Versão atual do XenMobile Server

Contents

Novidades no XenMobile Server 10.9 3

Novidades no XenMobile Server 10.8 8

Novidades no XenMobile Server 10.7 30

Avisos de terceiros 50

Problemas resolvidos 50

Problemas conhecidos 52

Arquitetura 53

Requisitos do sistema e compatibilidade 56

Compatibilidade do XenMobile 59

Sistemas operacionais compatíveis de dispositivos 61

Requisitos de porta 64

Escalabilidade e desempenho 73

Licenciamento 76

Conformidade com FIPS 140-2 83

Suporte a idiomas 84

Instalar e configurar 86

Configurar o modo FIPS com o XenMobile 102

Configurar o clustering 106

Guia de recuperação de desastres 117

Ativar servidores proxy 118

Configurar SQL Server 120

Propriedades do servidor 123

Opções da interface de linha de comando 139

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introdução aos fluxos de trabalho para o console XenMobile 155

Certificados e autenticação 159

NetScaler Gateway e XenMobile 171

Configure autenticação de domínio ou de domínio de segurança 180

Autenticação de certificado cliente ou certificado e domínio 187

Entidades PKI 211

Provedores de credenciais 236

Certificados APNs 245

SAML para login único com o ShareFile 252

Azure Active Directory como IDP 263

Credenciais derivadas 277

Atualização 297

Contas de usuário, funções e registro 302

Configurar funções com RBAC 319

Notificações 342

Dispositivos 354

ActiveSync Gateway 363

Android for Work 365

Clientes com “Android for Work legado for G Suite” 385

Registrar dispositivos iOS e macOS em massa 431

Propriedades do cliente 447

Implantar dispositivos macOS por meio do Apple DEP 459

Limite de registro de dispositivos 469

Registrar dispositivos 472

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Firebase Cloud Messaging **501**

Credenciais do Google Play **506**

Integração com os recursos do Apple Educação **507**

Controle de Acesso da Rede **535**

Samsung KNOX **538**

Ações de segurança **539**

Dispositivos compartilhados **553**

XenMobile Autodiscovery Service **558**

Políticas de dispositivo **564**

Políticas de dispositivo por plataforma **583**

Política de dispositivo de espelhamento de AirPlay **585**

Política de dispositivo do AirPrint **587**

Política de restrições de aplicativo do Android for Work **587**

Permissões do Android for Work **588**

Política de dispositivo do APN **590**

Política de dispositivo de acesso aos aplicativos **593**

Política de dispositivo de atributos de aplicativo **594**

Política de dispositivo de configuração de aplicativo **595**

Política de dispositivo de inventário de aplicativos **598**

Política de dispositivo de bloqueio de aplicativo **599**

Política de dispositivo de uso de rede de aplicativos **601**

Política de dispositivo de notificações de aplicativo **602**

Política de dispositivo de restrições de aplicativo **603**

Política de dispositivo de encapsulamento de aplicativo **604**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de desinstalação de aplicativo **608**

Política de dispositivo de restrições de desinstalação de aplicativo **609**

Política de dispositivo BitLocker **610**

Política de dispositivo de navegador **615**

Política de dispositivo de calendário (CalDav) **616**

Política de dispositivo celular **617**

Política de dispositivo do gerenciador de conexões **617**

Política de dispositivo de agendamento de conexão **618**

Política de dispositivo de contatos (CardDAV) **620**

Política de dispositivo Controlar atualizações do sistema operacional **621**

Política de dispositivo Copiar aplicativos para o contêiner da Samsung **625**

Política de dispositivo de credenciais **626**

Política de dispositivo de XML personalizado **632**

Política de dispositivo do Defender **633**

Política de dispositivo de excluir arquivos e pastas **635**

Política de dispositivo Excluir chaves e valores do Registro **635**

Política de dispositivo de Atestado de Integridade de Dispositivo **636**

Política de dispositivo de nome do dispositivo **637**

Política de dispositivo Configuração de Educação **638**

Política de dispositivo do Hub Empresarial **641**

Política de dispositivo do Exchange **642**

Política de dispositivo de arquivo **650**

Política de dispositivo FileVault **651**

Política de dispositivo de fonte **653**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de layout de tela inicial **654**

Política de dispositivo de importação do perfil de iOS e macOS **655**

Política de dispositivo do quiosque para Samsung SAFE **657**

Política de dispositivos de configuração de Launcher para Android **659**

Política de dispositivo do LDAP **660**

Política de dispositivo de localização **662**

Política de dispositivo de email **666**

Política de dispositivo de domínios gerenciados **668**

Políticas de dispositivo das opções de MDM **670**

Política de dispositivo de informação da organização **672**

Política de dispositivo de código secreto **672**

Política de dispositivo do ponto de acesso pessoal **685**

Política de dispositivo de remoção de perfil **685**

Política de dispositivo do perfil de provisionamento **686**

Política de dispositivo da remoção de perfil de provisionamento **688**

Política de dispositivo de proxy **688**

Política de dispositivo do Registro **690**

Suporte remoto à política de dispositivo **691**

Política de dispositivo de restrições **692**

Política de dispositivo em roaming **718**

Política de dispositivo de chave de licença MDM Samsung **719**

Política de dispositivo de firewall do Samsung SAFE **721**

Política de dispositivo do SCEP **722**

Siri e políticas de ditado **726**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de dispositivo de conta SSO 727

Política de dispositivo de criptografia de armazenamento 728

Política de dispositivo de loja 730

Política de dispositivo de Calendários inscritos 730

Política de dispositivo dos termos e condições 731

Política de dispositivo do VPN 731

Política de dispositivo de papel de parede 779

Política de dispositivo de filtro de conteúdo Web 780

Política de dispositivo de clipe Web 782

Política de dispositivo de WiFi 783

Política de dispositivo do certificado do Windows CE 795

Política de dispositivo Proteção de informações do Windows 796

Políticas de dispositivo das opções de XenMobile 801

Política de dispositivo de desinstalação do XenMobile 804

Adicionar aplicativos 804

Tipos de conector de aplicativo 846

Atualizar aplicativos MDX ou empresariais 847

Resumo das políticas de aplicativos MDX 849

Identidade visual do XenMobile Store e do Citrix Secure Hub 849

Citrix Launcher 851

Programa de compra por volume do iOS 853

XenApp e XenDesktop através do Citrix Secure Hub 861

Uso do ShareFile com o XenMobile 862

SmartAccess para aplicativos HDX 877

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar mídia 896

Implantar recursos 901

Macros 917

Ações automatizadas 948

Monitoração e suporte 956

Anonimizar dados nos pacotes de suporte 959

Verificações de conectividade 960

Programa de Melhoria de Experiência do Cliente 963

Logs 965

Provedor de serviços móveis 972

Relatórios 973

SNMP monitoring 978

Pacotes de suporte 987

Opções de suporte e suporte remoto 992

Syslog 1000

Exibir e analisar arquivos de log no XenMobile 1001

Ferramenta XenMobile Analyzer 1003

APIs REST 1022

Conector de Endpoint Management para Exchange ActiveSync 1024

Conector Citrix Gateway para Exchange ActiveSync 1077

Conceitos avançados 1093

Interação do XenMobile no local com o Active Directory 1093

Implantação do XenMobile 1098

Modos de gerenciamento 1100

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos de dispositivo **1107**

Segurança e experiência do usuário **1108**

Aplicativos **1128**

Comunidades do usuário **1135**

Estratégia de email **1143**

Integração do XenMobile **1152**

Requisitos para vários locais **1161**

Integração com o NetScaler Gateway e NetScaler **1162**

Considerações sobre SSO e proxy para aplicativos MDX **1173**

Autenticação **1179**

Arquitetura de referência para implantações locais **1195**

Propriedades do servidor **1205**

Políticas de dispositivos e aplicativos **1207**

Opções de registro do usuário **1219**

Ajuste das operações do XenMobile **1223**

Provisionamento e desprovisionamento de aplicativos **1229**

Operações baseadas em painel **1233**

Controle de Acesso Baseado em Função e Suporte XenMobile **1235**

Monitoramento de sistemas **1238**

Recuperação de desastres **1245**

Processo de Suporte Citrix **1249**

Enviar convites para registro em grupo no XenMobile **1250**

Configurar um servidor de atestado de integridade de dispositivo no local **1252**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar a autenticação baseada em certificado com o EWS para notificações por push do Secure Mail **1263**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Novidades no XenMobile Server 10.9

April 15, 2019

> Importante:
>
> Para se preparar para atualizações de dispositivos para o iOS 12: o tipo de conexão Citrix VPN na política de dispositivos VPN para iOS não suporta o iOS 12. Exclua sua política de dispositivo VPN e crie uma nova 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 10.9, durante o registro do usuário.

Serviço de migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para obter mais informações, entre em contato com o pessoal de vendas local da Citrix, com um engenheiro de sistemas ou com um parceiro Citrix. Estes blogs discutem o Serviço de Migração do XenMobile:

Novo serviço de migração do XenMobile

Criando o cenário para o XenMobile na Nuvem

Alteração do fluxo de trabalho de registro do MDM iOS

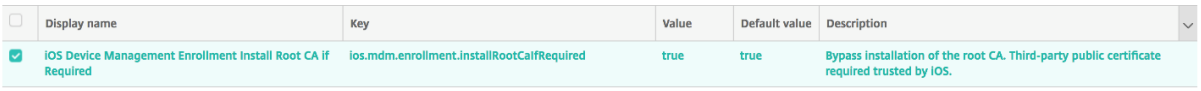
Para melhorar a segurança da plataforma reduzindo as instalações de perfis enganosas, a Apple planeja introduzir um novo fluxo de trabalho para registrar manualmente dispositivos no MDM. O novo fluxo de trabalho afeta todas as soluções MDM, incluindo o Citrix XenMobile Server.

O novo fluxo de trabalho de registro exigirá que os usuários instalem manualmente os perfis MDM. Para fazer isso, os usuários navegam até a página **Configurações**, tocam em **Geral** e, em seguida, tocam em **Perfis**. A lista de Perfis disponíveis para instalação é exibida em seguida. Se o usuário não instalar o perfil dentro de 24 horas após baixá-lo, o perfil será excluído automaticamente.

Não há alteração do registro MDM em servidores atribuídos no Apple Business Manager ou no Apple School Manager. No entanto, o fluxo de trabalho para o registro manual no MDM é alterado. Atualmente, os usuários de dispositivos iOS recebem dois prompts durante o registro: para o certificado de dispositivo MDM e a AC raiz. Como parte da atualização da Apple, os usuários de dispositivos iOS receberão somente a solicitação do certificado de dispositivo MDM durante o registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Se você usa certificados confiáveis: para proporcionar uma melhor experiência ao usuário depois que a Apple implementar a alteração do fluxo de trabalho, 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 no MDM para simplificar a instalação do perfil para os usuários.



Display name	Key	Value	Default value	Description
iOS Device Management Enrollment Install Root CA if Required	ios.mdm.enrollment.installRootCaIfRequired	true	true	Bypass installation of the root CA. Third-party public certificate required trusted by iOS.

Se você usa certificados autoassinados: deixe o valor da propriedade `ios.mdm.enrollment.installRootCaIfRequired` definido como **`true`**. Os usuários continuarão a receber o prompt para instalar a AC raiz.

Para obter mais informações, consulte o blog Changes ahead for Citrix Endpoint Management MDM enrollment process.

Antes de uma atualização para o XenMobile 10.9

1. Atualize o seu Citrix License Server para 11.15 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.9.

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

   > Nota:
   >
   > Esteja ciente de que a data de Subscription Advantage (SA) no XenMobile 10.9 é 14 de setembro de 2018. A data de Subscription Advantage (SA) em sua licença Citrix deve ser posterior a essa data. Você pode ver sua data de SA ao lado da licença do 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 as em sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte https://support.citrix.com/article/CTX209580.

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

3. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a quantidade mínima de RAM recomendada é de 8 GB para ambientes de produção.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Após uma atualização para o XenMobile 10.9

Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: "Não é possível se conectar ao servidor VPP: o nome do host '192.0.2.0' não corresponde à entidade 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. Como padrão, a verificação do nome do host está ativada nas 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**.

Acesso ao XenMobile Tools a partir do console

Você pode acessar as ferramentas do XenMobile Tools no console XenMobile:

- **XenMobile Analyzer:** Identificar e fazer a triagem de possíveis problemas com sua implantação.
- **Portal APNs:** Enviar uma solicitação à Citrix para assinar um certificado de APNs, o qual você enviará posteriormente para a Apple.
- **Auto Discovery Service:** Solicitar e configurar o Auto Discovery para o XenMobile em seu domínio.
- **Gerenciar notificações por push:** Gerenciar notificações por push para aplicativos móveis de produtividade para dispositivos iOS e Windows.
- **MDX Service:** Preparar aplicativos que você pode gerenciar usando o XenMobile

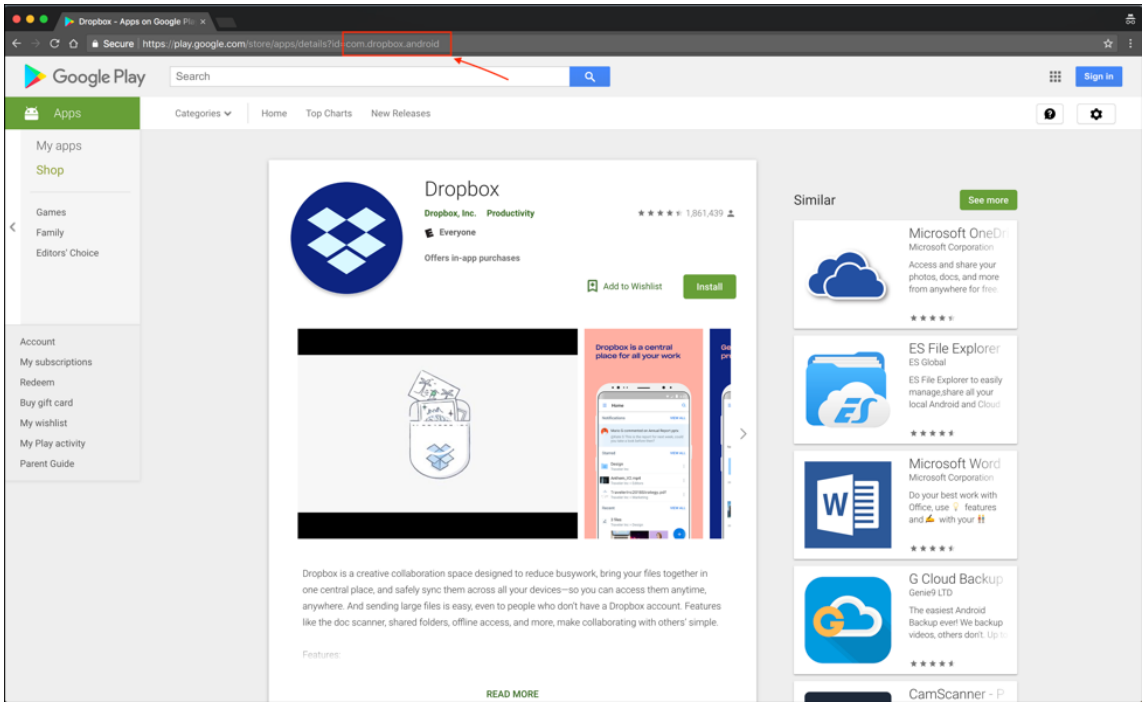
Para acessar essas ferramentas, vá para **Configurações > XenMobile Tools**.

Novo fluxo de trabalho para adicionar um aplicativo da Google Play Store

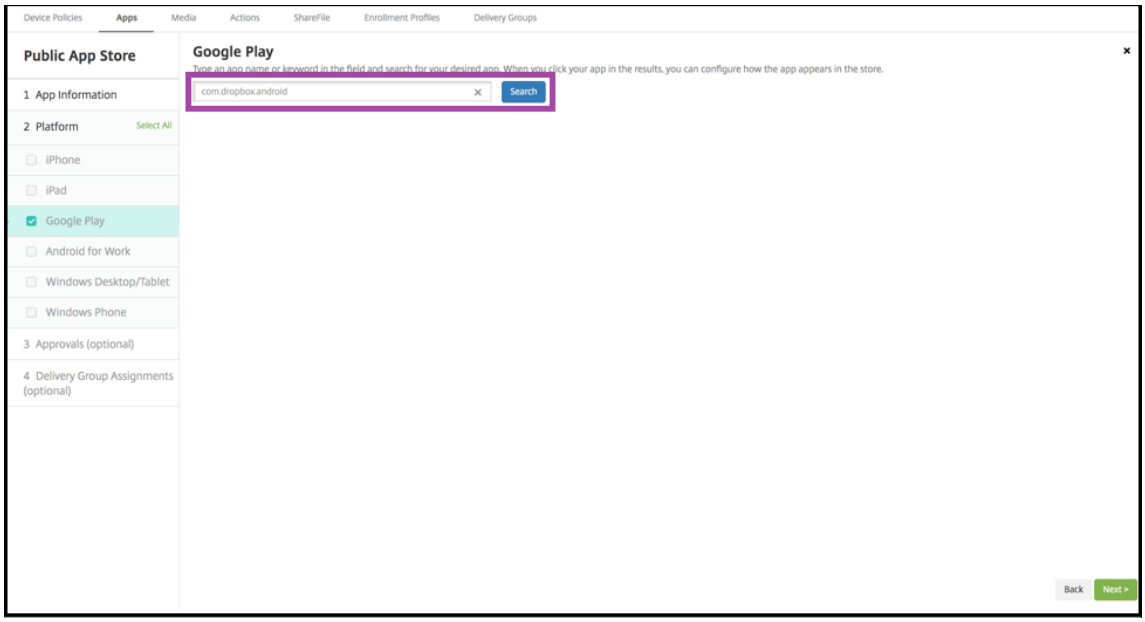
Em vez de especificar as credenciais do Google Play ao adicionar um aplicativo, você agora adiciona o ID do pacote do aplicativo Android na loja pública.

1. Na Google Play Store, copie o ID do pacote. O ID está na URL do aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

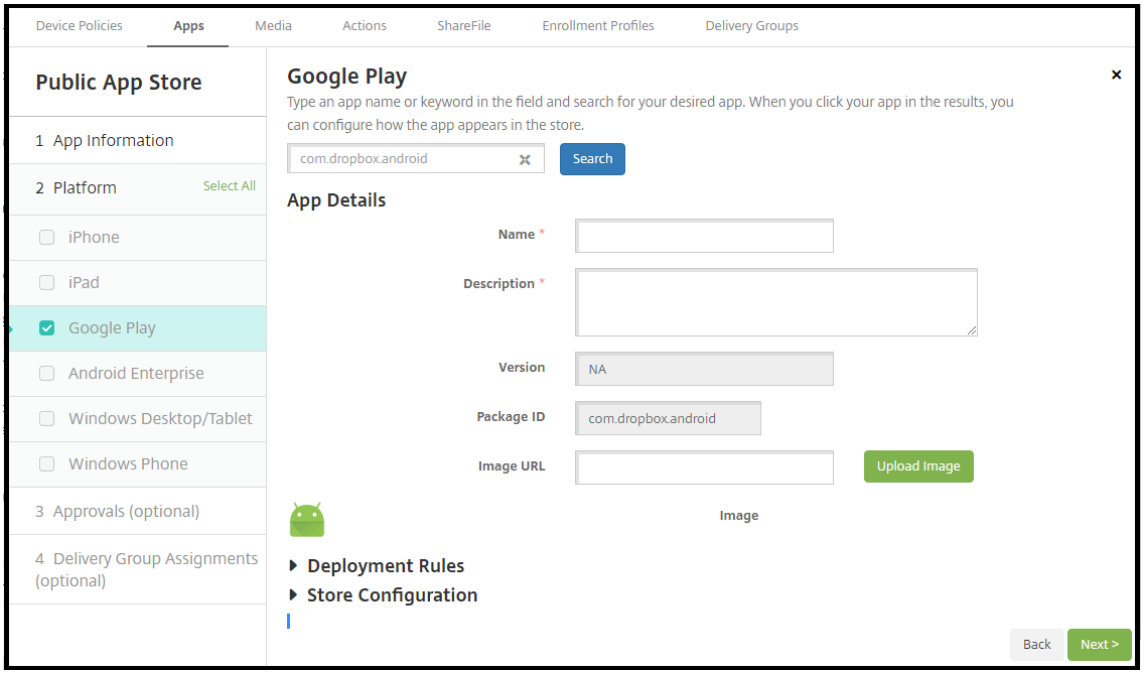


2. Ao adicionar um aplicativo da Loja Pública ao console Citrix Endpoint Management, cole o ID do pacote na barra de pesquisa.



3. Se o ID do pacote for válido, uma interface do usuário será exibida, permitindo que você insira detalhes do aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para obter mais informações, consulte Acrescentar um aplicativo de loja de aplicativos pública.

Novas APIs REST Públicas

- Uma nova versão da API Obter dispositivos por filtros fornece detalhes adicionais sobre dispositivos. Para obter informações, consulte a seção 3.16.2, Obter dispositivos por filtros (versão 2), no PDF XenMobile Public API for REST Services.
- Capacidade de regenerar a CA raiz, CA dos dispositivos, CA do servidor e renovar certificados de dispositivo

  O XenMobile Server usa as seguintes autoridades de certificação internamente para PKI: CA raiz, CA do dispositivo e CA do 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 “padrão”.

  Você pode renovar as CAs para dispositivos iOS, macOS e Android suportados usando o console do XenMobile Server ou a API REST pública. Para dispositivos Windows registrados, os usuários devem registrar novamente os seus dispositivos para receber uma nova CA de dispositivo.

  As seguintes APIs estão disponíveis para atualizar ou regenerar as CAs de PKI internas no XenMobile Server e renovar os certificados de dispositivo emitidos por essas autoridades de certificação.

  - Criar novas autoridades de certificação (CAs) de grupo.
  - Ativar novas CAs e desative CAs antigas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Renovar o certificado do dispositivo em uma lista de dispositivos configurada. Os dispositivos já registrados continuam a funcionar sem interrupções. Um certificado de dispositivo é emitido quando um dispositivo se reconecta 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 mais informações, consulte as seguintes seções no arquivo PDF XenMobile Public API for REST Services:

- Seção 3.16.58, Renew Device Certificate
- Seção 3.23, Refresh XenMobile CA Group

Como parte desse recurso, uma nova ação de segurança, **Renovação de certificado**, está disponível no console **Gerenciar dispositivos**. Esta ação renova o certificado de registro no dispositivo.

Pré-requisitos:

- Por padrão, esses novos recursos de renovação de certificado estão desativados. Para ativar os recursos de renovação de certificado, defina o valor para a propriedade do servidor **refresh.internal.ca** para **True**.

> Importante:
>
> Se o seu NetScaler estiver configurado para descarga de SSL, quando você gerar um novo certificado, assegure-se de atualizar seu balanceador de carga com o novo cacert.perm. Para obter mais informações sobre a configuração do Netscaler Gateway, consulte Para usar o modo de descarga de SSL para VIPs NetScaler.

Novidades no XenMobile Server 10.8

April 15, 2019

XenMobile Server 10.8 (download em PDF)

Para obter informações sobre como atualizar, consulte Atualização.

> Importante:
>
> **Antes de atualizar para o XenMobile 10.8**
>
> Atualize o seu Citrix License Server para 11.14.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.8.
>
> Para um ambiente em cluster: Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no XenMobile Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

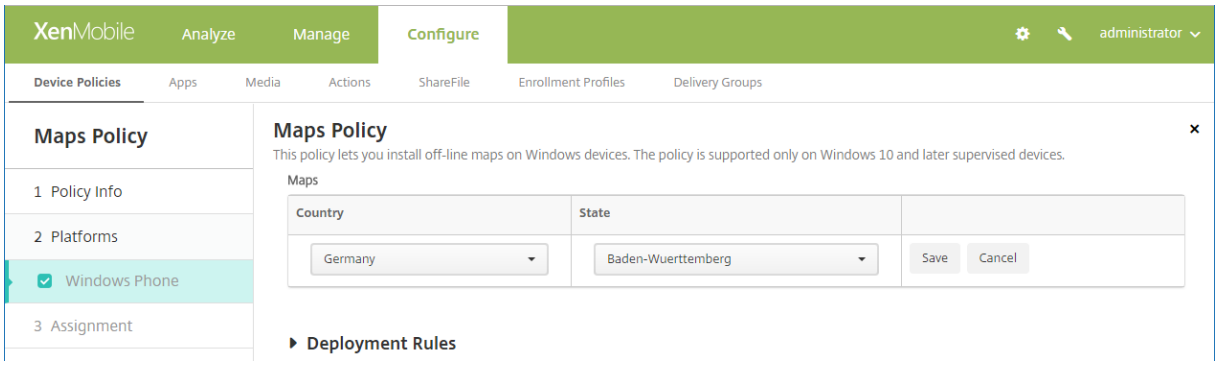
> **Após uma atualização para o XenMobile 10.8**
>
> Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não tiver alterado sua configuração de conexão, verifique os erros no log do XenMobile Server, como os seguintes: não é possível se conectar ao servidor VPP: o nome do host "192.0.2.0" não corresponde ao assunto do certificado fornecido pelo par.
>
> Se você receber o erro de validação de certificado, desative a verificação de nome de host no XenMobile Server. Como padrão, a verificação do nome do host está ativada nas 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**.

Para obter correções de bugs, consulte Problemas resolvidos.

> Importante:
>
> O TouchDown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido e fim de suporte da vida útil em 2 de julho de 2018. Para obter informações, consulte o artigo de suporte da Symantec, TouchDown End-of-Life, End-of-Availability, and End-of-Support announcement.

Instalar mapas offline nos dispositivos de telefone supervisionados Windows 10

Os dispositivos de telefone Windows 10 suportam mapas offline. Use a política de dispositivo Mapas para especificar quais mapas devem ser baixados para os dispositivos. O provedor de serviços de configuração (CSP) Microsoft Maps atualmente oferece suporte para mapas da Alemanha, do Reino Unido e dos Estados Unidos.



Novas restrições para dispositivos supervisionados que executam o iOS

As seguintes restrições agora estão disponíveis para os dispositivos iOS executados no modo supervisionado. A versão mínima compatível para cada restrição é informada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

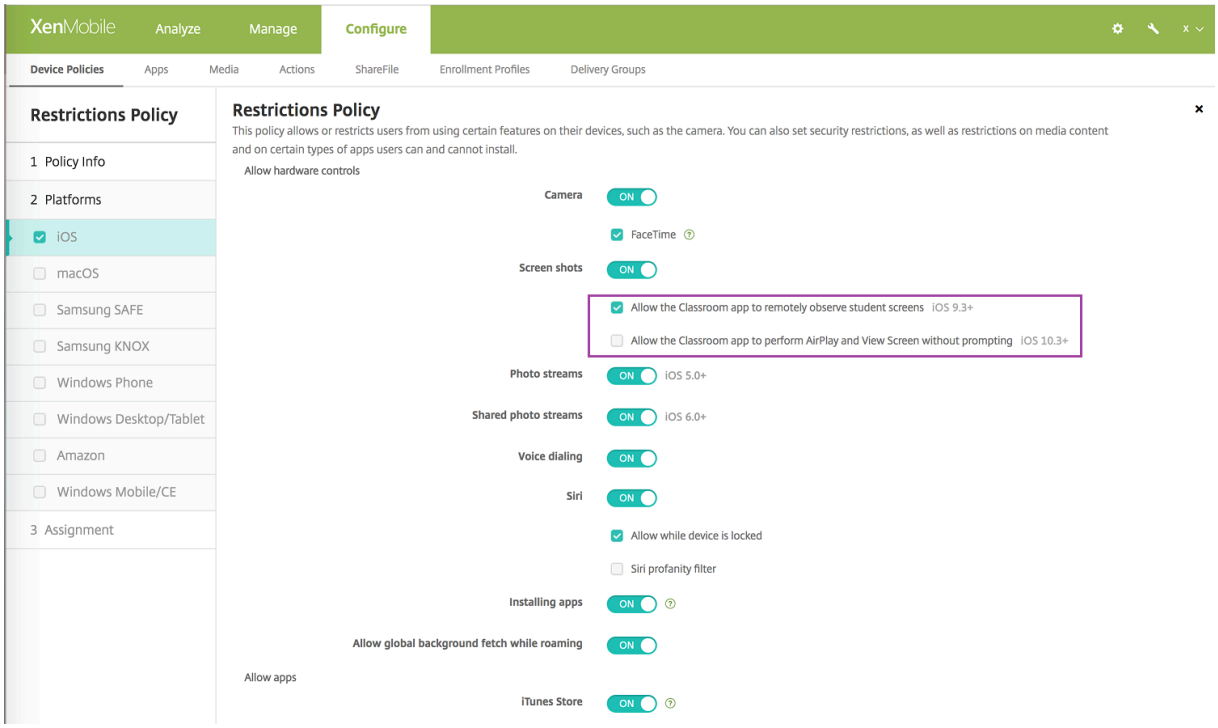
- **Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos:** se essa restrição não estiver selecionada, o professor não poderá usar o aplicativo Sala de Aula para observar as telas dos alunos remotamente. A configuração padrão está selecionada, um professor pode usar o aplicativo Sala de Aula para observar as telas dos alunos. A configuração de **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar** determina se os alunos receberão uma solicitação para conceder a permissão ao professor. Para dispositivos supervisionados executando o iOS 9.3 (versão mínima).
- **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 10.3 (versão mínima).
- **Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Aula bloqueará automaticamente os dispositivos do usuário a um aplicativo e bloqueará o dispositivo sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Associar automaticamente às classes do aplicativo Sala de Aula sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Sula associará automaticamente os usuários às classes, sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir AirPrint:** se essa restrição estiver definida como **Desativado**, os usuários não poderão imprimir com o AirPrint. A configuração padrão é **Ativado**. Quando essa restrição está **Ativada**, estas restrições extras são exibidas. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir o armazenamento de credenciais do AirPrint em Chaves:** se essa restrição não estiver selecionada, o nome de usuário e a senha do AirPrint não serão armazenados em Chaves. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir a descoberta de impressoras AirPrint usando iBeacons:** se essa restrição não estiver selecionada, a descoberta do iBeacon de impressoras AirPrint será desativada. Desabilitar a descoberta evita que sinalizadores falsos do AirPrint Bluetooth causem phishing no tráfego da rede. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir AirPrint apenas para destinos com certificados confiáveis:** se essa restrição for selecionada, os usuários poderão usar o AirPrint para imprimir apenas em destinos com certificados confiáveis. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Adicionar configurações de VPN:** se essa restrição estiver definida como **Desativado**, os usuários não poderão criar configurações de VPN. A configuração padrão é **Ativado**. Para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

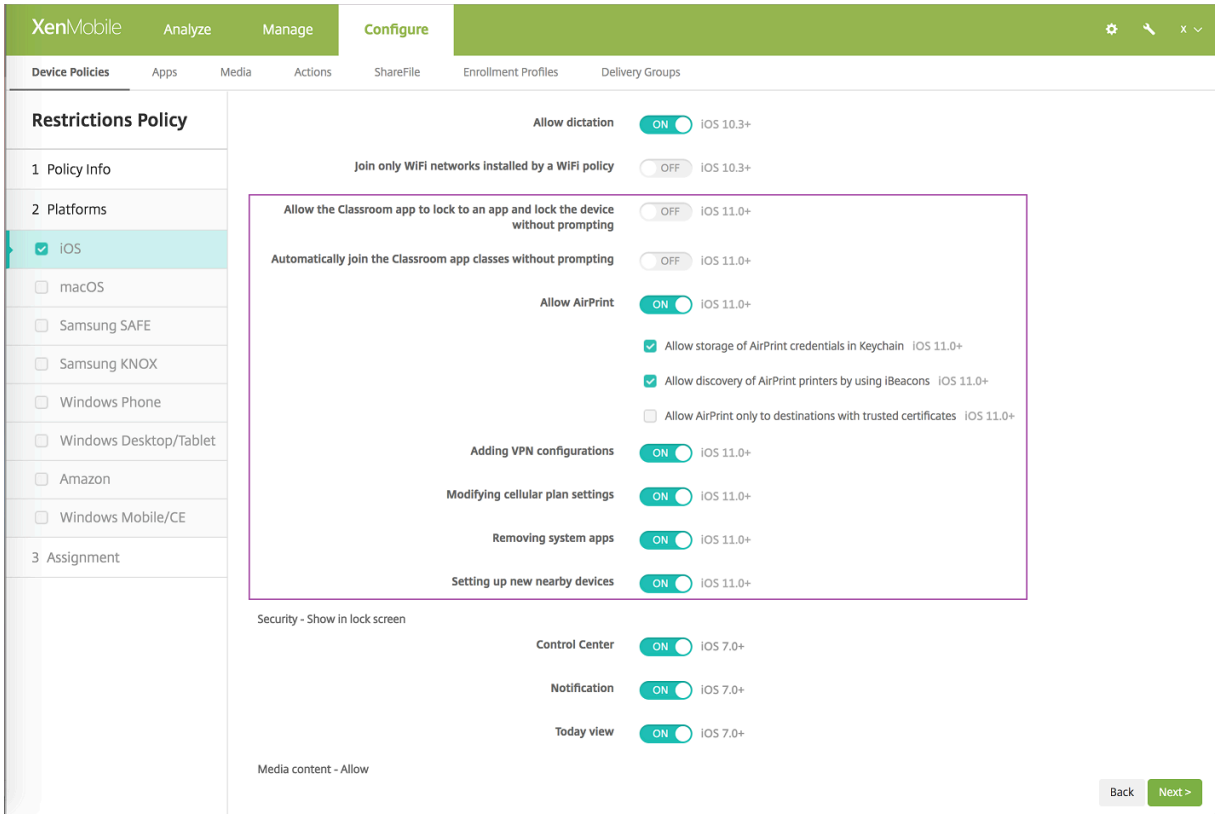
dispositivos supervisionados executando o iOS 11 (versão mínima).

- **Modificar as configurações do plano de celular:** se essa restrição estiver definida como **Desativado**, os usuários não poderão modificar as configurações do plano de celular. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Remover aplicativos do sistema:** se essa restrição estiver definida como **Desativado**, os usuários não poderão remover aplicativos de sistema de seus dispositivos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Configurando novos dispositivos próximos:** se essa restrição estiver definida como **Desativado**, os usuários não poderão configurar novos dispositivos próximos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

Para configurar as restrições, vá para **Configurar > Políticas de dispositivo**. Para obter mais informações sobre como configurar restrições, consulte Política de dispositivo de restrições.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

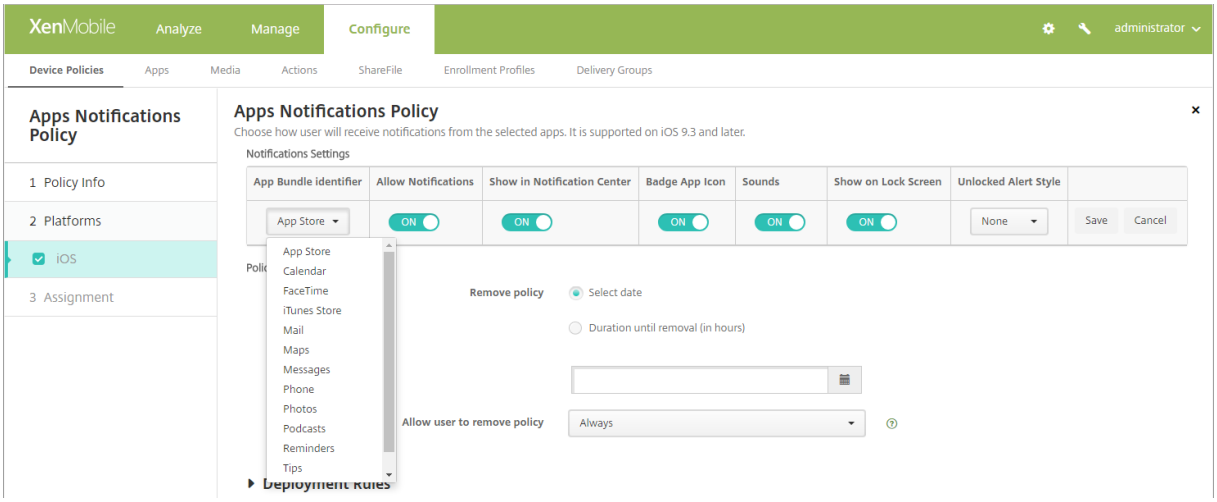


Além disso, agora você pode pular a tela de seleção do teclado no Assistente de Configuração. Para fazer isso, edite a política de dispositivo Restrições para iOS e, na configuração do **Painel Preferências do Sistema**, selecione **Teclado**.

Definir como as notificações do aplicativo são exibidas nos dispositivos iOS

A política de Notificações de Aplicativos permite controlar como os usuários do iOS recebem notificações de aplicativos especificados. Essa política é compatível em dispositivos com o iOS 9.3 ou versões posteriores. Para adicionar a política, acesse **Configurar > Políticas de dispositivo**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Configurações de notificação:

- **Identificador do pacote de aplicativos:** especifique os aplicativos aos quais você deseja aplicar essa política.
- **Permitir notificações:** selecione **I** para permitir notificações.
- **Mostrar no Centro de notificação:** selecione **I** para mostrar notificações no Centro de Notificação dos dispositivos dos usuários.
- **Ícone de Aviso nos Aplicativos:** selecione **I** para mostrar um ícone de aviso do aplicativo com as notificações.
- **Sons:** selecione **I** para incluir sons com as notificações.
- **Mostrar na tela de bloqueio:** selecione **I** para mostrar notificações na tela de bloqueio dos dispositivos do usuário.
- **Estilo de alerta desbloqueado:** na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.

Suporte para o novo cliente Cisco AnyConnect VPN para iOS

A Cisco está desativando o cliente Cisco AnyConnect que foi baseado em uma estrutura VPN agora obsoleta. A Cisco renomeou esse cliente como Cisco Legacy AnyConnect. O ID do pacote está inalterado, com.cisco.anyconnect.gui.

A Cisco tem um novo cliente chamado Cisco AnyConnect. O novo cliente fornece uma conexão mais confiável para recursos internos e suporte para aplicativos de UDP e TCP que têm a VPN por aplicativo. O ID do pacote para o novo cliente é com.cisco.anyconnect. A Cisco suporta o novo cliente para iOS 10 (versão mínima).

- **Para continuar a usar o cliente AnyConnect legado:** se você ainda pode usar o cliente legado, não é necessário alterar a sua política de dispositivo VPN existente para iOS. A política continua a funcionar até que a Cisco elimine o suporte ao cliente legado. A partir desta versão, a opção

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tipo de conexão Cisco AnyConnect foi renomeada para **Cisco Legacy AnyConnect** no console XenMobile Server.

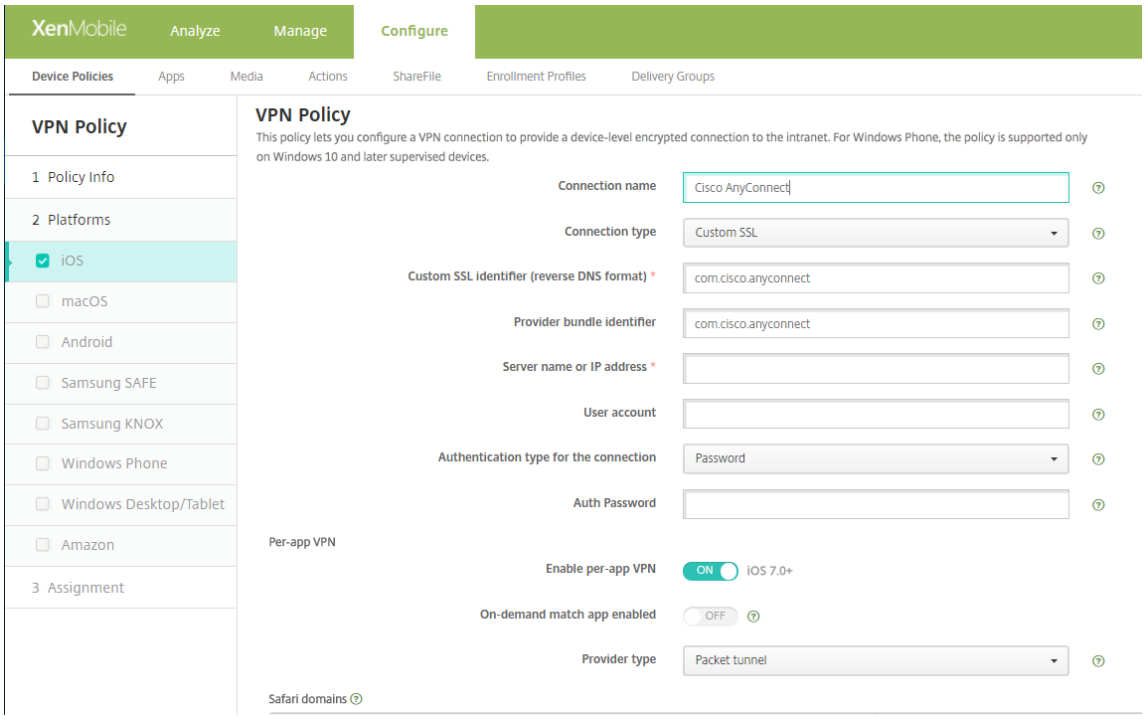
- **Para usar o novo cliente Cisco AnyConnect:** o novo cliente Cisco AnyConnect não detecta uma política de dispositivo XenMobile VPN criada com a opção **Tipo de conexão** como **Cisco AnyConnect**.

Para usar o novo cliente Cisco AnyConnect, configure o XenMobile Server da seguinte maneira.

1. Vá para **Configurar > Políticas de dispositivo** e adicione uma política de VPN para iOS.
2. Na página da plataforma **Política de VPN**, defina as configurações. As configurações listadas aqui são necessárias para o Cisco AnyConnect.

   - **Nome da conexão:** Cisco AnyConnect
   - **Tipo de conexão:** SSL personalizado
   - **Identificador SSL personalizado (formato DNS inverso):** com.cisco.anyconnect
   - **Identificador de pacote de provedor:** com.cisco.anyconnect
   - **Tipo de provedor:** Túnel de pacote

   Outras configurações, como **Tipo de autenticação para a conexão** e **Habilitar VPN por aplicativo**, dependem do seu caso de uso. Para obter informações, consulte “Configurar o protocolo SSL personalizado” em Configurações de iOS.



3. Configure regras de implantação e escolha grupos de entrega para a política de dispositivo VPN. Implemente essa política em dispositivos iOS.
4. Faça o upload do cliente Cisco AnyConnect de https://itunes.apple.com/us/app/cisco-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

anyconnect/id1135064690?mt=8, adicione o aplicativo ao XenMobile Server e implemente o aplicativo em dispositivos iOS.

5. Remova a política de dispositivo VPN antiga de dispositivos iOS.

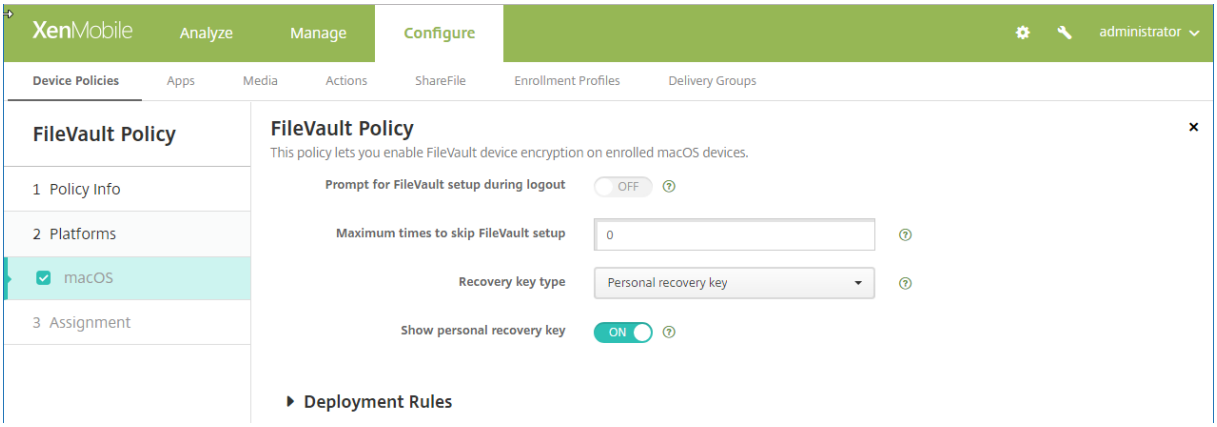
Para mais informações, consulte o artigo de suporte do XenMobile https://support.citrix.com/article/CTX227708.

Criptografia do dispositivo FileVault em dispositivos macOS registrados

O recurso de Criptografia de disco do FileVault do macOS protege o volume do sistema, criptografando seu conteúdo. Com o FileVault ativado em um dispositivo macOS, um usuário efetua login com a senha da conta sempre que o dispositivo é iniciado. Se o usuário perde a sua senha, uma chave de recuperação permite desbloquear o disco e redefinir sua senha.

A política do dispositivo XenMobile, FileVault, habilita as telas de configuração do usuário do FileVault e define as configurações, como as chaves de recuperação. Para obter mais informações sobre o FileVault, consulte o artigo de suporte da Apple, https://support.apple.com/en-us/HT204837.

Para adicionar a política, vá para **Configurar > Políticas de dispositivo**, adicione a política **FileVault** e defina estas configurações do macOS.



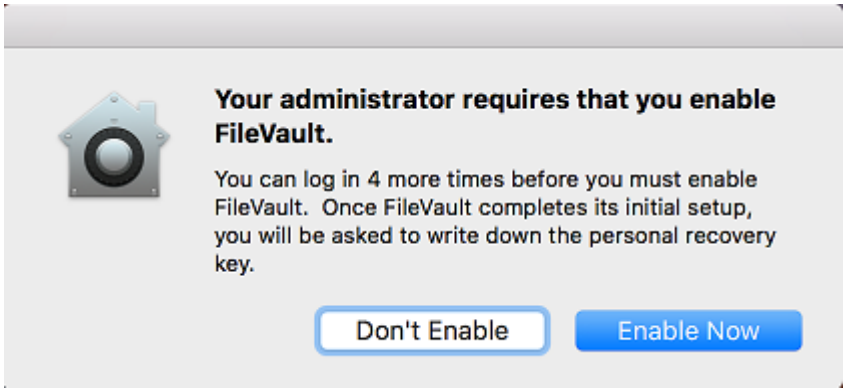
- **Solicitar a configuração do FileVault durante o logout:** se estiver **I**, solicita que o usuário ative o FileVault durante os próximos N logouts, conforme especificado pela opção **Número máximo de vezes para ignorar a configuração do FileVault**. Se o valor for **O**, o aviso de senha do FileVault não aparecerá.

  Depois de implantar a política FileVault com essa configuração ativada, a seguinte tela aparece quando um usuário faz o logoff do dispositivo. A tela dá ao usuário a opção de ativar o FileVault antes de logoff.

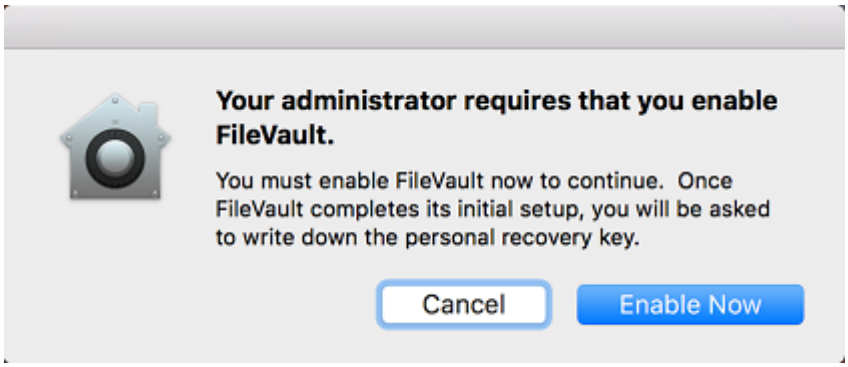
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** não for **0**: depois que você implantar a política do FileVault com essa configuração desativada e, quando o usuário fizer logon, a tela a seguir será exibida.



Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** for **0** ou o usuário tiver ignorado a configuração do número máximo de vezes, a tela a seguir será exibida.

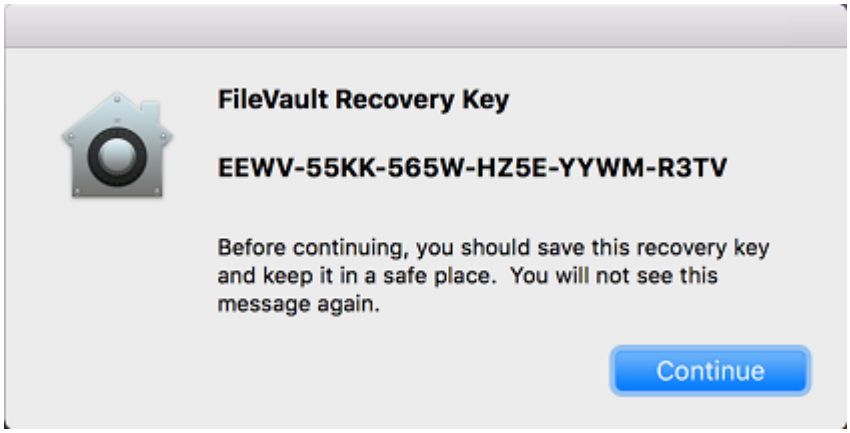


- **Número máximo de vezes para ignorar a configuração do FileVault:** o número máximo de vezes que o usuário pode ignorar a configuração do FileVault. Quando o usuário atinge o máximo, ele deve configurar o FileVault para efetuar login. Se o valor for **0**, o usuário deverá ativar o FileVault durante a primeira tentativa de login. O padrão é **0**.
- **Tipo de chave de recuperação:** um usuário que esquece sua senha pode digitar uma chave de recuperação para desbloquear o disco e redefinir sua senha. Opções de chave de recuperação:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Chave de recuperação pessoal:** uma chave de recuperação pessoal é exclusiva para um usuário. Durante a configuração do FileVault, um usuário escolhe se deseja criar uma chave de recuperação ou permitir que sua conta do iCloud desbloqueie os seus respectivos discos. Para mostrar a chave de recuperação ao usuário após a conclusão da configuração do FileVault, ative **Exibir a chave de recuperação pessoal**. Mostrar a chave permite que o usuário registre a chave para uso futuro. Para obter informações sobre o gerenciamento de chave de recuperação, consulte o artigo de suporte da Apple, https://support.apple.com/en-us/HT204837.
  - **Chave de recuperação institucional:** você pode criar uma chave de recuperação institucional (ou principal) e o certificado FileVault, que você usa para desbloquear dispositivos. Para obter informações, consulte o artigo de suporte da Apple, https://support.apple.com/en-us/HT202385. Use o XenMobile para implantar o certificado FileVault nos dispositivos. Para obter informações, consulte Certificados e autenticação.
  - **Chave de recuperação pessoal e institucional:** ao ativar os dois tipos de chave de recuperação, você deve desbloquear um dispositivo de usuário somente se o usuário perder sua chave de recuperação pessoal.

- **Exibir a chave de recuperação pessoal:** se estiver **I**, exibe a chave de recuperação pessoal para o usuário depois de ativar o FileVault no dispositivo. O padrão é **I**.



Suporte para Samsung Enterprise Firmware-Over-The-Air

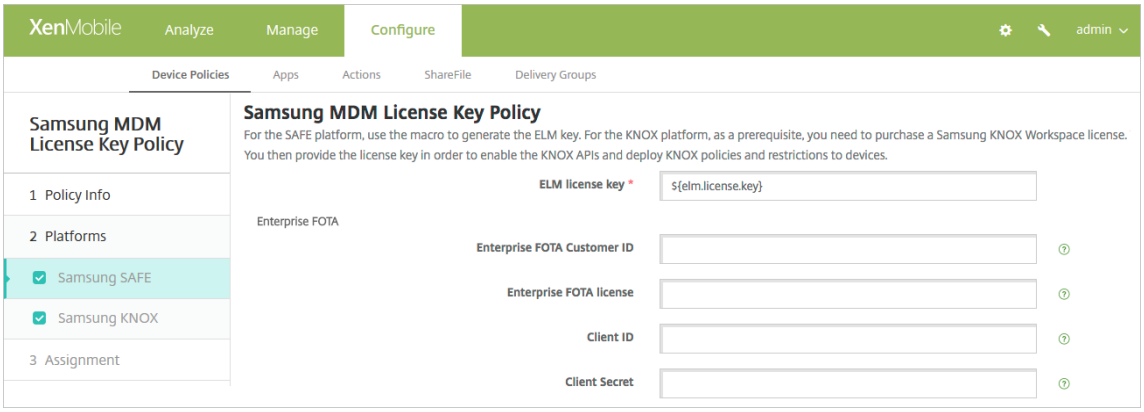
O Samsung Enterprise FOTA (E-FOTA) permite determinar quando os dispositivos são atualizados e a versão do firmware a ser usada. O E-FOTA permite que você teste as atualizações antes de implantá-las, para garantir que as atualizações sejam compatíveis com seus aplicativos. Você pode forçar os dispositivos a atualizarem com a versão de firmware mais recente disponível, sem exigir a interação do usuário.

Samsung suporta E-FOTA para dispositivos Samsung KNOX 2.7.1 (versão mínima) que executam firmware autorizado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar uma política E-FOTA:

1. Crie uma política de chave de licença de MDM Samsung com as chaves e as informações de licença que você recebeu da Samsung. O XenMobile Server valida e registra as informações.

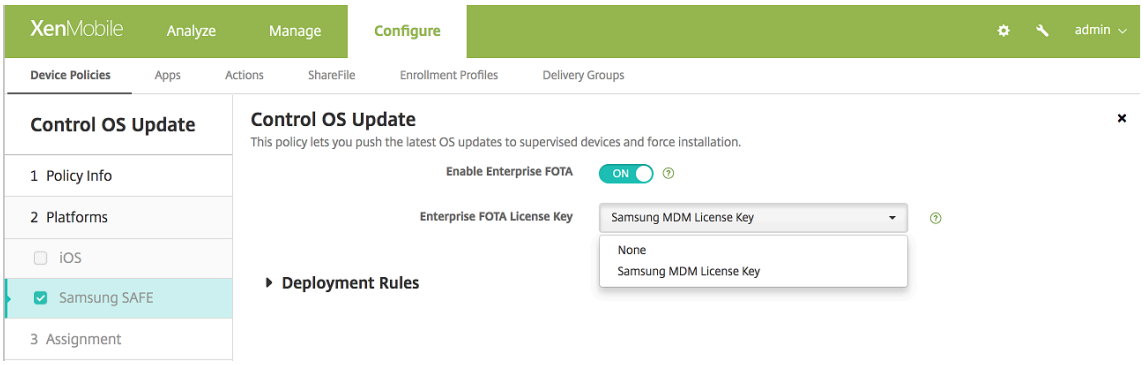


   - **Chave de licença ELM:** esse campo contém a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite a macro `${ elm.license.key }` .

   Digite as seguintes informações fornecidas pela Samsung quando você adquiriu um pacote E-FOTA:

   - **ID de cliente do Enterprise FOTA**
   - **Licença do Enterprise FOTA**
   - **ID de cliente**
   - **Código secreto do cliente**

2. Crie uma política de controle de atualização do sistema operacional.



   Defina estas configurações:

   - **Ativar Enterprise FOTA:** defina como **Ativado**.
   - **Chave de licença Enterprise FOTA:** selecione o nome da política de chave de licença Samsung MDM que você criou na etapa 1.

3. Implante a política de controle de atualização de sistema operacional no Secure Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Segurança aprimorada de perfis de trabalho do Android for Work

Código secreto de perfil de trabalho

Em dispositivos que executam o Android 7.0 e versões posteriores, você agora pode exigir um código secreto para aplicativos dentro de um perfil de trabalho do Android for Work. Os usuários são solicitados a inserir o código secreto quando tentam abrir os aplicativos no perfil de trabalho. Quando os usuários digitam o código secreto, eles podem acessar aplicativos no perfil de trabalho.

Você configura um requisito de código secreto somente para o perfil de trabalho ou para o dispositivo.

Para configurar um requisito de código secreto para o perfil de trabalho, vá para **Configurar > Políticas de dispositivo**, adicione a política de **Código secreto** e defina estas configurações:

- **Desafio de segurança do perfil de trabalho:** ative esta configuração para exigir que os usuários concluam um desafio de segurança para acessar aplicativos que são executados em um perfil de trabalho do Android for Work. Essa opção não está disponível para dispositivos Android anteriores ao Android 7.0. O padrão é **O**.
- **Requisitos de código secreto para desafio de segurança de perfil de trabalho:**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é 6.
  - **Reconhecimento biométrico:** selecione se o reconhecimento biométrico deve ser ativado. Se você habilitar essa opção, o campo **Caracteres obrigatórios** ficará oculto. O padrão é **O**. Esse recurso não é compatível no momento.
  - **Caracteres obrigatórios:** configura como os códigos secretos são compostos. Use **Sem restrições** somente para dispositivos que executam o Android 7.0. Android 7.1 e versões posterior não oferecem suporte à configuração **Sem restrições**. O padrão é **Letras e números**.

Políticas de segurança padrão

Por padrão, as configurações de **Depuração de USB** e **Fontes desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

Cancelar o registro de um Android for Work Enterprise

O XenMobile agora permite cancelar o registro de um enterprise do Android for Work usando o console do XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile Server abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile Server tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite

© 1999-2019 Citrix Systems, Inc. All rights reserved.

