- Processo de suporte Citrix

Modos de Gerenciamento

Para cada instância do XenMobile® (um único servidor ou um cluster de nós), você pode escolher se deseja gerenciar dispositivos, aplicativos ou ambos. O XenMobile usa os seguintes termos para os modos de gerenciamento de dispositivos e aplicativos:

- Modo de gerenciamento de dispositivos móveis (modo MDM)
- Modo de gerenciamento de aplicativos móveis (modo MAM)
- Modo MDM+MAM (modo Enterprise)

Gerenciamento de dispositivos móveis (modo MDM)

Importante:

Se você configurar o modo MDM e depois mudar para o modo ENT, certifique-se de usar a mesma autenticação (Active Directory). O XenMobile não oferece suporte à alteração do modo de autenticação após o registro do usuário. Para obter mais informações, consulte Atualização.

Com o MDM, você pode configurar, proteger e dar suporte a dispositivos móveis. O MDM permite proteger dispositivos e dados em dispositivos em nível de sistema. Você pode configurar políticas, ações e funções de segurança. Por exemplo, você pode apagar um dispositivo seletivamente se ele for perdido, roubado ou estiver fora de conformidade. Embora o gerenciamento de aplicativos não esteja disponível no modo MDM, você pode entregar aplicativos móveis, como aplicativos de lojas públicas e aplicativos corporativos, neste modo. A seguir estão casos de uso comuns para o modo MDM:

- O MDM é uma consideração para dispositivos de propriedade corporativa onde políticas ou restrições de gerenciamento em nível de dispositivo, como limpeza completa, limpeza seletiva ou geolocalização, são necessárias.
- Quando os clientes exigem o gerenciamento de um dispositivo real, mas não exigem políticas MDX, como conteinerização de aplicativos, controles sobre o compartilhamento de dados de aplicativos ou micro VPN.
- Quando os usuários precisam apenas de e-mail entregue aos seus clientes de e-mail nativos em seus dispositivos móveis, e o Exchange ActiveSync ou o Client Access Server já está acessível externamente. Neste caso de uso, você pode usar o MDM para configurar a entrega de e-mail.
- Ao implantar aplicativos corporativos nativos (não-MDX), aplicativos de lojas de aplicativos públicas ou aplicativos MDX entregues de lojas públicas. Considere que uma solução MDM sozinha pode não impedir o vazamento de dados de informações confidenciais entre aplicativos no dispositivo. O vazamento de dados pode ocorrer com operações de copiar e colar ou Salvar como em aplicativos do Office 365.

Gerenciamento de aplicativos móveis (modo MAM)

O MAM protege os dados do aplicativo e permite controlar o compartilhamento de dados do aplicativo. O MAM também permite o gerenciamento de dados e recursos corporativos, separadamente dos dados pessoais. Com o XenMobile configurado para o modo MAM, você pode usar aplicativos móveis habilitados para MDX para fornecer conteinerização e controle por aplicativo. O termo modo MAM também é chamado de modo somente MAM. Este termo distingue este modo de um modo MAM legado.

Ao usar políticas MDX, o XenMobile fornece controle no nível do aplicativo sobre o acesso à rede (como micro VPN), interação entre aplicativo e dispositivo, criptografia de dados e acesso a aplicativos.

O MAM geralmente é adequado para dispositivos próprios (BYO) porque, embora o dispositivo não seja gerenciado, os dados corporativos permanecem protegidos. O MDX possui muitas políticas somente MAM que não exigem um controle MDM.

O MAM também oferece suporte aos aplicativos de produtividade móvel. Esse suporte inclui entrega segura de e-mail para o Citrix Secure Mail, compartilhamento de dados entre os aplicativos de produtividade móvel seguros e armazenamento seguro de dados no Citrix Files. Para obter detalhes, consulte aplicativos de produtividade móvel.

O MAM geralmente é adequado para os seguintes exemplos:

- Você entrega aplicativos móveis, como aplicativos MDX, gerenciados no nível do aplicativo.
- Você não é obrigado a gerenciar dispositivos no nível do sistema.

MDM+MAM (Modo Empresarial)

MDM+MAM é um modo híbrido, também chamado de Modo Empresarial, que habilita todos os conjuntos de recursos disponíveis na solução XenMobile Enterprise Mobility Management (EMM). A configuração do XenMobile com o modo MDM+MAM habilita os recursos de MDM e MAM.

O XenMobile permite que você especifique se os usuários podem optar por não participar do gerenciamento de dispositivos ou se você exige o gerenciamento de dispositivos. Essa flexibilidade é útil para ambientes que incluem uma mistura de casos de uso. Esses ambientes podem ou não exigir o gerenciamento de um dispositivo por meio de políticas MDM para acessar seus recursos MAM.

MDM+MAM é adequado para os seguintes exemplos:

- Você tem um único caso de uso em que MDM e MAM são necessários. O MDM é necessário para acessar seus recursos MAM.
- Alguns casos de uso exigem MDM, enquanto outros não.
- Alguns casos de uso exigem MAM, enquanto outros não.

Você especifica o modo de gerenciamento para o XenMobile Server por meio da propriedade **Server Mode**. Você configura a definição no console do XenMobile. O modo pode ser MDM, MAM ou ENT (para MDM+MAM).

A edição do XenMobile para a qual você tem uma licença determina os modos de gerenciamento e outros recursos disponíveis, conforme mostrado na tabela a seguir.

Edição XenMobile MDM	**Edição XenMobile Advanced**
Recursos MDM	Recursos MDM
-	Recursos MAM
-	SDK MAM
Secure Hub	Secure Hub
-	Secure Mail
-	Secure Web

Modos de gerenciamento e perfis de registro

Os modos de gerenciamento e os perfis de registro funcionam juntos. Você usa um perfil de registro para configurar as opções de registro de gerenciamento de dispositivos e gerenciamento de aplicativos para dispositivos Android e iOS. Para Android, as opções de registro disponíveis para o modo de servidor MDM+MAM diferem das opções para o modo MDM. Para obter mais informações, consulte Perfis de registro.

Gerenciamento de Dispositivos e Registro MDM

Um ambiente XenMobile Enterprise pode incluir uma mistura de casos de uso, alguns dos quais exigem gerenciamento de dispositivos por meio de políticas MDM para permitir o acesso a recursos MAM. Antes de implantar aplicativos de produtividade móvel para usuários, avalie completamente seus casos de uso e decida se deve exigir o registro MDM. Se você decidir mais

tarde alterar o requisito para o registro MDM, é provável que os usuários precisem registrar novamente seus dispositivos.

> **Nota:**
>
> Para especificar se você exige que os usuários se registrem no MDM, use a propriedade do XenMobile Server **Enrollment Required** no console do XenMobile (**Settings > Server Properties**). Essa propriedade global do servidor se aplica a todos os usuários e dispositivos para a instância do XenMobile. A propriedade se aplica somente quando o Modo de Servidor XenMobile é ENT.

> A seguir, um resumo das vantagens e desvantagens (juntamente com as mitigações) de exigir o registro MDM em uma implantação no modo XenMobile Enterprise.

Quando o registro MDM é opcional

Vantagens:

- Os usuários podem acessar recursos MAM sem colocar seus dispositivos sob gerenciamento MDM. Essa opção pode aumentar a adoção pelos usuários.
- Capacidade de proteger o acesso a recursos MAM para proteger dados corporativos.
- Políticas MDX como **App Passcode** podem controlar o acesso a aplicativos para cada aplicativo MDX.
- A configuração do Citrix ADC, XenMobile Server e tempos limite por aplicativo, juntamente com o Citrix PIN, fornecem uma camada extra de proteção.
- Embora as ações MDM não se apliquem ao dispositivo, algumas políticas MDX estão disponíveis para negar o acesso MAM. A negação seria baseada em configurações do sistema, como dispositivos com jailbreak ou root.
- Os usuários podem escolher se desejam registrar seu dispositivo com MDM durante o primeiro uso.

Desvantagens:

- Os recursos MAM estão disponíveis para dispositivos não registrados no MDM.
- As políticas e ações de MDM estão disponíveis apenas para dispositivos registrados no MDM.

Opções de mitigação:

- Faça com que os usuários concordem com os termos e condições da empresa que os responsabilizam caso optem por não cumprir as regras. Peça aos administradores para monitorar dispositivos não gerenciados.
- Gerencie o acesso e a segurança de aplicativos usando temporizadores de aplicativos. Valores de tempo limite diminuídos aumentam a segurança, mas podem afetar a experiência do usuário.
- Um segundo ambiente XenMobile com registro MDM obrigatório é uma opção. Ao considerar esta opção, tenha em mente a sobrecarga adicional de gerenciar dois ambientes e os recursos adicionais necessários.

Quando o registro MDM é obrigatório

Vantagens:

- Capacidade de restringir o acesso aos recursos MAM apenas a dispositivos gerenciados por MDM.
- As políticas e ações de MDM podem ser aplicadas a todos os dispositivos no ambiente, conforme desejado.
- Os usuários não podem optar por não registrar seus dispositivos.

Desvantagens:

- Exige que todos os usuários se registrem no MDM.
- Pode diminuir a adoção para usuários que se opõem ao gerenciamento corporativo de seus dispositivos pessoais.

Opções de mitigação:

- Eduque os usuários sobre o que o XenMobile realmente gerencia em seus dispositivos e quais informações os administradores podem acessar.
- Você pode usar um segundo ambiente XenMobile, com um Modo de Servidor MAM (também chamado de modo somente MAM), para dispositivos que não precisam de gerenciamento MDM. Ao considerar esta opção, tenha em mente a sobrecarga adicional de gerenciar dois ambientes e os recursos adicionais necessários.

Sobre os modos MAM e MAM herdado

O XenMobile 10.3.5 introduziu um novo modo de servidor somente MAM. Para distinguir os modos MAM anteriores e novos, a documentação usa estes termos. O novo modo é chamado de somente MAM ou MA, o modo MAM anterior é chamado de modo MAM herdado.

O modo somente MAM está em vigor quando a propriedade **Modo de Servidor** do XenMobile é MAM. Os dispositivos se registram no modo MAM.

A funcionalidade MAM herdada está em vigor quando a propriedade **Modo de Servidor** do XenMobile é ENT e os usuários optam por não participar do gerenciamento de dispositivos. Nesse caso, os dispositivos se registram no modo MAM. Os usuários que optam por não participar do gerenciamento MDM continuam a receber a funcionalidade MAM herdada.

> **Nota:**
>
> Anteriormente, definir a propriedade Modo de Servidor como MAM tinha o mesmo efeito que defini-la como ENT: os usuários que optaram por não participar do gerenciamento MDM recebiam a funcionalidade MAM herdada.

A tabela a seguir resume a configuração de **Modo de Servidor** a ser usada para um tipo de licença específico e modo de dispositivo desejado:

Suas licenças são para esta edição	**Você deseja que os dispositivos se registrem neste modo**	**Defina a propriedade Modo de Servidor como**
Enterprise/ Advanced/MDM	Modo MDM	MDM
Enterprise/Avançado	Modo MAM (também chamado de modo somente MAM)	MAM
Enterprise/Avançado	Modo MDM+MAM	ENT (Usuários que optam por não usar o gerenciamento de dispositivos operam no modo MAM herdado.)

O modo somente MAM oferece suporte aos seguintes recursos que antes estavam disponíveis apenas para ENT.

- **Autenticação baseada em certificado:** O modo somente MAM oferece suporte à autenticação baseada em certificado. Os usuários experimentam acesso contínuo aos seus aplicativos mesmo quando a senha do Active Directory expira. Se você usar autenticação

baseada em certificado para dispositivos MAM, deverá configurar seu Citrix Gateway. Por padrão, em **XenMobile Settings > Citrix Gateway**, a opção Deliver the user certificate for authentication é definida como **Off**, o que significa que a autenticação por nome de usuário e senha é usada. Altere essa configuração para **On** para habilitar a autenticação por certificado.

- **Portal de Autoatendimento:** Para permitir que os usuários realizem seus próprios bloqueios e limpezas de aplicativos. Essas ações se aplicam a todos os aplicativos no dispositivo. Você pode configurar as ações de Bloqueio de Aplicativo e Limpeza de Aplicativo em **Configure > Actions**.
- **Todos os modos de segurança de registro:** Incluindo Alta Segurança, URL de Convite e Dois Fatores, configurados por meio de **Manage > Enrollment Invitations**.
- **Limite de registro de dispositivo para dispositivos Android e iOS:** A Propriedade do Servidor **Number of Devices Per User** foi movida para **Configure > Enrollment Profiles** e agora se aplica a todos os modos de servidor.
- **APIs somente MAM:** Para dispositivos somente MAM, você pode chamar serviços REST usando qualquer cliente REST e a API REST do XenMobile para chamar serviços que o console do XenMobile expõe.
- As APIs somente MAM permitem que você:
  - Envie um URL de convite e um PIN de uso único.
  - Emita bloqueio e limpeza de aplicativo em dispositivos.

A tabela a seguir resume as diferenças entre a funcionalidade MAM herdada e a funcionalidade somente MAM.

Cenários de Registro e Outros Recursos	**MAM Herdado (o modo do servidor é ENT)**	**Modo somente MAM (o modo do servidor é MAM)**
Autenticação por certificado	Não suportado.	Suportado. Para autenticação por certificado, o Citrix Gateway é necessário.
Requisito de implantação	O XenMobile Server não precisa ser diretamente acessível a partir dos dispositivos.	O XenMobile Server não precisa ser diretamente acessível a partir dos dispositivos.
Opção de registro	Use o FQDN do Citrix Gateway ou, ao usar o FQDN	Use o FQDN do XenMobile Server.

	do MDM, opte por não registrar.	
Métodos de registro*	Nome de usuário + Senha	Nome de usuário + Senha, Alta Segurança, URL de Convite, URL de Convite+PIN, URL de Convite + Senha, Dois Fatores, Nome de usuário + PIN
Bloqueio e limpeza de aplicativos	Compatível.	Compatível.
Opções do Portal de Autoatendimento para bloqueio e limpeza de aplicativos	Não compatível.	Compatível.
Comportamento de limpeza de aplicativos	Os aplicativos permanecem no dispositivo, mas não são utilizáveis. O XenMobile exclui a conta apenas no cliente.	Os aplicativos permanecem no dispositivo, mas não são utilizáveis. O XenMobile exclui a conta apenas no cliente.
Ações automatizadas para usuários somente MAM.	Ações de evento, propriedade de dispositivo e propriedade de usuário são compatíveis. Não oferece suporte a ações automatizadas baseadas em aplicativos instalados.	Suporta ações de evento, propriedade de dispositivo, propriedade de usuário e algumas ações baseadas em aplicativos, incluindo limpeza e bloqueio de aplicativos.
Ação integrada quando um usuário do Active Directory é excluído	Suporta limpeza de aplicativos.	Suporta limpeza de aplicativos.
Limite de registro	Compatível; configurado por meio de um perfil de registro.	Compatível; configurado por meio de um perfil de registro.
Inventário de software	Compatível. O XenMobile lista os aplicativos instalados em um dispositivo	Não compatível.

*__Sobre as notificações:__ SMTP é o único método compatível para enviar convites de registro.

> **Importante:**
>
> Para o modo somente MAM, os usuários previamente registrados devem registrar novamente seus dispositivos. Certifique-se de fornecer aos usuários o FQDN do XenMobile Server de que precisam para o registro. No modo somente MAM, assim como no modo ENT, os dispositivos são registrados usando o FQDN do XenMobile Server. (No modo MAM herdado, os dispositivos são registrados usando o FQDN do Citrix Gateway.)

Requisitos do Dispositivo

Um ponto importante a considerar para qualquer implantação é o dispositivo que você planeja implementar. Nas plataformas iOS, Android e Windows, as opções são muitas. Para obter uma lista de dispositivos compatíveis com o XenMobile, consulte Plataformas de dispositivos compatíveis.

Em um ambiente de traga seu próprio dispositivo (BYOD), uma mistura de plataformas compatíveis é possível. No entanto, considere as limitações no artigo Plataformas de dispositivos compatíveis ao informar os usuários sobre os dispositivos que eles podem registrar. Mesmo que você permita apenas um ou dois dispositivos em seu ambiente, o XenMobile® funciona de forma ligeiramente diferente em dispositivos iOS, Android e Windows. Diferentes conjuntos de recursos estão disponíveis em cada plataforma.

Além disso, nem todos os designs de aplicativos visam fatores de forma de tablet e telefone. Antes de fazer alterações generalizadas, teste os aplicativos para garantir que eles se ajustem à tela do dispositivo que você deseja implementar.

Você também pode considerar os fatores de registro. Apple e Google oferecem programas de registro empresarial. Através do Programa de Implantação da Apple e do Google Android Enterprise, você pode adquirir dispositivos pré-configurados e prontos para uso pelos funcionários.

Para obter mais informações sobre o registro, consulte Opções de Registro de Usuário.

Segurança e Experiência do Usuário

A segurança é importante para qualquer organização, mas é preciso encontrar um equilíbrio entre segurança e experiência do usuário. Por exemplo, você pode ter um ambiente altamente seguro que é difícil para os usuários utilizarem. Ou, seu ambiente pode ser tão amigável ao usuário que o

controle de acesso não é tão rigoroso. As outras seções deste manual virtual cobrem os recursos de segurança em detalhes. O objetivo deste artigo é fornecer uma visão geral das preocupações comuns de segurança e das opções de segurança disponíveis no XenMobile.

Aqui estão algumas considerações importantes a ter em mente para cada caso de uso:

- Você deseja proteger apenas alguns aplicativos, o dispositivo inteiro ou ambos?
- Como você deseja que seus usuários autenticar sua identidade? Você planeja usar LDAP, autenticação baseada em certificado ou uma combinação dos dois?
- Como você deseja manipular os tempos limite da sessão do usuário? Lembre-se de que existem diferentes valores de tempo limite para serviços em segundo plano, Citrix ADC e para poder acessar aplicativos offline.
- Você quer que os usuários configurem uma senha no nível do dispositivo, uma senha no nível do aplicativo ou ambos? Quantas tentativas de logon você deseja conceder aos usuários? Lembre-se de como os requisitos extras de autenticação por aplicativo implementados com o MAM podem impactar a experiência do usuário.
- Que outras restrições você deseja impor aos usuários? Você quer que os usuários acessem serviços em nuvem como a Siri? O que eles podem e não podem fazer com cada aplicativo que você disponibiliza a eles? Você deseja implantar políticas de Wi-Fi corporativo para evitar que planos de dados celulares sejam consumidos dentro dos escritórios?

Aplicativo versus Dispositivo

Uma das primeiras coisas a considerar é se deve proteger apenas certos aplicativos usando o gerenciamento de aplicativos móveis (MAM). Ou se você também deseja gerenciar o dispositivo inteiro usando o gerenciamento de dispositivos móveis (MDM). Mais comumente, se você não exige controle no nível do dispositivo, você gerencia apenas aplicativos móveis, especialmente se sua organização suporta Bring Your Own Device (BYOD).

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da loja de aplicativos. Em vez de controles no nível do dispositivo, como limpeza seletiva ou completa, você controla o acesso aos aplicativos através de políticas de aplicativo. As políticas, dependendo dos valores que você definir, exigem que o dispositivo verifique o XenMobile rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

O MDM permite proteger um dispositivo inteiro, incluindo a capacidade de fazer um inventário de todo o software em um dispositivo. Você pode impedir o registro se o dispositivo estiver com jailbreak, root ou tiver software inseguro instalado. No entanto, assumir esse nível de controle faz

com que os usuários hesitem em permitir tanto poder sobre seus dispositivos pessoais e pode reduzir as taxas de registro.

Autenticação

A autenticação é onde grande parte da experiência do usuário acontece. Se sua organização já está executando o Active Directory, usar o Active Directory é a maneira mais simples de fazer com que seus usuários acessem o sistema.

Outra parte significativa da experiência do usuário de autenticação são os tempos limite. Um ambiente de alta segurança pode fazer com que os usuários façam logon toda vez que acessam o sistema, mas essa opção não é ideal para todas as organizações. Por exemplo, fazer com que os usuários insiram suas credenciais toda vez que desejam acessar seu e-mail pode impactar significativamente a experiência do usuário.

Entropia do Usuário

Para maior segurança, você pode habilitar um recurso chamado *entropia do usuário*. O Citrix Secure Hub™ e alguns outros aplicativos geralmente compartilham dados comuns, como senhas, PINs e certificados, para garantir que tudo funcione corretamente. Essas informações são armazenadas em um cofre genérico dentro do Secure Hub. Se você habilitar a entropia do usuário por meio da opção **Criptografar Segredos**, o XenMobile cria um novo cofre chamado UserEntropy. O XenMobile move as informações do cofre genérico para o novo cofre. Para que o Secure Hub ou outro aplicativo acesse os dados, os usuários devem inserir uma senha ou PIN.

Habilitar a entropia do usuário adiciona outra camada de autenticação em vários locais. Como resultado, os usuários devem inserir uma senha ou PIN cada vez que um aplicativo exigir acesso a dados compartilhados, incluindo certificados, no cofre UserEntropy.

Você pode aprender mais sobre a entropia do usuário lendo Sobre o MDX Toolkit na documentação do XenMobile. Para ativar a entropia do usuário, você pode encontrar as configurações relacionadas em Propriedades do cliente.

Políticas

As políticas MDX e MDM oferecem grande flexibilidade às organizações, mas também podem restringir os usuários. Por exemplo, você pode querer bloquear o acesso a aplicativos em nuvem, como Siri ou iCloud, que têm o potencial de enviar dados confidenciais para vários locais. Você pode configurar uma política para bloquear o acesso a esses serviços, mas lembre-se de que tal política pode ter consequências não intencionais. O microfone do teclado iOS também depende do acesso à nuvem e você pode bloquear o acesso a esse recurso também.

Aplicativos

O Enterprise Mobility Management (EMM) se divide em Mobile Device Management (MDM) e Mobile Application Management (MAM). Enquanto o MDM permite que as organizações protejam e controlem dispositivos móveis, o MAM facilita a entrega e o gerenciamento de aplicativos. Com a crescente adoção do BYOD, você pode tipicamente implementar uma solução MAM para auxiliar na entrega de aplicativos, licenciamento de software, configuração e gerenciamento do ciclo de vida do aplicativo.

Com o XenMobile, você pode ir um passo além para proteger esses aplicativos configurando políticas MAM específicas e configurações de VPN para evitar vazamento de dados e outras ameaças de segurança. O XenMobile oferece às organizações a flexibilidade para implantar qualquer uma das seguintes soluções:

- Ambiente somente MAM
- Ambiente somente MDM
- Ambiente XenMobile Enterprise Unificado que oferece funcionalidade MDM e MAM na mesma plataforma

Além da capacidade de entregar aplicativos a dispositivos móveis, o XenMobile oferece a conteinerização de aplicativos por meio da tecnologia MDX. O MDX protege os aplicativos por meio de criptografia que é separada da criptografia em nível de dispositivo fornecida pela plataforma. Você pode apagar ou bloquear o aplicativo, e os aplicativos estão sujeitos a controles granulares baseados em políticas. Fornecedores de software independentes (ISVs) podem aplicar esses controles usando o Mobile Apps SDK.

Em um ambiente corporativo, os usuários utilizam vários aplicativos móveis para auxiliar em suas funções de trabalho. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente e aplicativos nativos. O XenMobile categoriza esses aplicativos da seguinte forma:

Aplicativos públicos: Esses aplicativos incluem aplicativos gratuitos ou pagos disponíveis em uma loja de aplicativos pública, como a Apple App Store ou o Google Play. Fornecedores externos à organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Essa opção permite que seus clientes baixem os aplicativos diretamente da Internet. Você pode usar vários aplicativos públicos em sua organização, dependendo das necessidades dos usuários. Exemplos de tais aplicativos incluem GoToMeeting, Salesforce e aplicativos EpicCare.

A Citrix não oferece suporte para download de binários de aplicativos diretamente de lojas de aplicativos públicas e, em seguida, empacotá-los com o MDX Toolkit para distribuição corporativa.

Para habilitar aplicativos de terceiros para MDX, entre em contato com o fornecedor do aplicativo para obter os binários do aplicativo. Você pode empacotar os binários usando o MDX Toolkit ou integrar o MAM SDK com os binários.

Aplicativos internos: Muitas organizações têm desenvolvedores internos que criam aplicativos que fornecem funcionalidades específicas e são desenvolvidos e distribuídos independentemente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos fornecidos por ISVs. Você pode implantar esses aplicativos como aplicativos nativos ou pode conteinerizar os aplicativos usando uma solução MAM, como o XenMobile. Por exemplo, uma organização de saúde pode criar um aplicativo interno que permite aos médicos visualizar informações de pacientes em dispositivos móveis. Uma organização pode então habilitar o aplicativo com o MAM SDK ou empacotá-lo com MDM para proteger as informações do paciente e habilitar o acesso VPN ao servidor de banco de dados de pacientes de back-end.

Aplicativos Web e SaaS: Esses aplicativos incluem aplicativos acessados de uma rede interna (aplicativos Web) ou de uma rede pública (SaaS). O XenMobile também permite que você crie aplicativos Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) para aplicativos Web existentes. Para obter detalhes, consulte Tipos de conectores de aplicativos. Por exemplo, você pode usar o Google Apps SAML para SSO baseado em Security Assertion Markup Language (SAML) para o Google Apps.

Aplicativos de produtividade móvel: Aplicativos desenvolvidos pela Citrix que estão incluídos na licença do XenMobile. Para obter detalhes, consulte Sobre aplicativos de produtividade móvel. A Citrix também oferece outros aplicativos prontos para negócios que os ISVs desenvolvem usando o Mobile Apps SDK.

Aplicativos HDX: Aplicativos hospedados no Windows que você publica com o StoreFront. Se você tiver um ambiente Citrix Virtual Apps and Desktops™, poderá integrar os aplicativos ao XenMobile para disponibilizá-los aos usuários inscritos.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração e a arquitetura subjacentes diferem. Por exemplo, se vários grupos de usuários com diferentes níveis de permissão consomem um único aplicativo, você pode precisar de grupos de entrega separados para implantar duas versões do aplicativo. Além disso, você deve garantir que a associação ao grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos do usuário.

Você também pode querer gerenciar o licenciamento de aplicativos iOS usando a compra por volume da Apple. Esta opção exige que você se registre para a compra por volume da Apple e configure as configurações de compra por volume do XenMobile no console do XenMobile para distribuir os aplicativos com as licenças de compra por volume. Vários casos de uso como esses tornam importante avaliar e planejar sua estratégia de MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia de MAM definindo o seguinte:

Tipos de aplicativos: Liste os diferentes tipos de aplicativos que você planeja suportar e, em seguida, categorize-os. Por exemplo: aplicativos públicos, nativos, de produtividade móvel, Web, internos, aplicativos ISV e assim por diante. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajuda você a alinhar as configurações do XenMobile que são necessárias para cada tipo de aplicativo. Por exemplo, certos aplicativos podem não se qualificar para empacotamento ou podem exigir o Mobile Apps SDK para habilitar APIs especiais para interação com outros aplicativos.

Requisitos de rede: Configure aplicativos com requisitos específicos de acesso à rede com as configurações apropriadas. Por exemplo, certos aplicativos podem precisar de acesso à sua rede interna por meio de uma VPN. Alguns aplicativos podem exigir acesso à Internet para rotear o acesso via DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você deve configurar várias configurações de acordo. A definição dos requisitos de rede por aplicativo ajuda a finalizar suas decisões arquitetônicas precocemente, o que simplifica o processo geral de implementação.

Requisitos de segurança: É fundamental definir os requisitos de segurança que se aplicam a aplicativos individuais ou a todos os aplicativos. Esse planejamento garante que você crie as configurações corretas ao instalar o XenMobile Server. Embora configurações como as políticas MDX se apliquem a aplicativos individuais, as configurações de sessão e autenticação se aplicam a todos os aplicativos. Alguns aplicativos podem ter requisitos específicos de criptografia, conteinerização, empacotamento, autenticação, geofencing, senha ou compartilhamento de dados que você pode descrever antecipadamente para simplificar sua implantação.

Requisitos de implantação: Você pode querer usar uma implantação baseada em políticas para permitir que apenas usuários compatíveis baixem os aplicativos publicados. Por exemplo, você pode querer que certos aplicativos exijam qualquer um dos seguintes:

- a criptografia baseada na plataforma do dispositivo está habilitada
- o dispositivo é gerenciado
- o dispositivo atende a uma versão mínima do sistema operacional
- certos aplicativos estão disponíveis apenas para usuários corporativos

Você também pode querer que certos aplicativos estejam disponíveis apenas para usuários corporativos. Descreva esses requisitos com antecedência para que você possa configurar as regras ou ações de implantação apropriadas.

Requisitos de licenciamento: Mantenha um registro dos requisitos de licenciamento relacionados a aplicativos. Essas anotações ajudam você a gerenciar o uso de licenças de forma eficaz e a decidir se deve configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo iOS gratuito ou pago, a Apple impõe requisitos de licenciamento ao aplicativo, exigindo que os usuários façam login em sua conta do iTunes. Você pode se registrar para a compra por volume da Apple para distribuir e gerenciar esses aplicativos via XenMobile. A compra por volume permite que os usuários baixem os aplicativos sem precisar fazer login em sua conta do iTunes. Além disso, ferramentas como Samsung SAFE e Samsung Knox têm requisitos de licenciamento especiais, que você precisa concluir antes de implantar esses recursos.

Requisitos de lista de permissões e lista de bloqueios: Você provavelmente deseja impedir que os usuários instalem ou usem alguns aplicativos. Crie uma lista de permissões de aplicativos que tornam um dispositivo não compatível. Em seguida, configure políticas para serem acionadas quando um dispositivo se tornar não compatível. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode cair na lista de bloqueios por algum motivo. Nesse caso, você pode adicionar o aplicativo a uma lista de permissões e indicar que o aplicativo é aceitável para uso, mas não é obrigatório. Além disso, lembre-se de que os aplicativos pré-instalados em novos dispositivos podem incluir alguns aplicativos comumente usados que não fazem parte do sistema operacional. Esses aplicativos podem entrar em conflito com sua estratégia de lista de bloqueios.

Caso de uso de aplicativos

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Os aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

- **Aplicativos de produtividade móvel:** Aplicativos iOS e Android fornecidos pela Citrix.
- **Secure Mail:** Aplicativo de e-mail, calendário e contatos.
- **Secure Web:** Navegador web seguro que fornece acesso à Internet e a sites de intranet.
- **Citrix Files:** Aplicativo para acessar dados compartilhados e para compartilhar, sincronizar e editar arquivos.

LOJA DE APLICATIVOS PÚBLICA

- **Secure Hub:** Cliente usado por todos os dispositivos móveis para se comunicar com o XenMobile. A TI envia configurações de segurança, configurações e aplicativos móveis para dispositivos móveis por meio do cliente Secure Hub. Dispositivos Android e iOS se registram no XenMobile por meio do Secure Hub.
- **Citrix Receiver™:** Aplicativo móvel que permite aos usuários abrir aplicativos hospedados por Virtual Apps and Desktops em dispositivos móveis.
- **GoToMeeting:** Um cliente de reunião online, compartilhamento de desktop e videoconferência que permite aos usuários se reunir com outros usuários de computador, clientes ou colegas via Internet em tempo real.
- **Salesforce1:** O Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúne todos os Chatter, CRM, aplicativos personalizados e processos de negócios em uma experiência unificada para qualquer usuário do Salesforce.
- **RSA SecurID:** Token baseado em software para autenticação de dois fatores.
- **Aplicativos EpicCare:** Esses aplicativos fornecem aos profissionais de saúde acesso seguro e portátil a prontuários de pacientes, listas de pacientes, agendamentos e mensagens.
    - **Haiku:** Aplicativo móvel para iPhone e telefones Android.
    - **Canto:** Aplicativo móvel para iPad
    - **Rover:** Aplicativos móveis para iPhone e iPad.

HDX: Esses aplicativos são entregues via Citrix Virtual Apps™ e Desktops.

- **Epic Hyperspace:** Aplicativo cliente Epic para gerenciamento de prontuários eletrônicos de saúde.

ISV

- **Vocera:** Aplicativo móvel de voz sobre IP e mensagens compatível com HIPAA que estende os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, via smartphones iPhone e Android.

APLICATIVOS INTERNOS

- **HCMail:** Aplicativo que ajuda a compor mensagens criptografadas, pesquisar catálogos de endereços em servidores de e-mail internos e enviar as mensagens criptografadas para os contatos usando um cliente de e-mail.

APLICATIVOS WEB INTERNOS

- **PatientRounding:** Aplicativo web usado para registrar informações de saúde do paciente por diferentes departamentos.
- **Outlook Web Access:** Permite o acesso a e-mails via navegador web.
- **SharePoint:** Usado para compartilhamento de arquivos e dados em toda a organização.

A tabela a seguir lista as informações básicas necessárias para a configuração do MAM.

Nome do Aplicativo	Tipo de Aplicativo	Empacotamento MDX	iOS	Android
Secure Mail	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Web	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim
Citrix Files	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo Público	NA	Sim	Sim
Citrix Receiver	Aplicativo Público	NA	Sim	Sim
GoToMeeting	Aplicativo Público	ND	Sim	Sim
Salesforce1	Aplicativo Público	ND	Sim	Sim
RSA SecurID	Aplicativo Público	ND	Sim	Sim
Epic Haiku	Aplicativo Público	NA	Sim	Sim

Epic Canto	Aplicativo Público	NA	Sim	Não
Epic Rover	Aplicativo Público	NA	Sim	Não
Epic Hyperspace	Aplicativo HDX™	NA	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo Interno	Sim	Sim	Sim
PatientRounding	Aplicativo Web	NA	Sim	Sim
Outlook Web Access	Aplicativo Web	NA	Sim	Sim
SharePoint	Aplicativo Web	NA	Sim	Sim

As tabelas a seguir listam requisitos específicos que você pode consultar ao configurar políticas MAM no XenMobile.

NOME DO APLICATIVO	VPN NECESSÁRIA	INTERAÇÃO (COM APLICATIVOS FORA DO CONTÊINER)	INTERAÇÃO (DE APLICATIVOS FORA DO CONTÊINER)	CRIPTOGRAFIA BASEADA NA PLATAFORMA DO DISPOSITIVO
Secure Mail	S	Permitido Seletivamente	Permitido	Não necessário
Secure Web	S	Permitido	Permitido	Não necessário

NOME DO APLICATIVO	VPN NECESSÁRIA	INTERAÇÃO (COM APLICATIVOS FORA DO CONTÊINER)	INTERAÇÃO (DE APLICATIVOS FORA DO CONTÊINER)	CRIPTOGRAFIA BASEADA NA PLATAFORMA DO DISPOSITIVO
Citrix Files	S	Permitido	Permitido	Não necessário
Secure Hub	S	N/A	N/A	N/A
Citrix Receiver	S	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
Salesforce1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	S	N/A	N/A	N/A
Epic Canto	S	N/A	N/A	N/A
Epic Rover	S	N/A	N/A	N/A
Epic Hyperspace	S	N/A	N/A	N/A
Vocera	S	Bloqueado	Bloqueado	Não necessário
HCMail	S	Bloqueado	Bloqueado	Obrigatório
PatientRounding	S	N/A	N/A	Obrigatório
Outlook Web Access	S	N/A	N/A	Não obrigatório
SharePoint	S	N/A	N/A	Não necessário

NOME DO APLICATIVO	FILTRAGEM DE PROXY	LICENCIAMENTO	CERCAMENTO GEOGRÁFICO	SDK DE APLICATIVOS MÓVEIS	VERSÃO MÍNIMA DO SISTEMA OPERACIONAL
Secure Mail	Necessário	N/A	Necessário Seletivamente	N/A	Imposto
Secure Web	Obrigatório	N/A	Não obrigatório	N/A	Imposto
Citrix Files	Obrigatório	N/A	Não obrigatório	N/A	Imposto
Secure Hub	Não obrigatório	Compra por volume	Não necessário	N/A	Não imposto
Citrix Receiver	Não necessário	Compra em volume	Não necessário	N/A	Não imposto
GoToMeeting	Não necessário	Compra em volume	Não necessário	N/A	Não imposto
Salesforce1	Não necessário	Compra por volume	Não necessário	N/A	Não aplicado
RSA SecurID	Não necessário	Compra por volume	Não necessário	N/A	Não aplicado
Epic Haiku	Não necessário	Compra por volume	Não obrigatório	N/A	Não imposto
Epic Canto	Não obrigatório	Compra em volume	Não obrigatório	N/A	Não imposto
Epic Rover	Não obrigatório	Compra em volume	Não obrigatório	N/A	Não imposto
Epic Hyperspace	Não obrigatório	N/A	Não obrigatório	N/A	Não imposto
Vocera	Obrigatório	N/A	Obrigatório	Obrigatório	Imposto

NOME DO APLICATIVO	FILTRAGEM DE PROXY	LICENCIAMENTO	CERCAMENTO GEOGRÁFICO	SDK DE APLICATIVOS MÓVEIS	VERSÃO MÍNIMA DO SISTEMA OPERACIONAL
HCMail	Obrigatório	N/A	Obrigatório	Obrigatório	Imposto
PatientRound-ing	Obrigatório	N/A	Não obrigatório	N/A	Não imposto
Outlook Web Access	Obrigatório	N/A	Não obrigatório	N/A	Não imposto
SharePoint	Obrigatório	N/A	Não obrigatório	N/A	Não aplicado

Comunidades de Usuários

Toda organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários executam diferentes tarefas e funções de escritório usando vários recursos que você fornece por meio dos dispositivos móveis dos usuários. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis que você fornece. Ou, os usuários podem usar seus dispositivos móveis pessoais, o que lhes permite acessar ferramentas que estão sujeitas a certas regras de conformidade de segurança.

À medida que mais comunidades de usuários utilizam dispositivos móveis, o Gerenciamento de Mobilidade Empresarial (EMM) torna-se crítico para prevenir vazamentos de dados e impor restrições de segurança. Para um gerenciamento de dispositivos móveis eficiente e mais sofisticado, você pode categorizar suas comunidades de usuários. Isso simplifica o mapeamento de usuários para recursos e garante que as políticas de segurança corretas sejam aplicadas aos usuários certos.

O exemplo a seguir ilustra como as comunidades de usuários de uma organização de saúde são classificadas para EMM.

Caso de uso de comunidades de usuários

Esta organização de saúde de exemplo fornece recursos tecnológicos e acesso a múltiplos usuários, incluindo funcionários da rede e afiliados, e voluntários. A organização optou por implementar a solução EMM apenas para usuários não executivos.

As funções e papéis dos usuários para esta organização podem ser divididos em subgrupos, incluindo: clínicos, não clínicos e contratados. Um conjunto selecionado de usuários recebe dispositivos móveis corporativos, enquanto outros podem acessar recursos limitados da empresa a partir de seus dispositivos pessoais. Para impor o nível certo de restrições de segurança e prevenir vazamentos de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado, seja ele emitido pela empresa ou BYOD. Além disso, os usuários podem registrar apenas um único dispositivo.

A seção a seguir fornece uma visão geral dos papéis e funções de cada subgrupo:

CLÍNICO

- Enfermeiros
- Médicos (Clínicos, Cirurgiões e assim por diante)
- Especialistas (Nutricionistas, anestesiologistas, radiologistas, cardiologistas, oncologistas e assim por diante)
- Médicos externos (Médicos não-funcionários e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (Trabalhadores de escritório e móveis que prestam serviços médicos para visitas domiciliares a pacientes)
- Especialista em Pesquisa (Trabalhadores do Conhecimento e Usuários Avançados em seis Institutos de Pesquisa realizando pesquisa clínica para encontrar respostas para questões na medicina)
- Educação e Treinamento (Enfermeiros, médicos e especialistas em educação e treinamento)

NÃO CLÍNICO

- Serviços Compartilhados (Trabalhadores de escritório que executam várias funções de back office, incluindo: RH, Folha de Pagamento, Contas a Pagar, Serviço de Cadeia de Suprimentos e assim por diante)
- Serviços Médicos (Trabalhadores de escritório que executam várias soluções de gestão de saúde, serviços administrativos e processos de negócios para provedores, incluindo: Serviços Administrativos, Análise e Inteligência de Negócios, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e assim por diante)
- Serviços de Suporte (Trabalhadores de escritório que executam várias funções não clínicas, incluindo: Administração de Benefícios, Integração Clínica, Comunicações, Gestão de Remuneração e Desempenho, Serviços de Instalações e Propriedades, Sistemas de

Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos, e assim por diante.)

- Programas Filantrópicos (Trabalhadores de escritório e móveis que executam várias funções em apoio a programas filantrópicos)

CONTRATADOS

- Parceiros fabricantes e fornecedores (No local e conectados remotamente via VPN site-a-site, fornecendo várias funções de suporte não clínico)

Com base nas informações precedentes, a organização criou as seguintes entidades. Para obter mais informações sobre grupos de entrega no XenMobile, consulte Implantar recursos.

UNIDADES ORGANIZACIONAIS (OUS) E GRUPOS DO ACTIVE DIRECTORY

Para OU **=** Recursos do XenMobile:

- OU = Clínico; Grupos =
  - XM-Enfermeiros
  - XM-Médicos
  - XM-Especialistas
  - XM-Médicos Externos
  - XM-Serviços de Saúde Domiciliar
  - XM-Especialista em Pesquisa
  - XM-Educação e Treinamento
- OU = Não Clínico; Grupos =
  - XM-Serviços Compartilhados
  - XM-Serviços Médicos
  - XM-Serviços de Suporte
  - XM-Programas Filantrópicos

USUÁRIOS E GRUPOS LOCAIS DO XENMOBILE

Para Grupo= Contratados, Usuários =

- Fornecedor1
- Fornecedor2
- Fornecedor 3

- … Fornecedor 10

GRUPOS DE ENTREGA DO XENMOBILE

- Clínico-Enfermeiros
- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos Externos
- Clínico-Serviços de Saúde Domiciliar
- Clínico-Especialista em Pesquisa
- Clínico-Educação e Treinamento
- Não Clínico-Serviços Compartilhados
- Serviços Não Clínicos - Médicos
- Serviços Não Clínicos - Suporte
- Programas Não Clínicos - Filantrópicos

MAPEAMENTO DE GRUPO DE ENTREGA E GRUPO DE USUÁRIOS

Grupos do Active Directory	**Grupos de Entrega do XenMobile**
XM-Enfermeiros	Clínico-Enfermeiros
XM-Médicos	Clínico-Médicos
XM-Especialistas	Clínico-Especialistas
XM-Médicos Externos	Clínico-Médicos Externos
XM-Serviços de Saúde Domiciliar	Clínico - Serviços de Saúde Domiciliar
XM-Especialista em Pesquisa	Clínico-Especialista em Pesquisa
XM-Educação e Treinamento	Clínico-Educação e Treinamento
XM-Serviços Compartilhados	Não Clínico-Serviços Compartilhados
XM-Serviços Médicos	Não Clínico-Serviços Médicos
XM-Serviços de Suporte	Não Clínico-Serviços de Suporte

XM-Programas Filantrópicos	Não Clínico-Programas Filantrópicos

MAPEAMENTO DE GRUPO DE ENTREGA E RECURSOS

As tabelas a seguir ilustram os recursos atribuídos a cada grupo de entrega neste caso de uso. A primeira tabela mostra as atribuições de aplicativos móveis. A segunda tabela mostra os aplicativos públicos, aplicativos HDX e recursos de gerenciamento de dispositivos.

Grupos de Entrega do XenMobile	**Aplicativos Móveis Citrix**	**Aplicativos Móveis Públicos**	**Aplicativos Móveis HDX**
Clínico-Enfermeiros	X		
Clínico-Médicos			
Clínico-Especialistas			
Clínico-Médicos Externos	X		
Clínico-Serviços de Saúde Domiciliar	X		
Clínico-Especialista em Pesquisa	X		
Clínico-Educação e Treinamento		X	X
Serviços Compartilhados Não Clínicos		X	X
Serviços Médicos Não Clínicos		X	X
Serviços de Suporte Não Clínicos	X	X	X

Programas Filantrópicos Não Clínicos	X	X	X
Contratados	X	X	X

Grupos de Entrega do XenMobile	**Aplicativo Público: RSA SecurID**	**Aplicativo Público: EpicCare Haiku**	**Aplicativo HDX: Epic Hyperspace**	**Política de Senha**	**Restrições de Dispositivo**	**Ações Automatizadas**	**Política de Wi-Fi**
Enfermeiros Clínicos							X
Clínico-Médicos					X		
Clínico-Especialistas							
Clínico-Médicos Externos							
Clínico-Serviços de Saúde Domiciliar							
Clínico-Especialista em							

Pesquisa							
Clínico-Educação e Treinamento		X	X				
Não Clínico-Serviços Compartilhados		X	X				
Não Clínico-Serviços Médicos		X	X				
Serviços de Suporte Não Clínico		X	X				

NOTAS E CONSIDERAÇÕES

- O XenMobile cria um grupo de entrega padrão chamado Todos os Usuários durante a configuração inicial. Se você não desativar este Grupo de Entrega, todos os usuários do Active Directory terão o direito de se inscrever no XenMobile.
- O XenMobile sincroniza usuários e grupos do Active Directory sob demanda usando uma conexão dinâmica com o servidor LDAP.
- Se um usuário fizer parte de um grupo que não está mapeado no XenMobile, esse usuário não poderá se inscrever. Da mesma forma, se um usuário for membro de vários grupos, o XenMobile categoriza o usuário como estando apenas nos grupos mapeados para o XenMobile.

- Para tornar a inscrição MDM obrigatória, você deve definir a opção Inscrição Obrigatória como Verdadeiro nas Propriedades do Servidor no console do XenMobile. Para obter detalhes, consulte Propriedades do Servidor.
- Você pode excluir um grupo de usuários de um grupo de entrega do XenMobile excluindo a entrada no banco de dados do SQL Server, em dbo.userlistgrps. **Cuidado:** Antes de executar esta ação, crie um backup do XenMobile e do banco de dados.

Sobre a Propriedade do Dispositivo no XenMobile

Você pode agrupar usuários de acordo com o proprietário do dispositivo de um usuário. A propriedade do dispositivo inclui dispositivos de propriedade corporativa e dispositivos de propriedade do usuário, também conhecidos como traga seu próprio dispositivo (BYOD). Você pode controlar como os dispositivos BYOD se conectam à sua rede em dois locais no console do XenMobile: nas regras de implantação para cada tipo de recurso e através das propriedades do servidor na página **Configurações**. Para obter detalhes sobre as regras de implantação, consulte Configurando Regras de Implantação na documentação do XenMobile. Para obter detalhes sobre as propriedades do servidor, consulte Propriedades do Servidor.

Você pode exigir que todos os usuários BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que possam acessar os aplicativos. Ou, você pode dar aos usuários acesso a aplicativos corporativos sem também gerenciar seus dispositivos.

Quando você define a configuração do servidor **wsapi.mdm.required.flag** como **true**, o XenMobile gerencia todos os dispositivos BYOD, e qualquer usuário que recusar a inscrição terá o acesso aos aplicativos negado. Considere definir **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança, juntamente com uma experiência de usuário positiva ao inscrever dispositivos de usuário no XenMobile.

Se você deixar **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários podem recusar a inscrição, mas ainda podem acessar os aplicativos em seus dispositivos através da XenMobile Store. Considere definir **wsapi.mdm.required.flag** como **false** em ambientes nos quais restrições de privacidade, legais ou regulatórias exigem nenhum gerenciamento de dispositivo, apenas gerenciamento de aplicativos corporativos.

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da XenMobile Store. Em vez de controles no nível do dispositivo, como limpeza seletiva ou completa, você controla o acesso aos aplicativos por meio de políticas de aplicativos. As políticas, dependendo dos valores que você definir, exigem que o dispositivo verifique o XenMobile Server rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Requisitos de Segurança

O número de considerações de segurança ao implantar um ambiente XenMobile pode rapidamente se tornar esmagador. Existem muitas peças e configurações interligadas. Para ajudar você a começar e escolher um nível aceitável de proteção, a Citrix fornece recomendações para Segurança Alta, Mais Alta e Mais Elevada, conforme descrito na tabela a seguir.

Sua escolha do modo de implantação envolve mais do que apenas preocupações de segurança. É importante também revisar os requisitos do caso de uso e decidir se você pode mitigar as preocupações de segurança antes de escolher seu modo de implantação.

Alta: O uso dessas configurações proporciona uma experiência de usuário ideal, mantendo um nível básico de segurança aceitável para a maioria das organizações.

Mais Alta: Essas configurações criam um equilíbrio mais forte entre segurança e usabilidade.

Mais Elevada: Seguir essas recomendações proporciona um alto nível de segurança, ao custo da usabilidade e da adoção pelo usuário.

Considerações de segurança do modo de implantação

A tabela a seguir especifica os modos de implantação para cada nível de segurança.

Segurança Alta	**Segurança Mais Alta**	**Segurança Mais Elevada**
MAM ou MDM	MDM+MAM	MDM+MAM; mais FIPS

Observações:

- Dependendo do caso de uso, uma implantação somente MDM ou somente MAM pode atender aos requisitos de segurança e proporcionar uma boa experiência ao usuário.
- Se você não precisa de conteinerização de aplicativos, micro VPN ou políticas específicas de aplicativos, o MDM é suficiente para gerenciar e proteger dispositivos.
- Para casos de uso como BYOD, nos quais a conteinerização de aplicativos por si só pode satisfazer todos os requisitos de negócios e segurança, a Citrix recomenda o modo somente MAM.
- Para ambientes de alta segurança (e dispositivos corporativos), a Citrix recomenda MDM+MAM para aproveitar todas as capacidades de segurança disponíveis. Certifique-se de impor o registro MDM.

- Opções FIPS para ambientes com as mais altas necessidades de segurança, como o governo federal.

Se você habilitar o modo FIPS, você deve configurar o SQL Server para criptografar o tráfego SQL.

Considerações de segurança do Citrix ADC e Citrix Gateway

A tabela a seguir especifica as recomendações do Citrix ADC e Citrix Gateway para cada nível de segurança.

Alta Segurança	**Segurança Mais Alta**	**Segurança Máxima**
O Citrix ADC é recomendado. O Citrix Gateway é necessário para MAM e ENT; recomendado para MDM	Citrix ADC padrão para configuração do assistente XenMobile com ponte SSL se o XenMobile estiver na DMZ. Ou descarregamento SSL, se necessário para atender aos padrões de segurança quando o XenMobile Server estiver na rede interna.	Descarregamento SSL com criptografia de ponta a ponta

Observações:

- Expor o XenMobile Server à Internet através de NAT ou de proxies e balanceadores de carga de terceiros existentes pode ser uma opção para MDM. No entanto, essa configuração exige que o tráfego SSL termine no XenMobile Server, o que representa um risco potencial de segurança.
- Para ambientes de alta segurança, o Citrix ADC com a configuração padrão do XenMobile geralmente atende ou excede os requisitos de segurança.
- Para ambientes MDM com as mais altas necessidades de segurança, a terminação SSL no Citrix ADC permite a inspeção de tráfego no perímetro e mantém a criptografia SSL de ponta a ponta.
- Opções para definir cifras SSL/TLS.
- O hardware SSL FIPS Citrix ADC também está disponível.
- Para obter mais informações, consulte Integração com Citrix Gateway e Citrix ADC.

Considerações de segurança de registro

A tabela a seguir especifica as recomendações do Citrix ADC e do Citrix Gateway para cada nível de segurança.

Alta Segurança	**Segurança Mais Alta**	**Segurança Máxima**
Somente associação a Grupo do Active Directory. Grupo de Entrega de Todos os Usuários desativado.	Modo de segurança de registro somente por convite. Somente associação a Grupo do Active Directory. Grupo de Entrega de Todos os Usuários desativado	Modo de segurança de registro vinculado ao ID do Dispositivo. Somente associação a Grupo do Active Directory. Grupo de Entrega de Todos os Usuários desativado

Observações:

- A Citrix geralmente recomenda que você restrinja o registro apenas a usuários em grupos predefinidos do Active Directory. Essa configuração exige a desativação do Grupo de Entrega Todos os usuários integrado.
- Você pode usar convites de registro para restringir o registro a usuários com um convite. Os convites de registro não estão disponíveis para dispositivos Windows.
- Você pode usar convites de registro de PIN único (OTP) como uma solução de autenticação de dois fatores e para controlar o número de dispositivos que um usuário pode registrar. Os convites OTP não estão disponíveis para dispositivos Windows.

Considerações de segurança do código de acesso do dispositivo

A tabela a seguir especifica as recomendações de código de acesso do dispositivo para cada nível de segurança.

Segurança Alta	**Segurança Mais Alta**	**Segurança Mais Elevada**
Recomendado. A segurança alta é necessária para a criptografia em nível de dispositivo. Imposto usando MDM. Você pode definir a segurança alta como obrigatória apenas para MAM	Imposto usando MDM, uma política MDX ou ambos.	Imposto usando MDM e política MDX. Política de código de acesso complexo do MDM.

usando a política MDX, Comportamento de dispositivo não compatível.		

Observações:

- A Citrix recomenda o uso de um código de acesso do dispositivo.
- Você pode impor um código de acesso do dispositivo por meio de uma política MDM.
- Você pode usar uma política MDX para tornar um código de acesso do dispositivo um requisito para usar aplicativos gerenciados. Por exemplo, para casos de uso BYOD.
- A Citrix recomenda combinar as opções de política MDM e MDX para aumentar a segurança em ambientes MDM+MAM.
- Para ambientes com os mais altos requisitos de segurança, você pode configurar políticas de senha complexas e aplicá-las com MDM. Você pode configurar ações automáticas para notificar administradores ou emitir limpezas seletivas/completas do dispositivo quando um dispositivo não estiver em conformidade com uma política de senha.

Aplicativos

O Enterprise Mobility Management (EMM) divide-se em Mobile Device Management (MDM) e Mobile Application Management (MAM). Enquanto o MDM permite que as organizações protejam e controlem dispositivos móveis, o MAM facilita a entrega e o gerenciamento de aplicativos. Para apoiar a adoção de BYOD, você pode tipicamente implementar uma solução MAM, como o XenMobile®, para auxiliar com o seguinte:

- entrega de aplicativos
- licenciamento de software
- configuração
- gerenciamento do ciclo de vida do aplicativo

Você pode exigir ou permitir que os usuários também optem pelo gerenciamento de MDM.

Com o XenMobile, você pode ir um passo além para proteger esses aplicativos configurando políticas MAM e configurações de VPN específicas para evitar vazamentos de dados e outras ameaças de segurança. O XenMobile fornece às organizações a flexibilidade para implantar sua solução como um(a):

- ambiente somente MAM

- ambiente somente MDM
- ambiente XenMobile Enterprise Unificado que oferece funcionalidade MDM e MAM

Além da capacidade de entregar aplicativos para dispositivos móveis, o XenMobile oferece a conteinerização de aplicativos por meio da tecnologia MDX. Os aplicativos estão sujeitos a controles granulares baseados em políticas. Fornecedores de software independentes (ISVs) podem aplicar esses controles usando o SDK de Aplicativos Móveis.

Em um ambiente corporativo, os usuários usam vários aplicativos móveis para auxiliar em sua função de trabalho. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente ou aplicativos nativos. O XenMobile categoriza esses aplicativos da seguinte forma:

- **Aplicativos públicos:** Esses aplicativos incluem aplicativos gratuitos ou pagos disponíveis em uma loja de aplicativos pública, como a Apple App Store ou o Google Play. Fornecedores externos à organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Essa opção permite que seus clientes baixem os aplicativos diretamente da Internet. Você pode usar vários aplicativos públicos em sua organização, dependendo das necessidades dos usuários. Exemplos desses aplicativos incluem GoToMeeting, Salesforce e aplicativos EpicCare.
    - **Se você usa o SDK MAM:** Obtenha os binários do aplicativo do seu fornecedor de aplicativos. Em seguida, integre o SDK MAM ao aplicativo.
    - **Se você usa o MDX Toolkit:** A Citrix® não oferece suporte ao download de binários de aplicativos diretamente de lojas de aplicativos públicas e, em seguida, ao empacotamento deles com o MDX Toolkit para distribuição corporativa. Para empacotar aplicativos de terceiros, trabalhe com o fornecedor do aplicativo para obter os binários do aplicativo. Você pode então empacotar os binários usando o MDX Toolkit.
- **Aplicativos internos:** Muitas organizações têm desenvolvedores internos que criam aplicativos que fornecem funcionalidades específicas e são desenvolvidos e distribuídos independentemente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos fornecidos por ISVs. Você pode implantar esses aplicativos como aplicativos nativos ou pode conteinerizar os aplicativos usando uma solução MAM, como o XenMobile.

  Por exemplo, uma organização de saúde pode criar um aplicativo interno que permite aos médicos visualizar informações de pacientes em dispositivos móveis. Uma organização pode

então proteger as informações do paciente e habilitar o acesso VPN ao banco de dados do paciente usando um dos seguintes:

  - MAM SDK
  - MDX Toolkit

- **Aplicativos Web e SaaS:** Esses aplicativos incluem aplicativos acessados de uma rede interna (aplicativos Web) ou por uma rede pública (SaaS). O XenMobile também permite criar aplicativos Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) para aplicativos Web existentes. Para obter detalhes, consulte (/pt-br/xenmobile/server/apps/app-connector-types.html). Por exemplo, você pode usar o Google Apps SAML para SSO baseado em Security Assertion Markup Language (SAML) para o Google Apps.
- **Aplicativos de produtividade móvel:** Os aplicativos de produtividade móvel são aplicativos desenvolvidos pela Citrix que estão incluídos na licença do XenMobile. Para obter detalhes, consulte Sobre aplicativos de produtividade móvel. A Citrix também oferece outros aplicativos prontos para negócios que os ISVs desenvolvem usando o Mobile Apps SDK.
- **Aplicativos HDX:** Os aplicativos HDX são aplicativos hospedados no Windows que você publica com o StoreFront. Se você usa o Citrix Virtual Apps and Desktops™ e o Citrix Workspace™, os aplicativos HDX estão disponíveis para usuários inscritos.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração subjacente pode diferir. Por exemplo, vários grupos de usuários com diferentes níveis de permissões podem consumir um único aplicativo. Nesse caso, você pode criar grupos de entrega separados para implantar duas versões separadas do mesmo aplicativo. Além disso, você deve garantir que a associação ao grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos dos usuários.

Você também pode gerenciar o licenciamento de aplicativos iOS usando a compra por volume da Apple. Esta opção exige que você se registre no programa de compra por volume e configure as configurações de compra por volume no console do XenMobile. Essa configuração permite distribuir os aplicativos com as licenças de compra por volume. Vários casos de uso tornam importante avaliar e planejar sua estratégia de MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia de MAM definindo o seguinte:

- **Tipos de aplicativos:** Liste os diferentes tipos de aplicativos que você planeja suportar e categorize-os, como aplicativos públicos, nativos, Web, internos ou ISV. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajuda a alinhar as várias configurações do XenMobile que são necessárias para

cada tipo de aplicativo. Por exemplo, alguns aplicativos podem exigir o uso do Mobile Apps SDK para habilitar APIs especiais para interação com outros aplicativos.

- **Requisitos de rede:** Configure as configurações de aplicativos que possuem requisitos específicos de acesso à rede. Por exemplo, certos aplicativos podem precisar de acesso à sua rede interna por meio da VPN. Alguns aplicativos podem exigir acesso à Internet para rotear o acesso via DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você deve configurar várias configurações de acordo. A definição de requisitos de rede por aplicativo ajuda a finalizar suas decisões arquitetônicas desde o início, o que simplifica o processo geral de implementação.
- **Requisitos de segurança:** Você pode definir requisitos de segurança para aplicar a aplicativos individuais ou a todos os aplicativos.
    - Configurações, como as políticas MDX, aplicam-se a aplicativos individuais
    - As configurações de sessão e autenticação aplicam-se a todos os aplicativos
    - Alguns aplicativos podem ter requisitos específicos de conteinerização, MDX, autenticação, geofencing, senha ou compartilhamento de dados

  Delineie esses requisitos com antecedência para simplificar sua implantação. Para obter detalhes sobre segurança no Endpoint Management, consulte Segurança e Experiência do Usuário.
- **Requisitos de implantação** - Você pode querer usar uma implantação baseada em políticas para permitir que apenas usuários compatíveis baixem os aplicativos publicados. Por exemplo, certos aplicativos podem exigir que o dispositivo seja gerenciado ou que o dispositivo atenda a uma versão mínima do sistema operacional. Você também pode querer que certos aplicativos estejam disponíveis apenas para usuários corporativos. Delineie esses requisitos com antecedência para que você possa configurar as regras ou ações de implantação apropriadas.
- **Requisitos de licenciamento:** Mantenha um registro dos requisitos de licenciamento relacionados ao aplicativo. Suas anotações podem ajudá-lo a gerenciar o uso da licença de forma eficaz e decidir se deve configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo iOS gratuito ou pago, a Apple impõe requisitos de licenciamento ao aplicativo. Como resultado, os usuários devem fazer login em sua conta da Apple App Store.

  No entanto, você pode se registrar para a compra por volume da Apple para distribuir e gerenciar esses aplicativos usando o XenMobile. A compra por volume permite que os usuários baixem os aplicativos sem precisar fazer login em sua conta da Apple App Store.

Algumas plataformas, como Samsung SAFE e Samsung Knox, têm requisitos especiais de licenciamento a serem concluídos antes de implantar esses recursos.

- **Requisitos de lista de permissões e lista de bloqueios:** Você pode identificar aplicativos que não deseja que os usuários instalem ou usem. A criação de uma lista de bloqueios define um evento de não conformidade. Você pode então configurar políticas para serem acionadas quando o evento ocorrer. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode cair na lista de bloqueios por algum motivo. Nesse caso, você pode adicionar o aplicativo a uma lista de permissões e indicar que o aplicativo é aceitável para uso, mas não é obrigatório. Além disso, lembre-se de que os aplicativos pré-instalados em novos dispositivos podem incluir alguns aplicativos comumente usados que não fazem parte do sistema operacional. Tais aplicativos podem entrar em conflito com sua estratégia de lista de bloqueios.

Caso de Uso

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Os aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

Aplicativos de produtividade móvel: Aplicativos iOS e Android fornecidos pela Citrix. Para obter detalhes, consulte aplicativos de produtividade móvel.

Citrix Secure Hub™: Cliente usado por todos os dispositivos móveis para se comunicar com o XenMobile. Você envia configurações de segurança, configurações e aplicativos móveis para dispositivos móveis usando o Secure Hub. Dispositivos Android e iOS se registram no XenMobile através do Secure Hub.

Citrix Receiver: Aplicativo móvel que permite aos usuários de dispositivos móveis abrir aplicativos hospedados pelo Citrix Virtual Apps.

GoToMeeting: Um cliente de reunião online, compartilhamento de desktop e videoconferência que permite aos usuários se reunir com outros usuários de computador, clientes ou colegas via Internet em tempo real.

SalesForce1: O Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúne todos os Chatter, CRM, aplicativos personalizados e processos de negócios em uma experiência unificada para qualquer usuário do Salesforce.

RSA SecurID: Token baseado em software para autenticação de dois fatores.

Aplicativos EpicCare: Esses aplicativos fornecem aos profissionais de saúde acesso seguro e portátil a prontuários de pacientes, listas de pacientes, agendamentos e mensagens.

Haiku: Aplicativo móvel para iPhone e telefones Android.

Canto: Aplicativo móvel para iPad

Rover: Aplicativos móveis para iPhone e iPad.

HDX™: O Citrix Virtual Apps entrega aplicativos HDX.

- **Epic Hyperspace:** Aplicativo cliente Epic para gerenciamento de prontuários eletrônicos de saúde.

ISV:

- **Vocera:** Aplicativo móvel de voz sobre IP e mensagens compatível com HIPAA que estende os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, via smartphones iPhone e Android.

Aplicativos internos:

- **HCMail:** Aplicativo que ajuda a compor mensagens criptografadas, pesquisar catálogos de endereços em servidores de e-mail internos e enviar as mensagens criptografadas para os contatos usando um cliente de e-mail.

Aplicativos web internos:

- **PatientRounding:** Aplicativo web usado para registrar informações de saúde do paciente por diferentes departamentos.
- **Outlook Web Access:** Permite o acesso a e-mails via navegador web.
- **SharePoint:** Usado para compartilhamento de arquivos e dados em toda a organização.

A tabela a seguir lista as informações básicas necessárias para a configuração do MAM.

Nome do Aplicativo	**Tipo de Aplicativo**	**Integração do SDK MAM ou Empacotamento MDX**	**iOS**	**Android**
Secure Mail	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim

Secure Web	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim
Citrix Files	Aplicativo XenMobile	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo Público	N/A	Sim	Sim
Citrix Receiver	Aplicativo Público	N/A	Sim	Sim
GoToMeeting	Aplicativo Público	N/A	Sim	Sim
SalesForce1	Aplicativo Público	N/A	Sim	Sim
RSA SecurID	Aplicativo Público	N/A	Sim	Sim
Epic Haiku	Aplicativo Público	N/A	Sim	Sim
Epic Canto	Aplicativo Público	N/A	Sim	Não
Epic Rover	Aplicativo Público	N/A	Sim	Não
Epic Hyperspace	Aplicativo HDX	N/A	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo Interno	Sim	Sim	Sim
PatientRounding	Aplicativo Web	N/A	Sim	Sim

Outlook Web Access	Aplicativo Web	N/A	Sim	Sim
SharePoint	Aplicativo Web	N/A	Sim	Sim

A tabela a seguir lista requisitos específicos que você pode consultar ao configurar políticas MAM no XenMobile.

NOME DO APLICATIVO	VPN NECESSÁRIA	INTERAÇÃO (COM APLICATIVOS FORA DO CONTÊINER)	INTERAÇÃO (DE APLICATIVOS FORA DO CONTÊINER)	FILTRAGEM DE PROXY	LICENCIAMENTO	CERCAMENTO GEOGRÁFICO	SDK DE APLICATIVOS MÓVEIS	VERSÃO MÍNIMA DO SISTEMA OPERACIONAL
Secure Mail	S	Permitido Seletivamente	Permitido	Obrigatório	N/A	Obrigatório Seletivamente	N/A	Imposto
Secure Web	S	Permitido	Permitido	Obrigatório	N/A	Não obrigatório	N/A	Imposto
Citrix Files	S	Permitido	Permitido	Obrigatório	N/A	Não obrigatório	N/A	Imposto
Secure Hub	S	N/A	N/A	Não obrigatório	Compra por volume	Não obrigatório	N/A	Não imposto
Citrix Receiver	S	N/A	N/A	Não necessário	Compra em	Não necessário	N/A	Não imposto

NOME DO APLICATIVO	VPN NECESSÁRIA	INTERAÇÃO (COM APLICATIVOS FORA DO CONTÊINER)	INTERAÇÃO (DE APLICATIVOS FORA DO CONTÊINER)	FILTRAGEM DE PROXY	LICENCIAMENTO	CERCAMENTO GEOGRÁFICO	SDK DE APLICATIVOS MÓVEIS	VERSÃO MÍNIMA DO SISTEMA OPERACIONAL
					volume			
GoTo Meeting	N	N/A	N/A	Não necessário	Compra por volume	Não obrigatório	N/A	Não imposto
Sales Force 1	N	N/A	N/A	Não obrigatório	Compra por volume	Não obrigatório	N/A	Não imposto
RSA SecurID	N	N/A	N/A	Não necessário	Compra por volume	Não necessário	N/A	Não aplicado
Epic Haiku	S	N/A	N/A	Não necessário	Compra por volume	Não necessário	N/A	Não imposto
Epic Canto	S	N/A	N/A	Não necessário	Compra por volume	Não necessário	N/A	Não imposto
Epic Rover	S	N/A	N/A	Não necessário	Compra por volume	Não obrigatório	N/A	Não imposto

NOME DO APLICATIVO	VPN NECESSÁRIA	INTERAÇÃO (COM APLICATIVOS FORA DO CONTÊINER)	INTERAÇÃO (DE APLICATIVOS FORA DO CONTÊINER)	FILTRAGEM DE PROXY	LICENCIAMENTO	CERCAMENTO GEOGRÁFICO	SDK DE APLICATIVOS MÓVEIS	VERSÃO MÍNIMA DO SISTEMA OPERACIONAL
Epic Hyperspace	S	N/A	N/A	Não obrigatório	N/A	Não obrigatório	N/A	Não imposto
Vocera	S	Bloqueado	Bloqueado	Obrigatório	N/A	Obrigatório	Obrigatório	Imposto
HCMail	S	Bloqueado	Bloqueado	Obrigatório	N/A	Obrigatório	Obrigatório	Imposto
Ronda de Pacientes	S	N/A	N/A	Obrigatório	N/A	Não obrigatório	N/A	Não imposto
Outlook Web Access	S	N/A	N/A	Obrigatório	N/A	Não necessário	N/A	Não aplicado
Share Point	S	N/A	N/A	Obrigatório	N/A	Não necessário	N/A	Não aplicado

Comunidades de Usuários

Toda organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários realizam diferentes tarefas e funções de escritório usando vários recursos que você fornece por meio de dispositivos móveis do usuário. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis que você fornece,

ou os usuários podem usar dispositivos móveis pessoais, o que lhes permite acessar ferramentas que estão sujeitas a certas regras de conformidade de segurança.

Com mais comunidades de usuários usando dispositivos móveis, o Enterprise Mobility Management (EMM) torna-se crítico para prevenir vazamentos de dados e para impor restrições de segurança organizacional. Para um gerenciamento de dispositivos móveis eficiente e mais sofisticado, você pode categorizar suas comunidades de usuários. Isso simplifica o mapeamento de usuários para recursos e garante que as políticas de segurança corretas se apliquem aos usuários certos.

A categorização de comunidades de usuários pode incluir o uso dos seguintes componentes:

- Unidades Organizacionais (OUs) e Grupos do Active Directory

  Usuários adicionados a grupos de segurança específicos do Active Directory podem receber políticas e recursos, como aplicativos. A remoção de usuários dos grupos de segurança do Active Directory remove o acesso aos recursos do XenMobile® previamente permitidos.
- Usuários e grupos locais do XenMobile

  Para usuários que não possuem uma conta no Active Directory, você pode criar os usuários como usuários locais do XenMobile. Você pode adicionar usuários locais a grupos de entrega e provisionar recursos para eles da mesma forma que os usuários do Active Directory.
- Grupos de entrega do XenMobile

  Se vários grupos de usuários com diferentes níveis de permissões forem consumir um único aplicativo, talvez seja necessário criar grupos de entrega separados. Com grupos de entrega separados, você pode implantar duas versões separadas do mesmo aplicativo.
- Mapeamento de grupo de entrega e grupo de usuários

  Mapeamentos de grupo de entrega para grupo do Active Directory podem ser um-para-um ou um-para-muitos. Atribua políticas e aplicativos base a um mapeamento de grupo de entrega um-para-muitos. Atribua políticas e aplicativos específicos da função a mapeamentos de grupo de entrega um-para-um.
- Mapeamento de Grupo de Entrega e Recursos de Aplicativos

  Atribua aplicativos específicos a cada grupo de entrega.
- Mapeamento de Grupo de Entrega e Recursos de MDM

  Atribua aplicativos e recursos específicos de gerenciamento de dispositivos a cada grupo de entrega. Por exemplo, configure um grupo de entrega com qualquer combinação dos

seguintes: Tipos de aplicativos (públicos, HDX™ e assim por diante), aplicativos específicos por tipo de aplicativo e recursos como políticas de dispositivo e ações automatizadas.

O exemplo a seguir ilustra como as comunidades de usuários de uma organização de saúde são classificadas para EMM.

Caso de Uso

Esta organização de saúde de exemplo fornece recursos tecnológicos e acesso a múltiplos usuários, incluindo funcionários da rede e afiliados, e voluntários. A organização optou por implementar a solução EMM apenas para usuários não executivos.

Você pode dividir as funções e papéis dos usuários para esta organização em subgrupos, incluindo: clínicos, não clínicos e contratados. Um conjunto selecionado de usuários recebe dispositivos móveis corporativos, enquanto outros podem acessar recursos limitados da empresa a partir de seus dispositivos pessoais (BYOD). Para impor o nível apropriado de restrições de segurança e prevenir vazamentos de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado. Além disso, os usuários podem registrar apenas um único dispositivo.

As seções a seguir fornecem uma visão geral dos papéis e funções de cada subgrupo.

Clínico

- Enfermeiros
- Médicos (Clínicos, Cirurgiões e assim por diante)
- Especialistas (Nutricionistas, flebotomistas, anestesiologistas, radiologistas, cardiologistas, oncologistas e assim por diante)
- Médicos externos (Médicos não funcionários e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (Trabalhadores de escritório e móveis que prestam serviços médicos para visitas domiciliares a pacientes)
- Especialista em Pesquisa (Trabalhadores do Conhecimento e Usuários Avançados em seis Institutos de Pesquisa realizando pesquisa clínica para encontrar respostas para questões na medicina)
- Educação e Treinamento (Enfermeiros, médicos e especialistas em educação e treinamento)

Não Clínico

- Serviços Compartilhados (Funcionários de escritório realizando várias funções de back-office, incluindo: RH, Folha de Pagamento, Contas a Pagar, Serviço de Cadeia de Suprimentos e assim por diante)
- Serviços Médicos (Funcionários de escritório realizando várias funções de gestão de saúde, serviços administrativos e soluções de processos de negócios para provedores, incluindo: Serviços Administrativos, Análise e Inteligência de Negócios, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e assim por diante)
- Serviços de Suporte (Funcionários de escritório realizando várias funções não clínicas, incluindo: Administração de Benefícios, Integração Clínica, Comunicações, Gestão de Remuneração e Desempenho, Serviços de Instalações e Propriedades, Sistemas de Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos e assim por diante.)
- Programas Filantrópicos (Funcionários de escritório e móveis que realizam várias funções em apoio a programas filantrópicos)

Contratados

- Parceiros fabricantes e fornecedores (No local e conectados remotamente via VPN site-a-site, fornecendo várias funções de suporte não clínicas)

Com base nas informações anteriores, a organização criou as seguintes entidades. Para obter mais informações sobre grupos de entrega no XenMobile, consulte Implantar recursos na documentação do produto XenMobile.

Unidades Organizacionais (OUs) e Grupos do Active Directory

Para OU = Recursos do XenMobile

- OU = Clínico; Grupos =
  - XM-Enfermeiros
  - XM-Médicos
  - XM-Especialistas
  - XM-Médicos Externos
  - XM-Serviços de Saúde Domiciliar
  - XM-Especialista em Pesquisa

    - XM-Educação e Treinamento
- OU = Não Clínico; Grupos =
    - XM-Serviços Compartilhados
    - XM-Serviços Médicos
    - XM-Serviços de Suporte
    - XM-Programas Filantrópicos

Usuários e Grupos Locais do XenMobile

Para Grupo= Contratados, Usuários =

- Fornecedor1
- Fornecedor2
- Fornecedor 3
- … Fornecedor 10

Grupos de Entrega do XenMobile

- Enfermeiros Clínicos
- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos Externos
- Clínico-Serviços de Saúde Domiciliar
- Clínico-Especialista em Pesquisa
- Clínico-Educação e Treinamento
- Não Clínico-Serviços Compartilhados
- Não Clínico-Serviços Médicos
- Não Clínico-Serviços de Suporte
- Não Clínico-Programas Filantrópicos

Mapeamento de Grupo de Entrega e Grupo de Usuários

Grupos do Active Directory	**Grupos de Entrega do XenMobile**
XM-Enfermeiros	Clínico-Enfermeiros

XM-Médicos	Clínico-Médicos
XM-Especialistas	Clínico-Especialistas
XM-Médicos Externos	Clínico-Médicos Externos
XM-Serviços de Saúde Domiciliar	Clínico-Serviços de Saúde Domiciliar
XM-Especialista em Pesquisa	Clínico-Especialista em Pesquisa
XM-Educação e Treinamento	Clínico-Educação e Treinamento
XM-Serviços Compartilhados	Não Clínico-Serviços Compartilhados
XM-Serviços Médicos	Serviços Médicos Não Clínicos
Serviços de Suporte XM	Serviços de Suporte Não Clínicos
Programas Filantrópicos XM	Programas Filantrópicos Não Clínicos

Mapeamento de Aplicativos para Grupos de Entrega e Recursos

	Secure Mail	**Secure Web**	**ShareFile**	**Receiver**	**SalesForce 1**	**RSA SecurID**	**EpicCare Haiku**	**Epic Hyperspace**
Enfermeiros Clínicos	X	X	X					
Clínico-Médicos								
Clínico-Especialistas								

Clínico - Médicos Externos	X		X					
Clínico - Serviços de Saúde Domiciliar	X		X					
Clínico - Especialista em Pesquisa	X		X					
Clínico - Educação e Treinamento							X	X
Serviços Compartilhados Não Clínicos							X	X
Serviços Médic							X	X

os Não Clínicos								
Serviços de Suporte Não Clínicos	X		X				X	X
Programas Filantrópicos Não Clínicos	X		X				X	X
Contratados	X		X	X	X		X	X

Mapeamento de Grupo de Entrega e Recursos de Recursos MDM

	MDM: Política de senha	MDM: Restrições de dispositivo	MDM: Ações automatizadas	MDM: Política de Wi-Fi
Clínico-Enfermeiros				X
Clínico-Médicos		X		
Clínico-Especialistas				
Clínico-Médicos Externos				

Clínico-Serviços de Saúde Domiciliar				
Clínico-Especialista em Pesquisa				
Clínico-Educação e Treinamento				
Não Clínico-Serviços Compartilhados				
Não Clínico-Serviços Médicos				
Não Clínico-Serviços de Suporte				
Não Clínico-Programas Filantrópicos				
Contratados				X

Notas e considerações

- O XenMobile cria um grupo de entrega padrão chamado Todos os Usuários durante a configuração inicial. Se você não desativar este Grupo de Entrega, todos os usuários do Active Directory terão o direito de se registrar no XenMobile.
- O XenMobile sincroniza usuários e grupos do Active Directory sob demanda usando uma conexão dinâmica com o servidor LDAP.
- Se um usuário fizer parte de um grupo que não está mapeado no XenMobile, esse usuário não poderá se registrar. Da mesma forma, se um usuário for membro de vários grupos, o

XenMobile categorizará o usuário apenas como estando nos grupos mapeados para o XenMobile.

- Para tornar o registro MDM obrigatório, defina a opção **Registro Obrigatório** como **True** em **Propriedades do Servidor** no console do XenMobile. Para obter detalhes, consulte Propriedades do Servidor.
- Para excluir um grupo de usuários de um grupo de entrega do XenMobile, exclua a entrada no banco de dados do SQL Server, em dbo.userlistgrps.

> **Cuidado:**
>
> Antes de realizar esta ação, crie um backup do XenMobile e do banco de dados.

Sobre a Propriedade do Dispositivo no XenMobile

Você pode agrupar usuários de acordo com o proprietário de um dispositivo de usuário. A propriedade do dispositivo inclui dispositivos de propriedade corporativa e dispositivos de propriedade do usuário, também conhecidos como traga seu próprio dispositivo (BYOD). Você pode controlar como os dispositivos BYOD se conectam à sua rede em dois locais no console do XenMobile: em Regras de Implantação e por meio das propriedades do Servidor XenMobile na página **Configurações**. Para obter detalhes sobre as regras de implantação, consulte Implantar recursos na documentação do XenMobile. Para obter detalhes sobre as propriedades do servidor, consulte Propriedades do Servidor neste manual.

Ao definir as propriedades do servidor, você pode exigir que todos os usuários BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que possam acessar os aplicativos. Ou, você pode dar aos usuários acesso a aplicativos corporativos sem também gerenciar seus dispositivos.

Quando você define a propriedade do servidor **wsapi.mdm.required.flag** como **true**, o XenMobile gerencia todos os dispositivos BYOD, e qualquer usuário que recusar o registro terá o acesso aos aplicativos negado. Considere definir **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança e uma experiência de usuário positiva durante o registro.

Se você deixar **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários podem recusar o registro. No entanto, eles podem acessar aplicativos em seus dispositivos através da XenMobile Store. Considere definir **wsapi.mdm.required.flag** como **false** em

ambientes nos quais restrições de privacidade, legais ou regulatórias exigem nenhum gerenciamento de dispositivo, apenas gerenciamento de aplicativos corporativos.

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da XenMobile Store. Em vez de controles no nível do dispositivo, como limpeza seletiva ou completa, você controla o acesso aos aplicativos por meio de políticas de aplicativos. Algumas configurações de política exigem que o dispositivo verifique o Servidor XenMobile rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Estratégia de E-mail

O acesso seguro ao e-mail a partir de dispositivos móveis é um dos principais impulsionadores por trás de qualquer iniciativa de gerenciamento de mobilidade de uma organização. Decidir sobre a estratégia de e-mail adequada é frequentemente um componente chave de qualquer design do XenMobile®. O XenMobile oferece várias opções para acomodar diferentes casos de uso, com base em requisitos de segurança, experiência do usuário e integração. Este artigo aborda o processo típico de decisão de design e as considerações para escolher a solução certa, desde a seleção do cliente até o fluxo de tráfego de e-mail.

Escolhendo Seus Clientes de E-mail

A seleção do cliente geralmente está no topo da lista para o design geral da estratégia de e-mail. Você pode escolher entre vários clientes: Citrix Secure Mail™, e-mail nativo incluído em um sistema operacional de plataforma móvel específico, ou outros clientes de terceiros disponíveis nas lojas de aplicativos públicas. Dependendo das suas necessidades, você pode, possivelmente, suportar as comunidades de usuários com um único cliente (padrão) ou pode ter que usar uma combinação de clientes.

A tabela a seguir descreve algumas considerações de design para as diferentes opções de cliente disponíveis:

Tópico	**Secure Mail**	**Nativo (por exemplo, iOS Mail)**	**E-mail de terceiros**
Edição Mínima do XenMobile	Avançado	MDM	MDM
Configuração	Perfis de conta do Exchange	Perfis de conta do Exchange configurados via uma política MDM. O	Geralmente requer configuração manual pelo usuário.

	configurados via uma política MDX.	suporte para Android é limitado a: SAFE/ KNOX e Android Enterprise. Todos os outros clientes são considerados clientes de terceiros.	
Segurança	Seguro por design, oferecendo a mais alta segurança. Usa políticas MDX com níveis adicionais de criptografia de dados. O Secure Mail é um aplicativo totalmente gerenciado via uma política MDX. Camada adicional de autenticação com Citrix PIN.	Baseado no conjunto de recursos do fornecedor/ aplicativo. Oferece maior segurança. Usa configurações de criptografia do dispositivo (sem segurança via políticas MDX). Depende da autenticação em nível de dispositivo para acesso ao aplicativo.	Baseado no conjunto de recursos do fornecedor/ aplicativo. Oferece alta segurança.
Integração	Permite a interação com aplicativos gerenciados (MDX) por padrão. Abre URLs da web com o Citrix Secure Web. Salva arquivos e anexa arquivos do Citrix Files. Entra e disca diretamente para o GoToMeeting.	Só pode interagir com outros aplicativos não gerenciados (não-MDX) por padrão.	Só pode interagir com outros aplicativos não gerenciados (não-MDX) por padrão.
Implantação/ Licenciamento	Você pode enviar o Secure Mail via MDM, diretamente de lojas de aplicativos públicas. Incluído com o	Aplicativo cliente incluído com o sistema operacional da plataforma. Sem requisitos de	Pode ser enviado via MDM, como um aplicativo empresarial ou diretamente de lojas de aplicativos

	licenciamento XenMobile Advanced e Enterprise.	licenciamento adicionais.	públicas. Modelo de licenciamento/custos associados baseados no fornecedor do aplicativo.
Suporte	Suporte de um único fornecedor para o cliente e a solução EMM (Citrix). Informações de contato de suporte incorporadas no Secure Hub/recursos de registro de depuração de aplicativos. Um cliente para dar suporte.	Suporte definido pelo fornecedor (Apple/ Google). Pode ser necessário dar suporte a diferentes clientes com base na plataforma do dispositivo.	Suporte definido pelo fornecedor. Um cliente para dar suporte, assumindo que o cliente de terceiros seja compatível com todas as plataformas de dispositivos gerenciados.

Fluxo de tráfego de e-mail e considerações de filtragem

Esta seção discute os três principais cenários e considerações de design sobre o fluxo de tráfego de e-mail (ActiveSync) no contexto do XenMobile.

Cenário 1: Exchange Exposto

Ambientes que suportam clientes externos geralmente têm serviços Exchange ActiveSync expostos à internet. Clientes Mobile ActiveSync se conectam por meio desse caminho voltado para o exterior, através de um proxy reverso (por exemplo, Citrix ADC) ou de um Edge Server. Esta opção é necessária para o uso de clientes de e-mail nativos ou de terceiros, tornando esses clientes a escolha popular para este cenário. Embora não seja uma prática comum, você também pode usar o cliente Secure Mail neste cenário. Ao fazer isso, você se beneficia dos recursos de segurança oferecidos pelo uso de políticas MDX e gerenciamento do aplicativo.

Cenário 2: Tunelado via Citrix ADC (micro VPN e STA)

Este cenário é o padrão ao usar o cliente Secure Mail devido às suas capacidades de micro VPN. Neste caso, o cliente Secure Mail estabelece uma conexão segura com o ActiveSync via Citrix Gateway. Em essência, você pode considerar o Secure Mail como o cliente que se conecta diretamente ao ActiveSync a partir da rede interna. Os clientes Citrix frequentemente padronizam

o Secure Mail como o cliente ActiveSync móvel de escolha. Essa decisão faz parte de uma iniciativa para evitar expor os serviços ActiveSync à internet em um Exchange Server exposto, conforme descrito no primeiro cenário.

Apenas aplicativos com MAM SDK habilitado ou empacotados com MDX podem usar a função de micro VPN. Este cenário não se aplica a clientes nativos se você usar o empacotamento MDX. Embora possa ser possível empacotar clientes de terceiros com o MDX Toolkit, essa prática não é comum. O uso de clientes VPN em nível de dispositivo para permitir acesso tunelado para clientes nativos ou de terceiros provou ser complicado e não uma solução viável.

Cenário 3: Serviços Exchange hospedados na nuvem

Serviços Exchange hospedados na nuvem, como o Microsoft Office 365, estão se tornando mais populares. No contexto do XenMobile, este cenário pode ser tratado da mesma forma que o primeiro cenário, pois o serviço ActiveSync também é exposto à internet. Neste caso, os requisitos do provedor de serviços em nuvem ditam as escolhas do cliente. As escolhas geralmente incluem suporte para a maioria dos clientes ActiveSync, como Secure Mail e outros clientes nativos ou de terceiros.

O XenMobile pode agregar valor em três áreas para este cenário:

- Clientes com políticas MDX e gerenciamento de aplicativos com Secure Mail
- Configuração do cliente com o uso de uma política MDM em clientes de e-mail nativos suportados
- Opções de filtragem do ActiveSync com o uso do conector do Endpoint Management para Exchange ActiveSync

Considerações sobre a filtragem de tráfego de e-mail

Assim como na maioria dos serviços expostos à internet, você deve proteger o caminho e fornecer filtragem para acesso autorizado. A solução XenMobile inclui dois componentes projetados especificamente para fornecer recursos de filtragem do ActiveSync para clientes nativos e de terceiros: Citrix Gateway connector™ para Exchange ActiveSync e Endpoint Management connector para Exchange ActiveSync.

Citrix Gateway connector para Exchange ActiveSync

O Citrix Gateway connector para Exchange ActiveSync fornece filtragem do ActiveSync no perímetro, usando o Citrix ADC como um proxy para o tráfego do ActiveSync. Como resultado, o componente de filtragem fica no caminho do fluxo de tráfego de e-mail, interceptando o e-mail à medida que ele entra ou sai do ambiente. O Citrix Gateway connector para Exchange ActiveSync

atua como um intermediário entre o Citrix ADC e o XenMobile Server. Quando um dispositivo se comunica com o Exchange por meio do servidor virtual ActiveSync no Citrix ADC, o Citrix ADC executa uma chamada HTTP para o serviço do conector para Exchange ActiveSync. Esse serviço então verifica o status do dispositivo com o XenMobile. Com base no status do dispositivo, o conector para Exchange ActiveSync responde ao Citrix ADC para permitir ou negar a conexão. Você também pode configurar regras estáticas para filtrar o acesso com base no usuário, agente e tipo ou ID do dispositivo.

Essa configuração permite que os serviços do Exchange ActiveSync sejam expostos à internet com uma camada adicional de segurança para evitar acesso não autorizado. As considerações de design incluem o seguinte:

- Windows Server: O conector para o componente Exchange ActiveSync requer um Windows Server.
- Conjunto de regras de filtragem: O conector para Exchange ActiveSync foi projetado para filtragem com base no estado e nas informações do dispositivo, e não nas informações do usuário. Embora você possa configurar regras estáticas para filtrar por ID de usuário, não existem opções para filtrar com base na associação a grupos do Active Directory, por exemplo. Se houver um requisito para filtragem de grupo do Active Directory, você poderá usar o conector do Endpoint Management para Exchange ActiveSync.
- Escalabilidade do Citrix ADC: Dada a exigência de proxy de tráfego ActiveSync via Citrix ADC: O dimensionamento adequado da instância do Citrix ADC é crítico para suportar a carga de trabalho adicional de todas as conexões SSL do ActiveSync.
- Cache Integrado do Citrix ADC: A configuração do conector para Exchange ActiveSync no Citrix ADC usa a função de Cache Integrado para armazenar em cache as respostas do conector para Exchange ActiveSync. Como resultado dessa configuração, o Citrix ADC não precisa emitir uma solicitação para o Citrix Gateway connector para Exchange ActiveSync para cada transação ActiveSync em uma determinada sessão. Essa configuração também é crítica para desempenho e escala adequados. O Cache Integrado está disponível com o Citrix ADC Platinum Edition ou você pode licenciar o recurso separadamente para as edições Enterprise.
- Políticas de filtragem personalizadas: Pode ser necessário criar políticas personalizadas do Citrix ADC para restringir determinados clientes ActiveSync fora dos clientes móveis nativos padrão. Essa configuração requer conhecimento sobre solicitações HTTP do ActiveSync e criação de políticas de resposta do Citrix ADC.
- Clientes Secure Mail: O Secure Mail possui recursos de micro VPN que eliminam a necessidade de filtragem no perímetro. O cliente Secure Mail geralmente seria tratado como um cliente ActiveSync interno (confiável) quando conectado através do Citrix Gateway. Se for

necessário suporte para clientes nativos e de terceiros (com o conector para Exchange ActiveSync) e clientes Secure Mail: a Citrix recomenda que o tráfego do Secure Mail não flua através do servidor virtual Citrix ADC usado para o conector para Exchange ActiveSync. Você pode realizar esse fluxo de tráfego via DNS e evitar que a política do conector para Exchange ActiveSync afete os clientes Secure Mail.

Para um diagrama do Citrix Gateway connector para Exchange ActiveSync em uma implantação do XenMobile, consulte Arquitetura de Referência para Implantações Locais.

Conector do Endpoint Management para Exchange ActiveSync

O conector do Endpoint Management para Exchange ActiveSync é um componente do XenMobile que fornece filtragem do ActiveSync no nível do serviço Exchange. Como resultado, a filtragem ocorre apenas quando o e-mail atinge o serviço Exchange, em vez de quando ele entra no ambiente XenMobile. O Mail Manager usa o PowerShell para consultar o Exchange ActiveSync para obter informações de parceria de dispositivos e controlar o acesso por meio de ações de quarentena de dispositivos. Essas ações colocam os dispositivos em e fora da quarentena com base nos critérios de regra do conector do Endpoint Management para Exchange ActiveSync. Semelhante ao Citrix Gateway connector para Exchange ActiveSync, o conector do Endpoint Management para Exchange ActiveSync verifica o status do dispositivo com o XenMobile para filtrar o acesso com base na conformidade do dispositivo. Você também pode configurar regras estáticas para filtrar o acesso com base no tipo ou ID do dispositivo, versão do agente e associação a grupos do Active Directory.

Esta solução não requer o uso do Citrix ADC. Você pode implantar um conector do Endpoint Management para Exchange ActiveSync sem alterar o roteamento para o tráfego ActiveSync existente. As considerações de design incluem:

- Windows Server: O conector do Endpoint Management para o componente Exchange ActiveSync exige que você implante o Windows Server.
- Conjunto de regras de filtragem: Assim como o conector do Citrix Gateway para Exchange ActiveSync, o conector do Endpoint Management para Exchange ActiveSync inclui regras de filtragem para avaliar o estado do dispositivo. Além disso, o conector do Endpoint Management para Exchange ActiveSync também oferece suporte a regras estáticas para filtrar com base na associação a grupos do Active Directory.
- Integração com o Exchange: O conector do Endpoint Management para Exchange ActiveSync requer acesso direto ao Exchange Client Access Server (CAS) que hospeda a função ActiveSync e controle sobre as ações de quarentena do dispositivo. Esse requisito pode

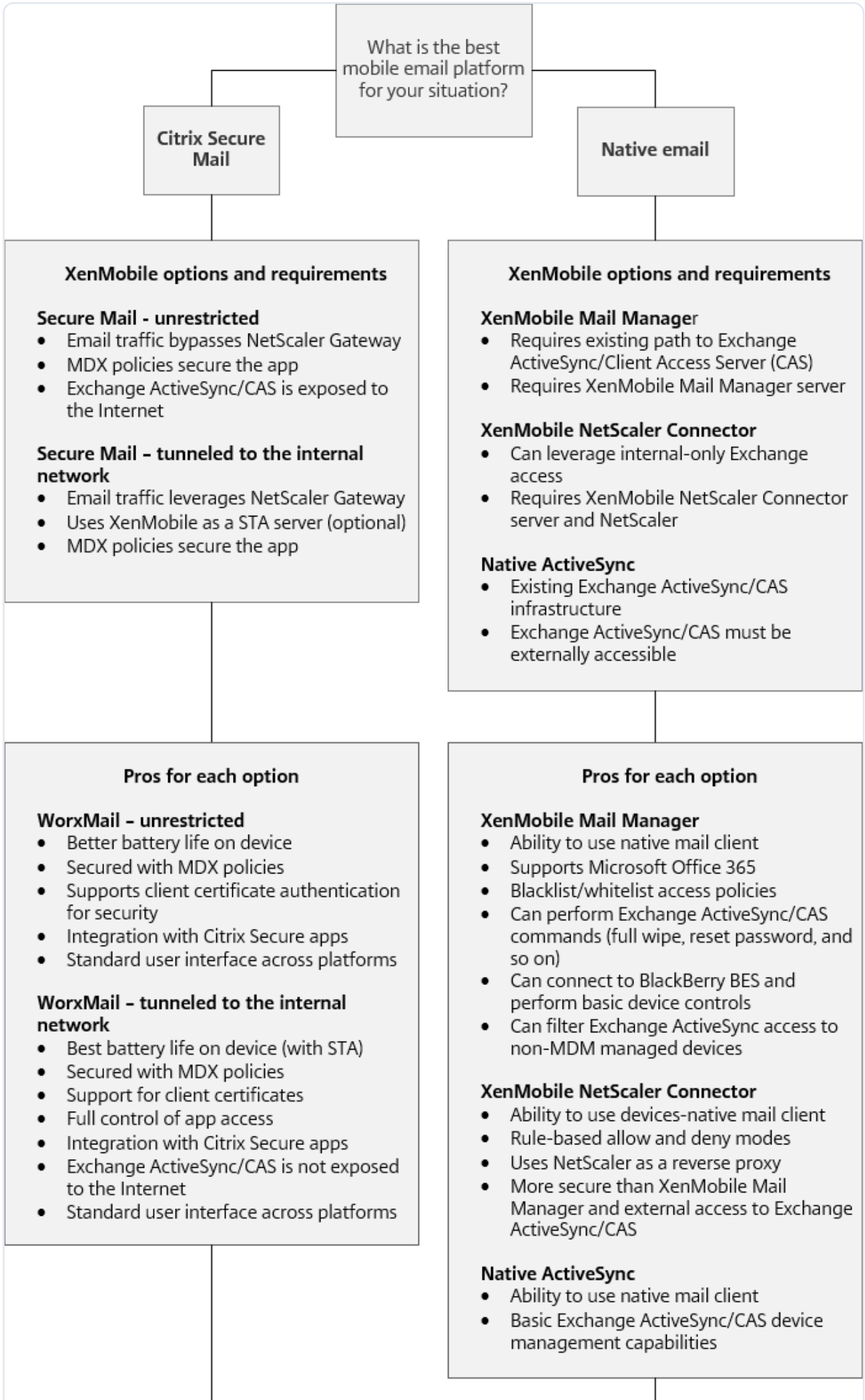
apresentar um desafio dependendo da arquitetura do ambiente e da postura de segurança. É fundamental que você avalie este requisito técnico antecipadamente.

- Outros clientes ActiveSync: Como o conector do Endpoint Management para Exchange ActiveSync está filtrando no nível de serviço do ActiveSync, considere outros clientes ActiveSync fora do ambiente XenMobile. Você pode configurar regras estáticas do conector do Endpoint Management para Exchange ActiveSync para evitar impacto não intencional em outros clientes ActiveSync.
- Funções estendidas do Exchange: Através da integração direta com o Exchange ActiveSync, o conector do Endpoint Management para Exchange ActiveSync oferece a capacidade do XenMobile de realizar uma limpeza do Exchange ActiveSync em um dispositivo móvel. O conector do Endpoint Management para Exchange ActiveSync também permite que o XenMobile acesse informações sobre dispositivos Blackberry e execute outras operações de controle.