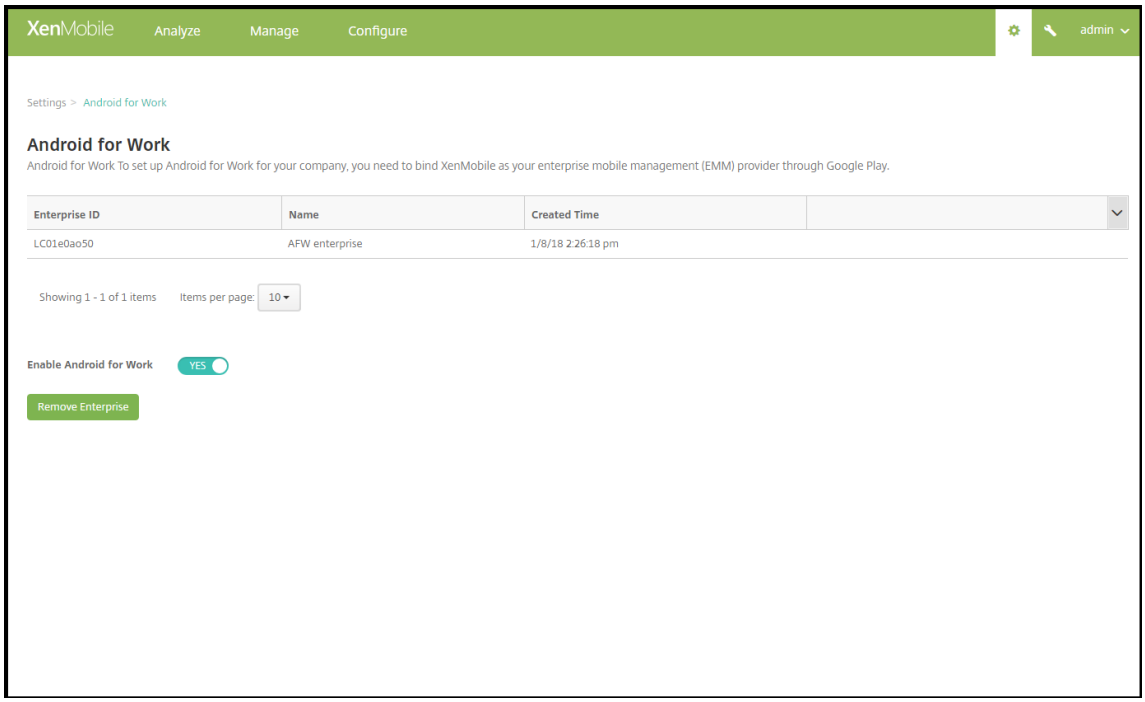
o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista branca de bloqueio de pop-up.

Depois que o registro do enterprise do Android for Work for cancelado:

- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android for Work re-definidos para o estado padrão. As políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work aplicadas anteriormente não afetam mais as operações.
- Embora o XenMobile gerencie dispositivos inscritos no Enterprise, o Google não os gerencia. Você não pode adicionar novos aplicativos do Android for Work. Você não pode aplicar novas políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work. Você ainda pode aplicar outras políticas, como Agendamento, Senha e Restrições a esses dispositivos. Os dispositivos precisam ser registrados novamente para permitir que novas políticas de aplicativos do Android for Work e políticas específicas do Android for Work sejam aplicadas.
- Se você tentar registrar dispositivos no Android for Work, eles serão registrados como dispositivos Android, não como dispositivos Android for Work.

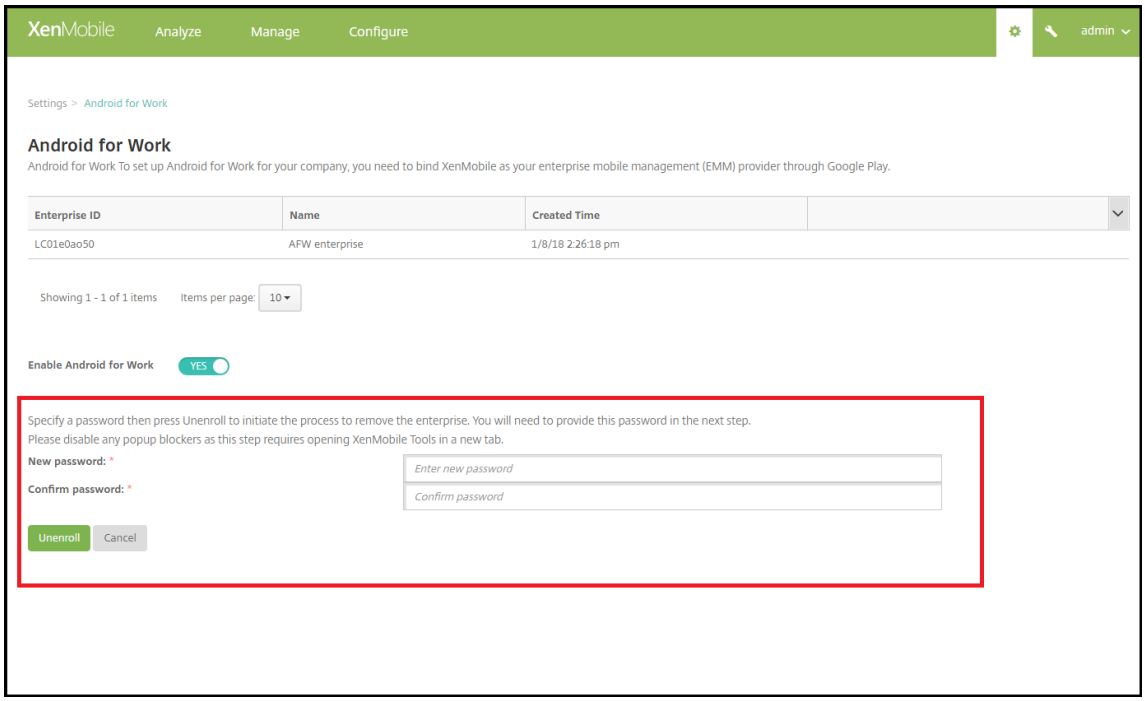
Para cancelar o registro de um Android for Work Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Na página Configurações, clique em **Android for Work**.
3. Clique em **Remover Enterprise**.

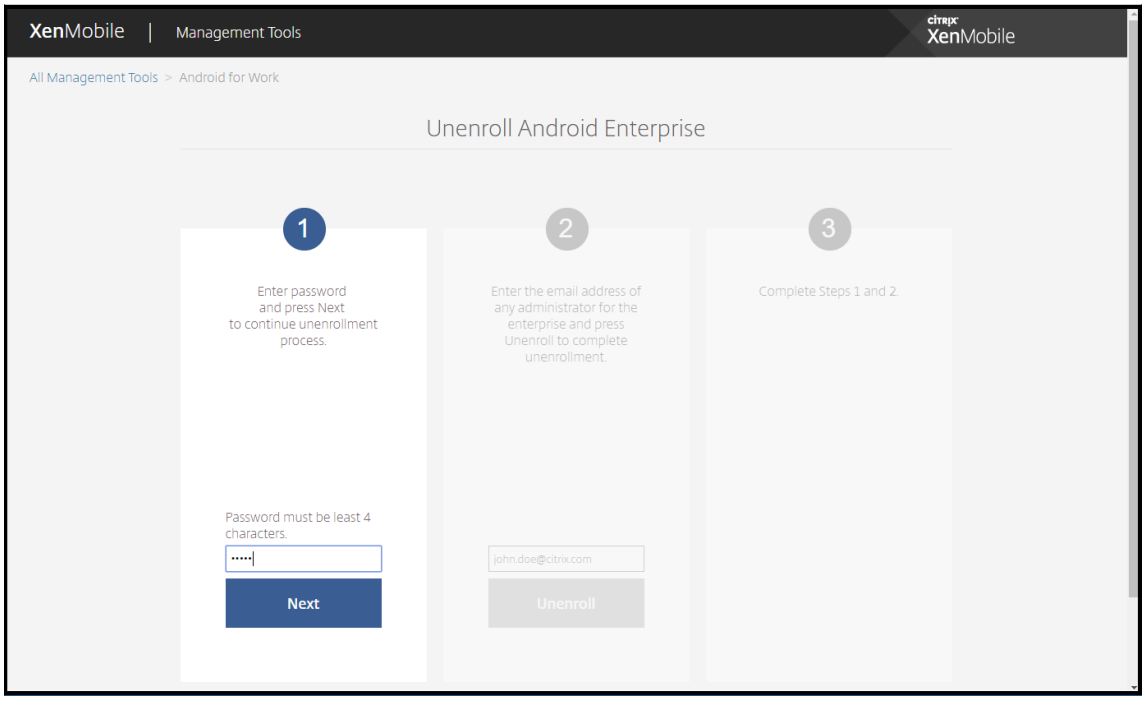


© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Especifique uma senha. Você precisará da senha na próxima etapa para concluir o cancelamento do registro. Em seguida, clique em **Cancelar registro**.

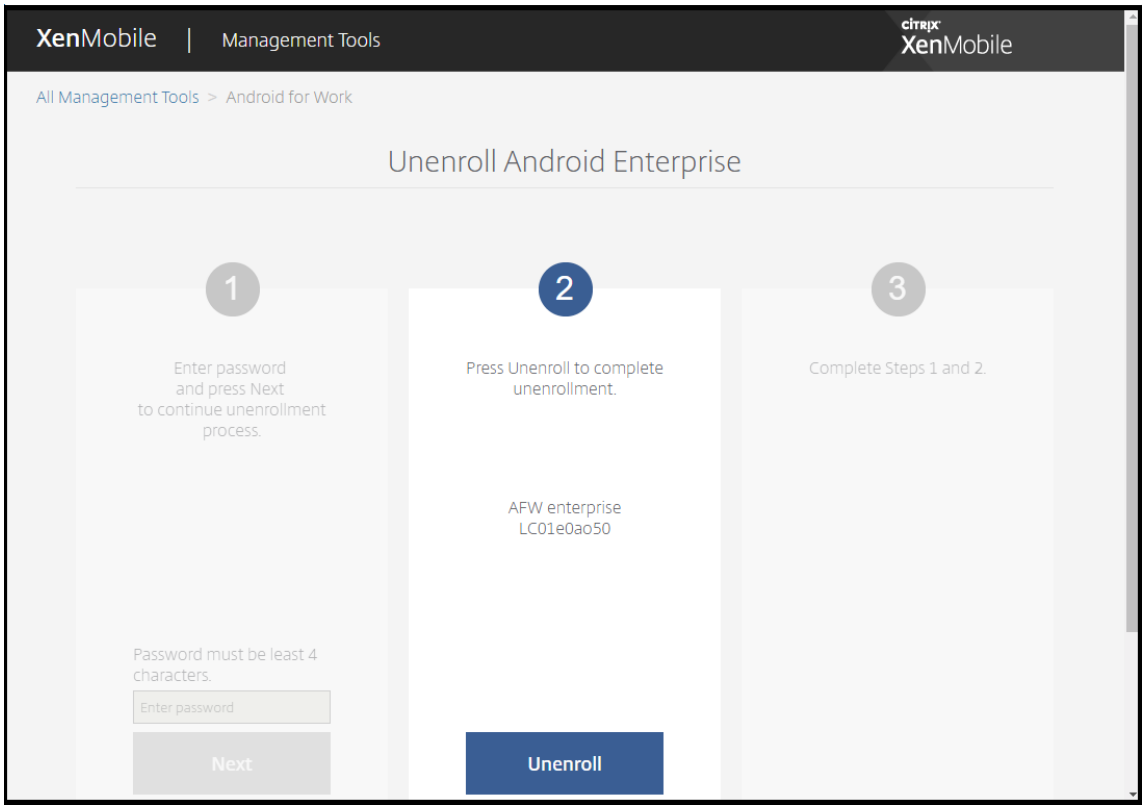


5. Quando a página do XenMobile Tools for aberta, insira a senha que você criou na etapa anterior.



6. Clique em **Cancelar registro**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Especificar o comportamento quando aplicativos do Android for Work solicitam permissões perigosas

Para solicitações a aplicativos do Android for Work que estão em perfis de trabalho: uma nova política de dispositivo permite configurar como essas solicitações lidam com o que o Google chama de permissões “perigosas”. Você controla se os usuários devem conceder ou negar uma solicitação de permissão de aplicativos. Esse recurso é para dispositivos que executam o Android 7.0 e versões posteriores.

O Google define permissões perigosas como permissões que dão a um aplicativo acesso ao seguinte:

- Dados ou recursos que envolvem informações particulares do usuário.
- Recursos que podem afetar os dados armazenados de um usuário ou a operação de outros aplicativos. Por exemplo, a capacidade de ler contatos do usuário é uma permissão perigosa.

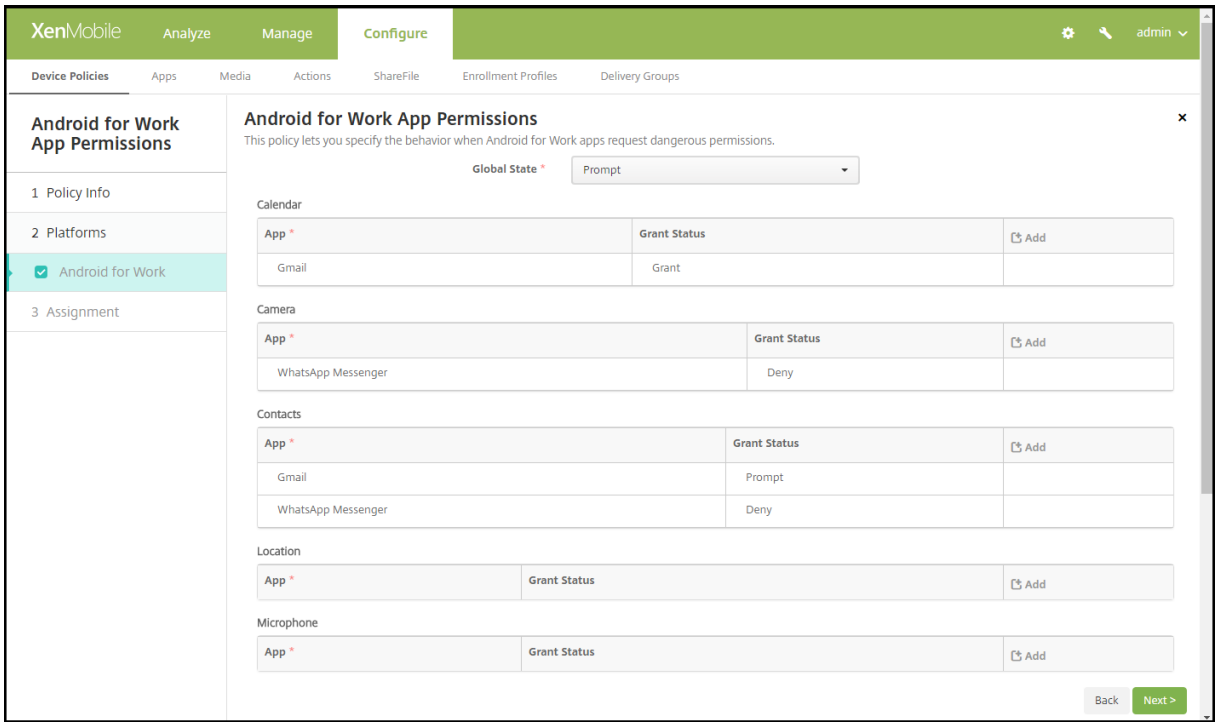
Para aplicativos do Android for Work que estão em perfis de trabalho: você pode configurar um estado global que controla o comportamento de todas as solicitações de permissões perigosas para os aplicativos. Você também pode controlar o comportamento de solicitações de permissões perigosas para grupos de permissão individual, conforme definido pelo Google, para cada aplicativo. Essas configurações individuais substituem o estado global.

Para obter informações sobre como o Google define grupos de permissões, consulte o Guia de desenvolvedores do Android.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por padrão, os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.

Para configurar permissões para aplicativos do Android for Work, vá para **Configurar > Políticas de dispositivos** e adicione a política de **Permissões de aplicativos do Android for Work**. Essa política se aplica somente aos aplicativos que você adiciona e aprova no console do Google Play primeiro e, depois, adiciona ao XenMobile como aplicativos de loja pública.



Defina estas configurações.

- **Estado global:** controla o comportamento de todas as solicitações de permissões perigosas. Na lista, clique em **Solicitar**, **Conceder** ou **Negar**. O padrão é **Solicitar**.
  - **Solicitar:** solicita aos usuários para conceder ou negar solicitações de permissões perigosas.
  - **Conceder:** concede todas as solicitações de permissões perigosas sem avisar aos usuários.
  - **Negar:** nega todas as solicitações de permissões perigosas sem avisar aos usuários.
- Para substituir o **Estado global** de um grupo de permissões, defina um comportamento individual para o grupo de permissões. Para definir as configurações de um grupo de permissões, clique em **Adicionar**, escolha um aplicativo na lista e escolha um **Status de concessão**.

SNMP Monitoring

Você pode ativar o SNMP Monitoring no XenMobile Server para permitir que os sistemas de monitoramento consultem e obtenham informações nos nós do XenMobile. As consultas usam parâmetros,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

como Carga do processador, Média da carga, Uso da memória e Conectividade. Para obter mais informações sobre o SNMP v3, como especificações de autenticação e criptografia, consulte a documentação oficial do SNMP para RFC 3414.

Para mais informações sobre o SNMP Monitoring, consulte SNMP monitoring.

Suporte para o driver Microsoft JDBC para SQL Server

O XenMobile Server agora suporta o driver JDBC (Microsoft Java Database Connectivity) para SQL Server. O driver jTDS permanece como o driver padrão quando você instala o XenMobile Server no local ou atualiza de um XenMobile Server que use o driver jTDS.

Para ambos os drivers, o XenMobile é compatível com a autenticação do SQL Server ou com a autenticação do Windows, com SSL 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 contata o Kerberos para obter os detalhes do Centro de Distribuição de Chave (KDC) Kerberos. Se os detalhes necessários não estiverem disponíveis, a CLI do XenMobile solicita o endereço IP do servidor do Active Directory.

Para mudar do driver jTDS para o driver Microsoft JDBC, use SSH para todos os nós do XenMobile Server. Em seguida, use a CLI do XenMobile para definir as configurações. As etapas variam de acordo com a sua configuração do driver jTDS atual. Para obter mais informações, consulte Drivers do SQL Server.

Alterações na propriedade do servidor para melhorar o ajuste do servidor

Para várias propriedades do servidor usadas para ajustar as operações do XenMobile, os valores padrão agora correspondem às recomendações fornecidas em Ajuste das operações do XenMobile. Você também pode saber mais sobre as propriedades do servidor em Propriedades do servidor.

Aqui estão as propriedades de servidor atualizado, com seus novos valores padrão entre parênteses:

- hibernate.c3p0.timeout (120 segundos)
- Intervalo de pulsação de serviços de envio por push: ios.apns.heartbeat.interval, windows.wns.heartbeat.interval, gcm.heartbeat.interval (20 horas)
- auth.ldap.connect.timeout (60000)
- auth.ldap.read.timeout (60000)
- Tamanho do pool de conexão APNS de MDM iOS
- Implantação em segundo plano (1440 minutos)
- Inventário de hardware em segundo plano (1440 minutos)
- Intervalo para verificação de usuário do Active Directory excluído (15 minutos)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Além disso, o valor padrão da seguinte propriedade do servidor foi alterado para a configuração recomendada em Propriedades do servidor:

- Bloquear registro de dispositivos Android com root e iOS com jailbreak (verdadeiro)

Agora você pode ajustar ainda mais o XenMobile Server por meio das seguintes propriedades de servidor personalizadas que antes não eram documentadas.

- Chave personalizada: **hibernate.c3p0.min_size**

  Essa propriedade do XenMobile Server, uma chave personalizada, determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. O padrão é **50**.

  Para alterar essa configuração, você deve adicionar uma propriedade de servidor ao XenMobile Server com a seguinte configuração:

  - Chave: **chave personalizada**
  - Chave: **hibernate.c3p0.min_size**
  - Valor: **50**
  - Nome de exibição: **hibernate.c3p0.min_size=*nnn***
  - Descrição: **conexões de banco de dados ao SQL**

- Chave personalizada: **hibernate.c3p0.idle_test_period**

  Essa propriedade do XenMobile Server, uma chave personalizada, determina o tempo ocioso em segundos antes de uma conexão ser validada automaticamente. O padrão é **30**.

  Para alterar essa configuração, você deve adicionar uma propriedade de servidor ao XenMobile Server com a seguinte configuração:

  - 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 de hibernação**

Pesquisa otimizada de propriedades de dispositivos

Anteriormente, uma pesquisa de dispositivos na página **Gerenciar > Dispositivos** incluía todas as propriedades do dispositivo por padrão, o que deixava a pesquisa lenta. Agora, o escopo de pesquisa padrão inclui apenas as seguintes propriedades do dispositivo:

- Número de série
- IMEI
- Endereço MAC WiFi
- Endereço MAC Bluetooth

© 1999-2019 Citrix Systems, Inc. All rights reserved.

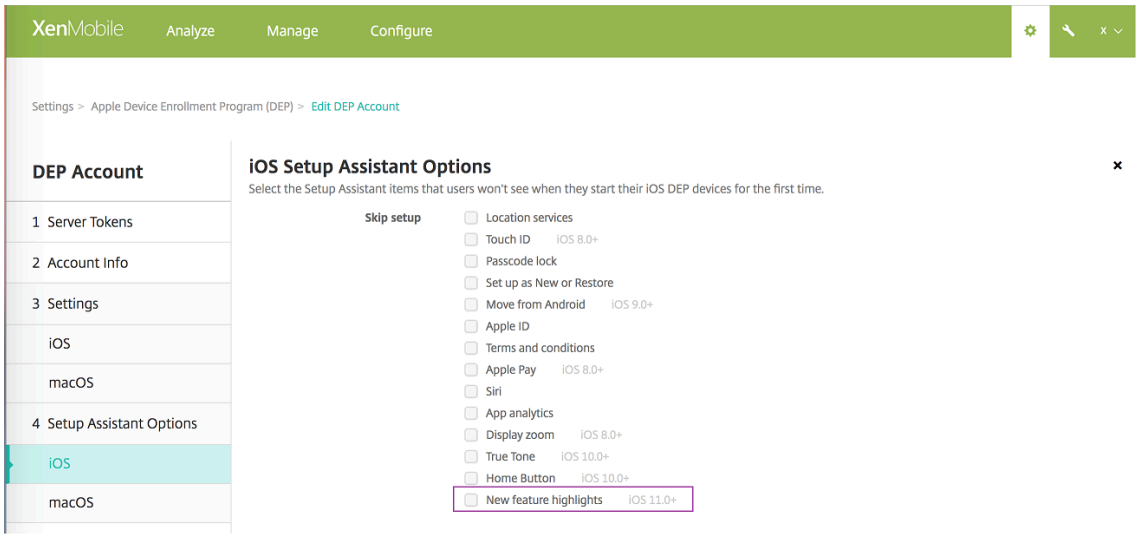
- Active Sync ID
- Nome de usuário

Você pode configurar o escopo da pesquisa usando uma nova propriedade do servidor, **include.device.properties.during.search**, cujo padrão é **false**. Para incluir todas as propriedades de dispositivo em uma pesquisa do dispositivo, altere a configuração para **true**.

Outras melhorias

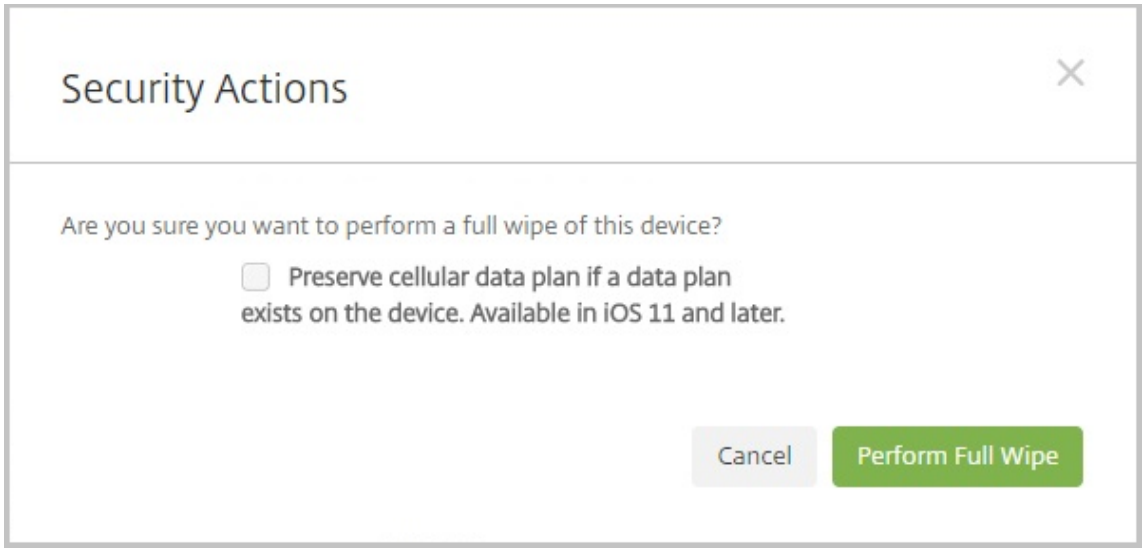
- **Nova Opção do Assistente de Instalação do iOS: Destaques do novo recurso.** O item Assistente de Instalação do iOS, **Destaques do novo recurso**, configura essas telas informativas de integração: Acessar o Dock em qualquer lugar e Alternar entre aplicativos recentes. Você pode optar por omitir essas telas de integração nas etapas do Assistente de Instalação do iOS, quando os usuários iniciarem seus dispositivos pela primeira vez.

  Destaques do novo recurso está disponível para iOS 11.0 (versão mínima). O padrão é desmarcar essa opção para todos os itens.

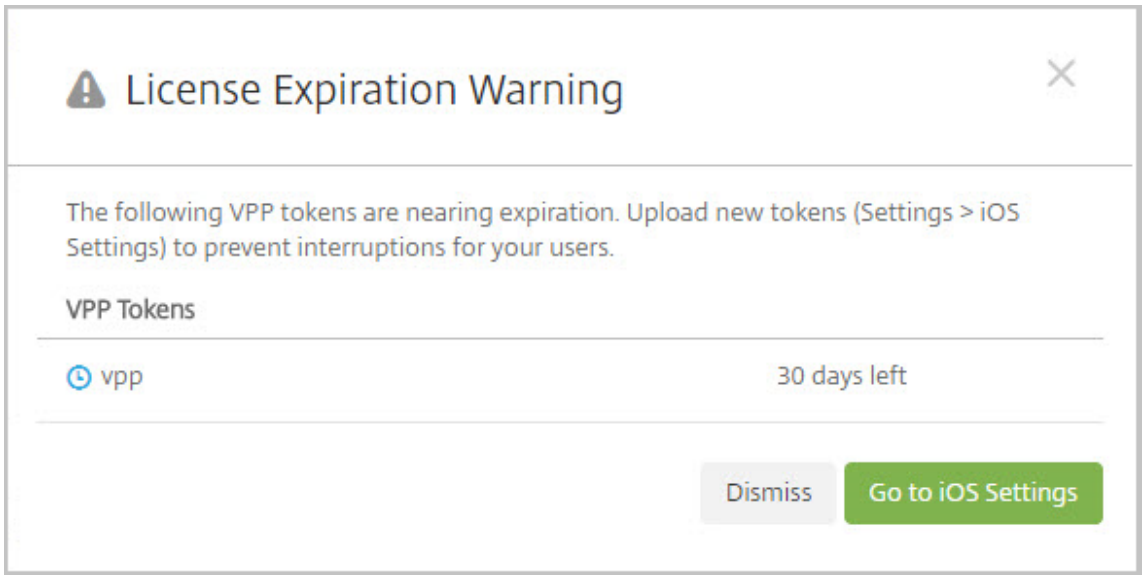


- Ao realizar um apagamento completo de um dispositivo iOS 11 que tenha um plano de dados celulares, você pode optar por preservar o plano de dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



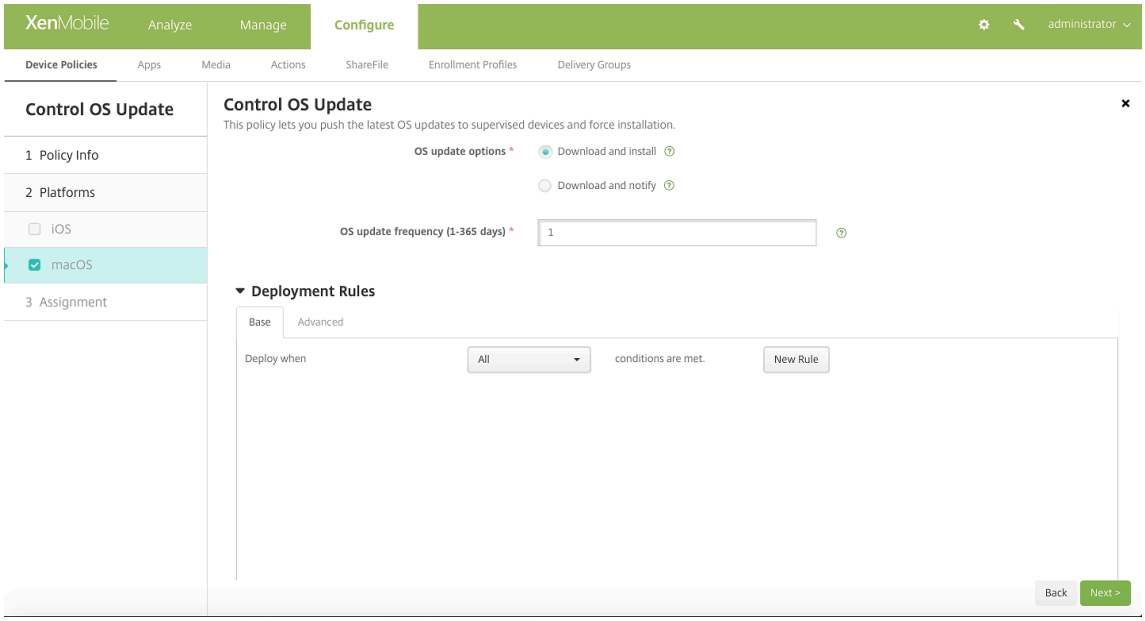
- O XenMobile agora exibe um Aviso de Expiração de Licença quando os tokens Apple VPP ou DEP estão prestes a expirar ou expiraram.



- A interface do console XenMobile para aplicativos macOS VPP mudou da seguinte forma:
  - **Em Configurar > Aplicativos, você pode filtrar aplicativos pelo macOS VPP.** Partes da interface que não se aplicam a um aplicativo macOS VPP agora são omitidas. Por exemplo, a seção de configuração da loja não aparece porque não existe um Secure Hub para macOS. A opção de importação de chaves VPP não é exibida.
  - **Em Gerenciar > Dispositivos, as Propriedades do Usuário incluem Desativar conta VPP.**
- **Política de dispositivo Controlar atualização do sistema operacional para macOS**. Agora você pode usar a política de controle de atualização do sistema operacional para implantar atualizações de sistema operacional em dispositivos macOS que são supervisionados ou são

© 1999-2019 Citrix Systems, Inc. All rights reserved.

implementados por meio do Apple DEP.



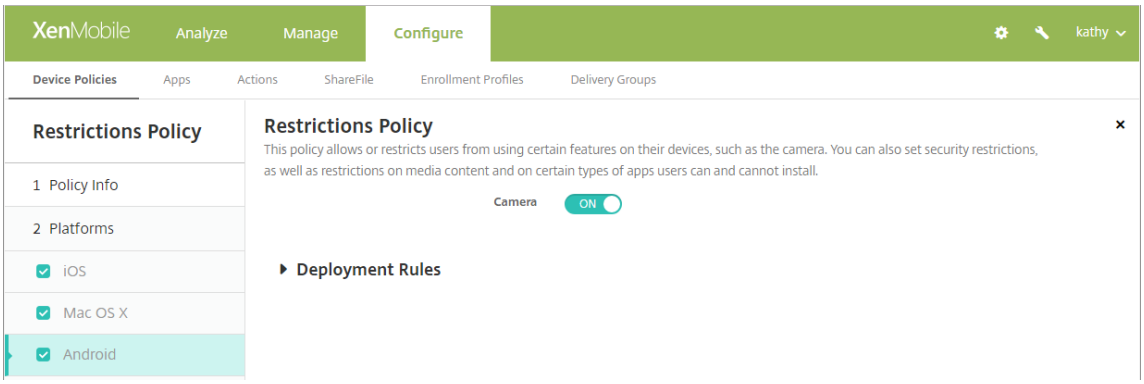
- **Opção para permitir que vários usuários usem um dispositivo Samsung SAFE**. A política de dispositivo Restrições agora inclui a opção de controle de hardware **Permitir vários usuários**. Essa opção, para MDM 4.0 e posterior, tem o padrão **o**.
- **Desativar aplicativos em dispositivos Samsung SAFE**. Agora você usa a política de dispositivo Restrições para impedir que uma lista de aplicativos instalados sejam executados em dispositivos Samsung SAFE. As opções **Navegador**, **YouTube** e **Google Play/Marketplace** estão obsoletas.

  Por padrão, a nova configuração **Desativar aplicativos** está **desativada**, o que significa que os aplicativos estão ativados. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado**, clique em **Adicionar** na tabela **Lista de Aplicativos** e digite o nome do pacote do aplicativo.

  Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: suponha que você desative `com.example1` e `com.example2`. Mais tarde, você altera a lista para `com.example1` e `com.example3`. Nesse caso, o XenMobile ativa `com.example.2`.
- Agora, a página **Gerenciar> Dispositivos** inclui essas propriedades de dispositivo adicionais relatadas por dispositivos Android:
  - Código da operadora (relatado somente por dispositivos que executam o Samsung MDM 5.7 ou superior)
  - Número do modelo (relatado somente por dispositivos que executam o Samsung MDM versão 2.0 ou superior)
- **Política de dispositivo Restrições agora inclui uma política para desativar a câmera nos dispositivos Android**. Para configurar a política, vá para **Configurar > Políticas de dispositivo**,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

clique em **Adicionar** e clique em **Restrições**. Por padrão, o uso da câmera está ativado. Para desativar o uso da câmera, altere a configuração da **Câmera** para **desativado**.



- **Formatos de data e hora baseados na localidade**. A data e a hora exibidas nas páginas **Gerenciar > Dispositivos** e **Gerenciar > Usuários** agora são formatadas de acordo com a localidade. Por exemplo, as 18h do dia 15 de outubro de 2017 aparece assim:

```
U.S. (en-US): 10/15/17 06:00:00 pm
U.K. (en-GB): 15/10/17 18:00:00
South Africa (en-ZA): 2017/10/15 06:00:00 pm
```

- A política de dispositivo Samsung SAFE Firewall é renomeada para a política de dispositivo Firewall.
- O número padrão de arquivos de backup incluídos nos pacotes de suporte foi reduzido para 100 nos arquivos a seguir. O tamanho padrão desses arquivos é 10 MB.
  - DebugLogFile
  - AdminAuditLogFile
  - UserAuditLogFile
  - HibernateStats.log

  Quando o pacote de suporte inclui 100 arquivos de log para cada uma dessas categorias, o arquivo de log é transferido. Se você configurar um número máximo mais baixo de arquivos de log (**Solução de problemas e suporte -> Configurações de log**), os arquivos de log externos serão imediatamente excluídos daquele nó de servidor.
- A página **Configurações > Syslog** agora inclui uma opção para enviar logs de depuração do XenMobile Server para um servidor syslog.
- **Atualizações à API pública do XenMobile para serviços REST**.
- A API pública do XenMobile para serviços REST inclui essas novas APIs: Para obter mais informações, baixe o arquivo PDF XenMobile Public API for REST Services e consulte as seções indicadas a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Get Users by Filter (seção 3.12.1)

  Essa nova API substitui a API obsoleta para obter todos os usuários, Get All Users.
- Revoke Enrollment Token (seção 3.19.6)
- Remove Enrollment Token (seção 3.19.7)

Novidades no XenMobile Server 10.7

April 15, 2019

XenMobile Server 10.7 (download em PDF)

> Nota:
>
> O TouchDown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido e fim de suporte da vida útil em 2 de julho de 2018. Para obter informações, consulte o artigo de suporte da Symantec, TouchDown End-of-Life, End-of-Availability, and End-of- Support announcement.

Para obter informações sobre como atualizar, consulte Atualização. Para acessar o console de gerenciamento do XenMobile, use somente o nome de domínio totalmente qualificado do XenMobile Server ou os endereços IP do nó.

> Importante:
>
> **Após uma atualização para o XenMobile 10.7**
>
> Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não tiver alterado sua configuração de conexão, verifique os erros no log do XenMobile Server, como os seguintes: não é possível se conectar ao servidor VPP: o nome do host “192.0.2.0” não corresponde ao assunto do certificado fornecido pelo par.
>
> Se você receber o erro de validação de certificado, desative a verificação de nome de host no XenMobile Server. Como padrão, a verificação do nome do host está ativada nas 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**.

Para obter correções de bugs, consulte Problemas resolvidos.

Integração com os recursos do Apple Educação

Você pode usar o XenMobile Server como sua solução de gerenciamento de dispositivos móveis (MDM) em um ambiente que usa o Apple Educação. O XenMobile suporta os aprimoramentos do Apple Edu-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cação introduzidos no iOS 9.3, incluindo o Apple School Manager e o aplicativo Classroom para iPad. A nova política de dispositivo de Configuração do XenMobile Education configura os dispositivos de instrutor e estudante para uso com o Apple Educação.

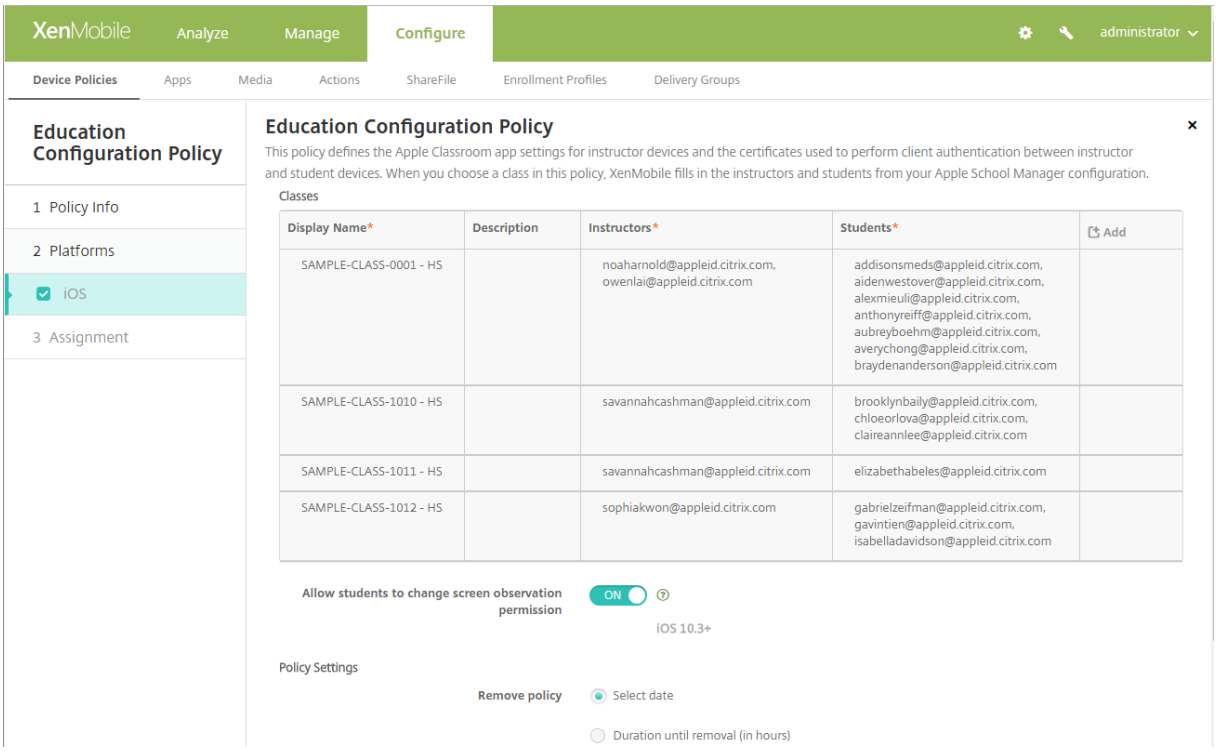
O seguinte vídeo fornece um tour rápido das alterações feitas ao Apple School Manager e ao XenMobile Server.

Configuração do Citrix XenMobile Education: integre os recursos do Apple Educação com o XenMobile

Você fornece iPads pré-configurados e supervisionados para instrutores e alunos. Essa configuração inclui:

- Registro do Apple School Manager DEP no XenMobile
- Uma conta do ID do Apple gerenciada e configurada com uma nova senha
- Aplicativos VPP e iBooks obrigatórios

Para obter detalhes sobre a integração com os recursos do Apple Education, consulte Integração com os recursos do Apple Educação e Política de dispositivo Configuração de Educação.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Implantar iBooks nos dispositivos iOS

Você pode usar o XenMobile para implantar iBooks que obtém por meio do Programa Apple Volume Purchase (VPP). Depois de configurar uma conta VPP no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura iBooks para implantação em dispositivos iOS escolhendo grupos de entrega e especificando regras de implantação.

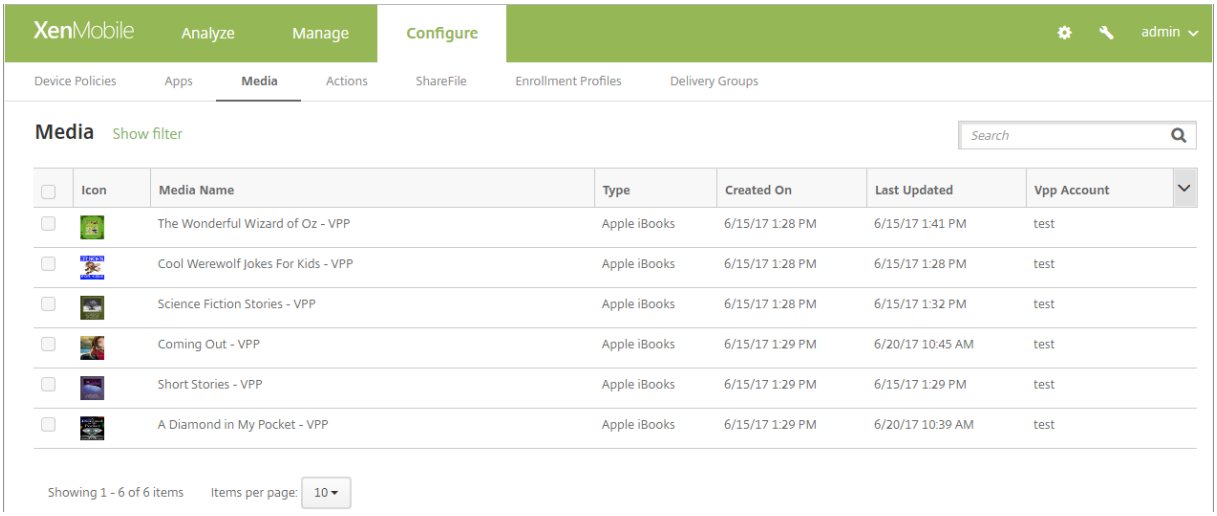
A primeira vez que um usuário recebe um iBook e aceita a licença VPP, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple iBook. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala iBooks como mídia necessária. Se um usuário exclui um livro instalado do seu dispositivo, o livro permanece no aplicativo iBook, pronto para download.

Pré-requisitos

- Dispositivos iOS (versão mínima iOS 8)
- Configure iOS VPP no XenMobile, como descrito em Volume Purchase Plan do iOS.

Configurar iBooks

Os iBooks obtidos através do VPP aparecem na página **Configurar > Mídia**. Para obter mais informações, consulte Adicionar mídia.



Política de dispositivo BitLocker

O Windows 10 Enterprise inclui um recurso de criptografia de disco chamado BitLocker, que fornece proteções de arquivos e sistemas adicionais contra o acesso não autorizado de um dispositivo perdido ou roubado. Para obter mais proteção, você pode usar o BitLocker com chips TPM (Trusted Platform

© 1999-2019 Citrix Systems, Inc. All rights reserved.

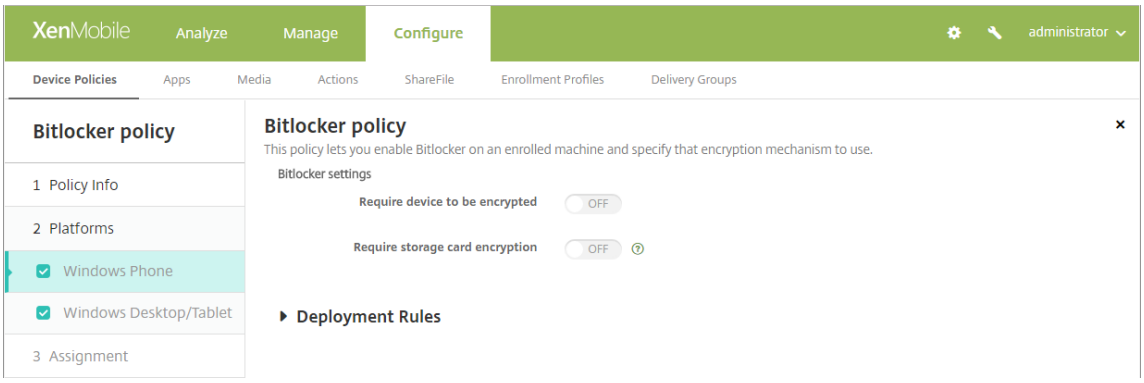
Module), versão 1.2 ou posterior. Um chip TPM manipula operações criptográficas e gera, armazena e limita o uso de chaves criptográficas.

Começando com o Windows 10, compilação 1703, as políticas do MDM podem controlar o BitLocker. Você pode usar a política de dispositivo de BitLocker no XenMobile para definir as configurações disponíveis no Assistente de BitLocker nos dispositivos Windows 10. Por exemplo, em um dispositivo com o BitLocker habilitado, o BitLocker pode solicitar aos usuários:

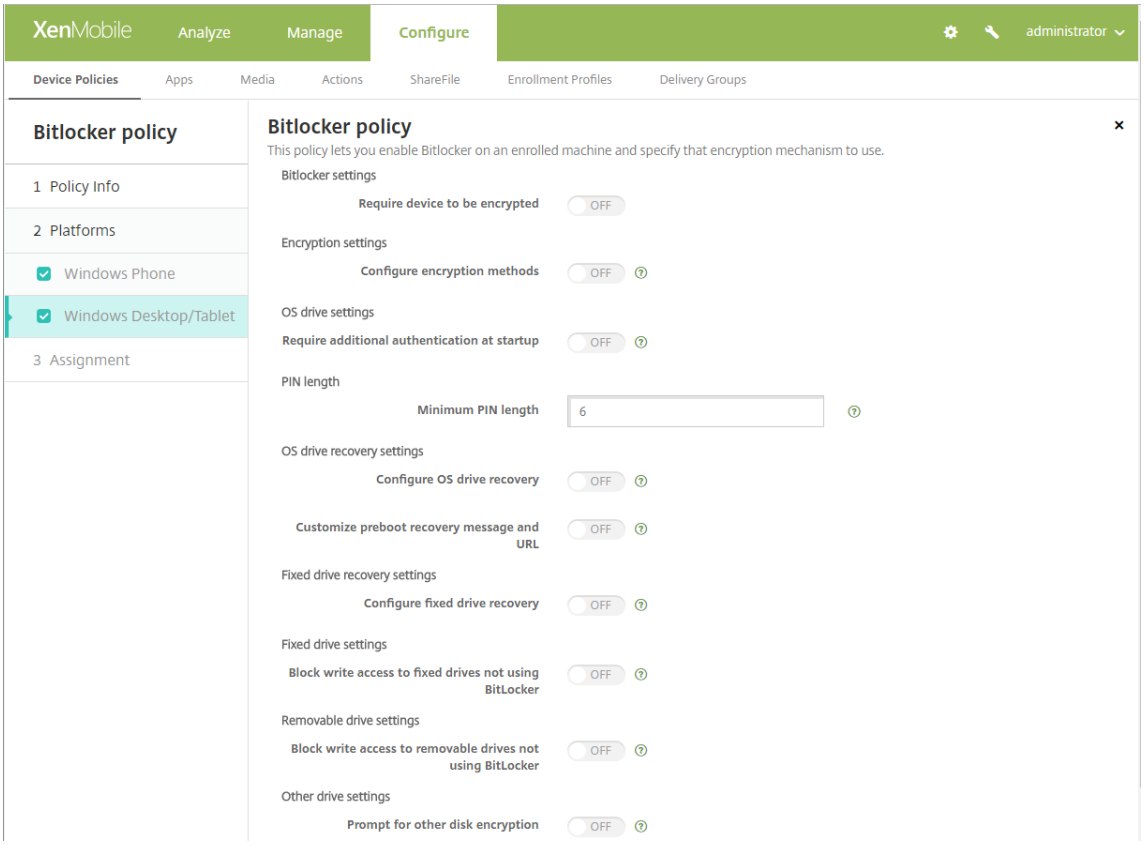
- Como eles querem desbloquear sua unidade na inicialização
- Como fazer backup da sua chave de recuperação
- Como desbloquear uma unidade fixa.

A configuração da política do dispositivo BitLocker também configura se:

- Ativar o BitLocker em dispositivos sem chip TPM
- Mostrar opções de recuperação na interface BitLocker.
- Negar acesso de gravação a uma unidade fixa ou removível quando o BitLocker não está habilitado.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para obter mais informações sobre a política de dispositivo do BitLocker, consulte Política de dispositivo BitLocker.

Novas restrições para dispositivos supervisionados que executam o iOS 10.3 e versões posteriores

As restrições permitem impedir que os usuários executem certas ações em seus dispositivos e sejam implementadas através de políticas de dispositivos.

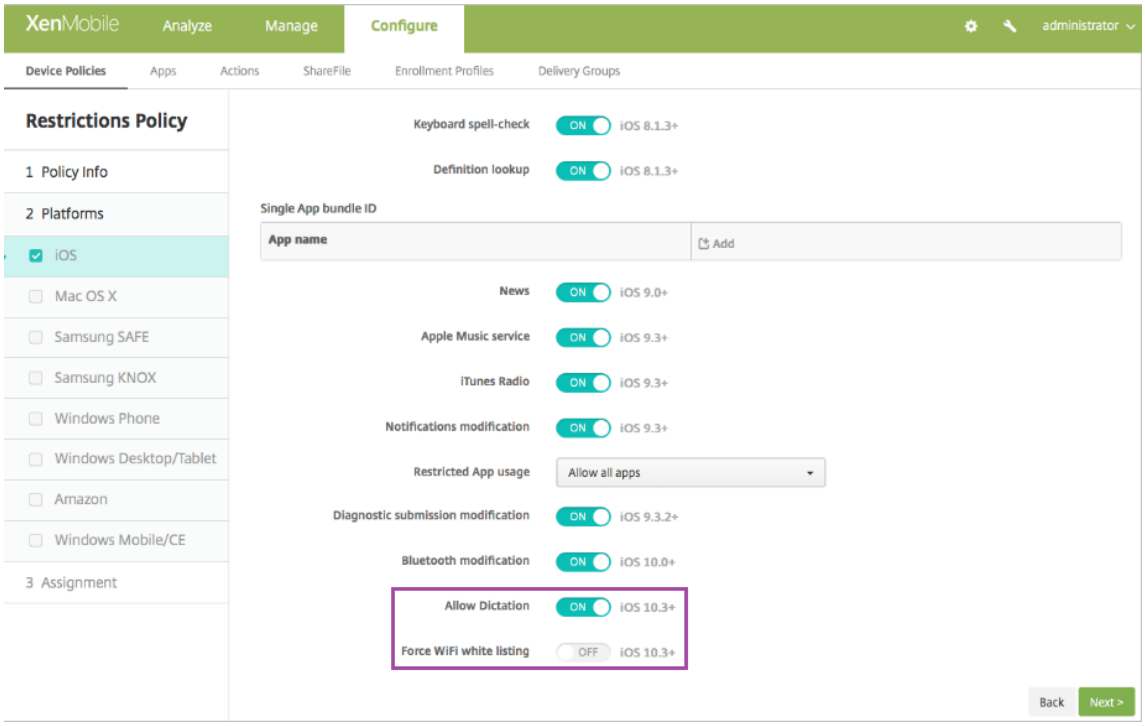
As seguintes restrições agora estão disponíveis para os dispositivos que executam o iOS 10.3 e versões posteriores, no modo supervisionado:

- **Permitir ditado:** supervisionado somente. Se essa restrição é definida como **Desativado**, a entrada de ditado não é permitida. A configuração padrão é **Ativado**. Para iOS 10.3 e posterior.
- **Forçar conexão de WiFi ao inserir na lista branca:** opcional. Apenas supervisionado. Se esta restrição estiver definida como **Ativado**, o dispositivo pode se juntar a redes Wi-Fi somente quando elas tiverem sido configuradas através de um perfil de configuração. O padrão é **Desativado**. Para iOS 10.3 e posterior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para definir essas restrições

1. No console XenMobile, selecione **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.
2. Selecione **Adicionar**. A página **Adicionar uma Nova Política** é exibida.
3. Clique em **Restrições**. A página de restrições **Informações sobre a política** é exibida.
4. No painel **Informações sobre a política**, digite as seguintes informações:
   - **Nome da política:** digite um nome descritivo para a política.
   - **Descrição:** digite uma descrição opcional para a política.
5. Clique em **Avançar**. A página **Plataforma de política** é exibida.
6. Selecione **iOS**.
7. Clique em **Avançar** até aparecer a página que mostra a seção ID de pacote único de aplicativos. Defina as restrições.



Para obter mais informações sobre como configurar restrições, consulte Política de dispositivo de restrições.

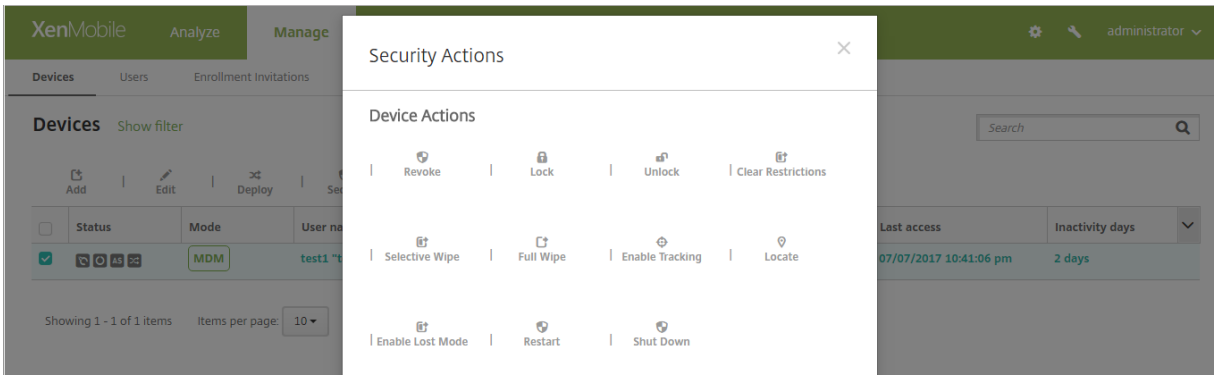
Reiniciar ou desligar um dispositivo iOS supervisionado

Você pode usar ações de segurança para reiniciar ou desligar um dispositivo iOS supervisionado (versão mínima 10.3). Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e

© 1999-2019 Citrix Systems, Inc. All rights reserved.

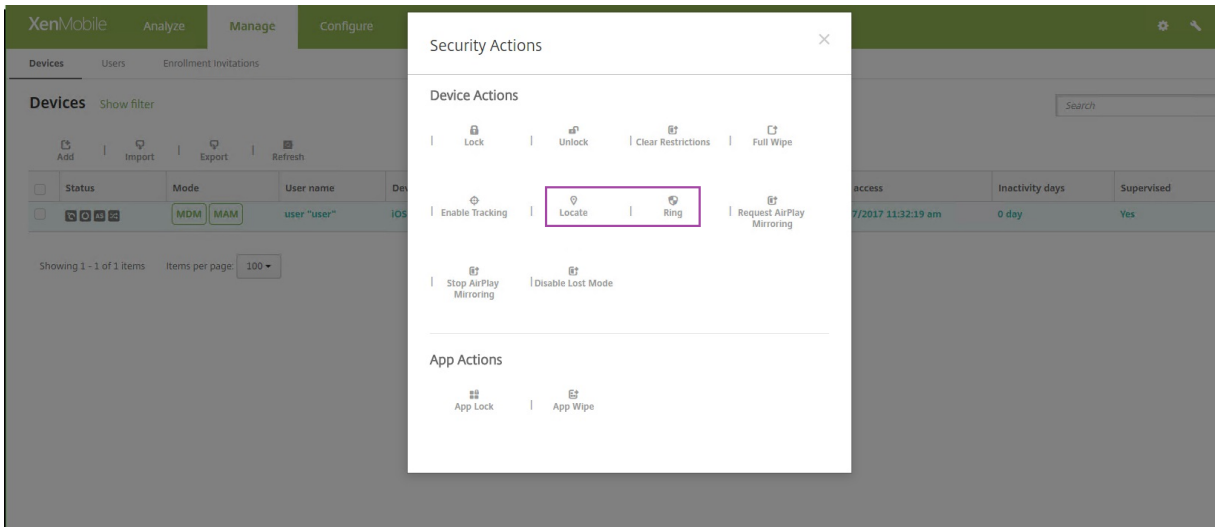
em **Reiniciar** ou **Desligar**.

Um dispositivo é reiniciado imediatamente quando recebe o comando **Reiniciar**. Os dispositivos iOS bloqueados por senha não reingressam às redes Wi-Fi após o reinício, portanto, poderão não se comunicar com o servidor. Um dispositivo é desligado imediatamente quando recebe o comando **Desligar**.