Para um diagrama do conector do Endpoint Management para Exchange ActiveSync em uma implantação do XenMobile, consulte Arquitetura de Referência para Implantações Locais.

Árvore de Decisão da Plataforma de E-mail

A figura a seguir ajuda você a distinguir os prós e contras entre o uso de e-mail nativo ou soluções de Secure Mail em sua implantação do XenMobile. Cada escolha permite opções e requisitos associados do XenMobile para habilitar o acesso ao servidor, rede e banco de dados. Os prós e contras incluem detalhes sobre segurança, política e considerações de interface do usuário.


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
XenMobile options and requirements
Secure Mail - unrestricted
• Email traffic bypasses NetScaler Gateway
• MDX policies secure the app
• Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
• Email traffic leverages NetScaler Gateway
• Uses XenMobile as a STA server (optional)
• MDX policies secure the app
XenMobile options and requirements
XenMobile Mail Manager
• Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
• Requires XenMobile Mail Manager server
XenMobile NetScaler Connector
• Can leverage internal-only Exchange access
• Requires XenMobile NetScaler Connector server and NetScaler
Native ActiveSync
• Existing Exchange ActiveSync/CAS infrastructure
• Exchange ActiveSync/CAS must be externally accessible
Pros for each option
WorxMail – unrestricted
• Better battery life on device
• Secured with MDX policies
• Supports client certificate authentication for security
• Integration with Citrix Secure apps
• Standard user interface across platforms
WorxMail – tunneled to the internal network
• Best battery life on device (with STA)
• Secured with MDX policies
• Support for client certificates
• Full control of app access
• Integration with Citrix Secure apps
• Exchange ActiveSync/CAS is not exposed to the Internet
• Standard user interface across platforms
Pros for each option
XenMobile Mail Manager
• Ability to use native mail client
• Supports Microsoft Office 365
• Blacklist/whitelist access policies
• Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
• Can connect to BlackBerry BES and perform basic device controls
• Can filter Exchange ActiveSync access to non-MDM managed devices
XenMobile NetScaler Connector
• Ability to use devices-native mail client
• Rule-based allow and deny modes
• Uses NetScaler as a reverse proxy
• More secure than XenMobile Mail Manager and external access to Exchange ActiveSync/CAS
Native ActiveSync
• Ability to use native mail client
• Basic Exchange ActiveSync/CAS device management capabilities

Integração do XenMobile®

Este artigo aborda o que considerar ao planejar como o XenMobile deve se integrar com sua rede e soluções existentes. Por exemplo, se você já estiver usando o Citrix ADC para Virtual Apps and Desktops:

- Você usa a instância existente do Citrix ADC ou uma instância nova e dedicada?
- Você deseja integrar os aplicativos HDX que são publicados usando o StoreFront™ com o XenMobile?
- Você planeja usar o Citrix Files com o XenMobile?
- Você tem uma solução de Controle de Acesso à Rede que deseja integrar ao XenMobile?
- Você implanta proxies da web para todo o tráfego de saída da sua rede?

Citrix ADC e Citrix Gateway

O Citrix Gateway é obrigatório para os modos XenMobile ENT e MAM. O Citrix Gateway fornece um caminho de micro VPN para acesso a todos os recursos corporativos e oferece suporte a autenticação multifator forte. O balanceamento de carga do Citrix ADC é necessário para todos os modos de dispositivo do XenMobile Server:

- Se você tiver vários XenMobile Servers
- Ou, se o XenMobile Server estiver dentro da sua DMZ ou rede interna (e, portanto, o tráfego flui dos dispositivos para o Citrix ADC e para o XenMobile)

Você pode usar instâncias existentes do Citrix ADC ou configurar novas para o XenMobile. As seções a seguir descrevem as vantagens e desvantagens de usar instâncias existentes ou novas e dedicadas do Citrix ADC.

Citrix ADC MPX compartilhado com um VIP do Citrix Gateway criado para o XenMobile

Vantagens:

- Usa uma instância comum do Citrix ADC para todas as conexões remotas do Citrix: Citrix Virtual Apps and Desktops™, VPN completa e VPN sem cliente.
- Usa as configurações existentes do Citrix ADC, como para autenticação de certificado e para acessar serviços como DNS, LDAP e NTP.
- Usa uma única licença de plataforma do Citrix ADC.

Desvantagens:

- É mais difícil planejar a escala quando você manipular dois casos de uso diferentes no mesmo Citrix ADC.
- Às vezes, você precisa de uma versão específica do Citrix ADC para um caso de uso do Citrix Virtual Apps™ and Desktops. Essa mesma versão pode ter problemas conhecidos para o XenMobile. Ou o XenMobile pode ter problemas conhecidos para a versão do Citrix ADC.
- Se um Citrix Gateway existir, você não poderá executar o assistente do Citrix ADC para XenMobile uma segunda vez para criar a configuração do Citrix ADC para XenMobile.
- Exceto quando licenças Platinum são usadas para Citrix Gateway 11.1 ou posterior: As licenças de acesso de usuário instaladas no Citrix ADC e necessárias para conectividade VPN são agrupadas. Como essas licenças estão disponíveis para todos os servidores virtuais do Citrix ADC, outros serviços além do XenMobile podem potencialmente consumi-las.

Instância dedicada do Citrix ADC VPX/MPX

Vantagens:

A Citrix recomenda usar uma instância dedicada do Citrix ADC.

- Mais fácil de planejar a escala e separa o tráfego do XenMobile de uma instância do Citrix ADC que já pode estar com recursos limitados.
- Evita problemas quando o XenMobile e o Citrix Virtual Apps and Desktops precisam de diferentes versões de software do Citrix ADC. A recomendação geral é usar a versão e a compilação mais recentes e compatíveis do Citrix ADC para o XenMobile.
- Permite a configuração do Citrix ADC pelo XenMobile através do assistente integrado do Citrix ADC para XenMobile.
- Separação virtual e física de serviços.
- Exceto quando licenças Platinum são usadas para Citrix Gateway 11.1 ou posterior: As licenças de acesso de usuário necessárias para o XenMobile estão disponíveis apenas para os Serviços XenMobile no Citrix ADC.

Desvantagens:

- Requer a configuração de serviços extras no Citrix ADC para oferecer suporte à configuração do XenMobile.
- Requer outra licença de plataforma do Citrix ADC. Licencie cada instância do Citrix ADC para o Citrix Gateway.

Para obter informações sobre o que considerar ao integrar o Citrix ADC e o Citrix Gateway com cada modo do XenMobile Server, consulte Integração com Citrix ADC e Citrix Gateway.

StoreFront

Se você tiver um ambiente Citrix Virtual Apps and Desktops, poderá integrar aplicativos HDX™ com o XenMobile usando o StoreFront. Ao integrar aplicativos HDX com o XenMobile:

- Os aplicativos ficam disponíveis para usuários registrados no XenMobile.
- Os aplicativos são exibidos na Loja XenMobile junto com outros aplicativos móveis.
- O XenMobile usa o site legado PNAgent (serviços) no StoreFront.
- Quando o Citrix Receiver™ é instalado em um dispositivo, os aplicativos HDX são iniciados usando o Receiver.

O StoreFront tem uma limitação de um site de serviço por instância do StoreFront. Suponha que você tenha várias lojas e queira segmentá-las de outros usos de produção. Nesse caso, a Citrix geralmente recomenda que você considere uma nova instância do StoreFront e um site de serviços para o XenMobile.

As considerações incluem:

- Existem requisitos de autenticação diferentes para o StoreFront? O site de serviços do StoreFront requer credenciais do Active Directory para logon. Clientes que usam apenas autenticação baseada em certificado não podem enumerar aplicativos através do XenMobile usando o mesmo Citrix Gateway.
- Usar a mesma loja ou criar uma nova?
- Usar o mesmo servidor StoreFront ou um diferente?

As seções a seguir observam as vantagens e desvantagens de usar storefronts separados ou combinados para Receiver e aplicativos de produtividade móvel.

Integre sua instância existente do StoreFront com um XenMobile Server

Vantagens:

- Mesma loja: Nenhuma configuração adicional do StoreFront é necessária para o XenMobile, supondo que você use o mesmo VIP do Citrix ADC para acesso HDX. Suponha que você escolha usar a mesma loja e queira direcionar o acesso do Receiver para um novo VIP do Citrix ADC. Nesse caso, adicione a configuração apropriada do Citrix Gateway ao StoreFront.
- Mesmo servidor StoreFront: Usa a instalação e configuração existentes do StoreFront.

Desvantagens:

- Mesma loja: Qualquer reconfiguração do StoreFront para suportar cargas de trabalho do Virtual Apps and Desktops pode afetar negativamente o XenMobile também.
- Mesmo servidor StoreFront: Em ambientes grandes, considere a carga adicional do uso do PNAgent pelo XenMobile para enumeração e inicialização de aplicativos.

Use uma nova instância dedicada do StoreFront para integração com o XenMobile Server

Vantagens:

- Nova loja: Quaisquer alterações de configuração da loja do StoreFront para XenMobile não devem afetar as cargas de trabalho existentes do Virtual Apps and Desktops.
- Novo servidor StoreFront: As alterações de configuração do servidor não devem afetar o fluxo de trabalho do Virtual Apps and Desktops. Além disso, a carga fora do uso do PNAgent pelo XenMobile para enumeração e lançamento de aplicativos não deve afetar a escalabilidade.

Desvantagens:

- Nova loja: Configuração da loja do StoreFront.
- Novo servidor StoreFront: Requer nova instalação e configuração do StoreFront.

Para mais informações, consulte Virtual Apps and Desktops through Citrix Secure Hub na documentação do XenMobile.

ShareFile e Citrix Files

> **Aviso:**
>
> Este recurso será descontinuado se o ShareFile (agora Progress) deixar de oferecer suporte.

> O Citrix Files permite que os usuários acessem e sincronizem todos os seus dados de qualquer dispositivo. Com o Citrix Files, os usuários podem compartilhar dados com segurança com pessoas dentro e fora da organização. Se você integrar o ShareFile com o XenMobile Advanced Edition ou Enterprise Edition, o XenMobile poderá fornecer ao Citrix Files:

- Autenticação de logon único para usuários do aplicativo XenMobile.
- Provisionamento de contas de usuário baseado no Active Directory.
- Políticas abrangentes de controle de acesso.

Os usuários móveis podem se beneficiar do conjunto completo de recursos da conta Enterprise.

Alternativamente, você pode configurar o XenMobile para integrar-se apenas com conectores de zona de armazenamento. Através dos conectores de zona de armazenamento, o Citrix Files fornece acesso a:

- Documentos e pastas
- Compartilhamentos de arquivos de rede
- Em sites do SharePoint: Coleções de sites e bibliotecas de documentos.

Os compartilhamentos de arquivos conectados podem incluir as mesmas unidades de rede domésticas usadas em ambientes Citrix Virtual Apps and Desktops. Você usa o console do XenMobile para configurar a integração com o Citrix Files ou conectores de zonas de armazenamento. Para obter mais informações, consulte Citrix Files use with XenMobile.

As seções a seguir abordam as perguntas a serem feitas ao tomar decisões de design para o Citrix Files.

Integrar com Citrix Files ou apenas conectores de zona de armazenamento

Perguntas a fazer:

- Você deseja armazenar dados em zonas de armazenamento gerenciadas pela Citrix?
- Você deseja fornecer aos usuários recursos de compartilhamento e sincronização de arquivos?
- Você deseja permitir que os usuários acessem arquivos no site do Citrix Files? Ou acessem conteúdo do Office 365 e conectores de Nuvem Pessoal a partir de dispositivos móveis?

Decisão de design:

- Se a resposta a qualquer uma dessas perguntas for "sim", integre com o Citrix Files.
- Uma integração apenas com conectores de zona de armazenamento oferece aos usuários iOS acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos de rede. Nesta configuração, você não configura um subdomínio do ShareFile, não provisiona usuários para o Citrix Files nem hospeda dados do Citrix Files. O uso de conectores de zona de armazenamento com o XenMobile está em conformidade com as restrições de segurança contra o vazamento de informações do usuário para fora da rede corporativa.

Localização do servidor do controlador de zonas de armazenamento

Perguntas a fazer:

- Você precisa de armazenamento local ou recursos como conectores de zona de armazenamento?
- Se estiver usando recursos locais do Citrix Files, onde os controladores de zonas de armazenamento estarão localizados na rede?

Decisão de design:

- Determine se os servidores do controlador de zonas de armazenamento serão localizados na nuvem do Citrix Files, em seu sistema de armazenamento local de locatário único ou em armazenamento em nuvem de terceiros compatível.
- Os controladores de zonas de armazenamento exigem algum acesso à internet para se comunicar com o Plano de Controle do Citrix Files. Você pode se conectar de várias maneiras, incluindo acesso direto, configurações NAT/PAT ou configurações de proxy.

Conectores de zona de armazenamento

Perguntas a fazer:

- Quais são os caminhos de compartilhamento CIFS?
- Quais são os URLs do SharePoint?

Decisão de design:

- Determine se os controladores de zonas de armazenamento locais são necessários para acessar esses locais.
- Devido à comunicação do conector de zona de armazenamento com recursos internos, como repositórios de arquivos, compartilhamentos CIFS e SharePoint: a Citrix recomenda que os controladores de zonas de armazenamento residam na rede interna, atrás de firewalls DMZ e sejam acessados pelo Citrix ADC.

Integração SAML com XenMobile Enterprise

Perguntas a fazer:

- A autenticação do Active Directory é necessária para o Citrix Files?
- O primeiro uso do aplicativo Citrix Files para XenMobile requer SSO?
- Existe um IdP padrão em seu ambiente atual?
- Quantos domínios são necessários para usar o SAML?
- Existem vários aliases de e-mail para usuários do Active Directory?
- Há alguma migração de domínio do Active Directory em andamento ou agendada para breve?

Decisão de design:

Ambientes XenMobile Enterprise podem optar por usar SAML como mecanismo de autenticação para o Citrix Files. As opções de autenticação são:

- Usar o XenMobile Server como Provedor de Identidade (IdP) para SAML

Esta opção pode proporcionar uma excelente experiência do usuário e automatizar a criação de contas do Citrix Files, além de habilitar recursos de SSO para aplicativos móveis.

- O XenMobile Server é aprimorado para este processo: Ele não requer a sincronização do Active Directory.
- Usar a Ferramenta de Gerenciamento de Usuários do Citrix Files para provisionamento de usuários.
- Usar um fornecedor terceirizado compatível como IdP para SAML

Se você tiver um IdP existente e compatível e não precisar de recursos de SSO para aplicativos móveis, esta opção pode ser a melhor para você. Esta opção também exige o uso da Ferramenta de Gerenciamento de Usuários do Citrix Files para provisionamento de contas.

O uso de soluções IdP de terceiros, como o ADFS, também pode fornecer recursos de SSO no lado do cliente Windows. Certifique-se de avaliar os casos de uso antes de escolher seu IdP SAML do Citrix Files.

Além disso, para satisfazer ambos os casos de uso, você pode configurar o ADFS e o XenMobile como um IdP duplo.

Aplicativos móveis

Perguntas a fazer:

- Qual aplicativo móvel do Citrix Files você planeja usar (público, MDM, MDX)?

Decisão de design:

- Você distribui aplicativos de produtividade móvel da Apple App Store e Google Play Store. Com essa distribuição pública da loja de aplicativos, você obtém aplicativos empacotados na página de downloads da Citrix.
- Se a segurança for baixa e você não precisar de conteinerização, o aplicativo público do Citrix Files pode não ser adequado. Em um ambiente somente MDM, você pode entregar a versão MDM do aplicativo Citrix Files usando o XenMobile no modo MDM.
- Para obter mais informações, consulte Aplicativos e Citrix Files para XenMobile.

Segurança, políticas e controle de acesso

Perguntas a fazer:

- Quais restrições você exige para usuários de desktop, web e dispositivos móveis?
- Quais configurações padrão de controle de acesso você deseja para os usuários?
- Qual política de retenção de arquivos você planeja usar?

Decisão de design:

- O Citrix Files permite gerenciar permissões de funcionários e segurança de dispositivos. Para obter informações, consulte Permissões de Funcionários e Gerenciamento de Dispositivos e Aplicativos.
- Algumas configurações de segurança de dispositivo do Citrix Files e políticas MDX controlam os mesmos recursos. Nesses casos, as políticas do XenMobile têm precedência, seguidas pelas configurações de segurança de dispositivo do Citrix Files. Exemplos: Se você desabilitar aplicativos externos no Citrix Files, mas habilitá-los no XenMobile, os aplicativos externos serão desabilitados no Citrix Files. Você pode configurar os aplicativos para que o XenMobile não exija um PIN/senha, mas o aplicativo Citrix Files exija um PIN/senha.

Zonas de armazenamento padrão versus restritas

Perguntas a fazer:

- Você exige zonas de armazenamento restritas?

Decisão de design:

- Uma zona de armazenamento padrão é destinada a dados não sensíveis e permite que os funcionários compartilhem dados com não-funcionários. Esta opção suporta fluxos de trabalho que envolvem o compartilhamento de dados fora do seu domínio.
- Uma zona de armazenamento restrita protege dados confidenciais: Somente usuários de domínio autenticados podem acessar os dados armazenados na zona.

Proxies da Web

O cenário mais provável para rotear o tráfego do XenMobile por meio de um proxy HTTP(S)/SOCKS é o seguinte: Quando a sub-rede em que o XenMobile Server reside não tem acesso de saída à Internet para os endereços IP necessários da Apple, Google ou Microsoft. Você pode especificar as configurações do servidor proxy no XenMobile para rotear todo o tráfego da Internet para o servidor proxy. Para obter mais informações, consulte Habilitar servidores proxy.

A tabela a seguir descreve as vantagens e desvantagens do proxy mais comum usado com o XenMobile.

Opção	Vantagens	Desvantagens
Use um proxy HTTP(S)/ SOCKS com um XenMobile Server.	Nos casos em que as políticas não permitem conexões de saída à Internet da sub-rede do XenMobile Server: Você pode configurar um proxy HTTP(S) ou SOCKS para fornecer conectividade com a Internet.	Se o servidor proxy falhar, a conectividade APNs (iOS) ou Firebase Cloud Messaging (Android) será interrompida. Como resultado, as notificações de dispositivo falham para todos os dispositivos iOS e Android.
Use um proxy HTTP(S) com o Secure Web.	Você pode monitorar o tráfego HTTP/HTTPS para garantir que a atividade da Internet esteja em conformidade com os padrões da sua organização.	Essa configuração exige que todo o tráfego da Internet do Secure Web seja tunelado de volta para a rede corporativa antes de ser enviado de volta para a Internet. Se sua conexão com a Internet restringir a navegação: Essa configuração pode afetar o desempenho da navegação na Internet.

A configuração do perfil de sessão do Citrix ADC para tunelamento dividido afeta o tráfego da seguinte forma.

Quando o tunelamento dividido do Citrix ADC está **desativado**:

- Se a política de **Acesso à rede** do MDX estiver definida como **Tunelado para a rede interna:** Todo o tráfego é forçado a usar a micro VPN ou VPN sem cliente (cVPN) de volta para o Citrix Gateway.
- Configure as políticas/perfis de tráfego do Citrix ADC para o servidor proxy e vincule-os ao VIP do Citrix Gateway.

> **Importante:**

> Certifique-se de excluir o tráfego cVPN do Secure Hub do proxy.

- Para obter mais informações, consulte Tráfego do XenMobile Secure Hub através do servidor proxy no modo de navegação segura.

Quando o **Citrix ADC Split Tunneling** está **ativado**:

- Quando os aplicativos são configurados com a política de **Acesso à rede** do MDX definida como **Tunelado para a rede interna**: Os aplicativos primeiro tentam obter o recurso da web diretamente. Se o recurso da web não estiver publicamente disponível, esses aplicativos então recorrem ao Citrix Gateway.
- Configure as políticas e perfis de tráfego do Citrix ADC para o servidor proxy. Em seguida, vincule essas políticas e perfis ao VIP do Citrix Gateway.

> **Importante:**

> Certifique-se de excluir o tráfego cVPN do Secure Hub do proxy.

> A configuração do perfil de sessão do seu Citrix ADC para **Split DNS** (em **Experiência do cliente**) funciona de forma semelhante ao Split Tunneling.

Com o **Split DNS** ativado e definido como **Ambos**:

- O cliente primeiro tenta resolver o FQDN localmente e, em seguida, recorre ao Citrix ADC para resolução de DNS em caso de falha.

Com o **Split DNS** definido como **Remoto**:

- A resolução de DNS ocorre apenas no Citrix ADC.

Com **Split DNS** definido como **Local**:

- O cliente tenta resolver o FQDN localmente. O Citrix ADC não é usado para resolução de DNS.

Controle de Acesso

As empresas podem gerenciar dispositivos móveis dentro e fora das redes. Soluções de Gerenciamento de Mobilidade Empresarial, como o XenMobile, são excelentes para fornecer segurança e controles para dispositivos móveis, independentemente da localização. No entanto,

ao combiná-las com uma solução de Controle de Acesso à Rede (NAC), você pode adicionar QoS e um controle mais granular aos dispositivos internos à sua rede. Essa combinação permite estender a avaliação de segurança do dispositivo XenMobile por meio de sua solução NAC. Sua solução NAC pode então usar a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação.

Você pode usar qualquer uma dessas soluções para aplicar políticas NAC:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

A Citrix não garante a integração para outras soluções NAC.

As vantagens da integração de uma solução NAC com o XenMobile incluem o seguinte:

- Melhor segurança, conformidade e controle para todos os endpoints em uma rede corporativa.
- Uma solução NAC pode:
  - Detectar dispositivos no instante em que tentam se conectar à sua rede.
  - Consultar o XenMobile para atributos do dispositivo.
  - Usar essas informações do dispositivo para determinar se deve permitir, bloquear, limitar ou redirecionar esses dispositivos. Essas decisões dependem das políticas de segurança que você escolher aplicar.
- Uma solução NAC fornece aos administradores de TI uma visão de dispositivos não gerenciados e não compatíveis.

Para uma descrição dos filtros de conformidade NAC suportados pelo XenMobile e uma visão geral da configuração, consulte Controle de Acesso à Rede.

Requisitos de Múltiplos Sites

É possível arquitetar e configurar implantações do XenMobile® que incluem múltiplos sites para alta disponibilidade e recuperação de desastres. Este artigo fornece uma visão geral dos modelos de alta disponibilidade e recuperação de desastres usados em implantações do XenMobile.

Alta Disponibilidade

- Para nós de cluster do XenMobile, o Citrix ADC gerencia o balanceamento de carga. Para mais informações, consulte Configurar Cluster

- Os nós do XenMobile Server operam em uma configuração ativo/ativo.
- Mais nós do XenMobile Server são adicionados a um cluster de alta disponibilidade conforme a capacidade é necessária. Um nó pode manipular até aproximadamente 8.500 dispositivos de usuário (consulte Escalabilidade e desempenho para mais detalhes).
- A Citrix® recomenda configurar servidores XenMobile "n+1": um servidor para cada 8.500 dispositivos de usuário e um servidor extra para redundância.
- A Citrix recomenda alta disponibilidade para todas as instâncias do Citrix ADC sempre que possível para permitir que as configurações sejam sincronizadas com um segundo Citrix ADC.
- O par padrão de alta disponibilidade do Citrix ADC opera em uma configuração ativo/passivo.

Uma implantação típica de alta disponibilidade do XenMobile geralmente inclui:

- Duas instâncias do Citrix ADC (VPX ou MPX). Se a plataforma Citrix ADC SDX for usada, a alta disponibilidade também deve ser considerada.
- Dois ou mais XenMobile Servers configurados com as mesmas configurações de banco de dados.

Recuperação de Desastres

É possível configurar o XenMobile para recuperação de desastres em dois data centers, com um data center ativo e um data center passivo. O Citrix ADC e o Global Server Load Balancing (GSLB) são usados para criar um caminho de dados ativo/ativo, de modo que a experiência do usuário seja a de uma configuração ativo/ativo.

Para recuperação de desastres, uma implantação do XenMobile inclui:

- Dois data centers - cada um contém uma ou mais instâncias do Citrix ADC, XenMobile Servers e bancos de dados SQL Server.
- Um servidor GSLB para direcionar o tráfego para os data centers. O servidor GSLB é configurado para a URL de registro do XenMobile e para a URL do Citrix Gateway que lida com o tráfego para o site.
- Quando você usa o assistente do Citrix ADC para XenMobile para configurar o Citrix Gateway, por padrão, o GSLB não está habilitado para resolver o tráfego para o servidor de registro do XenMobile e o tráfego para o Citrix Gateway, a caminho do servidor de balanceamento de carga MAM. Como resultado, mais etapas são necessárias. Para obter mais informações sobre como preparar e implementar essas etapas, consulte Recuperação de Desastres.
- Servidores SQL em cluster de Grupos de Disponibilidade Always On.
- A latência entre os XenMobile Servers e o SQL Server deve ser inferior a 5 ms.

Nota:

Os métodos de recuperação de desastres descritos neste manual fornecem apenas recuperação de desastres automatizada para a camada de acesso. Você deve iniciar manualmente todos os nós do XenMobile Server e o banco de dados SQL Server no site de failover antes que os dispositivos possam se conectar ao XenMobile Server.

Integração com Citrix Gateway e Citrix ADC

Quando integrado ao XenMobile®, o Citrix Gateway fornece um mecanismo de autenticação para acesso remoto de dispositivos à rede interna para dispositivos MAM. A integração permite que aplicativos de produtividade móvel se conectem a servidores corporativos na intranet por meio de uma micro VPN. A micro VPN é criada a partir dos aplicativos no dispositivo móvel para o Citrix Gateway. O Citrix Gateway fornece um caminho de micro VPN para acesso a todos os recursos corporativos e oferece forte suporte à autenticação multifator.

O balanceamento de carga do Citrix ADC é necessário para todos os modos de dispositivo do XenMobile Server nestes casos:

- Se você tiver vários XenMobile Servers
- Ou se o XenMobile Server estiver dentro da sua DMZ ou rede interna (e, portanto, o tráfego flui dos dispositivos para o Citrix ADC para o XenMobile)

Requisitos de integração para modos do XenMobile Server

Os requisitos de integração para Citrix Gateway e Citrix ADC diferem com base nos modos do XenMobile Server: MAM, MDM e ENT.

MAM

Com o XenMobile Server no modo MAM:

- **Citrix Gateway** é necessário. O Citrix Gateway fornece um caminho de micro VPN para acesso a todos os recursos corporativos e oferece forte suporte à autenticação multifator.
- **Citrix ADC** é recomendado para balanceamento de carga.

  A Citrix recomenda que você implante o XenMobile em uma configuração de alta disponibilidade, que requer um balanceador de carga na frente do XenMobile. Para obter detalhes, consulte Sobre os modos MAM e MAM herdado.

MDM

Com o XenMobile Server no modo MDM:

- O Citrix Gateway não é necessário. Para implantações MDM, a Citrix recomenda o Citrix Gateway para VPN de dispositivos móveis.
- O Citrix ADC é recomendado para segurança e balanceamento de carga.

  A Citrix recomenda que você implante um appliance Citrix ADC na frente do XenMobile Server, para segurança e balanceamento de carga. Para implantações padrão com o XenMobile na DMZ, a Citrix recomenda o assistente Citrix ADC para XenMobile juntamente com o balanceamento de carga do XenMobile Server no modo SSL Bridge. Você também pode considerar o SSL Offload para implantações em que:

  - O XenMobile Server reside na rede interna em vez da DMZ.
  - Ou sua equipe de segurança exige uma configuração de SSL Bridge.

  A Citrix não recomenda expor o XenMobile Server à Internet via NAT ou proxies ou balanceadores de carga de terceiros existentes para MDM. Essas configurações representam um risco potencial de segurança, mesmo que o tráfego SSL termine no XenMobile Server (SSL Bridge).

  Para ambientes de alta segurança, o Citrix ADC com a configuração padrão do XenMobile atende ou excede os requisitos de segurança.

  Para ambientes MDM com as mais altas necessidades de segurança, a terminação SSL no Citrix ADC permite inspecionar o tráfego no perímetro, mantendo a criptografia SSL de ponta a ponta. Para obter mais informações, consulte Requisitos de Segurança. O Citrix ADC oferece opções para definir cifras SSL/TLS e hardware SSL FIPS Citrix ADC.

ENT (MAM+MDM)

Com o XenMobile Server no modo ENT:

- O Citrix Gateway é necessário. O Citrix Gateway fornece um caminho de micro VPN para acesso a todos os recursos corporativos e oferece suporte robusto à autenticação multifator.

  Quando o modo do XenMobile Server é ENT e um usuário opta por não participar do registro MDM, o dispositivo opera no modo MAM herdado. No modo MAM herdado, os dispositivos se registram usando o FQDN do Citrix Gateway. Para obter detalhes, consulte Sobre os modos MAM e MAM Herdado.

- O Citrix ADC é recomendado para balanceamento de carga. Para obter mais informações, consulte o ponto sobre o Citrix ADC anteriormente neste artigo em "MDM".

> **Importante:**
>
> Para o registro inicial, o tráfego dos dispositivos do usuário é autenticado no XenMobile Server, independentemente de você configurar servidores virtuais de balanceamento de carga para SSL Offload ou SSL Bridge.

Decisões de Design

As seções a seguir resumem as muitas decisões de design a serem consideradas ao planejar uma integração do Citrix Gateway com o XenMobile.

Licenciamento e edição

Detalhes da decisão:

- Qual edição do Citrix ADC você planeja usar?
- Você aplicou licenças de Plataforma ao Citrix ADC?
- Se você precisar da funcionalidade MAM, aplicou as Licenças de Acesso Universal do Citrix ADC?

Orientação de design:

Certifique-se de aplicar as licenças apropriadas ao Citrix Gateway. Se você estiver usando o Citrix Gateway connector™ para Exchange ActiveSync, o cache integrado pode ser necessário. Portanto, você deve garantir que a Edição apropriada do Citrix ADC esteja em vigor.

Os requisitos de licença para habilitar os recursos do Citrix ADC são os seguintes.

- O balanceamento de carga do XenMobile MDM requer uma licença de plataforma padrão do Citrix ADC, no mínimo.
- O balanceamento de carga do ShareFile com o controlador de zonas de armazenamento requer uma licença de plataforma padrão do Citrix ADC, no mínimo.
- O XenMobile Advanced Edition (local) ou o Citrix Endpoint Management™ (nuvem) inclui as licenças universais do Citrix Gateway necessárias para MAM.

- O balanceamento de carga do Exchange requer uma licença de plataforma Citrix ADC Platinum ou uma licença de plataforma Citrix ADC Enterprise com a adição de uma licença de Cache Integrado.

Versão do Citrix ADC para XenMobile

Detalhes da decisão:

- Qual versão do Citrix ADC está sendo executada no ambiente XenMobile?
- Você precisa de uma instância separada?

Orientação de design:

A Citrix recomenda usar uma instância dedicada do Citrix ADC para seu servidor virtual Citrix Gateway. Certifique-se de que a versão e o build mínimos exigidos do Citrix ADC estejam em uso para o ambiente XenMobile. Normalmente, é melhor usar a versão e o build mais recentes compatíveis do Citrix ADC para o XenMobile. Se a atualização do Citrix Gateway afetar seu ambiente existente, uma segunda instância dedicada para o XenMobile pode ser apropriada.

Se você planeja compartilhar uma instância do Citrix ADC para XenMobile e outros aplicativos que usam conexões VPN, certifique-se de ter licenças VPN suficientes para ambos. Lembre-se de que os ambientes de teste e produção do XenMobile não podem compartilhar uma instância do Citrix ADC.

Certificados

Detalhes da decisão:

- Você exige um grau mais alto de segurança para o registro e acesso ao ambiente XenMobile?
- O LDAP não é uma opção?

Orientação de design:

A configuração padrão para o XenMobile é autenticação por nome de usuário e senha. Para adicionar outra camada de segurança para o registro e acesso ao ambiente XenMobile, considere usar a autenticação baseada em certificado. Você pode usar certificados com LDAP para autenticação de dois fatores, proporcionando um grau mais alto de segurança sem a necessidade de um servidor RSA.

Se você não permitir LDAP e usar cartões inteligentes ou métodos semelhantes, a configuração de certificados permite representar um cartão inteligente para o XenMobile. Os usuários então se

registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que um usuário tem acesso, o XenMobile cria e implanta o certificado usado para autenticar no ambiente XenMobile.

O XenMobile suporta Lista de Revogação de Certificados (CRL) apenas para uma Autoridade de Certificação de terceiros. Se você tiver um CA Microsoft configurado, o XenMobile usa o Citrix ADC para gerenciar a revogação. Ao configurar a autenticação baseada em certificado de cliente, considere se você precisa configurar a configuração da Lista de Revogação de Certificados (CRL) do Citrix ADC **Enable CRL Auto Refresh**. Esta etapa garante que o usuário de um dispositivo registrado apenas em MAM não possa autenticar usando um certificado existente no dispositivo. O XenMobile reemite um novo certificado, pois não restringe um usuário de gerar um certificado de usuário se um for revogado. Essa configuração aumenta a segurança das entidades PKI quando a CRL verifica entidades PKI expiradas.

Topologia de rede

Detalhes da decisão:

- Qual topologia do Citrix ADC é necessária?

Orientação de design:

A Citrix recomenda usar uma instância do Citrix ADC para o XenMobile. No entanto, talvez você não queira que o tráfego vá da rede interna para a DMZ. Nesse caso, considere configurar uma instância extra do Citrix ADC. Use uma instância do Citrix ADC para usuários internos e outra para usuários externos. Quando os usuários alternam entre as redes interna e externa, o cache de registros DNS pode resultar em um aumento nos prompts de logon do Secure Hub.

O XenMobile não oferece suporte a salto duplo do Citrix Gateway.

VIPs do Citrix Gateway dedicados ou compartilhados

Detalhes da decisão:

- Você usa atualmente o Citrix Gateway para Virtual Apps and Desktops?
- Você planeja que o XenMobile use o mesmo Citrix Gateway que o Virtual Apps and Desktops?
- Quais são os requisitos de autenticação para ambos os fluxos de tráfego?

Orientação de design:

Quando seu ambiente Citrix inclui XenMobile, além de Virtual Apps and Desktops, você pode usar a mesma instância do Citrix ADC e o servidor virtual do Citrix Gateway para ambos. Devido a possíveis conflitos de versionamento e isolamento de ambiente, uma instância dedicada do Citrix ADC e do Citrix Gateway são recomendadas para cada ambiente XenMobile. No entanto, se uma

instância dedicada do Citrix ADC não for uma opção, a Citrix recomenda usar um servidor virtual dedicado do Citrix Gateway para separar os fluxos de tráfego para o Secure Hub. Essa configuração substitui um servidor virtual compartilhado entre o XenMobile e o Virtual Apps and Desktops.

Se você usa autenticação LDAP, o Receiver e o Secure Hub podem autenticar para o mesmo Citrix Gateway sem problemas. Se você usa autenticação baseada em certificado, o XenMobile envia um certificado no contêiner MDX e o Secure Hub usa o certificado para autenticar com o Citrix Gateway. O Receiver é separado do Secure Hub e não pode usar o mesmo certificado que o Secure Hub para autenticar para o mesmo Citrix Gateway.

Você pode considerar a seguinte solução alternativa, que permite usar o mesmo FQDN para dois VIPs do Citrix Gateway.

- Crie dois VIPs do Citrix Gateway com o mesmo endereço IP. O VIP para o Secure Hub usa a porta padrão 443 e o VIP para Virtual Apps and Desktops (que implantam o Receiver) usa a porta 444.
- Como resultado, um FQDN é resolvido para o mesmo endereço IP.
- Para esta solução alternativa, você pode configurar o StoreFront™ para retornar um arquivo ICA para a porta 444, em vez da porta padrão, 443. Esta solução alternativa não exige que os usuários insiram um número de porta.

Tempos limite do Citrix Gateway

Detalhes da decisão:

- Como você deseja configurar os tempos limite do Citrix Gateway para o tráfego do XenMobile?

Orientação de design:

O Citrix Gateway inclui as configurações Tempo limite da sessão e Tempo limite forçado. Para obter detalhes, consulte Configurações recomendadas. Lembre-se de que existem diferentes valores de tempo limite para serviços em segundo plano, Citrix ADC e para acessar aplicativos offline.

Endereço IP do balanceador de carga do XenMobile para MAM

Detalhes da decisão:

- Você está usando endereços IP internos ou externos para VIPs?

Orientação de design:

Em ambientes onde você pode usar endereços IP públicos para VIPs do Citrix Gateway, atribuir o VIP e o endereço de balanceamento de carga do XenMobile dessa maneira causa falhas de registro.

Certifique-se de que o VIP de balanceamento de carga use um IP interno para evitar falhas de registro neste cenário. Este endereço IP virtual deve seguir o padrão RFC 1918 de endereços IP privados. Se você usar um endereço IP não privado para este servidor virtual, o Citrix ADC não poderá contatar o XenMobile Server com sucesso durante o processo de autenticação. Para obter detalhes, consulte `<https://support.citrix.com/article/CTX200430>`.

Mecanismo de balanceamento de carga MDM

Detalhes da decisão:

- Como o Citrix Gateway fará o balanceamento de carga dos XenMobile Servers?

Orientação de design:

Use SSL Bridge se o XenMobile estiver na DMZ. Use SSL Offload, se necessário para atender aos padrões de segurança, quando o XenMobile estiver na rede interna.

- Quando você faz o balanceamento de carga do XenMobile Server com VIPs do Citrix ADC no modo SSL Bridge, o tráfego da Internet flui diretamente para o XenMobile Server, onde as conexões são encerradas. O modo SSL Bridge é o modo mais simples de configurar e solucionar problemas.
- Quando você faz o balanceamento de carga do XenMobile Server com VIPs do Citrix ADC no modo SSL Offload, o tráfego da Internet flui diretamente para o Citrix ADC, onde as conexões são encerradas. O Citrix ADC então estabelece novas sessões do Citrix ADC para o XenMobile Server. O modo SSL Offload envolve complexidade extra durante a configuração e a solução de problemas.

Porta de serviço para balanceamento de carga MDM com SSL Offload

Detalhes da decisão:

- Se você planeja usar o modo SSL Offload para Balanceamento de Carga, qual porta o serviço de back-end usará?

Orientação de design:

Para SSL Offload, escolha a porta 80 ou 8443 da seguinte forma:

- Use a porta 80 de volta para o XenMobile Server, para um verdadeiro offloading.

- A criptografia de ponta a ponta, ou seja, a recriptografia do tráfego, não é suportada. Para obter detalhes, consulte o artigo de suporte da Citrix, Arquiteturas Suportadas entre NetScaler e XenMobile Server.

FQDN de Inscrição

Detalhes da decisão:

- O que você planeja usar como FQDN para inscrição e VIP de instância/balanceamento de carga do XenMobile?

Orientação de design:

A configuração inicial do primeiro XenMobile Server em um cluster exige que você forneça o FQDN do XenMobile Server. Esse FQDN deve corresponder à sua URL VIP de MDM e à sua URL VIP de LB MAM Interno. (Um registro de endereço interno do Citrix ADC resolve o VIP de LB MAM.) Para obter detalhes, consulte "FQDN de registro para cada modo de gerenciamento" mais adiante neste artigo.

Além disso, você deve usar o mesmo certificado que os seguintes:

- Certificado de ouvinte SSL do XenMobile
- Certificado VIP de LB MAM Interno
- Certificado VIP de MDM (se estiver usando SSL Offload para VIP de MDM)

> **Importante:**

> Depois de configurar o FQDN de registro, você não poderá alterá-lo. Um novo FQDN de registro exige um novo banco de dados do SQL Server e a reconstrução do XenMobile Server.

Tráfego do Secure Web

Detalhes da decisão:

- Você planeja restringir o Secure Web apenas à navegação na web interna?
- Você planeja habilitar o Secure Web para navegação na web interna e externa?

Orientação de design:

Se você planeja usar o Secure Web apenas para navegação na web interna, a configuração do Citrix Gateway é simples. O Secure Web deve alcançar todos os sites internos por padrão. Pode ser necessário configurar firewalls e servidores proxy.

Se você planeja usar o Secure Web para navegação interna e externa, deve habilitar o SNIP para ter acesso à Internet de saída. A TI geralmente vê os dispositivos registrados (usando o contêiner MDX) como uma extensão da rede corporativa. Assim, a TI normalmente deseja que as conexões do Secure Web retornem ao Citrix ADC, passem por um servidor proxy e, em seguida, saiam para a Internet. Por padrão, o Secure Web usa um túnel VPN por aplicativo de volta à rede interna para todo o acesso à rede. O Citrix ADC usa configurações de túnel dividido.

Para uma discussão sobre as conexões do Secure Web, consulte Configurando conexões de usuário.

Notificações push para Secure Mail

Detalhes da decisão:

- Você planeja usar notificações push?

Orientação de design para iOS:

Sua configuração do Citrix Gateway pode incluir Secure Ticket Authority (STA), com tunelamento dividido desativado. O Citrix Gateway deve permitir o tráfego do Secure Mail para as URLs do serviço de escuta da Citrix especificadas em Notificações push para Secure Mail para iOS.

Orientação de design para Android:

Use o Firebase Cloud Messaging (FCM) para controlar como e quando os dispositivos Android precisam se conectar ao XenMobile. Com o FCM configurado, qualquer ação de segurança ou comando de implantação aciona uma notificação push para o Secure Hub para solicitar que o usuário se reconecte ao XenMobile Server.

STAs HDX™

Detalhes da decisão:

- Quais STAs usar se você planeja integrar o acesso a aplicativos HDX?

Orientação de design:

Os STAs HDX devem corresponder aos STAs no StoreFront e devem ser válidos para o farm do Virtual Apps and Desktops.

Citrix Files e ShareFile

Detalhes da decisão:

- Você planeja usar controladores de zona de armazenamento no ambiente?
- Qual URL VIP do Citrix Files você planeja usar?

Orientação de design:

Se você incluir controladores de zona de armazenamento em seu ambiente, certifique-se de configurar corretamente o seguinte:

- VIP de Switch do Citrix Files (usado pelo Plano de Controle do Citrix Files para se comunicar com os servidores do Controlador de zona de armazenamento)
- VIPs de Balanceamento de Carga do Citrix Files
- Todas as políticas e perfis necessários

Para obter informações, consulte a documentação do controlador de zonas de armazenamento.

IdP SAML

Detalhes da decisão:

- Se o SAML for necessário para o Citrix Files, você deseja usar o XenMobile como o IdP SAML?

Orientação de design:

A melhor prática recomendada é integrar o Citrix Files com o XenMobile Advanced Edition ou XenMobile Advanced Edition (On-premises) ou Citrix Endpoint Management (nuvem), uma alternativa mais simples para configurar a federação baseada em SAML. Ao usar o Citrix Files com essas edições do XenMobile, o XenMobile fornece ao Citrix Files:

- Autenticação de logon único (SSO) de usuários de aplicativos de produtividade móveis
- Provisionamento de contas de usuário baseado no Active Directory
- Políticas abrangentes de controle de acesso

O console do XenMobile permite que você realize a configuração do Citrix Files e monitore os níveis de serviço e o uso da licença.

Existem dois tipos de clientes do Citrix Files: clientes do Citrix Files para XenMobile (também conhecidos como Citrix Files empacotados) e clientes móveis do Citrix Files (também conhecidos

como Citrix Files não empacotados). Para entender as diferenças, consulte Como os clientes do Citrix Files para XenMobile diferem dos clientes móveis do Citrix Files.

Você pode configurar o XenMobile e o ShareFile para usar SAML para fornecer acesso SSO a:

- Aplicativos móveis do Citrix Files
- Clientes do Citrix Files não empacotados, como o site, o plug-in do Outlook ou clientes de sincronização

Para usar o XenMobile como o IdP SAML para o Citrix Files, certifique-se de que as configurações adequadas estejam em vigor. Para obter detalhes, consulte SAML para SSO com Citrix Files.

Conexões diretas do ShareConnect

Detalhes da decisão:

- Os usuários devem acessar um computador host a partir de um computador ou dispositivo móvel executando o ShareConnect usando conexões diretas?

Orientação de design:

O ShareConnect permite que os usuários se conectem com segurança aos seus computadores por meio de iPads, tablets Android e telefones Android para acessar seus arquivos e aplicativos. Para conexões diretas, o XenMobile usa o Citrix Gateway para fornecer acesso seguro a recursos fora da rede local. Para obter detalhes de configuração, consulte ShareConnect.

FQDN de registro para cada modo de gerenciamento

Modo de gerenciamento	**FQDN de registro**
Enterprise (MDM+MAM) com registro MDM obrigatório	FQDN do Servidor XenMobile
Enterprise (MDM+MAM) com registro MDM opcional	FQDN do Servidor XenMobile ou FQDN do Citrix Gateway
Somente MDM	FQDN do Servidor XenMobile
Somente MAM (legado)	FQDN do Citrix Gateway
Somente MAM	FQDN do Servidor XenMobile

Resumo da Implantação

A Citrix recomenda que você use o assistente do Citrix ADC para XenMobile para garantir a configuração adequada. Você pode usar o assistente apenas uma vez. Se você tiver várias instâncias do XenMobile, como para ambientes de teste, desenvolvimento e produção, você deve configurar o Citrix ADC para os ambientes adicionais manualmente. Quando você tiver um ambiente funcionando, anote as configurações antes de tentar configurar o Citrix ADC manualmente para o XenMobile.

A decisão principal que você toma ao usar o assistente é se deve usar HTTPS ou HTTP para a comunicação com o Servidor XenMobile. HTTPS fornece comunicação de back-end segura, pois o tráfego entre o Citrix ADC e o XenMobile é criptografado. A recriptografia afeta o desempenho do Servidor XenMobile. HTTP oferece melhor desempenho do Servidor XenMobile. O tráfego entre o Citrix ADC e o XenMobile não é criptografado. As tabelas a seguir mostram os requisitos de porta HTTP e HTTPS para o Citrix ADC e o Servidor XenMobile.

HTTPS

A Citrix geralmente recomenda o SSL Bridge para configurações de servidor virtual MDM do Citrix ADC. Para uso do SSL Offload do Citrix ADC com servidores virtuais MDM, o XenMobile suporta apenas a porta 80 como serviço de back-end.

Modo de gerenciamento	Método de balanceamento de carga do Citrix ADC	Re-criptografia SSL	Porta do servidor XenMobile
MDM	Ponte SSL	N/A	443, 8443
MAM	Descarregamento SSL	Ativado	8443
Empresarial	MDM: Ponte SSL	N/A	443, 8443
Empresarial	MAM: Descarregamento SSL	Ativado	8443

HTTP

Modo de gerenciamento	Método de balanceamento de carga do Citrix ADC	Recriptografia SSL	Porta do servidor XenMobile
MDM	Descarregamento SSL	Não suportado	80
MAM	Descarregamento SSL	Ativado	8443
Empresarial	MDM: Descarregamento SSL	Não suportado	80
Empresarial	MAM: Descarregamento SSL	Ativado	8443

Para diagramas do Citrix Gateway em implantações do XenMobile, consulte Arquitetura de Referência para Implantações Locais.