Localizar ou chamar um dispositivo iOS supervisionado que está no modo perdido

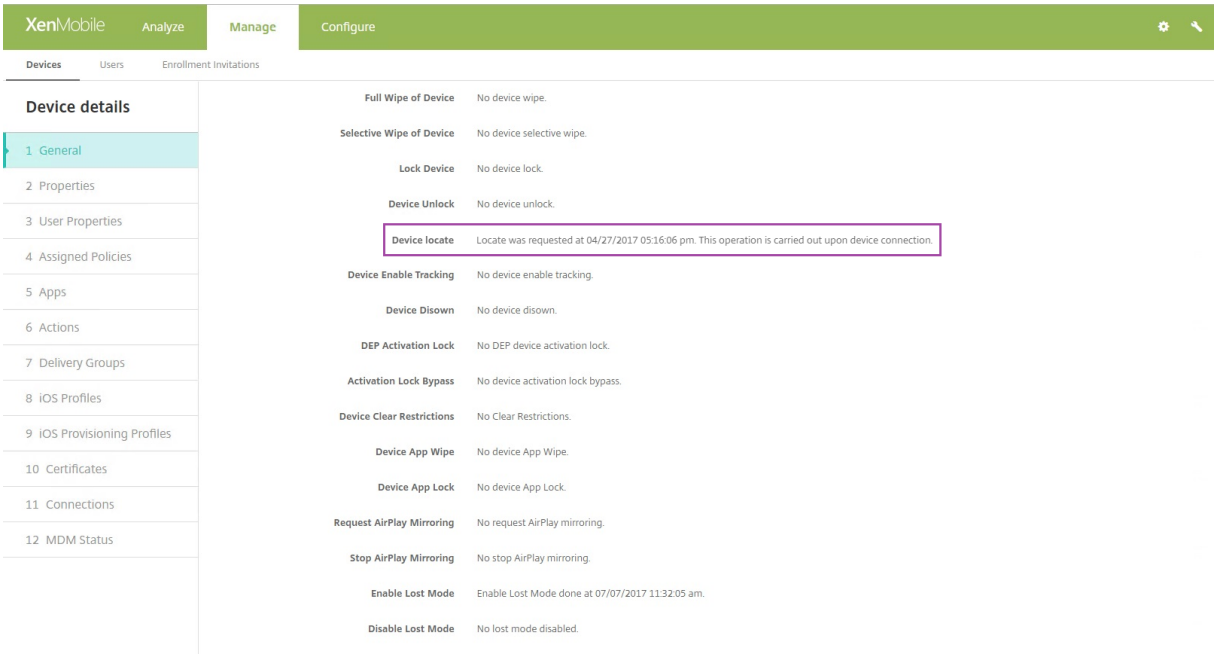
Depois de colocar um dispositivo iOS supervisionado no modo perdido, você pode usar ações de segurança para localizar ou fazer tocar o dispositivo. Um “toque” é o som do modo perdido que a Apple define para o dispositivo.



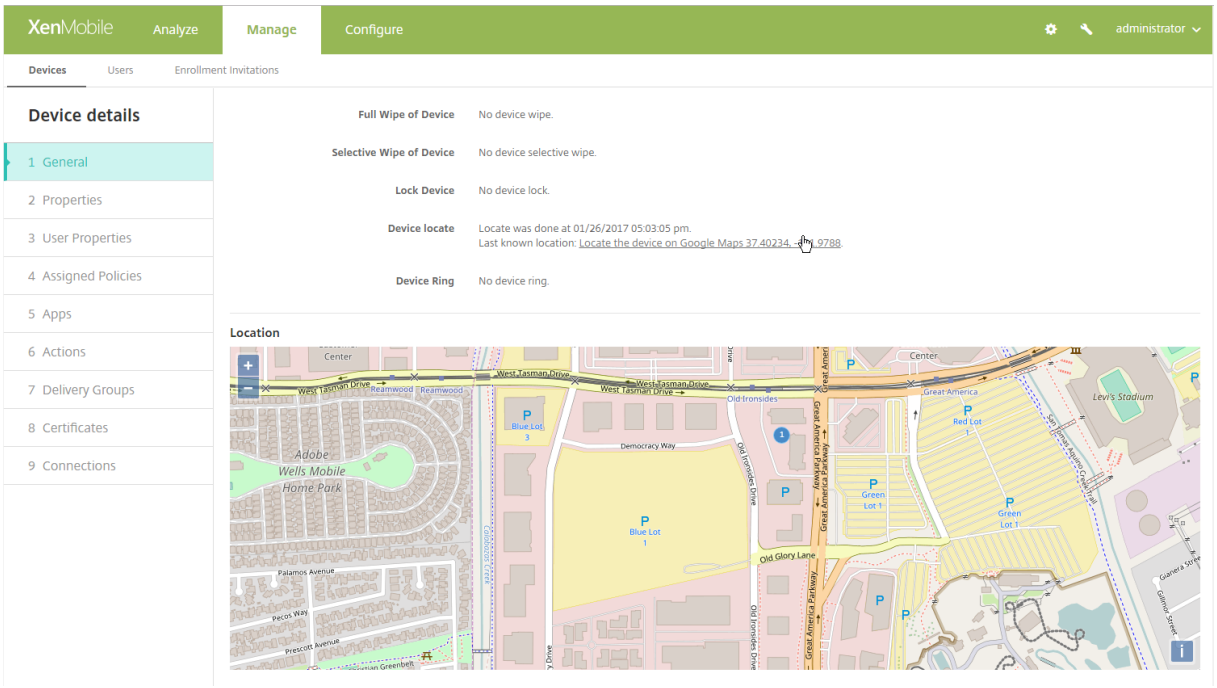
Para localizar um dispositivo que está no modo perdido

Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Localizar**. A página **Detalhes do dispositivo** fornece um status da solicitação de localização.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se o dispositivo for localizado, a página **Detalhes do dispositivo** inclui um mapa.



Para chamar um dispositivo que está no modo perdido (versão mínima iOS 10.3)

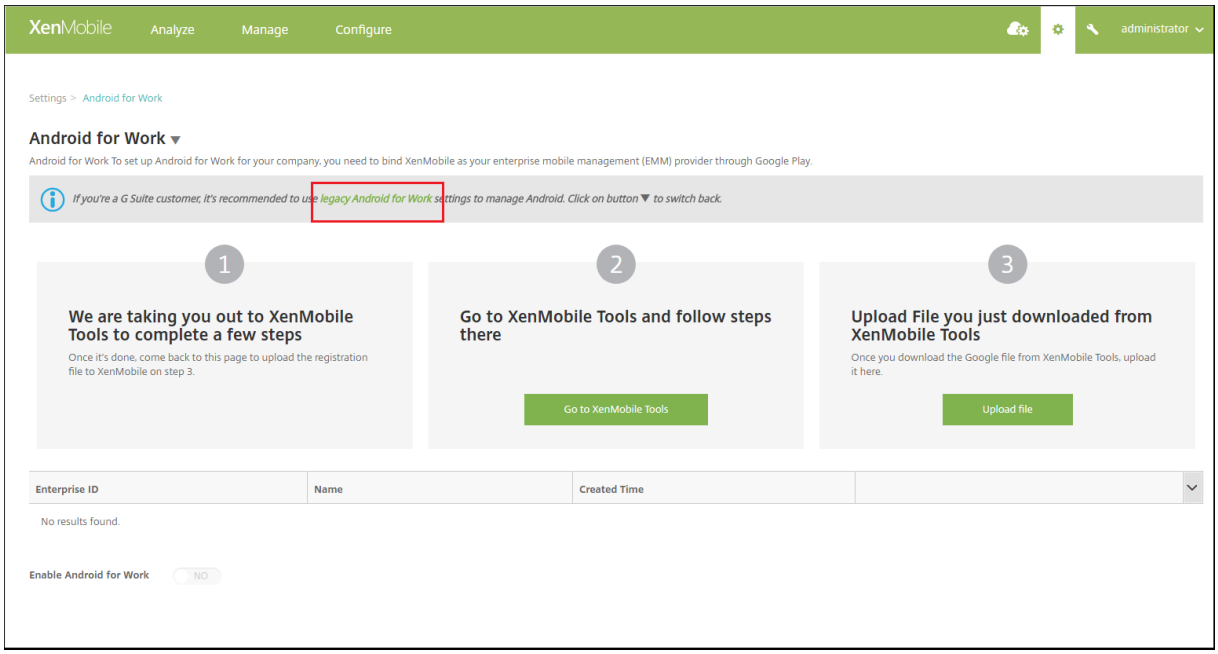
Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Tocar**. Na próxima vez em que o dispositivo se conecta, ele toca. Para interromper a chamada, o usuário clica no botão de alimentação. Para parar o toque do console XenMobile, use a ação de segurança **Desativar o Modo Perdido**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Suporte aprimorado do Android for Work

O XenMobile agora fornece uma maneira simples de configurar o Android for Work para sua organização. Usando as Ferramentas de Gerenciamento do XenMobile, você vincula o XenMobile como seu provedor de gerenciamento de mobilidade empresarial através do Google Play e cria uma empresa para o Android for Work.

> Nota:
>
> Os clientes do G Suite usam as configurações do Android for Work legado, conforme descrito em Clientes com "Android for Work legado for G Suite". Clique em **Android for Work legado** na página **Android for Work** nas configurações do XenMobile.



Você precisa:

- Suas credenciais de conta da Citrix para fazer logon no XenMobile Tools
- Suas credenciais corporativas de ID do Google para fazer login no Google Play

Para mais informações sobre o Android for Work, consulte Android for Work.

Suporte de atestado de integridade de dispositivo (DHA) no local

Agora você pode ativar o atestado de integridade de dispositivo (DHA, Device Health Attestation) para dispositivos móveis Windows 10 por meio de um servidor do Windows no local. Anteriormente, o DHA para XenMobile podia ser habilitado somente através do Microsoft Cloud.

Para habilitar o DHA no local, você primeiro configura um servidor DHA. Em seguida, você cria uma política do XenMobile Server para habilitar o serviço DHA local.

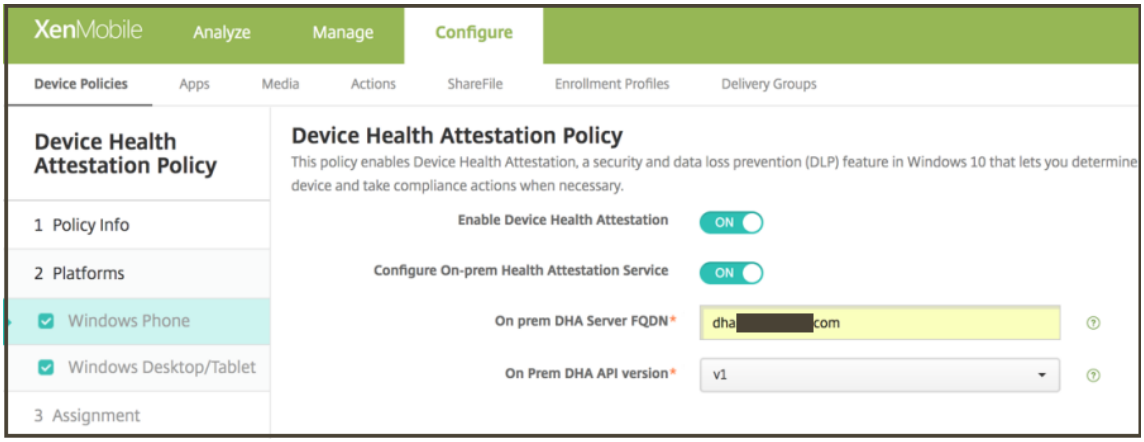
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar um DHA, você precisa de uma máquina executando o Windows Server 2016 Technical Preview 5 ou posterior. Você instala o DHA como uma função de servidor. Para obter instruções, consulte este artigo do Microsoft TechNet, Atestado de integridade de dispositivo.

Para a política do XenMobile Server habilitar o serviço DHA local:

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.
2. Se você já criou uma política para habilitar o DHA através do Microsoft Cloud, vá para a etapa 8.
3. Clique em **Adicionar** para adicionar uma política. É exibida a caixa de diálogo **Adicionar uma nova política**.
4. Clique em **Mais** e, em **Personalizado**, clique em **Política de atestado de integridade de dispositivo**. A página de informações sobre a **Política de atestado de integridade de dispositivo** é exibida.
5. No painel Informações sobre a política, insira as seguintes informações:
   - **Nome da política:** digite um nome descritivo para a política.
   - **Descrição:** digite uma descrição opcional para a política.
6. Clique em **Avançar**. A página Plataforma de política é exibida.
7. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.
8. Para cada plataforma escolhida:
   a) Defina **Ativar atestado de integridade do dispositivo como Ativado**.
   b) Defina **Configurar o serviço de atestado de integridade local** como **Ativado**.
   c) **FQDN do Serviço DHA no local:** insira o nome de domínio totalmente qualificado do servidor DHA que você configurou.
   d) **Versão da API DHA no local:** escolha a versão do serviço DHA instalado no servidor DHA.
9. Configure regras de implantação e escolha grupos de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para confirmar que a política foi envia para um dispositivo Windows 10 Mobile

1. No console XenMobile, clique em **Gerenciar > Dispositivos**.
2. Selecione o dispositivo.
3. Selecione **Propriedades**.
4. Role até “Atestado de integridade de dispositivo Windows”.

Mais macros para modelos de registro

Você pode usar essas novas macros ao criar modelos de registro para convites de registro do dispositivo:

```
${
 enrollment.urls }

${
 enrollment.ios.url }

${
 enrollment.macos.url }

${
 enrollment.android.url }

${
 enrollment.ios.platform }

${
 enrollment.macos.platform }
```

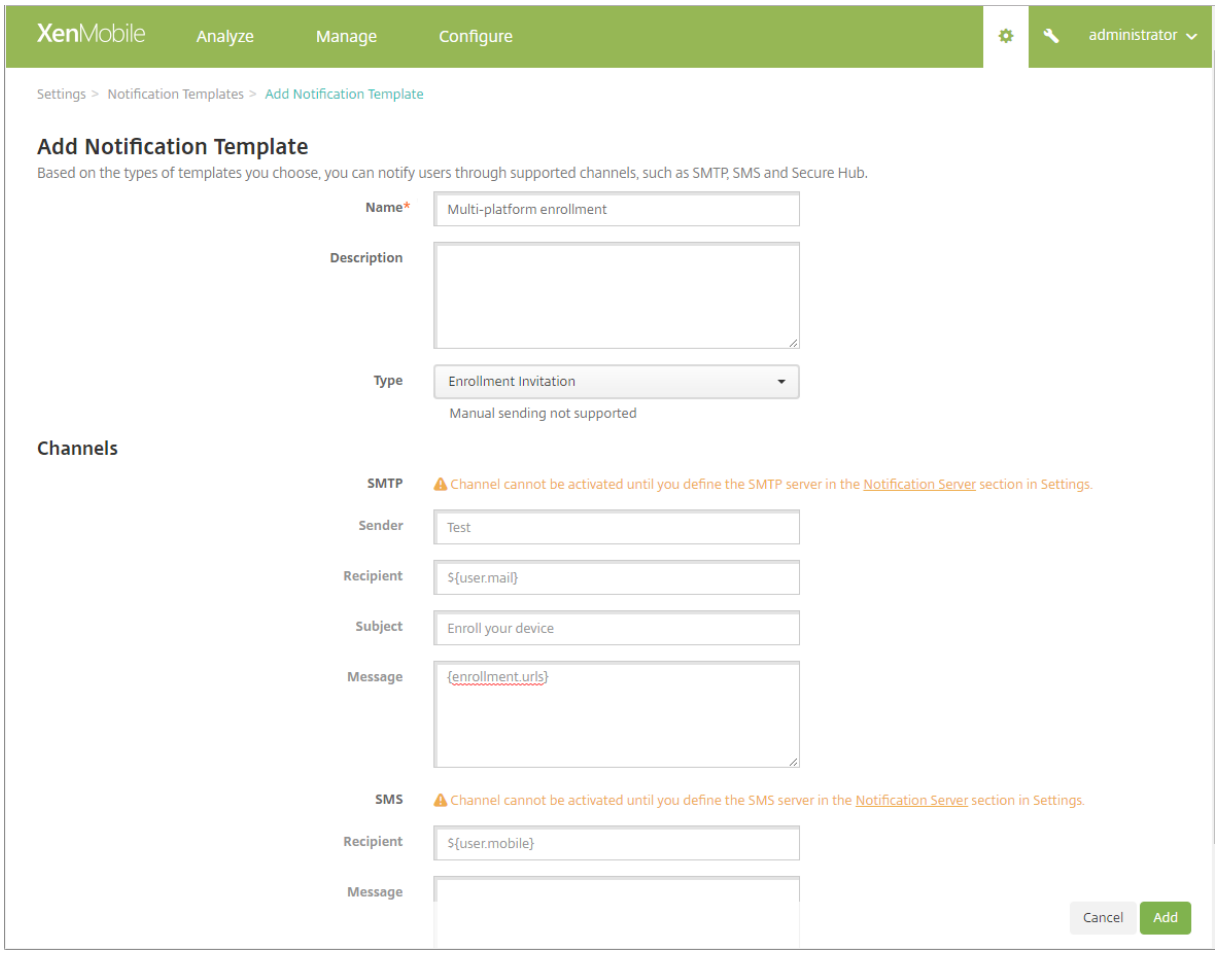
© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
18
19 ${
20  enrollment.android.platform }
21
22 ${
23  enrollment.agent }
```

Essas macros permitem que você crie modelos de registro que contêm URLs de registro para várias plataformas de dispositivos.

Este exemplo mostra como criar uma notificação que inclui URLs de registro para várias plataformas de dispositivo. A macro para a **Mensagem** é:

${enrollment.urls}



Esses exemplos mostram como criar mensagens para notificações que levam os usuários a clicar na URL de registro para as plataformas de seus dispositivos:

Exemplo 1

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
To enroll, please click the link below that applies to your device
   platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }
```

Exemplo 2

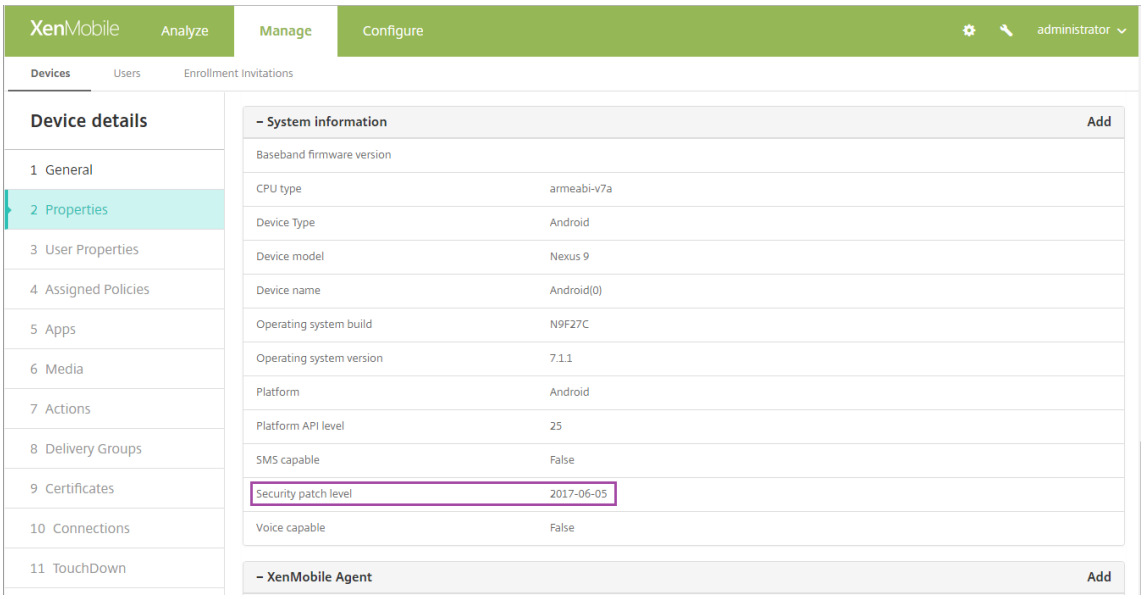
```
To enroll an iOS device, click the link ${
 enrollment.ios.url }
 .

To enroll a macOS device, click the link ${
 enrollment.macos.url }
 .

To enroll an Android device, click the link ${
 enrollment.android.url }
 .
```

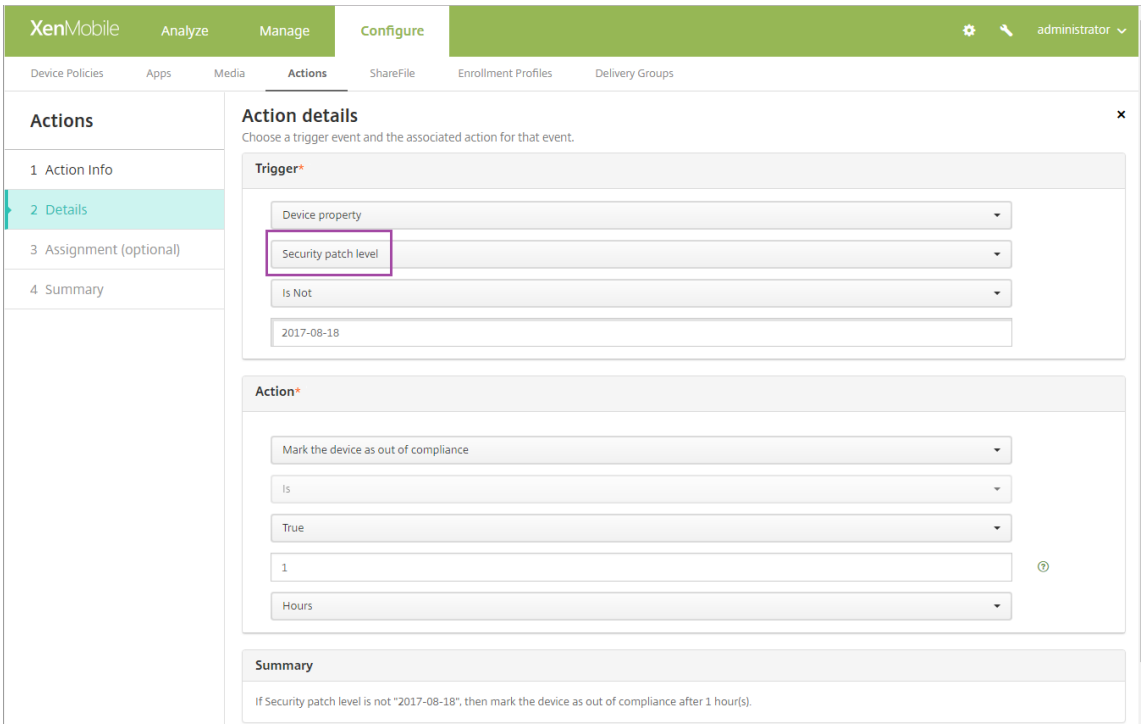
Outras melhorias

- O console XenMobile e o Portal de Ajuda automática estão agora disponíveis em espanhol.
- **XenMobile agora relata o nível de patch de segurança para dispositivos Android**. Você pode visualizar o **Nível de patch de segurança** na página **Gerenciar > Dispositivos** e em **Detalhes**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

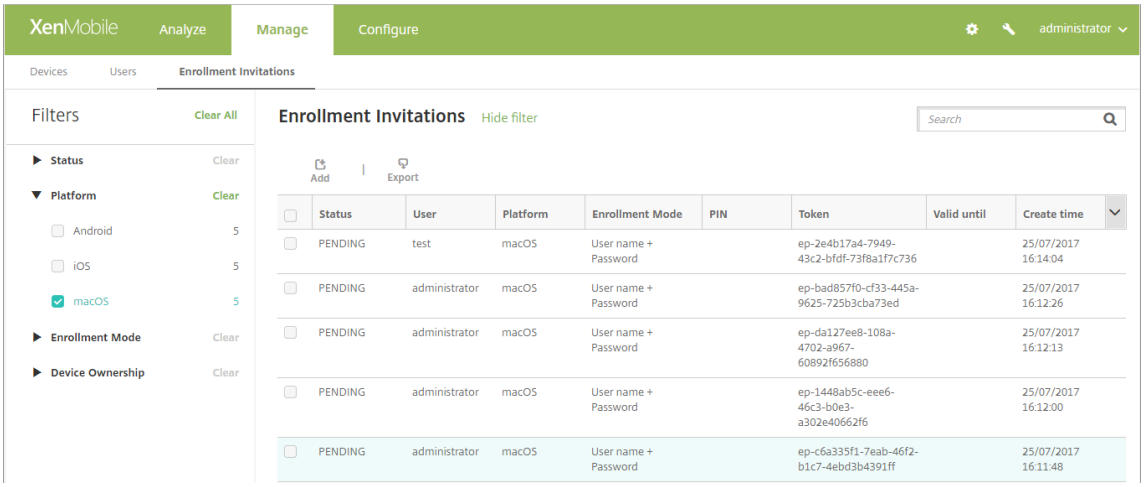
do dispositivo. Você também pode usar **Configurar > Ações** para criar uma ação que dispare o nível de patch de segurança.



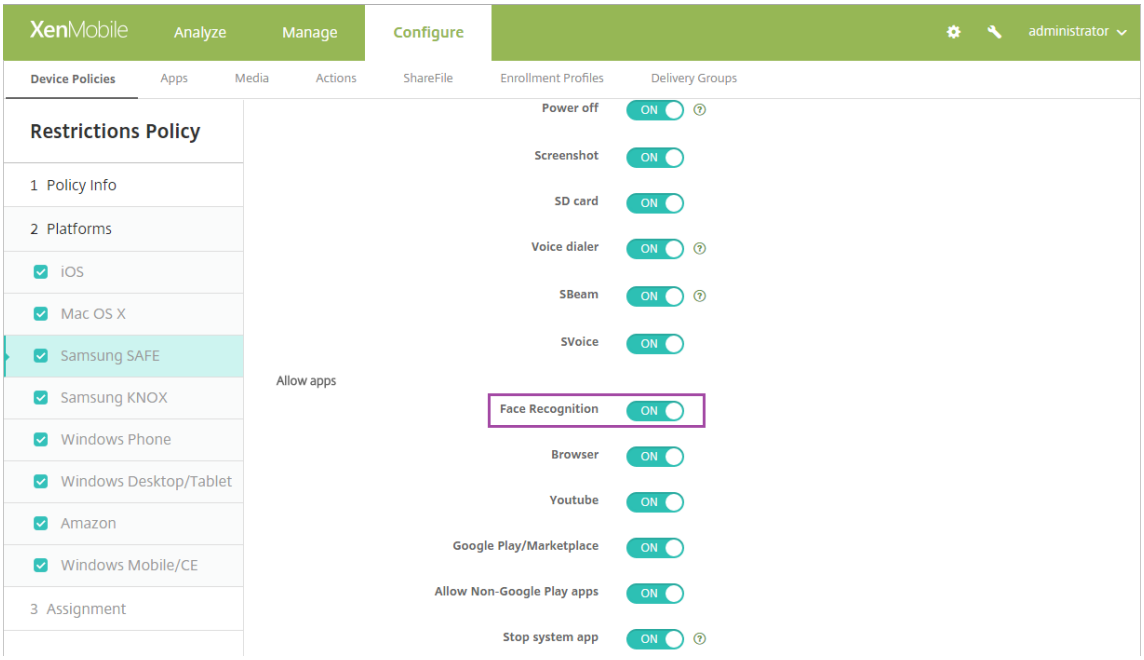


- **Filtrar convites de registro por macOS**. O filtro de plataforma de **Gerenciar > Convites para registro** agora inclui **macOS**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Configuração de política de Restrições para impedir que os usuários usem reconhecimento de face para desbloquear dispositivos Samsung Galaxy S8+**. A política de dispositivo de Restrições para Samsung SAFE agora inclui a configuração de **Reconhecimento de face**. Para bloquear o uso do reconhecimento de rosto para desbloquear o acesso ao dispositivo, vá em **Configurar > Políticas do Dispositivo** e edite a política de Restrições para definir **Reconhecimento de face** como **Desativado**.

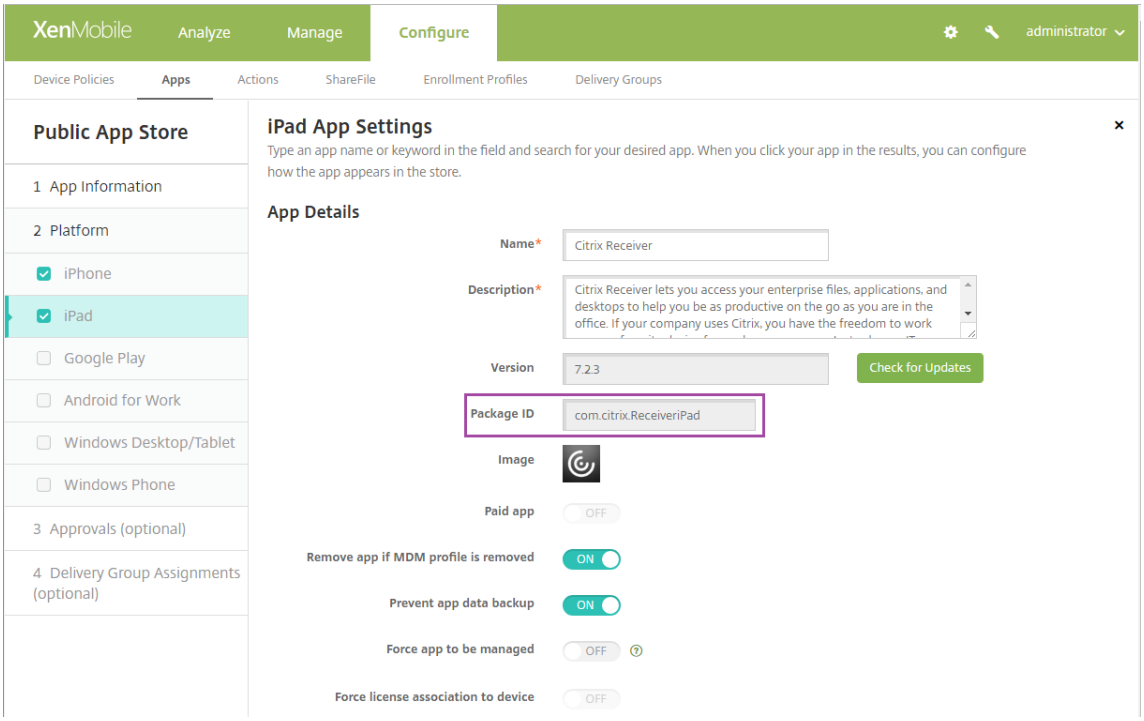


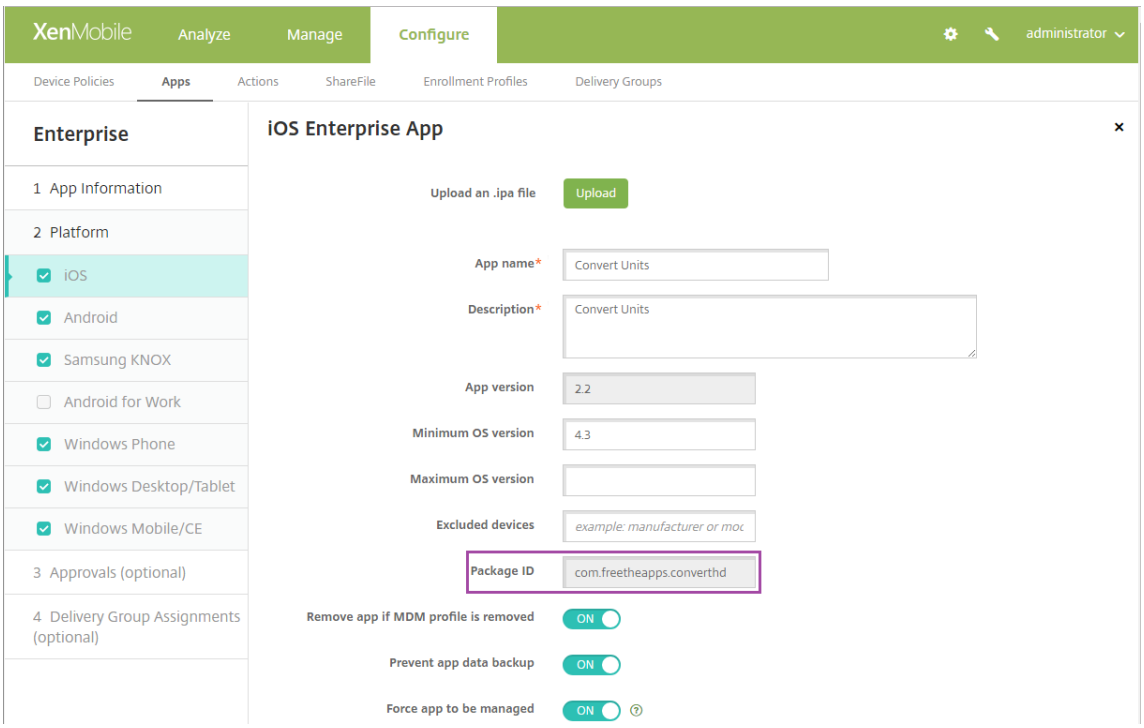
- **Os aplicativos macOS VPP necessários agora são suportados**. Agora você pode implantar aplicativos VPP do macOS como aplicativos necessários para usuários locais e Active Directory. Você pode visualizar os aplicativos VPP do macOS em **Configurar > Aplicativos**, onde pode filtrar os aplicativos por macOS VPP. Nessa página, a seção **Configuração da loja** não aparece para os aplicativos macOS VPP porque não existe um Secure Hub para macOS. Em **Gerenciar > Dispositivos**, as **Propriedades do Usuário** incluem Desativar conta VPP para as contas do

© 1999-2019 Citrix Systems, Inc. All rights reserved.

macOS VPP.

- **Configurar > Aplicativos agora mostra o ID do pacote para aplicativos da loja de aplicativos pública e aplicativos empresariais**

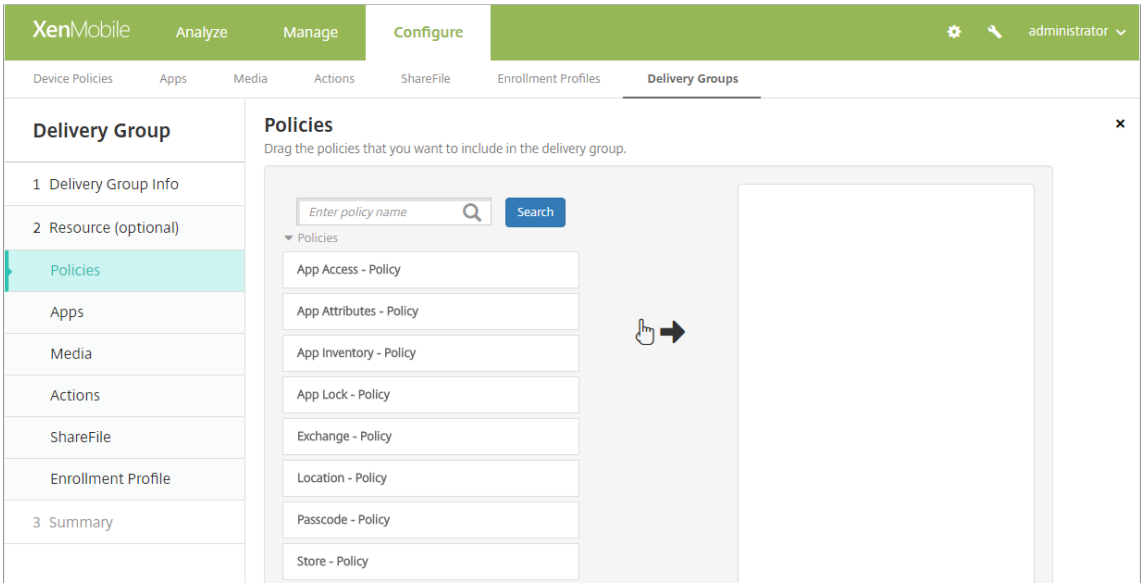


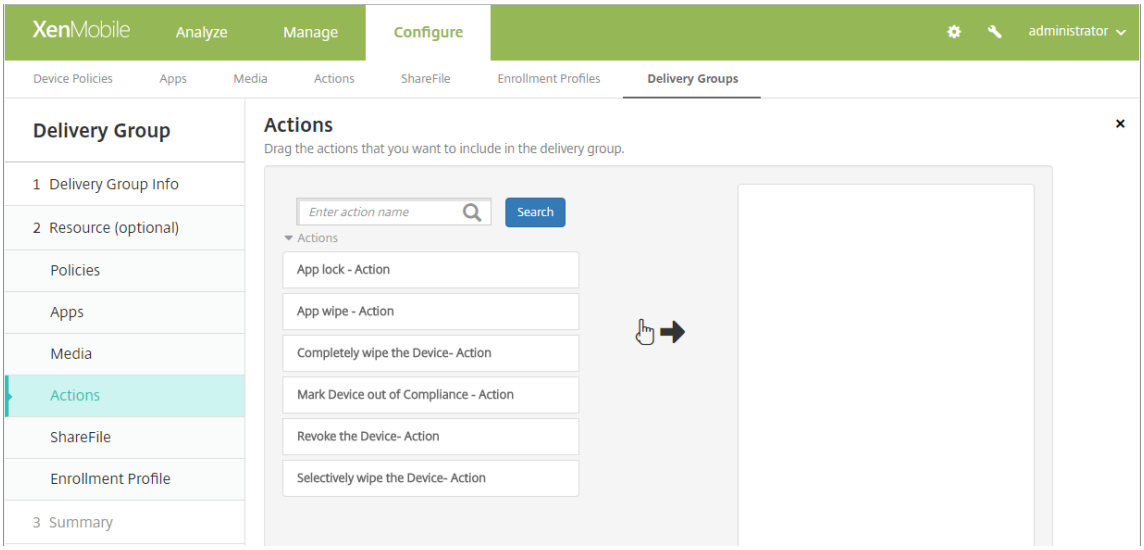


- **Lista de recursos em ordem alfabética para grupos de entrega.** Em **Configurar > Grupos de entrega**, todas as listas de recursos e os resultados da pesquisa são exibidos em ordem al-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

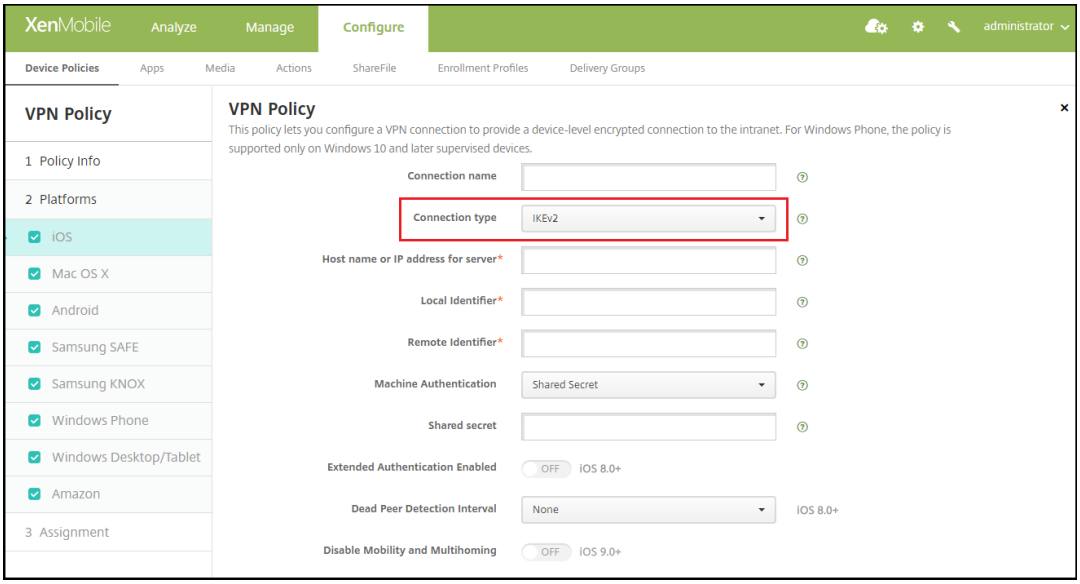
fabética.

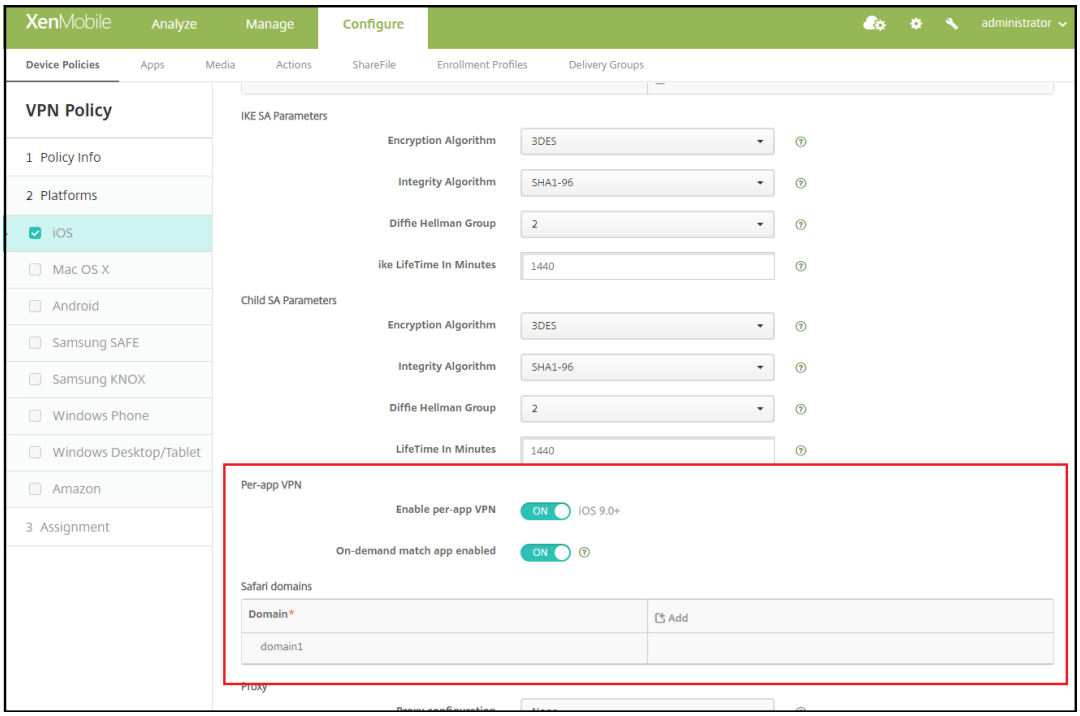




- Nas páginas **Gerenciar > Dispositivos** e **Gerenciar > Usuários**, as datas agora aparecem no formato de 24 horas, dd/mm/aaaa hh:mm:ss. As datas refletem o fuso horário local para usuários e dispositivos.
- **A política de VPN para dispositivos iOS agora oferece uma opção de VPN por aplicativo para políticas de VPN de tipo iKEv2.** Os dispositivos iOS 9.0 e posteriores suportam VPN por aplicativo para conexões iKEv2. As opções de **Ativar VPN por aplicativo** da VPN por aplicativo são:
  - Ativar VPN por aplicativo
  - Correspondência de aplicativo sob demanda ativada
  - Domínios do Safari

© 1999-2019 Citrix Systems, Inc. All rights reserved.





Na seção “iOS”, adicione à seção de tipo de conexão iKEv2:

Ativar VPN por aplicativo: selecione se a VPN por aplicativo deve ser ativada. O padrão é **O**. Disponível apenas no iOS 9.0 e versões posteriores.

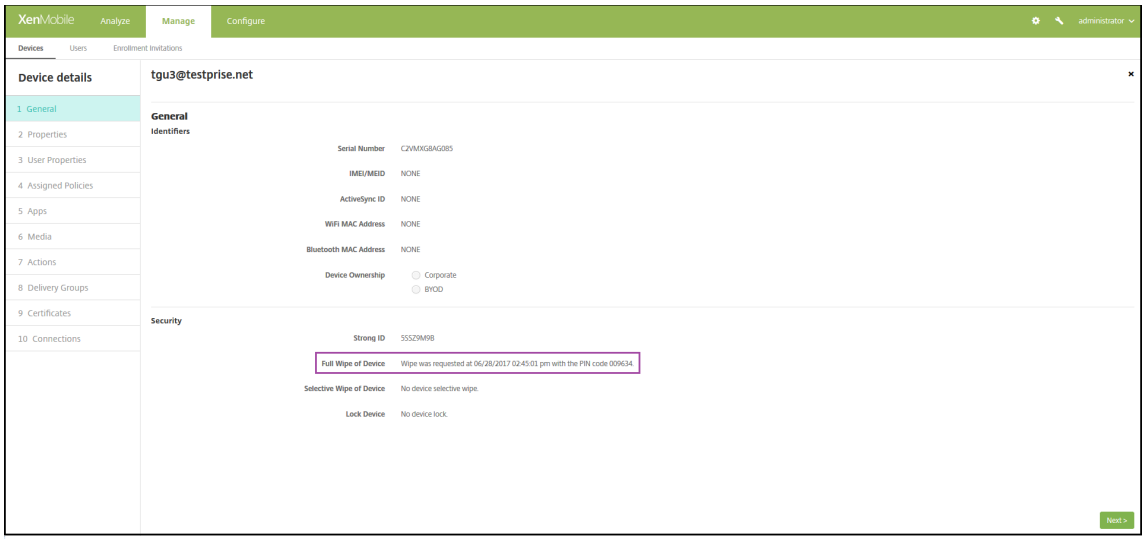
Correspondência de aplicativo sob demanda ativada: selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **O**.

Domínios Safari: clique em **Adicionar** para adicionar um nome de domínio do Safari.

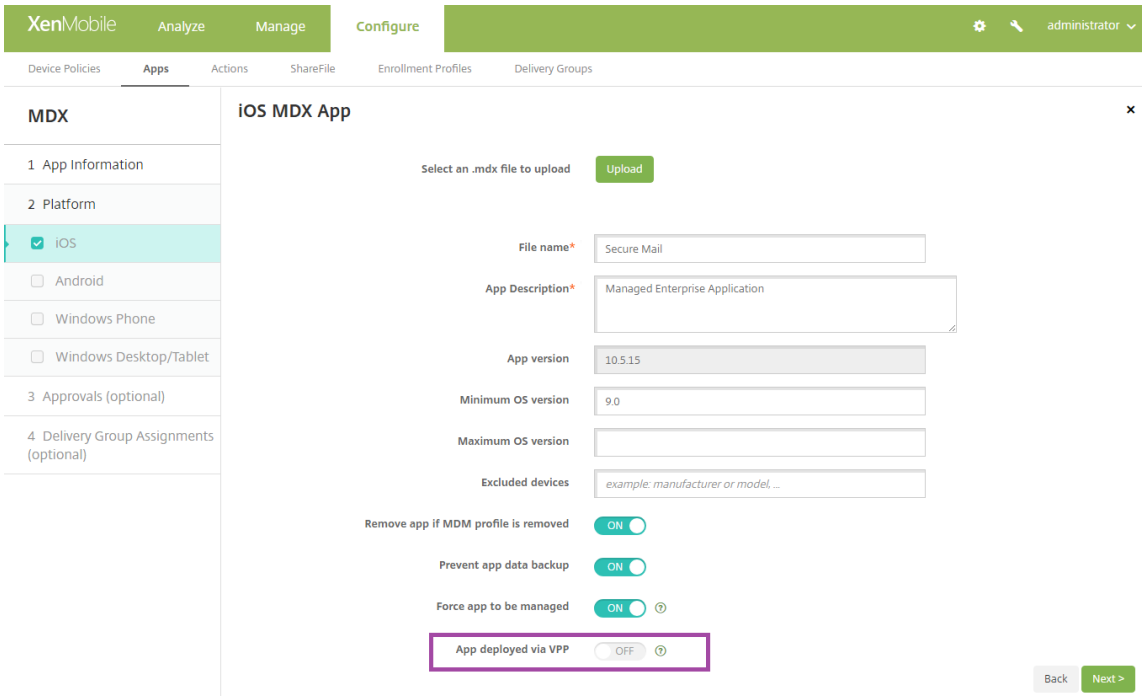
- **Limpe o código para dispositivos macOS mostrados no console XenMobile.** Os dispositivos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

macOS exigem que o usuário insira um código PIN depois que o dispositivo foi apagado. Se o usuário não se lembrar deste código, agora você pode procurar o código de limpeza na página de detalhes **Gerenciar > Dispositivo**.



- **Quando você usa o VPP para implantar um aplicativo MDX, a loja do Secure Hub agora mostra apenas a instância VPP do aplicativo.** Anteriormente, aplicativos VPP e MDX eram exibidos na loja. Essa alteração impede que os usuários finais instalem a versão MDX do aplicativo, o que exige que o usuário tenha uma conta do iTunes. Quando você adiciona um aplicativo MDX, há uma nova configuração, **Aplicativo implantado via VPP**. Altere essa configuração para **Ativar** se você planeja implantar o aplicativo usando VPP.

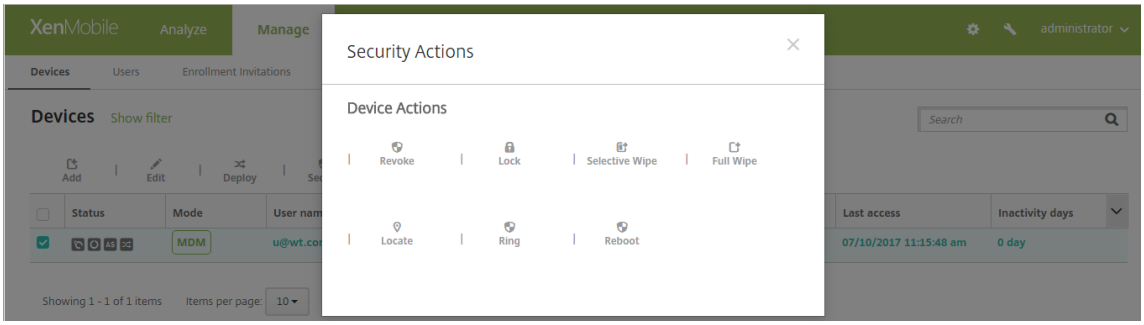


- **Melhor desempenho ao importar muitas licenças do VPP.** Essa otimização usa multithread-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ing. Uma nova propriedade de XenMobile Server, **MaxNumberOfWorker**, usa o padrão **3** (threads). Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, com um número maior de threads, como 6, uma importação VPP resulta em uso de CPU muito alto.

- No console XenMobile, todas as referências a Mac OS X, OS X, OSX, MACOSX e MacOS agora são macOS.
- **Reinicie um dispositivo Windows 10.** Agora você pode enviar uma ação de segurança, Reinicializar, para reinicializar um dispositivo. Em Windows Tablet e PCs, a mensagem "Sistema reinicializará em breve" aparece e a reinicialização ocorre em cinco minutos. No Windows Phone, não há mensagem de aviso para usuários, e a reinicialização ocorre após alguns poucos minutos.



Mudanças na API pública REST

Para os serviços REST de notificação de dispositivo, você agora pode notificar um dispositivo usando a ID de dispositivo, sem a necessidade de o XenMobile enviar um token.

Quando você usar a API REST pública do XenMobile para criar convites para registro, agora você pode:

- **Especificar um PIN personalizado.** Se o modo de registro exigir um PIN, você pode usar um PIN personalizado em vez de um gerado aleatoriamente pelo XenMobile Server. O tamanho do PIN deve coincidir com a configuração definida para o modo de registro. O tamanho do PIN padrão é 8. Por exemplo, uma solicitação pode incluir: "pin": "12345678"
- **Selecione várias plataformas.** Anteriormente, você podia usar a API REST para especificar apenas uma plataforma para um convite de registro. O campo "plataforma" é obsoleto e substituído por "plataformas". Por exemplo, uma solicitação pode incluir: "plataformas": ["iOS", "MACOSX"]

A API pública XenMobile para REST Services agora inclui as seguintes APIs:

- Obter por ID de contêiner
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Aplicativos WebLink
  - Aplicativos Web/SaaS
  - Aplicativos da loja pública
- Carregar o aplicativo em contêiner novo ou existente
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais
- Atualizar detalhes da plataforma dentro do contêiner para aplicativos móveis MDX e aplicativos da loja pública
- Adicionar ou atualizar aplicativo
  - Aplicativos WebLink
  - Aplicativos Web/SaaS
  - Aplicativos da loja pública
- Obter todos os conectores Web/SaaS ou obter conectores Web/Saas por nome do conector
- Excluir o contêiner de aplicativo
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais
  - Aplicativos WebLink
  - Aplicativos Web/SaaS

Para obter detalhes, consulte XenMobile Public API for REST Services.

Avisos de terceiros

March 6, 2019

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

Avisos de terceiros do XenMobile

Problemas resolvidos

October 4, 2018

O XenMobile 10.9 inclui os seguintes problemas resolvidos.

Para problemas corrigidos relacionados a aplicativos móveis de produtividade, consulte a página de cada aplicativo em Secure Hub, Secure Mail e Secure Web.

Em **Configurar > Políticas de dispositivos > Política de bloqueio de aplicativos**: depois de digitar o nome da política e ir para a página do iOS, os IDs dos pacotes não aparecem no menu ID do pacote

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de aplicativos. Depois que você alternar entre Android e iOS, os IDs dos pacotes de aplicativos serão exibidos. [CXM-39302]

Depois de atualizar para o XenMobile Server 10.7 ou posterior e registrar um dispositivo: a contagem de licenças mostrada no console XenMobile é muito maior do que o número real de dispositivos registrados. Esse problema é devido a um componente de terceiros. [CXM-40533]

Se uma conta DEP for uma organização EDU. Você não pode alterar a configuração de DEP "Exigir credenciais para o registro do dispositivo" no XenMobile Server 10.7. A opção está sempre ativada e não pode ser desativada. [CXM-51174]

Depois de adicionar uma propriedade personalizada com um caractere especial, você não pode acessar a página Dispositivos no console XenMobile. [CXM-51714]

Quando os usuários registrados no XenMobile Server por meio de "registro por e-mail" tentam alterar o Nome UPN no Active Directory, o dispositivo vai para um estado não gerenciado, causando o bloqueio/apagamento do aplicatvio. No entanto, quando o usuário tenta se registrar novamente com o novo UPN, ele é direcionado de volta à tela First Time Use (FTU). Para ativar a correção, defina a propriedade do servidor personalizada "refresh.user.using.objectguid" como "true". [CXM-52783]

Depois que um usuário se registra no Android for Work em um dispositivo Samsung usando um código QR, os aplicativos e as políticas não são implantados no dispositivo. [CXM-53973]

Ao registrar dispositivos usando o Android for Work, os UPNs dos usuários não mapeiam para o ID do usuário do G Suite existente. Em vez disso, um novo ID do usuário do G Suite é criado. [CXM-53977]

Sem nenhum proxy https configurado, você não pode enviar mensagens de texto SMS através do gateway Nexmo SMS. [CXM-54308]

Você não pode usar a API REST pública para implantar grupos de entrega. [CXM-55251]

Quando a propriedade do servidor "device.properties.userDefined1" não está definida, um valor adicionado à propriedade de detalhes do dispositivo User Defined#1 não é exibido corretamente. [CXM-55394]

Quando você instala um aplicativo corporativo do iOS sem uma versão do aplicativo em um dispositivo, o inventário do perfil do iOS não é atualizado no XenMobile. [CXM-55549]

Depois de atualizar do XenMobile 10.6 para o 10.8 RP1, o console da Web às vezes não responde depois que um administrador efetua login. Uma mensagem de erro exibe "TypeError: this.featureFlags is undefined". [CXM-55550]

O número de resultados visíveis em **Gerenciar > Usuários > Grupos Locais** agora é 500. [CXM-55601]

Os aplicativos corporativos não são atualizados silenciosamente em dispositivos supervisionados que executam o iOS 11.4 ou posterior. [CXM-55607]

Aplicativos B2B VPP Secure de terceiros não são exibidos conforme instalados no Secure Hub. [CXM-55889]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Informações correlatas

- Suporte do XenMobile Knowledge Center

Problemas conhecidos

April 15, 2019

No XenMobile 10.9 existem os seguintes problemas conhecidos.

Para problemas conhecidos relacionados a aplicativos móveis de produtividade, consulte a página de cada aplicativo em Secure Hub, Secure Mail e Secure Web.

Os convites de registro para dispositivos macOS se referem a MACOSX em vez de macOS. [CXM-32370]

Os administradores do RBAC podem atribuir a função de administrador padrão para os usuários novos ou existentes. Atribuir a função de administrador padrão deve ser restrita a super administradores. [CXM-37805]

Se o XenMobile Server estiver instalado no modo FIPS (Federal Information Processing Standards), você poderá alternar para o driver JDBC (Microsoft Java Database Connectivity) com a Autenticação do SQL. A mudança para o driver JDBC com a autenticação do Windows falha. [CXM-42619]

Se o SQL Server for implantado em um domínio filho ou se um logon de banco de dados do domínio filho for usado, o JDBC (Microsoft Java Database Connectivity) com a Autenticação do Windows falhará. [CXM-42969]

Nas páginas **Configurar > Políticas de dispositivo** e **Configurar > Aplicativos**: quando você classifica as listas pela coluna **Tipo**, os itens não aparecem na ordem correta. [CXM-43565]

Ao usar a página **Analisar > Relatórios** no Safari, não é possível exportar um gráfico como PDF. [CXM-45716]

Quando você faz o carregamento do último arquivo .apk do Chrome (com.android.chrome_v64.0.3282.137-328213700_Android-4.1) para o XenMobile em **Configurar > Aplicativos**, esta mensagem é exibida: 500 Erro interno do servidor. [CXM-45722]

Registro OTA para dispositivos macOS tem suporte apenas nos navegadores Safari e Chrome. [CXM-45872]

XenMobile Server 10.7 e 10.8 não são compatíveis com o Remote PostgreSQL 10.1.3. Use Remote PostgreSQL 9.5.1 or 9.5.11. [CXM-46253]

XenMobile não dá suporte a gerenciamento de aplicativos auto-hospedados para Android for Work. Observe que isso não é novo no XenMobile Server 10.8. As alterações feitas pelo Google interrompem todos os servidores novos e existentes com esse recurso. [CXM-46413]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ao usar o código QR para o registro do Android Enterprise, no ponto de aumento de NFC no dispositivo com redefinição de fábrica, a autenticação de segurança WPA2 (Wi-Fi) não está funcionando. [CXM-51621]

Depois de importar a imagem do XenMobile Server 10.8 ou 10.9 para o VMware ESXi 6.7 ou 6.5 Atualização 2: após reiniciar a máquina virtual, o aplicativo de configuração não inicia, o XenMobile Server entra no modo de recuperação e as configurações de IP são limpas. Como solução alternativa a esse problema, crie uma nova máquina virtual com uma NIC VMXNET3 e, em seguida, associe essa máquina virtual ao banco de dados da máquina virtual que entrou no modo de recuperação. [CXM-54581]

Em instalações XenMobile não padrão, o registro da Apple DEP falha. [CXM-55010]

A atualização do XenMobile Server para 10.9.0.9 está falhando no XenCenter. [CXM-55052]

Ao renovar uma autoridade de certificação para dispositivos macOS, se a renovação falhar, o status de renovação da CA fica inconsistente. [CXM-55079]

Em um cluster de servidor, se você gerar uma nova autoridade de certificação (CA) em um nó, não é possível ativar a autoridade de certificação padrão em nenhum outro nó. [CXM-55293]

Para dispositivos Android, quando uma renovação de certificado não é bem-sucedida ou é cancelada, a verificação dos registros do Grupo de Entrega mostra que a renovação do certificado de registro foi concluída com êxito. [CXM-55352]

Em configurações com criptografia SHA1 ativada, o registro com dispositivos iOS 12 falha. Para obter mais informações, consulte https://support.apple.com/en-us/HT207459 [CXM-55908]

Informações correlatas

- Suporte do XenMobile Knowledge Center

Arquitetura

April 15, 2019

Os componentes do XenMobile na arquitetura de referência do XenMobile que você optar por implantar se baseiam nos requisitos de gerenciamento de dispositivo ou aplicativo da sua organização. Os componentes do XenMobile são modulares e se baseiam uns nos outros. Por exemplo, para fornecer aos usuários na sua organização acesso remoto a aplicativos móveis e para acompanhar os tipos de dispositivo, você implanta o XenMobile com o NetScaler Gateway. O XenMobile é onde você gerencia os dispositivos e aplicativos, e o NetScaler Gateway permite que os usuários se conectem à sua rede.

Implantando componentes do XenMobile: você pode implantar o XenMobile para permitir que os usuários se conectem aos recursos na sua rede interna das seguintes maneiras:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Conexões com a rede interna. Se os seus usuários forem remotos, eles poderão se conectar usando uma VPN ou uma conexão micro VPN por meio do NetScaler Gateway. Essa conexão fornece acesso a aplicativos e áreas de trabalho na rede interna.
- Registro do dispositivo. Os usuários podem registrar dispositivos móveis no XenMobile para que você possa gerenciá-las no console XenMobile que se conecta aos recursos de rede.
- Aplicativos Web, SaaS e móveis. Os usuários podem acessar aplicativos Web, SaaS e móveis do XenMobile por meio do Secure Hub.
- Aplicativos e áreas de trabalho virtuais baseados no Windows. Os usuários podem se conectar com o Citrix Receiver ou um navegador da Web para acessar aplicativos e áreas de trabalho virtuais baseados no Windows do StoreFront ou na Web Interface.

Para obter algumas dessas capacidades para um XenMobile Server local, a Citrix recomenda a implantação dos componentes do XenMobile na seguinte ordem:

- NetScaler Gateway. Você pode definir as configurações do NetScaler Gateway para permitir a comunicação com o XenMobile, o StoreFront ou a Web Interface usando o assistente de Configuração Rápida. Antes de usar o assistente de Configuração Rápida no NetScaler Gateway, você deve instalar um dos seguintes componentes para configurar as comunicações: XenMobile, StoreFront ou Web Interface.
- XenMobile. Depois de instalar o XenMobile, você poderá definir políticas e configurações no console XenMobile, o que permite que os usuários registrem os dispositivos móveis dele. Você também pode configurar aplicativos móveis, Web e SaaS. Os aplicativos móveis podem incluir aplicativos da Apple App Store ou do Google Play. Os usuários também podem se conectar com aplicativos móveis que você prepara usando o MDX Toolkit e carrega para o console.
- MDX Toolkit. O MDX Toolkit pode preparar com segurança os aplicativos criados dentro da sua organização ou fora da sua empresa. Depois preparar um aplicativo, use o console XenMobile para adicioná-lo ao XenMobile e alterar a configuração de política, conforme necessário. Você também pode adicionar categorias de aplicativo, aplicar fluxos de trabalho e implantar aplicativos em grupos de entrega. Veja Sobre o MDX Toolkit.
- StoreFront (opcional). Você pode fornecer acesso a aplicativos e áreas de trabalho virtuais baseados no Windows do StoreFront por meio de conexões com o Receiver.
- ShareFile Enterprise (opcional). Se você implantar o ShareFile, poderá ativar a integração de diretório empresarial por meio do XenMobile, que atua como um provedor de identidade Security Assertion Markup Language (SAML). Para obter mais informações sobre como configurar os provedores de identidade para o ShareFile, consulte o site de suporte do ShareFile.

O XenMobile oferece gerenciamento de dispositivo e de aplicativo por meio do console XenMobile. Esta seção descreve a arquitetura de referência da implantação do XenMobile.

Em um ambiente de produção, a Citrix recomenda a implantação da solução XenMobile em uma configuração de cluster para escalabilidade e redundância de servidor. Além disso, o uso da capacidade de Descarga de SSL do NetScaler pode reduzir ainda mais a carga no servidor XenMobile e aumentar a

© 1999-2019 Citrix Systems, Inc. All rights reserved.

taxa de transferência. Para obter mais informações sobre como configurar o clustering para o XenMobile mediante a configuração de dois endereços IP virtuais de balanceamento de carga no NetScaler, consulte Armazenamento em cluster.

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

As seções a seguir descrevem diferentes arquiteturas de referência para a implantação do XenMobile. Para obter um diagrama detalhado da arquitetura de referência, consulte os artigos do XenMobile Deployment Handbook, Arquitetura de referência para implantações locais e Arquitetura. Para obter uma lista completa de portas, consulte Requisitos de porta (no local) e Requisitos de porta (na nuvem).

Modo de gerenciamento de dispositivo móvel (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 dá suporte à alteração para o modo de autenticação após o registro de usuário. Para obter mais informações, consulte Atualize do XenMobile 10.8 MDM Edition para Enterprise Edition.

O XenMobile MDM Edition permite o gerenciamento de dispositivos móveis. Para obter suporte à plataforma, consulte Sistemas operacionais compatíveis de dispositivos. Implante o XenMobile no modo MDM se você planejar usar somente os recursos MDM do XenMobile. Por exemplo, se você deseja fazer o seguinte.

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

No modelo recomendado, o XenMobile Server é posicionado no DMZ com um NetScaler opcional na frente, o que oferece uma proteção adicional ao XenMobile.

Modo de gerenciamento de aplicativos móveis (MAM)

MAM, também chamado de modo somente MAM, oferece gerenciamento de aplicativos móveis. Para obter suporte à plataforma, consulte Sistemas operacionais compatíveis de dispositivos. Implante o XenMobile no modo MAM se você planejar usar somente os recursos MAM do XenMobile sem registrar dispositivos para o MDM. Por exemplo, se você deseja fazer o seguinte.

- Proteger aplicativos e dados em dispositivos móveis BYO.
- Fornecer aplicativos móveis empresariais.
- Bloquear aplicativos e apagar os respectivos dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Os dispositivos não podem registrados no MDM.

Nesse modelo de implantação, o XenMobile Server é posicionado com o NetScaler Gateway na frente, o que oferece uma proteção adicional ao XenMobile.

Modo MDM+MAM

O uso dos modos MDM e MAM juntos permite o gerenciamento de aplicativos e dados móveis e o gerenciamento de dispositivos móveis. Para obter suporte à plataforma, consulte Sistemas operacionais compatíveis de dispositivos. Implante o XenMobile no modo ENT (empresa) se você planejar usar os recursos do MDM+MAM do XenMobile. Por exemplo, se você desejar:

- Gerenciar um dispositivo emitido pela empresa por meio do MDM
- Implantar aplicativos e políticas de dispositivo
- Recuperar um inventário de ativos
- Apagar dispositivos
- Fornecer aplicativos móveis empresariais
- Bloquear aplicativos e apagar os dados nos dispositivos

No modelo de implantação recomendado, o XenMobile Server é posicionado no DMZ com um NetScaler Gateway na frente, o que oferece uma proteção adicional ao XenMobile.

XenMobile na rede interna: outra opção de implantação é posicionar um XenMobile Server local na rede interna, em vez de no DMZ. Essa implantação será usada se a sua política de segurança exigir que somente os dispositivos de rede possam ser colocados no DMZ. Nessa implantação, o XenMobile Server não está na DMZ. Portanto, não há a necessidade de abrir portas no firewall interno para permitir o acesso ao SQL Server e aos servidores PKI do DMZ.

Requisitos do sistema e compatibilidade

April 15, 2019

> Nota:
>
> Este artigo aborda os requisitos do sistema e a compatibilidade do XenMobile Server 10.9. Para os requisitos do sistema para o Endpoint Management, consulte Requisitos do sistema.

Para conhecer mais requisitos e informações sobre compatibilidade, consulte os seguintes artigos:

- Compatibilidade do XenMobile
- Sistemas operacionais compatíveis de dispositivos
- Requisitos de porta
- Escalabilidade

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Licenciamento
- Conformidade com FIPS 140-2
- Suporte a idiomas

Para executar o XenMobile 10.9, você precisa atender aos seguintes requisitos mínimos do sistema:

- Uma das seguintes opções:
  - XenServer (versões com suporte: 6.5.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6); para obter detalhes, consulte XenServer
  - VMware (versões com suporte: ESXi 5.5, ESXi 6.0, ESXi 6.5.0 ou ESXi 6.7); para obter detalhes, consulte VMware
  - Hyper-V (versões com suporte: Windows Server 2012 R2 ou Windows Server 2016); para obter detalhes, consulte Hyper-V
- Processador dual core
- Quatro CPUs virtuais
- 8 GB de RAM para ambientes de produção; 4 GB de RAM para implantações de prova de conceito e ambientes de teste
- 50 GB de espaço em disco
- Citrix License Server 11.15.x ou posterior

> Importante:
>
> 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 do site 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 no 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 **Outro Linux 2.6.x (64 bits)**.
>   d) Para armazenamento de dados, selecione **Padrão**.
>   e) Durante a personalização, remova o disco rígido padrão, o controlador USB e a unidade de CD/DVD.
>   f) Em Rede, como o tipo de adaptador, selecione **VMXNET3.**
>   g) No ESXi, se seus discos forem locais, selecione **Controller SCSI** e **LSI Logic Parallel**. Se você estiver usando um disco compartilhado, selecione **VMware Paravirtual**.
>   h) Clique em Avançar para concluir a criação da máquina virtual.
> 4. Navegue até o seu armazenamento de dados e copie o arquivo .vmdk que você carregou anteriormente. Copie-o para o diretório da máquina virtual que você criou para o XenMo-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

bile.
5. Na interface da Web do ESXi, selecione a máquina virtual e edite as configurações.
6. Clique em **Adicionar disco rígido**.
7. Selecione o arquivo .vmdk copiado anteriormente e anexe-o à máquina virtual.
8. Clique em **Salvar**.
9. Ligue a sua máquina virtual.

Requisitos do sistema do NetScaler Gateway

Para executar o NetScaler Gateway com o XenMobile 10.9, você precisa atender aos seguintes requisitos mínimos do sistema.

- NetScaler Gateway (no local). Versões com suporte: 11.1, 12.0, 12.1
- Você também precisa ser capaz de se comunicar com o Active Directory, o que requer uma conta de serviço. Você só precisa ter o acesso de consulta e leitura.

Requisitos de banco de dados do XenMobile 10.9

O XenMobile requer um dos seguintes bancos de dados:

- Microsoft SQL Server

  O repositório do XenMobile dá suporte a um banco de dados do Microsoft SQL Server em execução em uma das seguintes versões com suporte. Para obter mais informações sobre bancos de dados do Microsoft SQL Server, consulte Microsoft SQL Server:

  - Microsoft SQL Server 2017
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2014 SP2 (CU11)
  - Microsoft SQL Server 2012 SP4

  O XenMobile dá suporte a Grupos de disponibilidade básicos SQL (Grupos de disponibilidade Always On) e ao Clustering SQL para alta disponibilidade de banco de dados.

  A Citrix recomenda usar o Microsoft SQL remotamente.

  > Importante:
  >
  > Verifique se a conta de serviço do SQL Server a ser usada com o XenMobile tem a permissão de função DBcreator. Registre a senha da conta do SQL Server especificada 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.
  >
  > Para obter mais informações sobre as contas de serviço do SQL Server, consulte as páginas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> abaixo no site da Microsoft Developer Network. Esses links apontam para informações do SQL Server 2014. Se você estiver usando uma versão diferente, escolha sua versão do servidor na lista **Outras versões**:
>
> - Configuração do servidor - Contas de serviço
> - Configurar contas de serviço e permissões do Windows
> - Funções de nível de servidor

- PostgreSQL (apenas para ambientes de teste). PostgreSQL está incluído no XenMobile. Você pode usá-lo localmente ou remotamente em ambientes de teste. A migração de banco de dados não é compatível. Você não pode mover os bancos de dados criados em um ambiente de teste para um ambiente de produção.

  Todas as edições do XenMobile dão suporte ao Remote PostgreSQL 9.5.1 e 9.5.11 para Windows, com as seguintes limitações: não recomendado para ambientes de produção. Suporte para até 300 dispositivos Uso do SQL Server no local por mais de 300 dispositivos. Sem suporte para clusters.

Compatibilidade do StoreFront

- StoreFront 3.15
- StoreFront 3.12
- StoreFront 3.0.5000.1
- XenApp e XenDesktop 7.18
- XenApp e XenDesktop 7.15 LTSR CU3
- XenApp e XenDesktop 7.6 LTSR CU5

Outra compatibilidade

- XenMobile Mail Manager 10.1.5.11
  - Versões mais antigas não são testadas
- XenMobile NetScaler Connector 8.5.1.11
  - Versões mais antigas não são testadas

Compatibilidade do XenMobile

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Este artigo aborda a compatibilidade com o XenMobile Server 10.9. Para componentes testados com o Endpoint Management, consulte Compatibilidade do Endpoint Management.

Para usar novos recursos, correções e atualizações de políticas, a Citrix recomenda que você instale a versão mais recente do MDX Toolkit, do Secure Hub e dos aplicativos móveis de produtividade. Você pode usar o MDX Service em vez do MDX Toolkit. Para obter detalhes, consulte XenMobile MDX Service.

> Importante:
>
> Citrix dará suporte tanto para distribuição empresarial quanto a distribuição de loja de aplicativos pública de aplicativos de produtividade XenMobile até 31 de dezembro de 2017. Para obter detalhes, consulte o Citrix Product Matrix. Agora, os produtos Citrix dão suporte apenas à distribuição pela loja de aplicativos pública.

Este artigo resume as versões dos componentes do XenMobile com suporte que você pode integrar.

Versões com suporte e caminhos de atualização

As versões mais recentes do Secure Hub, do MDX Toolkit e dos aplicativos móveis de produtividade são compatíveis com a versão mais recente, além das duas versões anteriores do XenMobile Server.

A versão mais recente dos aplicativos móveis de produtividade requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente.

XenMobile Server (no local)

- A Citrix oferece suporte a atualizações das duas últimas versões do XenMobile Server.
- Última versão do XenMobile Server:
  - XenMobile Server 10.9
- Atualizar de:
  - XenMobile Server 10.8.x
  - XenMobile Server 10.7.x

MDX Toolkit

- A Citrix oferece suporte para as três versões mais recentes (n.n.n) do MDX Toolkit.
- A versão mais recente do toolkit é MDX Toolkit 10.8.60 (para iOS e Android) para preparar aplicativos de terceiros. Você pode atualizar do MDX Toolkit 10.8.35. e 10.8.5 para o MDX Toolkit 10.8.60.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Você também pode usar o XenMobile MDX Service para preparar aplicativos. Para obter detalhes, consulte XenMobile MDX Service.

Aplicativos móveis de produtividade de lojas de aplicativos públicas

- A Citrix oferece suporte a atualizações das duas últimas versões.
  - Os usuários que têm atualizações automáticas ativadas recebem a versão mais recente da loja de aplicativos
  - O aplicativo mais recente é compatível com os dois arquivos MDX anteriores.
- Versões mais recentes de Secure Hub, Secure Mail e Secure Web para Android:
  - 10.8.60
  - 10.8.55
  - 10.8.50
- Versões mais recentes do Secure Hub, Secure Mail e Secure Web para iOS:
  - 10.8.60
  - 10.8.55
  - 10.8.50

> Nota:
>
> Os usuários acessam o ShareFile para XenMobile nas lojas de aplicativos públicas após a versão 6.5.

Suporte a navegadores

O XenMobile 10.9 é compatível com os seguintes navegadores:

- Internet Explorer, mas não as versões 9 ou anteriores
- Chrome
- Firefox
- Safari em dispositivos móveis para uso com o Portal de autoatendimento

O XenMobile 10.9 é compatível com a versão mais recente do navegador e com uma versão anterior à atual.

Sistemas operacionais compatíveis de dispositivos

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Este artigo aborda os sistemas operacionais de dispositivos compatíveis com o XenMobile Server 10.9. Para sistemas operacionais compatíveis com o Endpoint Management, consulte Sistemas operacionais compatíveis de dispositivos.

O XenMobile é compatível com dispositivos que executam as seguintes plataformas e sistemas operacionais para gerenciamento de mobilidade corporativa, incluindo gerenciamento de aplicativos e dispositivos. Devido a restrições de plataforma e recursos de segurança, o XenMobile não dá suporte a todas as funcionalidades em todas as plataformas.

As informações de plataforma de dispositivo com suporte neste artigo também se aplicam ao conector do XenMobile para Exchange ActiveSync e ao conector Citrix Gateway para Exchange ActiveSync.

> Nota:
>
> A Citrix dá suporte pelo menos à versão atual e anterior de cada principal plataforma de sistema operacional. Nem todos os recursos da versão mais recente do XenMobile funcionam em versões de plataformas mais antigas.

Lista de compatibilidade com o sistema operacional

O Citrix XenMobile suporta os seguintes sistemas operacionais:

- **Android:** 6.x, 7.x, 8.x, 9.x

  > Nota:
  >
  > O suporte para Android 5.x termina em 31 de dezembro de 2018.

- **iOS:** 11.x, 12.x
- **macOS:** 10.11 El Capitan, 10.12 Sierra, 10.13 High Sierra
- **Desktops e tablets Windows 10:** Windows 10 RS4 e RS5 (somente MDM)
- **Windows Phone:** Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 e RS5 (somente MDM)
- **Windows Mobile/CE:** (somente MDM). A partir do segundo trimestre de 2018, o suporte para dispositivos Windows Mobile/CE não está mais disponível para novos clientes.
- **Dispositivos Symbian:** A partir do segundo trimestre de 2018, o suporte para dispositivos Symbian não está mais disponível para novos clientes. A lista a seguir inclui alguns dos dispositivos Symbian suportados pelo XenMobile para clientes que configuraram esses dispositivos anteriormente.
  - Symbian 3

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Symbian S60 5th Edition
  - Symbian S60 3rd Edition, Pacote de recursos 2
  - Symbian S60 3rd Edition, Pacote de recursos 1
  - Symbian S60 3rd Edition
  - Symbian S60 2nd Edition, Pacote de recursos 3
  - Symbian S60 2nd Edition, Pacote de recursos 2

- **Samsung SAFE e KNOX:** Em dispositivos Samsung compatíveis, o XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung KNOX e as estende. O XenMobile requer que você habilite as APIs SAFE antes de implantar políticas e restrições SAFE. Para fazer isso, implante a chave interna Samsung Enterprise License Management (ELM) em um dispositivo. Para ativar a API Samsung KNOX:

  1. Compre uma licença do Samsung KNOX usando o Samsung KNOX License Management System (KLMS).
  2. Implante a chave Samsung ELM.

- **HTC:** Para políticas específicas da HTC, HTC API versão 0.5.0
- **Sony:** Para políticas específicas da Sony, Sony Enterprise SDK 2.0

Considerações sobre Android

Antes de atualizar para a plataforma Android P: Certifique-se de que sua infraestrutura de servidor está em conformidade com os certificados de segurança que tenham um nome de host correspondente na extensão subjectAltName (SAN). Para confirmar um nome de host, o servidor deve apresentar um certificado com uma SAN correspondente. Os certificados que não contêm uma SAN correspondente ao nome do host não são mais confiáveis. Para obter detalhes, consulte o artigo do site do desenvolvedor do Android em Android P behavior changes.

Com o lançamento do Android O (versão 8):

- O SSLv3 não é suportado com o Android O. O Google não suporta mais conexões SSLv3. Isso significa que aplicativos móveis de produtividade executados em dispositivos Android O não podem se conectar a servidores internos que estão usando conexões SSLv3. Se você tiver servidores que utilizam o SSLv3, é importante resolver essas limitações antes de implantar o Android O para evitar falhas de conectividade com os usuários.
- O suporte terminou para o Android 4.4x a partir da versão 10.6.20 da versão da loja de aplicativos pública dos aplicativos móveis de produtividade da Citrix.
- Aplicativos móveis de produtividade da Citrix e aplicativos preparados com MDX estão disponíveis em dispositivos Android com processadores baseados em ARM. Eles não são suportados em dispositivos Android com base em Intel x86 ou x64.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Considerações do iOS

Com o lançamento do iOS 11:

- O suporte a XenMobile para dispositivos iOS 8 terminou.
- O suporte a XenMobile para dispositivos iOS 9 que executam aplicativos móveis de produtividade da Citrix terminou em 31 de outubro de 2017.

Alguns dispositivos iOS aos quais o XenMobile oferece suporte:

- iPhone X
- iPhone 8, 8 Plus
- iPhone 7 Plus 10.2.1
- iPhone 6, 6 Plus, 6S Plus, 6S+, 5s
- iPhone 5, 5c (somente iOS 9.x)

BlackBerry

O gerenciamento de dispositivos BlackBerry é fornecido por meio do conector de XenMobile para Exchange ActiveSync. Para obter detalhes, consulte Conector do XenMobile para Exchange ActiveSync.

Requisitos de porta

April 15, 2019

Para ativar a comunicação dos dispositivos e dos aplicativos com o XenMobile, você abre portas específicas nos seus firewalls. As tabelas a seguir listam as portas que devem estar abertas.

Abrir portas para o NetScaler Gateway e o XenMobile gerenciarem aplicativos

Abra as seguintes portas para permitir conexões de usuário do Citrix Secure Hub, do Citrix Receiver e do NetScaler Gateway Plug-in por meio do NetScaler Gateway com os seguintes componentes:

- XenMobile
- StoreFront
- XenDesktop
- Conector Citrix Gateway para Exchange ActiveSync
- Outros recursos da rede internos, como sites da intranet

Para ativar o tráfego para iniciar Darkly do NetScaler, você pode usar os endereços IP anotados neste artigo do Support Knowledge Center.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para obter mais informações sobre o NetScaler Gateway, consulte a documentação do NetScaler Gateway. Essa documentação contém informações sobre os endereços IP do NetScaler (NSIP), IP de servidor virtual (VIP) e IP de sub-rede (SNIP).

Porta TCP	Descrição	Origem	Destino
21 ou 22	Usada para enviar pacotes de suporte para um servidor FTP ou SCP.	XenMobile	Servidor FTP ou SCP
53 (TCP e UDP)	Usada para conexões DNS.	NetScaler Gateway, XenMobile	Servidor DNS
80	O NetScaler Gateway transmite a conexão VPN para o recurso da rede interna por meio do segundo firewall. Geralmente, essa sitiuação ocorre quando os usuários fazem login com o NetScaler Gateway Plug-in.	NetScaler Gateway	Sites da Intranet
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 do StoreFront e Web Interface XML; NetScaler Gateway STA	XenDesktop e XenApp
123 (TCP e UDP)	Usada para os serviços do protocolo NTP.	NetScaler Gateway; XenMobile	Servidor NTP
389	Usada para conexões LDAP não seguras	NetScaler Gateway; XenMobile	Servidor de autenticação LDAP ou do Microsoft Active Directory

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
443	Usada para conexões com o StoreFront do Citrix Receiver ou com Receiver para Web para XenApp e XenDesktop.	Internet	NetScaler Gateway
443	Usada para conexões com o XenMobile para entrega Web, móvel e de aplicativo SaaS.	Internet	NetScaler Gateway
443	Usada para comunicação geral de dispositivo com o XenMobile Server	XenMobile	XenMobile
443	Usada para conexões de dispositivos móveis com o XenMobile para registro.	Internet	XenMobile
443	Usado para conexões do XenMobile ao conector Citrix Gateway para Exchange ActiveSync.	XenMobile	Conector Citrix Gateway para Exchange ActiveSync
443	Usado para conexões do conector Citrix Gateway do Exchange ActiveSync ao XenMobile.	Conector Citrix Gateway para Exchange ActiveSync	XenMobile
443	Usado para URL de retorno de chamada em implantações sem autenticação de certificado.	XenMobile	NetScaler Gateway

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
514	Usada para conexões entre o XenMobile e um servidor syslog.	XenMobile	Servidor Syslog
636	Usada para conexões LDAP seguras.	NetScaler Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory
1494	Usada para conexões ICA com aplicativos baseados em Windows na rede interna. A Citrix recomenda manter essa porta aberta.	NetScaler Gateway	XenApp ou XenDesktop
1812	Usada para conexões RADIUS.	NetScaler Gateway	Servidor de autenticação RADIUS
2598	Usada para conexões com aplicativos baseados em Windows na rede interna usando confiabilidade de sessão. A Citrix recomenda manter essa porta aberta.	NetScaler Gateway	XenApp ou XenDesktop
3268	Usada para conexões LDAP inseguras do Microsoft Global Catalog.	NetScaler Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory
3269	Usada para conexões LDAP seguras do Microsoft Global Catalog.	NetScaler Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
9080	Usado para tráfego HTTP entre o NetScaler e o conector Citrix Gateway para Exchange ActiveSync.	NetScaler	Conector Citrix Gateway para Exchange ActiveSync
30001	API de gerenciamento para preparação inicial do serviço HTTPS	LAN interna	Servidor XenMobile
9443	Usado para tráfego HTTPS entre o NetScaler e o conector Citrix Gateway para Exchange ActiveSync.	NetScaler	Conector Citrix Gateway para Exchange ActiveSync
45000; 80	Usada para comunicação entre duas VMs do XenMobile quando implantadas em um cluster. A porta 80 é para comunicação entre nós e para descarga de SSL.	XenMobile	XenMobile
8443	Usada para registro, XenMobile Store e gerenciamento de aplicativo móvel (MAM).	XenMobile; NetScaler Gateway; Dispositivos; Internet	XenMobile

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
4443	Usada para acesso ao console XenMobile por um administrador usando o navegador. Usada também para baixar logs e pacotes de suporte para todos os nós de cluster do XenMobile a partir de um nó.	Ponto de acesso (navegador); XenMobile	XenMobile
27000	Porta padrão usada para acessar o Citrix License Server externo.	XenMobile	Citrix License Server
7279	Porta padrão usada para fazer check-in e check-out das licenças da Citrix.	XenMobile	Citrix Vendor Daemon
161	Usada para tráfego SNMP usando o protocolo UDP.	SNMP Manager	XenMobile
162	Usada para enviar alertas de interceptação SNMP ao SNMP Manager do XenMobile. A origem é XenMobile e o destino é SNMP Manager.	XenMobile	SNMP Manager

Abrir portas do XenMobile para gerenciar dispositivos

Abra as seguintes portas para permitir que o XenMobile se comunique na sua rede.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
25	Porta SMTP padrão do serviço de notificação do XenMobile. Se o seu servidor SMTP usar uma porta diferente, verifique se o firewall bloqueia essa porta.	XenMobile	Servidor SMTP
80 e 443	Conexão da Loja de Aplicativos da Empresa com Apple iTunes App Store, Google Play (deve usar a porta 80) ou Windows Phone Store. Usada para o Apple Volume Purchase Program. Usada para publicar aplicativos das lojas de aplicativos usando o Citrix Mobile Self-Serve no iOS, o Secure Hub para Android ou o Secure Hub para Windows Phone.	XenMobile	`ax.itunes.apple.com` e `*.mzstatic.com`; `vpp.itunes.apple.com`; `login.live.com`; `*.notify.windows.com`; `play.google.com`, `android.clients.google.com`, `android.l.google.com`
80 ou 443	Usada para conexões de saída entre o XenMobile e o Nexmo SMS Notification Relay.	XenMobile	Nexmo SMS Relay Server
389	Usada para conexões LDAP inseguras.	XenMobile	Servidor de autenticação LDAP ou do Active Directory

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
443	Usada para registro e instalação do agente para Android e Windows Mobile.	Internet	XenMobile
443	Usada para registro e instalação do agente para dispositivos Android e Windows, o console Web XenMobile e o Cliente de Suporte Remoto do MDM.	Internet LAN e Wi-Fi	XenMobile
1433	Usada como padrão para conexões com um servidor do banco de dados remoto (opcional).	XenMobile	Servidor SQL
2195	Usada para as conexões de saída do serviço Apple Push Notification (APNs) com `gateway.push.apple.com` para notificações de dispositivo e envio por push da política de dispositivo iOS.	XenMobile	Internet (hosts APN que usam o endereço IP público 17.0.0.0/8)
2196	Usada para conexões de saída de APNs com `feedback.push.apple.com` para notificação de dispositivo e envio por push da política de dispositivo iOS.		

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Porta TCP	Descrição	Origem	Destino
5223	Usada para conexões de saída de APNs de dispositivos iOS em redes WiFi com `*.push.apple.com`.	Dispositivos iOS em redes WiFi	Internet (hosts APN que usam o endereço IP público 17.0.0.0/8)
8081	Usada para túneis de aplicativo do Cliente de Suporte Remoto do MDM opcional. Usa o padrão 8081.	Cliente de suporte remoto	XenMobile
8443	Usada para registro de dispositivos iOS e Windows Phone.	Internet: LAN e Wi-Fi	XenMobile

Requisito de porta para conectividade do Auto Discovery Service

Essa configuração de porta garante que os dispositivos Android que se conectam do Secure Hub para Android possam acessar o Citrix Auto Discovery Service (ADS) na rede interna. A capacidade de acessar o ADS é importante ao baixar qualquer atualização de segurança disponibilizada por meio do ADS.

> Nota:
>
> As conexões do ADS podem não dar suporte ao seu servidor proxy. Nesse cenário, permita que a conexão do ADS ignore o servidor proxy.

Se quiser permitir a fixação de certificado, oss seguintes pré-requisitos devem ser atendidos:

- **Coletar certificados de XenMobile Server e NetScaler.** Os certificados precisam estar no formato PEM e devem ser um certificado público e não a chave privada.
- **Entre em contato com a Citrix Support e faça uma solicitação para permitir a fixação de certificado.** Durante este processo, você será solicitado a fornecer seus certificados.

A fixação de certificado requer 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 ao Secure Hub para o ambiente no qual o dispositivo está se registrando. Para que o Secure Hub registre um dispositivo, o dispositivo deve atingir o ADS. Portanto, a abertura do acesso ao ADS na rede interna é essencial para possibilitar que os dispositivos sejam registrados.

Para permitir o acesso ao ADS para o Secure Hub para Android, abra a porta 443 para os seguintes endereços IP e FQDN:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

FQDN	Endereço IP	Porta	Uso de IP e porta
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS Communication

> Nota:
>
> Para versões do Secure Hub anteriores a 10.6.15, o FQDN é discovery.mdm.zenprise.com. Abra a porta 443 para os endereços IP 52.5.138.94 e 52.1.30.122.

Escalabilidade e desempenho

April 15, 2019

Entender a escala da sua infraestrutura do XenMobile desempenha um papel importante em como você decide implantar e configurar o XenMobile. Este artigo contém dados de testes de escalabilidade e orientação sobre como determinar requisitos de infraestrutura para desempenho e escalabilidade para implantações locais empresariais do XenMobile de pequena a larga escala.

A escalabilidade é definida aqui em termos da capacidade dos dispositivos já registrados na implantação de se reconectar à implantação ao mesmo tempo.

- A *Escalabilidade* é definida como o número máximo de dispositivos registrados na implantação.
- *Taxa de Login* é definida como a taxa máxima com que os dispositivos existentes podem se reconectar à implantação.

Os dados contidos neste artigo são derivados de testes nas implantações com tamanhos que vão de 10.000 a 75.000 dispositivos. Os testes abrangeram dispositivos móveis que usavam cargas de trabalho.

Todos os testes foram realizados com o XenMobile Enterprise Edition.

Os testes foram realizados usando o NetScaler Gateway 8200. Do dispositivo NetScaler com capacidade semelhante ou superior pode-se esperar que produza escalabilidade semelhante ou maior.

Segue um resumo dos resultados dos testes de escalabilidade.

Resumo dos resultados do teste de escalabilidade para implantações de até 75.000 dispositivos

Taxa de login (taxa de reconexão de usuários existentes) - Até 9.375 dispositivos por hora

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração usada:

- NetScaler Gateway
- MPX 8200
- XenMobile Enterprise Edition
- Cluster de 7 nós do XenMobile Server
- Banco de dados: banco de dados Microsoft SQL Server externo

Os resultados de teste por população de dispositivos e configuração de hardware

Número de dispositivos em operação	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 – cluster	N/D	3	5	7
XenMobile Server – dispositivo virtual	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 6	Memória = 24 GB de RAM; vCPUs = 8	Memória = 24 GB de RAM; vCPUs = 8
Active Directory	Memória = 4 GB de RAM; vCPUs = 2	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 4
Banco de dados Microsoft SQL Server externo	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 8	Memória = 24 GB de RAM; vCPUs = 16	Memória = 24 GB de RAM; vCPUs = 16

Perfil de escalabilidade

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração do Active Directory	Perfil usado
Usuários	100.000
Grupos	200.000
Níveis de aninhamento	5

Configuração do XenMobile Server	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	
Grupos do Active Directory por grupo de entrega	10	
SQL		
Número de bancos de dados	1	

Conexões de dispositivos e atividades de aplicativo

Estes testes de escalabilidade coletaram dados sobre a capacidade de dispositivos registrados em uma implantação para reconectar por um período de oito horas.

Os testes simularam um intervalo de reconexão durante o qual os dispositivos que estão sendo reconectados obtêm todas as políticas de segurança autorizadas, fazendo com que os nós do XenMobile Server fiquem sujeitos a condições de carga mais altas do que o normal. Durante as reconexões subsequentes, somente as políticas alteradas ou novas são enviadas para dispositivos iOS, diminuindo a carga nos nós do XenMobile Server.

Estes testes usaram uma mistura de 50% dispositivos iOS e 50% dispositivos Android.

Nesses testes, presume-se que os dispositivos Android que se reconectam receberam notificações GCM prévias.

Durante o intervalo de teste de 8 horas, ocorreram as seguintes atividades relativas a aplicativos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- O Secure Hub foi aberto uma vez para enumerar os aplicativos com direito
- 2 aplicativos Web SAML foram abertos
- 4 aplicativos MAM foram baixados
- 1 STA foi gerada para uso pelo Secure Mail
- 240 validações de ticket STA, uma para cada evento de Secure Mail reconectado através de uma micro VPN, foram executadas.

Arquitetura de referência

Para obter a arquitetura de referência para implantações usadas nesses testes de escalabilidade, consulte “Core MAM+MDM Reference Architecture” em Arquitetura de referência para implantações locais.

Restrições e limitações

Observe o seguinte ao considerar os resultados do teste de escalabilidade neste artigo:

- A plataforma Windows não foi testada.
- O envio por push de política foi testado para dispositivos iOS e Android.
- Cada nó do XenMobile Server é compatível com um máximo de 12.000 dispositivos simultaneamente.

Licenciamento

April 15, 2019

O XenMobile usa o Citrix Licensing para gerenciar licenças. O XenMobile Server e o NetScaler Gateway requerem licenças.

Para obter mais informações sobre o licenciamento de NetScaler Gateway, consulte a documentação do NetScaler Gateway. Para obter mais informações sobre o Citrix Licensing, consulte O sistema Citrix Licensing.

Quando você adquire o XenMobile Server, recebe uma mensagem de email de confirmação de pedido que contém instruções para a ativação das suas licenças. Os novos clientes devem se registrar em um programa de licença antes de fazer um pedido. Para obter mais informações sobre os programas e os modelos de licenciamento do XenMobile, consulte Licenciamento do XenMobile.

Para obter uma ficha técnica do XenMobile que mostra os recursos disponíveis em cada edição do XenMobile, consulte este PDF.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos

- Atualize o seu Citrix License Server para 11.15.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.9. Versões mais antigas de servidor de licenças não são compatíveis com a versão mais recente do XenMobile.
- Você deve instalar o Citrix Licensing antes de baixar as suas licenças do XenMobile. O nome do servidor no qual você instalou o Citrix Licensing é necessário para gerar o arquivo de licença. Quando você instala o XenMobile, o Citrix Licensing é instalado no servidor por padrão. Como alternativa, você pode usar uma implantação existente do Citrix Licensing para gerenciar as suas licenças do XenMobile. Para obter mais informações sobre como instalar, implantar e gerenciar o Citrix Licensing, consulte Como Licenciar o seu Produto.
- Se você pretende usar nós de cluster ou instâncias do XenMobile, terá de usar o Citrix Licensing em um servidor remoto.
- A Citrix recomenda que você mantenha cópias locais de todos os arquivos de licença que receber. Quando você salva uma cópia de backup do arquivo de configuração, todos os arquivos de licença são incluídos nesse backup. Se, no entanto, você reinstalar o XenMobile sem primeiro fazer backup do arquivo de configuração, precisará dos arquivos de licença originais.

Considerações sobre o licenciamento do XenMobile

Na ausência de uma licença, o XenMobile funciona com todos os recursos no modo de avaliação por um período de tolerância de 30 dias. Esse modo de avaliação pode ser usado somente uma vez, e o período de 30 dias é iniciado quando você instala o XenMobile. O acesso ao console da Web XenMobile nunca é bloqueado, quer uma licença válida do XenMobile esteja disponível ou não. No console XenMobile, você pode ver quantos dias restam do período de avaliação.

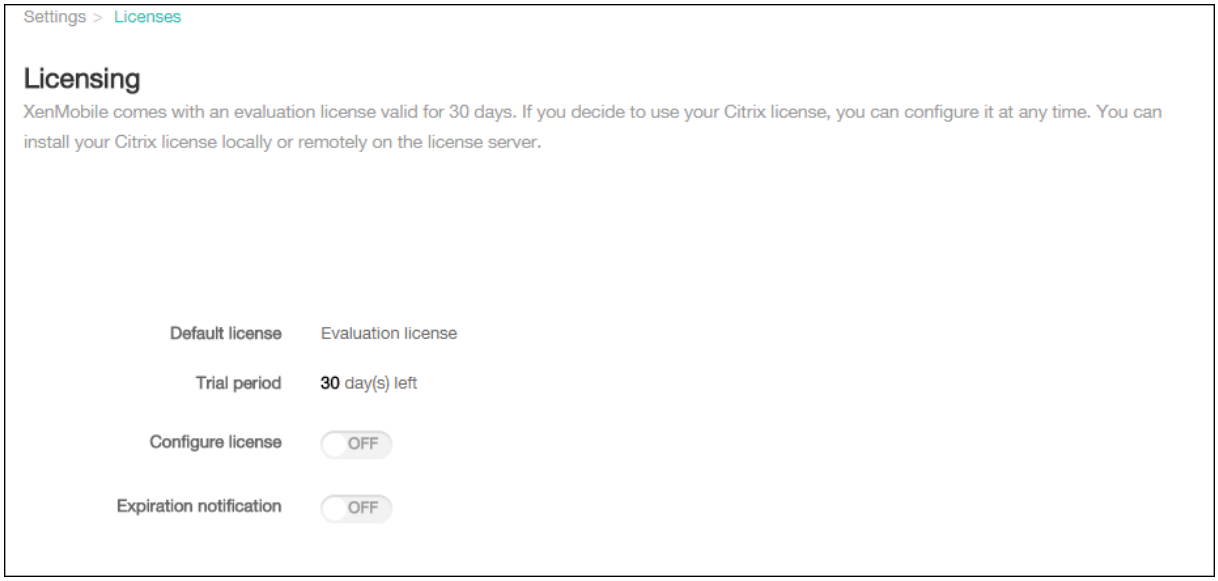
Embora o XenMobile permita que você carregue várias licenças, somente uma licença pode ser ativada por vez.

Quando uma licença do XenMobile expira, você não pode mais executar qualquer função de gerenciamento de dispositivo. 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 os programas e os modelos de licenciamento do XenMobile, consulte Licenciamento do XenMobile.

Para localizar a página Licenciamento no console XenMobile

Quando a página **Licenciamento** é exibida pela primeira vez depois que você instala o XenMobile, a licença é definida para o modo de avaliação de 30 dias padrão e ainda não está configurada. Você pode adicionar e configurar licenças nessa página.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Licenciamento**. A página **Licenciamento** é exibida.

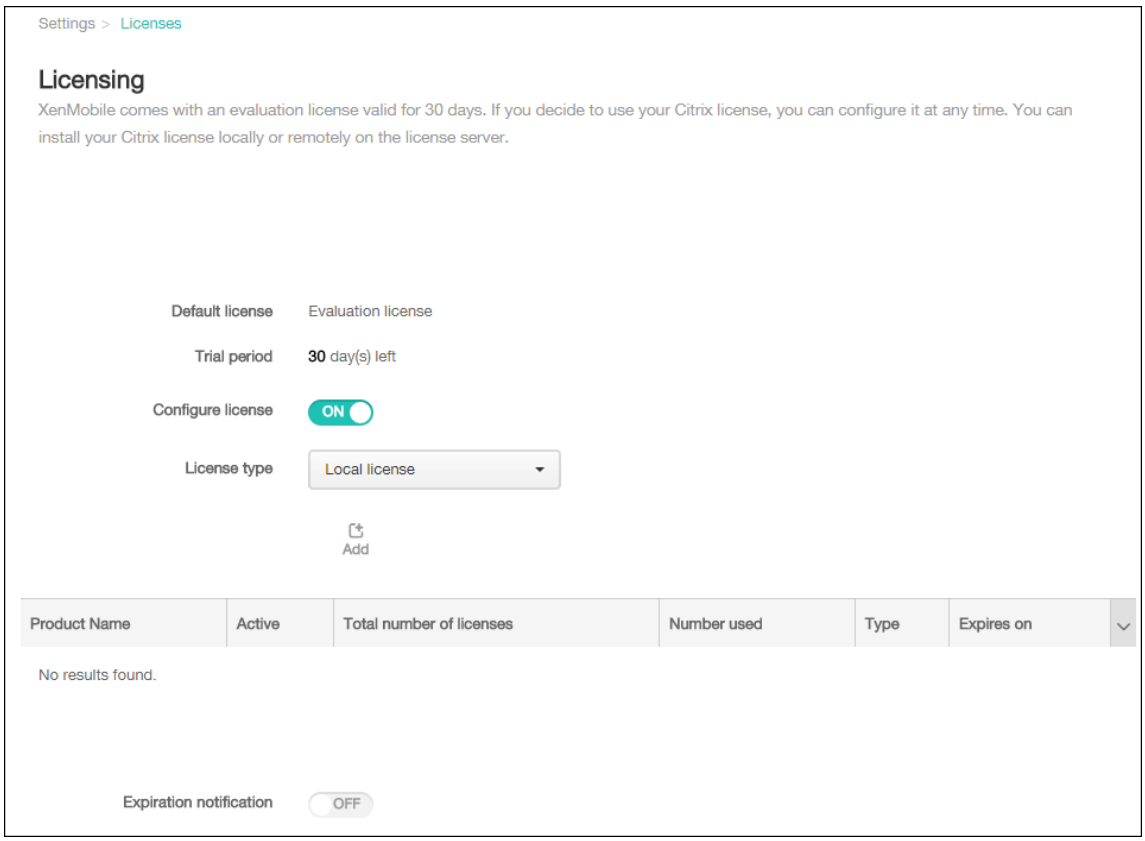
Para adicionar uma licença local

Quando você adiciona novas licenças, elas são exibidas na tabela. A primeira licença adicionada é ativada automaticamente. Se você adicionar várias licenças da mesma categoria, como Empresa, e tipo, essas licenças aparecem em uma única linha da tabela. Nesses casos, o **Número total de licenças** e o **Número usado** refletem a quantidade combinada das licenças comuns. A data **Expira em** mostra a data de expiração mais recente entre as licenças comuns.

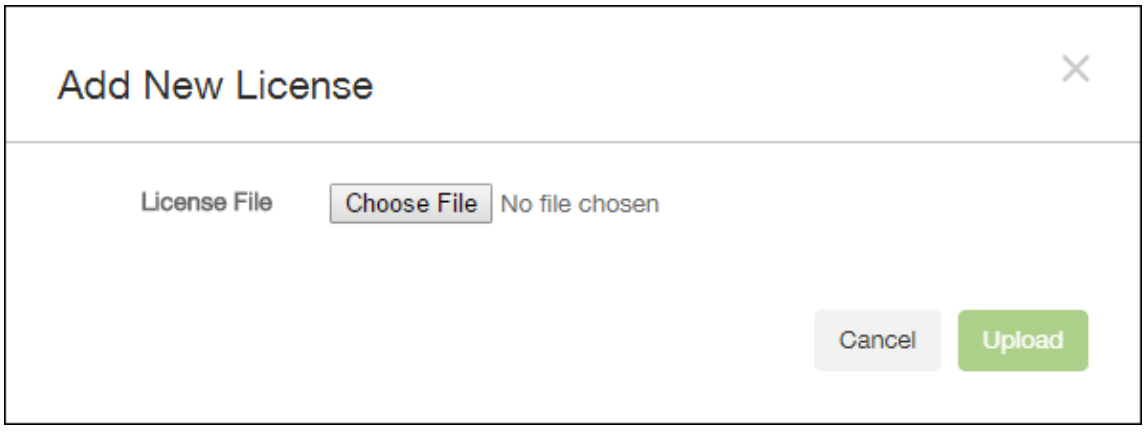
Gerencie todas as licenças locais usando o console XenMobile.

1. Obtenha um arquivo de licença do Simple License Service por meio do License Administration Console ou diretamente da sua conta em Citrix.com. Para obter detalhes, consulte a documentação do Citrix Licensing.
2. No console 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 **Ativada**. Aparecem a lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento**. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não tiver adicionado uma licença Citrix ainda, a tabela estará vazia.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

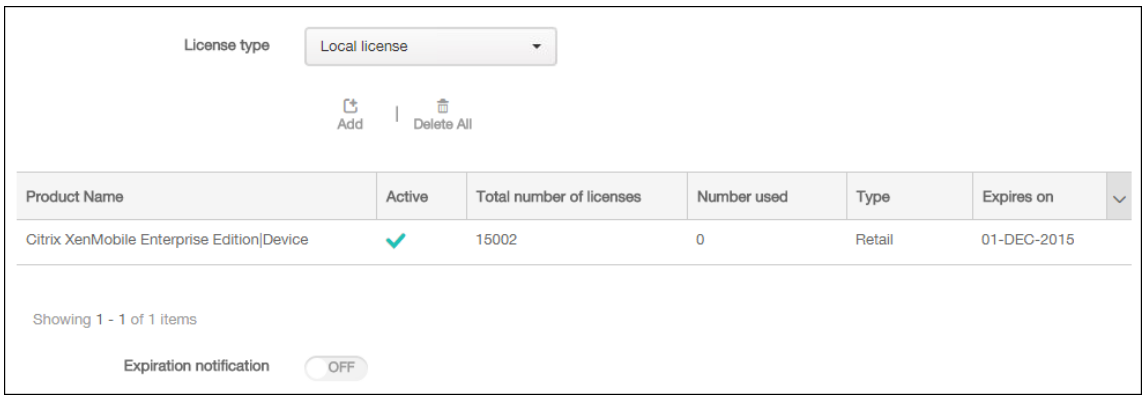


5. Verifique se **Tipo de licença** está definido como **Licença local** e clique em **Adicionar**. A caixa de diálogo **Adicionar nova licença** é exibida.



6. Na caixa de diálogo **Adicionar nova licença**, clique em **Escolher arquivo** e navegue até a localização do seu arquivo de licença.
7. Clique em **Carregar**. A licença é carregada localmente e é exibida na tabela.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



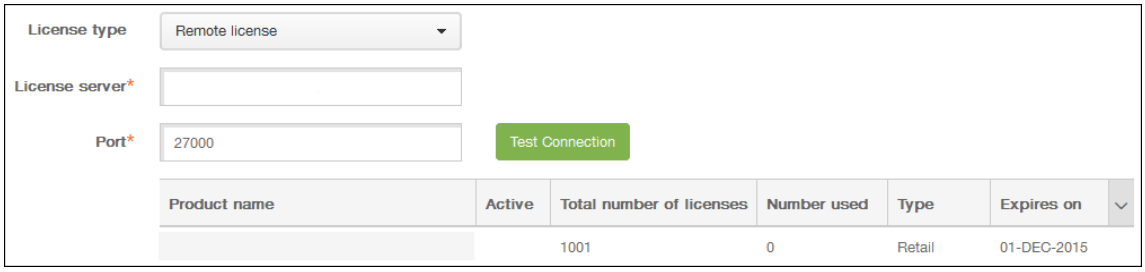
8. Quando a licença for exibida na tabela na página **Licenciamento**, ative-a. Se for a primeira licença na tabela, essa licença será ativada automaticamente.

Para adicionar uma licença remota

Se você estiver usando o servidor Citrix Licensing remoto, use-o para gerenciar *todas* as atividades de licenciamento. Para obter detalhes, consulte Como Licenciar o seu Produto.

1. Importe o certificado do servidor de licença para o XenMobile Server (**Configurações > Certificados**).
2. Por padrão, a verificação do nome do host está ativada nas 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**.

   Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar com o servidor VPP: o nome de host ‘192.0.2.0’ não corresponde à entidade do certificado fornecida pelo par correspondente”
3. Na página **Licenciamento**, defina **Configurar licença** como **Ativada**. Aparecem a lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento**. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não tiver adicionado uma licença Citrix ainda, a tabela estará vazia.
4. Defina **Tipo de licença** como **Licença remota**. Os campos **Servidor de licença** e **Porta** e o botão **Testar conexão** substituem o botão **Adicionar**.



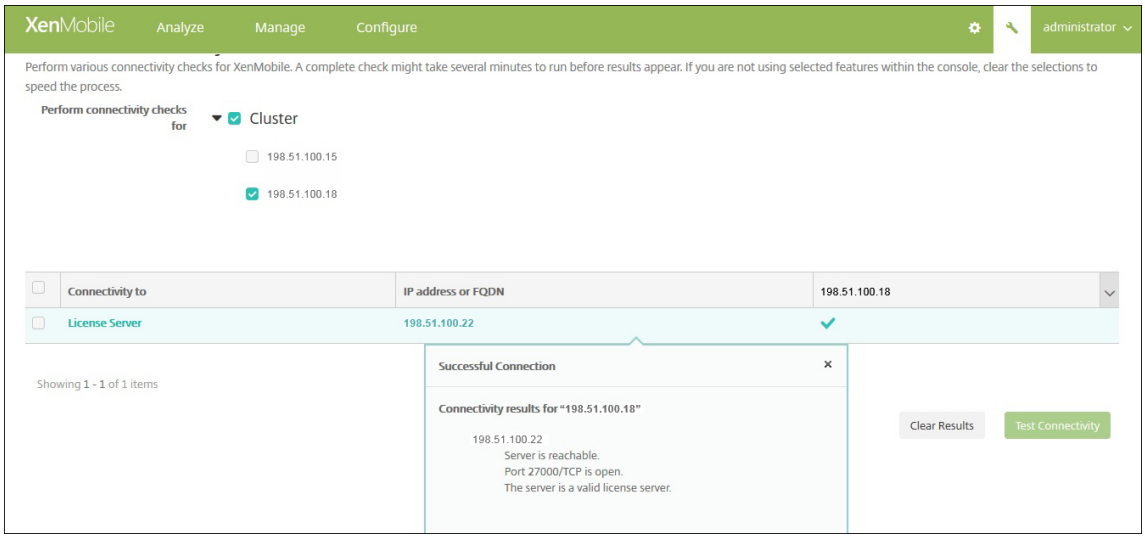
© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Defina estas configurações:
   - **Servidor de licenças:** digite o endereço IP ou nome de domínio totalmente qualificado (FQDN) do seu servidor remoto de licenciamento.
   - **Porta:** aceite a porta padrão ou digite o número da porta usada para comunicação com o servidor de licenciamento.
6. Clique em **Testar conexão**. Se a conexão for bem-sucedida, o XenMobile se conectar com o servidor de Licenciamento e a tabela Licenciamento é preenchida com licenças disponíveis. Se houver apenas uma licença, essa será ativada automaticamente.

   Quando você clica em **Testar conexão**, o XenMobile confirma o seguinte:

   - Que o XenMobile consegue se comunicar com o servidor de licenças.
   - Que as licenças no servidor de licenças são válidas.
   - Que 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**.

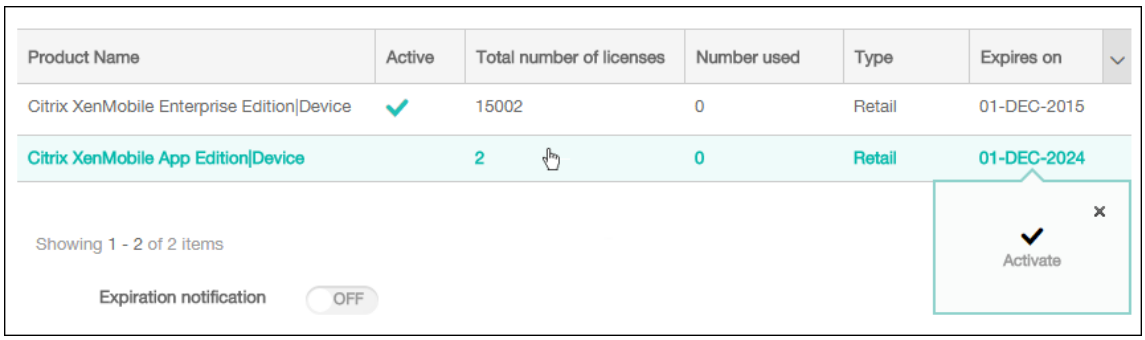


Para ativar uma licença diferente

Se você tiver várias licenças, poderá escolher a licença que desejar ativar. No entanto, somente uma licença pode estar ativa por vez.

1. Na página **Licenciamento**, na tabela **Licenciamento**, clique na linha da licença que você desejar ativar. Uma janela de confirmação **Ativar** é exibida ao lado da linha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



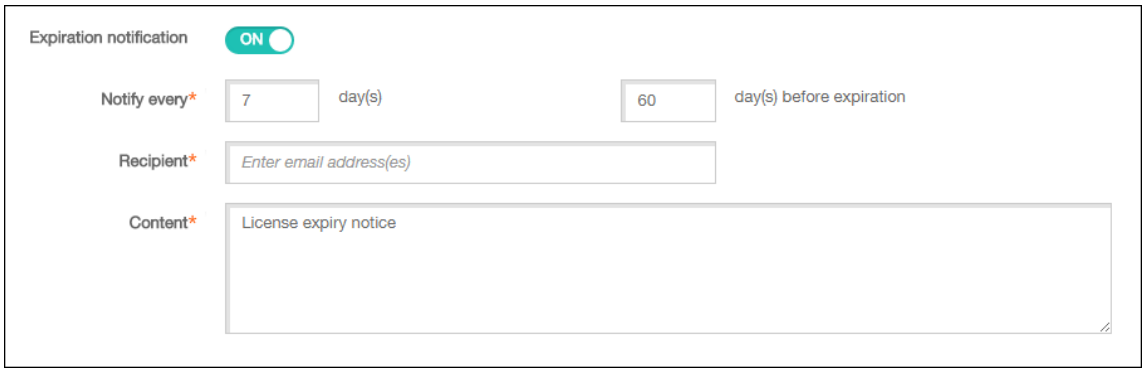
2. Clique em **Ativar**. A caixa de diálogo **Ativar** é exibida.
3. Clique em **Ativar**. A licença selecionada é ativada.

> Importante:
>
> Se você ativar a licença selecionada, a licença ativa no momento será desativada.

Para automatizar uma notificação de expiração

Depois de ativar licenças locais ou remotas, você poderá configurar o XenMobile para notificar você ou uma pessoa designada quando a data de expiração da licença estiver próxima.

1. Na página **Licenciamento**, defina **Notificação de expiração** como **Ativada**. Novos campos relacionados a notificação são exibidos.



2. Defina estas configurações:
   - **Notificar a cada:** digite:
   - A frequência com a qual as notificações são enviadas, como a cada **7** dias.
   - Quando começar a enviar notificações, como 60 dias antes da expiração da licença.
   - **Destinatário:** digite o seu endereço de email ou o endereço de email da pessoa responsável pela licença.
   - **Conteúdo:** digite uma mensagem de notificação de expiração que o destinatário verá na notificação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Clique em **Salvar**. Com base nas suas configurações, o XenMobile começa a enviar mensagens de email que contêm o texto que você digitou em **Conteúdo** ao destinatário inserido em **Destinatário**. As notificações são enviadas com a frequência que você definir.