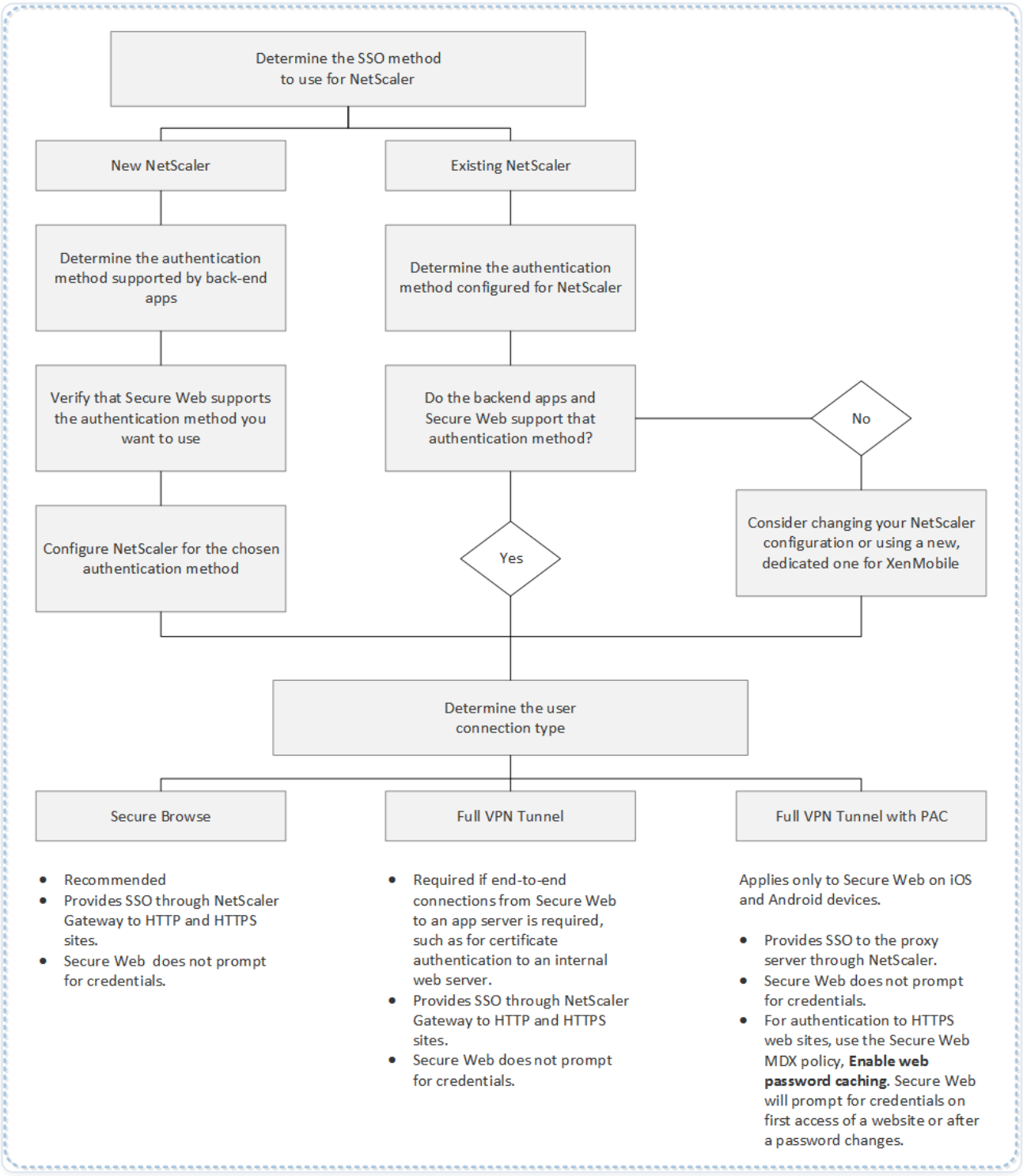
Considerações de SSO e Proxy para Aplicativos MDX

A integração do XenMobile com o Citrix ADC permite que você forneça aos usuários logon único (SSO) para todos os recursos de back-end HTTP/HTTPS. Dependendo dos seus requisitos de autenticação SSO, você pode configurar as conexões de usuário para um aplicativo MDX para usar uma destas opções:

- Navegação Segura, que é um tipo de VPN sem cliente
- Túnel VPN Completo

Se o Citrix ADC não for a melhor maneira de fornecer SSO em seu ambiente, você pode configurar um aplicativo MDX com cache de senha local baseado em política. Este artigo explora as várias opções de SSO e proxy com foco no Secure Web. Os conceitos se aplicam a outros aplicativos MDX.

O fluxograma a seguir resume o fluxo de decisão para SSO e conexões de usuário.



Métodos de Autenticação do Citrix ADC

Esta seção fornece informações gerais sobre os métodos de autenticação suportados pelo Citrix ADC.

Autenticação SAML

Ao configurar o Citrix ADC para Security Assertion Markup Language (SAML), os usuários podem se conectar a aplicativos web que suportam o protocolo SAML para logon único. O Citrix Gateway suporta o logon único do provedor de identidade (IdP) para aplicativos web SAML.

Configuração necessária:

- Configure o SAML SSO no perfil de tráfego do Citrix ADC.
- Configure o IdP SAML para o serviço solicitado.

Autenticação NTLM

Se o SSO para aplicativos web estiver ativado no perfil de sessão, o Citrix ADC executa a autenticação NTLM automaticamente.

Configuração necessária:

- Habilite o SSO no perfil de Sessão ou Tráfego do Citrix ADC.

Representação Kerberos

O XenMobile® oferece suporte a Kerberos apenas para o Secure Web. Ao configurar o Citrix ADC para SSO Kerberos, o Citrix ADC usa a representação quando uma senha de usuário está disponível para o Citrix ADC. Representação significa que o Citrix ADC usa as credenciais do usuário para obter o tíquete necessário para acessar serviços, como o Secure Web.

Configuração necessária:

- Configure a política de Sessão "Worx" do Citrix ADC para permitir que ela identifique o Realm Kerberos da sua conexão.
- Configure uma conta de Delegação Restrita de Kerberos (KCD) no Citrix ADC. Configure essa conta sem senha e vincule-a a uma política de tráfego no seu gateway XenMobile.
- Para esses e outros detalhes de configuração, consulte o blog da Citrix: WorxWeb e SSO de Representação Kerberos.

Delegação Restrita de Kerberos

O XenMobile oferece suporte a Kerberos apenas para o Secure Web. Ao configurar o Citrix ADC para SSO Kerberos, o Citrix ADC usa a delegação restrita quando uma senha de usuário não está disponível para o Citrix ADC.

Com a delegação restrita, o Citrix ADC usa uma conta de administrador especificada para obter tíquetes em nome de usuários e serviços.

Configuração necessária:

- Configure uma conta KCD no Active Directory com as permissões necessárias e uma conta KCD no Citrix ADC.

- Habilite o SSO no perfil de Tráfego do Citrix ADC.
- Configure o site de back-end para autenticação Kerberos.

Autenticação de Preenchimento de Formulário

Ao configurar o Citrix ADC para logon único baseado em formulário, os usuários podem fazer logon uma vez para acessar todos os aplicativos protegidos em sua rede. Esse método de autenticação se aplica a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Configure o SSO baseado em formulário no perfil de tráfego do Citrix ADC.

Autenticação HTTP Digest

Se você habilitar o SSO para aplicativos web no perfil de sessão, o Citrix ADC realizará a autenticação HTTP digest automaticamente. Esse método de autenticação se aplica a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Habilite o SSO no perfil de sessão ou tráfego do Citrix ADC.

Autenticação HTTP Básica

Se você habilitar o SSO para aplicativos web no perfil de sessão, o Citrix ADC realizará a autenticação HTTP básica automaticamente. Esse método de autenticação se aplica a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Habilite o SSO no perfil de sessão ou tráfego do Citrix ADC.

Secure Browse, Túnel VPN Completo ou Túnel VPN Completo com PAC

As seções a seguir descrevem os tipos de conexão de usuário para o Secure Web. Para obter mais informações, consulte este artigo do Secure Web na documentação da Citrix, Configurando conexões de usuário.

Túnel VPN Completo

As conexões que fazem túnel para a rede interna podem usar um túnel VPN completo. Use a política de modo VPN preferencial do Secure Web para configurar um túnel VPN completo. A Citrix recomenda o túnel VPN completo para conexões que usam certificados de cliente ou SSL de ponta a ponta para um recurso na rede interna. Um túnel VPN completo lida com qualquer

protocolo sobre TCP. Você pode usar um túnel VPN completo com dispositivos Windows, Mac, iOS e Android.

No modo de Túnel VPN Completo, o Citrix ADC não tem visibilidade dentro de uma sessão HTTPS.

Navegação Segura

As conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, conhecida como Navegação Segura. A Navegação Segura é a configuração padrão especificada para a política de **modo VPN preferencial** do Secure Web. A Citrix recomenda a Navegação Segura para conexões que exigem logon único (SSO).

No modo de Navegação Segura, o Citrix ADC divide a sessão HTTPS em duas partes:

- Do cliente para o Citrix ADC
- Do Citrix ADC para o servidor de recursos de back-end.

Dessa forma, o Citrix ADC tem visibilidade total de todas as transações entre o cliente e o servidor, permitindo que ele forneça SSO.

Você também pode configurar servidores proxy para o Secure Web quando usado no modo de navegação segura. Para obter detalhes, consulte o blog Tráfego do XenMobile WorxWeb por meio do servidor proxy no modo de navegação segura.

Túnel VPN Completo com PAC

Você pode usar um arquivo de Configuração Automática de Proxy (PAC) com uma implantação de túnel VPN completo para o Secure Web em dispositivos iOS e Android. O XenMobile oferece suporte à autenticação de proxy fornecida pelo Citrix ADC. Um arquivo PAC contém regras que definem como os navegadores da web selecionam um proxy para acessar um determinado URL. As regras do arquivo PAC podem especificar o tratamento para sites internos e externos. O Secure Web analisa as regras do arquivo PAC e envia as informações do servidor proxy para o Citrix Gateway. O Citrix Gateway não tem conhecimento do arquivo PAC ou do servidor proxy.

Para autenticação em sites HTTPS: A política MDX do Secure Web **Habilitar cache de senha da web** permite que o Secure Web autenticar e forneça SSO ao servidor proxy por meio do MDX.

Tunelamento Dividido do Citrix ADC

Ao planejar sua configuração de SSO e proxy, você também deve decidir se usará o tunelamento dividido do Citrix ADC. A Citrix recomenda que você use o tunelamento dividido do Citrix ADC somente se necessário. Esta seção fornece uma visão geral de como o tunelamento dividido

funciona: O Citrix ADC determina o caminho do tráfego com base em sua tabela de roteamento. Quando o tunelamento dividido do Citrix ADC está ativado, o Secure Hub distingue o tráfego de rede interno (protegido) do tráfego da Internet. O Secure Hub faz essa determinação com base no sufixo DNS e nos aplicativos da Intranet. O Secure Hub então tunela apenas o tráfego da rede interna através do túnel VPN. Quando o tunelamento dividido do Citrix ADC está desativado, todo o tráfego passa pelo túnel VPN.

- Se você preferir monitorar todo o tráfego devido a considerações de segurança, desative o tunelamento dividido do Citrix ADC. Como resultado, todo o tráfego passa pelo túnel VPN.
- Se você usar o Túnel VPN Completo com PAC, deverá desativar o tunelamento dividido do Citrix Gateway. Se o tunelamento dividido estiver ativado e você configurar um arquivo PAC, as regras do arquivo PAC substituirão as regras de tunelamento dividido do Citrix ADC. Um servidor proxy configurado em uma política de tráfego não substitui as regras de tunelamento dividido do Citrix ADC.

Por padrão, a política de **Acesso à rede** é definida como **Tunelado para a rede interna** para o Secure Web. Com essa configuração, os aplicativos MDX usam as configurações de tunelamento dividido do Citrix ADC. O padrão da política de **Acesso à rede** difere para alguns outros aplicativos de produtividade móvel.

O Citrix Gateway também possui um modo de tunelamento dividido reverso de micro VPN. Essa configuração suporta uma lista de exclusão de endereços IP que não são tunelados para o Citrix ADC. Em vez disso, esses endereços são enviados usando a conexão de internet do dispositivo. Para obter mais informações sobre o tunelamento dividido reverso, consulte a documentação do Citrix Gateway.

O XenMobile inclui uma **Lista de exclusão de tunelamento dividido reverso**. Para evitar que certos sites sejam tunelados através do Citrix Gateway: Adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou sufixos DNS que se conectam usando a LAN. Esta lista se aplica apenas ao modo Secure Browse com o Citrix Gateway configurado para tunelamento dividido reverso.

Autenticação

Em uma implantação do XenMobile®, várias considerações entram em jogo ao decidir como configurar a autenticação. Esta seção ajuda você a entender os vários fatores que afetam a autenticação, discutindo o seguinte:

- As principais políticas MDX, propriedades do cliente XenMobile e configurações do Citrix Gateway envolvidas na autenticação.

- As formas como essas políticas, propriedades do cliente e configurações interagem.
- As compensações de cada escolha.

Este artigo também inclui três exemplos de configurações recomendadas para graus crescentes de segurança.

De modo geral, uma segurança mais forte resulta em uma experiência de usuário menos otimizada, porque os usuários precisam se autenticar com mais frequência. Como você equilibra essas preocupações depende das necessidades e prioridades da sua organização. Ao revisar as três configurações recomendadas, você deve obter uma compreensão maior da interação das medidas de autenticação disponíveis e de como implantar melhor seu próprio ambiente XenMobile.

Modos de Autenticação

Autenticação online: Permite que os usuários acessem a rede XenMobile. Requer uma conexão com a Internet.

Autenticação offline: Ocorre no dispositivo. Os usuários desbloqueiam o cofre seguro e têm acesso offline a itens, como e-mails baixados, sites em cache e notas.

Métodos de Autenticação

FATOR ÚNICO

LDAP: Você pode configurar uma conexão no XenMobile para um ou mais diretórios, como o Active Directory, que é compatível com o Lightweight Directory Access Protocol (LDAP). Este é um método comumente usado para fornecer logon único (SSO) para ambientes corporativos. Você pode optar pelo PIN do Citrix com cache de senha do Active Directory para melhorar a experiência do usuário com LDAP, ao mesmo tempo em que oferece a segurança de senhas complexas no registro, expiração de senha e bloqueio de conta.

Para obter mais detalhes, consulte Domínio ou domínio mais STA.

Certificado de cliente: O XenMobile pode se integrar com autoridades de certificação padrão da indústria para usar certificados como o único método de autenticação online. O XenMobile fornece este certificado após o registro do usuário, o que requer uma senha única, URL de convite ou credenciais LDAP. Ao usar um certificado de cliente como método principal de autenticação, um PIN do Citrix é necessário em ambientes somente com certificado de cliente para proteger o certificado no dispositivo.

O XenMobile oferece suporte à Lista de Revogação de Certificados (CRL) apenas para uma Autoridade de Certificação de terceiros. Se você tiver uma CA da Microsoft configurada, o XenMobile usará o Citrix ADC para gerenciar a revogação. Ao configurar a autenticação baseada em certificado de cliente, considere se você precisa configurar a definição da Lista de Revogação de Certificados (CRL) do Citrix ADC, Habilitar Atualização Automática de CRL. Esta etapa garante que o usuário de um dispositivo no modo somente MAM não possa autenticar usando um certificado existente no dispositivo. O XenMobile reemite um novo certificado, pois não restringe um usuário de gerar um certificado de usuário se um for revogado. Essa configuração aumenta a segurança das entidades PKI quando a CRL verifica entidades PKI expiradas.

Para um diagrama que mostra a implantação necessária se você planeja usar autenticação baseada em certificado para usuários ou se você precisa usar sua Autoridade de Certificação (CA) corporativa para emitir certificados de dispositivo, consulte Arquitetura de Referência para Implantações Locais.

DOIS FATORES

LDAP + Certificado de Cliente: No ambiente XenMobile, essa configuração é a melhor combinação de segurança e experiência do usuário, com as melhores possibilidades de SSO acopladas à segurança fornecida pela autenticação de dois fatores no Citrix ADC. O uso de LDAP e certificados de cliente oferece segurança com algo que os usuários conhecem (suas senhas do Active Directory) e algo que eles têm (certificados de cliente em seus dispositivos). O Secure Mail (e alguns outros aplicativos de produtividade móvel) pode configurar e fornecer automaticamente uma experiência de usuário inicial perfeita com autenticação de certificado de cliente, com um ambiente de servidor de acesso de cliente Exchange configurado corretamente. Para usabilidade ideal, você pode combinar essa opção com o PIN do Citrix e o cache de senha do Active Directory.

LDAP + Token: Essa configuração permite a configuração clássica de credenciais LDAP, além de uma senha de uso único, usando o protocolo RADIUS. Para usabilidade ideal, você pode combinar essa opção com o PIN do Citrix e o cache de senha do Active Directory.

Políticas, Configurações e Propriedades de Cliente Importantes Envolvidas na Autenticação

As seguintes políticas, configurações e propriedades de cliente entram em jogo com as três configurações recomendadas a seguir:

Políticas MDX

Senha do aplicativo: Se **Ativado**, um PIN ou senha do Citrix é necessário para desbloquear o aplicativo quando ele inicia ou é retomado após um período de inatividade. O padrão é **Ativado**.

Para configurar o temporizador de inatividade para todos os aplicativos, defina o valor de INACTIVITY_TIMER em minutos no console do XenMobile em **Propriedades do Cliente** na guia **Configurações**. O padrão é 15 minutos. Para desativar o temporizador de inatividade, de modo que um prompt de PIN ou senha apareça apenas quando o aplicativo iniciar, defina o valor como zero.

> **Nota:**
>
> Se você selecionar Offline seguro para a política de chaves de criptografia, esta política será ativada automaticamente.

> **Sessão online necessária:** Se **Ativado**, o usuário deve ter uma conexão com a rede corporativa e uma sessão ativa para acessar o aplicativo no dispositivo. Se **Desativado**, uma sessão ativa não é necessária para acessar o aplicativo no dispositivo. O padrão é **Desativado**.

Período máximo offline (horas): Define o período máximo que um aplicativo pode ser executado sem reconfirmar o direito do aplicativo e atualizar as políticas do XenMobile. Ao definir o Período máximo offline, se o Secure Hub para iOS tiver um token Citrix Gateway válido, o aplicativo recuperará novas políticas para aplicativos MDX do XenMobile sem qualquer interrupção para os usuários. Se o Secure Hub não tiver um token Citrix ADC válido, os usuários devem autenticar através do Secure Hub para que as políticas do aplicativo sejam atualizadas. O token Citrix ADC pode se tornar inválido devido à inatividade da sessão do Citrix Gateway ou a uma política de tempo limite de sessão forçada. Quando os usuários fazem login no Secure Hub novamente, eles podem continuar executando o aplicativo.

Os usuários são lembrados de fazer login 30, 15 e 5 minutos antes do período expirar. Após a expiração, o aplicativo é bloqueado até que os usuários façam login. O padrão é **72 horas (3 dias)**. O período mínimo é de 1 hora.

> **Nota:**
>
> Tenha em mente que, em um cenário em que os usuários viajam com frequência e podem usar roaming internacional, o padrão de 72 horas (3 dias) pode ser muito curto.

> **Expiração do tíquete de serviços em segundo plano:** O período de tempo durante o qual um tíquete de serviço de rede em segundo plano permanece válido. Quando o Secure Mail se conecta através do Citrix Gateway a um servidor Exchange executando o ActiveSync, o XenMobile emite um token que o Secure Mail usa para se conectar ao servidor Exchange interno. Essa configuração de propriedade determina a duração durante a qual o Secure Mail pode usar o token sem exigir um novo token para autenticação e a conexão com o servidor Exchange. Quando o limite de tempo expira, os usuários devem fazer logon novamente para gerar um novo token. O padrão é de **168 horas (7 dias)**. Quando esse tempo limite expira, as notificações de e-mail são interrompidas.

Período de carência exigido para sessão online: Determina quantos minutos um usuário pode usar o aplicativo offline antes que a política de sessão online exigida o impeça de continuar o uso (até que a sessão online seja validada). O padrão é 0 (sem período de carência).

Para obter informações sobre políticas de autenticação, consulte:

- Se você usa o MAM SDK: Visão geral do MAM SDK
- Se você usa o MDX Toolkit: Políticas MDX para iOS e Políticas MDX para Android

Propriedades do cliente XenMobile

> **Nota:**

> As propriedades do cliente são uma configuração global que se aplica a todos os dispositivos que se conectam ao XenMobile.

> **PIN do Citrix:** Para uma experiência de logon simples, você pode optar por habilitar o PIN do Citrix. Com o PIN, os usuários não precisam inserir outras credenciais repetidamente, como seus nomes de usuário e senhas do Active Directory. Você pode configurar o PIN do Citrix como uma autenticação offline autônoma apenas, ou combinar o PIN com o cache de senha do Active Directory para simplificar a autenticação para usabilidade ideal. Você configura o PIN do Citrix em **Configurações > Cliente > Propriedades do Cliente** no console do XenMobile.

A seguir, um resumo de algumas propriedades importantes. Para obter mais informações, consulte Propriedades do cliente.

ENABLE_PASSCODE_AUTH

Nome de exibição: Habilitar autenticação de PIN do Citrix

Essa chave permite ativar a funcionalidade do PIN do Citrix. Com o PIN ou senha do Citrix, os usuários são solicitados a definir um PIN para usar em vez de sua senha do Active Directory. Você deve habilitar essa configuração se **ENABLE_PASSWORD_CACHING** estiver habilitado ou se o XenMobile estiver usando autenticação de certificado.

Valores possíveis: verdadeiro ou **falso**

Valor padrão: falso

ENABLE_PASSWORD_CACHING

Nome de exibição: Habilitar Cache de Senha do Usuário

Esta chave permite que a senha do Active Directory dos usuários seja armazenada em cache localmente no dispositivo móvel. Quando você define esta chave como verdadeiro, os usuários são solicitados a definir um PIN ou senha Citrix. A chave **ENABLE_PASSCODE_AUTH** deve ser definida como verdadeiro quando você define esta chave como **verdadeiro**.

Valores possíveis: verdadeiro ou **falso**

Valor padrão: falso

PASSCODE_STRENGTH

Nome de exibição: Requisito de Força do PIN

Esta chave define a força do PIN ou senha Citrix. Quando você altera esta configuração, os usuários são solicitados a definir um novo PIN ou senha Citrix na próxima vez que forem solicitados a autenticar.

Valores possíveis: Baixo, **Médio** ou **Forte**

Valor padrão: Médio

INACTIVITY_TIMER

Nome de exibição: Temporizador de inatividade

Esta chave define o tempo em minutos que os usuários podem deixar seus dispositivos inativos e, em seguida, acessar um aplicativo sem serem solicitados a fornecer um PIN ou senha Citrix. Para habilitar esta configuração para um aplicativo MDX, você deve definir a configuração **App Passcode** como **Ativado**. Se a configuração **App Passcode** for definida como **Desativado**, os

usuários são redirecionados para o Secure Hub para realizar uma autenticação completa. Quando você altera esta configuração, o valor entra em vigor na próxima vez que os usuários forem solicitados a autenticar. O padrão é 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nome de exibição: Habilitar Autenticação por Touch ID

Permite o uso do leitor de impressão digital (somente no iOS) para autenticação offline. A autenticação online ainda requer o método de autenticação primário.

ENCRYPT_SECRETS_USING_PASSCODE

Nome de exibição: Criptografar segredos usando Senha

Esta chave permite que dados confidenciais sejam armazenados no dispositivo móvel em um cofre secreto, em vez de em um armazenamento nativo baseado em plataforma, como o chaveiro do iOS. Esta chave de configuração permite uma criptografia forte de artefatos de chave, mas também adiciona entropia do usuário (um código PIN aleatório gerado pelo usuário que somente o usuário conhece).

Valores possíveis: verdadeiro ou **falso**

Valor padrão: falso

Configurações do Citrix ADC

Tempo limite de sessão: Se você habilitar esta configuração, o Citrix Gateway desconectará a sessão se o Citrix ADC não detectar atividade de rede durante o intervalo especificado. Essa configuração é aplicada a usuários que se conectam com o Plug-in do Citrix Gateway, Citrix Receiver™, Secure Hub ou por meio de um navegador da web. O padrão é **1440 minutos**. Se você definir esse valor como zero, a configuração será desabilitada.

Tempo limite forçado: Se você habilitar esta configuração, o Citrix Gateway desconectará a sessão após o término do intervalo de tempo limite, independentemente do que o usuário esteja fazendo. Quando o intervalo de tempo limite expira, não há ação que o usuário possa tomar para evitar a desconexão. Essa configuração é aplicada a usuários que se conectam com o Plug-in do Citrix Gateway, Citrix Receiver, Secure Hub ou por meio de um navegador da web. Se o Secure Mail estiver usando STA, um modo especial do Citrix ADC, a configuração de **Tempo limite forçado** não se aplica às sessões do Secure Mail. O padrão é **1440 minutos**. Se você deixar este valor em branco, a configuração será desabilitada.

Para obter mais informações sobre as configurações de tempo limite no Citrix Gateway, consulte a documentação do Citrix ADC.

Para obter mais informações sobre os cenários que solicitam aos usuários que autenticar com o XenMobile inserindo credenciais em seus dispositivos, consulte Cenários de Solicitação de Autenticação.

Configurações de configuração padrão

Essas configurações são os padrões fornecidos por:

- Assistente NetScaler® para XenMobile
- MAM SDK ou MDX Toolkit
- Console do XenMobile

CONFIGURAÇÃO	ONDE ENCONTRAR A CONFIGURAÇÃO	CONFIGURAÇÃO PADRÃO
Tempo limite da sessão	Citrix Gateway	1440 minutos
Forçar tempo limite	Citrix Gateway	1440 minutos
Período máximo offline	Políticas MDX	72 horas
Expiração do tíquete de serviços em segundo plano	Políticas MDX	168 horas (7 dias)
Sessão online necessária	Políticas MDX	Desativado
Período de carência para sessão online necessária	Políticas MDX	0
Senha do aplicativo	Políticas MDX	Ativado
Criptografar segredos usando senha	Propriedades do cliente XenMobile	falso
Habilitar Autenticação PIN do Citrix	Propriedades do cliente XenMobile	falso
Requisito de Força do PIN	Propriedades do cliente XenMobile	Médio

CONFIGURAÇÃO	ONDE ENCONTRAR A CONFIGURAÇÃO	CONFIGURAÇÃO PADRÃO
Tipo de PIN	Propriedades do cliente XenMobile	Numérico
Habilitar Cache de Senha do Usuário	Propriedades do cliente XenMobile	falso
Temporizador de Inatividade	Propriedades do cliente XenMobile	15
Habilitar Autenticação Touch ID	Propriedades do cliente XenMobile	falso

Configurações Recomendadas

Esta seção apresenta exemplos de três configurações do XenMobile que variam da segurança mais baixa e experiência de usuário ideal à segurança mais alta e experiência de usuário mais intrusiva. Esses exemplos devem fornecer pontos de referência úteis para determinar onde na escala você deseja posicionar sua própria configuração. A modificação dessas configurações pode exigir que você altere outras configurações também. Por exemplo, o período offline máximo deve ser sempre menor que o tempo limite da sessão.

Segurança Mais Alta

Esta configuração oferece o mais alto nível de segurança, mas contém compensações significativas de usabilidade.

Configuração	**Onde Encontrar a Configuração**	**Configuração Recomendada**	**Impacto no Comportamento**
Tempo limite da sessão	Citrix Gateway	1440	Os usuários inserem suas credenciais do Secure Hub somente quando a autenticação online é necessária — a cada 24 horas.
Forçar tempo limite	Citrix Gateway	1440	A autenticação online é estritamente

			exigida a cada 24 horas. A atividade não estende a vida útil da sessão.
Período offline máximo	Políticas MDX	23	Exige atualização da política todos os dias.
Expiração do tíquete de serviços em segundo plano	Políticas MDX	72 horas	Tempo limite para STA, o que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, tornar o tempo limite do STA maior do que o tempo limite da sessão evita que as notificações de e-mail parem sem avisar o usuário caso ele não abra o aplicativo antes que a sessão expire.
Sessão online exigida	Políticas MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de carência exigido para sessão online	Políticas MDX	0	Sem período de carência (se você ativou a Sessão Online exigida).
Senha do aplicativo	Políticas MDX	Ativado	Exigir uma senha para o aplicativo.

Criptografar segredos usando senha	Propriedades do cliente XenMobile	verdadeiro	Uma chave derivada da entropia do usuário protege o cofre.
Habilitar Autenticação PIN do Citrix	Propriedades do cliente XenMobile	verdadeiro	Habilite o PIN do Citrix para uma experiência de autenticação simplificada.
Requisito de Força do PIN	Propriedades do cliente XenMobile	Forte	Altos requisitos de complexidade de senha.
Tipo de PIN	Propriedades do cliente XenMobile	Alfanumérico	O PIN é uma sequência alfanumérica.
Habilitar Cache de Senha	Propriedades do cliente XenMobile	falso	A senha do Active Directory não é armazenada em cache e o PIN do Citrix é usado para autenticações offline.
Temporizador de Inatividade	Propriedades do cliente XenMobile	15	Se o usuário não usar aplicativos MDX ou Secure Hub durante este período, solicite autenticação offline.
Habilitar Autenticação Touch ID	Propriedades do cliente XenMobile	falso	Desabilita o Touch ID para casos de uso de autenticação offline no iOS.

Maior Segurança

Uma abordagem mais intermediária, esta configuração exige que os usuários se autenticarm com mais frequência — a cada 3 dias, no máximo, em vez de 7 — e oferece segurança mais forte. O

aumento do número de autenticações bloqueia o contêiner com mais frequência, garantindo a segurança dos dados quando os dispositivos não estão em uso.

Configuração	Onde Encontrar a Configuração	Configuração Recomendada	Impacto no Comportamento
Tempo limite da sessão	Citrix Gateway	4320	Os usuários inserem suas credenciais do Secure Hub somente quando a autenticação online é necessária - a cada 3 dias.
Forçar tempo limite	Citrix Gateway	Nenhum valor	As sessões são estendidas se houver alguma atividade.
Período máximo offline	Políticas MDX	71	Requer atualização da política a cada 3 dias. A diferença de uma hora é para permitir a atualização antes do tempo limite da sessão.
Expiração do tíquete de serviços em segundo plano	Políticas MDX	168 horas	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, tornar o tempo limite do STA maior do que o tempo limite da sessão evita que as notificações de e-mail parem sem avisar o usuário se

			ele não abrir o aplicativo antes que a sessão expire.
Sessão online necessária	Políticas MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de carência necessário para sessão online	Políticas MDX	0	Nenhum período de carência (se você ativou a Sessão Online necessária).
Senha do aplicativo	Políticas MDX	Ativado	Exigir uma senha para o aplicativo.
Criptografar segredos usando senha	Propriedades do cliente XenMobile	falso	Não exigir entropia do usuário para criptografar o cofre.
Habilitar Autenticação por PIN do Citrix	Propriedades do cliente XenMobile	verdadeiro	Habilita o PIN do Citrix para uma experiência de autenticação simplificada.
Requisito de Força do PIN	Propriedades do cliente XenMobile	Médio	Impõe regras de complexidade de senha média.
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	Um PIN é uma sequência numérica.
Habilitar Cache de Senha	Propriedades do cliente XenMobile	verdadeiro	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Temporizador de Inatividade	Propriedades do cliente XenMobile	30	Se o usuário não usar aplicativos MDX ou Secure Hub

			durante este período, solicite autenticação offline.
Habilitar Autenticação Touch ID	Propriedades do cliente XenMobile	verdadeiro	Habilita o Touch ID para casos de uso de autenticação offline no iOS.

Alta Segurança

Esta configuração, a mais conveniente para os usuários, oferece segurança de nível básico.

Configuração	Onde Encontrar a Configuração	Configuração Recomendada	Impacto no Comportamento
Tempo limite da sessão	Citrix Gateway	10080	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação online é necessária - a cada 7 dias.
Forçar tempo limite	Citrix Gateway	Nenhum valor	As sessões são estendidas se houver alguma atividade.
Período offline máximo	Políticas MDX	167	Requer atualização da política toda semana (a cada 7 dias). A diferença de uma hora é para permitir a atualização antes do tempo limite da sessão.

Expiração do tíquete de serviços em segundo plano	Políticas MDX	240	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, tornar o tempo limite do STA maior que o tempo limite da sessão evita que as notificações de e-mail parem sem avisar o usuário se ele não abrir o aplicativo antes que a sessão expire.
Sessão online necessária	Políticas MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de carência para sessão online necessária	Políticas MDX	0	Sem período de carência (se você ativou a Sessão Online necessária).
Senha do aplicativo	Políticas MDX	Ativado	Exigir uma senha para o aplicativo.
Criptografar segredos usando senha	Propriedades do cliente XenMobile	falso	Não exigir entropia do usuário para criptografar o cofre.
Habilitar Autenticação por PIN Citrix	Propriedades do cliente XenMobile	verdadeiro	Habilitar PIN Citrix para uma experiência de autenticação simplificada.

Requisito de Força do PIN	Propriedades do cliente XenMobile	Baixo	Sem requisitos de complexidade de senha
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	Um PIN é uma sequência numérica.
Habilitar Cache de Senha	Propriedades do cliente XenMobile	verdadeiro	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Temporizador de Inatividade	Propriedades do cliente XenMobile	90	Se o usuário não usar aplicativos MDX ou Secure Hub durante este período, solicite autenticação offline.
Habilitar Autenticação Touch ID	Propriedades do cliente XenMobile	verdadeiro	Habilita o Touch ID para casos de uso de autenticação offline no iOS.

Usando Autenticação Step-Up

Alguns aplicativos podem exigir autenticação aprimorada (por exemplo, um fator de autenticação secundário, como um token ou tempos limite de sessão agressivos). Você controla esse método de autenticação por meio de uma política MDX. O método também requer um servidor virtual separado para controlar os métodos de autenticação (no mesmo ou em appliances Citrix ADC separados).

CONFIGURAÇÃO	ONDE ENCONTRAR A CONFIGURAÇÃO	CONFIGURAÇÃO RECOMENDADA	IMPACTO NO COMPORTAMENTO
Citrix Gateway Alternativo	Políticas MDX	Requer o FQDN e a porta do dispositivo Citrix ADC secundário.	Permite autenticação aprimorada controlada pelas políticas de autenticação e sessão do

CONFIGURAÇÃO	ONDE ENCONTRAR A CONFIGURAÇÃO	CONFIGURAÇÃO RECOMENDADA	IMPACTO NO COMPORTAMENTO
			dispositivo Citrix ADC secundário.

Se um usuário abrir um aplicativo que faz logon na instância alternativa do Citrix Gateway, todos os outros aplicativos usarão essa instância do Citrix Gateway para se comunicar com a rede interna. A sessão só retorna para a instância do Citrix Gateway de segurança inferior quando a sessão expira da instância do Citrix Gateway com segurança aprimorada.

Usando Sessão Online Necessária

Para certos aplicativos, como o Secure Web, você pode querer garantir que os usuários executem um aplicativo apenas quando tiverem uma sessão autenticada e enquanto o dispositivo estiver conectado a uma rede. Esta política impõe essa opção e permite um período de carência para que os usuários possam concluir seu trabalho.

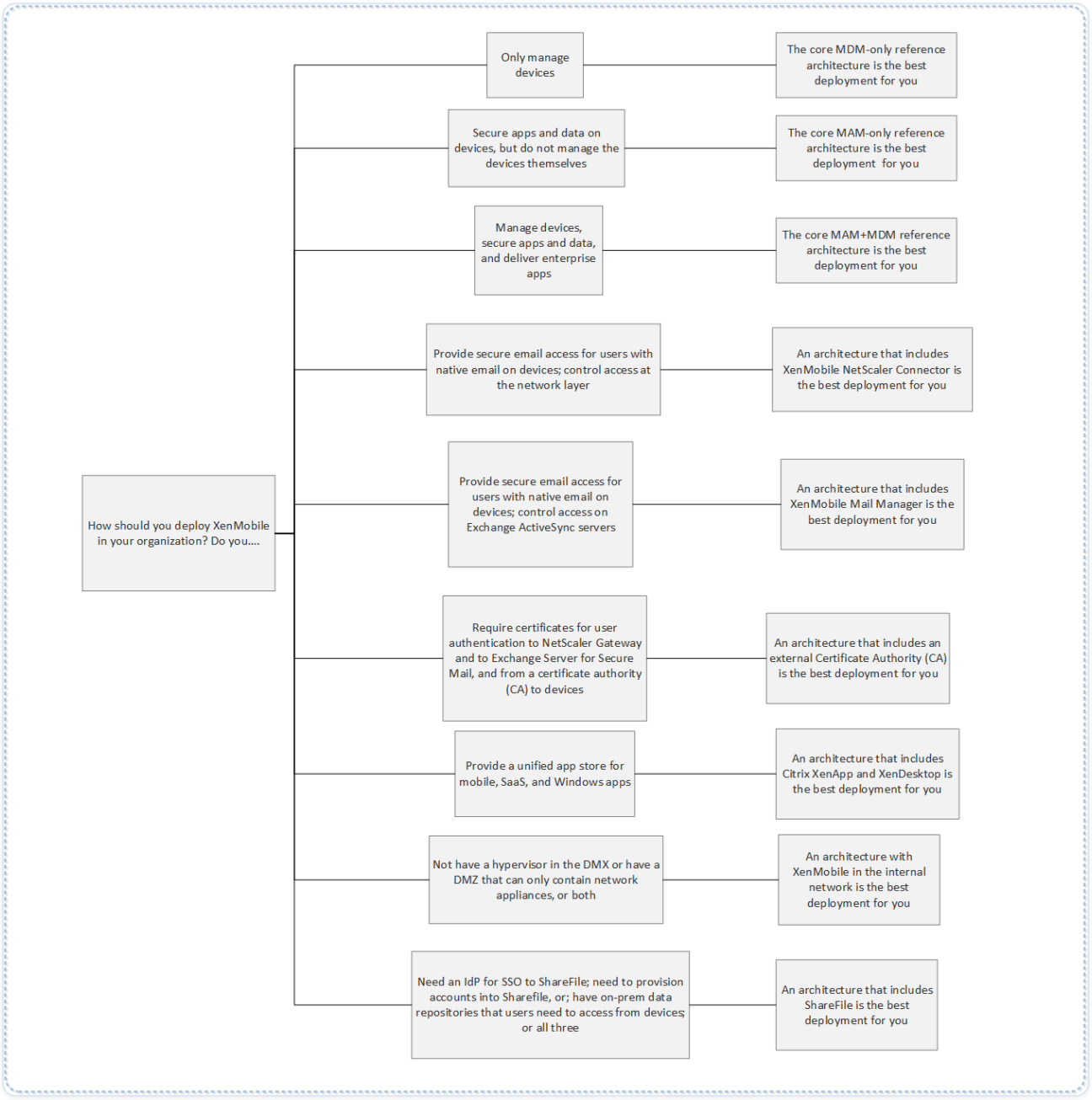
CONFIGURAÇÃO	ONDE ENCONTRAR A CONFIGURAÇÃO	CONFIGURAÇÃO RECOMENDADA	IMPACTO NO COMPORTAMENTO
Sessão online necessária	Políticas MDX	Ativado	Garante que o dispositivo esteja online e tenha um token de autenticação válido.
Período de carência da sessão online obrigatória	Políticas MDX	15	Permite um período de carência de 15 minutos antes que o usuário não possa mais usar os aplicativos

Arquitetura de Referência para Implantações Locais

As figuras neste artigo ilustram as arquiteturas de referência para a implantação do XenMobile localmente. Os cenários de implantação incluem MDM-only, MAM-only e MDM+MAM como as arquiteturas principais, e aqueles que incluem componentes, como o SNMP Manager, Citrix Gateway connector™ para Exchange ActiveSync, Endpoint Management connector para

Exchange ActiveSync e Virtual Apps and Desktops. As figuras mostram os componentes mínimos necessários para o XenMobile.

Use este gráfico como um guia geral para suas decisões de implantação.

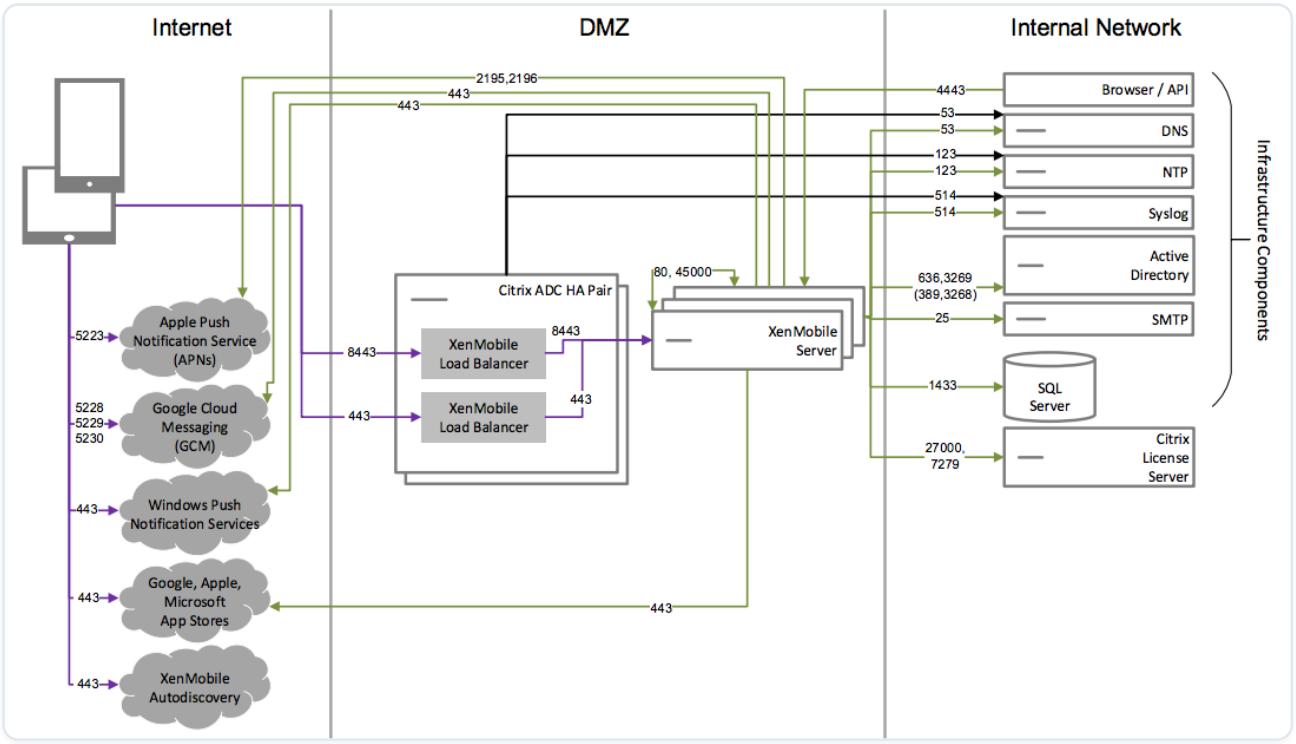


Nas figuras, os números nos conectores representam portas que você deve abrir para permitir conexões entre os componentes. Para uma lista completa de portas, consulte Requisitos de porta na documentação do XenMobile.

Arquitetura de Referência Principal Somente MDM

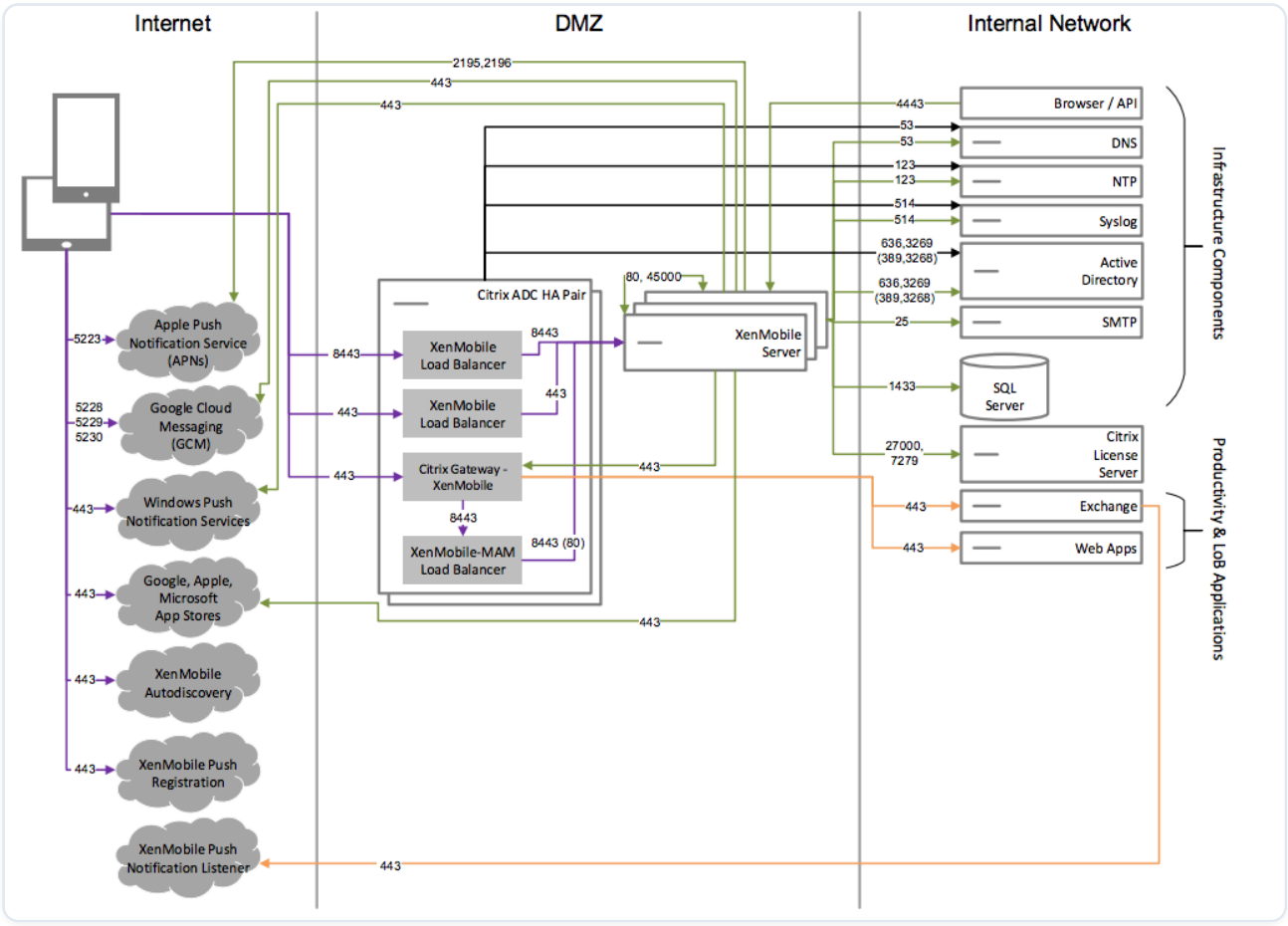
Implante esta arquitetura se você planeja usar apenas os recursos de MDM do XenMobile. Por exemplo, você precisa gerenciar um dispositivo corporativo por meio de MDM para implantar

políticas de dispositivo, aplicativos e para recuperar inventários de ativos e ser capaz de realizar ações em dispositivos, como uma limpeza de dispositivo.



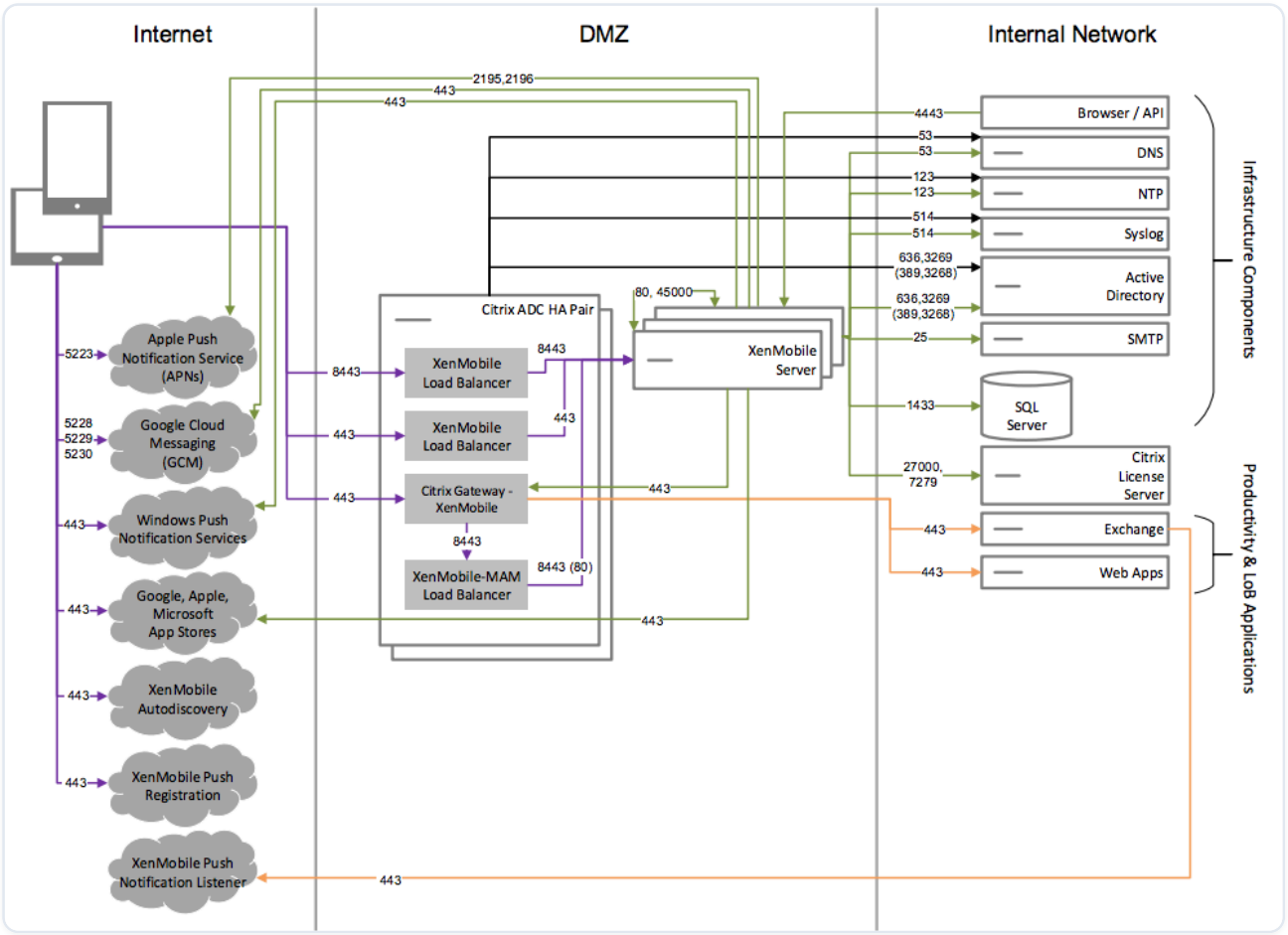
Arquitetura de Referência Principal Somente MAM

Implante esta arquitetura se você planeja usar apenas os recursos de MAM do XenMobile sem que os dispositivos se registrem para MDM. Por exemplo, você deseja proteger aplicativos e dados em dispositivos móveis BYO; você deseja entregar aplicativos móveis corporativos e pode bloquear aplicativos e limpar seus dados. Os dispositivos não podem ser registrados no MDM.