Conformidade com FIPS 140-2

March 6, 2019

O Federal Information Processing Standard (FIPS), emitido pelo US National Institute of Standards and Technologies (NIST). O FIPS especifica os requisitos de segurança para módulos criptográficos usados em sistemas de segurança. 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 ativar o modo FIPS do XenMobile somente durante a instalação inicial.
> - O gerenciamento somente de dispositivo móvel do XenMobile, o gerenciamento somente de aplicativo móvel do XenMobile e o XenMobile MDM+MAM são compatíveis com FIPS, desde que nenhum aplicativo HDX seja usado.

Todas as operações de criptografia de dados em repouso e dados em trânsito no iOS usam módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL e pela Apple. No Android, todas as operações de criptografia de dados em repouso e de dados em trânsito do dispositivo móvel para o NetScaler Gateway usam módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL.

Todas as operações de criptografia de dados em repouso e dados em trânsito para Gerenciamento de dispositivo móvel (MDM) em dispositivos Windows com suporte usam módulos criptográficos certificados pelo FIPS e fornecidos pela Microsoft.

Todas as operações de criptografia de dados em repouso e dados em trânsito no XenMobile MDM usam módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL. 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 acima para dispositivos móveis, além das operações criptográficas entre dispositivos móveis e o NetScaler Gateway.

Todas as operações de criptografia de dados em trânsito entre os dispositivos móveis iOS, Android e Windows e o NetScaler Gateway usam módulos criptográficos certificados pelo FIPS. O XenMobile usa um dispositivo NetScaler FIPS Edition hospedado no DMZ, equipado com um módulo FIPS certificado para proteger esses dados. Para obter mais informações, consulte a documentação do FIPS do NetScaler.

O MDX Vault criptografa os aplicativos preparados pelo MDX e os dados em repouso associados em dispositivos iOS e Android usando módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para obter a declaração de conformidade completa com o FIPS 140-2 do XenMobile, incluindo os módulos específicos usados em cada caso, contate o seu representante da Citrix.

Suporte a idiomas

October 4, 2018

Os aplicativos móveis de produtividade e o console XenMobile são adaptados para o uso em idiomas além do inglês. O suporte inclui caracteres e entradas de teclado de idiomas além do inglês, mesmo quando o aplicativo não está localizado no idioma preferencial dos usuários. Para obter mais informações sobre suporte à globalização de todos os produtos Citrix, consulte https://support.citrix.com/article/CTX119253.

Este artigo lista os idiomas com suporte na versão mais recente do XenMobile.

Console XenMobile e portal de autoajuda

- Francês
- Alemão
- Espanhol
- Japonês
- Coreano
- Português
- Chinês simplificado

Aplicativos móveis de produtividade

Um X indica que o aplicativo está disponível neste determinado idioma.

iOS e Android

Idioma	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japonês	X	X	X	X	X	X
Chinês simplificado	X	X	X	X	X	X
Chinês tradicional	X	X	X	X	X	X

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Idioma	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Francês	X	X	X	X	X	X
Alemão	X	X	X	X	X	X
Espanhol	X	X	X	X	X	X
Coreano	X	X	X	X	X	X
Português	X	X	X	X	X	X
Holandês	X	X	X	X	X	X
Italiano	X	X	X	X	X	X
Dinamarquês	X	X	X	X	X	X
Sueco	X	X	X	X	X	X
Hebraico	X	X	X	X	X	iOS somente
Árabe	X	X	X	X	X	X
Russo	X	X	X	X	X	X
Turco	X	X	Somente Android	-	-	-

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 idioma da direita para a esquerda

A tabela a seguir resume o suporte para texto em idiomas do Oriente Médio de cada aplicativo. Um X indica que o recurso está disponível para a plataforma. O suporte a idiomas da direita para a esquerda

© 1999-2019 Citrix Systems, Inc. All rights reserved.

não está disponível para dispositivos do Windows.

Aplicativo	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

Instalar e configurar

April 15, 2019

Antes de começar

Você pode usar a seguinte lista de verificação de pré-instalação para conhecer os pré-requisitos e configurações da instalação do XenMobile no local. Cada tarefa ou observação inclui uma coluna que indica o componente ou a função à qual o requisito se aplica.

O planejamento de uma implementação do XenMobile envolve muitas considerações. Para ver recomendações, perguntas comuns e casos de uso para o seu ambiente XenMobile completo, consulte o Manual de implantação do XenMobile.

Para conhecer as etapas de instalação, consulte a seção Instalar o XenMobile mais adiante neste artigo.

A lista de verificação da pré-instalação

Conectividade básica de rede

Estas são as configurações de rede que você precisa 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 NetScaler Gateway

© 1999-2019 Citrix Systems, Inc. All rights reserved.

| Anote o endereço IP público e local. |
Você precisa desses endereços IP para configurar o firewall para configurar a conversão de endereços de rede (NAT).	XenMobile e NetScaler Gateway	
Anote a máscara de sub-rede.	XenMobile e NetScaler Gateway	
Anote os endereços IP do DNS.	XenMobile e NetScaler Gateway	
Anote os endereços IP do servidor WINS (se aplicável).	NetScaler Gateway	
Identifique e anote o nome do host do NetScaler Gateway.	NetScaler Gateway	Este item não é o FQDN. O FQDN é contido no certificado de servidor assinado que é vinculado ao servidor virtual e ao qual os usuários se conectam. Você pode configurar o nome do host usando o Assistente de Instalação no NetScaler Gateway.	NetScaler 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 necessários.	XenMobile	
Um endereço IP público configurado no NetScaler Gateway	NetScaler Gateway	
Uma entrada de DNS externa para o NetScaler Gateway	NetScaler Gateway
Anote o endereço IP do servidor proxy da Web, a porta, a lista de hosts do proxy e o nome de usuário e senha do administrador. Essas configurações são opcionais se você implantar um servidor proxy em sua rede (se aplicável).	NetScaler Gateway	Você pode usar o sAMAccountName ou o nome principal do usuário (UPN) ao configurar o nome de usuário para o proxy da web.	XenMobile e NetScaler Gateway	
Anote o endereço IP do gateway padrão.	XenMobile e NetScaler Gateway	
Anote o endereço IP do sistema (NSIP) e a máscara de sub-rede.	NetScaler Gateway	
Anote o endereço IP de sub-rede (SNIP) e a máscara de sub-rede.	NetScaler Gateway	
Anote o endereço IP do servidor virtual do NetScaler Gateway e o FQDN do certificado. Para configurar vários servidores virtuais, anote todos os endereços IP virtuais e FQDNs dos certificados.	NetScaler Gateway	
Anote as redes internas que os usuários podem acessar através do NetScaler Gateway. Exemplo: 10.10.0.0/24. Insira todas as redes internas e segmentos de rede aos quais os usuários precisam acessar nesses casos: quando os usuários se conectam ao Secure Hub ou ao NetScaler Gateway Plug-in quando o túnel dividido está definido como Ativado.	NetScaler Gateway	
Certifique-se de que a conectividade de rede entre o XenMobile Server, o NetScaler Gateway, o Microsoft SQL Server externo e o servidor DNS esteja acessível.	XenMobile e NetScaler Gateway	

Licenciamento

O XenMobile exige a compra de opções de licenciamento para o NetScaler Gateway e o XenMobile. Para obter mais informações sobre o Citrix Licensing, consulte O sistema Citrix Licensing.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisito	Componente	Anote a localização
Obtenha licenças universais no site da Citrix. Para obter detalhes, consulte Licensing na documentação do NetScaler Gateway.	NetScaler Gateway, XenMobile e Citrix License Server	

Certificados

O XenMobile e NetScaler Gateway exigem certificados para permitir 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 NetScaler Gateway	

Portas

Abra as portas para permitir a comunicação com os componentes do XenMobile.

Pré-requisito	Componente	Observações
Portas abertas para o XenMobile	XenMobile e NetScaler Gateway	

Banco de dados

O XenMobile exige a configuração de conexão de banco de dados. O repositório do XenMobile requer um banco de dados do Microsoft SQL Server em execução em uma das seguintes versões com suporte mencionadas em Requisitos do sistema e compatibilidade. A Citrix recomenda usar o Microsoft SQL remotamente. PostgreSQL está incluído no XenMobile. Use o PostgreSQL local ou remotamente *apenas* em ambientes de teste.

Por padrão, o XenMobile usa o driver do banco de dados jTDS. Para usar o driver Microsoft JDBC para instalações do XenMobile Server no local, consulte Drivers do SQL Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisito	Componente	Observações
Endereço IP e porta Microsoft SQL Server. Verifique se a conta de serviço do SQL Server a ser usada no XenMobile tem a permissão de função DBcreator.	XenMobile	

Configurações do Active Directory

Pré-requisito	Componente	Observações
————	———	————
Anote o endereço IP e a porta do Active Directory para os servidores primários e secundários. Se você usar a porta 636, instale um certificado raiz de uma AC no XenMobile e altere a opção Use secure connections para Yes.	XenMobile e NetScaler Gateway	
Anote o nome de domínio do Active Directory.	XenMobile e NetScaler 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 NetScaler Gateway	
Anote o DN da Base do Usuário, que é o nível do diretório sob o qual os usuários estão localizados. Por exemplo: `cn=users,dc=ace,dc=com`. O NetScaler Gateway e o XenMobile usam o DN da base do usuário para consultar o Active Directory.	XenMobile e NetScaler Gateway	
Anote o DN de base do grupo, que é o nível do diretório em que os grupos estão localizados. O NetScaler Gateway e o XenMobile usam esse DN para consultar o Active Directory.	XenMobile e NetScaler Gateway	

Conexões entre o XenMobile e o NetScaler Gateway

Pré-requisito	Componente	Anote a configuração
Anote o nome de host do XenMobile.	XenMobile	
Anote o endereço IP ou o FQDN do XenMobile.	XenMobile	
Identifique os aplicativos que os usuários podem acessar.	NetScaler Gateway	

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisito	Componente	Anote a configuração
Anote a URL de Retorno de Chamada.	XenMobile	

Conexões de usuário: acesso ao XenDesktop, ao XenApp e ao Citrix Secure Hub

A Citrix recomenda que você use o assistente Quick Configuration no NetScaler para definir as configurações de conexão entre o XenMobile e o NetScaler Gateway, e entre o XenMobile e o Secure Hub. Você deve criar um segundo servidor virtual para habilitar conexões de usuário do Citrix Receiver e navegadores da Web. Essas conexões são para aplicativos baseados no Windows e áreas de trabalho virtuais no XenApp e XenDesktop. A Citrix recomenda que você também use o assistente Quick Configuration no NetScaler para definir essas configurações.

Pré-requisito	Componente	Anote a configuração
Anote o nome de host e a URL externa do NetScaler Gateway. A URL externa é o endereço da Web ao qual os usuários se conectam.	XenMobile	
Anote a URL de retorno de chamada do NetScaler Gateway.	XenMobile	
Anote os endereços IP e as máscaras de sub-rede do servidor virtual.	NetScaler Gateway	
Anote o caminho do Program Neighborhood Agent ou de um site do Site XenApp e XenDesktop.	NetScaler Gateway e XenMobile	
Anote o endereço IP ou o FQDN do servidor XenApp ou XenDesktop que executa a Secure Ticket Authority (STA) (somente para conexões ICA).	NetScaler Gateway	
Anote o FQDN público do XenMobile.	NetScaler Gateway	

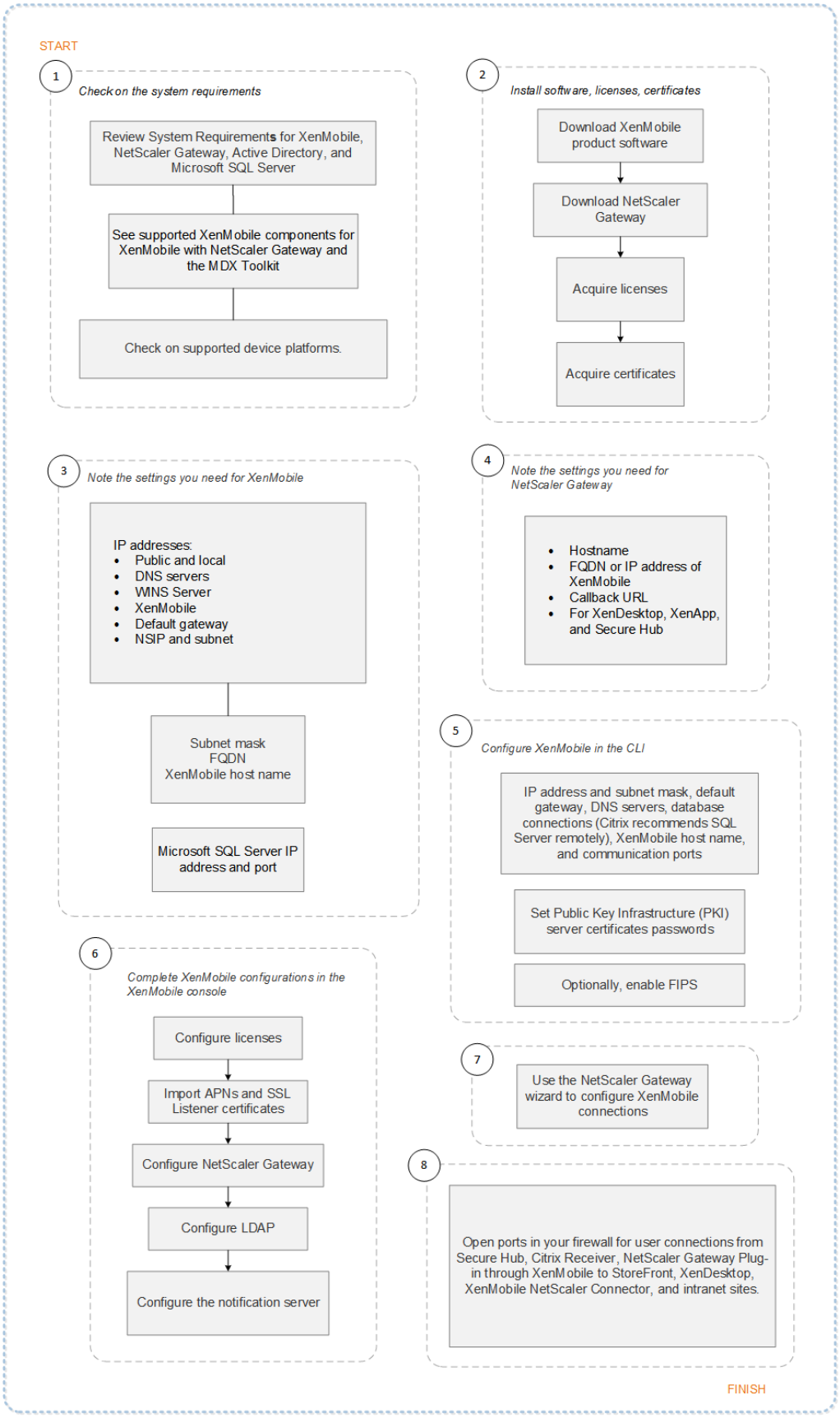
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisito	Componente	Anote a configuração
Note o FQDN público do Secure Hub.	NetScaler Gateway	

Fluxograma para implantação do XenMobile

Você pode usar este fluxograma para guiá-lo pelas etapas principais de implantação do XenMobile. Links para os tópicos sobre cada etapa encontram-se próximos à figura.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

1: Requisitos do sistema e compatibilidade

2: Instalar e configurar

3 e 4: Lista de verificação 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: Definição das configurações do seu ambiente do 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 do XenCenter ou do vSphere para instalar o XenMobile.

> Nota:
>
> Verifique se o hipervisor está configurado com o horário correto, seja usando um servidor NTP ou uma configuração manual, pois o XenMobile usa esse horário. Se você tiver problemas de fuso horário ao sincronizar o horário do XenMobile com um hipervisor, você pode evitar esses 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 do VMware ESXi. Antes de instalar o XenMobile no XenServer ou no VMware ESXi, você deve fazer o seguinte. Para obter detalhes, consulte a documentação do XenServer ou VMware.

- Instale o XenServer ou o VMware ESXi em um computador com os recursos de hardware adequados.
- Instale o XenCenter ou o vSphere em um computador separado. O computador que hospeda o XenCenter ou o vSphere se conecta ao host do XenServer ou do VMware ESXi por meio 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 2008 R2, o Windows Server 2012 ou o Windows Server 2012 R2 ativado para Hyper-V e funções em um computador com os 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. É possível reservar alguns NICs para o host.
- Exclua o arquivo Virtual Machines/<*UUID específico da compilação*>.xml
- Mova o arquivo Legacy/<*UUID específico da compilação*>.exp para Máquinas Virtuais

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Se você instalar o Windows Server 2008 R2 ou o Windows Server 2012, faça o seguinte:

Essas etapas são necessárias porque há duas versões diferentes do arquivo de manifesto do Hyper-V que representa a configuração da VM (.exp e .xml). As versões Windows Server 2008 R2 e Windows Server 2012 são compatíveis somente com .exp. Para essas versões, somente o arquivo de manifesto .exp deve estar em vigor antes da instalação.

O Windows Server 2012 R2 não exige essas etapas extras.

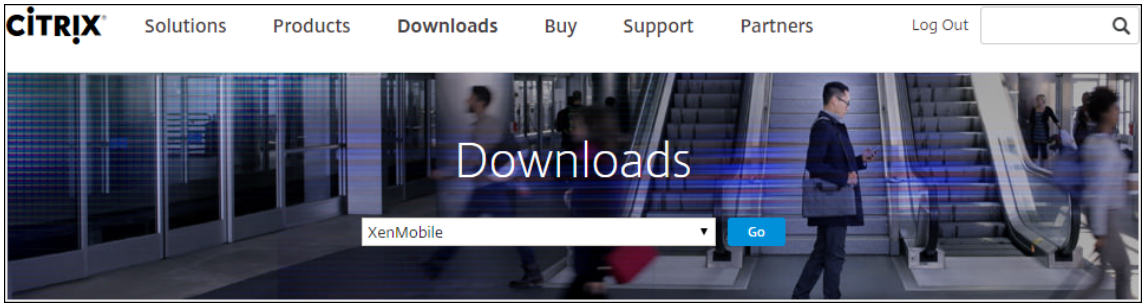
Modo FIPS 140-2. Para instalar o XenMobile Server no modo FIPS, conclua um grupo de pré-requisitos, conforme discutido em Configurar o modo FIPS com o XenMobile.

Baixar o software do produto XenMobile

Você pode baixar o software do produto no Site da Citrix. Faça login no site e use o link de Downloads para navegar até a página que contém o software que você deseja baixar.

Para baixar o software do XenMobile

1. Vá para o Site da Citrix.
2. Ao lado da caixa Pesquisar, clique em **Login** e faça login na sua conta.
3. Clique na guia **Downloads**.
4. Na página Downloads, na lista Selecionar um produto, clique em **XenMobile**.



5. Clique em **Ir**. A página XenMobile é exibida.
6. Expanda **XenMobile Server**.
7. Expanda **Software do produto**.
8. Clique em **XenMobile Server 10**.
9. Clique no menu **Ir para Download** e escolha a imagem virtual apropriada para usar para instalar o XenMobile. Alternativamente, role a página para localizar o botão **Download do arquivo** da imagem que deseja instalar.
10. Siga as instruções na tela para baixar o software.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para baixar o software do NetScaler Gateway

Você pode usar este procedimento para baixar o dispositivo virtual do NetScaler Gateway ou as atualizações de software para seu dispositivo existente do NetScaler Gateway.

1. Vá para o Site da Citrix.
2. Se você ainda não tiver feito login no site da Citrix, ao lado da caixa Pesquisar, clique em **Login** e faça login na sua conta.
3. Clique na guia **Downloads**.
4. Na página Downloads, na lista Selecionar um produto, clique em **NetScaler Gateway**.
5. Clique em **Ir**. A página NetScaler Gateway é exibida.
6. Na página NetScaler Gateway, expanda a versão do NetScaler Gateway que você executa.
7. Em **Firmware**, clique na versão do software do dispositivo que você desejar baixar.

   > Nota:
   >
   > Você também pode clicar em **Dispositivos virtuais** para baixar o NetScaler VPX. Quando você seleciona essa opção, recebe uma lista de softwares para a máquina virtual de cada hipervisor.

8. Clique na versão do software do dispositivo que você desejar baixar.
9. Na página do software do dispositivo da versão que você deseja baixar, clique na opção **Download** do dispositivo virtual adequado.
10. Siga as instruções na tela para baixar o software.

Configurar o XenMobile para a primeira utilização

1. Para configurar o endereço IP e a máscara de sub-rede, o gateway padrão, os servidores DNS e outros detalhes do XenMobile, use o console de linha de comando do XenCenter ou do vSphere.

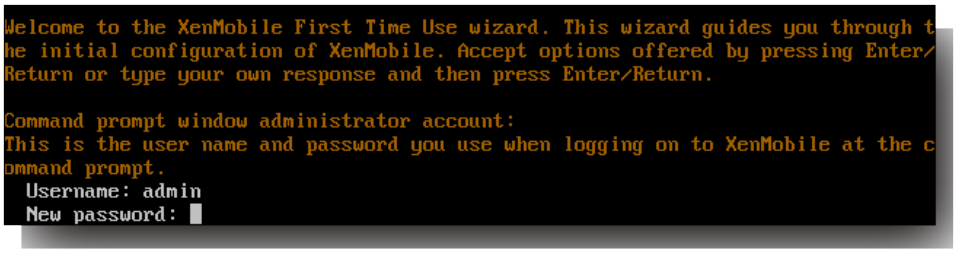
   > Nota:
   >
   > Quando você usa um cliente vSphere Web, recomendamos que você não configure as propriedades de rede durante o período em que implanta o modelo OVF na página **Personalizar modelo**. Agindo assim, em uma configuração de alta disponibilidade, você evita um problema com o endereço IP que ocorre quando você clona e depois reinicia a segunda máquina virtual do XenMobile.

2. Acesse o console de gerenciamento do XenMobile apenas com o nome de domínio totalmente qualificado do XenMobile Server ou dos endereços IP do nó.
3. Faça login e siga as etapas nas telas de login iniciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o XenMobile na janela do prompt de comando

1. Importe a máquina virtual do XenMobile para o Citrix XenServer, o Microsoft Hyper-V ou o VMware ESXi. Para obter detalhes, consulte a documentação do XenServer, Hyper-V ou VMware.
2. No seu hipervisor, selecione a máquina virtual do XenMobile importada e inicie a exibição do prompt de comando. Para obter detalhes, consulte a documentação do hipervisor.
3. Na página do console do hipervisor, crie uma conta de administrador para o XenMobile na janela do prompt de comando digitando o nome do usuário e a senha de administrador.

   > Importante:
   >
   > Quando você cria ou altera as senhas da conta do administrador do prompt de comando, dos certificados de servidor de Infraestrutura de Chave Pública (PKI) e do modo FIPS: o XenMobile impõe as seguintes regras a todos os usuários, exceto os 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) é exibido quando você digita a nova senha.

4. Forneça as seguintes informações da rede e, em seguida, digite **y** para confirmar as configurações:

   a) Endereço IP do XenMobile Server

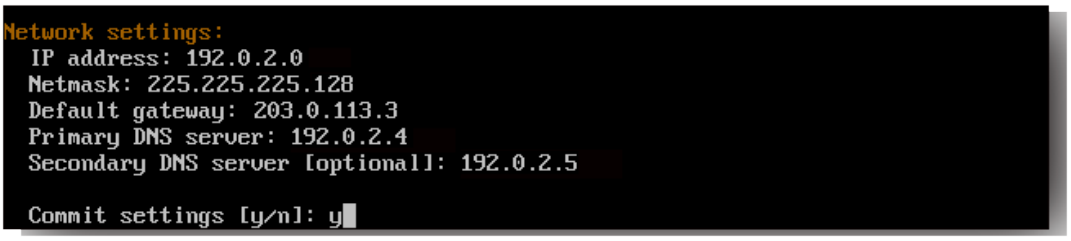
   b) Máscara de rede

   c) Gateway padrão, que é o endereço IP do gateway padrão no DMZ

   d) Servidor DNS principal, que é o endereço IP do servidor DNS

   e) Servidor DNS secundário (opcional)

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Os endereços mostrados nesta e nas imagens a seguir são não funcionais e fornecidos somente como exemplo.

5. Digite **y** para aumentar a segurança gerando uma senha de criptografia aleatória ou **n** para fornecer sua própria senha. A Citrix recomenda digitar **y** para gerar uma senha aleatória.

   A senha é usada como parte da proteção das chaves de criptografia usadas para proteger os seus dados confidenciais. Um hash da senha, armazenado no sistema de arquivos do servidor, é usado para recuperar as chaves durante a criptografia e decodificação de dados. A senha não pode ser exibida.

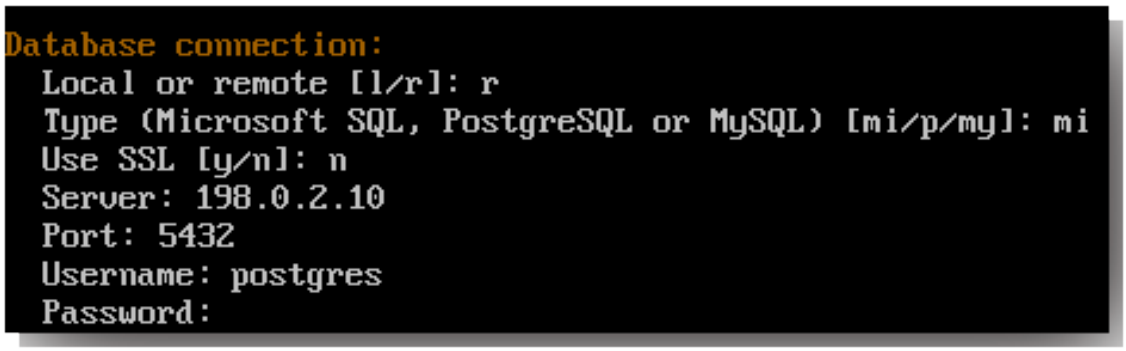
   > Nota:
   >
   > Se você pretende estender o seu ambiente e configurar mais servidores, forneça sua própria senha. Se você selecionar uma senha aleatória, não poderá visualizá-la.

6. Opcionalmente, ative o Federal Information Processing Standard (FIPS). Para obter detalhes sobre o FIPS, consulte FIPS. Além disso, é preciso atender a um grupo de pré-requisitos, conforme discutido em Configurar o modo FIPS com o XenMobile.

7. Forneça as seguintes informações para configurar a conexão do banco de dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- O seu banco de dados pode ser local ou remoto. Digite **l** para local ou **r** para remoto.
- Selecione o tipo do banco de dados. Digite **mi** para o Microsoft SQL ou digite **p** para o PostgreSQL.

  > Importante:
  >
  > – A Citrix recomenda usar o Microsoft SQL remotamente. PostgreSQL está incluído no XenMobile. Use o PostgreSQL local ou remotamente *apenas* em ambientes de teste.
  > – A migração de banco de dados não é compatível. Os 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 do SSL no seu banco de dados.
- Forneça o nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o XenMobile. Esse servidor de host fornece os serviços de gerenciamento de dispositivo e gerenciamento de aplicativo.
- Digite o seu número da porta do banco de dados se ele for diferente do número de porta padrão. A porta padrão do Microsoft SQL é 1433 e a porta padrão do PostgreSQL é 5432.
- Digite o nome de usuário do seu administrador de banco de dados.
- Digite a senha do seu administrador de 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 ativar o clustering de nós ou instâncias do XenMobile.

   > Importante:
   >
   > Se você ativar um cluster do XenMobile, depois de concluir a configuração do sistema, abra a porta 80 para ativar a comunicação em tempo real entre os membros de cluster. Conclua a instalação em todos os nós de cluster.

9. Digite o nome de domínio totalmente qualificado (FQDN) do XenMobile Server.



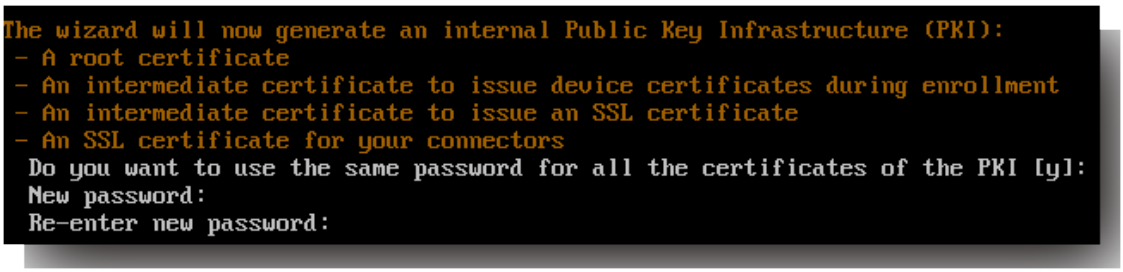
10. Pressione **Enter** para confirmar as configurações.
11. Identifique as portas de comunicação. Para obter detalhes sobre portas e seus respectivos usos, consulte Requisitos de porta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Aceite as portas padrão pressionando **Enter** (Return em um Mac).



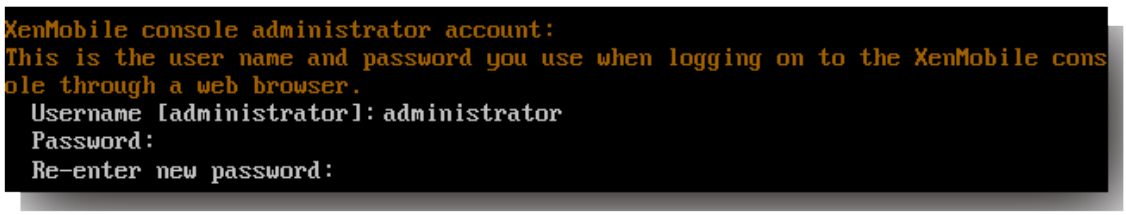
12. Ignore a próxima pergunta sobre atualização de uma versão anterior do XenMobile, pois você está instalando o XenMobile pela primeira vez.
13. Digite **y** se você desejar usar a mesma senha para todos os certificados de Infraestrutura de Chave Pública (PKI). Para obter detalhes sobre o recurso de PKI do XenMobile, consulte Carregando certificados.



> Importante:
>
> Se você pretende agrupar em cluster os nós, ou instâncias, do XenMobile, forneça senhas idênticas para os nós subsequentes.

14. Digite a nova senha e, em seguida, redigite-a para confirmá-la.

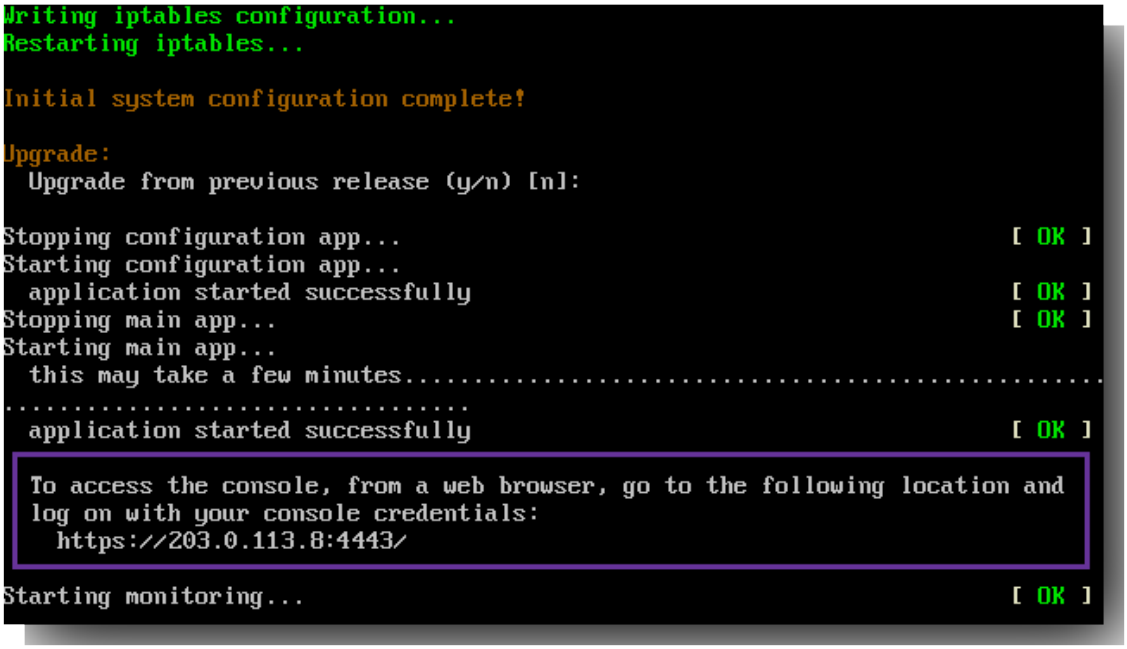
    Nenhum caractere (como asteriscos) é exibido quando você digita a nova senha.
15. Pressione **Enter** para confirmar as configurações.
16. Crie uma conta de administrador para fazer login no console XenMobile usando um navegador da Web. Certifique-se de anotar essas credenciais para uso posterior.



> Nota:
>
> Nenhum caractere (como asteriscos) é exibido quando você digita a nova senha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 a URL completa exibida na tela e continue essa configuração inicial do XenMobile no seu navegador da Web.

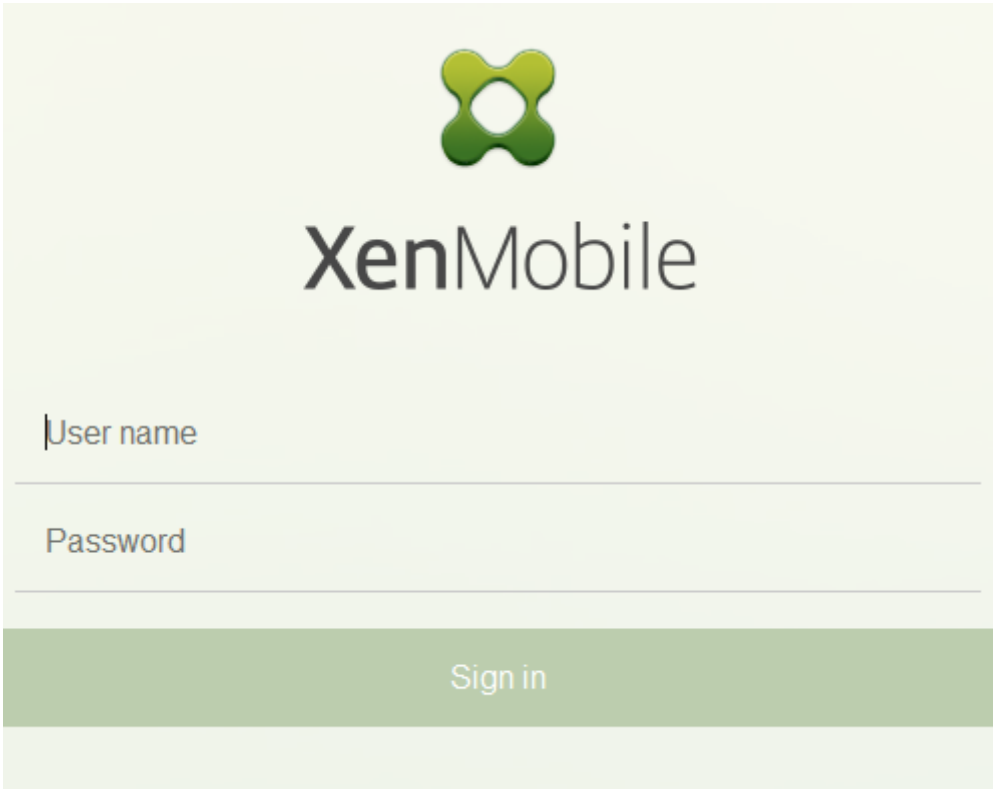


Configurar o XenMobile em um navegador da Web

Depois de concluir a parte inicial da configuração do XenMobile na janela do prompt de comando do hipervisor, conclua o processo no navegador da Web.

1. No navegador da Web, navegue até o local fornecido na conclusão da configuração da janela do prompt de comando.
2. Digite o nome do usuário e a senha da conta do administrador do console XenMobile que você criou na janela do prompt de comando.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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, além de como configurar notificações de expiração, consulte Licenciamento.

   > Importante:
   >
   > Se você pretende usar clustering do XenMobile mediante a adição de nós de cluster, ou instâncias, do XenMobile, precisará 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 de APNs e de ouvinte SSL. O gerenciamento de dispositivos iOS requer um certificado de APNs. Para obter detalhes sobre como trabalhar com certificados, consulte Certificados.

   > Nota:
   >
   > Essa etapa exige a reinicialização do servidor.

7. Se for adequado para o ambiente, configure o NetScaler Gateway. Para obter detalhes sobre como configurar o NetScaler Gateway, consulte NetScaler Gateway e XenMobile e Definição das configurações do seu ambiente do XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> - Você pode implantar o NetScaler Gateway no perímetro da sua rede interna (ou intranet). Essa implantação oferece um ponto único e seguro de acesso para os servidores, aplicativos e outros recursos de rede que residem na rede interna. Nessa implantação, todos os usuários remotos devem se conectar ao NetScaler Gateway antes que possam acessar qualquer recurso da rede interna.
> - Embora o NetScaler Gateway seja uma configuração opcional, depois que você inserir os dados na página, deverá limpar ou preencher os campos obrigatórios antes que possa sair da página.

8. Conclua a configuração do LDAP para acessar usuários e grupos do Active Directory. Para obter detalhes sobre como configurar a conexão LDAP, consulte Configuração de LDAP.
9. Configure o servidor de notificação para que ele seja capaz de enviar mensagens aos usuários. Para obter detalhes sobre como configurar o servidor de notificação, consulte Notificações.

Pós-requisito. Reinicie o XenMobile Server para ativar seus certificados.

Configurar o modo FIPS com o XenMobile

April 15, 2019

O modo FIPS (Federal Information Processing Standards) no XenMobile dá suporte a clientes do governo federal dos EUA, usando somente bibliotecas de certificado FIPS 140-2 para todas as operações de criptografia. Instalar o XenMobile Server com o modo FIPS garante que todos os dados do cliente e do servidor XenMobile sejam totalmente compatíveis com o FIPS 140-2. Essa conformidade se aplica aos dados em repouso e aos dados em trânsito.

Antes de instalar um XenMobile Server no modo FIPS, conclua os pré-requisitos a seguir.

- Use um SQL Server 2012 ou 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 os Manuais Online do SQL Server.
- A comunicação SSL segura exige que você instale um certificado SSL no seu SQL Server. O certificado SSL pode ser um certificado público de uma AC comercial ou um certificado autoassinado de uma AC interna. Atenção, o SQL Server 2014 não pode aceitar um certificado curinga. A Citrix recomenda, portanto, que você solicite um certificado SSL com o FQDN do SQL Server.
- Se você usar um certificado autoassinado para o SQL Server, obtenha uma cópia do certificado de CA raiz que emitiu o seu certificado autoassinado. Você importa o certificado da CA raiz para o XenMobile Server durante a instalação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração do modo FIPS

Você pode ativar o modo FIPS somente durante a instalação inicial do XenMobile Server. Não é possível ativar o modo FIPS após a conclusão da instalação. Portanto, se você planeja usar o modo FIPS, deverá instalar o XenMobile Server com o modo FIPS do início. Além disso, para clusters do XenMobile, todos os nós do cluster devem ter o FIPS ativado. Você não pode ter uma combinação de XenMobile Servers FIPS e não FIPS no mesmo cluster.

Há uma opção **Toggle FIPS mode** na interface de linha de comando do XenMobile que não se destina ao uso em produção. Essa opção se destina ao uso diagnóstico e não de produção, e não é compatível em um XenMobile Server de produção.

1. Durante a instalação inicial, ative **FIPS mode**.
2. Carregue o certificado de AC raiz para o SQL Server. Se você estiver usando um certificado SSL autoassinado em vez de um certificado público no seu SQL Server, selecione **Sim** para essa opção. Em seguida, você pode optar por um dos seguintes procedimentos:
    a) Copie e cole o certificado de AC.
    b) Importe o certificado de AC. Para importar o certificado de AC, você deve publicá-lo em um site que possa ser acessado do XenMobile Server usando uma URL HTTP. Para obter detalhes, consulte Upload do certificado no XenMobile.
3. Especifique o nome do servidor e a porta do SQL Server, as credenciais de login no SQL Server e o nome do banco de dados a ser criado para o XenMobile.

    > Nota:
    >
    > Você pode usar um login SQL ou uma conta do Active Directory para acessar o SQL Server, mas o login usado deve ter a função DBcreator.

4. Para usar uma conta do Active Directory, insira as credenciais no formato domínio\nome do usuário.
5. Depois de concluir essas etapas, prossiga com a instalação inicial do XenMobile.

Para confirmar que a configuração do modo FIPS foi bem-sucedida, faça login na interface de linha de comando do XenMobile. A frase **In FIPS Compliant Mode** é exibida na faixa de login.

Importando certificados

O procedimento a seguir descreve como configurar o modo FIPS no XenMobile importando o certificado, que é necessário quando você usa um hipervisor VMware.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos do SQL

1. A conexão com a instância do SQL do XenMobile precisa ser segura, e a versão do SQL Server deve ser 2012 ou 2014. Para proteger a conexão, consulte Como ativar a criptografia SSL de uma instância do SQL Server usando o Console de Gerenciamento Microsoft.
2. Se o serviço não for reiniciado corretamente, verifique o seguinte: abra **Services.msc**.
   a) Copie as informações de conta de login usadas para o serviço do SQL Server.
   b) Abra MMC.exe no SQL Server.
   c) Vá até **File > Add/Remove Snap-in** e clique duas vezes no item de certificados para adicionar o snap-in dos certificados. Selecione a conta de computador e o computador local nas duas páginas do assistente.
   d) Clique em **OK**.
   e) Expanda **Certificates (Local Computer) > Personal > Certificados** e localize o certificado SSL importado.
   f) Clique com o botão direito do mouse no certificado importado (selecionado no SQL Server Configuration Manager) e clique em **All Tasks > Manage Private Keys**.
   g) Em **Group or User names**, clique em **Add**.
   h) Insira o nome da conta de serviço do SQL que você copiou na etapa anterior.
   i) Limpe a opção **Allow Full Control**. Por padrão, as permissões Controle total e Leitura serão fornecidas à conta de serviço, mas ela precisa somente conseguir ler a chave privada.
   j) Feche o **MMC** e inicie o serviço SQL.
3. Verifique se o serviço SQL foi iniciado corretamente.

Pré-requisitos dos Serviços de Informações da Internet (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 **Authentication** do site padrão.
4. Defina **Anonymous** como **enabled**.
5. Marque a caixa de seleção de regras **Failed Request Tracking**.
6. O arquivo .cer não pode estar bloqueado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. Navegue até a localização do .cer em um navegador Internet Explorer do servidor local, `https://localhost/certname.cer`. O texto do certificado raiz é exibido no navegador.
8. Se o certificado raiz não for exibido no navegador Internet Explorer, verifique se o ASP está ativado no servidor IIS como se segue.
   a) Abra o Gerenciador de Servidores.
   b) Navegue até o assistente em **Gerenciar > Adicionar Funções e Recursos**.
   c) Nas funções de servidor, expanda **Servidor Web (IIS)**, expanda **Servidor Web**, expanda **Desenvolvimento de aplicativo** e selecione **ASP**.
   d) Clique em **Avançar** até a conclusão da instalação.
9. Abra o Internet Explorer e 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 configuração inicial do modo FIPS

Quando você concluir as etapas para configurar o XenMobile pela primeira vez no console de linha de comando, deverá concluir estas configurações para importar o certificado raiz. Para obter detalhes sobre as etapas de instalação, consulte Instalação do XenMobile.

- Ativar FIPS: Sim
- Carregar certificado raiz: Sim
- Copiar(c) ou Importar(i): i
- Digite o URL HTTP para importar: `https://<FQDN of IIS server>/cert.cer`
- Server: *FQDN do SQL Server*
- Port: 1433
- User name: a conta de serviço que pode criar o banco de dados (`domain\username`).
- Password: a senha da conta de serviço.
- Database: um nome de sua escolha.

Ativar o modo FIPS em dispositivos móveis

Por padrão, o modo FIPS está desativado em dispositivos móveis. Para ativar o modo FIPS, vá para **Configurações > Propriedades do cliente**, edite a propriedade **Ativar o modo FIPS** e defina o valor como **true**. Para obter mais informações, consulte Propriedades do cliente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o clustering

March 6, 2019

Para configurar o clustering, configure os dois endereços IP virtuais de balanceamento de carga a seguir no NetScaler.

- **Endereço IP virtual de balanceamento de carga do gerenciamento de dispositivo móvel (MDM):** Um endereço IP virtual de balanceamento de carga MDM é necessário para comunicação com os nós do XenMobile que estão configurados em um cluster. O balanceamento de carga é realizado no modo SSL Bridge.
- **Endereço IP virtual de balanceamento de carga do gerenciamento de aplicativo móvel (MAM):** Os endereços IP virtuais de balanceamento de carga MAM são necessários para que o NetScaler Gateway se comunique com os nós do XenMobile que estão configurados em um cluster. No XenMobile, por padrão, todo o tráfego do NetScaler Gateway é roteado para o endereço IP virtual do balanceamento de carga na porta 8443.

Os procedimentos deste artigo explicam como criar uma nova máquina virtual (VM) XenMobile e vincular a nova VM a uma VM existente. Essas etapas criam uma configuração de cluster.

Pré-requisitos

- O nó do XenMobile necessário está totalmente configurado.
- Configure o NTP em todos os nós do cluster e no banco de dados do XenMobile. Para que o armazenamento em cluster funcione corretamente, todos esses servidores devem ter o mesmo horário.
- Um endereço IP público para balanceador de carga MDM e um endereço IP privado para MAM.
- Certificados de servidor.
- Um IP livre para o endereço IP virtual do NetScaler Gateway.
- Com o XenMobile implantado em uma configuração de cluster e no modo somente MDM ou Enterprise (MDM+MAM): modifique a configuração do balanceador de carga do NetScaler para usar a **Persistência do endereço IP de origem** para todos os balanceadores de carga do NetScaler MDM, ou seja, servidores virtuais configurados para as portas 8443 e 443. Conclua essa configuração antes de dispositivos de usuários atualizarem 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 ver os diagramas de arquitetura de referência para o XenMobile 10.x nas configurações de cluster, consulte Arquitetura.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

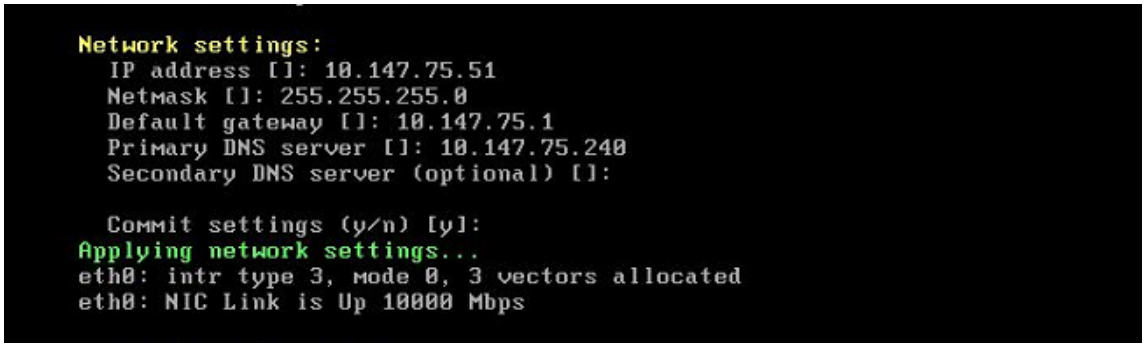
Instalando os nós de cluster do XenMobile

Com base no número de nós que você exigir, crie VMs do XenMobile. Aponte as novas VMs para o mesmo banco de dados e forneça as mesmas senhas do certificado PKI.

1. Abra o console da linha de comando da nova VM e insira a nova senha da conta de administrador.



2. Forneça os detalhes de configuração de rede, conforme mostrado na figura a seguir.



3. Se você desejar usar a senha padrão para proteção de dados, digite **y**; ou digite **n** e insira uma nova senha.

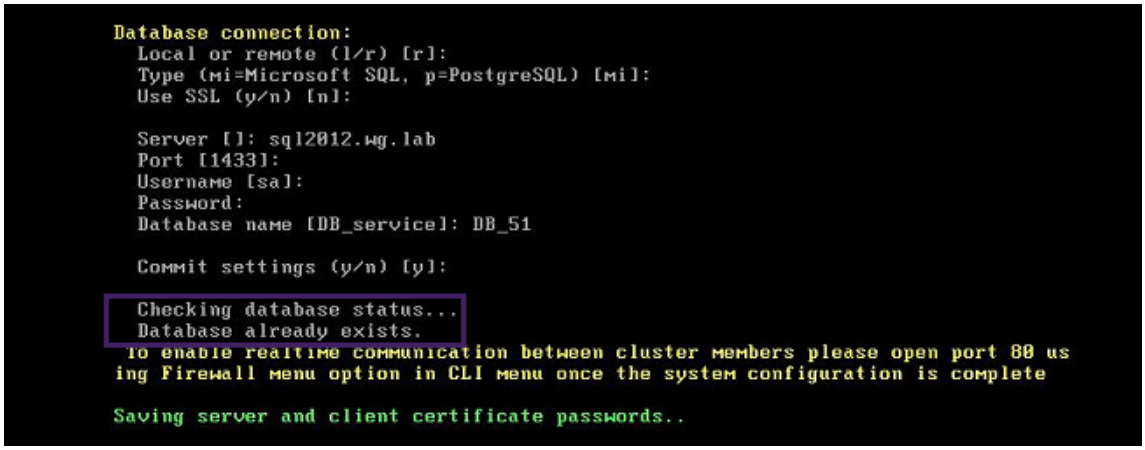


4. Se você desejar usar o modo FIPS, digite **y**; caso contrário, **n**.

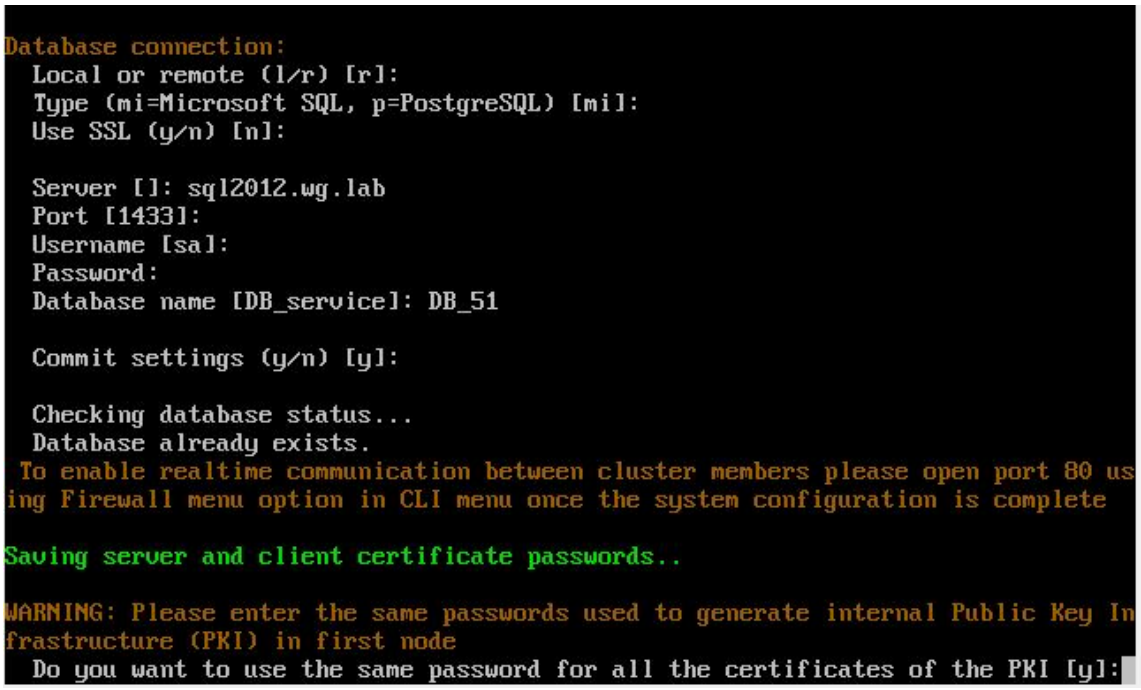


5. Configure o banco de dados para que você aponte para o mesmo banco de dados que a VM totalmente configurada anterior aponta. Você verá a mensagem: O banco de dados já existe.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

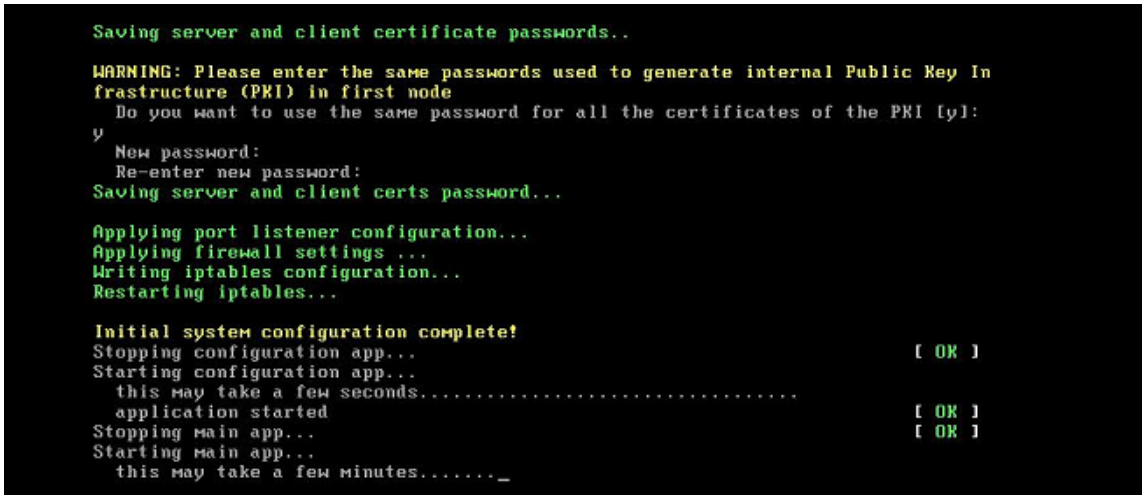


6. Insira as mesmas senhas dos certificados que você forneceu para a primeira VM.

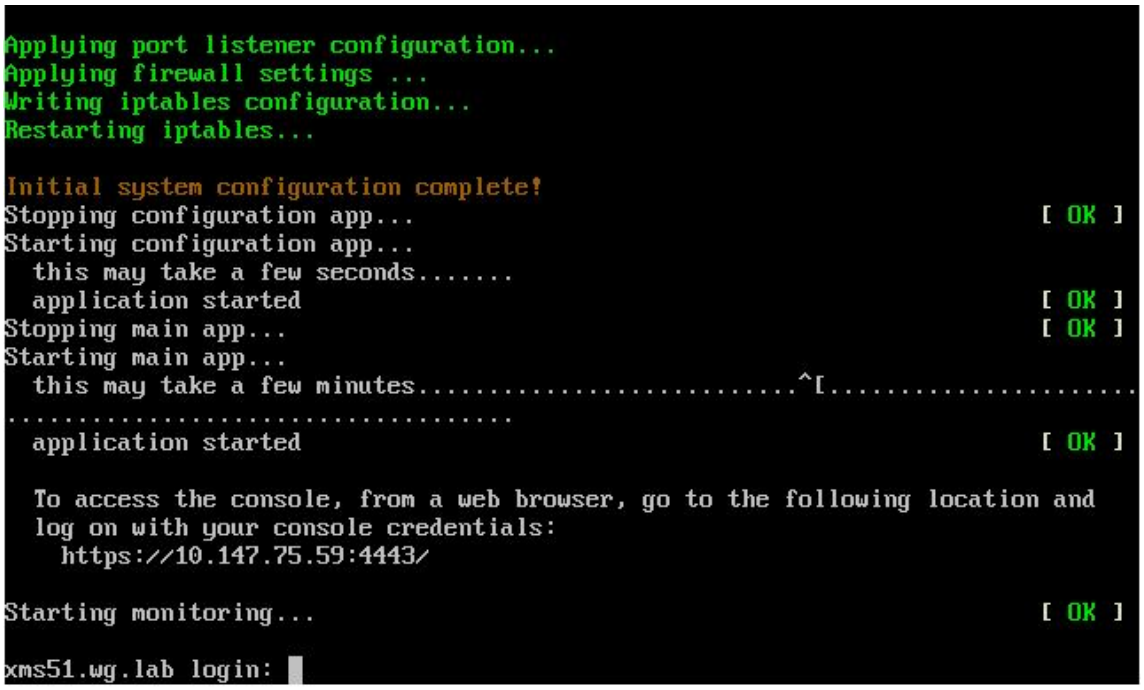


Depois que você tiver inserido a senha, a configuração inicial do segundo nó será concluída.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



7. Quando a configuração for concluída, o servidor será reiniciado e a caixa de diálogo de login será exibida.



> Nota:
>
> A caixa de diálogo de login é idêntica à caixa de diálogo de login da primeira VM. A correspondência é uma maneira de confirmar que ambas as VMs usam o mesmo servidor do banco de dados.