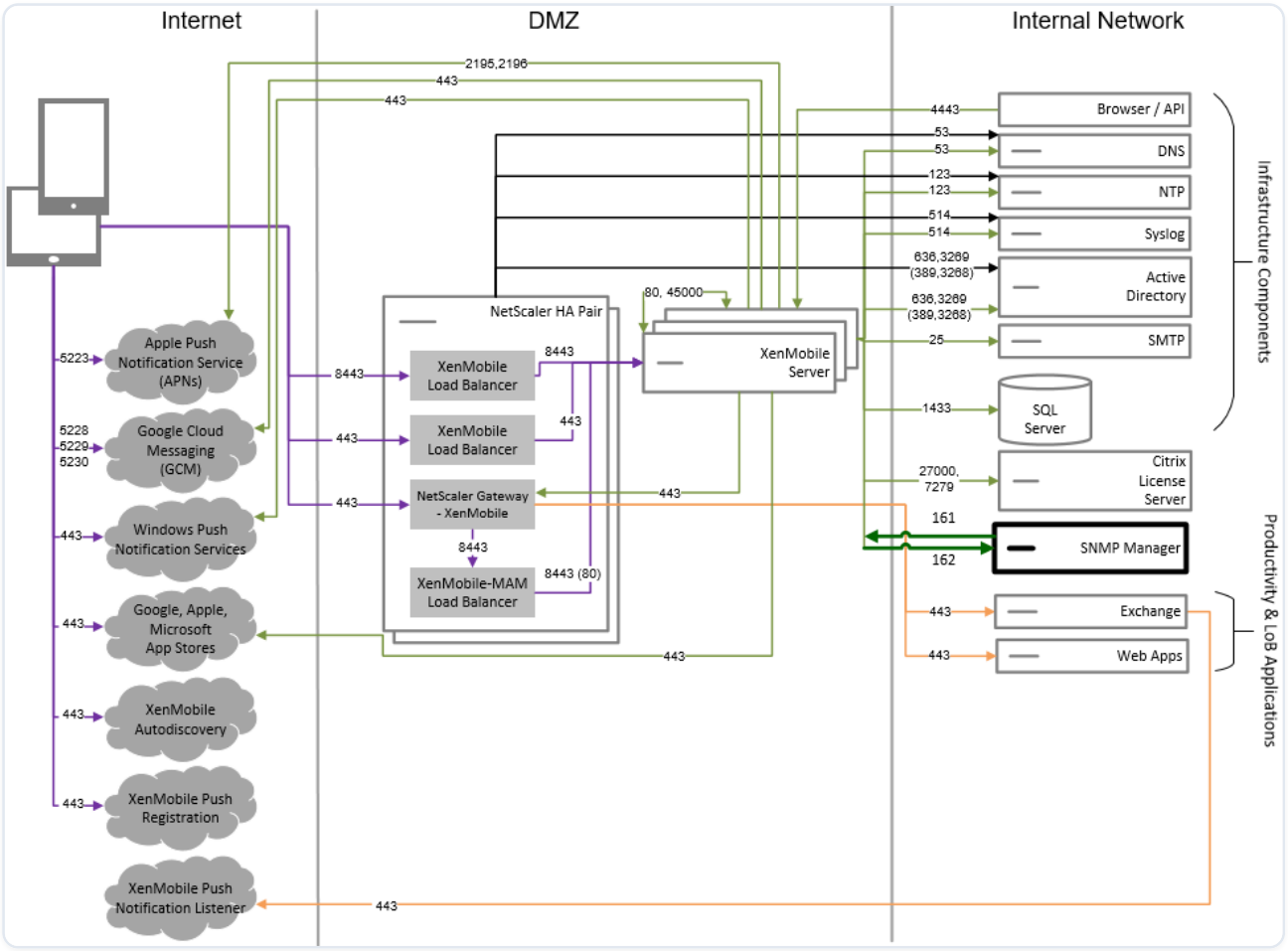
Arquitetura de Referência Principal MAM+MDM

Implante esta arquitetura se você planeja usar os recursos de MDM+MAM do XenMobile. Por exemplo, você deseja gerenciar um dispositivo corporativo via MDM; você deseja implantar políticas de dispositivo e aplicativos, recuperar um inventário de ativos e pode limpar dispositivos. Você também deseja entregar aplicativos móveis corporativos e pode bloquear aplicativos e limpar os dados nos dispositivos.



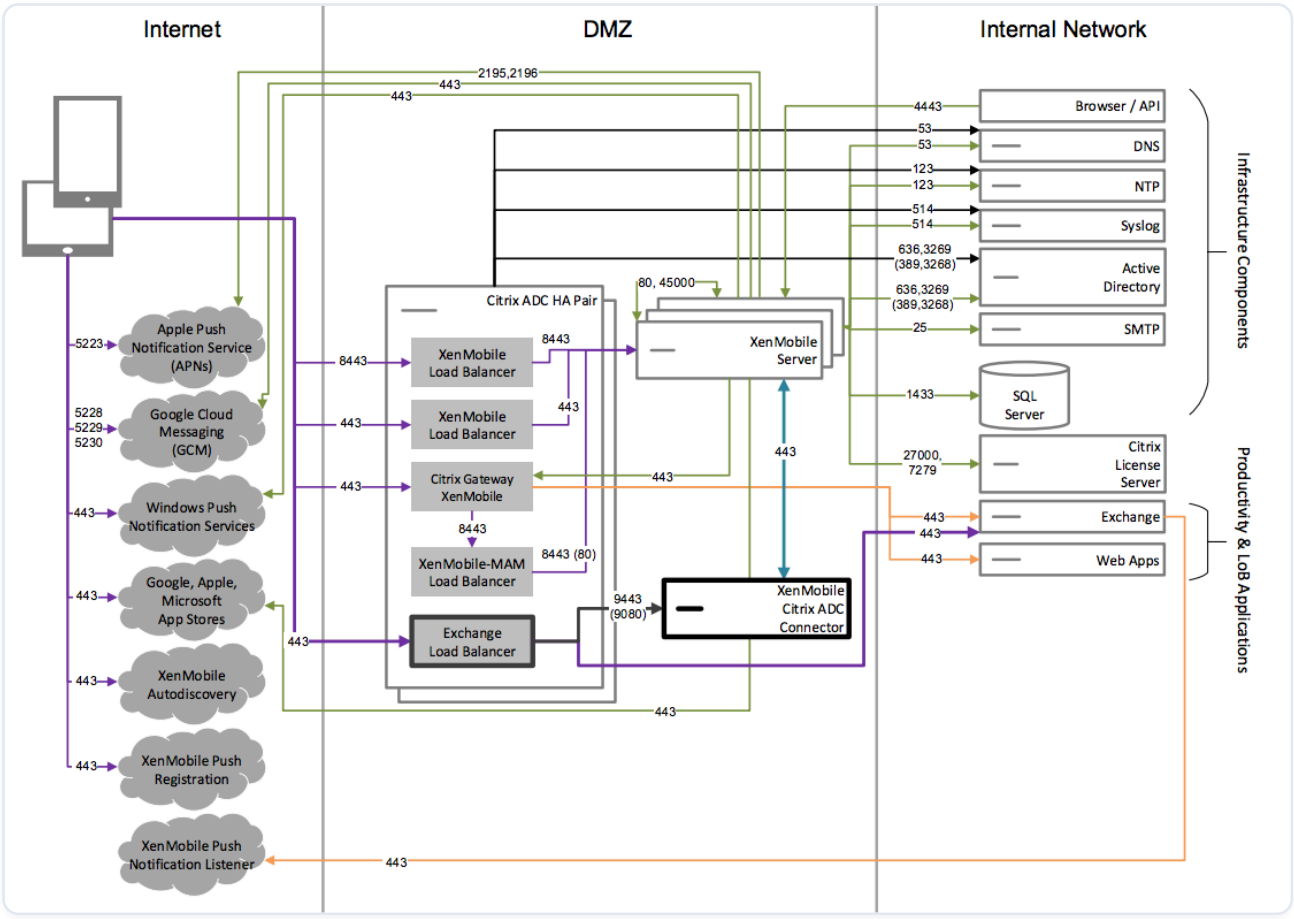
Arquitetura de Referência com SNMP

Implante esta arquitetura se você planeja habilitar o monitoramento SNMP com o XenMobile. Por exemplo, você deseja permitir que os sistemas de monitoramento consultem e obtenham informações sobre seus nós XenMobile. Para obter mais informações, consulte Monitoramento SNMP.



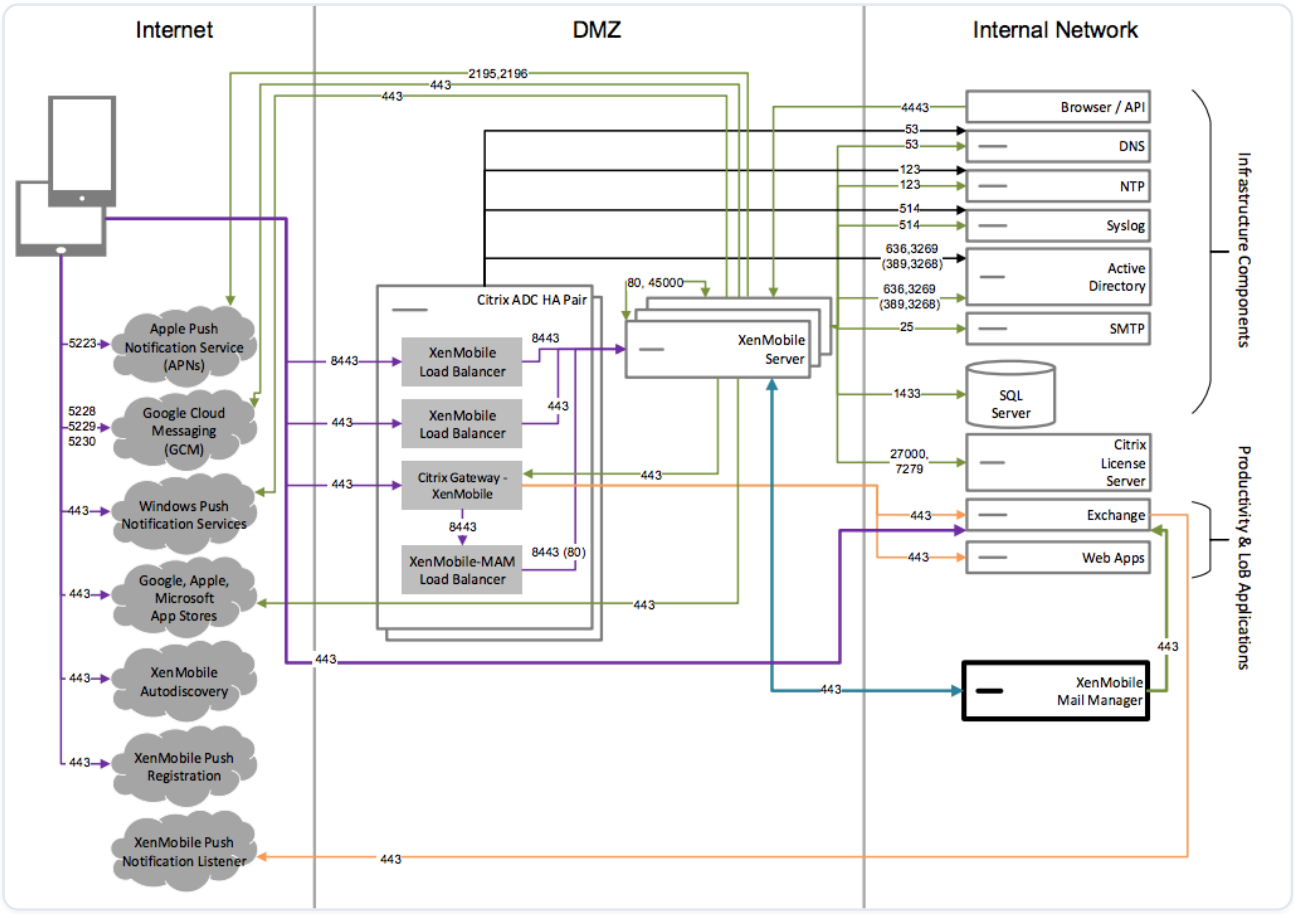
Arquitetura de Referência com conector Citrix Gateway para Exchange ActiveSync

Implante esta arquitetura se você planeja usar o conector Citrix Gateway para Exchange ActiveSync com o XenMobile. Por exemplo, você precisa fornecer acesso seguro a e-mail para usuários que usam aplicativos de e-mail móveis nativos. Esses usuários continuarão acessando o e-mail por meio de um aplicativo nativo ou você pode fazer a transição deles ao longo do tempo para o Citrix Secure Mail. O controle de acesso precisa ocorrer na camada de rede antes que o tráfego atinja os servidores Exchange ActiveSync. Embora o diagrama mostre o conector para Exchange ActiveSync implantado em uma arquitetura MDM e MAM, você também pode implantar o conector para Exchange ActiveSync da mesma forma como parte de uma arquitetura somente MDM.



Arquitetura de Referência com conector Endpoint Management para Exchange ActiveSync

Implante esta arquitetura se você planeja usar o conector Endpoint Management para Exchange ActiveSync com o XenMobile. Por exemplo, você deseja fornecer acesso seguro a e-mail para usuários que usam aplicativos de e-mail móveis nativos. Esses usuários continuarão acessando o e-mail por meio de um aplicativo nativo ou você pode fazer a transição dos usuários ao longo do tempo para o Secure Mail. Você pode obter controle de acesso nos servidores Exchange ActiveSync. Embora o diagrama mostre o conector Endpoint Management para Exchange ActiveSync implantado em uma arquitetura MDM e MAM, você também pode implantar o conector Endpoint Management para Exchange ActiveSync da mesma forma como parte de uma arquitetura somente MDM.

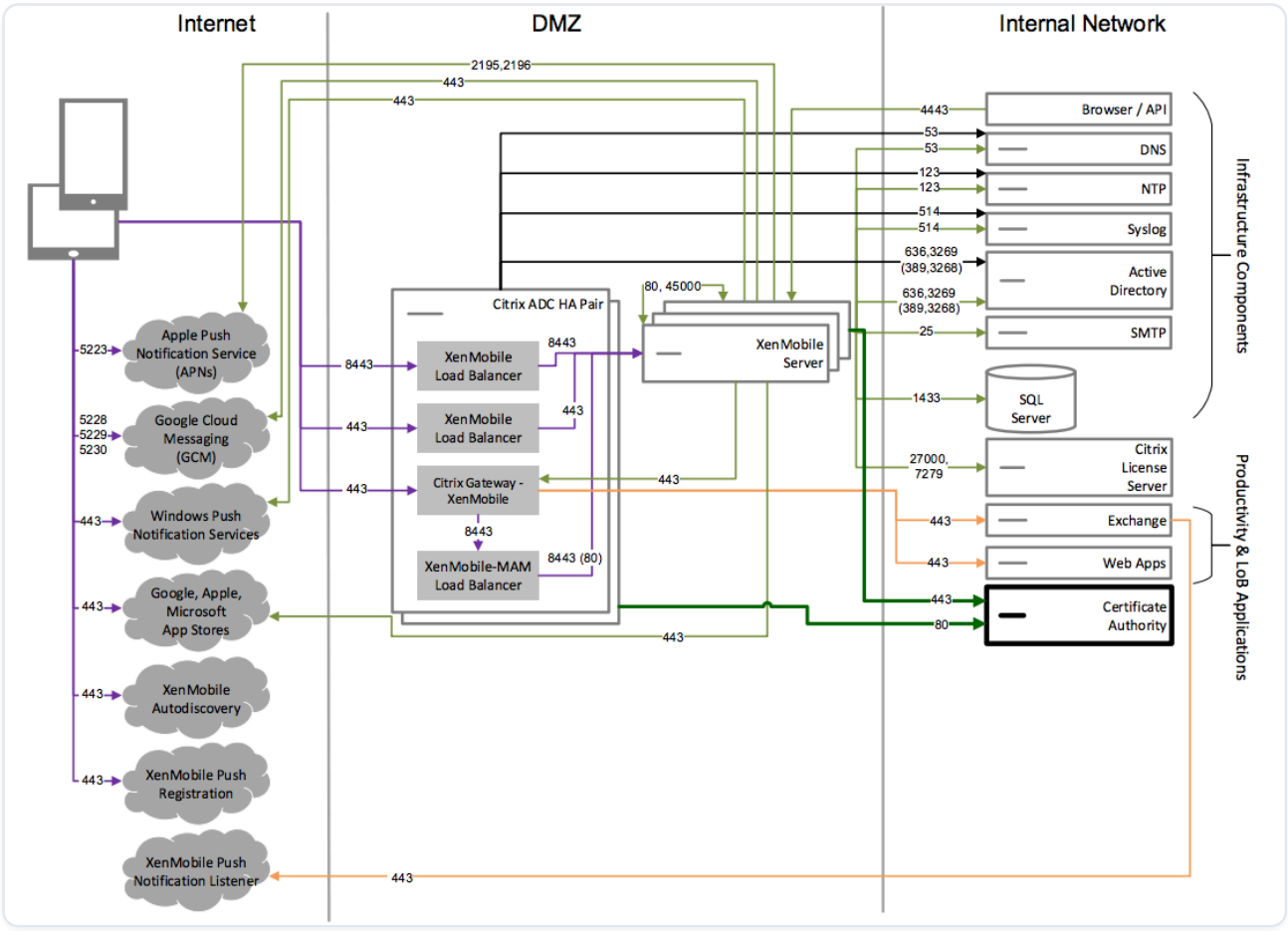


Arquitetura de Referência com Autoridade Certificadora Externa

Uma implantação que inclui uma autoridade certificadora externa é recomendada para atender a um ou mais dos seguintes requisitos:

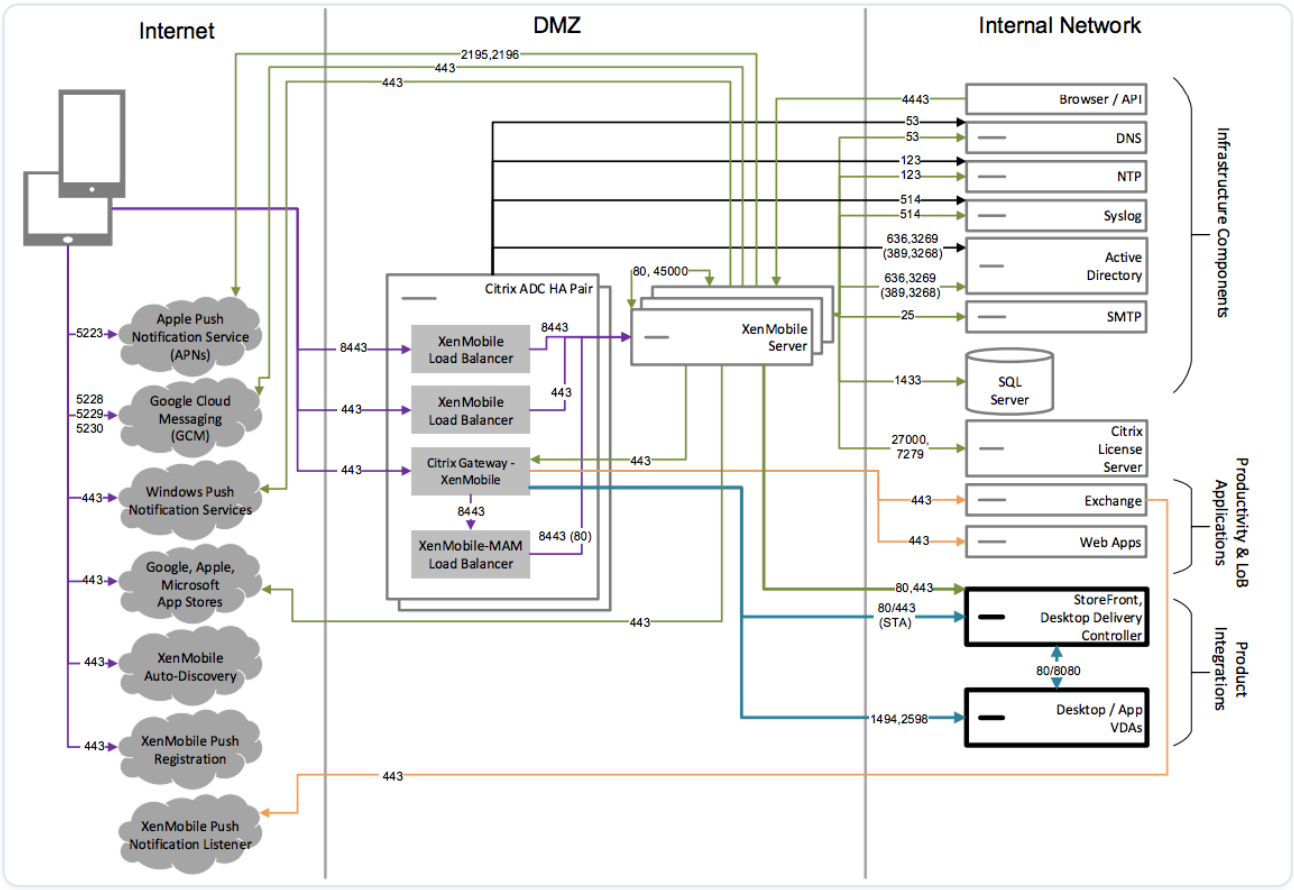
- Você exige certificados de usuário para autenticação de usuário no Citrix Gateway (para acesso à intranet).
- Você exige que os usuários do Secure Mail autenticar no Exchange Server usando um certificado de usuário.
- Você deve enviar certificados emitidos pela sua Autoridade Certificadora corporativa para dispositivos móveis para acesso Wi-Fi, por exemplo.

Embora o diagrama mostre uma autoridade certificadora externa implantada em uma arquitetura MDM+MAM, você também pode implantar uma Autoridade Certificadora externa da mesma forma como parte de uma arquitetura somente MDM ou somente MAM.



Arquitetura de Referência com Virtual Apps e Desktops

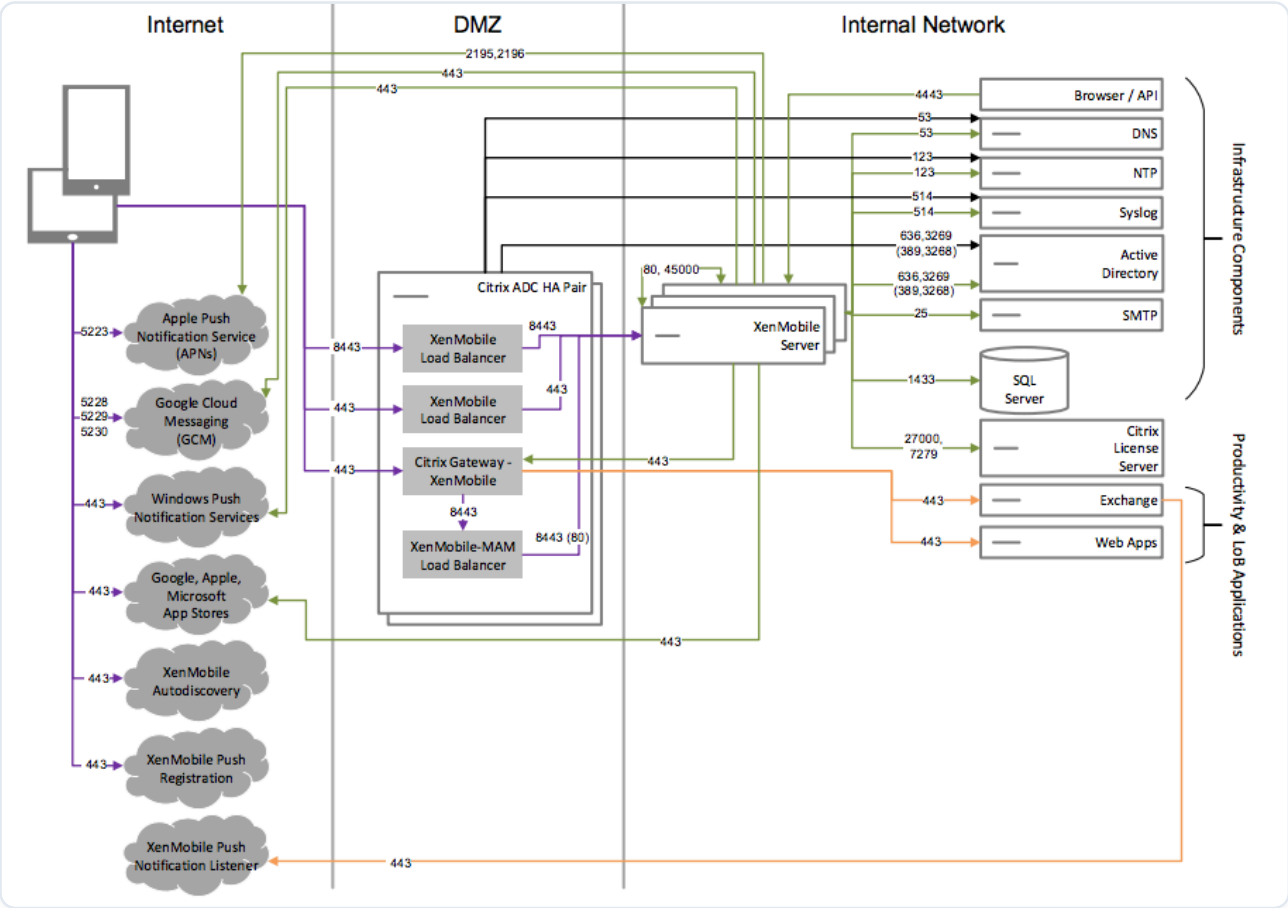
Implante esta arquitetura se você planeja integrar o Virtual Apps and Desktops com o XenMobile. Por exemplo, você precisa fornecer uma loja de aplicativos unificada para usuários móveis para todos os tipos de aplicativos (móveis, SaaS e Windows). Embora o diagrama mostre o Virtual Desktops implantado em uma arquitetura MDM e MAM, você também pode implantar esses desktops da mesma maneira como parte de uma arquitetura somente MAM.



Arquitetura de Referência com XenMobile na Rede Interna

Você pode implantar uma arquitetura com o XenMobile na rede interna para atender a um ou mais dos seguintes requisitos:

- Você não tem ou não tem permissão para ter um hypervisor na DMZ.
- Sua DMZ pode conter apenas dispositivos de rede.
- Seus requisitos de segurança exigem o uso de SSL Offload.



Arquitetura de Referência com ShareFile

Implante esta arquitetura se você deseja integrar o Citrix Files ou apenas conectores de zona de armazenamento com o XenMobile. A integração do Citrix Files permite que você atenda a um ou mais dos seguintes requisitos:

- Você precisa de um IdP para fornecer aos usuários um logon único (SSO) para ShareFile.com.
- Você precisa de uma maneira de provisionar contas no ShareFile.com.
- Você tem repositórios de dados locais que devem ser acessados de dispositivos móveis.

Uma integração apenas com conectores de zona de armazenamento oferece aos usuários acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos de rede. Nesta configuração, você não precisa configurar um subdomínio do ShareFile, provisionar usuários para o Citrix Files ou hospedar dados do Citrix Files.

Embora o diagrama mostre o Citrix Files implantado em uma arquitetura MDM+MAM, você também pode implantar o Citrix Files da mesma forma como parte de uma arquitetura somente MAM.

Diagrama de arquitetura de referência com Citrix Files(/en-us/xenmobile/server/media/reference-architecture-sharefile-storagezones.png)

Propriedades do servidor

As propriedades do servidor são propriedades globais que se aplicam a operações, usuários e dispositivos em toda uma instância do XenMobile®. A Citrix® recomenda que você avalie as propriedades do servidor abordadas neste artigo para o seu ambiente. Certifique-se de consultar a Citrix antes de alterar outras propriedades do servidor.

Uma alteração em algumas propriedades do servidor requer a reinicialização de cada nó. O XenMobile notifica você quando uma reinicialização é necessária.

Algumas propriedades do servidor ajudam a melhorar o desempenho e a estabilidade. Para obter detalhes, consulte Ajustando as Operações do XenMobile.

Entregar aplicativos Android legados para dispositivos Android Enterprise: Se `afw.allow.legacy.apps` estiver definido como `true`, os dispositivos Android Enterprise recebem aplicativos Android legados e aplicativos Android Enterprise. Se `false`, os dispositivos Android Enterprise recebem apenas aplicativos Android Enterprise. O padrão é `true`.

Permitir extensões de arquivo para a política de arquivos: Configure `file.extension.allowlist` com uma lista de tipos de arquivo separados por vírgulas que os administradores podem carregar usando a política de dispositivo Arquivos. Os seguintes tipos de arquivo não podem ser carregados mesmo se você os adicionar a esta lista de permissões:

- arquivo .cab
- arquivo .appx
- arquivo .ipa
- arquivo .apk
- arquivo .xap
- arquivo .mdx
- arquivo .exe

O valor padrão é

`7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,`

Acessar todos os aplicativos na Google Play Store gerenciada: Se `true`, o XenMobile torna todos os aplicativos da Google Play Store pública acessíveis a partir da Google Play Store

gerenciada. Definir esta propriedade como `true` permite os aplicativos da Google Play Store pública para todos os usuários do Android Enterprise. Os administradores podem então usar a política de dispositivo Restrições para controlar o acesso a esses aplicativos. O padrão é `false`.

Registro de perfil de trabalho do Android Enterprise em dispositivos de propriedade corporativa: Quando `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled` é definido como `true`, dispositivos com Android 11 ou posterior podem se registrar no modo de perfil de trabalho em dispositivos de propriedade corporativa (WPCOD). O console reflete as alterações para este modo de registro. Se definido como `false`, nenhuma configuração de WPCOD estará disponível. O valor padrão é `true`.

Configurações adicionais de restrições do Android Enterprise: Se a propriedade `afw.restriction.policy.v2` for definida como `true`, as seguintes configurações de restrição estarão disponíveis para dispositivos Android Enterprise:

- Permitir desinstalação de aplicativos
- Permitir compartilhamento Bluetooth

Para obter mais informações sobre essas configurações, consulte Política de dispositivo de restrições.

Restrições do Android Enterprise para dispositivos COPE: Defina `afw.restriction.cope` como `true` para habilitar a configuração **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho/Perfil de trabalho em dispositivos de propriedade corporativa** na política de dispositivo de restrições. O padrão é `true`. Para obter mais informações sobre essa configuração, consulte Política de dispositivo de restrições.

Permitir nomes de host para links da App Store do iOS: A propriedade `ios.app.store.allowed.hostnames` é uma lista de nomes de host permitidos usados ao carregar aplicativos públicos da App Store para o servidor usando as APIs públicas. Se você planeja carregar aplicativos públicos da App Store usando as APIs públicas em vez de carregar os aplicativos através do servidor, configure esta propriedade. O valor padrão é `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Porta APNs alternativa: Você pode usar a porta 2197 em vez da porta 443 para enviar e receber notificações APNs de `api.push.apple.com`. A porta usa a API do provedor APNs baseada em HTTP/2. Defina a propriedade `apns.http2.alternate.port.enabled` como `true` para usar a

porta 2197. O valor padrão da propriedade do servidor `apns.http2.alternate.port.enabled` é `false`.

Habilitar validação de senha para evitar usuários locais com senhas fracas: Se `enable.password.strength.validation` for definido como `true`, você não poderá adicionar usuários locais com uma senha fraca. Se definido como `false`, você poderá criar usuários locais com uma senha fraca. O padrão é `true`.

Bloquear registro de dispositivos Android com root e iOS com jailbreak: Quando esta propriedade é `true`, o XenMobile bloqueia registros para dispositivos Android com root e dispositivos iOS com jailbreak. O padrão é `true`. A configuração recomendada é `true` para todos os níveis de segurança.

Registro obrigatório: `wsapi.mdm.required.flag`, que se aplica apenas quando o Modo é ENT, especifica se você exige que os usuários se registrem no MDM. A propriedade se aplica a todos os usuários e dispositivos para a instância do XenMobile. Exigir o registro oferece um nível mais alto de segurança. No entanto, essa decisão depende se você deseja exigir o MDM. Por padrão, o registro não é obrigatório.

Quando esta propriedade é `false`, os usuários podem recusar o registro, mas ainda podem acessar aplicativos em seus dispositivos através da XenMobile Store. Quando esta propriedade é `true`, qualquer usuário que recusar o registro terá o acesso negado a quaisquer aplicativos.

Se você alterar esta propriedade depois que os usuários se registrarem, os usuários deverão se registrar novamente.

Para uma discussão sobre se é necessário exigir o registro MDM, consulte Gerenciamento de Dispositivos e Registro MDM.

Habilitar registro multimodo: A propriedade `enable.multimode.xms` permite criar perfis de registro em um XenMobile Server que controla as configurações de registro para gerenciamento de dispositivos e aplicativos para dispositivos Android e iOS. Além disso, o novo recurso de perfis de registro aprimorados permite o registro de dispositivos dedicados para Android e registro somente MAM para dispositivos Android e iOS. Quando esta propriedade é `false`, essas opções de registro não estão disponíveis ao configurar perfis de registro. O valor padrão é `true`. Dispositivos que se registram quando esta propriedade é `true` ainda funcionam se você alterar a propriedade para `false`.

Habilitar o Portal de Autoatendimento: Se `shp.console.enable` for `false`, ele impede o acesso ao Portal de Autoatendimento. Os usuários que navegar para o Portal de Autoatendimento

na porta 443 recebem um erro 404. Os usuários que navegar para o portal na porta 4443 recebem uma mensagem de "Acesso Negado". Se `true`, fornece acesso ao Portal de Autoatendimento pela porta 443. O padrão é `false`.

Limite de bloqueio de conta de usuário local: Usando a política de restrição, você pode definir um limite para tentativas de login de usuários do Active Directory. Use a chave `local.user.account.lockout.limit` para fazer o mesmo para contas de usuário locais. Depois que os usuários tentam fazer login o número de vezes especificado, eles não podem tentar novamente até que um determinado tempo passe. Configure esse tempo com a propriedade **Tempo de bloqueio de conta de usuário local**. O valor padrão é `6`.

Tempo de bloqueio de conta de usuário local: A propriedade `local.user.account.lockout.time` permite definir alguns minutos que devem passar antes que uma conta de usuário local bloqueada possa tentar fazer login novamente. O valor padrão é `30` minutos.

Restrição de tamanho máximo de upload de arquivo habilitada: Habilite a restrição do tamanho máximo de arquivo para uploads definindo `max.file.size.upload.restriction` como `true`. Se você habilitar essa restrição, configure o tamanho máximo do arquivo usando `max.file.size.upload.allowed`. O valor padrão para esta propriedade é `true`.

Tamanho máximo de upload de arquivo permitido: Com `max.file.size.upload.allowed`, você pode especificar um tamanho máximo de arquivo para qualquer upload. Os valores de exemplo incluem `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` ou `1 GiB`. O valor padrão é `5 MB`.

Tempo limite de inatividade em minutos: O número de minutos após os quais o XenMobile desconecta um usuário inativo que usou a API Pública do XenMobile Server para acessar o console do XenMobile ou qualquer aplicativo de terceiros. Um valor de tempo limite de `0` significa que um usuário inativo permanece conectado. Para aplicativos de terceiros que acessam a API, estar conectado é geralmente necessário. O padrão é `5`.

Instalação da CA Raiz de Registro de Gerenciamento de Dispositivos iOS, se Necessário: O fluxo de trabalho de registro mais recente da Apple exige que os usuários instalem manualmente os perfis MDM. Esse fluxo de trabalho não se aplica ao registro MDM em servidores atribuídos no Apple Business Manager ou Apple School Manager. No entanto, durante o registro manual no MDM, os usuários de dispositivos iOS recebem apenas o prompt do certificado do dispositivo MDM durante o registro.

Para proporcionar uma melhor experiência ao usuário durante o registro manual, a Citrix recomenda alterar a propriedade do servidor `ios.mdm.enrollment.installRootCaIfRequired` para **False**. O valor padrão é **True**. Com essa alteração, uma janela do Safari é aberta durante o registro MDM para simplificar a instalação do perfil para os usuários.

Intervalo de linha de base VPP: A propriedade `vpp.baseline` define o intervalo mínimo em que o XenMobile reimporta licenças de compra por volume da Apple. A atualização das informações da licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado da Compra por Volume. Por padrão, o XenMobile atualiza a linha de base da licença de Compra por Volume no mínimo a cada `1440` minutos.

Se você tiver muitas licenças de Compra por Volume instaladas (por exemplo, mais de 50.000), a Citrix recomenda que você aumente o intervalo da linha de base para reduzir a sobrecarga da importação de licenças. Se você espera alterações frequentes nas licenças de compra por volume da Apple, a Citrix recomenda que você diminua o valor para manter o XenMobile atualizado com as alterações. O intervalo mínimo entre as duas linhas de base é de 60 minutos. Como o trabalho cron é executado a cada 60 minutos, se o intervalo da linha de base de compra por volume for de 60 minutos, o intervalo entre as linhas de base pode ser atrasado em até 119 minutos.

Intervalo máximo de inatividade do console do Portal de Autoatendimento do XenMobile MDM (minutos): Este nome de propriedade reflete as versões mais antigas do XenMobile. A propriedade controla o intervalo máximo de inatividade do console do XenMobile. Esse intervalo é o número de minutos após os quais o XenMobile desconecta um usuário inativo do console do XenMobile. Um tempo limite de 0 significa que um usuário inativo permanece conectado. O padrão é `30`.

Suporte obsoleto para o gateway SMS Nexmo: A propriedade `deprecate.carrier.sms.gateway` remove o suporte para o gateway SMS Nexmo, que é definido como **True** por padrão. O SMS Nexmo também está obsoleto no Portal de Autoatendimento.

Suporte obsoleto para a interface do Provedor de Serviços Móveis (MSP): A propriedade `deprecate.mobile.service.provider` remove a interface MSP do console, que é definida como **True** por padrão.

Suporte obsoleto para a política de Proteção de Informações do Windows: Conforme o anúncio do Windows, o suporte para a Proteção de Informações do Windows (WIP) foi

descontinuado. A propriedade do servidor `windows.wip.deprecation` remove o suporte para WIP, que é definido como **True** por padrão.

Suporte obsoleto para o campo "Control Enterprise FOTA" na política de Atualização do SO de Controle para Android Enterprise: Se a propriedade `afw.disable.osupdate.efota` for definida como **True**, o campo **Control Enterprise FOTA** será descontinuado na política de Atualização do SO de Controle para Android Enterprise. O valor padrão é definido como **True**.

Suporte para aplicativos Enterprise em dispositivos macOS: Se a propriedade `mac.app.push` for definida como **True**, os aplicativos Enterprise são instalados automaticamente ao serem baixados em dispositivos que executam macOS. O valor padrão é **True**.

Suporte para eSIM em dispositivos iOS: Se a propriedade `ios.esim.support` for definida como **True**, o XenMobile Server obtém as informações do eSIM dos dispositivos iOS e exibe as propriedades do dispositivo relacionadas ao eSIM na interface do usuário.

Suporte para o campo "Domínio" na política de Wi-Fi para configurações 802.1x para Android Enterprise: Se a propriedade `afw.network.domain.support` for definida como **True**, o campo ***Domínio*** é adicionado nas **configurações 802.1x para Android Enterprise**.

Suporte para atualização automática de aplicativos opcionais no iOS: Se a propriedade `apple.ios.optional_app_update` for definida como **True**, os aplicativos opcionais no iOS assinados na loja Citrix Secure Hub também são atualizados automaticamente. O valor padrão é **False**.

Aprimoramento do relatório de dispositivo para Tentativas Totais de Implantação de Aplicativos e 100 Principais Aplicativos Instalados: Se a propriedade `device.report.enhancement.enabled` for definida como **True**, duas novas colunas **Versão do sistema operacional** e **Modelo do dispositivo** são adicionadas em **Tentativas Totais de Implantação de Aplicativos**, e o novo relatório de dispositivo **100 Principais Aplicativos Instalados** é adicionado para mostrar os 100 principais aplicativos instalados para cada plataforma.

Suporte para Retorno ao Serviço para iPhone e iPad: Quando a propriedade `ios.mdm.return.to.service` é definida como **True**, você pode usar o recurso Retorno ao Serviço para iPhones e iPads executando iOS 17 ou posterior. A configuração padrão para esta propriedade é **True**.

Suporte para a opção VPN sempre ativa na política de VPN para Android Enterprise: se a propriedade `afw.policy.vpn_always_on_lockdown` for definida como **True**, as opções

Habilitar VPN sempre ativa e **Habilitar bloqueio** são adicionadas na política de **VPN** para a plataforma Android Enterprise. O valor padrão é **True**.

Suporte obsoleto para a opção VPN sempre ativa na política de opções para Android Enterprise: A propriedade `afw.policy.hide_vpn_always_on` remove a opção **VPN sempre ativa** da política **Opções do XenMobile** na plataforma Android Enterprise. O valor padrão é **True**.

Alerta de Descontinuação do MDX Legado: Se a propriedade `legacy.mdx.deprecation.alert` for definida como **True**, um alerta aparece no console do XenMobile Server se você tiver aplicativos MDX publicados com o modo MDX legado. O valor padrão é **True**.

Suporte para Firebase Cloud Messaging migrado para usar a nova API http v1: Se a propriedade `afw.fcm.httpv1.migration` for definida como **True**, você pode usar o Firebase Cloud Messaging com a nova API HTTP v1. O valor padrão é **False**.

Suporte para Retorno ao Serviço para iPhone e iPad: Quando a propriedade `ios.mdm.return.to.service` é definida como **True**, você pode usar o recurso Retorno ao Serviço para iPhones e iPads executando iOS 17 ou posterior. A configuração padrão para esta propriedade é **True**.

Suporte para acessar e usar o aplicativo de e-mail do perfil de trabalho a partir do perfil pessoal: Quando a propriedade `afw.mailapp.crossworkprofile` é definida como **True**, ela habilita o recurso que permite o acesso e o uso do aplicativo de e-mail do perfil de trabalho a partir do perfil pessoal nas configurações do Android Enterprise. O padrão é **True**.

Suporte para Impor uma versão mínima do SO para concluir a configuração no Registro Automatizado: Quando a propriedade `ios.mdm.minimum_os_version.enrollment` é definida como **True**, você pode impor um requisito de versão mínima do SO para concluir a configuração durante o Registro Automatizado no iOS 17 ou posterior. O padrão é **True**.

Suporte para Samsung Knox Enhanced Attestation v3: Quando a propriedade `afw.knox.attestation.v3` é definida como **True**, você pode melhorar a funcionalidade de segurança em dispositivos Samsung Knox. O padrão é **True**.

Android Enterprise habilita feedback de configuração gerenciada: Se `afw.app_managed_configurations.feedback` for definido como **True**, os administradores podem obter feedback sobre os estados dos aplicativos de dispositivos Android configurados com políticas de configuração gerenciada. Se **False**, os administradores não recebem feedback. O padrão é **False**.

Tamanho do lote para atualizar o DB de feedback de configuração gerenciada do Android Enterprise: Se `android.managed.configuration.feedback.db.update.batch.size` estiver definido, ele define o tamanho do lote para atualizar o DB de feedback de configuração gerenciada do Android Enterprise. O tamanho pode ser configurado com base na capacidade do DB. O valor padrão é **100**, e o valor máximo é **1000**.

Intervalo de tempo de atualização do DB de feedback de configuração gerenciada do Android Enterprise: Se `android.managed.configuration.feedback.db.update.time.interval` estiver definido, ele define o intervalo de tempo para atualizar o DB de feedback de configuração gerenciada do Android Enterprise. O padrão é **6** horas.

Impor conformidade da política do Android Enterprise: Se a propriedade `afw.policy.compliance` estiver definida como **True**, os dispositivos Android registrados no modo Proprietário do Dispositivo permitem que os administradores gerenciem a conformidade do dispositivo. O padrão é **False**.

Remover dispositivos ABM do XMS quando não atribuídos ao servidor ABM MDM: Se `remove.unassigned.abm.devices` for **true**, o XMS remove os dispositivos que não estão mais atribuídos a este servidor. O padrão é **false**.

Suporte para novos mapeamentos de certificado fortes para autenticação baseada em certificado: Se a propriedade `all_platforms.certificate.strong.mapping` estiver definida como **True**, o XenMobile Server oferece suporte a novos mapeamentos de certificado fortes da Microsoft. O padrão é **True**.

Suporte para eSIM em dispositivos Android Enterprise: Se a propriedade `ae.esim.support` estiver definida como **True**, o XenMobile Server obtém as informações do eSIM dos dispositivos Android Enterprise e exibe as propriedades do dispositivo relacionadas ao eSIM na interface do usuário. O padrão é **True**.

Suporte para Gerenciamento Declarativo de Dispositivos (DDM): Se a propriedade `ios.mdm.declarative.management` estiver definida como **True**, o console do XenMobile Server permite configurar políticas de gerenciamento declarativo do iOS. O padrão é **False**.

Suporte para Imposição de Atualização de Software do iOS: Quando a propriedade `ios.mdm.software.update.settings` estiver definida como **True**, você pode configurar a política de dispositivo de Imposição de Atualização de Software no console do XenMobile Server. O padrão é **False**.

Suporte para aplicativo de inicialização automática em dispositivos Android Enterprise: Quando a propriedade `afw.launcher.auto_launch` estiver definida como **True**, a configuração **Aplicativo de inicialização automática** estará disponível para dispositivos Android Enterprise na política de dispositivo de Configuração do Launcher. O padrão é **False**.

Suporte para políticas DDM do iOS 27: Quando a propriedade `ios.mdm.ios27.ddm.support` estiver definida como **True**, o console do XenMobile Server permite configurar políticas de gerenciamento declarativo do iOS introduzidas no iOS 27. O padrão é **True**.

Políticas de Dispositivo e Aplicativo

As políticas de dispositivo e aplicativo do XenMobile® permitem otimizar o equilíbrio entre fatores, como:

- Segurança corporativa
- Proteção de dados e ativos corporativos
- Privacidade do usuário
- Experiências de usuário produtivas e positivas

O equilíbrio ideal entre esses fatores pode variar. Por exemplo, organizações altamente regulamentadas, como as financeiras, exigem controles de segurança mais rigorosos do que outras indústrias, como educação e varejo, nas quais a produtividade do usuário é uma consideração primária.

Você pode controlar e configurar políticas centralmente com base na identidade, dispositivo, localização e tipo de conectividade dos usuários para restringir o uso malicioso de conteúdo corporativo. No caso de um dispositivo ser perdido ou roubado, você pode desabilitar, bloquear ou apagar remotamente aplicativos e dados corporativos. O resultado geral é uma solução que aumenta a satisfação e a produtividade dos funcionários, ao mesmo tempo em que garante segurança e controle administrativo.

O foco principal deste artigo são as muitas políticas de dispositivo e aplicativo relacionadas à segurança.

Políticas que abordam riscos de segurança

As políticas de dispositivo e aplicativo do XenMobile abordam muitas situações que podem representar um risco de segurança, como as seguintes:

- Quando os usuários tentam acessar aplicativos e dados de dispositivos não confiáveis e locais imprevisíveis.