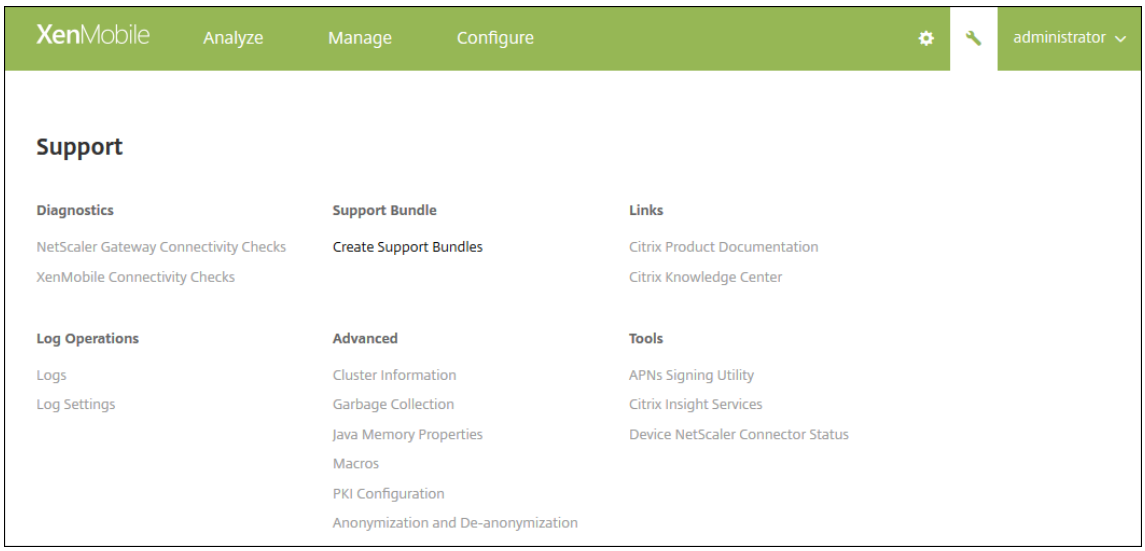
8. Use o nome de domínio totalmente qualificado (FQDN) do XenMobile para abrir o console XenMobile em um navegador da Web.
9. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

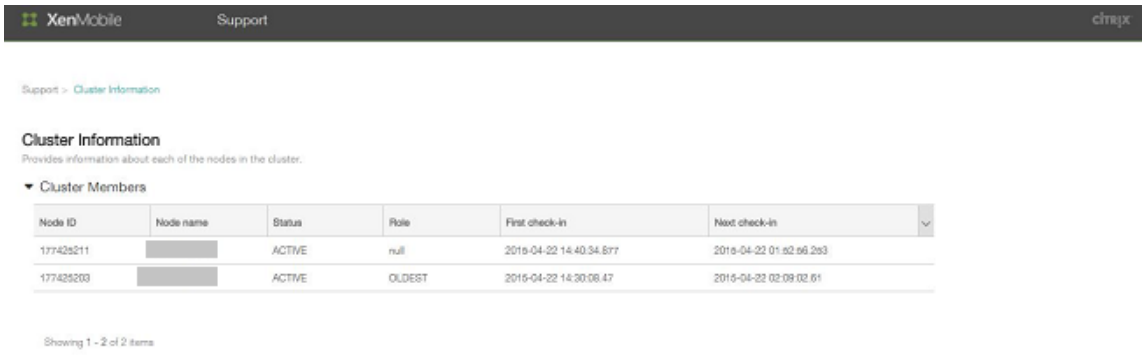


A página **Suporte** é aberta.

10. Em **Avançado**, clique em **Informações de Cluster**.



Todas as informações sobre o cluster, incluindo o membro do cluster, as informações de conexão do dispositivo, as tarefas e assim por diante, são exibidas. O novo nó agora é um membro do cluster.



Você pode adicionar outros nós seguindo as mesmas etapas. O primeiro cluster adicionado ao nó tem uma Função de **MAIS ANTIGO**. Clusters adicionados depois disso mostrarão uma Função de **NENHUM** ou **nulo**.

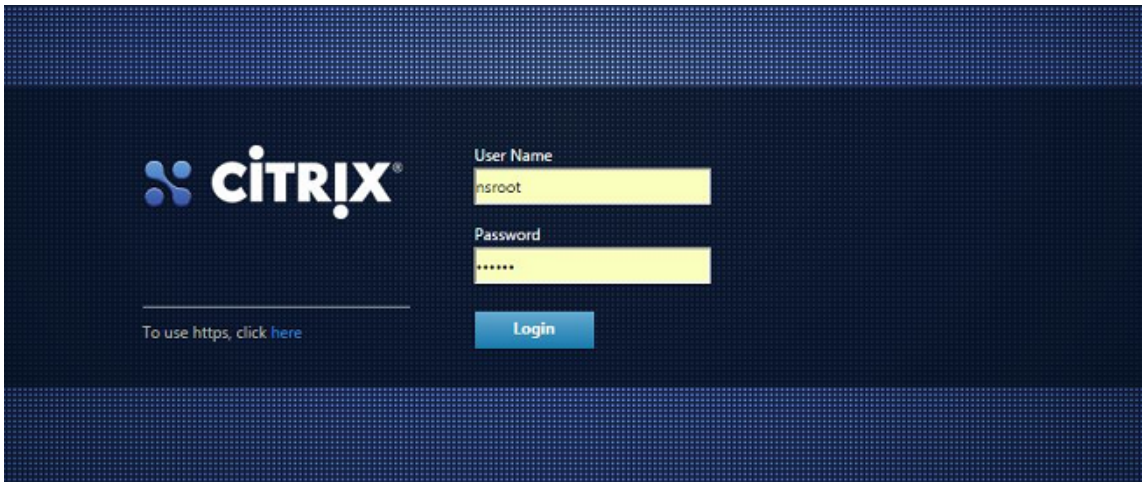
Para configurar o balanceamento de carga do cluster do XenMobile no NetScaler

Depois de adicionar os nós como membros do cluster do XenMobile, balanceie a carga dos nós para poder acessar os clusters. O balanceamento de carga é realizado por meio da execução do Assistente

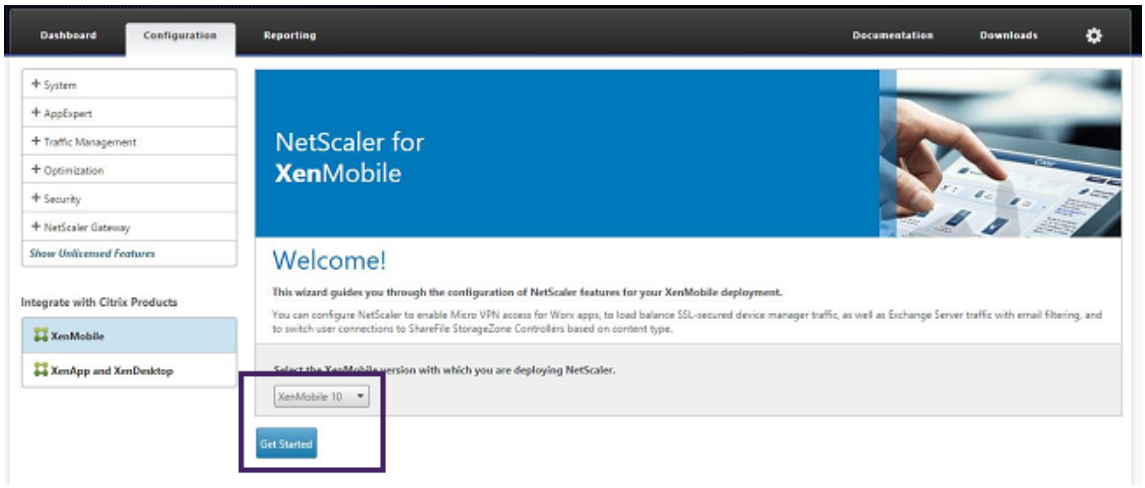
© 1999-2019 Citrix Systems, Inc. All rights reserved.

do XenMobile disponível no NetScaler. As etapas a seguir descrevem como balancear a carga do XenMobile executando o assistente.

1. Faça login no NetScaler.

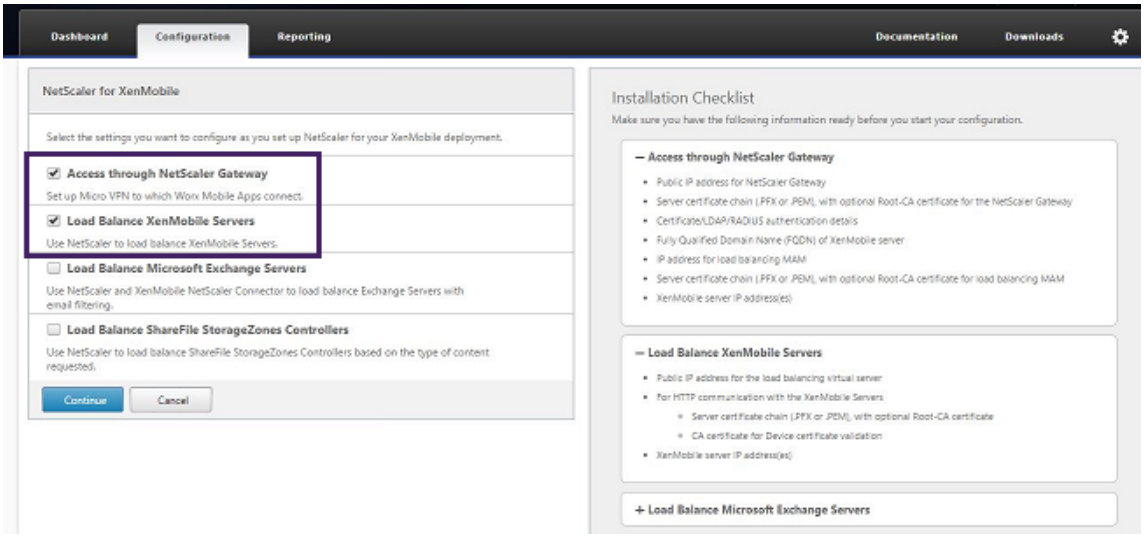


2. Na guia Configuration, clique em **XenMobile** e em **Get Started**.

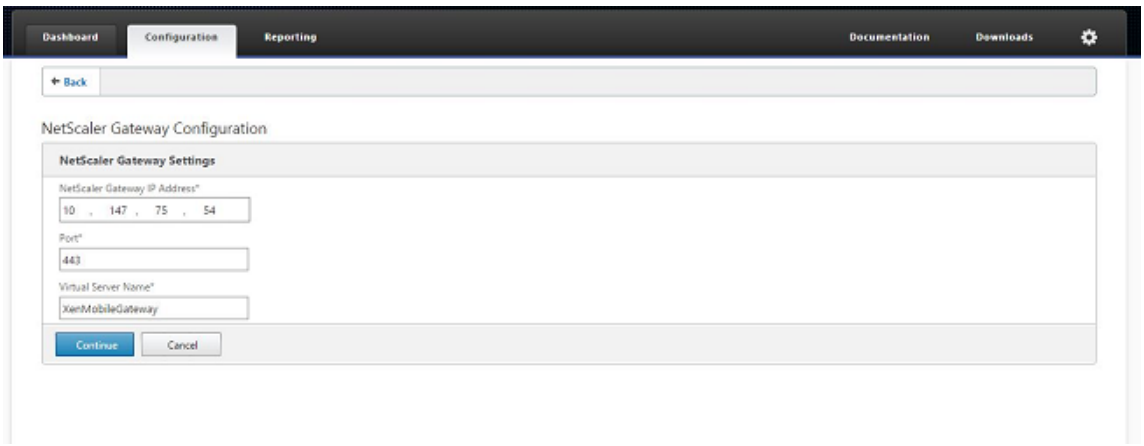


3. Marque as caixas de seleção **Access through NetScaler Gateway** e **Load Balance XenMobile Servers** e clique em **Continue**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

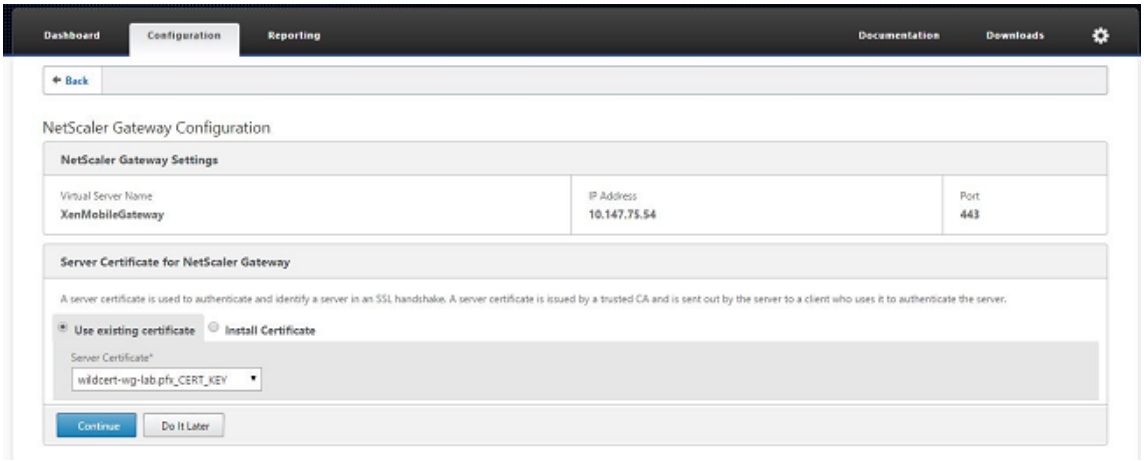


4. Insira o endereço IP do NetScaler Gateway e clique em **Continue**.

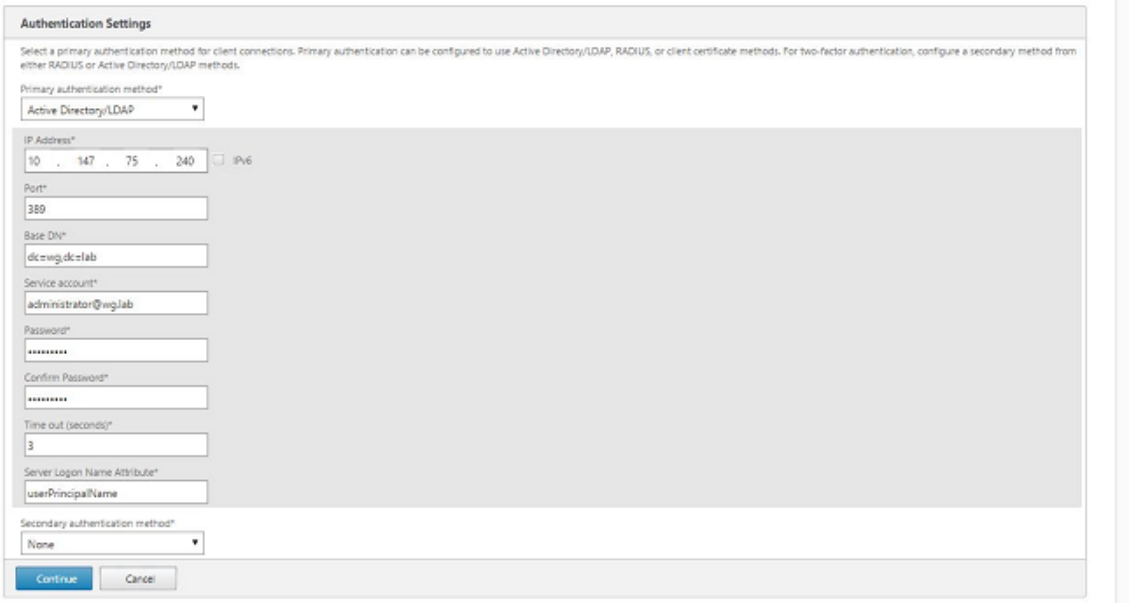


5. Associe o certificado de servidor ao endereço IP virtual do NetScaler Gateway executando uma das opções a seguir e clique em **Continue**.
   - Em **Use existing certificate**, selecione o certificado do servidor na lista.
   - Clique na guia **Install Certificate** para carregar um novo certificado de servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



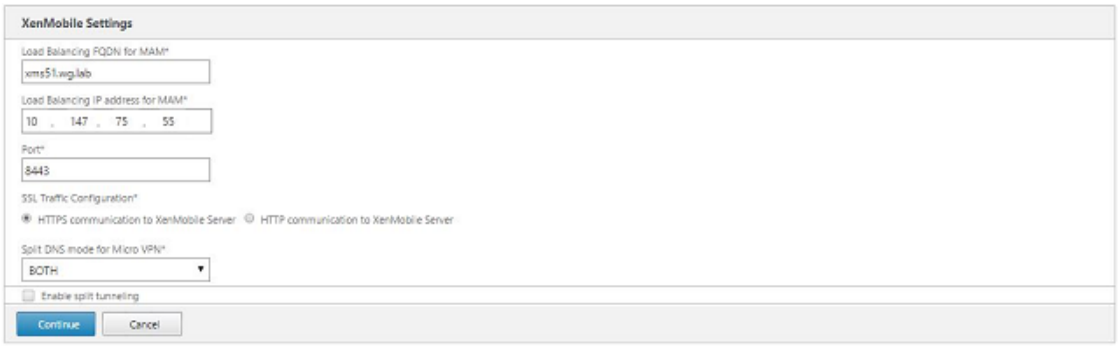
6. Insira os detalhes do servidor de Autenticação e clique em **Continue**.



> Nota:
>
> Confirme que o Server Logon Name Attribute seja o mesmo que você forneceu na configuração LDAP do XenMobile.

7. Nas configurações do XenMobile, insira o Load Balancing FQDN for MAM e clique em **Continue**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Confirme que o FQDN do endereço IP virtual de balanceamento de carga MAM e o FQDN do XenMobile sejam os mesmos.

8. Se você desejar usar o modo SSL Bridge (HTTPS), selecione **HTTPS communication to XenMobile Server**. No entanto, se você desejar usar a descarga de SSL, selecione **HTTP communication to XenMobile Server**, conforme mostrado na figura anterior. Para este artigo, a opção é o modo SSL Bridge (HTTPS).
9. Associe o certificado de servidor do endereço IP virtual de balanceamento de carga MAM e clique em Continue.

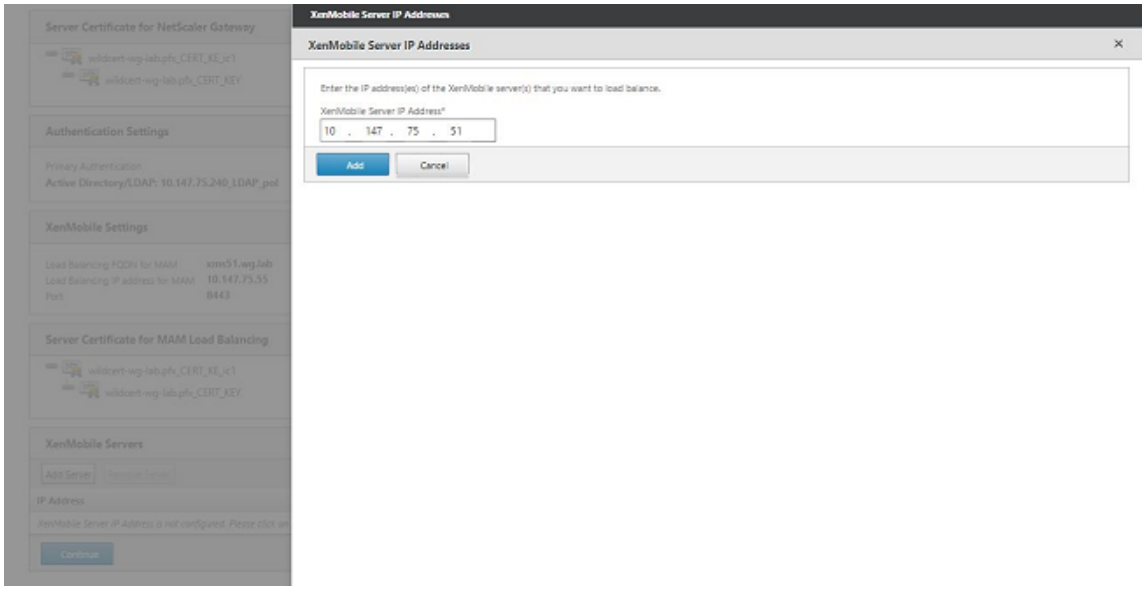


10. Em XenMobile Servers, clique em **Add Server** para adicionar os nós do XenMobile.

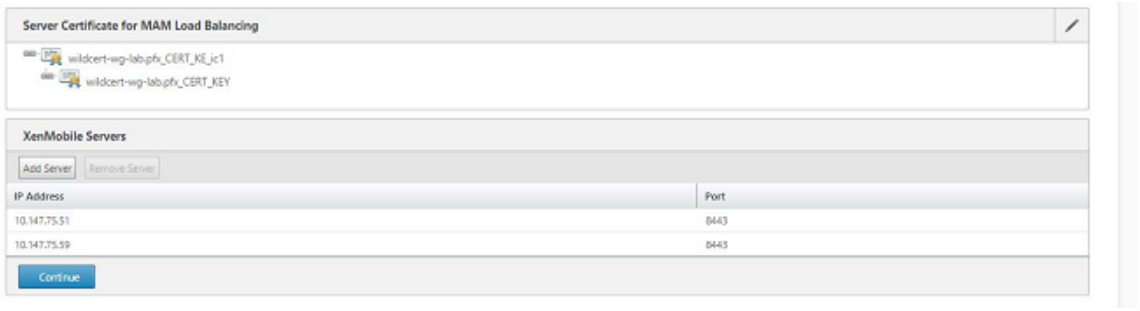


11. Insira o endereço IP do nó do XenMobile e clique em Add.

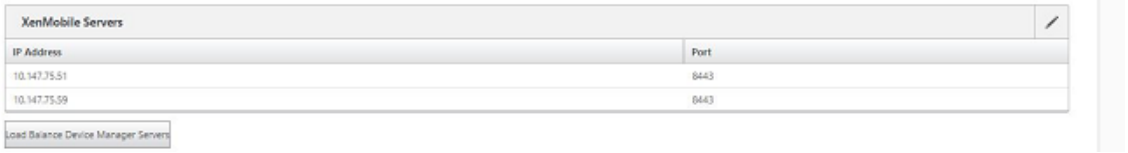
© 1999-2019 Citrix Systems, Inc. All rights reserved.



12. Repita as etapas 10 e 11 para adicionar mais nós do XenMobile que fazem parte do cluster do XenMobile. Você verá todos os nós do XenMobile que adicionou. Clique em Continue.

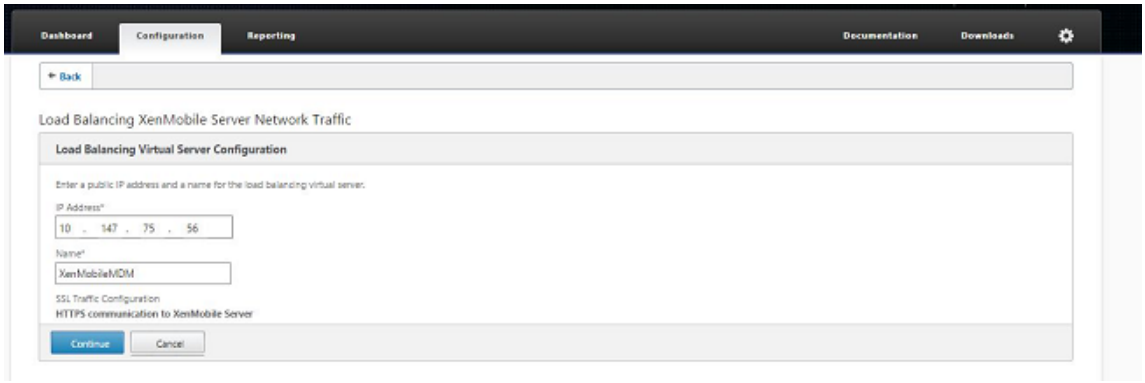


13. Clique em **Load Balance Device Manager Servers** para continuar com a configuração do balanceamento de carga MDM.

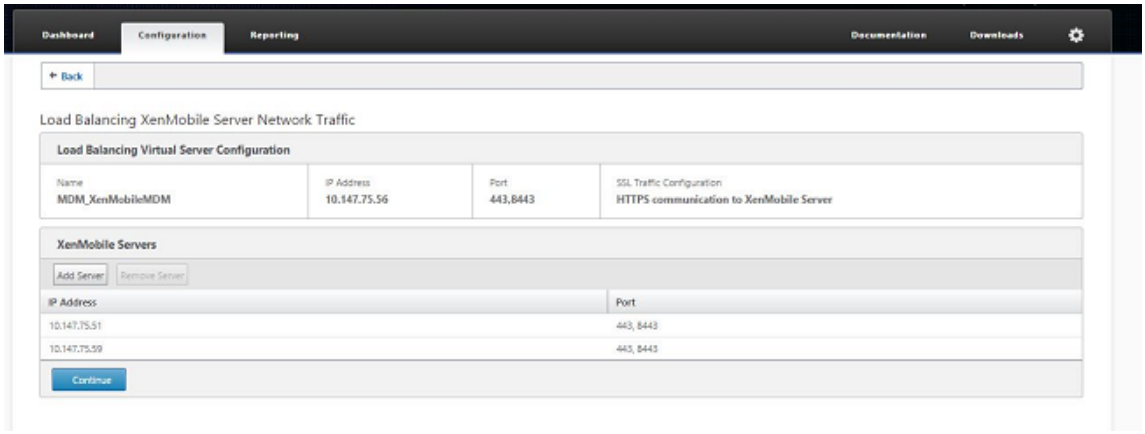


14. Insira o endereço IP a ser usado para o endereço IP de balanceamento de carga MDM e, em seguida, clique em **Continue**.

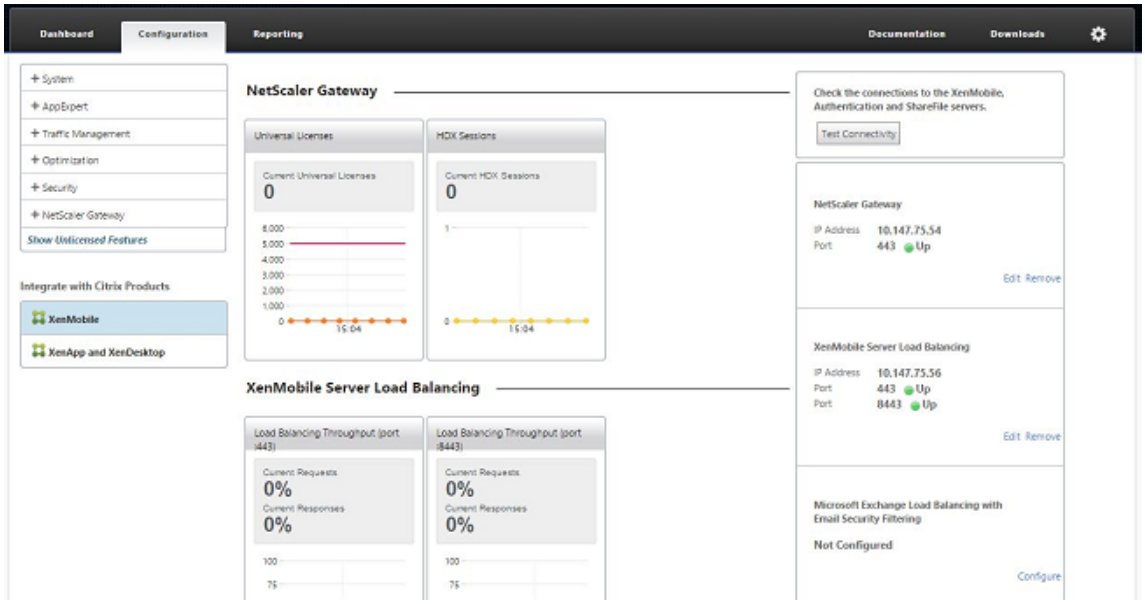
© 1999-2019 Citrix Systems, Inc. All rights reserved.



15. Depois que você vir os nós do XenMobile na lista, clique em **Continue** e, em seguida, clique em Done para concluir o processo.

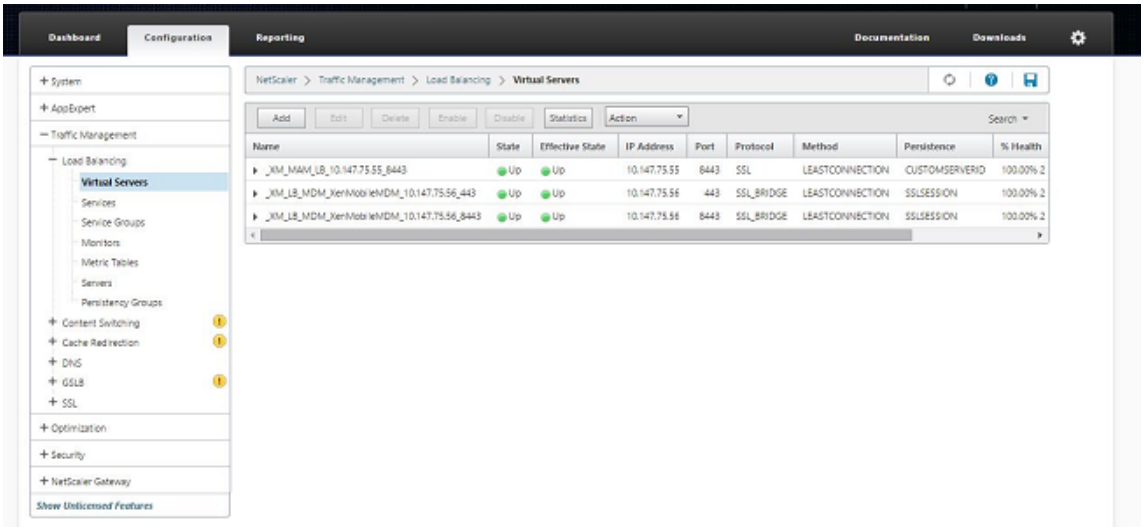


Você verá o status do endereço IP virtual na página XenMobile.

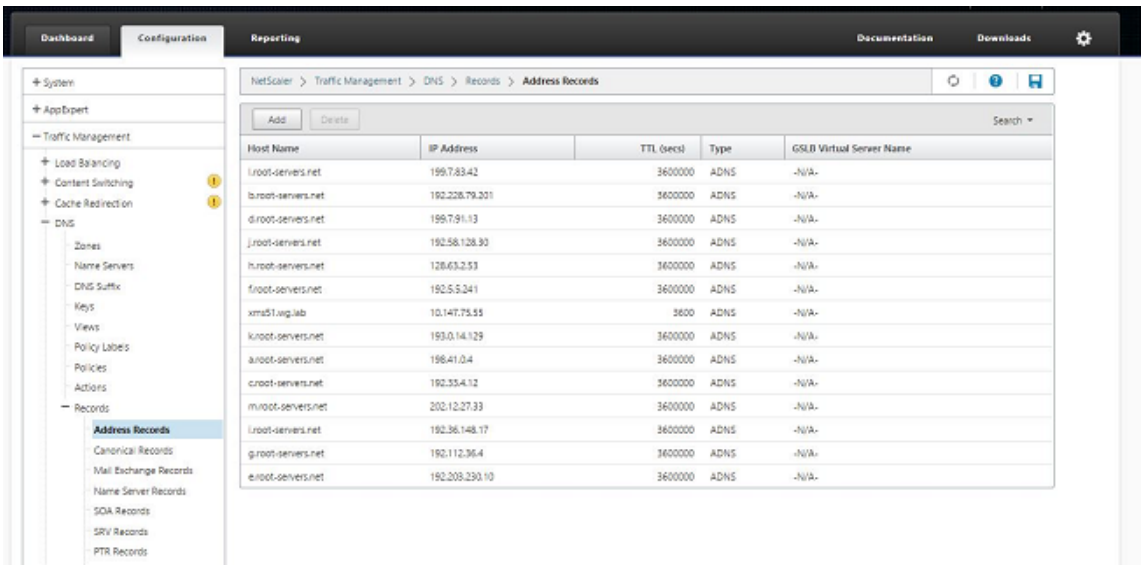


16. Para confirmar se os endereços IP virtuais estão em execução, clique na guia Configuration e navegue até **Traffic Management > Load Balancing > Virtual Servers**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Você também verá que a entrada DNS no NetScaler aponta para o endereço IP virtual do balanceamento de carga MAM.



Guia de recuperação de desastres

August 24, 2018

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais de recuperação de desastres usando uma estratégia de failover ativo-passivo. Para obter detalhes, consulte o artigo sobre Recuperação de desastres no manual de implantação do XenMobile.

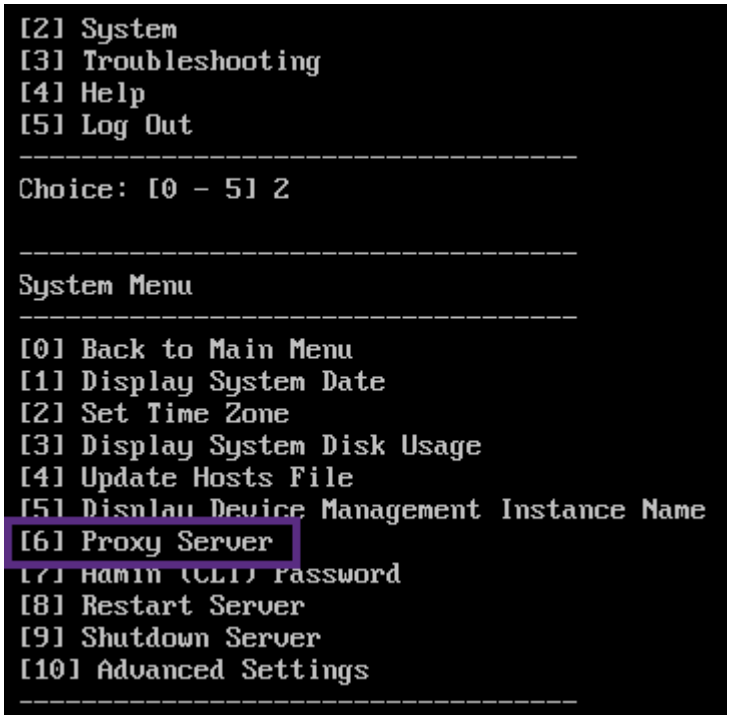
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ativar servidores proxy

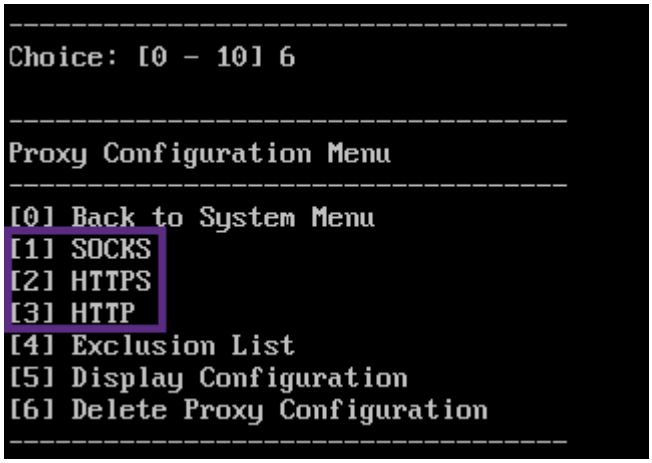
August 24, 2018

Para controlar o tráfego de saída da Internet, você pode configurar um servidor proxy no XenMobile para transportar o tráfego. Você configura um servidor proxy por meio da interface de linha de comando (CLI). Configurar o servidor proxy exige que você reinicie o sistema.

1. No menu principal da CLI do XenMobile, digite **2** para selecionar o menu System.
2. No menu System, digite **6** para selecionar o menu Proxy Server.



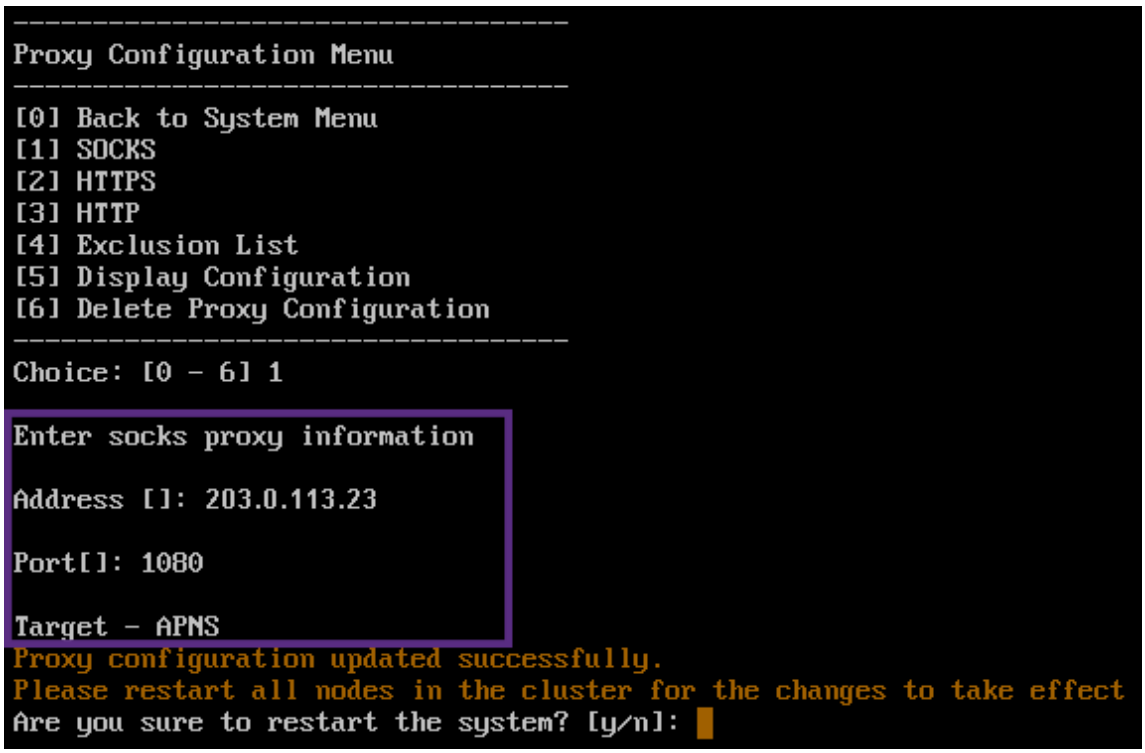
3. No menu Proxy Configuration, digite **1** para selecionar SOCKS, **2** para selecionar HTTPS ou **3** para selecionar HTTP.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

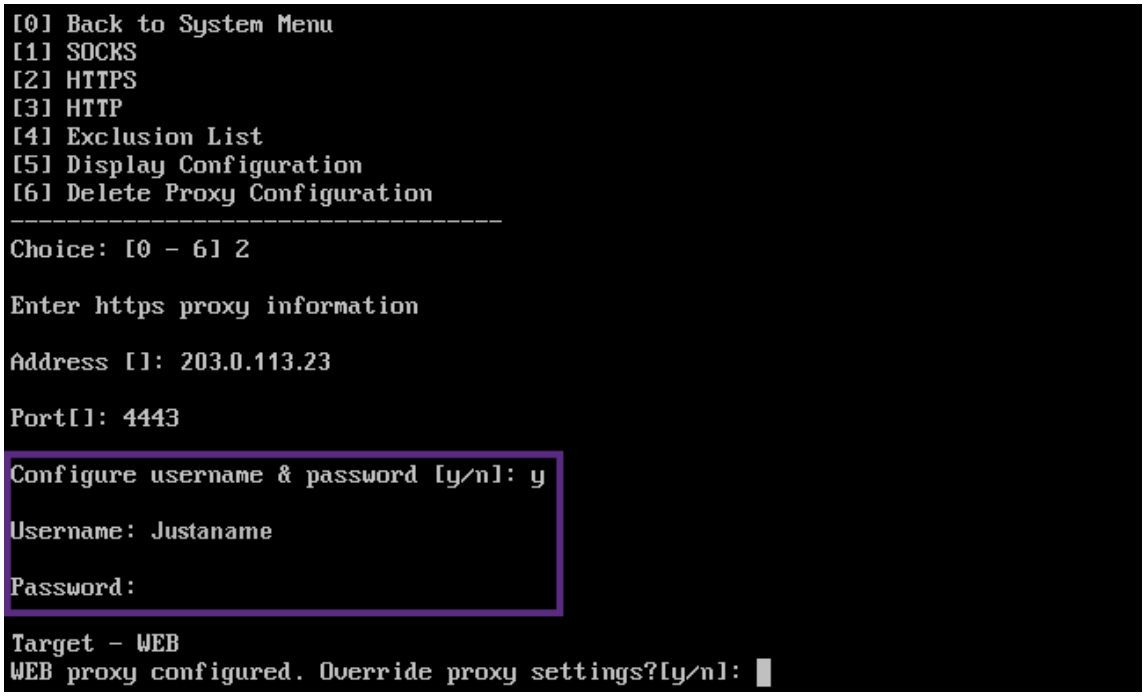
4. Digite o endereço IP, o número de porta e o destino do seu servidor proxy. Consulte a tabela a seguir para conhecer os tipos de destino compatíveis com cada tipo de servidor proxy.

Tipo de proxy	Destinos compatíveis
SOCKS	APNS
HTTP	APNS, Web. PKI
HTTPS	Web, PKI
HTTP com autenticação	Web, PKI
HTTPS com autenticação	Web, PKI



5. Se você optar por configurar um nome do usuário e uma senha para autenticação no servidor proxy, digite **y** e, em seguida, digite o nome do usuário e a senha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Digite **y** para terminar de configurar o servidor proxy.

Configurar SQL Server

March 6, 2019

Para conexões com o SQL Server de um XenMobile Server no local, você pode usar o driver padrão, jTDS ou o driver Microsoft Java Database Connectivity (JDBC). O driver jTDS é o driver padrão quando você:

- Instala o XenMobile Server no local.
- Atualize de um XenMobile Server configurado para usar o driver jTDS.

Para ambos os drivers, o XenMobile é compatível com a autenticação do SQL Server ou com a autenticação do Windows. Para essas combinações de autenticação e driver, o SSL pode estar ligado ou desligado.

Quando você usa a autenticação do Windows com o driver Microsoft JDBC, o driver usa a autenticação integrada com o Kerberos. O XenMobile contata o Kerberos para obter os detalhes do Centro de Distribuição de Chave (KDC) Kerberos. Se os detalhes necessários não estiverem disponíveis, a CLI do XenMobile solicita o endereço IP do servidor do Active Directory.

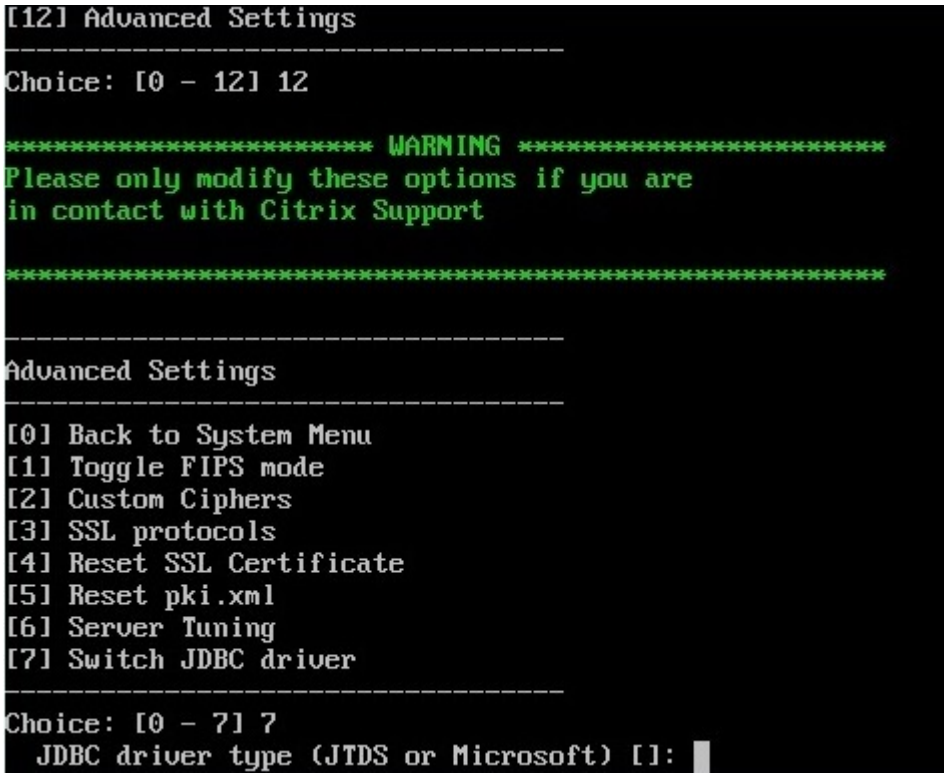
Para mudar do driver jTDS para o driver JDBC, use SSH para todos os nós do XenMobile Server e use o CLI do XenMobile para a configuração. As etapas variam acordo com a sua configuração do driver jTDS atual, da seguinte maneira.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mudar para Microsoft JDBC (autenticação do SQL Server)

Para concluir essas etapas, você precisa do nome de usuário do SQL Server e da senha.

1. Use SSH para todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o menu System.
3. Digite **12** para selecionar as configurações avançadas.
4. Digite **7** para selecionar mudar o driver JDBC e digite **m** para Microsoft.



5. Quando solicitado, digite **y** para escolher a autenticação SQL e, em seguida, digite o nome de usuário do SQL Server e a senha.
6. Repita as etapas para cada nó do XenMobile Server.
7. Reinicie cada nó do XenMobile Server.

Mudar para Microsoft JDBC (SSL está desativado; autenticação Windows)

Para concluir estas etapas, você precisa do nome e da senha do usuário do Active Directory, do realm Kerberos KDC e do nome de usuário KDC.

1. Use SSH para todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o menu System.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Digite **12** para selecionar as configurações avançadas.
4. Digite **7** para selecionar mudar o driver JDBC e digite **m**.
5. Quando solicitado 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 SQL Server.
7. Se o XenMobile não detectar automaticamente o realm Kerberos KDC, ele solicitará os detalhes KDC, incluindo o FQDN do SQL Server.
8. Quando solicitado se deseja usar SSL, digite **n**. XenMobile salva a configuração. Se o XenMobile não conseguir salvar a configuração devido a erros, ele mostra 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 XenMobile

Siga esta orientação para alterar a senha do banco de dados XenMobile, por exemplo, quando o Suporte Citrix direciona você para fazer uma alteração de senha.

> Importante:
>
> - Planeje uma janela de manutenção para alterar a senha do banco de dados. Uma alteração de senha deve ocorrer durante o tempo de inatividade do sistema.
> - Quando você alterar a senha, confirme que todos os nós do XenMobile estão 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. Você precisará reverter para a senha antiga no SQL Server, reiniciar o XenMobile e alterar a senha novamente.
> - Se o SQL Server usar a autenticação do Windows, faça a alteração da senha do banco de dados no Windows Active Directory.

1. Verifique se todos os nós do XenMobile Server estão em execução. Para um ambiente em cluster, coloque todos os nós em operação.
2. Bloqueie o tráfego de entrada de dispositivos para o XenMobile no balanceador de carga Netscaler desativando os vServers.
3. Para alterar a senha do banco de dados no SQL Server: faça login na CLI do XenMobile, navegue até **Configuração > Banco de dados** e insira a senha alterada quando solicitado:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
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 entrada dos dispositivos ativando os vServers no balanceador de carga do NetScaler.

Propriedades do servidor

March 6, 2019

O XenMobile apresenta muitas propriedades que se aplicam a operações de 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 configuradas com mais frequência, consulte Propriedades do servidor no manual virtual do XenMobile.

Definições de propriedade de servidor

Adicionar dispositivo sempre

- Se **true**, o XenMobile adiciona um dispositivo ao console XenMobile, mesmo que o processo de registro falhe, para que você possa ver quais dispositivos tentaram se registrar. O padrão é **false**.

Intervalo de limitação de emissão de certificado do cliente AG

- O período de tolerância entre a geração de certificados. Esse intervalo impede que o XenMobile gere vários certificados para um dispositivo em um curto período. A Citrix recomenda não alterar esse valor. O padrão é **30** minutos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tempo de execução de limpeza do log de auditoria

- A hora do início da limpeza do log de auditoria, formatado como HH:MM AM/PM. Exemplo: 04:00 AM. O padrão é **02:00 AM**.

Intervalo de limpeza de log de auditoria (em dias)

- O número de dias durante os quais o XenMobile mantém o log de auditoria. O padrão é **1**.

Agente de log de auditoria

- Se for **False**, a propriedade não registrará os eventos da interface do usuário (IU). O padrão é **false**.

Retenção de log de auditora (em dias)

- O número de dias durante os quais o XenMobile mantém o log de auditoria. O padrão é **7**.

auth.ldap.connect.timeout e auth.ldap.read.timeout

- Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do 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 da conexão LDAP**
  - Chave: **chave personalizada**
  - Chave: **auth.ldap.read.timeout**
  - Valor: **60000**
  - Nome de exibição: **auth.ldap.read.timeout**
  - Descrição: **tempo limite de leitura do LDAP**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Renovação de certificado em segundos

- O número de segundos antes que um certificado expire quais o XenMobile começa a renovar os certificados. Por exemplo, se um certificado expirará 30 de dezembro e esta propriedade é se 30 dias: se o dispositivo se conecta entre 1 de dezembro e 30 de dezembro, o XenMobile tenta renovar o certificado. O padrão é **2592000** segundos (30 dias).

Tempo limite de conexão

- O limite de inatividade de sessão, em minutos, após o qual o XenMobile fecha a conexão TCP a um dispositivo. A sessão permanece aberta. Aplica-se aos dispositivos Android e Windows CE e suporte remoto. O padrão é **5** minutos.

Tempo limite de conexão ao servidor de certificação Microsoft

- O número de segundos durante o qual o XenMobile espera por uma resposta do servidor de certificado. Se o servidor de certificados for lento e tiver uma grande quantidade de tráfego, você poderá aumentar esse valor para 60 segundos ou mais. Um servidor de certificado que não responde após 120 segundos precisa de manutenção. Padrão é **15000** milissegundos (15 segundos).

Canal de implantação padrão

- Determina como o XenMobile implanta um recurso com um dispositivo: no nível do usuário (**DEFAULT_TO_USER**) ou no nível de dispositivo. O padrão é **DEFAULT_TO_DEVICE**.

Implantar limpeza de log (em dias)

- O número de dias durante os quais o XenMobile deve manter o log de implantação. O padrão é **7**.

Desativar verificação de nome de host

- Por padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar com o servidor VPP: o nome de host ‘192.0.2.0’ não corresponde à entidade do certificado fornecida pelo par correspondente”. Se a verificação do nome do host interromper sua implantação, altere essa propriedade para **true**. O padrão é **false**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Desativar verificação do servidor SSL

- Se o valor for **True**, desativará a validação de certificado de servidor SSL quando todas as seguintes condições forem atendidas:
  - Você ativou a autenticação baseada em certificado no seu XenMobile Server
  - O servidor Microsoft CA é o emissor do certificado
  - Uma AC interna, em cuja raiz o XenMobile Server não confia, assinou o seu certificado.

O padrão é **true**.

Ativar console

- Se for **true**, permitirá o acesso do usuário ao console do Portal de autoajuda. O padrão é **true**.

Ativar relatórios de falhas

- Se for **true**, a Citrix coletará relatórios e diagnósticos de falhas para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se for **false**, não haverá coleta de dados. O valor padrão é **true**.

Ativar/desativar registro em log de estatísticas da hibernação para diagnóstico

- Se **true**, ativará o registro em log de estatísticas de Hibernação para ajudar na resoluçlão de problemas de desempenho de aplicativos. A Hibernação é um componente usado para conexões do XenMobile com o Microsoft SQL Server. Por padrão, o registro em log está desativado porque ele afeta o desempenho do aplicativo. Ative o registro em log por pouco tempo somente 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**.

Ativar OTAE do macOS

- Se for **false**, impedirá o uso de um link de registro para dispositivos macOS, o que significa que os usuários do macOS só podem se registrar usando um convite para registro. O padrão é **true**.

Ativar notificação gatilho

- Ativa ou desativa as notificações de cliente do Secure Hub. O valor **true** ativa notificações. O padrão é **true**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

force.server.push.required.apps

- Permite a implantação forçada dos aplicativos necessários em dispositivos Android e iOS em situações como as seguintes:
  - Carregue um novo aplicativo e marque-o conforme necessário.
  - Marque um aplicativo existente conforme necessário.
  - Quando o usuário exclui um aplicativo necessário.
  - Está disponível uma atualização do Secure Hub.

A implantação forçada de aplicativos obrigatórios é **false** por padrão. Crie a chave personalizada e defina **Valor** como **true** para ativar a implantação forçada. Durante a implantação forçada, os aplicativos obrigatórios habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, são atualizados imediatamente. A atualização ocorre mesmo se você configurar uma política MDX para um período de tolerância de atualização do aplicativo e o usuário optar por atualizar o aplicativo posteriormente.

- Chave: **chave personalizada**
- Chave: **force.server.push.required.apps**
- Valor: **false**
- Nome de exibição: **force.server.push.required.apps**
- Descrição: **forçar a implantação dos aplicativos obrigatórios**

Recepção completa de usuários do ActiveSync permitidos e negados

- O intervalo (em segundos) em que o XenMobile recebe uma lista completa (linha de base) dos usuários do ActiveSync permitidos e negados. O padrão é **28800** segundos.

hibernate.c3p0.idle_test_period

- Essa propriedade do XenMobile Server, uma chave personalizada, determina o tempo ocioso em segundos antes de uma conexão ser validada automaticamente. Configure a chave da seguinte maneira. 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 de hibernação**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

hibernate.c3p0.max_size

- Essa chave personalizada determina o número máximo de conexões que o XenMobile pode abrir no banco de dados do SQL Server. O XenMobile usa o valor especificado para esta chave personalizada como um limite superior. As conexões abrem somente se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados. Para obter mais informações, consulte Ajuste das operações do XenMobile. Configure a chave da seguinte maneira. O padrão é **1000**.
- Chave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nome de exibição: **hibernate.c3p0.max_size**
- Descrição: **conexões de banco de dados ao SQL**

hibernate.c3p0.min_size

- Essa chave personalizada determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. Configure a chave da seguinte maneira. O padrão é **100**.
- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de exibição: **hibernate.c3p0.min_size**
- Descrição: **conexões de banco de dados ao SQL**

hibernate.c3p0.timeout

- Essa chave personalizada determina o tempo limite de ociosidade, 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**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 com falha consecutivos, ele desativará a telemetria. O padrão é **false**.

Tempo limite de inatividade em minutos

- Se a propriedade **Tipo de tempo limite de WebServices** for **INACTIVITY_TIMEOUT:** essa propriedade define o número de minutos após os quais o XenMobile faz logut de um administrador inativo que fez o seguinte:
  - Usou a API pública do XenMobile para serviços REST para acessar o console XenMobile.
  - Usou a API pública do XenMobile para serviços REST para acessar os aplicativos de terceiros. Um tempo limite de **0** significa que um usuário inativo permanece conectado.

O padrão é **5**.

Instalação automática de registro de gerenciamento de dispositivo iOS ativada

- Se for true, essa propriedade reduzirá a quantidade de interação do usuário durante o registro do dispositivo. Os usuários precisam clicar em **Instalação de autoridade de certificação raiz** (se necessário) e em **Instalação do perfil MDM**.

Primeira etapa do registro de gerenciamento de dispositivos iOS em atraso

- Depois que um usuário insere suas credenciais durante o registro de dispositivo, este especifica o período de tempo a aguardar antes de avisar para instalar a AC de raiz. A Citrix recomenda que você edite essa propriedade apenas se você tiver problemas de latência ou velocidade de rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

Última etapa do registro de gerenciamento de dispositivos iOS em atraso

- Durante o registro de dispositivo, este valor da propriedade especifica o período de tempo de espera entre instalar o perfil MDM e iniciar o agente no dispositivo. A Citrix recomenda que você edite essa propriedade apenas se você tiver problemas de latência ou velocidade de rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Modo de entrega de identidade de gerenciamento de dispositivo iOS

- Especifica se o XenMobile distribui o certificado do MDM para dispositivos usando **SCEP** (recomendado por motivos de segurança) ou **PKCS12**. No modo de PKCS12, o par de chaves é gerado no servidor e nenhuma negociação é realizada. O padrão é **SCEP**.

Gerenciamento de dispositivo iOS tamanho de chave de identidade

- Define o tamanho das chaves privadas para identidades MDM, o serviço de perfil de iOS e identidades de agente do XenMobile iOS. O padrão é **1024**.

Gerenciamento de dispositivo iOS dias de renovação de identidade

- Especifica o número de dias antes da expiração do certificado que o XenMobile começa a renovação de certificados. Por exemplo: se um certificado expirar em 10 dias e esta propriedade for **10** dias, se um dispositivo se conectar 9 dias antes da expiração, o XenMobile emitirá um novo certificado. O padrão é **30** dias.

Senha da chave privada de iOS MDM APNS

- Essa propriedade contém a senha de APNs, que é necessária para o XenMobile para notificações por push para os servidores da Apple.

Período de inatividade antes que o dispositivo seja desconectado

- Especifica o tempo que 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

- Essa chave personalizada limita o número de dispositivos somente MAM que cada usuário pode registrar. Configure a chave da seguinte maneira. Um **Valor** de **0** permite registros ilimitados de dispositivos.
- Chave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nome para exibição = **MAM Only Device Max**
- Descrição = **limita o número de dispositivos MAM que cada usuário pode registrar.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

MaxNumberOfWorker

- O número de threads utilizados ao importar um várias licenças VPP. 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 VPP resulta em uso de CPU muito alto.

Single Sign-On do NetScaler

- Se for **false**, desativará o recurso de retorno de chamada do XenMobile durante o logon único do NetScaler para XenMobile. Se a configuração de NetScaler Gateway incluir uma URL de retorno de chamad, o XenMobile usa o recurso de retorno de chamada para verificar o ID da sessão do NetScaler Gateway. O padrão é **false**.

Número de uploads com falha consecutivos

- Exibe o número de falhas consecutivas durante uploads do Programa de aperfeiçoamento da experiência do cliente (CEIP). O XenMobile incrementa o valor quando um upload falha. Após 15 falhas de upload, o XenMobile desativa o CEIP, também conhecido como telemetria. Para obter mais informações, consulte a propriedade de servidor **Identifica se a telemetria está ativada ou não**. O XenMobile redefine o valor como **0** quando o 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**.

Recepção de alteração Incremental dos usuários permitidos e negados

- O número de segundos durante o qual o XenMobile espera por uma resposta do domínio ao executar um comando do PowerShell para obter um delta de dispositivos do ActiveSync. O padrão é **60** segundos.

Tempo limite de leitura para o servidor de certificação Microsoft

- O número de segundos durante o qual o XenMobile espera por uma resposta do servidor de certificado ao executar uma leitura. Caso o servidor de certificados seja lento e tenha uma grande quantidade de tráfego, você pode aumentar esse valor para 60 segundos ou mais. Um servidor

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de certificado que não responde após 120 segundos precisa de manutenção. Padrão é **15000** milissegundos (15 segundos).

Serviços Web REST

- Ativa 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 exportações de dispositivo. 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 de exportações e buscas da lista de dispositivos, mas pode reduzir a memória disponível. O padrão é **1000**.

Limpeza do log de sessões (em dias)

- O número de dias durante os quais o XenMobile deve manter o log de sessão. O padrão é **7**.

Modo de servidor

- Determina se o XenMobile é executado no modo MAM, MDM ou ENT (Enterprise), correspondente ao gerenciamento de aplicativo, gerenciamento de dispositivo ou gerenciamento de aplicativo e dispositivo. Defina a propriedade Modo de Servidor de acordo com a forma como você deseja que os dispositivos sejam registrados, conforme indicado na tabela abaixo. O padrão do Modo de Servidor é **ENT**, independentemente do tipo de licença.

Se você tiver uma licença XenMobile MDM Edition, o modo de servidor efetivo é sempre MDM, independentemente da forma como você definir o modo de servidor em Propriedades do servidor. Se você tiver uma licença do MDM Edition, não poderá ativar o gerenciamento de aplicativo 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 de Servidor como
Enterprise / Advanced	Modo MDM	MDM
Enterprise / Advanced	Modo MDM+MAM	ENT
MDM	Modo MDM	MDM

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O modo de servidor efetivo é uma combinação do tipo de licença e do modo de servidor. Para obter uma licença de MDM, o modo de servidor efetivo é sempre MDM, independentemente da configuração do modo de servidor. Para as licenças Enterprise e Advanced, o modo de servidor efetivo corresponde ao modo de servidor, se o modo de servidor é **ENT** ou **MDM**. Se o modo de servidor é **MAM**, o modo de servidor efetivo é ENT.

O XenMobile adiciona o modo de servidor ao log do servidor para cada uma dessas atividades: uma licença é ativada ou excluída, e quando você altera o modo de servidor nas Propriedades do Servidor. Para obter informações sobre como criar e exibir arquivos de log, consulte Logs e Exibir e analisar arquivos de log no XenMobile.

Tipo de configuração do ShareFile

- Especifica o tipo de armazenamento do ShareFile. **ENTERPRISE** ativa o modo ShareFile Enterprise. **CONNECTORS** fornece acesso somente para StorageZone Connectors que você cria por meio do console XenMobile. O padrão é **NONE**, que mostra a exibição inicial da tela **Configurar > ShareFile** em que você escolhe entre ShareFile Enterprise e Connectors. O padrão é **NONE**.

Tempo limite estático em minutos

- Se a propriedade **Tipo de tempo limite de WebServices** for **STATIC_TIMEOUT:** essa propriedade define o número de minutos após os quais o XenMobile faz logout de um administrador depois de usar o seguinte:
  - A API pública do XenMobile para serviços REST para acessar o console XenMobile.
  - A API pública do XenMobile para serviços REST para acessar qualquer aplicativo de terceiro.

O padrão é **60**.

Disparar supressão de mensagem de agente

- Ativa ou desativa as mensagens de cliente do Secure Hub. O valor **false** ativa as mensagens. O padrão é **true**.

Disparar supressão de som de agente

- Ativa ou desativa os sons de cliente do Secure Hub. O valor **false** ativa os sons. O padrão é **true**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Download de aplicativo não autenticado para dispositivos Android

- Se for **true**, você poderá baixar aplicativos auto-hospedados para dispositivos Android que executam o Android for Work. O XenMobile precisa dessa propriedade se a opção do Android for Work para fornecer estaticamente uma URL de download na Google Play Store estiver ativada. Nesse caso, as URLs de download não poderão incluir um tíquete de uso único (definido pela propriedade **XAM One-Time Ticket server**) que possua o token de autenticação. O padrão é **false**.

Download de aplicativo não autenticado para dispositivos Windows

- Usada somente para as versões mais antigas do Secure Hub que não validam tíquetes de uso único. Se for **false**, você poderá baixar aplicativos não autenticados do XenMobile para dispositivos Windows. O padrão é **false**.

Usar ID do ActiveSync para realizar um exclusão de dispositivo ActiveSync

- Se for **true**, o conector Endpoint Management para Exchange ActiveSync usará o identificador do ActiveSync como argumento para o método asWipeDevice. O padrão é **false**.

Propriedades do dispositivo definidas pelo usuário N

- Usada somente em dispositivos Windows CE. Essa chave personalizada permite obter as propriedades que você cria no Registro de dispositivos Windows CE. Depois que essas propriedades estiverem no banco de dados do XenMobile, você poderá criar regras de implantação com base em seus valores.
- Chave: **chave personalizada**
- Chave: **device.properties.userDefinedN**
- Valor: *definido pelo administrador*
- Nome de exibição: *definido pelo administrador*
- Descrição: *definida pelo administrador*

Usuários somente do Exchange

- Se for **true**, desativará a autenticação de usuário para usuários do ActiveSync Exchange. O padrão é **false**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Intervalo de linha de base do VPP

- O intervalo mínimo em que o XenMobile reimporta licenças do VPP da Apple. A atualização de informações de licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado do VPP. Por padrão, o XenMobile atualiza a linha de base da licença do VPP no mínimo a cada **720** minutos.

Se você tem muitas licenças do VPP 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 de importação de licenças. Se você espera mudanças frequentes de licenças do VPP da Apple: a Citrix recomenda reduzir o valor para manter o XenMobile atualizado com essas mudanças. O intervalo mínimo entre duas linhas de base é de 60 minutos. Além disso, o XenMobile realiza uma importação delta a cada 60 minutos para capturar as alterações desde a última importação. Portanto, se o intervalo de linha de base do VPP for de 60 minutos, o intervalo entre linhas de base poderá ser atrasado até 119 minutos.

Tipo de tempo limite do WebServices

- Especifica a expiração de um token de autenticação obtido na API pública. Se **STATIC_TIMEOUT**, o XenMobile considerará um token de autenticação como expirado após o valor especificado na propriedade de servidor **Static Timeout in Minutes**.

Se **INACTIVITY_TIMEOUT**, o XenMobile considerará um token de autenticação como expirado após o valor especificado na propriedade de servidor **InactivityTimeout in Minutes**. O padfrão é **STATIC_TIMEOUT**.

Validade estendida (5 anos) de certificado do Windows Phone MDM Windows Phone certificado do MDM

- O período de validade do certificado do dispositivo emitido por MDM para Windows Phone e Tablet. Os dispositivos usam um certificado de dispositivo para se autenticar no servidor MDM durante o gerenciamento de dispositivo. Se o valor for **true**, o período de validade será de cinco anos. Se o valor for **false**, o período de validade será de dois anos. O padrão é **true**.

Canal Windows WNS - Número de dias antes da renovação

- A frequência de renovação para ChannelURI. O padrão é **10** dias.

Intervalo de pulsação do Windows WNS

- O tempo de espera do XenMobile antes de se conectar a um dispositivo, depois de se conectar a ele a cada três minutos cinco vezes. O padrão é **6** horas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tíquete de uso único XAM

- O número de milissegundos durante os quais um token de autenticação de uso único (OTT) é válido para baixar um aplicativo. Essa propriedade funciona com as propriedades **Unauthenticated App download for Android** e **Unauthenticated App download for Windows**. Essas propriedades especificam se devem ser permitidos dowloads de aplicativos não autenticados. O padrão é **3600000**.

Intervalo inativo máximo de console do portal de autoajuda XenMobile MDM (minutos)

- O número de minutos após os quais o XenMobile faz logoff de um usuário inativo do portal de autoajuda XenMobile. Um tempo limite de **0** significa que um usuário inativo permanece conectado. O padrão é **30**.

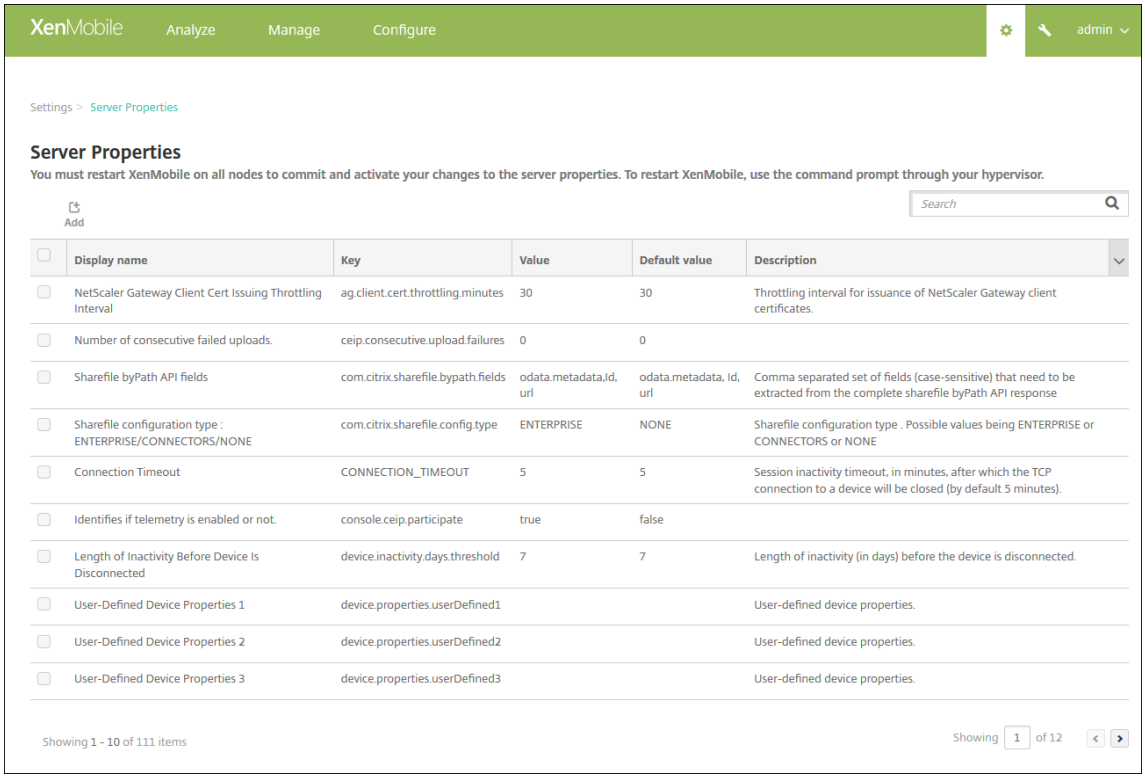
Adição, edição ou exclusão de propriedades do servidor

No XenMobile, você pode aplicar propriedades ao servidor. Depois de fazer alterações, você deverá reiniciar o XenMobile em todos os nós para confirmar e ativar as alterações.

> Nota:
>
> Para reiniciar o XenMobile, use o prompt de comando por meio do seu hipervisor.

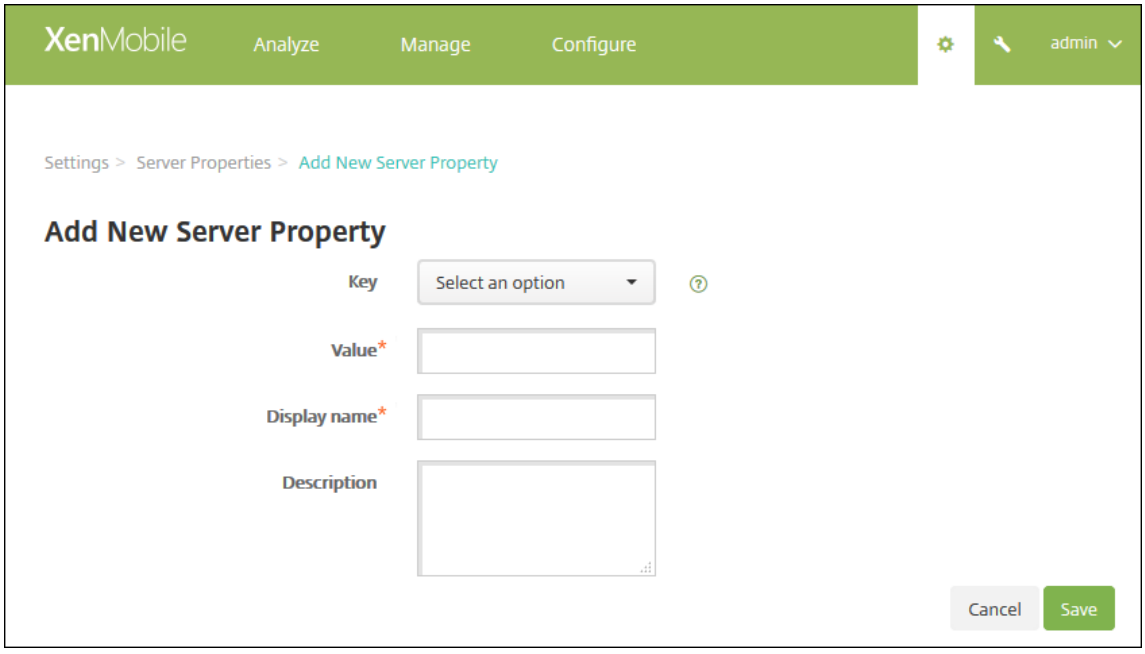
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Propriedades do servidor**. A página **Propriedades do servidor** é exibida. Você pode adicionar, editar ou excluir propriedades do servido nessa página.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para adicionar uma propriedade de servidor

1. Clique em **Adicionar**. A página **Adicionar Nova Propriedade de Servidor** é exibida.



2. Defina estas configurações:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Chave: na lista, selecione a chave adequada. As chaves diferenciam maiúsculas de minúsculas. Entre em contato com o suporte da Citrix antes de editar os valores de propriedade ou para solicitar uma chave especial.
- Valor: insira um valor de acordo com a chave selecionada.
- Nome para exibição: insira um nome para o valor da nova propriedade que é exibido na tabela **Propriedades do servidor**.
- Descrição: opcionalmente, digite uma descrição para a nova propriedade de servidor.

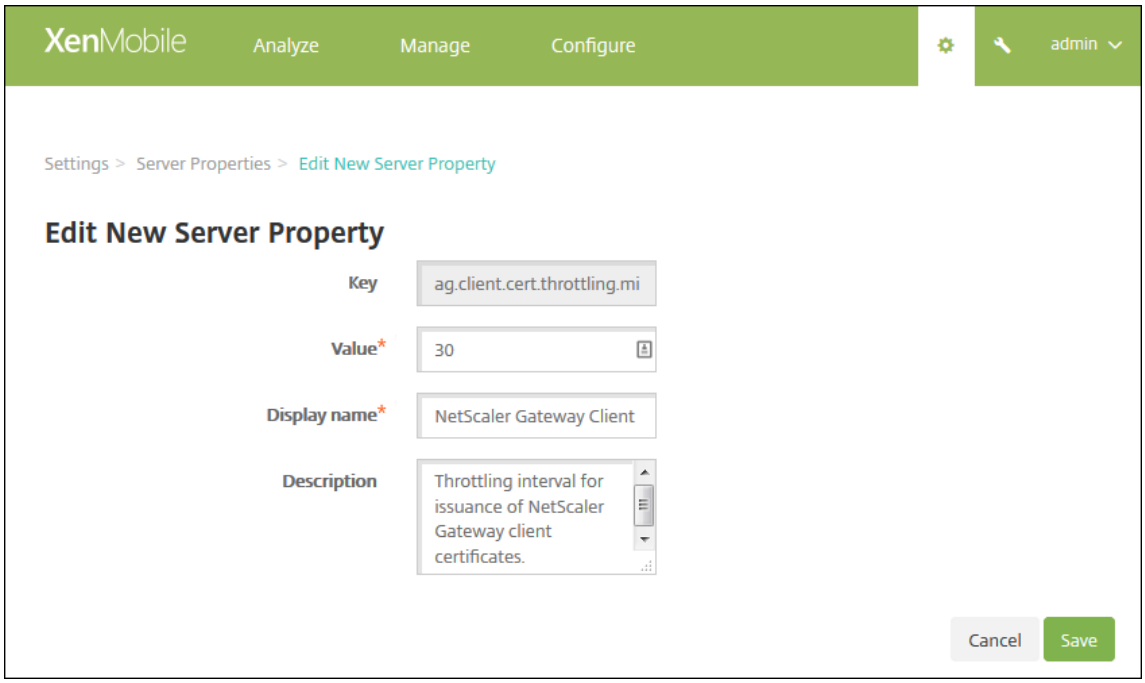
3. Clique em **Salvar**.

Para editar uma propriedade de servidor

1. Na tabela **Propriedades do servidor**, selecione a propriedade de servidor que você desejar editar.

   Quando você marca a caixa de seleção ao lado de uma propriedade de servidor, o menu de opções é exibido 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 **Edit**. A página **Editar nova propriedade de servidor** é exibida.



3. Altere as seguintes informações conforme apropriado:

   - Chave: você não pode alterar esse campo.
   - Valor: o valor da propriedade.
   - Nome de exibição: o nome da propriedade.
   - Descrição: a descrição da propriedade.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir uma propriedade de servidor

1. Na tabela **Propriedades do servidor**, selecione a propriedade de servidor que você desejar 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.

Opções da interface de linha de comando

April 15, 2019

Para uma instalação no local do XenMobile Server, você pode acessar as opções de CLI da seguinte maneira:

- **No hipervisor em que você instalou o XenMobile:** No seu hipervisor, selecione a máquina virtual XenMobile importada, inicie a exibição do prompt de comando e faça login na sua conta de administrador para o XenMobile. Para obter detalhes, consulte a documentação do hipervisor.
- **Se o SSH estiver habilitado no seu firewall, usando SSH:** Faça logon na sua conta de administrador para o XenMobile.

Você pode executar uma variedade de tarefas de configuração e resolução de problemas por meio do CLI. A figura a seguir mostra o menu de nível superior da CLI .



Opções de configuração

Veja a seguir exemplos do **Menu Configuration** e as configurações exibidas para cada opção.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```

[1] Network

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

[2] 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...
```

[3] Database

```
  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]:
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

[4] Listener Ports

```
 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 clustering

Veja a seguir exemplos do **Menu Clustering** 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
-----------------------------------
```

[1] Show Cluster Status

```
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
```

[2] Enable/Disable cluster

Quando você opta por ativar clusters, a seguinte mensagem é exibida:

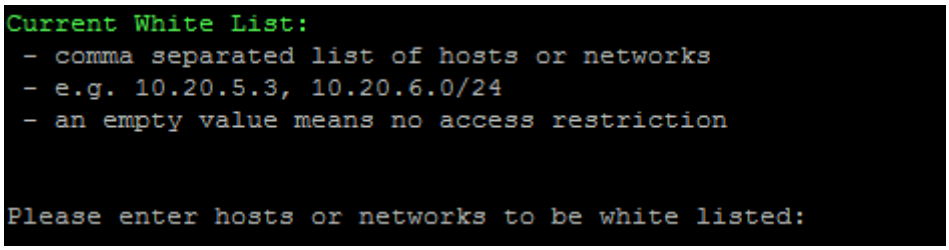
```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

Quando você opta por desativar clusters, a seguinte mensagem é exibida:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```

[3] Cluster member white list



[4] Enable or disable SSL offload

Quando você seleciona ativar ou desativar a descarga de SSL, a seguinte mensagem é exibida:

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster

Quando você seleciona exibir o Hazelcast Cluster, as seguintes opções são exibidas:

Membros do cluster Hazelcast:

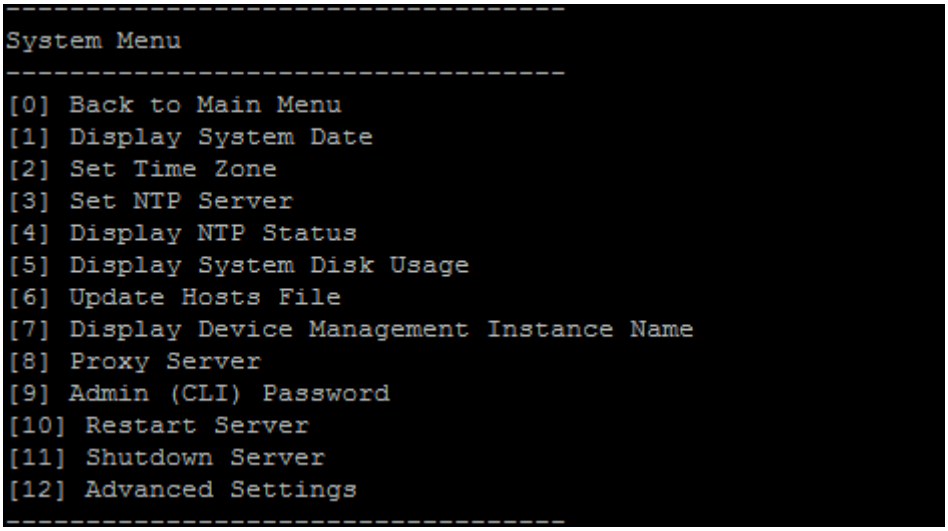
[[Endereços IP listados]]

> Nota:
>
> Se um nó configurado não fizer parte do cluster, reinicie o nó.

Opções do sistema

No **Menu System**, você pode exibir ou definir informações no nível do sistema, reiniciar ou desligar o servidor, ou ter acesso ao menu **Advanced Settings**.

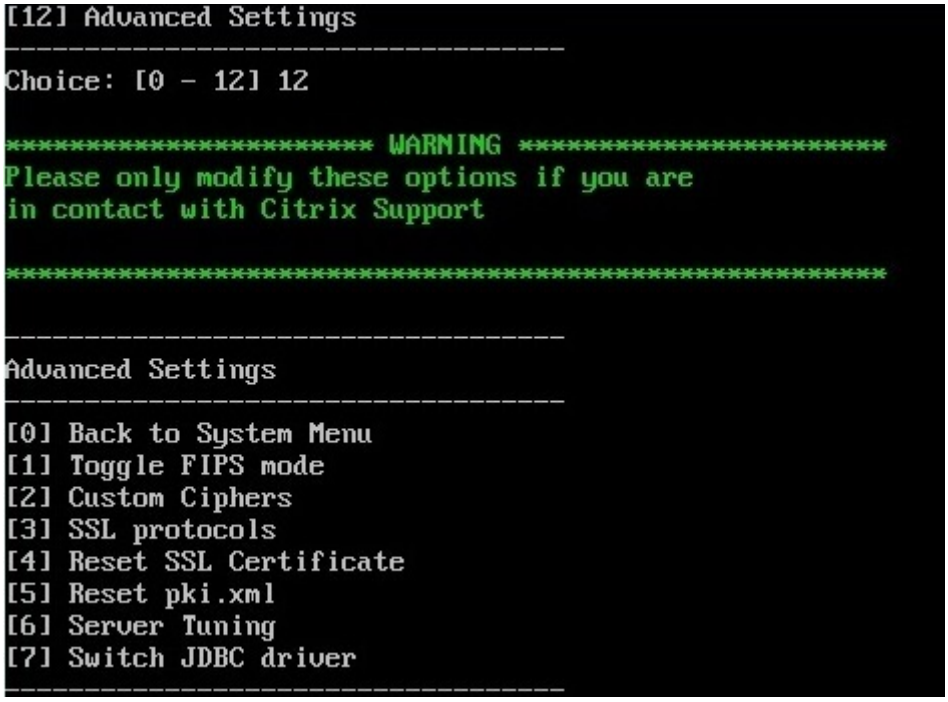
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Set NTP Server permite que você especifique as informações do servidor NTP. Se você tiver problemas de fuso horário ao sincronizar o horário do XenMobile com um hipervisor, você pode evitar esses problemas apontando o XenMobile para um servidor NTP. Reinicie todos os servidores de cluster após alterar essa opção.

Você também pode verificar o espaço em disco exibindo o item de menu **[5]Display System Disk Usage**.

[12] Advanced Settings



As opções de **Protocolos SSL** definem como padrão todos os protocolos permitidos. Após o aviso de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

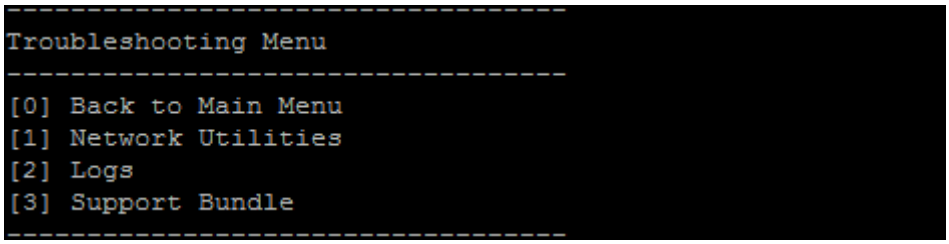
ativação **New SSL protocols to enable**, digite os protocolos que deseja ativar. O XenMobile desativará todos os protocolos que você não incluir na sua resposta. Por exemplo: para desativar TLSv1, digite **TLSv1.2,TLSv1.1** e, em seguida, digite **y** para reiniciar o XenMobile Server.

As opções de **Server Tuning** incluem o tempo limite de conexão do servidor, o máximo de conexões (pela porta) e o máximo de threads (pela porta).

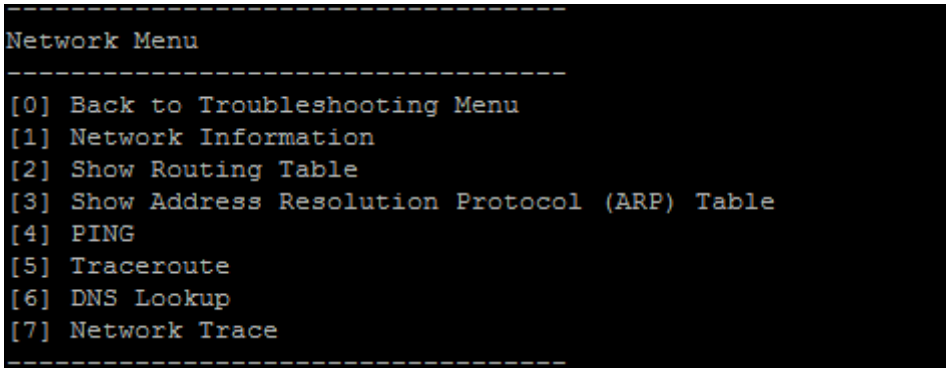
As opções de **Switch JDBC driver** são JDBC **jTDS** e **Microsoft**. O driver padrão é jTDS. Para obter informações sobre como alternar para o driver Microsoft JDBC, consulte Drivers do SQL Server.

Opções de solução de problemas

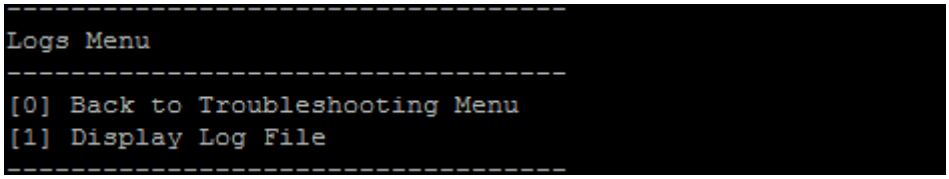
Veja a seguir é exemplos do **Menu Troubleshooting** e as configurações exibidas para cada opção.



[1] Network Utilities



[2] Logs



© 1999-2019 Citrix Systems, Inc. All rights reserved.

[3] Support Bundle

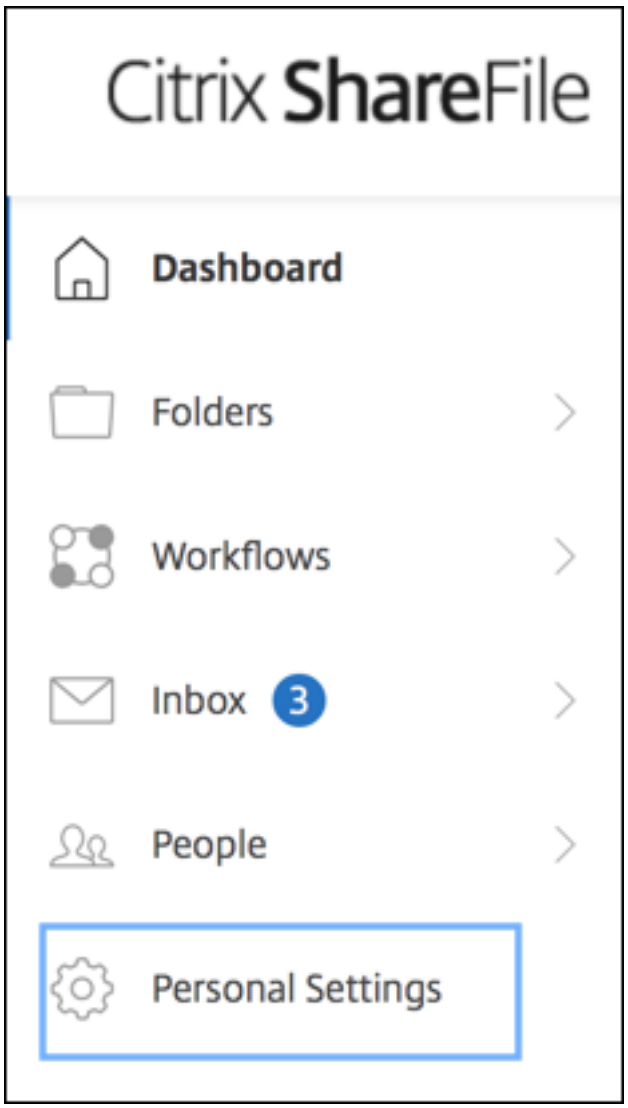
```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

Para carregar um pacote de suporte usando o ShareFile como o site FTP

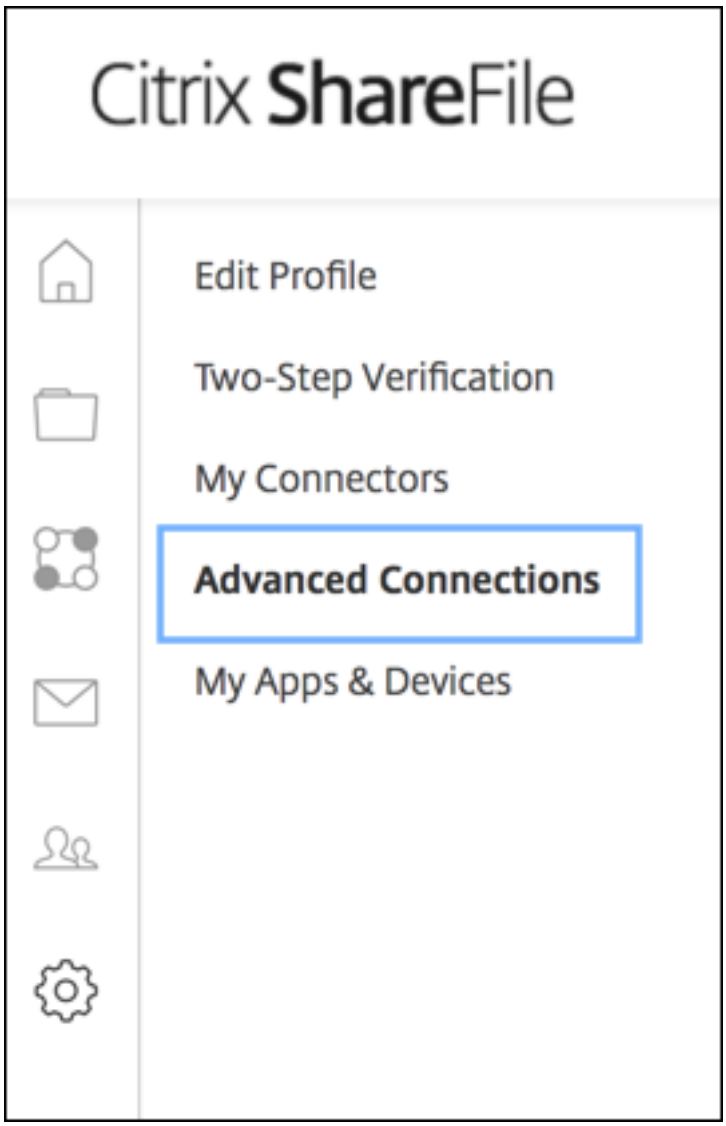
Antes de iniciar o carregamento de um pacote de suporte, configure os pré-requisitos a seguir no ShareFile:

1. Verifique os detalhes do login do FTP.
   a. Em um navegador da Web, abra https://citrix.sharefile.com.
   b. Clique em **Configurações pessoais** e depois clique em **Conexões avançadas**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

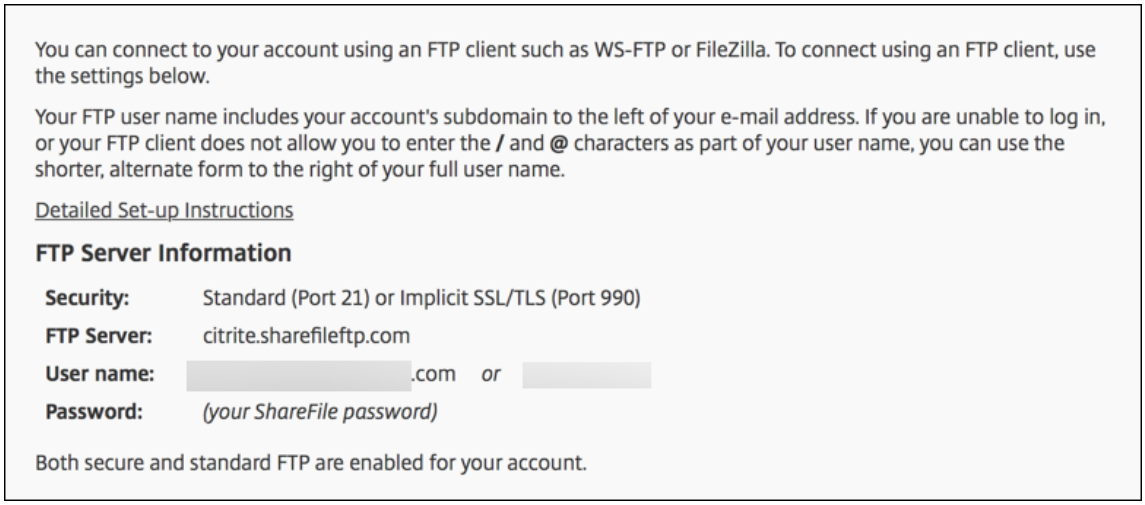


© 1999-2019 Citrix Systems, Inc. All rights reserved.



c. Nas informações do servidor FTP, em Nome do usuário, verifique se um ID de usuário alfanumérico é exibido, juntamente com os detalhes de subdomínio/nome de usuário padrão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

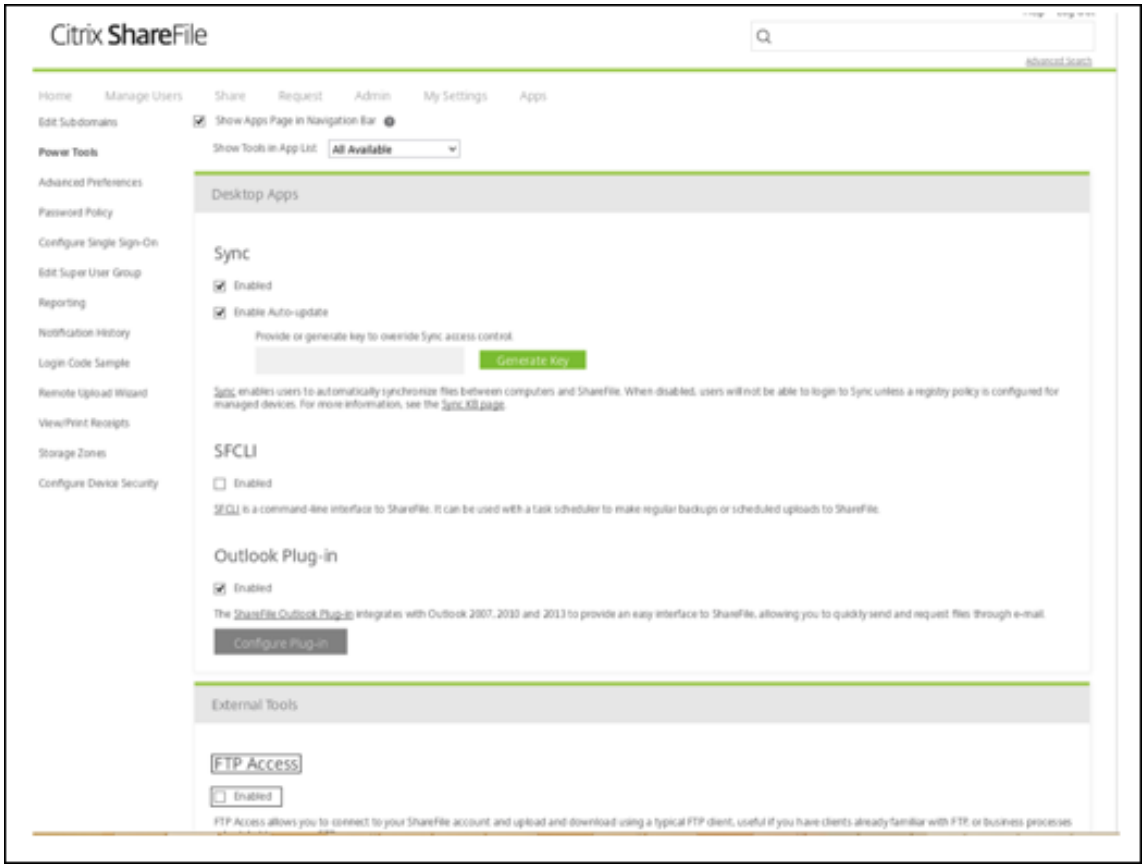


> **Notas:**
>
> - Como você está carregando um arquivo do XenMobile, que é um cliente FTP baseado em Linux CLI, não é possível inserir caracteres de barra invertida (/) e arroba (@) como parte de seu nome de usuário.
> - Se você não vir o ID de usuário alfanumérico, poderá solicitar esse ID de usuário ao administrador do ShareFile ou ao suporte do ShareFile.

2. Verifique se o servidor ShareFile está habilitado para comunicação FTP juntamente com FTPS. Idealmente, os administradores do ShareFile permitem que uma conta de usuário seja aberta para comunicação por FTP. Às vezes, no entanto, apenas a comunicação FTPS é permitida.

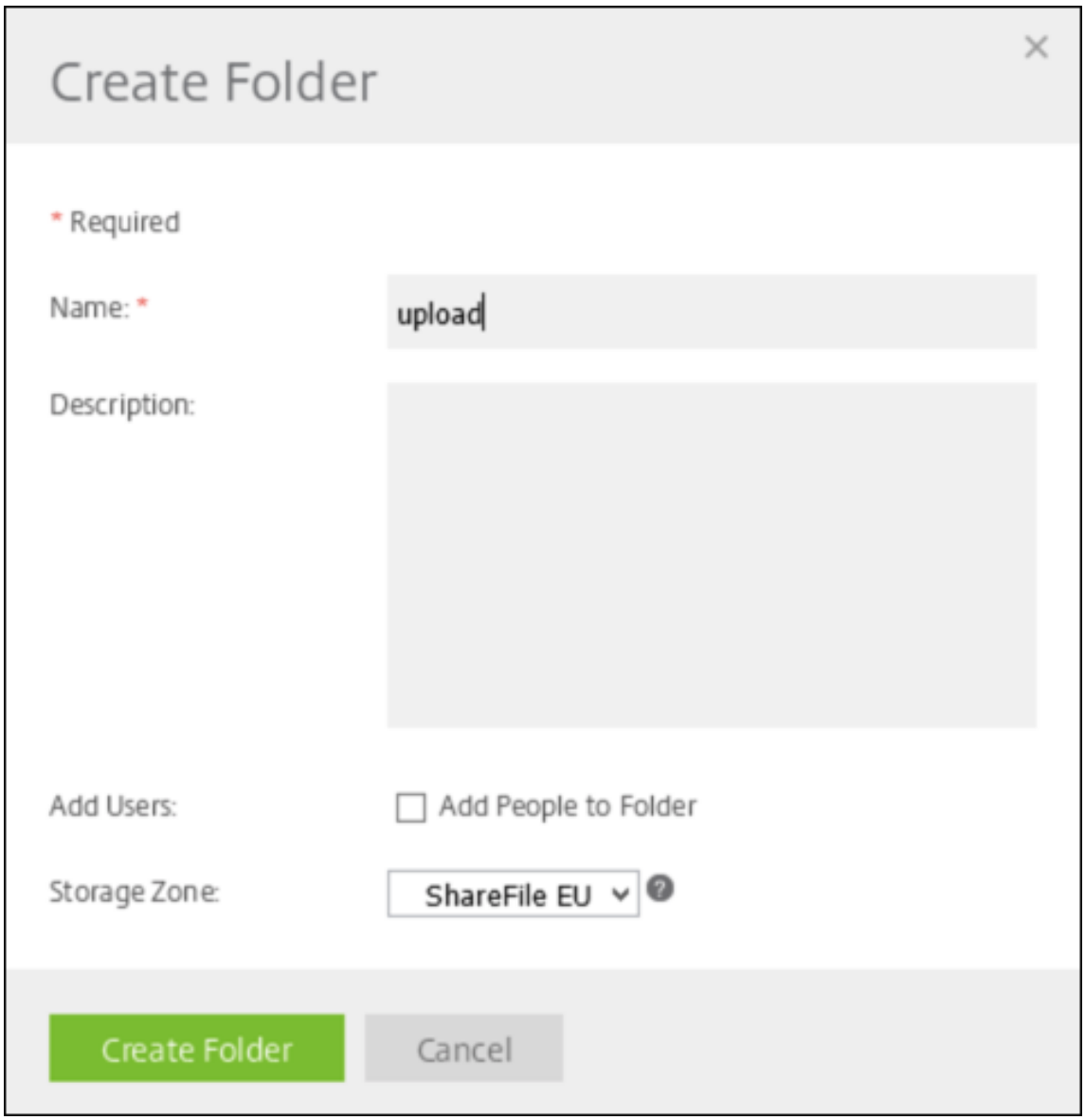
   Um usuário com direitos de administrador pode verificar e ativar essa configuração clicando em **Configurações**, **Configurações de administrador**, **Preferências avançadas** e, depois, em **Ativar ferramentas do ShareFile.** Em **Aplicativos externos**, **Acesso por FTP**, a caixa de seleção **Ativar** deve estar marcada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Crie uma pasta compartilhada para o cliente FTP usar como um diretório para o carregamento de arquivo. Clique em **Página inicial**, **Pastas** e depois clique em **Pastas pessoais**.
4. No canto direito, clique no ícone de sinal de adição (+), clique em **Criar pasta** e insira um nome para a pasta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Na CLI do XenMobile Server, no **Menu principal**, selecione **Solução de problemas > Pacote de suporte**. Em **Support Bundle Menu**, selecione **Generate Support Bundle**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Se houver um pacote de suporte existente, quando solicitado, digite **y** para substituir o pacote.

6. Carregue o pacote de suporte para o servidor FTP:

   uma. Selecione **Upload Support Bundle by using FTP**.

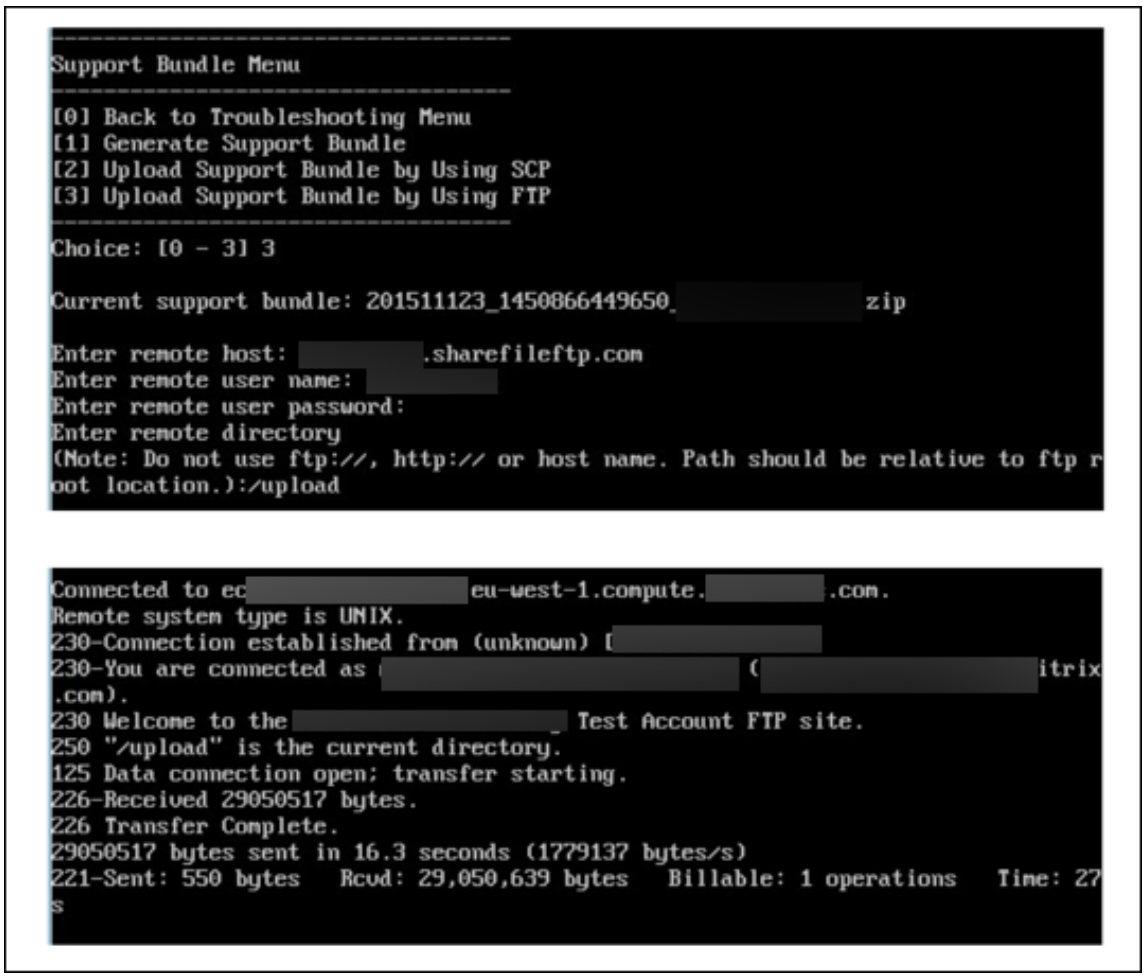
   b. Quando solicitado a **Digitar o nome de host**, digite o nome do seu servidor FTP. Quando o ShareFile for usado como servidor FTP, digite o nome da empresa seguido pelo nome do site FTP do Sharefile. Por exemplo, citrix.sharefileftp.com.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

c. Quando solicitado a **Digitar o nome do usuário remoto**, digite o ID do usuário alfanumérico.

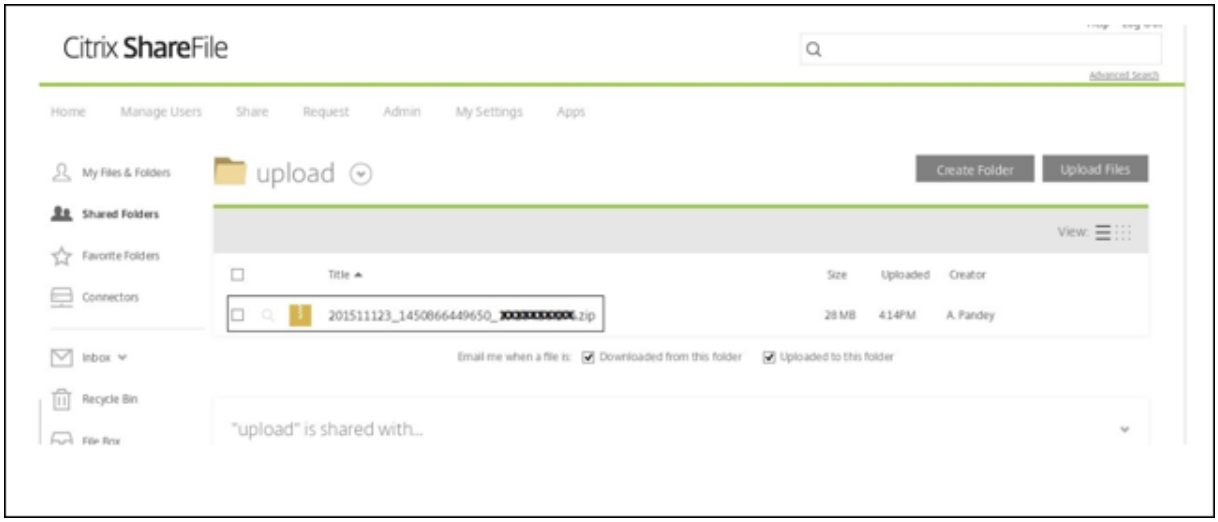
d. Quando solicitado a **Digitar a senha do usuário remoto**, digite a sua senha.

e. Quando solicitado a **Digitar o diretório remoto**, insira o nome da pasta compartilhada que você criou no ShareFile e pressione **Enter**.



Você pode visualizar o pacote de suporte carregado na pasta compartilhada que você criou no ShareFile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



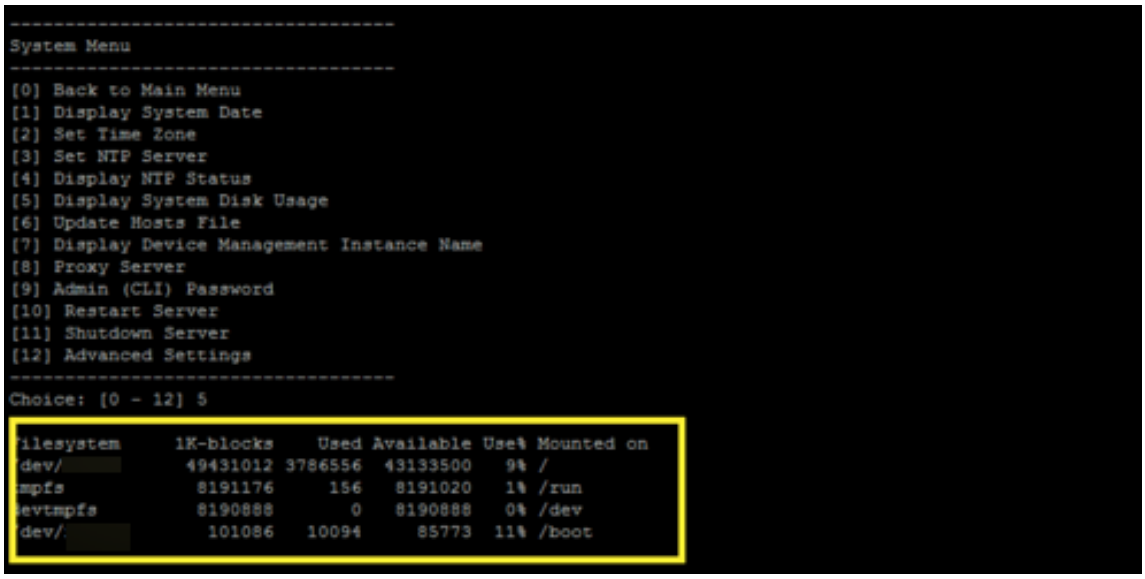
Para obter mais informações sobre o ShareFile FTP, consulte este artigo do Citrix Support Knowledge Center.

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 **System**.
2. No menu **System**, selecione a opção **Display System Disk Usage**.

   As informações do sistema de arquivos são exibidas.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introdução aos fluxos de trabalho para o console XenMobile

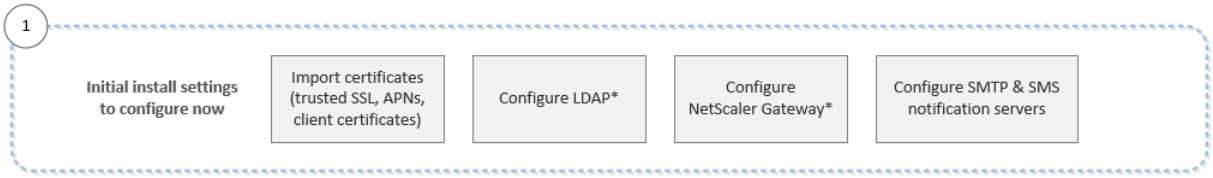
April 15, 2019

O console XenMobile é a ferramenta de gerenciamento unificado no XenMobile. Este artigo baseia-se no pressuposto de que você tenha instalado o XenMobile e esteja pronto para trabalhar no console. Se ainda for necessário instalar o XenMobile, consulte Instalação do XenMobile. Para obter mais detalhes sobre o suporte de navegador ao console XenMobile, consulte o artigo Compatibilidade do XenMobile.

Fluxo de trabalho das configurações iniciais

Depois que você terminar de configurar o XenMobile primeiro no console da linha de comando e, em seguida, no console XenMobile, o painel será aberto. Você não pode retornar para as telas de configuração inicial. Se você tiver deixado de lado algumas configurações de instalação, poderá configurar as seguintes configurações no console. Antes de iniciar a adição de usuários, aplicativos e dispositivos, conclua estas configurações de instalação. Para iniciar, 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 de Produtos Citrix:

- Autenticação
- NetScaler Gateway e XenMobile
- Notificações

Para dar suporte a plataformas Windows, iOS e Android, você deve ter a seguinte configuração de conta.

Android

- Crie credenciais do Google Play. Para obter detalhes, consulte Launch do Google Play.
- Crie uma conta de administrador do Android for Work. Para obter detalhes, consulte Android for Work.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Verifique o seu nome de domínio junto ao Google. Para obter detalhes, consulte Verify your domain for G Suite.
- Ative APIs e crie uma conta de serviço do Android for Work. Para obter detalhes, consulte Android enterprise Help.

iOS

- Crie um ID Apple e uma conta de desenvolvedor. Para obter detalhes, consulte o site Apple Developer Program.
- Crie um certificado Apple Push Notification Service (APNs). Se você planeja gerenciar dispositivos iOS com a sua implantação do XenMobile Server, precisará de um certificado Apple APNs. Se usar notificações por push para a implantação do Secure Mail, você também precisa de um certificado APNs da Apple. Para obter detalhes sobre como obter certificados de APNs da Apple, consulte o Apple Push Certificates Portal. Para obter mais informações sobre XenMobile e APNs, consulte Certificados APNs e Notificações por Push para o Secure Mail para iOS.
- Crie um token de empresa do Volume Purchase Program (VPP). Para obter detalhes, consulte Apple Volume Purchasing Program.

Windows

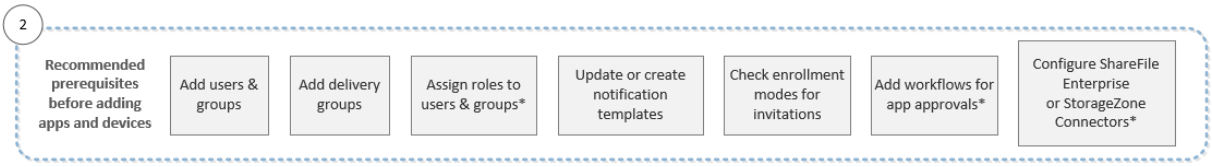
- Crie uma conta de desenvolvedor da Microsoft Windows Store. Para obter detalhes, consulte Account types, locations, and fees.
- Obtenha um ID de Publicador da Microsoft Windows Store. Para obter detalhes, consulte Manage account settings and profile info.
- Adquira um certificado empresarial da Symantec. Para obter detalhes, consulte Company app distribution for Windows Phone.
- Você deverá ter um certificado SSL público disponível se planeja usar a descoberta automática do XenMobile para o registro do Windows Phone. Para obter detalhes, consulte XenMobile Autodiscovery Service.
- Crie um Application Enrollment Token (AET). Para obter detalhes, consulte How to generate an application enrollment token for Windows Phone.

Fluxo de trabalho dos pré-requisitos do console

Este fluxo de trabalho mostra os pré-requisitos que você deve configurar antes de adicionar aplicativos e dispositivos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Os itens com um asterisco são opcionais.



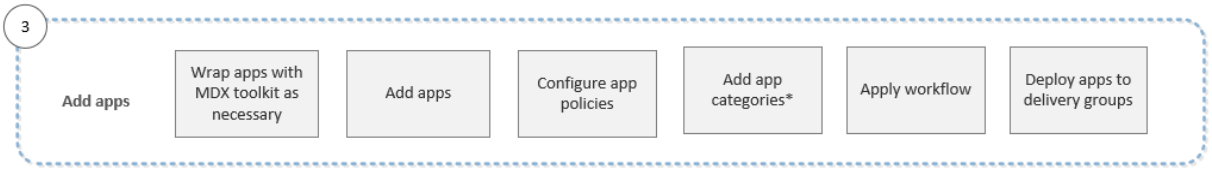
Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- Contas de usuário, funções e registro
- Implantar recursos
- Configurar funções com RBAC
- Notificações
- Criar e gerenciar fluxos de trabalho
- Uso do ShareFile com o XenMobile

Adicionar fluxo de trabalho de aplicativos

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida quando você adiciona aplicativos ao 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 de Produtos Citrix:

- Sobre o MDX Toolkit
- Adicionar aplicativos
- Resumo das políticas do MDX
- Criar e gerenciar fluxos de trabalho
- Implantar recursos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar fluxo de trabalho de dispositivos

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida durante a adição e o registro de dispositivos no XenMobile.