- Quando os usuários transferem dados de um dispositivo para outro.
- Quando um usuário não autorizado tenta acessar dados.
- Quando um usuário que deixou a empresa usou seu próprio dispositivo (BYOD).
- Quando um usuário extravia um dispositivo.
- Quando os usuários devem acessar a rede de forma segura sempre.
- Quando os usuários têm seu próprio dispositivo gerenciado e você deve separar os dados de trabalho dos dados pessoais.
- Quando um dispositivo está ocioso e requer a verificação das credenciais do usuário novamente.
- Quando os usuários copiam e colam conteúdo sensível em sistemas de e-mail desprotegidos.
- Quando os usuários recebem anexos de e-mail ou links da web com dados sensíveis em um dispositivo que contém contas pessoais e da empresa.

Essas situações se relacionam a duas principais áreas de preocupação ao proteger dados da empresa, que são quando os dados estão:

- Em repouso
- Em trânsito

Como o XenMobile protege dados em repouso

Dados armazenados em dispositivos móveis são chamados de dados em repouso. O XenMobile usa a criptografia de dispositivo fornecida pelas plataformas iOS e Android. O XenMobile complementa a criptografia baseada em plataforma com recursos como verificação de conformidade, disponível por meio do Citrix MAM SDK.

Os recursos de gerenciamento de aplicativos móveis (MAM) no XenMobile permitem gerenciamento, segurança e controle completos sobre aplicativos de produtividade móvel, aplicativos habilitados para MDX e seus dados associados.

O SDK de Aplicativos Móveis permite que os aplicativos sejam implantados no XenMobile por meio do uso da tecnologia de contêiner de aplicativos Citrix MDX. A tecnologia de contêiner separa aplicativos e dados corporativos de aplicativos e dados pessoais em um dispositivo do usuário. A separação de dados permite proteger qualquer aplicativo móvel desenvolvido sob medida, de terceiros ou BYO com controles abrangentes baseados em políticas.

O XenMobile também inclui criptografia no nível do aplicativo. O XenMobile criptografa separadamente os dados armazenados em qualquer aplicativo habilitado para MDX sem exigir uma senha de dispositivo e sem exigir que você gerencie o dispositivo para aplicar a política.

As políticas e o SDK de Aplicativos Móveis permitem que você:

- Separe aplicativos e dados corporativos e pessoais em um contêiner móvel seguro.
- Proteja aplicativos com criptografia e outras tecnologias móveis de Prevenção de Perda de Dados (DLP).

As políticas MDX fornecem muitos controles operacionais. Você pode habilitar a integração perfeita entre aplicativos habilitados para MAM SDK ou empacotados em MDX, enquanto também controla toda a comunicação. Dessa forma, você pode aplicar políticas, como garantir que os dados sejam acessíveis apenas por aplicativos habilitados para MAM SDK ou empacotados em MDX.

Além do controle de políticas de dispositivo e aplicativo, a melhor maneira de proteger os dados em repouso é a criptografia. O XenMobile adiciona uma camada de criptografia a quaisquer dados armazenados em um aplicativo habilitado para MDX, dando a você controle de política sobre recursos como criptografia de arquivo público, criptografia de arquivo privado e exclusões de criptografia. O SDK de aplicativos móveis usa criptografia AES de 256 bits compatível com FIPS 140-2 com chaves armazenadas em um Citrix Secret Vault protegido.

Como o XenMobile protege os dados em trânsito

Os dados em movimento entre os dispositivos móveis do usuário e sua rede interna são chamados de dados em trânsito. A tecnologia de contêiner de aplicativos MDX fornece acesso VPN específico do aplicativo à sua rede interna por meio do Citrix Gateway.

Considere a situação em que um funcionário deseja acessar os seguintes recursos que residem na rede corporativa segura a partir de um dispositivo móvel:

- O servidor de e-mail corporativo
- Um aplicativo web habilitado para SSL hospedado na intranet corporativa
- Documentos armazenados em um servidor de arquivos ou Microsoft SharePoint

O MDX permite o acesso a todos esses recursos corporativos a partir de dispositivos móveis por meio de uma micro VPN específica do aplicativo. Cada dispositivo tem seu próprio túnel micro VPN dedicado.

A funcionalidade de micro VPN não requer uma VPN em todo o dispositivo, o que pode comprometer a segurança em dispositivos móveis não confiáveis. Como resultado, a rede interna não é exposta a malware ou ataques que possam infectar todo o sistema corporativo. Aplicativos móveis corporativos e aplicativos móveis pessoais podem coexistir em um único dispositivo.

Para oferecer níveis ainda mais fortes de segurança, você pode configurar aplicativos habilitados para MDX com uma política de Citrix Gateway Alternativo, usada para autenticação e para sessões de micro VPN com um aplicativo. Você pode usar um Citrix Gateway Alternativo com a política de sessão online obrigatória para forçar os aplicativos a se reautenticarem no gateway específico. Tais gateways normalmente teriam requisitos de autenticação diferentes (maior garantia) e políticas de gerenciamento de tráfego.

Além dos recursos de segurança, o recurso de micro VPN também oferece técnicas de otimização de dados, incluindo algoritmos de compressão. Os algoritmos de compressão garantem que:

- Apenas dados mínimos são transferidos
- A transferência é feita no menor tempo possível. A velocidade melhora a experiência do usuário, que é um fator chave de sucesso na adoção de dispositivos móveis.

Reavalie suas políticas de dispositivo periodicamente, como nestas situações:

- Quando uma nova versão do XenMobile inclui políticas novas ou atualizadas devido ao lançamento de atualizações do sistema operacional do dispositivo
- Ao adicionar um tipo de dispositivo:

  Embora muitas políticas sejam comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas para seu sistema operacional. Como resultado, você pode encontrar diferenças entre dispositivos iOS, Android e Windows, e até mesmo entre dispositivos Android de diferentes fabricantes.
- Para manter a operação do XenMobile sincronizada com as mudanças empresariais ou do setor, como novas políticas de segurança corporativas ou regulamentações de conformidade
- Quando uma nova versão do MAM SDK inclui políticas novas ou atualizadas
- Ao adicionar ou atualizar um aplicativo
- Para integrar novos fluxos de trabalho para seus usuários como resultado de novos aplicativos ou novos requisitos

Políticas de Aplicativo e Cenários de Caso de Uso

Embora você possa escolher quais aplicativos estão disponíveis através do Secure Hub, você também pode querer definir como esses aplicativos interagem com o XenMobile. Use as políticas de aplicativo:

- Se você quiser que os usuários autenticar após um certo período de tempo.
- Se você quiser fornecer aos usuários acesso offline às suas informações.

As seções a seguir incluem algumas das políticas e exemplos de uso.

- Para obter uma lista das políticas de terceiros que você pode integrar em seu aplicativo iOS e Android usando o MAM SDK, consulte Visão geral do MAM SDK.
- Para uma lista de todas as políticas MDX por plataforma, consulte Políticas MDX em Resumo.

Políticas de autenticação

- **Senha do dispositivo**

  Por que usar esta política: Habilite a política de senha do dispositivo para garantir que um usuário possa acessar um aplicativo MDX somente se o dispositivo tiver uma senha de dispositivo habilitada. Esse recurso garante o uso da criptografia iOS no nível do dispositivo.

  Exemplo de usuário: Habilitar esta política significa que o usuário deve definir uma senha em seu dispositivo iOS antes de poder acessar o aplicativo MDX.

- **Senha do aplicativo**

  Por que usar esta política: Habilite a política de senha do aplicativo para que o Secure Hub solicite que um usuário autenticar no aplicativo gerenciado antes que ele possa abrir o aplicativo e acessar os dados. O usuário pode autenticar com sua senha do Active Directory, PIN Citrix ou TouchID do iOS, dependendo do que você configurar em Propriedades do Cliente nas Configurações do XenMobile Server. Você pode definir um temporizador de inatividade em Propriedades do Cliente para que, com o uso contínuo, o Secure Hub não solicite que o usuário autenticar no aplicativo gerenciado novamente até que o temporizador expire.

  A senha do aplicativo difere de uma senha do dispositivo porque, com uma política de senha do dispositivo enviada para um dispositivo, o Secure Hub solicita que o usuário configure uma senha ou PIN, que ele deve desbloquear antes de poder acessar seu dispositivo ao ligá-lo ou quando o temporizador de inatividade expirar. Para obter mais informações, consulte Autenticação no XenMobile.

Exemplo de usuário: Ao abrir o aplicativo Citrix Secure Web™ no dispositivo, o usuário deve inserir seu PIN Citrix antes de poder navegar em sites se o período de inatividade tiver expirado.

- **Sessão online necessária**

  Por que usar esta política: Se um aplicativo exigir acesso a um aplicativo web (serviço web) para ser executado, habilite esta política para que o XenMobile solicite ao usuário que se conecte à rede corporativa ou tenha uma sessão ativa antes de usar o aplicativo.

  Exemplo de usuário: Quando um usuário tenta abrir um aplicativo MDX que tem a política de sessão online necessária habilitada, ele não pode usar o aplicativo até que se conecte à rede usando um serviço de celular ou Wi-Fi.

- **Período máximo offline**

  Por que usar esta política: Use esta política como uma opção de segurança adicional para garantir que os usuários não possam executar um aplicativo offline por longos períodos sem reconfirmar o direito ao aplicativo e atualizar as políticas do XenMobile.

  Exemplo de usuário: Se você configurar um aplicativo MDX com um Período máximo offline, o usuário poderá abrir e usar o aplicativo offline até que o período do temporizador offline expire. Nesse ponto, o usuário deve se reconectar à rede via serviço de celular ou Wi-Fi e se reautenticar, se solicitado.

Políticas de Acesso Diversas

- **Período de carência para atualização de aplicativo (horas)**

  Por que usar esta política: O período de carência para atualização de aplicativo é o tempo disponível para o usuário antes que ele precise atualizar um aplicativo que tenha uma versão mais recente lançada na XenMobile Store. No momento da expiração, o usuário deve atualizar o aplicativo antes de poder acessar os dados no aplicativo. Ao definir esse valor, leve em consideração as necessidades de sua força de trabalho móvel, especialmente aqueles que podem passar longos períodos offline ao viajar internacionalmente.

  Exemplo de usuário: Você carrega uma nova versão do Secure Mail na XenMobile Store e, em seguida, define um período de carência para atualização do aplicativo de 6 horas. Todos os usuários do Secure Mail veem uma mensagem solicitando que atualizem seu aplicativo Secure Mail, até que as 6 horas expirem. Quando as 6 horas expiram, o Secure Hub direciona os usuários para a XenMobile Store.

- **Período de sondagem ativa (minutos)**

Por que usar esta política: O período de sondagem ativa é o intervalo em que o XenMobile verifica os aplicativos para saber quando realizar ações de segurança, como Bloqueio de Aplicativo e Limpeza de Aplicativo.

Exemplo de usuário: Se você definir a política de Período de sondagem ativa para 60 minutos, quando você enviar o comando Bloqueio de Aplicativo do XenMobile para o dispositivo, o bloqueio ocorrerá dentro de 60 minutos a partir da última sondagem.

Políticas de comportamento de dispositivo não compatível

Quando um dispositivo fica abaixo dos requisitos mínimos de conformidade, a política de comportamento de dispositivo não compatível permite que você selecione a ação a ser tomada. Para obter informações, consulte Comportamento de dispositivo não compatível.

Políticas de Interação de Aplicativos

Por que usar essas políticas: Use as políticas de Interação de Aplicativos para controlar o fluxo de documentos e dados de aplicativos MDX para outros aplicativos no dispositivo. Por exemplo, você pode impedir que um usuário mova dados para seus aplicativos pessoais fora do contêiner ou cole dados de fora do contêiner em aplicativos contêinerizados.

Exemplo de usuário: Você define uma política de interação de aplicativo como Restrita, o que significa que um usuário pode copiar texto do Secure Mail para o Secure Web, mas não pode copiar esses dados para seu navegador pessoal Safari ou Chrome que está fora do contêiner. Além disso, um usuário pode abrir um documento anexado do Secure Mail no Citrix Files ou Quick Edit, mas não pode abrir o documento anexado em seus próprios aplicativos pessoais de visualização de arquivos que estão fora do contêiner.

Políticas de Restrições de Aplicativos

Por que usar essas políticas: Use as políticas de Restrição de Aplicativos para controlar quais recursos os usuários podem acessar de um aplicativo MDX enquanto ele está aberto. Isso ajuda a garantir que nenhuma atividade maliciosa possa ocorrer enquanto o aplicativo está em execução. As políticas de Restrição de Aplicativos variam ligeiramente entre iOS e Android. Por exemplo, no iOS você pode bloquear o acesso ao iCloud enquanto o aplicativo MDX está em execução. No Android, você pode interromper o uso de NFC enquanto o aplicativo MDX está em execução.

Exemplo de usuário: Se você habilitar a política de Restrição de Aplicativos para bloquear a ditado no iOS em um aplicativo MDX, o usuário não poderá usar a função de ditado no teclado do iOS enquanto o aplicativo MDX estiver em execução. Assim, os dados que os usuários ditam não são passados para o serviço de ditado em nuvem de terceiros não seguro. Quando o usuário abre

seu aplicativo pessoal fora do contêiner, a opção de ditado permanece disponível para o usuário para suas comunicações pessoais.

Políticas de Acesso à Rede de Aplicativos

Por que usar essas políticas: Use as políticas de Acesso à Rede de Aplicativos para fornecer acesso de um aplicativo MDX no contêiner do dispositivo a dados localizados na sua rede corporativa. Para a política de acesso à rede, defina a opção **Tunelado para a rede interna** para automatizar uma micro VPN do aplicativo MDX através do Citrix ADC para um serviço web de back-end ou armazenamento de dados.

Exemplo de usuário: Quando um usuário abre um aplicativo MDX, como o Secure Web, que tem o tunelamento ativado, o navegador abre e inicia um site da intranet sem que o usuário precise iniciar uma VPN. O aplicativo Secure Web acessa automaticamente o site interno usando a tecnologia de micro VPN.

Políticas de Geolocalização e Geofencing de Aplicativos

Por que usar essas políticas: As políticas que controlam a geolocalização e o geofencing de aplicativos incluem longitude do ponto central, latitude do ponto central e raio. Essas políticas contêm acesso aos dados nos aplicativos MDX a uma área geográfica específica. As políticas definem uma área geográfica por um raio de coordenadas de latitude e longitude. Se um usuário tentar usar um aplicativo fora do raio definido, o aplicativo permanecerá bloqueado e o usuário não poderá acessar os dados do aplicativo.

Exemplo de usuário: Um usuário pode acessar dados de fusões e aquisições enquanto estiver em seu local de trabalho. Quando eles se movem para fora do local de trabalho, esses dados confidenciais tornam-se inacessíveis.

Políticas do Aplicativo Secure Mail

- **Serviços de rede em segundo plano**

  Por que usar essa política: Os serviços de rede em segundo plano no Secure Mail usam a Autoridade de Ticket Seguro (STA), que é efetivamente um proxy SOCKS5 para se conectar através do Citrix Gateway. A STA suporta conexões de longa duração e oferece melhor duração da bateria em comparação com a micro VPN. Assim, a STA é ideal para e-mails que se conectam constantemente. A Citrix recomenda que você configure essas configurações para o Secure Mail. O assistente do Citrix ADC para XenMobile configura automaticamente a STA para o Secure Mail.

  Exemplo de usuário: Quando a STA não está ativada e um usuário Android abre o Secure Mail, ele é solicitado a abrir uma VPN, que permanece aberta no dispositivo. Quando a STA

está ativada e o usuário Android abre o Secure Mail, o Secure Mail se conecta perfeitamente sem a necessidade de VPN.

- **Intervalo de sincronização padrão**

  Por que usar essa política: Essa configuração especifica o número padrão de dias de e-mail que são sincronizados com o Secure Mail quando o usuário acessa o Secure Mail pela primeira vez. Duas semanas de e-mail levam mais tempo para sincronizar do que 3 dias e prolongam o processo de configuração para o usuário.

  Exemplo de usuário: Se o intervalo de sincronização padrão for definido como 3 dias quando o usuário configurar o Secure Mail pela primeira vez, ele poderá ver todos os e-mails em sua Caixa de Entrada que recebeu do presente até 3 dias no passado. Se um usuário quiser ver e-mails com mais de 3 dias, ele pode fazer uma pesquisa. O Secure Mail então mostra os e-mails mais antigos armazenados no servidor. Após instalar o Secure Mail, cada usuário pode alterar essa configuração para melhor atender às suas necessidades.

Políticas de Dispositivo e Comportamento de Caso de Uso

As políticas de dispositivo, às vezes chamadas de políticas MDM, determinam como o XenMobile funciona com os dispositivos. Embora muitas políticas sejam comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas para seu sistema operacional. A lista a seguir inclui algumas das políticas de dispositivo e discute como você pode usá-las. Para obter uma lista de todas as políticas de dispositivo, consulte os artigos em Políticas de dispositivo.

- **Política de inventário de aplicativos**

  Por que usar esta política: Implante a política de inventário de aplicativos em um dispositivo se você precisar ver os aplicativos instalados por um usuário. Se você não implantar a política de inventário de aplicativos, poderá ver apenas os aplicativos que um usuário instalou da XenMobile Store e não quaisquer aplicativos instalados pessoalmente. Você deve usar esta política se quiser bloquear a execução de determinados aplicativos em dispositivos corporativos.

  Exemplo de usuário: Um usuário com um dispositivo gerenciado por MDM não pode desabilitar essa funcionalidade. Os aplicativos instalados pessoalmente pelo usuário são visíveis para os administradores do XenMobile.

- **Política de bloqueio de aplicativos**

  Por que usar esta política: A política de Bloqueio de Aplicativos, para Android, permite bloquear ou permitir aplicativos. Por exemplo, ao permitir aplicativos, você pode configurar um

dispositivo de quiosque. Normalmente, você implanta a política de bloqueio de aplicativos apenas em dispositivos corporativos, pois ela limita os aplicativos que os usuários podem instalar. Você pode definir uma senha de substituição para fornecer acesso do usuário a aplicativos bloqueados.

Exemplo de usuário: Suponha que você implante uma política de bloqueio de aplicativos que bloqueia o aplicativo Angry Birds. O usuário pode instalar o aplicativo Angry Birds do Google Play, mas quando ele abre o aplicativo, uma mensagem o informa que o administrador bloqueou o aplicativo.

- **Política de agendamento de conexão**

  Por que usar esta política: Você deve usar a política de agendamento de conexão para que os dispositivos Windows Mobile possam se conectar de volta ao XenMobile Server para gerenciamento de MDM, envio de aplicativos e implantação de políticas. Para dispositivos Android, Android Enterprise e Chrome OS, use o Google Firebase Cloud Messaging (FCM), em vez desta política, para controlar as conexões com o XenMobile Server. As opções de agendamento são as seguintes:

  - **Sempre:** Mantém a conexão ativa permanentemente. A Citrix recomenda esta opção para segurança otimizada. Ao escolher **Sempre**, use também a política de temporizador de conexão para garantir que a conexão não esteja esgotando a bateria. Ao manter a conexão ativa, você pode enviar comandos de segurança como limpeza ou bloqueio para o dispositivo sob demanda. Você também deve selecionar a opção Agendamento de Implantação **Implantar para conexão sempre ativa** em cada política que você implantar no dispositivo.
  - **Nunca:** Conecta-se manualmente. A Citrix não recomenda esta opção para implantações de produção porque a opção **Nunca** impede que você implante políticas de segurança nos dispositivos; assim, os usuários nunca recebem novos aplicativos ou políticas.
  - **A cada:** Conecta-se no intervalo designado. Quando esta opção está em vigor e você envia uma política de segurança, como um bloqueio ou uma limpeza, o XenMobile processa a política no dispositivo na próxima vez que o dispositivo se conecta.
  - **Definir agendamento:** Quando ativado, o XenMobile tenta reconectar o dispositivo do usuário ao XenMobile Server após uma perda de conexão de rede e monitora a conexão transmitindo pacotes de controle em intervalos regulares dentro do período que você definir.

Exemplo de usuário: Você deseja implantar uma política de senha para dispositivos registrados. A política de agendamento garante que os dispositivos se conectem de volta ao servidor em um intervalo regular para coletar a nova política.

- **Política de Credenciais**

  Por que usar esta política: Frequentemente usada com uma política de Wi-Fi, a política de Credenciais permite implantar certificados para autenticação em recursos internos que exigem autenticação por certificado.

  Exemplo de usuário: Você implanta uma política de Wi-Fi que configura uma rede sem fio no dispositivo. A rede Wi-Fi requer um certificado para autenticação. A política de Credenciais implanta um certificado que é então armazenado no keystore do sistema operacional. O usuário pode então selecionar o certificado ao se conectar ao recurso interno.

- **Política do Exchange**

  Por que usar esta política: Com o XenMobile, você tem duas opções para entregar e-mail do Microsoft Exchange ActiveSync.

  - **Aplicativo Secure Mail:** Entregue e-mail usando o aplicativo Secure Mail que você distribui da loja de aplicativos pública ou da XenMobile Store.
  - **Aplicativo de e-mail nativo:** Use a política do Exchange para habilitar o e-mail ActiveSync para o cliente de e-mail nativo no dispositivo. Com a política do Exchange para e-mail nativo, você pode usar macros para preencher os dados do usuário a partir de seus atributos do Active Directory, como ${user.username} para preencher o nome de usuário e ${user.domain} para preencher o domínio do usuário.

  Exemplo de usuário: Ao enviar a política do Exchange, você envia os detalhes do Exchange Server para o dispositivo. O Secure Hub então solicita que o usuário autenticar e o e-mail dele começa a sincronizar.

- **Política de Localização**

  Por que usar esta política: A política de Localização permite geolocalizar dispositivos em um mapa, se o dispositivo tiver GPS habilitado para o Secure Hub. Depois de implantar esta política e enviar um comando de localização do XenMobile Server, o dispositivo responde com as coordenadas de localização.

  Exemplo de usuário: Ao implantar a política de localização e o GPS estiver habilitado no dispositivo, se os usuários extraviarem o dispositivo, eles podem fazer login no Portal de Autoajuda do XenMobile e escolher a opção de localização para ver a localização do

dispositivo em um mapa. O usuário decide permitir que o Secure Hub use os serviços de localização. Você não pode impor o uso de serviços de localização quando os usuários registram um dispositivo por conta própria. Outra consideração para usar esta política é o efeito na vida útil da bateria.

- **Política de Senha**

  Por que usar esta política: A política de senha permite que você imponha um código PIN ou senha em um dispositivo gerenciado. Esta política de senha permite que você defina a complexidade e os tempos limite para a senha no dispositivo.

  Exemplo de usuário: Ao implantar uma política de senha em um dispositivo gerenciado, o Secure Hub solicita que o usuário configure uma senha ou PIN, que ele deve desbloquear antes de poder acessar o dispositivo ao ligá-lo ou quando o temporizador de inatividade expirar.

- **Política de remoção de perfil**

  Por que usar esta política: Suponha que você implante uma política para um grupo de usuários e, mais tarde, precise remover essa política de um subconjunto dos usuários. Você pode remover a política para usuários selecionados criando uma política de remoção de perfil e usando as regras de implantação para implantar a política de remoção de perfil apenas para nomes de usuário especificados.

  Exemplo de usuário: Ao implantar uma política de remoção de perfil em dispositivos de usuário, os usuários podem não notar a alteração. Por exemplo, se a política de remoção de perfil remover uma restrição que desabilitava a câmera do dispositivo, o usuário não saberá que o uso da câmera agora é permitido. Considere informar os usuários quando as alterações afetarem sua experiência de usuário.

- **Política de restrições**

  Por que usar esta política: A política de restrições oferece muitas opções para bloquear e controlar recursos e funcionalidades no dispositivo gerenciado. Você pode habilitar centenas de opções de restrição para dispositivos compatíveis, desde desabilitar a câmera ou o microfone em um dispositivo até impor regras de roaming e acesso a serviços de terceiros, como lojas de aplicativos.

  Exemplo de usuário: Se você implantar uma restrição em um dispositivo iOS, o usuário pode não conseguir acessar o iCloud ou a App Store da Apple.

- **Política de termos e condições**

Por que usar esta política: Você pode precisar informar os usuários sobre as implicações legais de ter seu dispositivo gerenciado. Além disso, você pode querer garantir que os usuários estejam cientes dos riscos de segurança quando os dados corporativos são enviados para o dispositivo. O documento personalizado de Termos e Condições permite que você publique regras e avisos antes que o usuário se inscreva.

Exemplo de usuário: Um usuário vê as informações de Termos e Condições durante o processo de inscrição. Se ele se recusar a aceitar as condições estabelecidas, o processo de inscrição é encerrado e ele não poderá acessar os dados corporativos. Você pode gerar um relatório para fornecer às equipes de RH/Jurídico/Conformidade para mostrar quem aceitou ou recusou os termos.

- **Política de VPN**

  Por que usar esta política: Use a política de VPN para fornecer acesso a sistemas de back-end usando tecnologia de VPN Gateway mais antiga. A política oferece suporte a vários provedores de VPN, incluindo Cisco AnyConnect, Juniper e Citrix VPN. Também é possível vincular esta política a uma CA e habilitar a VPN sob demanda, se o gateway VPN suportar esta opção.

  Exemplo de usuário: Com a política de VPN habilitada, o dispositivo de um usuário abre uma conexão VPN quando o usuário acessa um domínio interno.

- **Política de Webclip**

  Por que usar esta política: Use a política de Webclip se você quiser enviar para os dispositivos um ícone que abre diretamente para um site. Um web clip contém um link para um site e pode incluir um ícone personalizado. Em um dispositivo, um web clip se parece com um ícone de aplicativo.

  Exemplo de usuário: Um usuário pode clicar em um ícone de web clip para abrir um site da internet que fornece serviços que ele deve acessar. Usar um link da web é mais conveniente do que precisar abrir um aplicativo de navegador e digitar um endereço de link.

- **Política de Wi-Fi**

  Por que usar esta política: A política de Wi-Fi permite implantar detalhes da rede Wi-Fi, como SSID, dados de autenticação e dados de configuração, em um dispositivo gerenciado.

  Exemplo de usuário: Ao implantar a política de Wi-Fi, o dispositivo se conecta automaticamente à rede Wi-Fi e autentica o usuário para que ele possa obter acesso à rede.

- **Política de Proteção de Informações do Windows**

Por que usar esta política: Use a política de Proteção de Informações do Windows (WIP) para proteger contra o vazamento potencial de dados corporativos. Você pode especificar os aplicativos que exigem a Proteção de Informações do Windows no nível de imposição que você definir. Por exemplo, você pode bloquear qualquer compartilhamento de dados inadequado ou avisar sobre compartilhamento de dados inadequado e permitir que os usuários ignorem a política. Você pode executar o WIP silenciosamente enquanto registra e permite o compartilhamento de dados inadequado.

Exemplo de usuário: Suponha que você configure a política WIP para bloquear o compartilhamento de dados inadequado. Se um usuário copiar ou salvar um arquivo protegido em um local não protegido, uma mensagem semelhante à seguinte aparecerá: Você não pode colocar conteúdo protegido pelo trabalho neste local.

- **Política da Loja XenMobile**

  Por que usar esta política: A Loja XenMobile é uma loja de aplicativos unificada onde os administradores podem publicar todos os aplicativos corporativos e recursos de dados necessários para seus usuários. Um administrador pode adicionar:

  - Aplicativos web, aplicativos SaaS e aplicativos habilitados para MAM SDK ou aplicativos empacotados em MDX
  - Aplicativos de produtividade móvel da Citrix
  - Aplicativos móveis nativos, como arquivos .ipa ou .apk
  - Aplicativos da Apple App Store e Google Play
  - Links da web
  - Citrix Virtual Apps™ publicados usando o Citrix StoreFront

  Exemplo de usuário: Depois que um usuário registra seu dispositivo no XenMobile, ele acessa a Loja XenMobile por meio do aplicativo Citrix Secure Hub™. O usuário pode então ver todos os aplicativos e serviços corporativos disponíveis para ele. Os usuários podem clicar em um aplicativo para instalá-lo, acessar os dados, avaliar e revisar o aplicativo e baixar atualizações de aplicativos da Loja XenMobile.

Opções de Registro de Usuário

Você pode fazer com que os usuários registrem seus dispositivos no XenMobile de várias maneiras. Antes de considerar os detalhes, decida quais dispositivos você deseja registrar em MDM+MAM, MDM ou MAM. Para obter mais informações sobre esses modos de gerenciamento, consulte Modos de Gerenciamento.

No nível mais alto, existem quatro opções de registro:

- **Convite de Registro:** Envie um convite de registro ou URL de convite para os usuários. Convites de registro e URLs não estão disponíveis para dispositivos Windows.
- **Portal de Autoatendimento:** Configure um portal que os usuários podem visitar para baixar o Secure Hub e registrar seus dispositivos ou enviar a si mesmos um convite de registro.
- **Registro Manual:** Envie um e-mail, manual ou outra comunicação para informar aos usuários que o sistema está disponível para registro. Os usuários então baixam o Secure Hub e registram seus dispositivos manualmente.
- **Empresarial:** Outra opção para o registro de dispositivos é através de um Programa de Implantação da Apple e do Google Android Enterprise. Através de cada um desses programas, você pode comprar dispositivos pré-configurados e prontos para uso pelos funcionários. Para obter mais informações, consulte os artigos do Programa de Implantação da Apple em Suporte da Apple e a documentação do Google Android Enterprise no site do Android Enterprise.

Convite de Registro

Você pode enviar um convite de registro por e-mail para usuários com dispositivos iOS, macOS, Android Enterprise e Android legado. Convites de registro e URLs não estão disponíveis para dispositivos Windows.

Você também pode enviar um link de instalação via SMTP ou SMS para usuários com dispositivos iOS, macOS, Android ou Windows. Para obter mais informações, consulte Registrar dispositivos.

Se você optar por usar o método de convite de registro, você pode:

- Escolher os modos de segurança de registro **URL de Convite**, **URL de Convite + PIN** ou **URL de Convite + Senha**.
- Usar qualquer combinação dos modos.
- Ativar ou desativar os modos na página **Configurações**.

Para obter informações sobre cada modo de segurança de registro, consulte Configurar modos de segurança de registro.

Os convites servem para muitos propósitos. O uso mais comum de convites é para notificar os usuários de que o sistema está disponível e que eles podem se registrar. As URLs de convite são únicas. Depois que um usuário usa uma URL de convite, a URL não está mais disponível. Você pode usar essa propriedade para limitar os usuários ou dispositivos que se registram em seu sistema.

Ao configurar um perfil de registro, você pode controlar o número de dispositivos que usuários específicos podem registrar, com base em grupos do Active Directory. Por exemplo, você pode permitir que sua divisão Financeira tenha apenas um dispositivo por usuário.

Esteja ciente dos custos extras e das armadilhas de certas opções de registro. Por exemplo, o envio de convites por SMS requer infraestrutura extra. Para obter mais informações sobre esta opção, consulte Notificações.

Juntamente com o envio de convites por e-mail, certifique-se de que os usuários tenham uma maneira de acessar o e-mail fora do Secure Hub. Você pode usar um modo de segurança de registro de senha de uso único (OTP) como alternativa às senhas do Active Directory para o registro de MDM.

Portal de Autoatendimento

Você pode solicitar um convite de registro através do Portal de Autoatendimento. Para obter informações sobre como configurar o Portal de Autoatendimento, consulte Configurar modos de segurança de registro.

Registro Manual

Com o registro manual, os usuários se conectam ao XenMobile por meio do AutoDiscovery ou inserindo as informações do servidor. Com o AutoDiscovery, os usuários fazem login apenas com seu endereço de e-mail ou credenciais do Active Directory no formato Nome Principal do Usuário. Sem o AutoDiscovery, eles devem inserir o endereço do servidor e suas credenciais do Active Directory. Para obter mais informações sobre como configurar o AutoDiscovery, consulte Serviço AutoDiscovery do XenMobile.

Você pode facilitar o registro manual de várias maneiras. Você pode criar um guia, distribuí-lo aos usuários e fazer com que eles se registrem. Você pode fazer com que seu departamento de TI registre manualmente grupos de usuários em determinados horários. Você pode usar qualquer método semelhante em que os usuários devem inserir suas credenciais, informações do servidor ou ambos.

Integração de Usuários

Depois de configurar seu ambiente, você precisa decidir como integrar os usuários ao seu ambiente. Uma seção anterior neste artigo discute os detalhes dos modos de segurança de registro de usuário. Esta seção discute a maneira como você se comunica com os usuários.

Registro Aberto versus Convite Seletivo

Ao integrar usuários, você pode permitir o registro por meio de dois métodos básicos:

- Registro aberto. Por padrão, qualquer usuário com credenciais LDAP e as informações do ambiente XenMobile® pode se registrar.
- Registro limitado. Você pode limitar o número de usuários permitindo apenas que usuários com convites se registrem. Você também pode limitar o registro aberto por um grupo do Active Directory.

Com o método de convite, você também pode limitar o número de dispositivos que um usuário pode registrar. Na maioria das situações, o registro aberto é aceitável, mas há algumas coisas a considerar:

- Para o registro MAM, você pode limitar facilmente o registro aberto por meio da associação a grupos do Active Directory.
- Para o registro MDM, você pode limitar o número de dispositivos que podem ser registrados com base na associação a grupos do Active Directory. Se você permitir apenas dispositivos corporativos em seu ambiente, essa limitação geralmente não é um problema. No entanto, você pode considerar este método em um ambiente de trabalho BYOD se quiser limitar o número de dispositivos em seu ambiente.

O convite seletivo é geralmente feito com menos frequência porque exige um pouco mais de trabalho do que o registro aberto. Para que os usuários registrem seus dispositivos em seu ambiente, você deve enviar um convite exclusivo para cada usuário. Para obter informações sobre como enviar um convite de registro, consulte Envio de um convite de registro.

Embora você possa usar grupos do Active Directory para criar convites em lotes, você deve realizar essa abordagem em ondas.

Primeiro Contato com os Usuários

Depois de decidir entre registro aberto ou convite seletivo e configurar esses ambientes, você deve informar os usuários sobre suas opções de registro.

Se você usar o método de convite seletivo, e-mail e mensagens SMS fazem parte do processo. Você também pode enviar e-mails através do console do XenMobile para registro aberto. Para obter detalhes, consulte Envio de um convite de registro.

Em ambos os casos, lembre-se de que, para e-mail, você precisa de um servidor SMTP. Para mensagens de texto, você precisa de um servidor SMS. Esses servidores podem representar um custo extra a ser considerado ao tomar sua decisão. Antes de selecionar um método, considere como você espera que os novos usuários acessem as informações, como e-mail. Se você deseja

que todos os usuários acessem seus e-mails através do XenMobile, enviar-lhes um e-mail de convite seria problemático.

Você também pode enviar comunicações por outros meios fora do XenMobile para um ambiente de registro aberto. Para essa opção, certifique-se de incluir todas as informações relevantes. Informe os usuários onde eles podem obter o aplicativo Secure Hub e qual método usar para se registrar. Se você tiver a descoberta desativada, forneça também aos usuários o endereço do servidor XenMobile. Para saber mais sobre o AutoDiscovery, consulte Serviço AutoDiscovery do XenMobile.

Ajustando as Operações do XenMobile®

O desempenho e a estabilidade das operações do XenMobile envolvem muitas configurações em todo o XenMobile e dependem da sua configuração de banco de dados Citrix ADC e SQL Server. Este artigo foca nas configurações que os administradores mais frequentemente configuram, relacionadas ao ajuste e otimização do XenMobile. A Citrix recomenda que você avalie cada uma das configurações neste artigo antes de implantar o XenMobile.

> **Importante:**

> Estas diretrizes assumem que a CPU e a RAM do XenMobile Server são adequadas para o número de dispositivos. Para mais informações sobre escalabilidade, consulte Escalabilidade e desempenho.

> As seguintes propriedades do servidor se aplicam globalmente a operações, usuários e dispositivos em toda uma instância do XenMobile. Uma alteração em algumas propriedades do servidor requer a reinicialização de cada nó do XenMobile Server. O XenMobile o notifica quando uma reinicialização é necessária.

Estas diretrizes de ajuste aplicam-se a ambientes clusterizados e não clusterizados.

hibernate.c3p0.idle_test_period

Esta propriedade do XenMobile Server, uma Chave Personalizada, determina o tempo ocioso em segundos antes que uma conexão seja automaticamente validada. Configure a chave da seguinte forma. O padrão é **30**.

- Chave: **Chave Personalizada**
- Chave: **hibernate.c3p0. idle_test_period**

- Valor: **120**
- Nome de exibição: **hibernate.c3p0. idle_test_period**
- Descrição: **Período de teste ocioso do Hibernate**

hibernate.c3p0.max_size

Esta chave personalizada determina o número máximo de conexões que o XenMobile pode abrir para o banco de dados SQL Server. O XenMobile usa o valor que você especifica para esta chave personalizada como um limite superior. As conexões são abertas apenas se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados.

Observe a seguinte equação em uma configuração em cluster. Sua conexão c3p0 multiplicada pelo número de nós é igual ao seu número máximo real de conexões que o XenMobile pode abrir para o banco de dados SQL Server.

Em configurações em cluster e não em cluster, definir o valor muito alto com um SQL Server subdimensionado pode causar problemas de recursos no lado do SQL durante o pico de carga. Definir o valor muito baixo significa que você pode não conseguir aproveitar os recursos SQL disponíveis.

Configure a chave da seguinte forma. O padrão é **1000**.

- Chave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nome de exibição: **hibernate.c3p0.max_size**
- Descrição: Conexões de BD ao SQL

hibernate.c3p0.min_size

Esta Chave Personalizada determina o número mínimo de conexões que o XenMobile abre para o banco de dados SQL Server. Configure a chave da seguinte forma. O padrão é **100**.

- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de exibição: **hibernate.c3p0.min_size**
- Descrição: Conexões de BD ao SQL

hibernate.c3p0.timeout

Esta Chave Personalizada determina o tempo limite de inatividade. Se você usar um failover de cluster de banco de dados, a Citrix recomenda que você adicione esta Chave Personalizada e a configure para reduzir o tempo limite de inatividade. O padrão é **120**.

- Chave: **Custom Key**
- Chave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nome de exibição: **hibernate.c3p0.timeout**
- Descrição: Tempo limite de inatividade do banco de dados

Intervalo de Pulsação dos Serviços de Push

Essa configuração determina com que frequência um dispositivo iOS verifica se uma notificação APNs não foi entregue nesse ínterim. Aumentar a frequência da pulsação do APNs pode otimizar as comunicações do banco de dados. Um valor muito alto pode adicionar carga desnecessária. Essa configuração se aplica apenas ao iOS. O padrão é de **20** horas.

Se você tiver muitos dispositivos iOS em seu ambiente, o intervalo de pulsação pode levar a uma carga maior do que o necessário. Ações de segurança, como limpeza seletiva, bloqueio e limpeza completa, não dependem dessa pulsação. O motivo é que uma notificação APNs é enviada ao dispositivo quando essas ações são executadas.

Esse valor governa a rapidez com que uma política é atualizada após alterações na associação de Grupo do Active Directory. Como tal, muitas vezes é adequado aumentar esse valor para algo entre 12 e 20 horas para reduzir a carga.

Tamanho do pool de conexão APNS do MDM iOS

Um pool de conexão APNs muito pequeno pode afetar negativamente o desempenho da atividade APNs quando você tem mais de 100 dispositivos. Problemas de desempenho incluem implantação mais lenta de aplicativos e políticas em dispositivos e registro de dispositivos mais lento. O padrão é **1**. Recomendamos que você aumente esse valor em 1 para cada 400 dispositivos, aproximadamente.

auth.ldap.connect.timeout

Para compensar respostas LDAP lentas, a Citrix recomenda que você adicione propriedades de servidor para a seguinte Chave Personalizada.

- Chave: **Custom Key**

- Chave: **auth.ldap.connect.timeout**
- Valor: **60000**
- Nome de exibição: **auth.ldap.connect.timeout**
- Descrição: **Tempo limite de conexão LDAP**

auth.ldap.read.timeout

Para compensar respostas LDAP lentas, a Citrix recomenda que você adicione propriedades de servidor para a seguinte Chave Personalizada.

- Chave: **Chave Personalizada**
- Chave: **auth.ldap.read.timeout**
- Valor: **60000**
- Nome de exibição: **auth.ldap.read.timeout**
- Descrição: **Tempo limite de leitura LDAP**

Outras Otimizações de Servidor

Propriedade do Servidor	Configuração Padrão	Por que Alterar Esta Configuração?
Implantação em Segundo Plano	1.440 minutos	A frequência para implantações de políticas em segundo plano, em minutos. Aplica-se apenas a conexões sempre ativas para dispositivos Android. Aumentar a frequência das implantações de políticas reduz a carga do servidor. A configuração recomendada é **1440** (24 horas).
Inventário de Hardware em Segundo Plano	1.440 minutos	A frequência para o inventário de hardware em segundo plano, em minutos. Aplica-se apenas a conexões sempre ativas para dispositivos Android. Aumentar a frequência do

		inventário de hardware reduz a carga do servidor. A configuração recomendada é **1440** (24 horas).
Intervalo para verificar usuário excluído do Active Directory	15 minutos	O tempo de sincronização padrão para o Active Directory é de **15** minutos. O valor **0** impede que o XenMobile verifique usuários excluídos do Active Directory. A configuração recomendada é de **15** minutos.
MaxNumberOfWorker	3	O número de threads usados ao importar muitas licenças de compra por volume. O padrão é **3**. Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, com um número maior de threads, como 6, uma importação de compra por volume resulta em alto uso da CPU.

Como verificar deadlocks em um banco de dados SQL e excluir dados históricos

Quando você vir deadlocks, execute a seguinte consulta para vê-los. Em seguida, um administrador de banco de dados ou a equipe do Microsoft SQL pode confirmar as informações.

Consulta SQL

```
SELECT


db.name DB_Service,


tl.request_session_id,
```

```
wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address =
wt.resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id =
tl.resource_associated_entity_id
```

```
INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id =
tl.request_session_id



INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id =
wt.blocking_session_id



CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1



CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2



GO
```

Limpar o banco de dados

Importante:

Faça backup do seu banco de dados antes de fazer alterações nas tabelas.

1. Execute a seguinte consulta para verificar os dados históricos.

```
select COUNT(*) as total_record from dbo.EWDEPLOY_HISTO;

select COUNT(*) as total_record from dbo.EWSESS;

select COUNT(*) as total_record from dbo.EWAUDIT;
```

2. Exclua os dados das três tabelas anteriores.

Nota:

> Você pode não ver dados históricos em uma tabela. Se for o caso, pule a execução da consulta de truncamento para essa tabela específica.

```
truncate TABLE dbo.EWDEPLOY_HISTO;

truncate TABLE dbo.EWSESS;

truncate TABLE dbo.EWAUDIT;
```

3. Desbloqueie as consultas SELECT que foram bloqueadas devido a deadlocks. Esta etapa cuida de deadlocks futuros.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT ON
WITH ROLLBACK IMMEDIATE
```

4. Por padrão, a limpeza do banco de dados é de sete dias para reter dados de retenção de sessão e retenção de auditoria, o que é alto para muitos usuários. Altere o valor de limpeza para 1 ou 2 dias. Nas propriedades do servidor, faça a seguinte alteração:

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day

zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day

zdm.dbcleanup.auditRetentionTimeInDays=1 day
```

Limpar órfãos na tabela KEYSTORE

Se os nós do XenMobile apresentarem baixo desempenho, verifique se a tabela KEYSTORE está muito grande. O XenMobile Server armazena certificados de registro nas tabelas ENROLLMENT_CERTIFICATE e KEYSTORE. Ao excluir ou registrar novamente dispositivos, os certificados na tabela ENROLLMENT_CERTIFICATE são excluídos. As entradas na tabela KEYSTORE permanecem, o que pode causar problemas de desempenho. Execute o procedimento a seguir para limpar os órfãos da tabela KEYSTORE.

> **Importante:**

> Faça backup do seu banco de dados antes de fazer alterações nas tabelas.

1. Execute a seguinte consulta para verificar os dados históricos.

```
select COUNT(*) from KEYSTORE
```

2. Verifique se há órfãos na tabela KEYSTORE com a seguinte consulta.

```
WITH cte(KEYSTORE_ID)

AS (SELECT KEYSTORE_ID

    FROM ENROLLMENT_CERTIFICATE

    UNION

    SELECT CA_KEYSTORE_ID

    FROM LDAP_CONFIG

    UNION

    SELECT CLIENT_KEYSTORE_ID

    FROM LDAP_CONFIG

    UNION

    SELECT KEYSTORE_ID

    FROM SAML_SERVICE_PROVIDER

    UNION

    SELECT KEYSTORE_ID

    FROM SERVER_CERTIFICATE)

SELECT keystore.id

FROM keystore

    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
```

```
WHERE KEYSTORE_ID IS NULL;
```

3. Limpe os órfãos usando a seguinte consulta.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
    WHERE id IN
    (
        SELECT keystore.id
```

```
        FROM keystore

            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID

        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'

    );
```

4. Adicione um índice à tabela KEYSTORE para melhorar a eficiência da pesquisa.

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";

ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;

CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("ID",
"TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "DESCRIPTION",
"ALIAS", "MODIFICATION_DATE");
```

Operações Baseadas em Painel

Você pode visualizar informações rapidamente acessando o painel do console XenMobile®. Com essas informações, você pode ver problemas e sucessos rapidamente usando widgets.

O painel é geralmente a tela que aparece quando você faz login pela primeira vez no console XenMobile. Para acessar o painel de outro local no console, clique em **Analisar**. Clique em **Personalizar** no painel para editar o layout da página e os widgets que aparecem.

- **Meus Painéis:** Você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e visualizar cada um selecionando o painel salvo.
- **Estilo de Layout:** Nesta linha, você pode selecionar quantos widgets aparecem no seu painel e como os widgets são organizados.
- **Seleção de Widget:** Você pode escolher quais informações aparecem no seu painel.
    - **Notificações:** Marque a caixa de seleção acima dos números à esquerda para adicionar uma barra de Notificações acima dos seus widgets. Esta barra mostra o número de dispositivos compatíveis, dispositivos inativos e dispositivos apagados ou registrados nas últimas 24 horas.
    - **Dispositivos por Plataforma:** Exibe o número de dispositivos gerenciados e não gerenciados por plataforma.

- **Dispositivos por Operadora:** Exibe o número de dispositivos gerenciados e não gerenciados por operadora. Clique em cada barra para ver um detalhamento por plataforma.
- **Dispositivos Gerenciados por Plataforma:** Exibe o número de dispositivos gerenciados por plataforma.
- **Dispositivos Não Gerenciados por Plataforma:** Exibe o número de dispositivos não gerenciados por plataforma. Os dispositivos que aparecem neste gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.
- **Dispositivos por Status do Gateway ActiveSync:** Exibe o número de dispositivos agrupados por status do Gateway ActiveSync. As informações mostram o status Bloqueado, Permitido ou Desconhecido. Você pode clicar em cada barra para detalhar os dados por plataforma.
- **Dispositivos por Propriedade:** Exibe o número de dispositivos agrupados por status de propriedade. As informações mostram o status de propriedade corporativa, de funcionário ou desconhecida.
- **Implantações de Grupo de Entrega com Falha:** Exibe o número total de implantações com falha por pacote. Apenas pacotes que tiveram implantações com falha aparecem.
- **Dispositivos por Motivo de Bloqueio:** Exibe o número de dispositivos bloqueados pelo ActiveSync
- **Aplicativos Instalados:** Ao usar este widget, você pode digitar o nome de um aplicativo, e um gráfico exibirá informações sobre esse aplicativo.
- **Uso de Licenças de Aplicativos de Compra por Volume:** Exibe estatísticas de uso de licenças para aplicativos de compra por volume da Apple.

Casos de uso

Alguns exemplos das muitas maneiras pelas quais você pode usar os widgets do painel para monitorar seu ambiente são os seguintes.

- Você implantou aplicativos de produtividade móvel e está recebendo tíquetes de suporte sobre falhas na instalação de aplicativos de produtividade móvel em dispositivos. Use os widgets **Dispositivos Fora de Conformidade** e **Aplicativos Instalados** para ver os dispositivos que não têm aplicativos de produtividade móvel instalados.
- Você gostaria de monitorar dispositivos inativos para poder removê-los do seu ambiente e recuperar licenças. Use o widget **Dispositivos Inativos** para acompanhar essa estatística.

- Você está recebendo tíquetes de suporte sobre dados que não estão sendo sincronizados corretamente. Você pode querer usar os widgets **Dispositivos por Status do Gateway ActiveSync** e **Dispositivos por Motivo de Bloqueio** para determinar se o problema está relacionado ao ActiveSync.

Relatórios

Depois que seu ambiente estiver configurado e os usuários se registrarem, você poderá executar relatórios para saber mais sobre sua implantação. O XenMobile vem com vários relatórios integrados para ajudá-lo a ter uma imagem melhor dos dispositivos em execução em seu ambiente. Para obter detalhes, consulte Relatórios.

> **Importante:**
>
> Embora seja possível usar o SQL Server para criar relatórios personalizados, a Citrix® não recomenda este método. Usar o banco de dados SQL Server dessa maneira pode ter consequências imprevistas em sua implantação do XenMobile. Se você decidir seguir este método de relatório, certifique-se de que as consultas SQL sejam executadas usando uma conta somente leitura.

Controle de Acesso Baseado em Função e Suporte XenMobile®

O XenMobile usa controle de acesso baseado em função (RBAC) para restringir o acesso de usuários e grupos às funções do sistema XenMobile, como o console XenMobile, Suporte Remoto e API pública. Este artigo descreve as funções integradas ao XenMobile e inclui considerações para decidir sobre um modelo de suporte para o XenMobile que usa RBAC.

> **Nota:**
>
> O Suporte Remoto não está mais disponível para novos clientes a partir de January 1, 2019. Clientes existentes podem continuar a usar o produto, no entanto, a Citrix® não oferece aprimoramentos ou correções.

Funções Integradas

Você pode alterar o acesso concedido às seguintes funções integradas e pode adicionar funções. Para o conjunto completo de permissões de acesso e recursos associados a cada função e suas configurações padrão, baixe Padrões de Controle de Acesso Baseado em Função da

documentação do XenMobile. Para uma definição de cada recurso, consulte Configurar funções com RBAC na documentação do XenMobile.

Função de administrador

Acesso padrão concedido:

- Acesso total ao sistema, exceto ao Suporte Remoto.
- Por padrão, os administradores podem realizar algumas tarefas de suporte, como verificar a conectividade e criar pacotes de suporte.

Considerações:

- Alguns ou todos os seus administradores precisam de acesso ao Suporte Remoto? Se sim, você pode editar a função de Administrador ou adicionar funções de Administrador.
- Para restringir ainda mais o acesso para alguns administradores ou grupos de administradores, adicione funções com base no modelo de Administrador e edite as permissões.

Suporte

Acesso padrão concedido:

- Acesso ao Suporte Remoto.

Considerações:

- Para implantações locais do XenMobile Server: O suporte remoto permite que os representantes do seu help desk assumam o controle remoto de dispositivos móveis Android gerenciados. A transmissão de tela é suportada apenas em dispositivos Samsung Knox.
- O suporte remoto não está disponível para implantações locais em cluster do XenMobile Server.

Usuário

Acesso padrão concedido:

- Acesso restrito ao console do XenMobile: recursos do dispositivo (como apagar, bloquear/desbloquear dispositivo; bloquear/desbloquear contêiner; ver localização e definir restrições geográficas; tocar o dispositivo; redefinir senha do contêiner); adicionar, remover e enviar convites de registro.

Considerações:

- A função de Usuário permite que você capacite os usuários a se ajudarem.
- Para oferecer suporte a dispositivos compartilhados, crie uma função de usuário para o registro de dispositivos compartilhados.

Considerações para um Modelo de Suporte do XenMobile

Os modelos de suporte que você pode adotar podem variar amplamente e podem envolver terceiros que manipular o suporte de nível 1 e 2, enquanto os funcionários manipular o suporte de nível 3 e 4. Independentemente de como você distribui a carga de suporte, tenha em mente as considerações nesta seção específicas para sua implantação do XenMobile e base de usuários.

Os usuários têm dispositivos corporativos ou BYO? A principal questão que influencia o suporte é quem possui os dispositivos dos usuários em seu ambiente XenMobile. Se seus usuários tiverem dispositivos corporativos, você poderá oferecer um nível de suporte mais baixo, como forma de bloquear os dispositivos. Nesse caso, você pode fornecer um help desk que auxilia os usuários com problemas de dispositivo e como usar os dispositivos. Dependendo dos tipos de dispositivos que você precisa suportar, considere como você pode usar as funções de Provisionamento e Suporte de Dispositivos RBAC para seu help desk.

Se seus usuários tiverem dispositivos BYO, sua organização pode esperar que os usuários encontrem suas próprias fontes de suporte para dispositivos. Nesse caso, o suporte que sua organização oferece é mais um papel administrativo focado em questões específicas do XenMobile.

Qual é o seu modelo de suporte para desktops? Considere se o seu modelo de suporte para desktops é apropriado para outros dispositivos corporativos. Você pode usar a mesma organização de suporte? Que treinamento extra eles precisam?

Deseja conceder aos usuários acesso ao Portal de Autoatendimento do XenMobile? Use **Configurações > Registro** para habilitar o Portal de Autoatendimento para um modo de segurança de registro. No Portal de Autoatendimento, os usuários podem gerar links de registro que lhes permitem registrar seus dispositivos ou enviar a si mesmos um convite de registro. Consulte Configurar modos de segurança de registro.

Monitoramento de Sistemas

Para garantir o tempo de atividade ideal para acesso e conectividade de aplicativos, você deve monitorar os seguintes componentes principais no ambiente XenMobile®.

Servidor XenMobile

O XenMobile Server gera e armazena logs no armazenamento local que você também pode exportar para um servidor de log do sistema (syslogs). Você pode configurar as definições de log para especificar restrições de tamanho, nível de log, ou pode criar loggers personalizados para filtrar eventos específicos. Você pode consultar os logs do XenMobile Server a qualquer momento a partir do console do XenMobile. Você também pode exportar informações nos logs via servidor syslog para seus servidores de log Splunk de produção.

A lista a seguir descreve os diferentes tipos de arquivos de log disponíveis no XenMobile:

Arquivo de log de depuração: Contém informações de nível de depuração sobre os principais serviços web do XenMobile, incluindo mensagens de erro e ações relacionadas ao servidor.

Formato da mensagem:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>
```

- onde `<id>` é um identificador exclusivo como sessionID.
- onde `<log message>` é a mensagem fornecida pelo aplicativo.

Arquivo de log de auditoria do administrador: Contém informações de auditoria sobre a atividade no console do XenMobile.

> **Nota:**
>
> O mesmo formato é usado para logs de auditoria do administrador e do usuário.
>
> Formato da mensagem:

Exceto pelos valores obrigatórios de Data e Carimbo de Data/Hora, todos os outros atributos são opcionais. Os campos opcionais são representados com " " na mensagem.

```
<date> <timestamp> "<username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>" "<application name>" "<app user id>" "<user agent>" "<details>"
```

A tabela a seguir lista os eventos de log de auditoria do administrador disponíveis:

MENSAGENS DE LOG DE AUDITORIA DO ADMINISTRADOR PARA EVENTOS	STATUS
Login	sucesso/falha
Logout	sucesso/falha
Obter administrador	sucesso/falha
Atualizar administrador	sucesso/falha
Obter aplicativo	sucesso/falha
Adicionar aplicativo	sucesso/falha
Atualizar aplicativo	sucesso/falha
Excluir aplicativo	sucesso/falha
Vincular aplicativo	sucesso/falha
Desvincular aplicativo	sucesso/falha
Desabilitar aplicativo	sucesso/falha
Habilitar aplicativo	sucesso/falha
Obter categoria	sucesso/falha
Adicionar categoria	sucesso/falha
Atualizar categoria	sucesso/falha
Excluir categoria	sucesso/falha
Adicionar certificado	sucesso/falha
Excluir certificado	sucesso/falha
Certificado ativo	sucesso/falha
Certificado CSR	sucesso/falha
Exportar certificado	sucesso/falha

MENSAGENS DE LOG DE AUDITORIA DO ADMINISTRADOR PARA EVENTOS	STATUS
Excluir cadeia de certificados	sucesso/falha
Adicionar cadeia de certificados	sucesso/falha
Obter conector	sucesso/falha
Adicionar conector	sucesso/falha
Excluir conector	sucesso/falha
Atualizar conector	sucesso/falha
Obter dispositivo	sucesso/falha
Bloquear dispositivo	sucesso/falha
Desbloquear dispositivo	sucesso/falha
Limpar dispositivo	sucesso/falha
Desfazer limpeza do dispositivo	sucesso/falha
Excluir dispositivo	sucesso/falha
Obter função	sucesso/falha
Adicionar função	sucesso/falha
Atualizar função	sucesso/falha
Excluir função	sucesso/falha
Vincular função	sucesso/falha
Desvincular função	sucesso/falha
Atualizar configurações	sucesso/falha
Atualizar e-mail de fluxo de trabalho	sucesso/falha
Adicionar fluxo de trabalho	sucesso/falha

MENSAGENS DE LOG DE AUDITORIA DO ADMINISTRADOR PARA EVENTOS	STATUS
Excluir fluxo de trabalho	sucesso/falha
Adicionar Active Directory	sucesso/falha
Atualizar Active Directory	sucesso/falha
Adicionar masteruserlist	sucesso/falha
Atualizar masteruserlist	sucesso/falha
Atualizar DNS	sucesso/falha
Atualizar Rede	sucesso/falha
Atualizar servidor de log	sucesso/falha
Transferir log do servidor de log	sucesso/falha
Atualizar syslog	sucesso/falha
Atualizar atualizações do receiver	sucesso/falha
Atualizar servidor de horário	sucesso/falha
Atualizar confiança	sucesso/falha
Adicionar registro de serviço	sucesso/falha
Atualizar registro de serviço	sucesso/falha
Atualizar e-mail do receiver	sucesso/falha
Carregar patch	sucesso/falha
Importar instantâneo	sucesso/falha
Obter detalhes do aplicativo da loja de aplicativos	sucesso/falha
Atualizar MDM	sucesso/falha

MENSAGENS DE LOG DE AUDITORIA DO ADMINISTRADOR PARA EVENTOS	STATUS
Excluir MDM	sucesso/falha
Adicionar HDX	sucesso/falha
Atualizar HDX	sucesso/falha
Excluir HDX	sucesso/falha
Adicionar Marca	sucesso/falha
Excluir Marca	sucesso/falha
Atualizar descarregamento SSL	sucesso/falha
Adicionar propriedade da conta	sucesso/falha
Excluir propriedade da conta	sucesso/falha
Atualizar propriedade da conta	sucesso/falha
Adicionar beacon	sucesso/falha

Arquivo de log de auditoria do usuário: Contém informações relacionadas à atividade do usuário de dispositivos registrados.

> **Nota:**
>
> O mesmo formato é usado para logs de auditoria de usuário e de administrador.
>
> Formato da mensagem:

Exceto pelos valores obrigatórios de Data e Carimbo de Data/Hora, todos os outros atributos são opcionais. Os campos opcionais são representados com " " na mensagem. Por exemplo,

```
<date> <timestamp> " <username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>" " <application name>" "<app user id>" "<user agent>" "<details>"
```

A tabela a seguir lista os eventos de log de auditoria do usuário disponíveis:

MENSAGENS DE LOG DE AUDITORIA DO USUÁRIO PARA EVENTOS	STATUS
Login	sucesso/falha
Tempo limite da sessão	sucesso/falha
Assinar	sucesso/falha
Cancelar inscrição	sucesso/falha
Pré-lançamento	sucesso/falha
AGEE SSO	sucesso/falha
Token SAML para Citrix Files	sucesso/falha
Registro de dispositivo	sucesso/falha
Verificação de dispositivo	bloquear/limpar
Atualização de dispositivo	sucesso/falha
Atualização de token	sucesso/falha
Segredo salvo	sucesso/falha
Segredo recuperado	sucesso/falha
Usuário iniciou a alteração da senha	sucesso/falha
Download do cliente móvel	sucesso/falha
Logout	sucesso/falha
Serviço de Descoberta	sucesso/falha
Serviço de Endpoint	sucesso/falha

FUNÇÕES MDM	STATUS
REGHIVE	sucesso/falha

FUNÇÕES MDM	STATUS
Inventário de Cab	sucesso/falha
Cab	sucesso/falha
Instalação automática de Cab	sucesso/falha
Instalação de shell de Cab	sucesso/falha
Criação de pasta Cab	sucesso/falha
Obtenção de arquivo Cab	sucesso/falha
Criar pasta de arquivo	sucesso/falha
Obter arquivo	sucesso/falha
Arquivo enviado	sucesso/falha
Criar pasta de script	sucesso/falha
Obter script	sucesso/falha
Script enviado	sucesso/falha
Execução de script shell	sucesso/falha
Execução automática de script	sucesso/falha
Inventário de APK	sucesso/falha
APK	sucesso/falha
Instalação de shell APK	sucesso/falha
Instalação automática de APK	sucesso/falha
Criar pasta APK	sucesso/falha
Obtenção de arquivo APK	sucesso/falha
Aplicativo APK	sucesso/falha

FUNÇÕES MDM	STATUS
Aplicativo EXT	sucesso/falha
Obter lista	sucesso/falha
Lista enviada	sucesso/falha
Localizar dispositivo	sucesso/falha
CFG	sucesso/falha
Desbloquear	sucesso/falha
Limpeza do SharePoint	sucesso/falha
Configuração do SharePoint	sucesso/falha
Remover perfil	sucesso/falha
Remover aplicativo	sucesso/falha
Remover aplicativo não gerenciado	sucesso/falha
Remover perfil não gerenciado	sucesso/falha
Aplicativo IPA	sucesso/falha
Aplicativo EXT	sucesso/falha
Aplicar código de resgate	sucesso/falha
Aplicar configurações	sucesso/falha
Habilitar rastreamento de dispositivo	sucesso/falha
Política de gerenciamento de aplicativos	sucesso/falha
Limpeza de cartão SD	sucesso/falha
Anexo de e-mail criptografado	sucesso/falha
Marca	sucesso/falha

FUNÇÕES MDM	STATUS
Navegador seguro	sucesso/falha
Navegador de contêiner	sucesso/falha
Desbloqueio de contêiner	sucesso/falha
Redefinição de senha do contêiner	sucesso/falha
Credenciais de autenticação do cliente AG	sucesso/falha

O Citrix ADC também monitora o estado do serviço web do XenMobile, que é configurado com sondas de monitoramento inteligentes para simular solicitações HTTP para cada nó do cluster do XenMobile Server. As sondas determinam se o serviço está online e, em seguida, respondem com base na resposta recebida. Caso um nó não responda como esperado, o Citrix ADC marca o servidor como inativo. Além disso, o Citrix ADC remove o nó do pool de balanceamento de carga e registra o evento para uso na geração de alertas por meio da solução de monitoramento do Citrix ADC.

Você também pode usar ferramentas de monitoramento de hipervisor padrão para monitorar as máquinas virtuais do XenMobile e fornecer alertas relevantes sobre métricas de utilização de CPU, memória e armazenamento.

SQL Server e banco de dados

O desempenho do SQL Server e do banco de dados afeta diretamente os serviços do XenMobile. A instância do XenMobile requer acesso ao banco de dados sempre e fica offline (por exemplo, para de responder) em caso de interrupção na infraestrutura SQL. O console do XenMobile pode continuar a funcionar por um tempo após quaisquer problemas de espaço em disco com o SQL Server. Para garantir o tempo de atividade máximo do banco de dados e desempenho adequado para a carga de trabalho do XenMobile, você deve monitorar proativamente o estado dos seus SQL Servers. Para obter mais informações sobre como monitorar seus SQL Servers, consulte Visão geral de monitoramento e ajuste de desempenho. Além disso, você deve ajustar a alocação de recursos para CPU, memória e armazenamento para garantir os acordos de nível de serviço à medida que seu ambiente XenMobile continua a crescer.

Citrix ADC

O Citrix ADC oferece a capacidade de registrar métricas no armazenamento interno ou enviar logs para um servidor de log externo. Você pode configurar o servidor syslog para exportar logs do

Citrix ADC para seus servidores de log Splunk de produção. Os seguintes níveis de log estão disponíveis no Citrix ADC:

- Emergência
- Alerta
- Crítico
- Erro
- Aviso
- Informação

Os arquivos de log também são armazenados no armazenamento do Citrix ADC no diretório /var/log/ns.log e nomeados newnslog. O Citrix ADC faz o rollover e compacta os arquivos usando o algoritmo GZIP. Os nomes dos arquivos de log são newnslog.xx.gz, onde xx representa um número sequencial.

O Citrix ADC também oferece suporte a traps e alertas SNMP como uma opção de monitoramento. Para obter uma lista de traps SNMP, consulte Monitoramento SNMP.

Recuperação de Desastres

Você pode arquitetar e configurar implantações do XenMobile® que incluem vários sites para recuperação de desastres usando uma estratégia de failover ativo-passivo.

A estratégia de recuperação de desastres recomendada discutida neste artigo consiste em:

- Um único site ativo do XenMobile no data center de uma localização geográfica, atendendo a todos os usuários corporativos globalmente, conhecido como site primário.
- Um segundo site do XenMobile no data center de uma segunda localização geográfica, conhecido como site de recuperação de desastres. Este site de recuperação de desastres fornece failover de site ativo-passivo caso ocorra uma falha de data center em todo o site no site primário. O site primário inclui XenMobile, banco de dados SQL e infraestrutura Citrix ADC para facilitar o failover e fornecer aos usuários acesso ao XenMobile em caso de falha de conectividade com o site primário.

Os servidores XenMobile no site de recuperação de desastres permanecem offline durante as operações normais e são colocados online apenas durante cenários de recuperação de desastres, onde é necessário um failover completo do site primário para o site de recuperação de desastres. Os servidores SQL no site de recuperação de desastres devem estar ativos e prontos para

atender às conexões antes de iniciar os servidores XenMobile no site de recuperação de desastres.

Esta estratégia de recuperação de desastres depende do failover manual da camada de acesso do Citrix ADC por meio de alterações de DNS para rotear as conexões MDM e MAM para o site de recuperação de desastres em caso de interrupção.

> **Nota:**
>
> Para usar essa arquitetura, você deve ter um processo em vigor para backups assíncronos dos bancos de dados e alguma forma de garantir alta disponibilidade para a infraestrutura SQL.

Processo de Failover de Recuperação de Desastres

1. Se você estiver testando seu processo de failover de recuperação de desastres, desligue os servidores XenMobile no site primário para simular uma falha do site.
2. Altere os registros DNS públicos para os servidores XenMobile para apontar para os endereços IP externos do site de recuperação de desastres.
3. Altere o registro DNS interno para o SQL Server para apontar para o endereço IP do SQL Server do site de recuperação de desastres.
4. Coloque os bancos de dados SQL do XenMobile online no site de recuperação de desastres. Certifique-se de que o SQL Server e o banco de dados estejam ativos e prontos para atender às conexões dos servidores XenMobile locais ao site.
5. Ligue os servidores XenMobile no site de recuperação de desastres.

Processo de Atualização do Servidor XenMobile

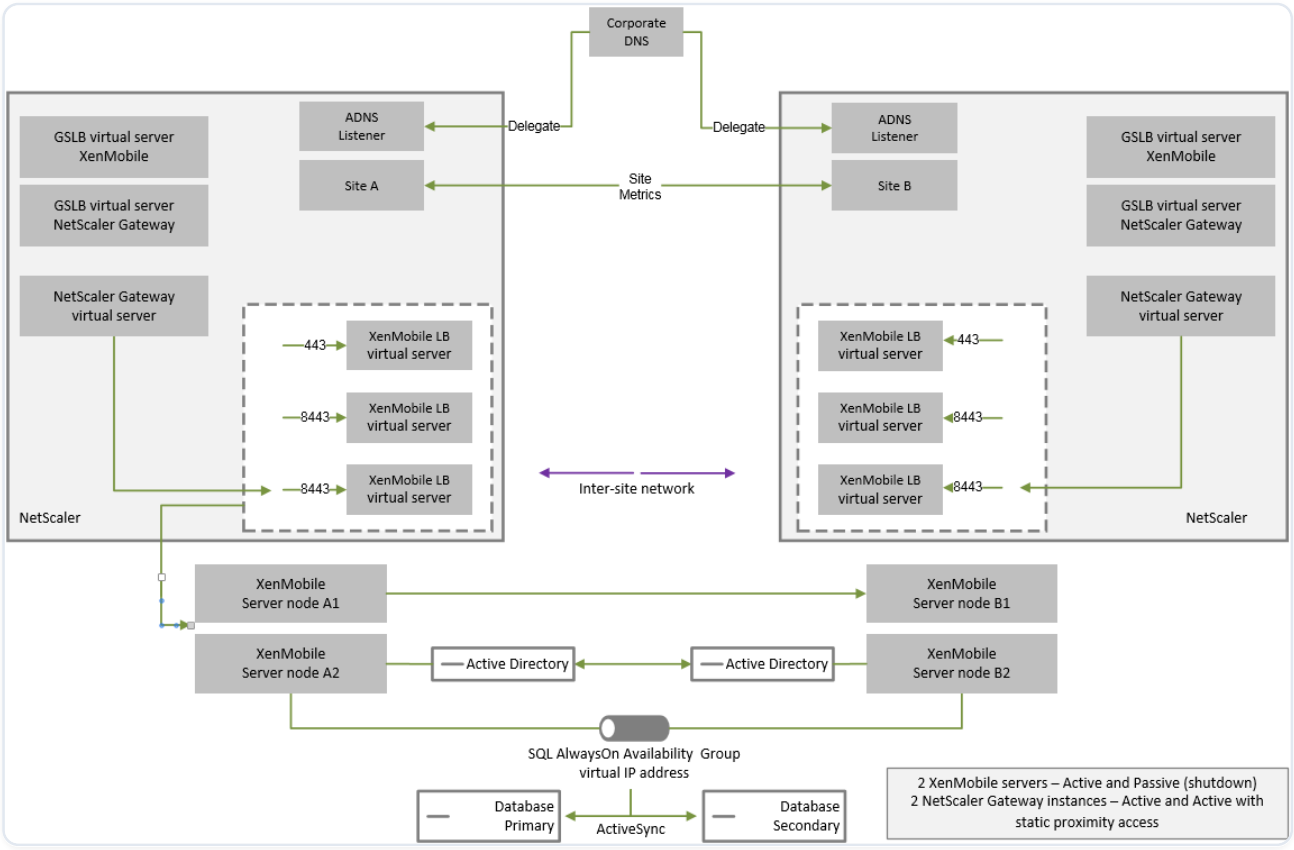
Siga estas etapas sempre que atualizar o XenMobile com patches e versões para manter o código dos servidores primário e de recuperação de desastres uniforme.

1. Certifique-se de que os Servidores XenMobile no site primário foram corrigidos ou atualizados.
2. Certifique-se de que o registro DNS para o SQL Server esteja sendo resolvido para o banco de dados SQL Server ativo no site primário.
3. Coloque os Servidores XenMobile do site de recuperação de desastres online. Os servidores se conectam ao banco de dados do site primário pela WAN apenas durante o processo de atualização.

4. Aplique os patches e atualizações necessários a todos os Servidores XenMobile do site de recuperação de desastres.
5. Reinicie os Servidores XenMobile e confirme se o patch ou a atualização foi bem-sucedido.

Diagrama de Arquitetura de Referência de Recuperação de Desastres

O diagrama a seguir mostra a arquitetura de alto nível para uma implantação de recuperação de desastres do XenMobile.



GSLB para Recuperação de Desastres

Um elemento chave desta arquitetura é o uso do Global Server Load Balancing (GSLB) para direcionar o tráfego para o data center correto.

Por padrão, o assistente do Citrix ADC para XenMobile configura o Citrix Gateway de uma forma que não permite o uso de GSLB para recuperação de desastres. Portanto, você deve tomar medidas adicionais.

Como o GSLB Funciona

O GSLB é, em sua essência, uma forma de DNS. Os dispositivos Citrix ADC participantes atuam como servidores DNS autoritativos e resolvem registros DNS para o endereço IP correto

(geralmente o VIP que deve receber o tráfego). O dispositivo Citrix ADC verifica a integridade do sistema antes de responder a uma consulta DNS que direciona o tráfego para esse sistema.

Quando um registro é resolvido, o papel do GSLB na resolução do tráfego está completo. O cliente se comunica diretamente com o endereço IP virtual (VIP) de destino. O comportamento do cliente DNS desempenha um papel importante no controle de como e quando um registro expira. Isso está amplamente fora dos limites do sistema Citrix ADC. Como tal, o GSLB está sujeito às mesmas limitações da resolução de nomes DNS. Os clientes armazenam respostas em cache, portanto, o balanceamento de carga dessa forma não é tão em tempo real quanto o balanceamento de carga tradicional.

A configuração do GSLB no Citrix ADC, incluindo sites, serviços e monitores, existe para fornecer a resolução de nomes DNS correta.

A configuração real para publicação de servidores (neste cenário, a configuração que o assistente do Citrix ADC para XenMobile cria) não é afetada pelo GSLB. O GSLB é um serviço separado no Citrix ADC.

Desafios com a Delegação de Domínio ao Usar GSLB com XenMobile

O assistente do Citrix ADC para XenMobile configura o Citrix Gateway para XenMobile. Este assistente gera três servidores virtuais de balanceamento de carga e um servidor virtual Citrix Gateway.

Dois dos servidores virtuais de balanceamento de carga manipular o tráfego MDM, nas portas 443 e 8443. O Citrix Gateway recebe o tráfego MAM e o encaminha para o terceiro servidor, o servidor virtual de balanceamento de carga MAM, na porta 8443. Todo o tráfego para o servidor virtual de balanceamento de carga MAM é passado através do Citrix Gateway.

O servidor virtual de balanceamento de carga MAM requer o mesmo certificado SSL que os Servidores XenMobile e usa o mesmo FQDN usado para registrar dispositivos. O servidor de balanceamento de carga MAM também usa a mesma porta (8443) que um dos servidores de balanceamento de carga MDM. Para permitir que o tráfego seja resolvido, o assistente do Citrix ADC para XenMobile cria um registro DNS local no Citrix Gateway. O registro DNS corresponde ao FQDN usado para registrar dispositivos.

Esta configuração é eficaz quando a URL do Servidor XenMobile não é uma URL de domínio GSLB. Se uma URL de domínio GSLB for usada como a URL do Servidor XenMobile, conforme exigido para recuperação de desastres, o registro DNS local impede que o Citrix Gateway resolva o tráfego para os servidores de balanceamento de carga MDM.

Usando o Método CNAME para Recuperação de Desastres GSLB

Para resolver os desafios apresentados pela configuração padrão criada pelo assistente do Citrix ADC para XenMobile, você pode criar um registro CNAME para o FQDN do Servidor XenMobile no domínio pai (`company.com`) e apontar um registro na subzona delegada (`gslb.company.com`) para a qual o Citrix ADC é autoritário. Isso permite a criação do registro DNS A estático para o endereço VIP de balanceamento de carga MAM necessário para resolver o tráfego.

1. No DNS externo, crie um CNAME para o FQDN do Servidor XenMobile que aponta para o FQDN do domínio GSLB no Citrix ADC GSLB. Você precisa de dois domínios GSLB: um para tráfego MDM e outro para tráfego MAM (Citrix Gateway).

   Exemplo:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. Na instância do Citrix Gateway de cada site, crie um servidor virtual GSLB com um FQDN que seja para onde o registro CNAME está apontando.

   Exemplo:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   Ao usar o assistente do Citrix ADC para XenMobile para implantar o Citrix Gateway, use a URL do XenMobile Server ao configurar o servidor de balanceamento de carga MAM. Isso cria um registro DNS A estático para a URL do XenMobile Server.

3. Teste com clientes se registrando no Secure Hub usando a URL do XenMobile Server (`xms.company.com`).

   Este exemplo usa os seguintes FQDNs:

   - `xms.company.com` é a URL usada pelo tráfego MDM e por dispositivos que se registram, que é configurada neste exemplo usando o assistente do Citrix ADC para XenMobile.
   - `xms.gslb.company.com` é o FQDN do domínio GSLB para o XenMobile Server.

Processo de Suporte Citrix

Você pode recorrer aos Serviços de Suporte Técnico da Citrix para ajudar com problemas relacionados aos produtos Citrix. O grupo oferece soluções alternativas e resoluções e trabalha em conjunto com as equipes de desenvolvimento para oferecer soluções.

Os Serviços Citrix ConsultingSM ou os Serviços Citrix Education oferecem ajuda relacionada a treinamento de produtos, aconselhamento sobre uso de produtos, configuração, instalação ou design e arquitetura de ambiente.

A Citrix Consulting ajuda com projetos relacionados a produtos Citrix, incluindo provas de conceito, avaliação de impacto econômico, verificações de integridade da infraestrutura, análise de requisitos de design, verificação de design de arquitetura, integração e desenvolvimento de processos operacionais.

A Citrix EducationSM oferece treinamento e certificação de TI de primeira linha em tecnologias de virtualização, nuvem e rede da Citrix.

A Citrix recomenda que você aproveite ao máximo os Recursos de Autoajuda e as recomendações da Citrix antes de criar um caso de suporte. Por exemplo, existem vários locais onde você pode acessar artigos e boletins escritos por especialistas técnicos da Citrix, consultar a documentação do produto para soluções e tecnologias Citrix, ou ler conversas diretas de executivos, equipes de produto e especialistas técnicos da Citrix. Consulte as páginas Knowledge Center, Product documentation e Blogs, respectivamente.

Para assistência mais interativa, você pode participar de fóruns de discussão onde pode fazer perguntas e obter respostas reais de outros clientes, compartilhar ideias, opiniões, informações técnicas e melhores práticas dentro de grupos de usuários e grupos de interesse, ou interagir com engenheiros de Suporte Citrix que monitoram os sites de redes sociais do Suporte Citrix. Consulte as páginas Support Forums e Citrix Community), respectivamente.

Você também tem acesso a cursos de treinamento e certificação para desenvolver suas habilidades. Consulte Citrix Education.

O Citrix Insight Services oferece uma plataforma de solução de problemas online simples e um verificador de integridade para seu ambiente Citrix. Disponível para XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor e Citrix Gateway. Consulte Analysis Tool.

Para buscar suporte técnico, você pode criar um caso de suporte por telefone ou via web. Você pode usar a web para problemas de baixa e média gravidade e a opção de telefone para problemas de alta gravidade. Para entrar em contato com o suporte para problemas do XenMobile, consulte Citrix Support Services.

Se você busca um ponto de contato único altamente treinado com vasta experiência na entrega de soluções Citrix, a Citrix Services oferece um Gerente de Relacionamento Técnico. Para obter mais informações sobre as ofertas e benefícios dos serviços Citrix, consulte Citrix Worldwide Services.

Enviando convites de inscrição de grupo no XenMobile®

Você pode enviar convites de inscrição para grupos e grupos aninhados no XenMobile Server. Convites de inscrição não estão disponíveis para dispositivos Windows.

Ao configurar o convite de grupo, você pode especificar uma ou várias plataformas de dispositivo. Você também pode marcar dispositivos para que possa, por exemplo, distinguir dispositivos de propriedade da empresa de dispositivos de propriedade do funcionário. Em seguida, você define o tipo de autenticação para os dispositivos do usuário.

> **Nota:**
>
> Se você planeja usar modelos de notificação personalizados, deve configurar os modelos antes de configurar os modos de segurança de inscrição. Para obter mais informações sobre modelos de notificação, consulte Criar e atualizar modelos de notificação.
>
> Para obter mais informações sobre configurações básicas de contas de usuário, funções e modos de segurança e convites de inscrição, consulte Contas de usuário, funções e inscrição.

Etapas gerais

1. No console do XenMobile, navegar para **Gerenciar > Convites de Inscrição**.
2. Clique em **Adicionar** no canto superior esquerdo da tela e, em seguida, clique em **Adicionar Convite**.
3. Clique em **Grupo** no menu **Destinatário**.

   Esta etapa permite que você escolha uma ou várias plataformas. Se você tiver uma mistura de diferentes plataformas de sistema operacional em sua empresa, escolha todas as plataformas. Limpe a seleção da plataforma apenas se tiver certeza de que nenhum usuário está usando a plataforma específica.
4. Você pode optar por marcar dispositivos durante o processo de convite. Escolha **Corporativo** ou **Funcionário**.

   A marcação facilita a separação de dispositivos de propriedade da empresa e dispositivos de propriedade do funcionário.
5. Na lista **Domínio**, escolha o domínio no qual o grupo existe.

6. Na lista **Grupo**, selecione o grupo do Active Directory para o qual você deseja enviar os convites.
7. O **Modo de inscrição** permite definir o tipo de segurança de autenticação que você prefere para os usuários.

    - Nome de usuário + Senha
    - Alta Segurança
    - URL de Convite
    - URL de Convite + PIN
    - URL de Convite + Senha
    - Dois Fatores
    - Nome de usuário + PIN

    > **Observação:**
    >
    > Para enviar convites de inscrição, você só pode usar os modos de segurança de inscrição **URL de Convite**, **URL de Convite + PIN** ou **URL de Convite + Senha**. Para dispositivos que se inscrevem com **Nome de usuário + Senha**, **Dois Fatores** ou **Nome de usuário + PIN**, os usuários devem inserir manualmente suas credenciais no Secure Hub.

8. Para os modelos **Download do Agente**, **URL de Inscrição**, **PIN de Inscrição** e **Confirmação de Inscrição**, escolha o modelo de notificação personalizado que você criou no passado ou escolha o padrão listado.

    Se você planeja usar modelos de notificação personalizados, você deve configurar os modelos antes de configurar os modos de segurança de inscrição. Para obter mais informações sobre modelos de notificação, consulte Notificações.

    Para esses modelos de notificação, use a configuração do seu servidor SMTP configurado no XenMobile. Defina suas informações de SMTP primeiro antes de prosseguir.

    > **Observação:**

> As opções **Expirar após** e **Tentativas Máximas** mudam com base na opção **Modo de inscrição** que você escolher. Você não pode alterar essas opções.

9. Selecione ATIVADO para **Enviar convite** e então clique em **Salvar e Enviar** para concluir o processo.

Suporte a grupos aninhados

Você pode usar grupos aninhados para enviar convites. Normalmente, grupos aninhados são usados em ambientes de grande escala onde grupos com permissões semelhantes estão vinculados uns aos outros.

navegar para **Configurações > LDAP** e então habilite a opção **Suporte a grupo aninhado**.

Solução de problemas e limitações conhecidas

Problema: Convites estão sendo enviados para usuários mesmo que eles tenham sido removidos de um grupo do Active Directory.

Solução: Dependendo do tamanho do seu ambiente Active Directory, pode levar até seis horas para que as alterações se propaguem para todos os servidores. Se um usuário ou grupo aninhado for removido recentemente, o XenMobile ainda pode considerar esses usuários como parte do grupo.

Portanto, é melhor esperar até seis horas antes de enviar outro convite de grupo para o seu grupo.

Configurando um servidor de Atestado de Integridade de Dispositivo (DHA) local

Você pode habilitar o Atestado de Integridade de Dispositivo (DHA) para dispositivos móveis Windows 10 e Windows 11 por meio de um servidor Windows local. Para habilitar o DHA localmente, primeiro você configura um servidor DHA.

Depois de configurar o servidor DHA, você cria uma política do XenMobile Server para habilitar o serviço DHA local. Para obter informações sobre como criar esta política, consulte Política de dispositivo de Atestado de Integridade de Dispositivo.

Pré-requisitos para um servidor DHA

- Um servidor executando o Windows Server Technical Preview 5 ou posterior, instalado usando a opção de instalação Experiência Desktop.
- Um ou mais dispositivos cliente Windows 10 e Windows 11. Esses dispositivos devem ter TPM 1.2 ou 2.0 executando a versão mais recente do Windows.
- Estes certificados:
  - **Certificado SSL DHA:** Um certificado SSL x.509 que se encadeia a uma raiz confiável corporativa com uma chave privada exportável. Este certificado protege as comunicações de dados DHA em trânsito, incluindo as seguintes comunicações:
    - servidor para servidor (serviço DHA e servidor MDM)
    - servidor para cliente (serviço DHA e um dispositivo Windows 10 ou Windows 11)
  - **Certificado de assinatura DHA:** Um certificado x.509 que se encadeia a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA usa este certificado para assinatura digital.
  - **Certificado de criptografia DHA:** Um certificado x.509 que se encadeia a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA também usa este certificado para criptografia.
- Escolha um destes modos de validação de certificado:
  - **EKCert:** O modo de validação EKCert é otimizado para dispositivos em organizações que não estão conectadas à Internet. Dispositivos que se conectam a um serviço DHA executando no modo de validação EKCert não têm acesso direto à Internet.
  - **AIKCert:** O modo de validação AIKCert é otimizado para ambientes operacionais que têm acesso à Internet. Dispositivos que se conectam a um serviço DHA executando no modo de validação AIKCert devem ter acesso direto à Internet e podem obter um certificado AIK da Microsoft.

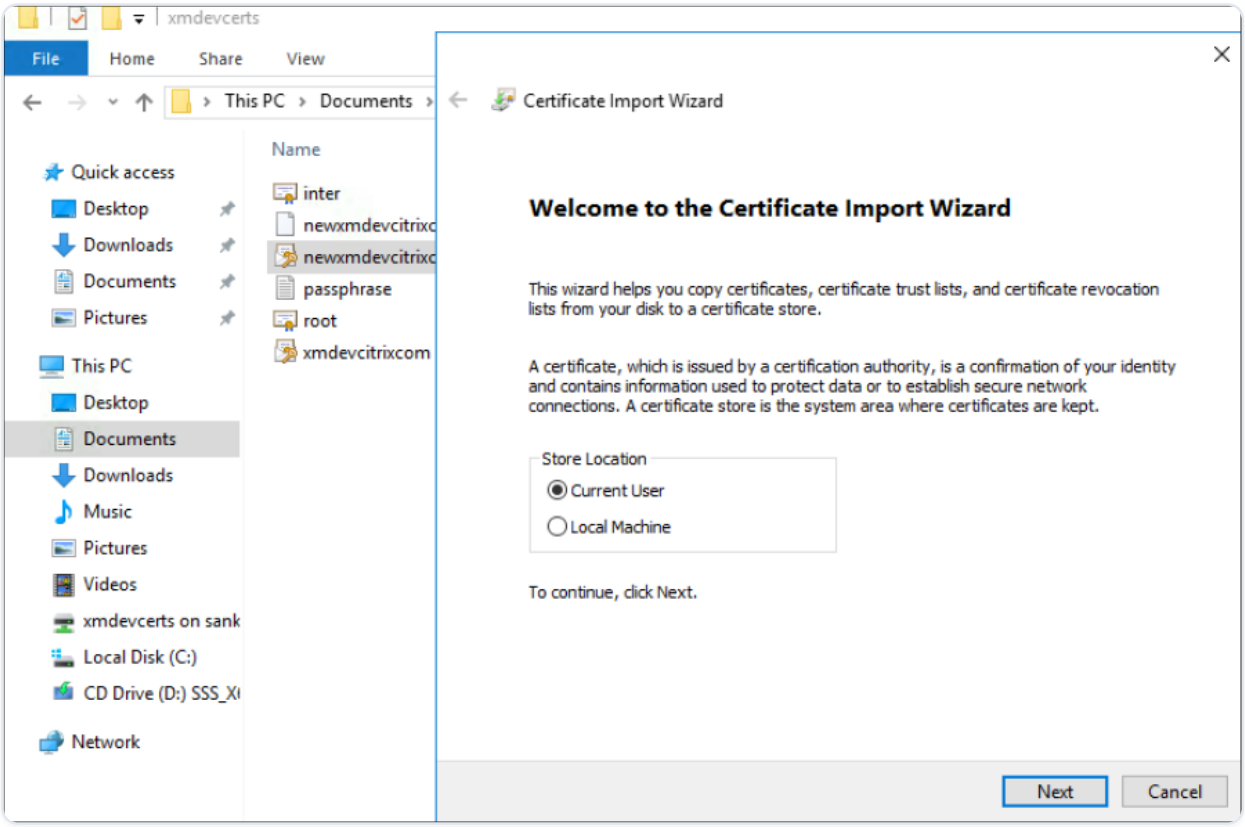
Adicionar a função de servidor DHA ao servidor Windows

1. No servidor Windows, se o Gerenciador do Servidor ainda não estiver aberto, clique em **Iniciar** e depois em **Gerenciador do Servidor**.
2. Clique em **Adicionar funções e recursos**.
3. Na página **Antes de começar**, clique em **Avançar**.

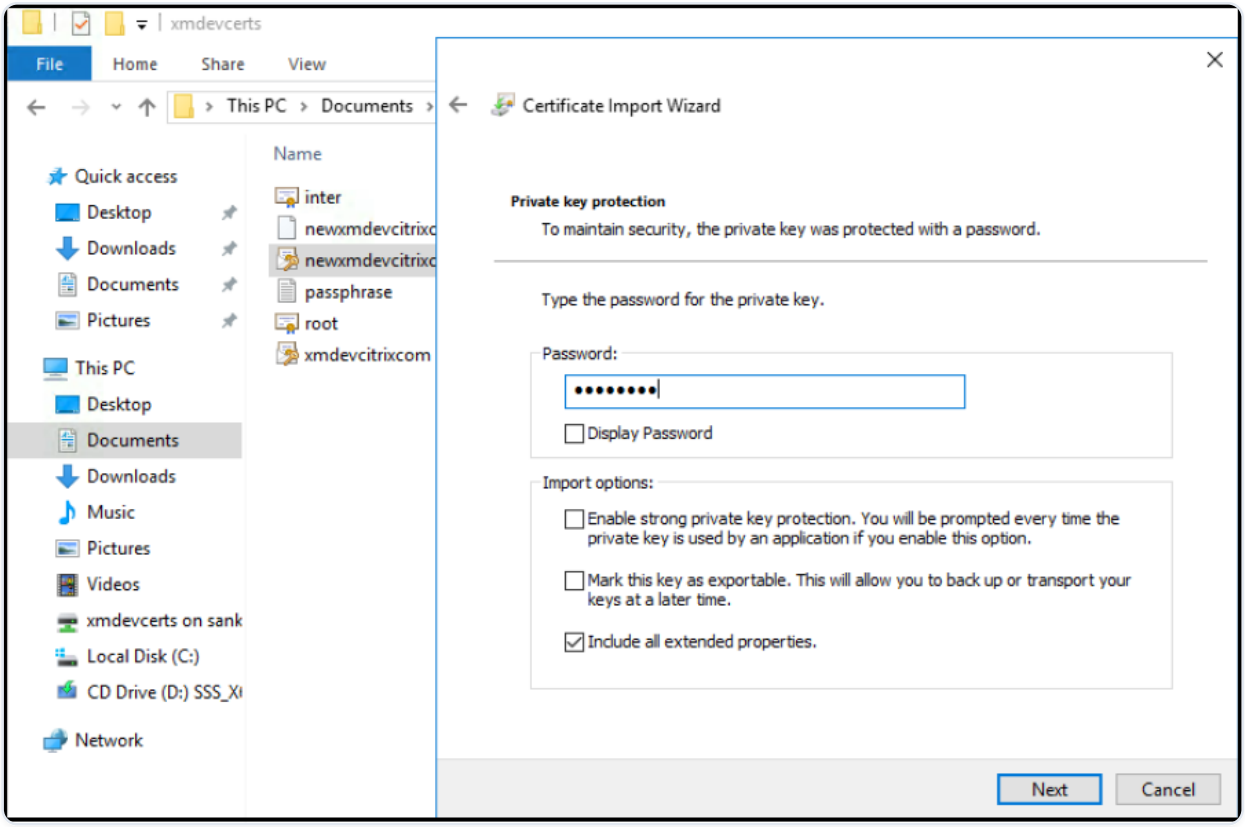
4. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e depois em **Avançar**.
5. Na página **Selecionar servidor de destino**, clique em **Selecionar um servidor do pool de servidores**, selecione o servidor e depois clique em **Avançar**.
6. Na página **Selecionar funções de servidor**, selecione a caixa de seleção Atestado de Integridade do Dispositivo.
7. Opcional: Clique em **Adicionar Recursos** para instalar outros serviços de função e recursos necessários.
8. Clique em **Avançar**.
9. Na página **Selecionar recursos**, clique em **Avançar**.
10. Na página **Função de Servidor Web (IIS)**, clique em **Avançar**.
11. Na página **Selecionar serviços de função**, clique em **Avançar**.
12. Na página **Serviço de Atestado de Integridade do Dispositivo**, clique em **Avançar**.
13. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
14. Quando a instalação for concluída, clique em **Fechar**.

Adicionar o certificado SSL ao armazenamento de certificados do servidor

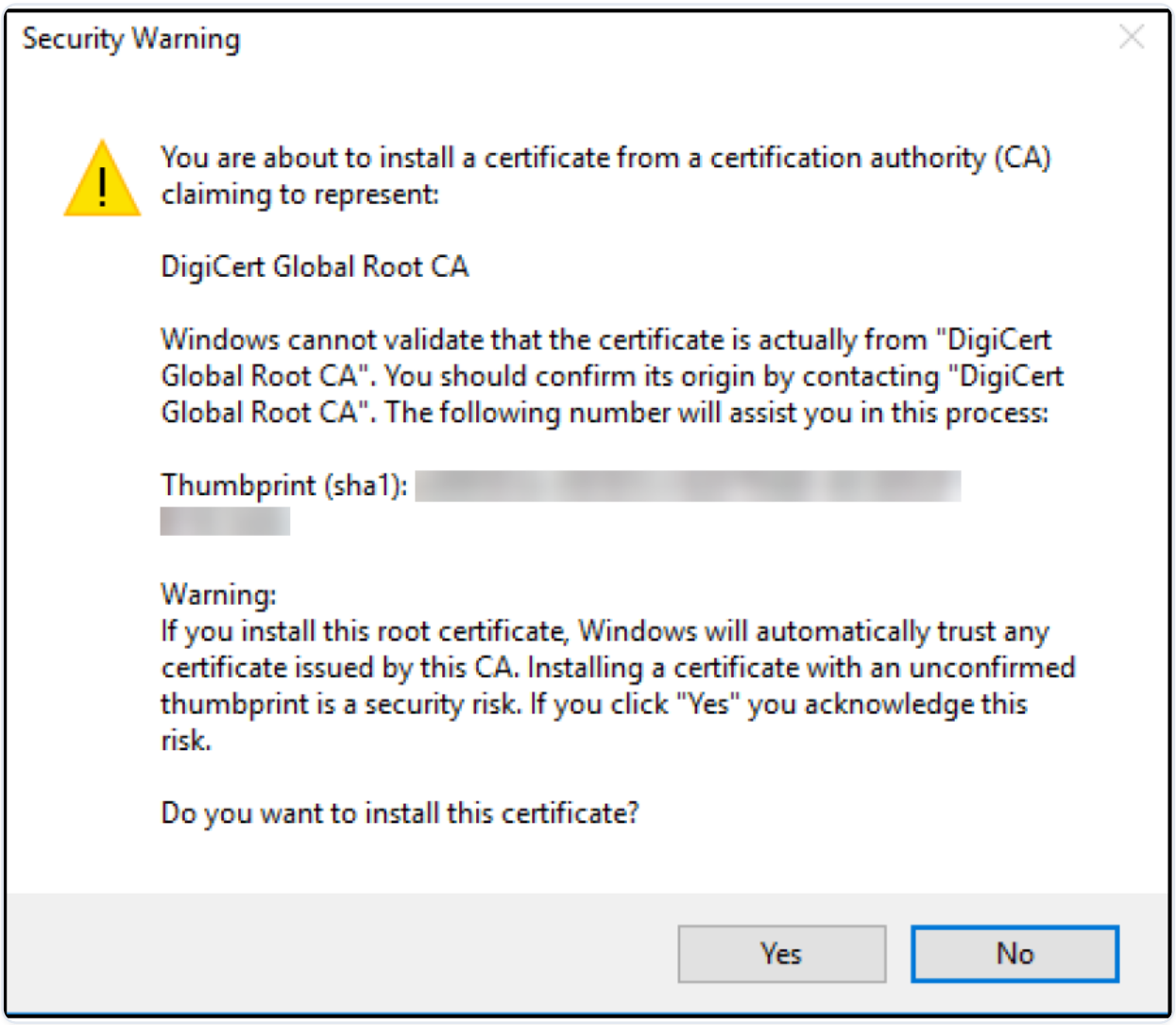
1. Vá para o arquivo de certificado SSL e selecione-o.
2. Selecione **Usuário atual** como o local de armazenamento e clique em **Avançar**.



3. Digite a senha da chave privada.
4. Certifique-se de que a opção de importação **Incluir todas as propriedades estendidas** esteja selecionada. Clique em **Avançar**.



5. Quando esta janela aparecer, clique em **Sim**.



6. Confirme se o certificado está instalado:

   a. Abra uma janela do Prompt de Comando.

   b. Digite **mmc** e pressione a tecla Enter. Para visualizar certificados no armazenamento da máquina local, você deve estar na função de Administrador.

   c. No menu Arquivo, clique em **Adicionar/Remover Snap-in**.

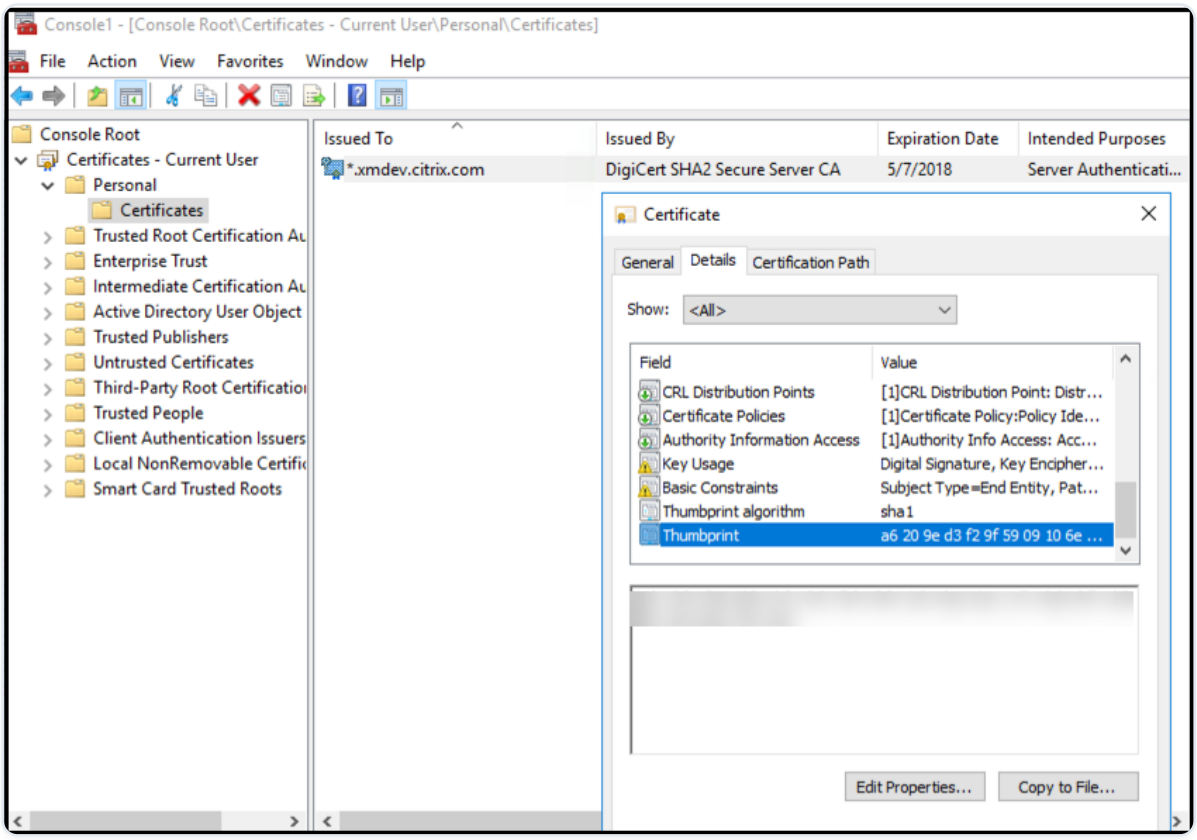
   d. Clique em **Adicionar**.

   e. Na caixa de diálogo Adicionar Snap-in Autônomo, selecione **Certificados**.

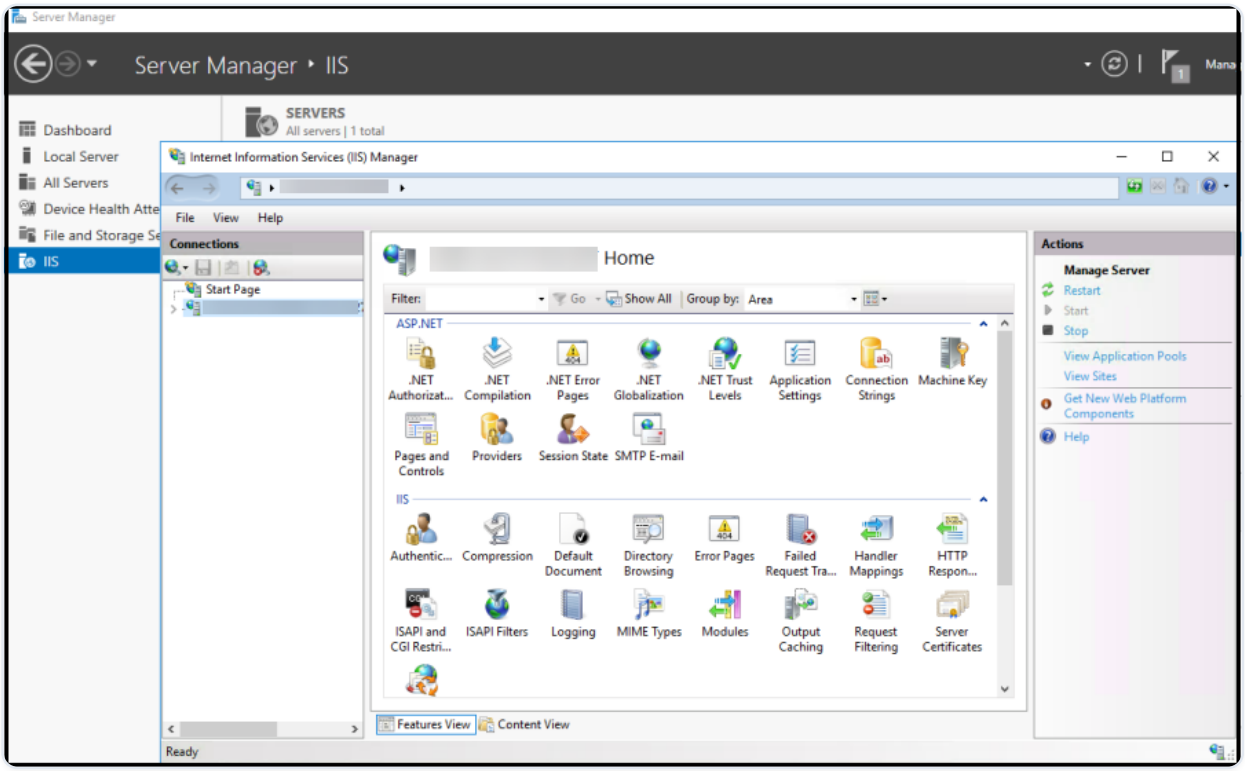
   f. Clique em **Adicionar**.

   g. Na caixa de diálogo **Certificates snap-in**, selecione **Minha conta de usuário**. (Se você estiver conectado como titular de uma conta de serviço, selecione **Conta de serviço**.)

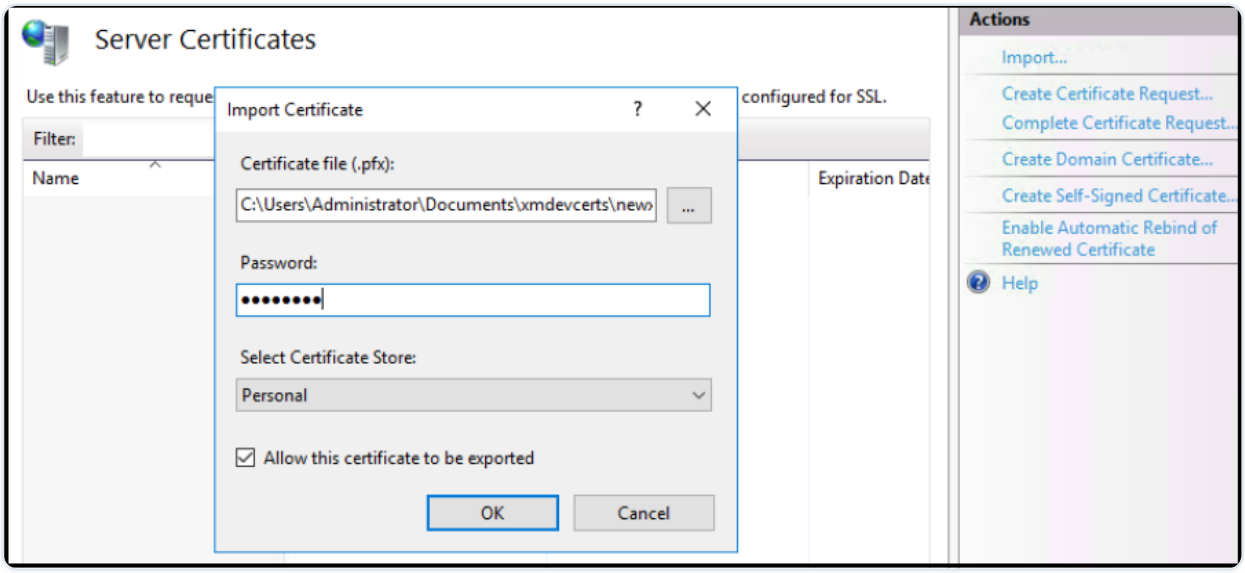
   h. Na caixa de diálogo Selecionar Computador, clique em **Concluir**.



7. Vá para **Gerenciador de Servidores > IIS** e selecione **Certificados de Servidor** na lista de ícones.

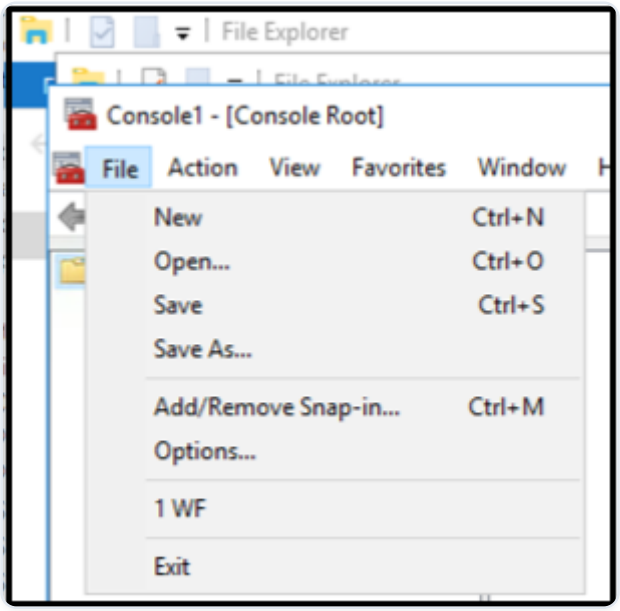


8. No menu Ação, selecione **Importar...** para importar o certificado SSL.

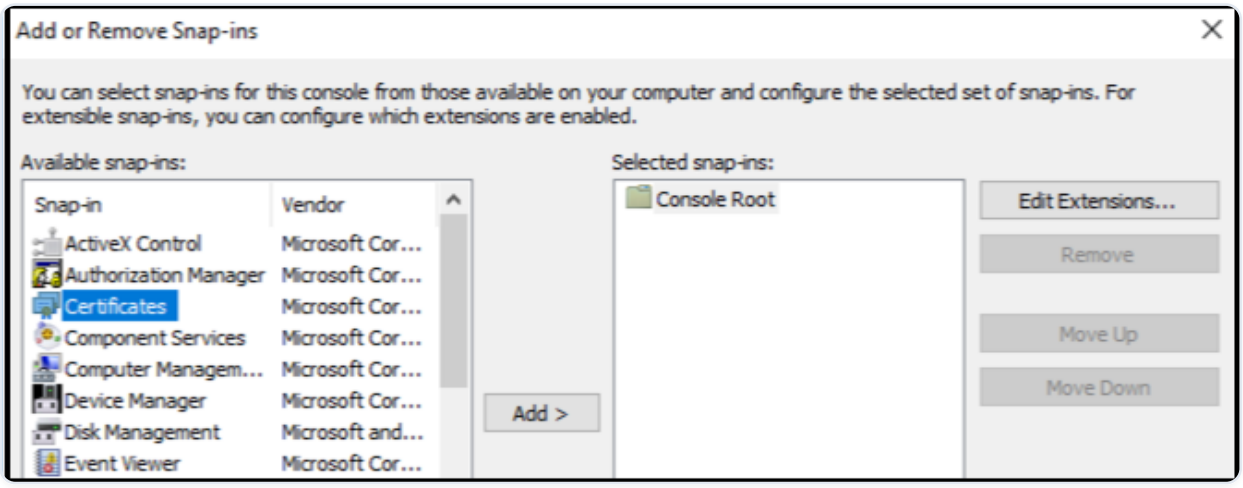


Recupere e salve a impressão digital do certificado

1. Na barra de pesquisa do Explorador de Arquivos, digite **mmc**.
2. Na janela Raiz do Console, clique em **Arquivo > Adicionar/Remover Snap-in…**.



3. Selecione o certificado de um snap-in disponível e adicione-o aos snap-ins selecionados.



4. Selecione **Minha conta de usuário**.

   Imagem de Adicionar ou Remover Snap-ins do Windows(/en-us/xenmobile/server/media/configure-dha-thumbprint3.png)

5. Selecione o certificado e clique em **OK**.

   Imagem de Adicionar ou Remover Snap-ins do Windows(/en-us/xenmobile/server/media/configure-dha-thumbprint4.png)

6. Clique duas vezes no certificado e selecione a guia **Detalhes**. Role para baixo para ver o thumbprint do certificado.

   Imagem de Adicionar ou Remover Snap-ins do Windows(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. Copie o thumbprint para um arquivo. Remova os espaços ao usar o thumbprint em comandos do PowerShell.

Instalar os certificados de assinatura e criptografia

Execute estes comandos do PowerShell no servidor Windows para instalar os certificados de assinatura e criptografia.

Substitua o espaço reservado ReplaceWithThumbprint e coloque-o entre aspas duplas, conforme mostrado.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
```

```
$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

Extrair o certificado raiz TPM e instalar o pacote de certificados confiáveis

Execute estes comandos no servidor Windows:

```
mkdir .\TrustedTpm


expand -F:\* .\TrustedTpm.cab .\TrustedTpm


cd .\TrustedTpm


.\setup.cmd
```

Configurar o serviço DHA

Execute este comando no servidor Windows para configurar o serviço DHA.

Substitua o espaço reservado ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint


-SigningCertificateThumbprint ReplaceWithThumbprint


-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint
```

```
-SupportedAuthenticationSchema "AikCertificate"
```

Execute estes comandos no servidor Windows para configurar a política de cadeia de certificados para o serviço DHA:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

Responda a estes prompts da seguinte forma:

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on target
"WIN-N27D1FKCEBT".

    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?
```

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

```
    Setting initial configuration for Device Health Attestation Service.


    Set initial configuration?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Registering User Access Logging.


    Register User Access Logging?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Verificar a configuração

Para verificar se o DHASActiveSigningCertificate está ativo, execute este comando no servidor:

`Get-DHASActiveSigningCertificate`

Se o certificado estiver ativo, o tipo de certificado (Assinatura) e o thumbprint serão exibidos.

Para verificar se o DHASActiveSigningCertificate está ativo, execute estes comandos no servidor

Substitua o placeholder ReplaceWithThumbprint e coloque-o entre aspas duplas, conforme mostrado.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force


Get-DHASActiveEncryptionCertificate
```

Se o certificado estiver ativo, o thumbprint aparecerá.

Para fazer uma verificação final, acesse este URL:

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1
```

Se o serviço DHA estiver em execução, aparecerá “Método não permitido”.



Configurando a autenticação baseada em certificado com EWS para notificações push do Secure Mail

Contribuído por Vijay Kumar Kunchakuri

Para garantir que as notificações push do Secure Mail funcionem, você deve configurar o Exchange Server para autenticação baseada em certificado. Isso é necessário quando o Secure Hub é registrado no XenMobile® com autenticação baseada em certificado.

Você precisa configurar o diretório virtual do Active Sync e do Exchange Web Services (EWS) no Exchange Mail Server com autenticação baseada em certificado.

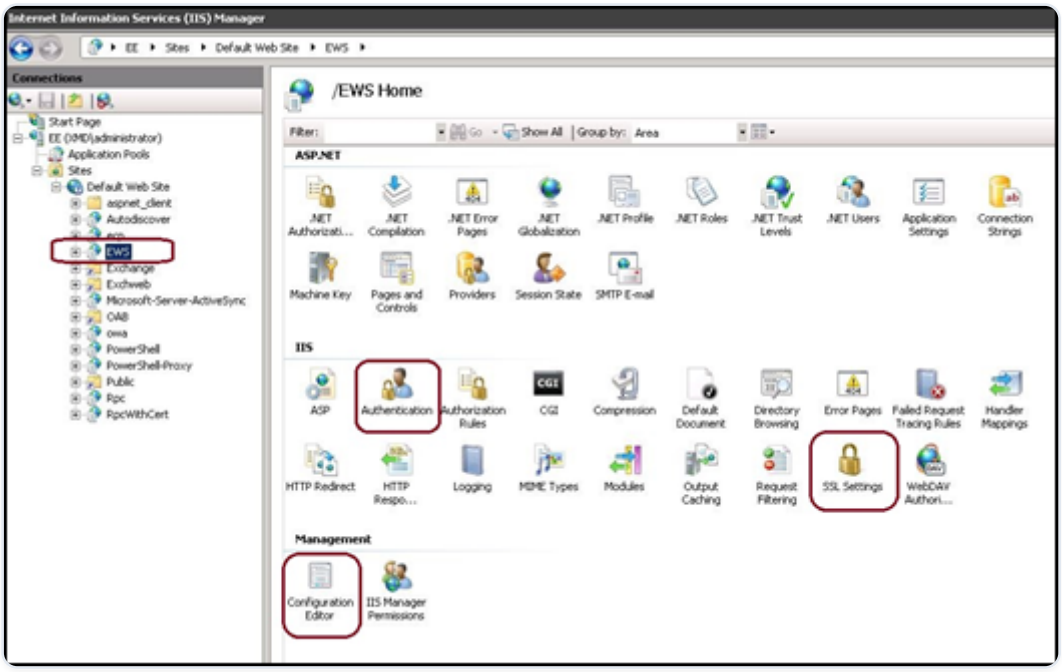
A menos que você conclua essas configurações, a assinatura para notificações push do Secure Mail falhará e nenhuma atualização de selo ocorrerá no Secure Mail.

Este artigo descreve as etapas para configurar a autenticação baseada em certificado. As configurações são especificamente para o diretório virtual EWS no Exchange Server.

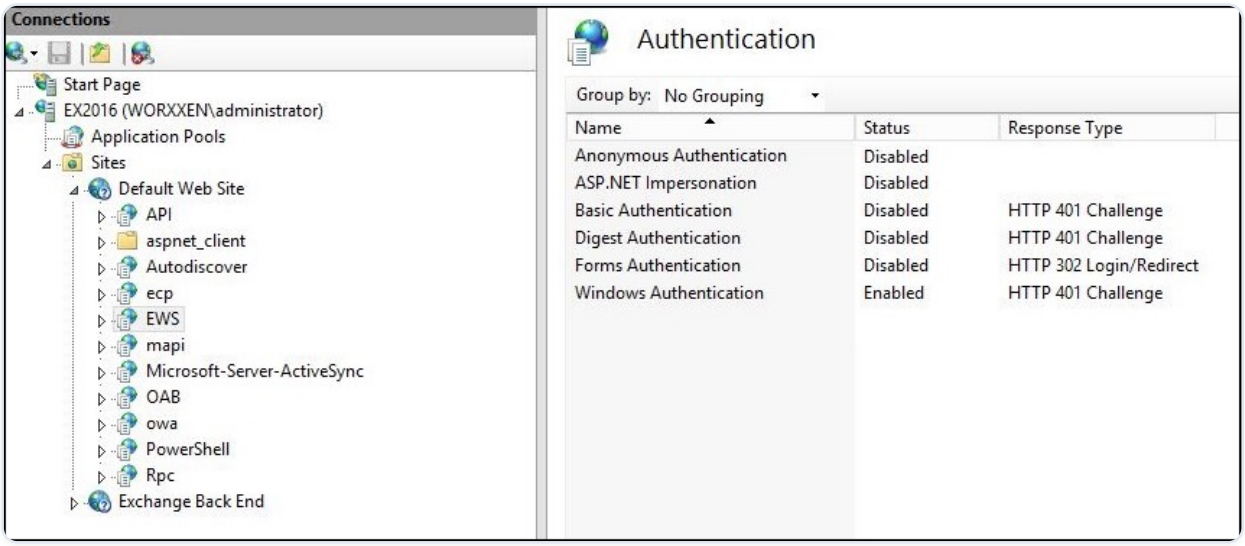
Para começar com a configuração, faça o seguinte:

1. Faça logon no servidor ou servidores onde o diretório virtual EWS está instalado.
2. Abra o Console do Gerenciador do IIS.
3. Em **Default Web Site**, clique no diretório virtual EWS.

   Os snap-ins de Autenticação, SSL, Editor de Configuração estão no lado direito do Console do Gerenciador do IIS



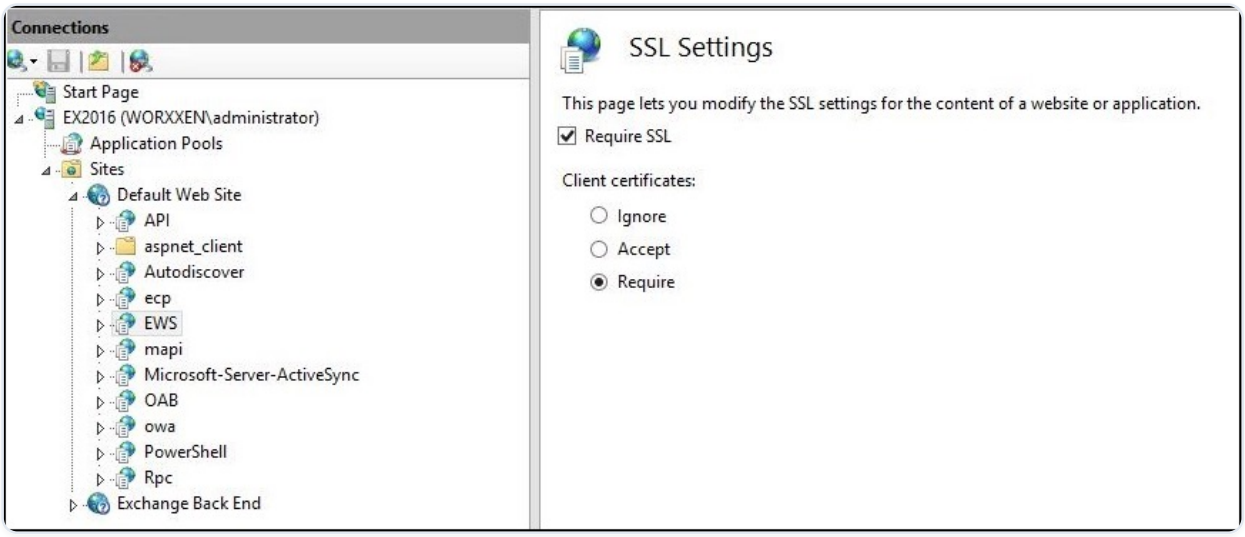
4. Certifique-se de que as configurações de **Autenticação** para EWS estejam configuradas conforme mostrado na figura a seguir.



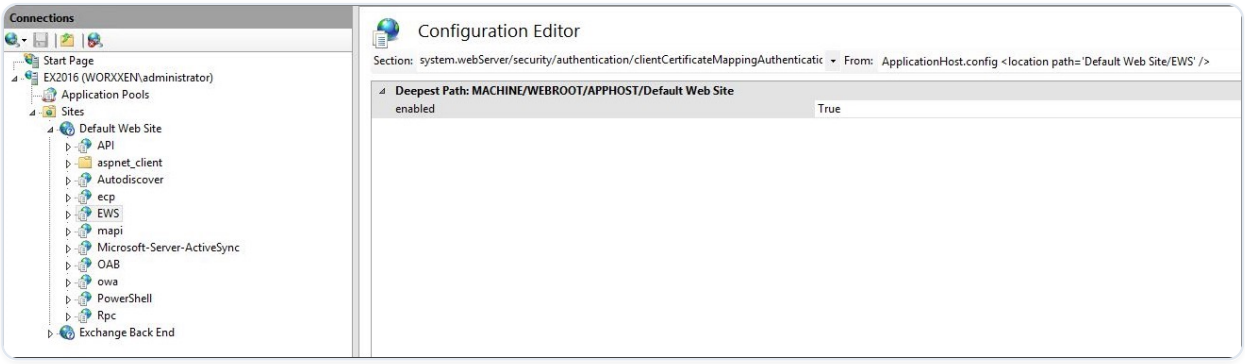
5. Configure as **Configurações de SSL** para o diretório virtual EWS.

    a. Marque a caixa de seleção **Require SSL**.

    b. Em **Client Certificates**, clique em **Require**. Você pode definir esta opção como **Accept** se outros clientes de e-mail EWS se conectarem com nome de usuário e senha como credenciais para autenticar e se conectar ao Exchange Server.



6. Clique em **Configuration Editor**. Na lista suspensa **Section**, navegar para a seguinte seção:
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. Defina o valor **enabled** como **True**.

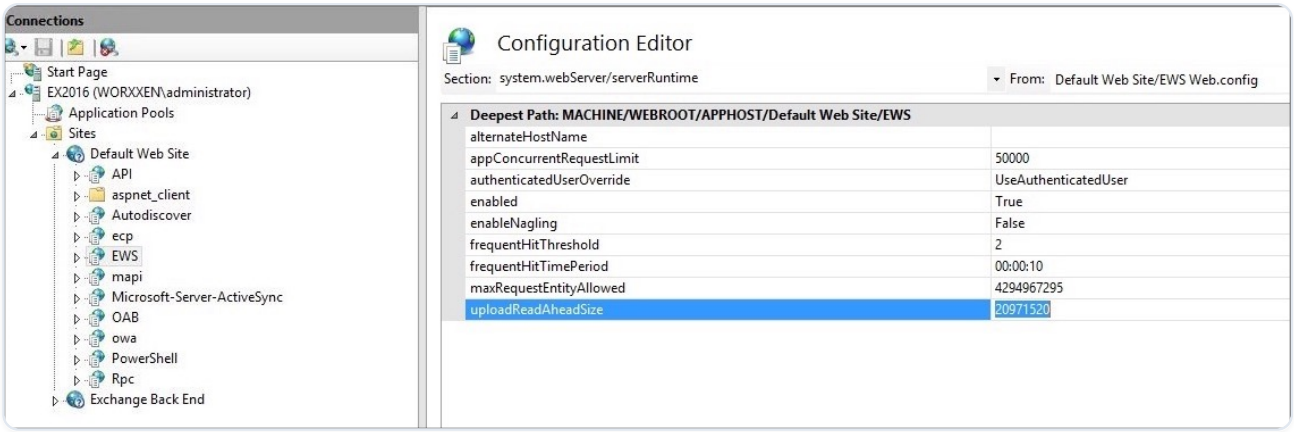


8. Clique em **Configuration Editor**. Na lista suspensa **Section**, navegar para a seguinte seção:
   - **system.webServer/serverRuntime**
9. Defina o valor **uploadReadAheadSize** como **10485760** (10 MB) ou **20971520** (20 MB) ou para um valor conforme exigido pela sua organização.

> **Importante:**
>
> Se você não definir este valor corretamente, a autenticação baseada em certificado ao assinar notificações push do EWS pode falhar com um código de erro 413.
>
> Não defina este valor como **0.**

Para mais informações, consulte os seguintes recursos de terceiros:

- Tempo de execução do servidor Microsoft IIS
- Butsch Client Management Blog



Para obter mais informações sobre como solucionar problemas do Secure Mail com notificações push do iOS, consulte este artigo do Citrix Support Knowledge Center.

Informações relacionadas

Notificações push para Secure Mail para iOS

Integrar o Gerenciamento de Dispositivos Móveis (MDM) do XenMobile® com o Cisco Identity Services Engine (ISE)

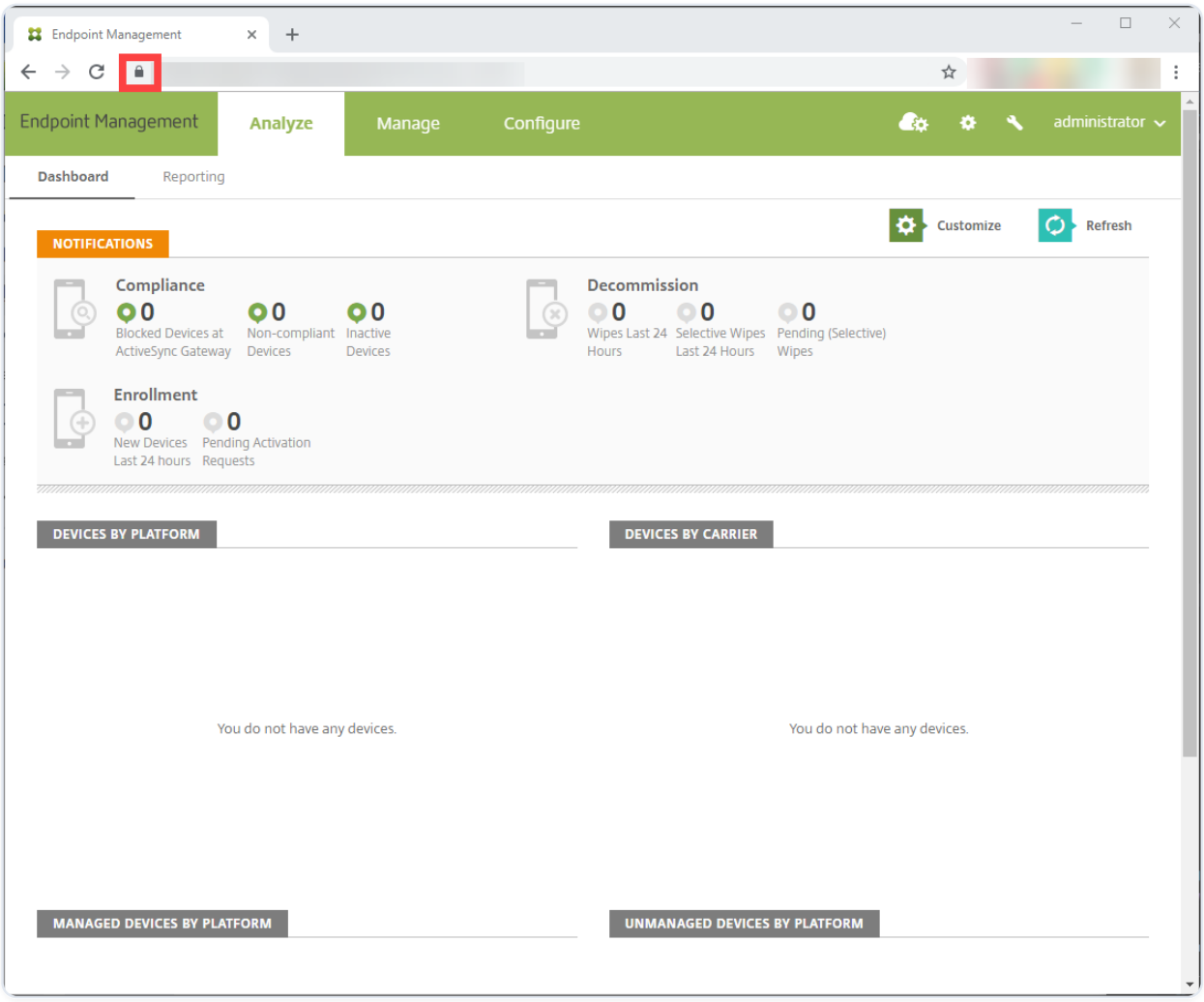
O Cisco ISE é usado para implantar, proteger, monitorar, integrar e gerenciar dispositivos móveis no local de trabalho. O software baixado para o dispositivo móvel controla o seguinte:

- Distribuição de aplicativos e patches
- Dados e configuração no endpoint

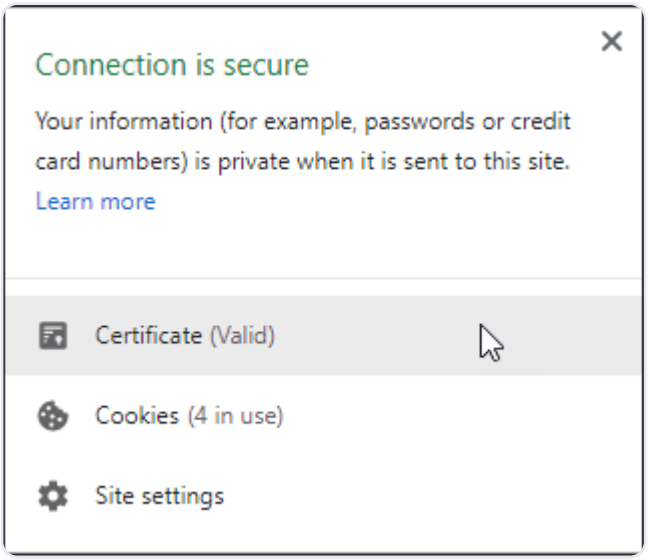
O XenMobile pode se integrar ao Cisco ISE para gerenciar dispositivos não conformes e não gerenciados no console do Cisco ISE. O XenMobile também permite que você permita, negue ou coloque em quarentena seletivamente o acesso a serviços corporativos.

Para configurar a integração com o XenMobile, crie uma conta de serviço local no XenMobile Server com a função RBAC de administrador atribuída a ela. Essa função permite que o Cisco ISE acesse a API do XenMobile. O ISE precisa confiar no certificado do XenMobile. Para baixar este certificado, abra um navegador da web e navegar para o URL do seu servidor e faça login.

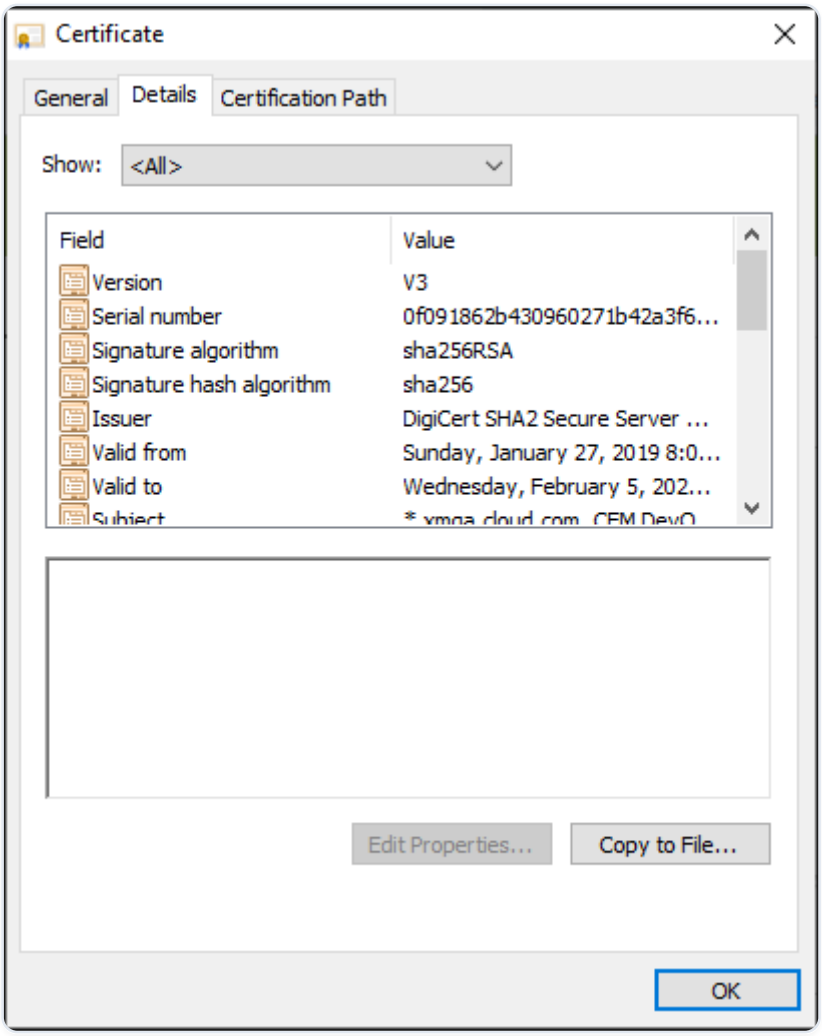
1. Após fazer login, clique no cadeado ao lado do URL na barra de endereços.



2. Clique em **Certificado**.



3. Selecione a guia **Detalhes** e clique em **Copiar para Arquivo**.



4. Siga o assistente para salvar o certificado localmente.
5. Faça login no seu console do Cisco ISE e importe o certificado do XenMobile que você baixou anteriormente. Importe o certificado para o armazenamento de Certificados Confiáveis do Cisco ISE. Isso é necessário para que o Cisco ISE confie na comunicação com o XenMobile Server.

    a. navegar para **Administração > Sistema > Certificados > Gerenciamento de Certificados > Certificados Confiáveis**. Clique em **Importar**.

    b. Dê um nome ao certificado e marque as caixas para **Confiar para autenticação dentro do ISE** e **Confiar para autenticação de Serviços Cisco**.

6. Adicione o XenMobile como um MDM externo dentro do Cisco ISE.

    a. navegar para **Administração > Recurso de Rede > MDM Externo**. Clique em **Adicionar** e preencha o seguinte:

        - **Host do Servidor:** Seu FQDN do XenMobile

- **Porta:** 443
- **Nome da instância:** O nome da instância do seu XenMobile Server. O nome da instância é "zdm" por padrão na maioria das implantações.
- **Nome de Usuário:** Digite o nome do usuário que você criou para esta tarefa. O usuário deve ser uma conta de administrador local no grupo RBAC de administrador original.
- **Senha:** A senha para o usuário que você acabou de adicionar.
- Marque onde diz **Habilitar**.

7. Se o teste for bem-sucedido, clique em **Enviar**.

Para obter mais informações sobre o Cisco ISE, consulte a documentação da Cisco.

> **Observação:**
>
> A integração do ISE não é suportada com o Endpoint Management hospedado.

Histórico de Documentos do Citrix XenMobile® Server

A tabela a seguir descreve alterações importantes na documentação do produto XenMobile Server. Para receber notificações sobre essas atualizações, assine o feed RSS.

DATA	ALTERAÇÃO	DESCRIÇÃO
27 Jan 2026	Notas de Versão para XenMobile Server 10.16 Rolling Patch 8	
20 Nov 2025	Notas de Versão para XenMobile Server 10.15 Rolling Patch 13	
13 Nov 2025	Notas de Versão para XenMobile Server 10.16 Rolling Patch 7	
23 Oct 2025	Notas de Versão para XenMobile Server 10.15 Rolling Patch 12	
26 Sep 2025	Notas de Versão para XenMobile Server 10.16 Rolling Patch 6	
13 May 2025	Notas de Versão para XenMobile Server 10.15 Rolling Patch 11	Consulte o artigo de suporte CTX693257.
15 Apr 2025	Notas de Versão para XenMobile Server 10.16 Rolling Patch 5	Consulte o artigo de suporte CTX692919.

DATA	ALTERAÇÃO	DESCRIÇÃO
27 Jan 2025	Notas de Versão para XenMobile Server 10.15 Rolling Patch 10	Consulte o artigo de suporte CTX692560.
18 Dec 2024	Notas de Versão para XenMobile Server 10.16 Rolling Patch 4	Consulte o artigo de suporte CTX692370.
04 Dec 2024	Notas de Versão para XenMobile Server 10.15 Rolling Patch 9	Consulte o artigo de suporte CTX692268.
28 Aug 2024	Notas de Versão para XenMobile Server 10.16 Rolling Patch 3	Consulte o artigo de suporte CTX691503.
11 Jul 2024	Notas de Versão para XenMobile Server 10.15 Rolling Patch 8	Consulte o artigo de suporte CTX691107.
02 Jul 2024	Notas de Versão para XenMobile Server 10.16 Rolling Patch 2	Consulte o artigo de suporte CTX678043.
17 Jun 2024	Notas de Versão para XenMobile Server 10.16 Rolling Patch 1	Consulte o artigo de suporte CTX677872.
06 Jun 2024	Notas de Versão para XenMobile Server 10.15 Rolling Patch 7	Consulte o artigo de suporte CTX677079.
08 Mar 2024	Notas de Versão para XenMobile Server 10.14 Rolling Patch 13	Consulte o artigo de suporte CTX628921.
06 Mar 2024	Notas de Versão para XenMobile Server 10.15 Rolling Patch 6	Consulte o artigo de suporte CTX625010.

DATA	ALTERAÇÃO	DESCRIÇÃO
13 Nov 2023	Notas de Versão para XenMobile Server 10.15 Rolling Patch 5	Consulte o artigo de suporte CTX583748.
19 Oct 2023	Notas de Versão para XenMobile Server 10.14 Rolling Patch 12	Consulte o artigo de suporte CTX582535.
18 Sep 2023	Notas de Versão para XenMobile Server 10.15 Rolling Patch 4	Consulte o artigo de suporte CTX579528.
19 Jul 2023	Notas de Versão para XenMobile Server 10.15 Rolling Patch 3	Consulte o artigo de suporte CTX565649.
31 May 2023	Notas de Versão para XenMobile Server 10.14 Rolling Patch 11	Consulte o artigo de suporte CTX558678.
26 Apr 2023	Notas de Versão para XenMobile Server 10.15 Rolling Patch 2	Consulte o artigo de suporte CTX546782.
11 Apr 2023	Adicionado um problema corrigido às Notas de Versão para XenMobile Server 10.14 Rolling Patch 10	Consulte problemas corrigidos.
23 Mar 2023	Notas de Versão para XenMobile Server 10.14 Rolling Patch 10	Consulte o artigo de suporte CTX491036.
23 Feb 2023	Notas de Versão para XenMobile Server 10.15 Rolling Patch 1	Consulte o artigo de suporte CTX478719.
20 Dec 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 9	Consulte o artigo de suporte CTX477055.

DATA	ALTERAÇÃO	DESCRIÇÃO
16 Nov 2022	Artigos atualizados para a versão 10.15 do XenMobile Server	Para um resumo dos recursos novos e alterados, consulte Novidades no XenMobile Server 10.15.
22 Sep 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 8	Consulte o artigo de suporte CTX464099.
08 Sep 2022	Notas de Versão para XenMobile Server 10.13 Rolling Patch 10	Consulte o artigo de suporte CTX463922.
18 Aug 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 7	Consulte o artigo de suporte CTX463691.
14 Jun 2022	Notas de Versão para XenMobile Server 10.13 Rolling Patch 9	Consulte o artigo de suporte CTX460128.
23 May 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 6	Consulte o artigo de suporte CTX459871.
12 Apr 2022	Notas de Versão para XenMobile Server 10.13 Rolling Patch 8	Consulte o artigo de suporte CTX447596.
30 Mar 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 5	Consulte o artigo de suporte CTX399411.
01 Mar 2022	Notas de Versão para XenMobile Server 10.13 Rolling Patch 7	Consulte o artigo de suporte CTX341602.
26 Jan 2022	Notas de Versão para XenMobile Server 10.14 Rolling Patch 4	Consulte o artigo de suporte CTX339069.

DATA	ALTERAÇÃO	DESCRIÇÃO
22 Dec 2021	Notas de Versão para XenMobile Server 10.14 Rolling Patch 3	Consulte o artigo de suporte CTX335897.
21 Dec 2021	Notas de Versão para XenMobile Server 10.13 Rolling Patch 6	Consulte o artigo de suporte CTX335875.
21 Dec 2021	Notas de Versão para XenMobile Server 10.12 Rolling Patch 11	Consulte o artigo de suporte CTX335861.
16 Dec 2021	Notas de Versão para XenMobile Server 10.12 Rolling Patch 10	Consulte o artigo de suporte CTX335785.
15 Dec 2021	Notas de Versão para XenMobile Server 10.14 Rolling Patch 2	Consulte o artigo de suporte CTX335763.
15 Dec 2021	Notas de Versão para XenMobile Server 10.13 Rolling Patch 5	Consulte o artigo de suporte CTX335753.
19 Nov 2021	Notas de Versão para XenMobile Server 10.14 Rolling Patch 1	Consulte o artigo de suporte CTX335342.
08 Oct 2021	Notas de Versão para XenMobile Server 10.12 Rolling Patch 9	Consulte o artigo de suporte CTX331040.
15 Sep 2021	Artigos atualizados para a versão 10.14 do XenMobile Server	Para um resumo dos recursos novos e alterados, consulte Novidades no XenMobile Server 10.14.
11 Aug 2021	Notas de Versão para XenMobile Server 10.13 Rolling Patch 4	Consulte o artigo de suporte CTX324159.

DATA	ALTERAÇÃO	DESCRIÇÃO
02 Jun 2021	Notas de Versão para XenMobile Server 10.12 Rolling Patch 8	Consulte o artigo de suporte CTX316910.
13 May 2021	Notas de Versão para XenMobile Server 10.13 Rolling Patch 3	Consulte o artigo de suporte CTX315034.
27 Apr 2021	Descrição atualizada da ação de segurança "Localizar"	Consulte Ações de segurança.
23 Apr 2021	Adicionado um exemplo de ação	Consulte Ações automatizadas.
01 Apr 2021	Adicionada descrição dos requisitos de VPN por aplicativo	Consulte Política de dispositivo VPN.
24 Feb 2021	Adicionado anúncio sobre a preparação necessária antes de atualizar endpoints para iOS 14.5	Consulte Antes de atualizar endpoints para iOS 14.5.
17 Dec 2020	Nova política de dispositivo para controlar como os aplicativos gerenciados instalados são atualizados no Android Enterprise	Consulte Política de dispositivo de atualização automática de aplicativos gerenciados
18 Nov 2020	Adicionada uma solução alternativa para um problema de logon único relacionado ao Citrix ADC local	Consulte Antes de atualizar um Citrix ADC local.
26 Oct 2020	Artigos atualizados para a versão 10.13 do XenMobile Server	Para um resumo dos recursos novos e alterados, consulte Novidades no XenMobile Server 10.13.
02 Jul 2020	Adicionada uma linha do tempo e um plano de ação	Consulte Prepare seus dispositivos Android para as próximas alterações.

DATA	ALTERAÇÃO	DESCRIÇÃO
	para a descontinuação da criptografia MDX	
19 Jun 2020	Abordados os termos “blacklist” e “whitelist” na documentação. Alterado para “lista de bloqueio” e “lista de permissão”.	O console do Endpoint Management atualmente inclui os termos “blacklist” e “whitelist”. Atualizamos a documentação. Estamos em processo de alteração dos termos no console do produto para uma próxima versão.
04 May 2020	Adicionada uma nota sobre os novos requisitos de certificado TLS para certificados confiáveis em iOS, iPadOS e macOS.	Consulte Certificados.
18 Feb 2020	Terminologia atualizada	Em toda a documentação, a terminologia do NetScaler®, NetScaler Gateway, ShareFile e controlador de zonas de armazenamento foi atualizada. Alguns componentes do console ainda podem exibir os nomes antigos.
06 Feb 2020	Artigos atualizados para a versão 10.12 do XenMobile Server	Para um resumo dos recursos novos e alterados, consulte Novidades no XenMobile Server 10.12.
06 Nov 2019	Adicionada uma seção sobre a migração do Apple VPP para ABM ou ASM	Consulte Migração do Programa de Compra por Volume da Apple para o Apple Business Manager (ABM) e o Apple School Manager (ASM).

DATA	ALTERAÇÃO	DESCRIÇÃO
04 Sep 2019	Artigos atualizados para a versão 10.11 do XenMobile Server	Para um resumo dos recursos novos e alterados, consulte Novidades no XenMobile Server 10.11.
15 May 2019	Seção de registro de dispositivo iOS atualizada	Adicionado vídeo e etapas atualizadas para o registro de dispositivo iOS 12. Consulte Registrar dispositivos iOS.
10 May 2019	Nova seção sobre Entrust PKI	Seção adicionada ao artigo "Entidades PKI": Entidades PKI.
03 Apr 2019	Nova seção para as etapas de renovação do Apple DEP	Seção adicionada a "Implantar dispositivos através do Apple DEP": Renovar sua inscrição no Programa de Implantação da Apple.
02 Apr 2019	Artigos atualizados para a versão 8.5.3 do conector Gateway para Exchange ActiveSync	Para um resumo dos recursos novos e alterados, consulte Novidades na versão 8.5.3.
26 Mar 2019	Sintaxe do nome da loja do Secure Hub atualizada	Adicionada nota sobre o requisito alfanumérico para o nome da "Loja" em Marca da loja de aplicativos e do Citrix Secure Hub.
06 Mar 2019	Artigos atualizados para a versão 10.1.9 do conector Endpoint Management para Exchange ActiveSync	Para um resumo dos recursos novos e alterados, consulte Novidades na versão 10.1.9.
01 Feb 2019	Artigos atualizados para a versão 10.1.8 do conector Endpoint Management para Exchange ActiveSync	Para um resumo dos recursos novos e alterados, consulte Novidades na versão 10.1.8.

DATA	ALTERAÇÃO	DESCRIÇÃO
23 Jan 2019	Terminologia "Secure Browse" atualizada	Em toda a documentação, a configuração MDX "Secure Browse" foi renomeada para "Tunneled Web SSO". Para obter informações, consulte Acesso à Rede de Aplicativos para iOS e Acesso à Rede de Aplicativos para Android.