> Nota:
>
> Os itens com um asterisco são opcionais.

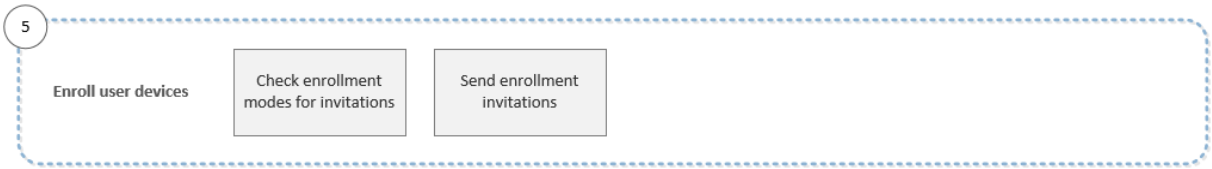


Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- Dispositivos
- Sistemas operacionais compatíveis de dispositivos
- Implantar recursos
- Monitoração e suporte
- Ações automatizadas

Registrar o fluxo de trabalho de dispositivos do usuário

Este fluxo de trabalho mostra uma ordem recomendada de registro de dispositivos de usuário no XenMobile.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos da Documentação de Produtos Citrix:

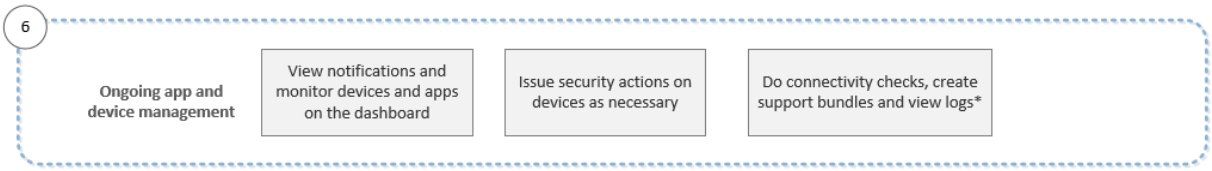
- Contas de usuário, funções e registro
- Notificações

Fluxo de trabalho contínuo de gerenciamento de aplicativos e dispositivos

Este fluxo de trabalho mostra atividades de gerenciamento de aplicativo e dispositivo que você pode realizar no console.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> 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 Monitoração e suporte.

Certificados e autenticação

April 15, 2019

Componentes têm uma função na autenticação durante operações do XenMobile:

- **XenMobile Server:** o XenMobile Server é o local em que você define a segurança do registro e a experiência do registro. Opções para a integração de usuários incluem:
  - Tornar o registro aberto para todos ou apenas por convite.
  - Exigir autenticação de dois fatores ou autenticação de três fatores. Através das propriedades do cliente no XenMobile, você pode ativar Autenticação do PIN da Citrix e configurar a complexidade e o período de vencimento do PIN.
- **NetScaler:** o NetScaler oferece o encerramento de sessões de micro VPN SSL. O NetScaler também oferece segurança em trânsito de rede e permite que você defina a experiência de autenticação usada cada vez que um usuário acessa um aplicativo.
- **Secure Hub:** o Secure Hub e o XenMobile Server trabalham em conjunto nas operações de registro. O Secure Hub é a entidade em um dispositivo que se comunica com o NetScaler: quando uma sessão expira, o Secure Hub obtém um tíquete de autenticação do NetScaler e passa o tíquete para os aplicativos MDX. A Citrix recomenda o uso de certificate pinning, o que impede ataques de intermediários. 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 contêiner: o Secure Hub envia as políticas, cria uma sessão com o NetScaler quando um aplicativo atinge o tempo limite e define o tempo limite de autenticação do MDX e a experiência de autenticação. O Secure Hub também é responsável por detecção de jailbreak, verificações de localização geográfica e as políticas que você aplicar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Políticas de MDX:** as políticas de MDX criam o cofre de dados no dispositivo. As políticas de MDX conexões direcionam conexões de micro VPN de volta para o NetScaler, impõem restrições de modo offline como tempos limite.

Para obter mais informações sobre a configuração de autenticação, incluindo uma visão geral dos métodos de autenticação de fator único e dois fatores, consulte o artigo sobre Autenticação do manual de implantação.

Você pode usar certificados no XenMobile para criar conexões seguras e autenticar usuários. O restante deste artigo aborda certificados. Para obter outros detalhes de configuração, consulte os seguintes artigos:

- Configure autenticação de domínio ou de domínio de segurança
- Autenticação de certificado cliente ou certificado e domínio
- Entidades PKI
- Provedores de credenciais
- Certificados APNs
- SAML para login único com o ShareFile
- Configurações do servidor do Active Directory do Microsoft Azure

Certificados

Por padrão, o XenMobile vem com um certificado de Protocolo SSL gerado durante a instalação para proteger os fluxos de comunicação com o servidor. A Citrix recomenda substituir o certificado SSL por um certificado SSL confiável de uma autoridade de certificação (AC) conhecida.

> Nota:
>
> Os dispositivos iOS 10.3 não oferecem suporte a certificados autoassinados. Se o XenMobile usa certificados autoassinados, os usuários não podem registrar dispositivos iOS 10.3 para o XenMobile. Para registrar dispositivos que executam o iOS 10.3 ou posterior no XenMobile, você deve usar certificados confiáveis do SSL no XenMobile.

O XenMobile também usa o seu próprio serviço de Infraestrutura de Chave Pública (PKI) ou obtém certificados da CA dos certificados cliente. Todos os produtos Citrix são compatíveis com certificados curinga e Nome Alternativo da Entidade (SAN). Para a maioria das implementações, você precisa somente de dois certificados curinga ou SAN.

A autenticação de certificado cliente fornece uma camada extra de segurança para os aplicativos móveis e permite aos usuários acessar facilmente aplicativos HDX. Quando a autenticação de certificado de cliente está configurada, os usuários digitam o PIN da Citrix para acesso com logon único (SSO) a aplicativos compatíveis com o XenMobile. O PIN da Citrix também simplifica o processo de autenticação do usuário. O PIN da Citrix é usado para proteger um certificado de cliente ou salvar credenciais do Active Directory localmente no dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e criar um certificado de serviço de Notificação por Push da Apple (APNs) da Apple. Para ver as etapas, consulte Certificados APNs.

A seguinte tabela mostra o formato e o tipo de certificado para cada componente do XenMobile:

Componente do XenMobile	Formato do certificado	Tipo de certificado exigido
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (o NetScaler Gateway converte PFX em PEM automaticamente).
Servidor XenMobile	.p12 (.pfx em computadores baseados no Windows)	SSL, SAML, APNs (o XenMobile também gera uma PKI completa durante o processo de instalação). Importante: o XenMobile Server não suporta certificados com a extensão .pem. Para usar um certificado .pem, divida o arquivo .pem em um certificado e uma chave e importe cada um deles para o XenMobile Server.
StoreFront	PFX (PKCS #12)	SSL, Raiz

O XenMobile dá suporte a certificados de ouvinte SSL e certificados de cliente com comprimentos de 4096, 2048 e 1024 bits. Esteja ciente de que 1024 bits certificados podem ser comprometidos facilmente.

Para o NetScaler Gateway e o XenMobile Server, a Citrix recomenda a obtenção de certificados de servidor de uma AC pública, como Verisign, DigiCert ou Thawte. Você pode criar uma Solicitação de Assinatura de Certificado (CSR) do NetScaler Gateway ou do utilitário de configuração do XenMobile. Depois de criar a CSR, você a envia para a AC assinar. Quando a AC retorna o certificado assinado, você pode instalá-lo no NetScaler Gateway ou no XenMobile.

Carregando certificados no XenMobile

Cada certificado que você carrega tem uma entrada na tabela de Certificados, incluindo um resumo do seu conteúdo. Quando você configura os componentes de integração PKI que exigem um certificado, escolha um certificado de servidor que satisfaça os critérios dependentes de contexto. Por

© 1999-2019 Citrix Systems, Inc. All rights reserved.

exemplo, você pode querer configurar o XenMobile para integrá-lo à sua CA da Microsoft. A conexão com a CA da Microsoft deve ser autenticada usando um certificado cliente.

Esta seção fornece procedimentos gerais para carregar certificados. Para obter detalhes sobre como criar, carregar e configurar certificados cliente, consulte Autenticação de certificado cliente ou certificado e domínio.

Requisitos de chave privada

O XenMobile pode ou não possuir a chave privada de um determinado certificado. Da mesma forma, o XenMobile pode ou não exigir uma chave privada para os certificados que você carrega.

Carregando certificados para o console

Ao carregar certificados para o console, você tem duas opções principais:

- Você pode clicar para importar um keystore. Em seguida, você deve identificar a entrada no repositório keystore que deseja instalar, a menos que você esteja carregando um formato PKCS #12.
- Você pode clicar para importar um certificado.

Você pode carregar o certificado de CA (sem a chave privada) que o CA usa para assinar solicitações. Você também pode carregar um certificado de cliente SSL (com a chave privada) para autenticação de cliente.

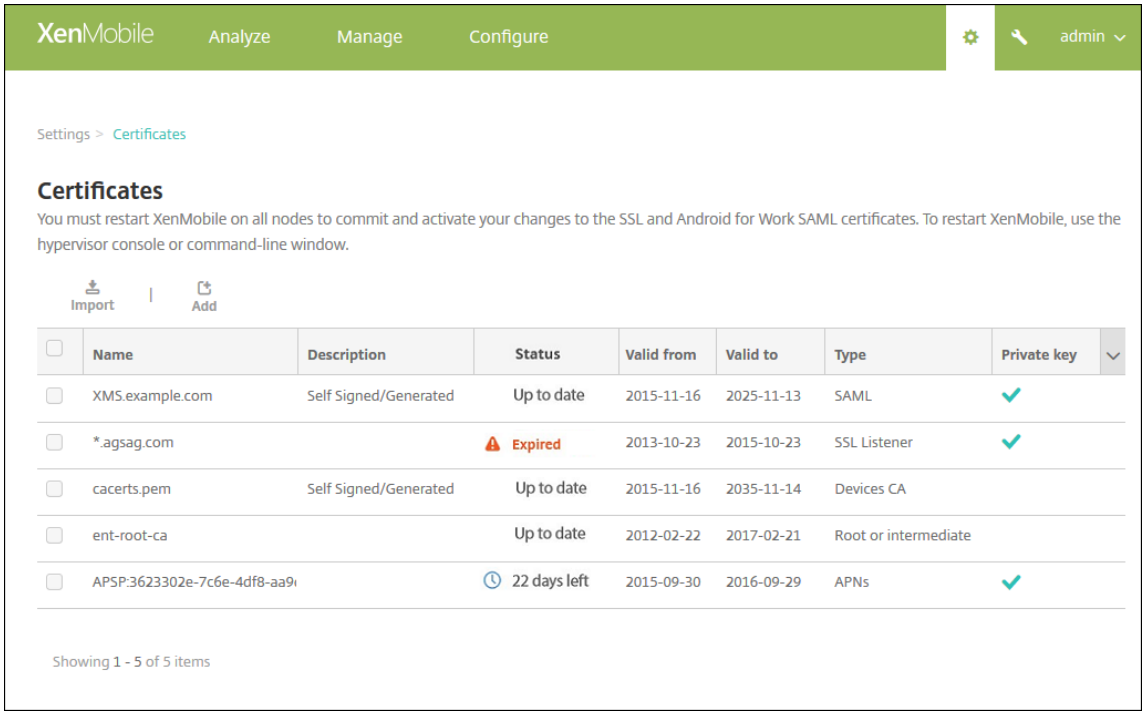
Quando você configura a entidade CA da Microsoft, você pode especificar o certificado de autoridade de certificação. Você pode selecionar o certificado de CA de uma lista de todos os certificados de servidor são certificados de CA. Da mesma forma, ao configurar a autenticação de cliente, você pode selecionar em uma lista de todos os certificados de servidor para os quais o XenMobile tem a chave privada.

Para importar um keystore

Por natureza, os keystores, que são os repositórios de certificados de segurança, podem conter várias entradas. Quando você carrega de um keystore, precisa especificar o alias de entrada que identifica a entrada que deseja carregar. Se você não especificar um alias, a primeira entrada da loja será carregada. Como os arquivos PKCS #12 geralmente contêm apenas uma entrada, o campo de alias não é exibido quando você seleciona PKCS #12 como o tipo de keystore.

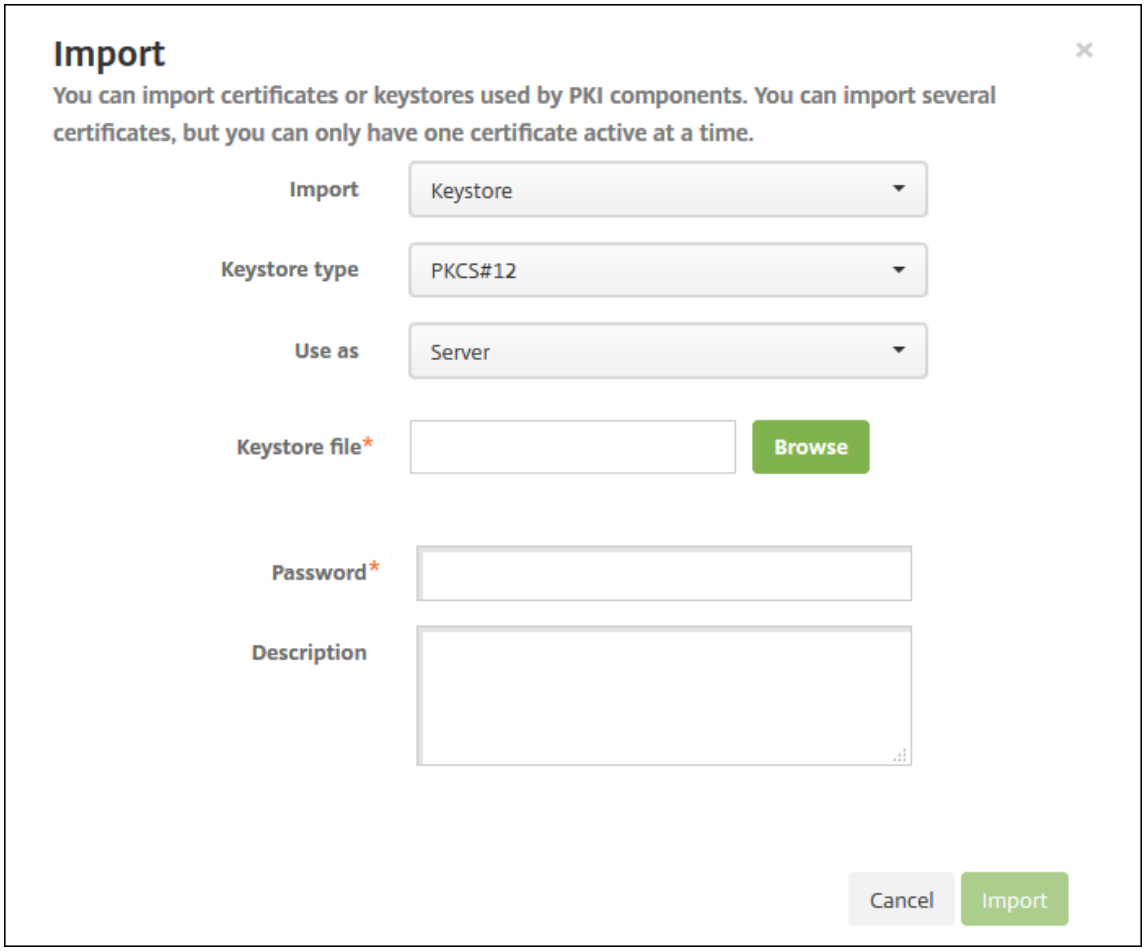
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Certificados**. A página **Certificados** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
4. Defina estas configurações:
    - **Importar:** na lista, clique em **Keystore**. A caixa de diálogo **Importar** é alterada para refletir as opções de keystore disponíveis.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Tipo de keystore:** na lista, clique em **PKCS #12**.
- **Usar como:** na lista, clique em como você pretende usar o certificado. As opções disponíveis são:
  - **Servidor**. Os certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que é carregado para o console da Web do XenMobile. Eles incluem certificados AC, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar os certificados de servidor como um armazenamento dos certificados que você deseja implantar em dispositivos. Esse uso se aplica especialmente a CAs usadas para estabelecer a confiança no dispositivo.
  - **SAML**. A certificação Security Assertion Markup Language (SAML) permite que você forneça o acesso de SSO a servidores, sites e aplicativos.
  - **APNs**. Os certificados de APNs da Apple permitem o gerenciamento de dispositivo móvel por meio da Rede Push da Apple.
  - **Ouvinte SSL**. O Ouvinte do protocolo SSL notifica o XenMobile sobre as atividades de criptografia SSL.
- **Arquivo keystore:** navegue para localizar o keystore que você deseja importar do tipo de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

arquivo .p12 (ou .pfx nos computadores baseados em Windows).
- **Senha:** digite a senha atribuída ao certificado.
- **Descrição:** opcionalmente, digite uma descrição para o keystore para ajudá-lo a distinguilo de outros keystores.

5. Clique em **Importar**. O keystore é adicionado à tabela 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 nessa cadeia para criar uma entrada de certificado do servidor para cada um. Essa operação só funcionará se os certificados na entrada do arquivo ou repositório de chaves formarem uma cadeia. Por exemplo, se cada certificado subsequente da cadeia for o emissor do certificado anterior.

Você pode adicionar uma descrição opcional para o certificado importado. A descrição só anexa o primeiro certificado na cadeia. Você pode atualizar a descrição dos certificados restantes mais tarde.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e 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 já não estiver selecionada, clique em **Certificado**.
4. A caixa de diálogo **Importar** é alterada para refletir as opções de certificado disponíveis. Em **Usar como**, selecione como você planeja usar o keystore. As opções disponíveis são:
    - **Servidor**. Os certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que é carregado para o console da Web do XenMobile. Eles incluem certificados AC, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar os certificados de servidor como um armazenamento dos certificados que você deseja implantar em dispositivos. Essa opção se aplica especialmente a CAs usadas para estabelecer a confiança no dispositivo.
    - **SAML**. A certificação Security Assertion Markup Language (SAML) permite que você forneça o acesso de logon único (SSO) a servidores, sites e aplicativos.
    - **Ouvinte SSL**. O Ouvinte do protocolo SSL notifica o XenMobile sobre as atividades de criptografia SSL.
5. Navegue para localizar o keystore que você deseja importar do tipo de arquivo .p12 (ou .pfx nos computadores baseados em Windows).
6. Procure para localizar um arquivo de chave privada opcional para o certificado. A chave privada é usada para criptografia e descriptografia junto com o certificado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. Digite uma descrição para o certificado, opcionalmente, para ajudar a identificá-lo dos outros certificados.
8. Clique em **Importar**. O certificado é adicionado à tabela Certificados.

Atualizando um certificado

O XenMobile permite que somente um certificado por chave pública exista no sistema a qualquer momento. Se você tentar importar um certificado para o mesmo par de chaves como um certificado já importado, poderá substituir a entrada existente ou excluir a entrada.

Para atualizar de forma eficaz os certificados, no console XenMobile, faça o seguinte: Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e clique em **Certificados**. Na caixa de diálogo **Importar**, importe o novo certificado.

Quando você atualiza um certificado de servidor, os componentes que estavam usando o certificado anterior passam automaticamente a usar o novo certificado. Da mesma forma, se você tiver implantado o certificado do servidor em dispositivos, o certificado será atualizado automaticamente na próxima implantação.

Atualizando um certificado

O XenMobile Server usa as seguintes autoridades de certificação internamente para PKI: CA raiz, CA do dispositivo e CA do 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 “padrão”.

Você pode renovar as CAs para dispositivos iOS, macOS e Android suportados usando o console do XenMobile Server ou a API REST pública. Para dispositivos Windows registrados, os usuários devem registrar novamente os seus dispositivos para receber uma nova CA de dispositivo.

As seguintes APIs estão disponíveis para atualizar ou regenerar as CAs de PKI internas no XenMobile Server e renovar os certificados de dispositivo emitidos por essas autoridades de certificação.

- Criar novas autoridades de certificação (CAs) de grupo.
- Ativar novas CAs e desative CAs antigas.
- Renovar o certificado do dispositivo em uma lista de dispositivos configurada. Os dispositivos já registrados continuam a funcionar sem interrupções. Um certificado de dispositivo é emitido quando um dispositivo se reconecta 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 mais informações, consulte as seguintes seções no arquivo PDF XenMobile Public API for REST Services:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
- Seção 3.16.58, Renew Device Certificate
- Seção 3.23, Refresh XenMobile CA Group
```

Como parte desse recurso, uma nova ação de segurança, **Renovação de certificado**, está disponível no console **Gerenciar dispositivos**. Esta ação renova o certificado de registro no dispositivo.

Pré-requisitos

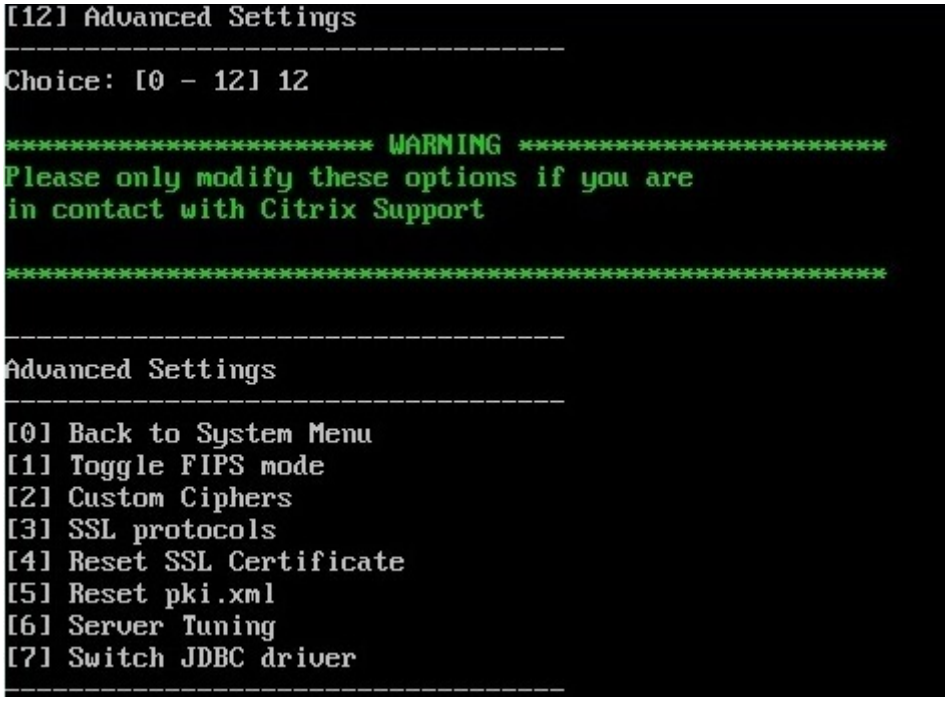
- Por padrão, esse recurso de atualização de certificado está desativado. Para ativar os recursos de atualização de certificado, defina o valor para a propriedade do servidor **refresh.internal.ca** para **True**.

> Importante:
>
> Se o seu NetScaler estiver configurado para descarga de SSL, quando você gerar um novo certificado, assegure-se de atualizar seu balanceador de carga com o novo cacert.perm. Para obter mais informações sobre a configuração do Netscaler Gateway, consulte Para usar o modo de descarga de SSL para VIPs NetScaler.

Opção de CLI para redefinir a senha do certificado de autoridade de certificação do servidor para nós do cluster

Depois de gerar um certificado de 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 de certificados de CA**. Se você redefinir a senha quando não houver um novo certificado de CA, o XenMobile não redefinirá a senha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Administração de certificado do XenMobile

Recomendamos que você liste os certificados que usar na implantação do XenMobile, especialmente quanto às suas datas de expiração e senhas associadas. Esta seção destina-se a ajudá-lo a facilitar a administração de certificados no XenMobile.

Seu ambiente pode incluir alguns dos seguintes certificados ou todos eles:

- Servidor XenMobile
  - Certificado SSL para MDM FQDN
  - Certificado (SAML para ShareFile)
  - Certificados raiz e de AC intermediários para os certificados acima e quaisquer outros recursos internos (StoreFront/Proxy etc.)
  - Certificado de APNs para gerenciamento de dispositivo iOS
  - Certificados de APNs internos 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 da Apple (por aplicativo)
  - Certificado Apple APNs (para uso com o Citrix Secure Mail)
  - Arquivo Android KeyStore
  - Windows Phone – Certificado Symantec
- NetScaler

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Certificado SSL para MDM FQDN
- Certificado SSL para FQDN de Gateway
- Certificado SSL para o FQDN do ShareFile SZC
- Certificado SSL para o balanceamento de carga do Exchange (configuração de descarregamento)
- Certificado SSL para balanceamento de carga de StoreFront
- Certificados raiz e de AC intermediários para os precedentes acima

Política de expiração de certificado do XenMobile

Se você permitir um certificado expire, o certificado se torna inválido. Você não pode mais executar transações seguras no seu ambiente e não poderá acessar recursos do XenMobile.

> Nota:
>
> A Autoridade de Certificação (AC) exibe um aviso para você renovar seu certificado SSL antes da data de expiração.

Certificado de APNs para o Citrix Secure Mail

Os certificados do Apple Push Notification Service (APNs) expiram todo ano. Lembre-se de criar um certificado SSL de APNs e atualizá-lo no portal da Citrix antes que o certificado expire. Se o certificado expirar, os usuários verão discrepâncias com as notificações por push do Secure Mail. Além disso, você não poderá mais enviar notificações por push relativas aos seus aplicativos.

Certificado de APNs para gerenciamento de dispositivo iOS

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e crie um certificado de serviço de APNs da Apple. Se o certificado expirar, os usuários não podem se registrar no XenMobile e você não pode gerenciar os respectivos dispositivos iOS. Para obter detalhes, consulte Certificados APNs.

Você pode exibir o status do certificado de APNs e data de vencimento fazendo logon no Apple Push Certificates Portal. Faça 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:

```
1 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.
2
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
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 do iOS)

Um aplicativo que é executado em um dispositivo iOS físico (diferente de aplicativos na Apple App Store) tem esses requisitos de assinatura:

- Atribua ao aplicativo um perfil de provisionamento.
- Atribua ao aplicativo um certificado de distribuição correspondente.

Para verificar se você tem um certificado de distribuição do iOS válido, faça o seguinte:

1. No portal Apple Enterprise Developer, crie uma ID de Aplicativo explícita para cada aplicativo que deseja preparar com o MDX Toolkit. Um exemplo de ID de aplicativo aceitável é: `com.CompanyName.ProductName`.
2. No portal Apple Enterprise Developer, vá para **Provisioning Profiles > Distribution** e crie um perfil de provisionamento interno. Repita esta etapa para cada ID de Aplicativo criada na etapa anterior.
3. Baixe todos os perfis de provisionamento. Para obter detalhes, consulte Preparação de aplicativos móveis iOS.

Para confirmar que todos os certificados de XenMobile Server são válidos, faça o seguinte:

1. No console XenMobile, clique em **Configurações > Certificados**.
2. Verifique se todos os certificados de APNs, incluindo os certificados de ouvinte SSL, raiz e intermediário são válidos.

Android KeyStore

O KeyStore é um arquivo que contém os certificados usados para assinar o aplicativo Android. Quando o período de validade da sua chave expira, os usuários não poderão mais atualizar em interrupções para novas versões do seu aplicativo.

Certificado empresarial da Symantec para Windows Phones

A Symantec é o provedor exclusivo de certificados de assinatura para o serviço Hub de Aplicativos Microsoft. Os desenvolvedores e editores de software entram no Hub de Aplicativos para distribuir

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aplicativos Windows Phone e Xbox 360 para download através do Windows Marketplace. Para obter detalhes, consulte Symantec Code Signing Certificates for Windows Phone na documentação da Symantec.

Se o certificado expirar, os usuários do Windows phone não podem se registrar. Os usuários do Windows Phone não podem registrar, instalar um aplicativo publicado e assinado pela empresa, nem iniciar um aplicativo da empresa que foi instalada no telefone.

NetScaler

Para obter detalhes sobre como tratar de expiração do certificado do NetScaler, consulte How to handle certificate expiry on NetScaler no Citrix Support Knowledge Center.

Um certificado NetScaler expirado impede que os usuários se registrem e acessem o armazenamento. 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 acompanhar seus certificados do NetScaler. O Centro notificará você quando o certificado expirar. Essas ferramentas auxiliam na monitoração dos seguintes certificados do NetScaler:

- Certificado SSL para MDM FQDN
- Certificado SSL para FQDN de Gateway
- Certificado SSL para o FQDN do ShareFile SZC
- Certificado SSL para o balanceamento de carga do Exchange (configuração de descarregamento)
- Certificado SSL para balanceamento de carga de StoreFront
- Certificados raiz e de AC intermediários para os certificados acima

NetScaler Gateway e XenMobile

April 15, 2019

Quando você configura o NetScaler Gateway usando o XenMobile, estabelece o mecanismo de autenticação para o acesso remoto do dispositivo à rede interna. Essa funcionalidade permite que os aplicativos em um dispositivo móvel acessem servidores corporativos localizados na intranet. O XenMobile cria uma micro VPN entre os aplicativos no dispositivo e o NetScaler Gateway.

Você configura o NetScaler Gateway para uso com o XenMobile Server exportando um script do XenMobile executado no NetScaler Gateway.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos para usar o script de configuração do NetScaler Gateway

Requisitos do NetScaler:

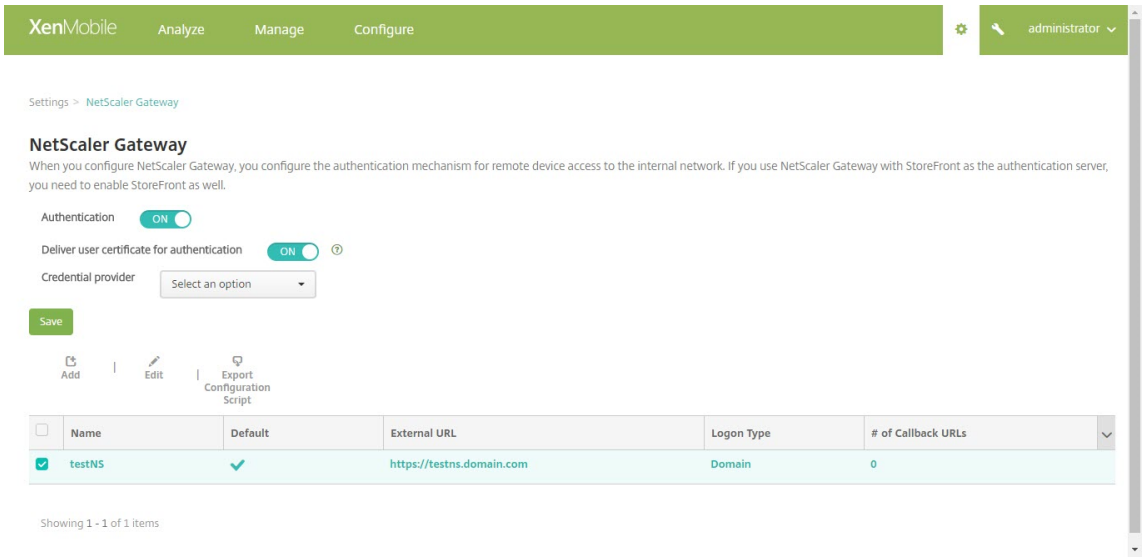
- NetScaler (versão mínima 11.0, Compilação 70.12).
- O endereço IP do NetScaler deve estar configurado e ter conectividade com o servidor LDAP, a menos que o LDAP tenha balanceamento de carga.
- O endereço IP do NetScaler Subnet (SNIP) deve estar configurado, ter conectividade com os servidores back-end necessários e ter acesso à rede pública por meio da porta 8443/TCP.
- O DNS deve poder resolver domínios públicos.
- O NetScaler deve estar licenciado com licenças de Plataforma/Universais ou de Avaliação. Para obter informações, consulte https://support.citrix.com/article/CTX126049.
- Um certificado SSL do NetScaler Gateway deve estar carregado e instalado no NetScaler. Para obter informações, consulte https://support.citrix.com/article/CTX136023.

Requisitos do XenMobile:

- XenMobile Server (versão mínima 10.6).
- O servidor LDAP deve estar configurado.

Configurar a autenticação para o acesso de dispositivos remotos à rede interna

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **NetScaler Gateway**. A página **NetScaler Gateway** é exibida. No exemplo a seguir, existe uma instância do NetScaler Gateway.



3. Defina estas configurações:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

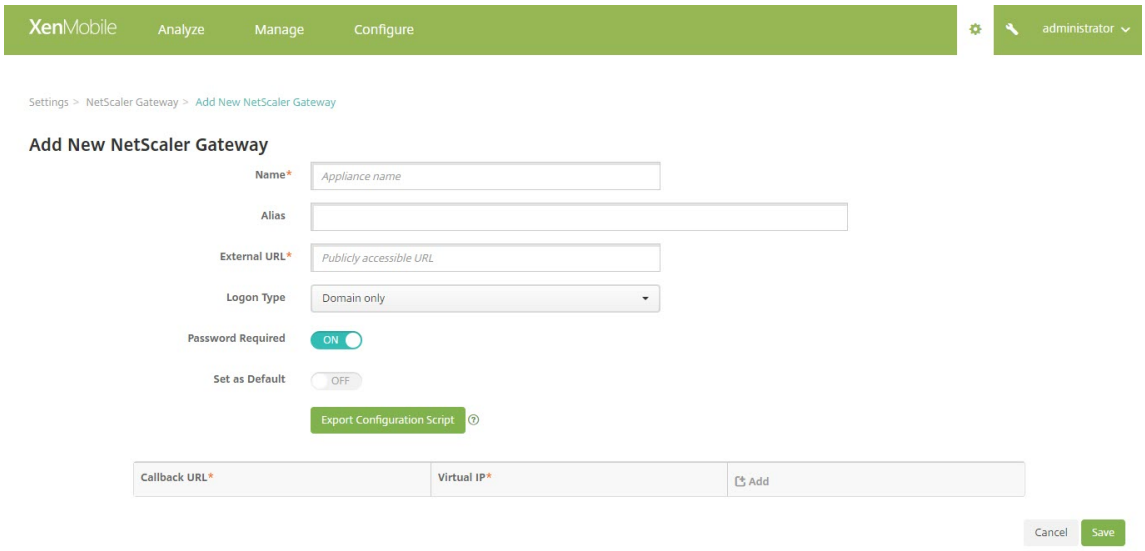
- **Autenticação:** selecione se a autenticação deve ser ativada. O padrão é **I**.
- **Entregar certificado de usuário para autenticação:** selecione se o XenMobile deve compartilhar o certificado de autenticação com o Secure Hub para que o NetScaler Gateway manipule a autenticação de certificado cliente. O padrão é **O**.
- **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 NetScaler Gateway

Depois de salvar as configurações de autenticação, adicione uma instância do NetScaler Gateway ao XenMobile.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é aberta.
2. Em **Servidor**, clique em **NetScaler Gateway**. A página **NetScaler Gateway** é exibida.
3. Clique em **Adicionar**. A página **Adicionar novo NetScaler Gateway** é exibida.



4. Defina estas configurações:

- **Nome:** digite um nome para a instância do NetScaler Gateway.
- **Alias:** inclua opcionalmente um nome de alias para o NetScaler Gateway.
- **URL externa:** digite a URL acessível publicamente do NetScaler Gateway. Por exemplo, `https://receiver.com`.
- **Tipo de login:** escolha um tipo de login. Os tipos incluem **Somente domínio**, **Somente token de segurança**, **Domínio e token de segurança**, **Certificado**, **Certificado e domínio**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

e **Certificado e token de segurança**. A configuração padrão para o campo **Senha obrigatória** muda com base no **Tipo de login** 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 o XenMobile e o NetScaler Gateway, consulte Configurar a autenticação para vários domínios.

Se você usar **Certificado e token de segurança**, não necessárias configurações adicionais no NetScaler Gateway para dar suporte ao Secure Hub. Para obter informações, consulte Configuração do XenMobile para autenticação de certificado e token de segurança.

Para obter mais informações, consulte Autenticação no Manual de implantação.

- **Senha obrigatória:** selecione se a autenticação de senha deve ser exigida. O padrão varia de acordo com o **Tipo de login** escolhido.
- **Definir como padrão:** selecione se esse NetScaler Gateway deve ser usado como padrão. O padrão é **O**.
- **Exportar script de configuração:** clique no botão para exportar um pacote de configuração carregado no NetScaler Gateway para defini-lo com as configurações do XenMobile. Para obter informações, consulte “Configurar um NetScaler Gateway local para uso com o XenMobile Server”, após estas etapas.
- **URL de retorno de chamada** e **IP virtual**: salve suas configurações antes de adicionar esses campos. Para obter informações, consulte Adicionar uma URL de retorno de chamada ao IP virtual da VPN do NetScaler Gateway neste artigo.

5. Clique em **Salvar**.

   O novo NetScaler Gateway é adicionado e exibido na tabela. Para editar ou excluir uma instância, clique no nome na lista.

Configurar um NetScaler Gateway para uso com o XenMobile Server

Para configurar um NetScaler Gateway local para uso com o XenMobile Server, realize as seguintes etapas gerais, detalhadas neste artigo:

1. Baixe um script e os arquivos relacionados do XenMobile Server. Consulte o arquivo leiame fornecido com o script para obter as instruções detalhadas mais recentes.
2. Verifique se o seu ambiente atende aos pré-requisitos.
3. Atualize o script do seu ambiente.
4. Execute o script no NetScaler.
5. Teste a configuração.

O script configura essas configurações do NetScaler Gateway exigidas pelo XenMobile:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

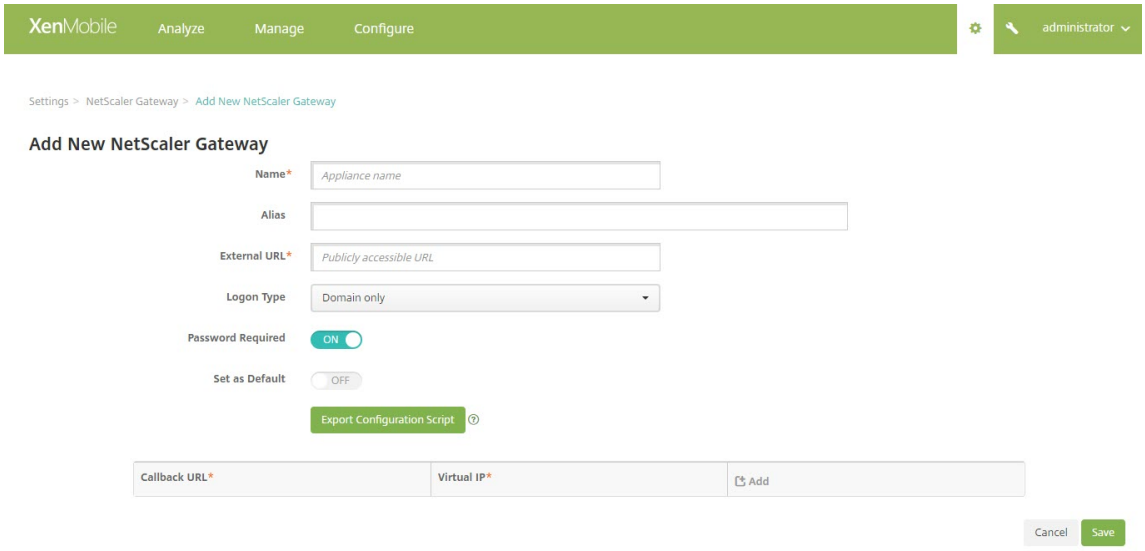
- Servidores NetScaler Gateway necessários para MDM e MAM
- Políticas de sessão para os servidores virtuais do NetScaler Gateway
- Detalhes do XenMobile Server
- Políticas de autenticação e ações para o servidor virtual NSG.
  O script descreve as definições de configuração de LDAP.
- Ações e políticas de tráfego para o servidor proxy
- Perfil de acesso sem cliente
- Registro de DNS local estático no NetScaler
- Outras associações: política de serviço, certificado de CA

O script não manipula a seguinte configuração:

- Balanceamento de carga do Exchange
- Balanceamento de carga do ShareFile
- Configuração de proxy ICA
- Descarga de SSL

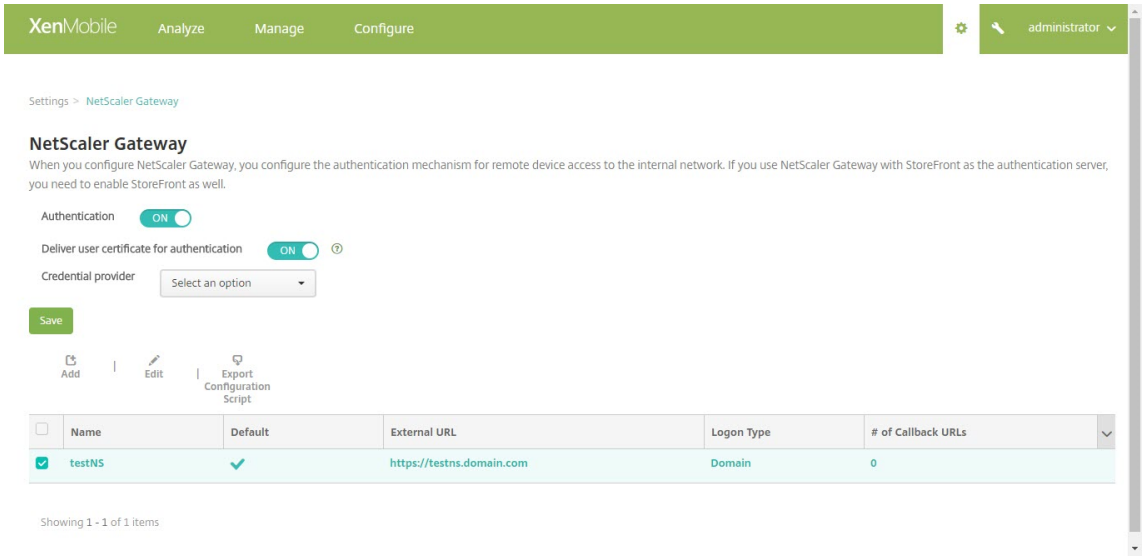
Para baixar, atualizar e executar o script

1. Se estiver adicionando um NetScaler Gateway, clique em **Exportar script de configuração** na página **Adicionar novo NetScaler Gateway**.



   Ou, se você adicionar uma instância do NetScaler Gateway e clicar em **Salvar** antes de exportar o script, retorne à página **Configurações > NetScaler Gateway**, selecione o NetScaler, clique em **Exportar script de configuração** e, em seguida, clique em **Download**.

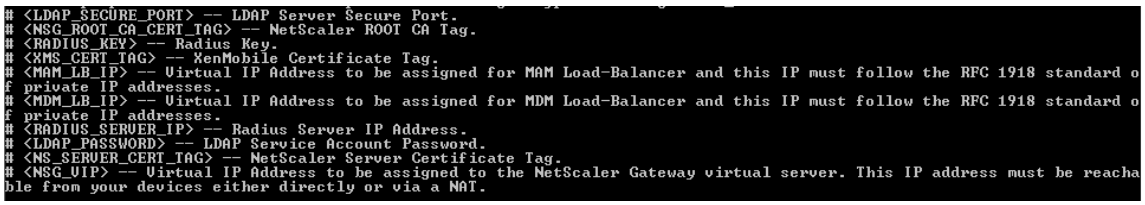
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Depois de clicar em **Exportar script de configuração**, o XenMobile criará um pacote de script .tar.gz. O pacote de script inclui:

- Arquivo Leiame com instruções detalhadas
- Script que contém comandos da CLI do NetScaler usados para configurar os componentes necessários no NetScaler
- Certificado de CA de raiz pública e o certificado de CA intermediária do XenMobile Server (esses certificados, para descarga de SSL, não são necessários para a versão atual)
- Script que contém os comandos da CLI do NetScaler para remover a configuração do NetScaler

2. Edite o script (NSGConfigBundle_CREATESCRIPT.txt) para substituir todos os espaços reservados por detalhes do seu ambiente.



3. Execute o script editado no bash shell NetScaler, conforme descrito no arquivo leiame incluído no pacote de script. Por exemplo:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management
 Password> batch -f ”/var/NSGConfigBundle_CREATESCRIPT.txt”
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

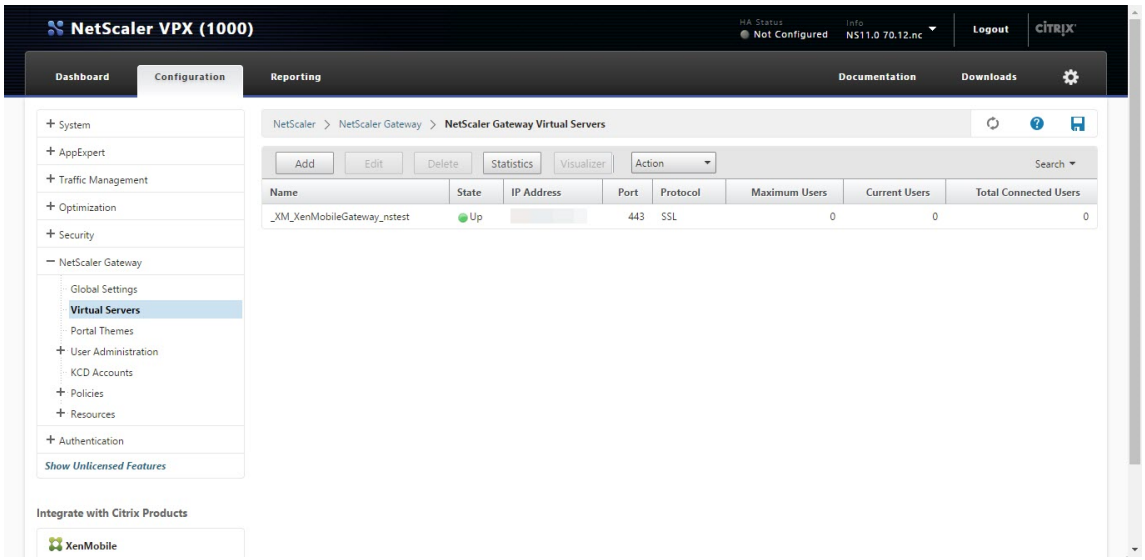
```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you 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#
```

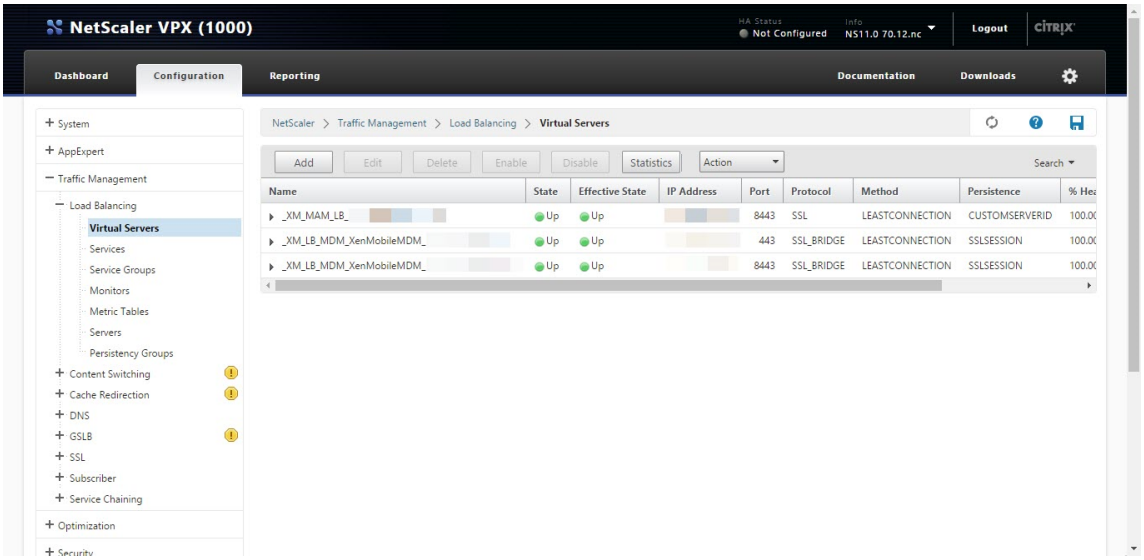
Testar a configuração

1. Valide que o servidor virtual do NetScaler Gateway mostra um estado de **UP**.



2. Valide que o servidor virtual de balanceamento de carga proxy mostra um estado de **UP**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Abra um navegador da Web, conecte-se à URL do NetScaler Gateway e tente autenticar. Se a autenticação falhar, esta mensagem será exibida: HTTP Status 404 - Não encontrado
4. Registre um dispositivo e verifique se ele obtém os registros de MDM e MAM.

Adicionar uma URL de retorno de chamada ao IP virtual da VPN do NetScaler Gateway

Depois de adicionar a instância do NetScaler Gateway, você poderá adicionar uma URL de retorno de chamada e especificar um endereço IP virtual do NetScaler Gateway. Essas configurações são opcionais, mas podem ser definidas para obter segurança extra, especialmente quando o XenMobile Server está na DMZ.

1. Em **Configurações > NetScaler Gateway**, selecione o NetScaler Gateway e clique em **Editar**.
2. Na tabela, clique em **Adicionar**.
3. Para **URL de retorno de chamada**, digite o nome de domínio totalmente qualificado (FQDN). A URL de retorno de chamada verifica se uma solicitação é proveniente do NetScaler Gateway.

   Certifique-se de que a URL de retono de chamada seja resolvida para um endereço IP acessível no XenMobile Server. A URL de retorno de chamada pode ser uma URL externa do NetScaler Gateway ou alguma outra URL.
4. Digite o endereço **IP virtual** do NetScaler Gateway e clique em **Salvar**.

Configurar a autenticação para vários domínios

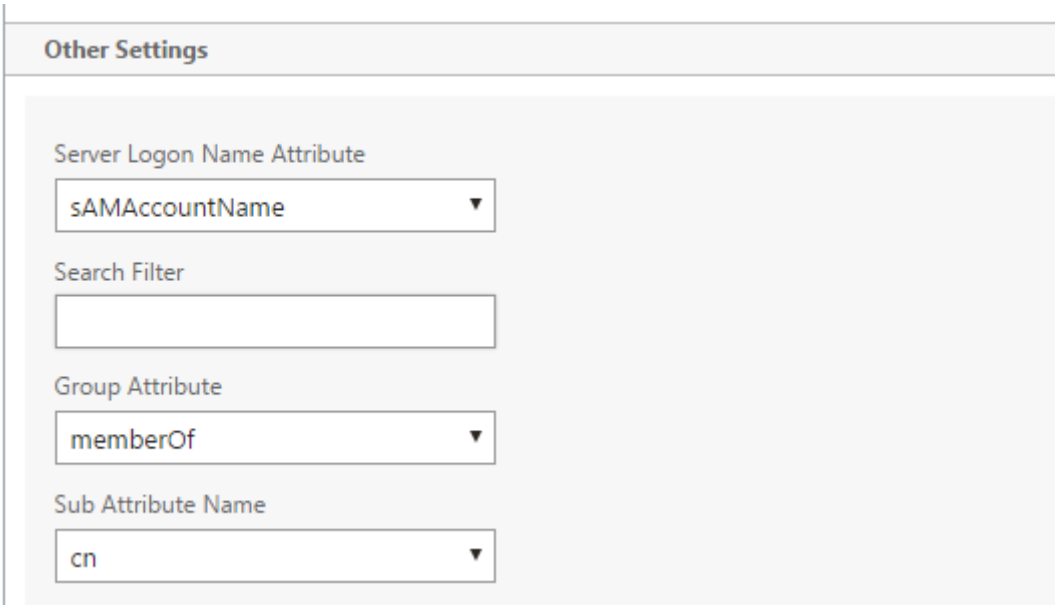
Se você tiver várias instâncias do XenMobile Server, como ambientes de teste, desenvolvimento e produção, deverá configurar o NetScaler Gateway para os ambientes adicionais manualmente. (Você pode usar o assistente NetScaler para XenMobile apenas uma vez.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração do NetScaler Gateway

Para configurar políticas de autenticação do NetScaler Gateway e uma política de sessão para um ambiente de vários domínios:

1. No utilitário de configuração do NetScaler Gateway, na guia **Configuration**, expanda **NetScaler Gateway > Policies > Authentication**.
2. No painel de navegação, clique em **LDAP**.
3. Clique para editar o perfil LDAP. Mude o **Server Logon Name Attribute** para **userPrincipalName** ou para o atributo que você deseja usar para pesquisas. Anote o atributo que você especificar. Você deve fornecê-lo ao definir as configurações de LDAP no console XenMobile.



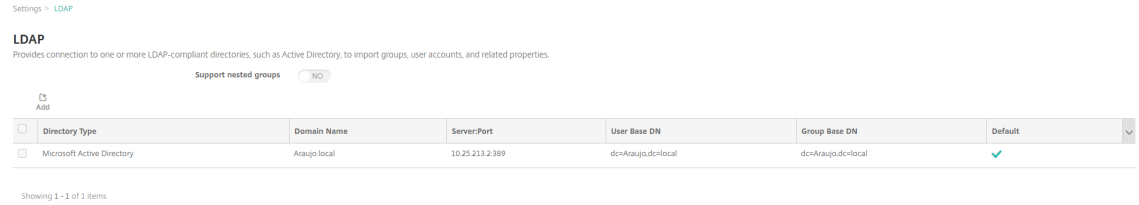
4. Repita essas etapas para cada política LDAP. Uma política LDAP separada é necessária para cada domínio.
5. Na política de sessão associada ao servidor virtual NetScaler Gateway, navegue até **Edit session profile > Published Applications**. Certifique-se de que **Single Sign-On Domain** esteja em branco.

Configuração do XenMobile Server

Para configurar o LDAP para um ambiente XenMobile de vários domínios:

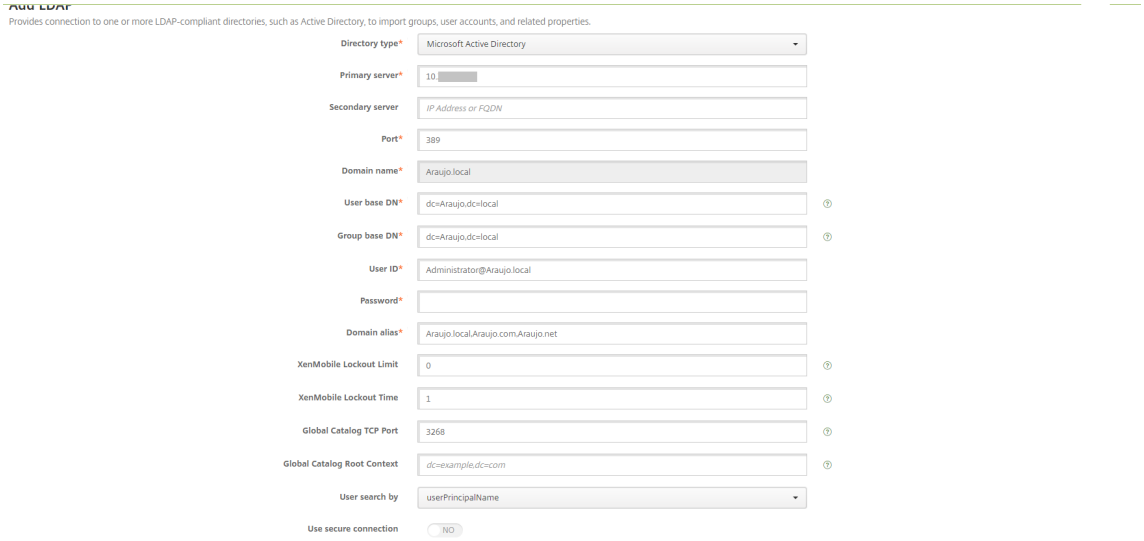
1. No console XenMobile, vá para **Configurações > LDAP** e adicione ou edite um diretório.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 os domínios. Por exemplo: domain1.com,domain2.com,domain3.com
   - Certifique-se de que o campo **Pesquisa de usuário por** corresponde ao **Server Logon Name Attribute** especificado na política LDAP do NetScaler Gateway.



Configure autenticação de domínio ou de domínio de segurança

April 15, 2019

O XenMobile dá suporte a autenticação baseada em domínio com relação a um ou mais diretórios que estão em conformidade com o protocolo LDAP. Você pode configurar uma conexãono XenMobile para um ou mais diretórios e depois usar a configuração de LDAP para importar grupos, contas de usuários e propriedades correlatas.

O LDAP é um protocolo de aplicativo neutro quanto ao fornecedor e de software livre para acesso e manutenção de serviços de informações de diretório distribuído sobre uma rede Protocolo IP. Os serviços de informações de diretório são usados para compartilhar informações sobre os usuários, os sistemas, as redes, os serviços e os aplicativos disponíveis em toda a rede.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Um uso comum do LDAP é fornecer logon único (SSO, Single Sign-on) para usuários, em que 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 do LDAP conectando-se a um servidor LDAP, chamado de Directory System Agent (DSA). O cliente envia uma solicitação de operação para o servidor, e o servidor responde com a autenticação adequada.

> Importante:
>
> O XenMobile não dá 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

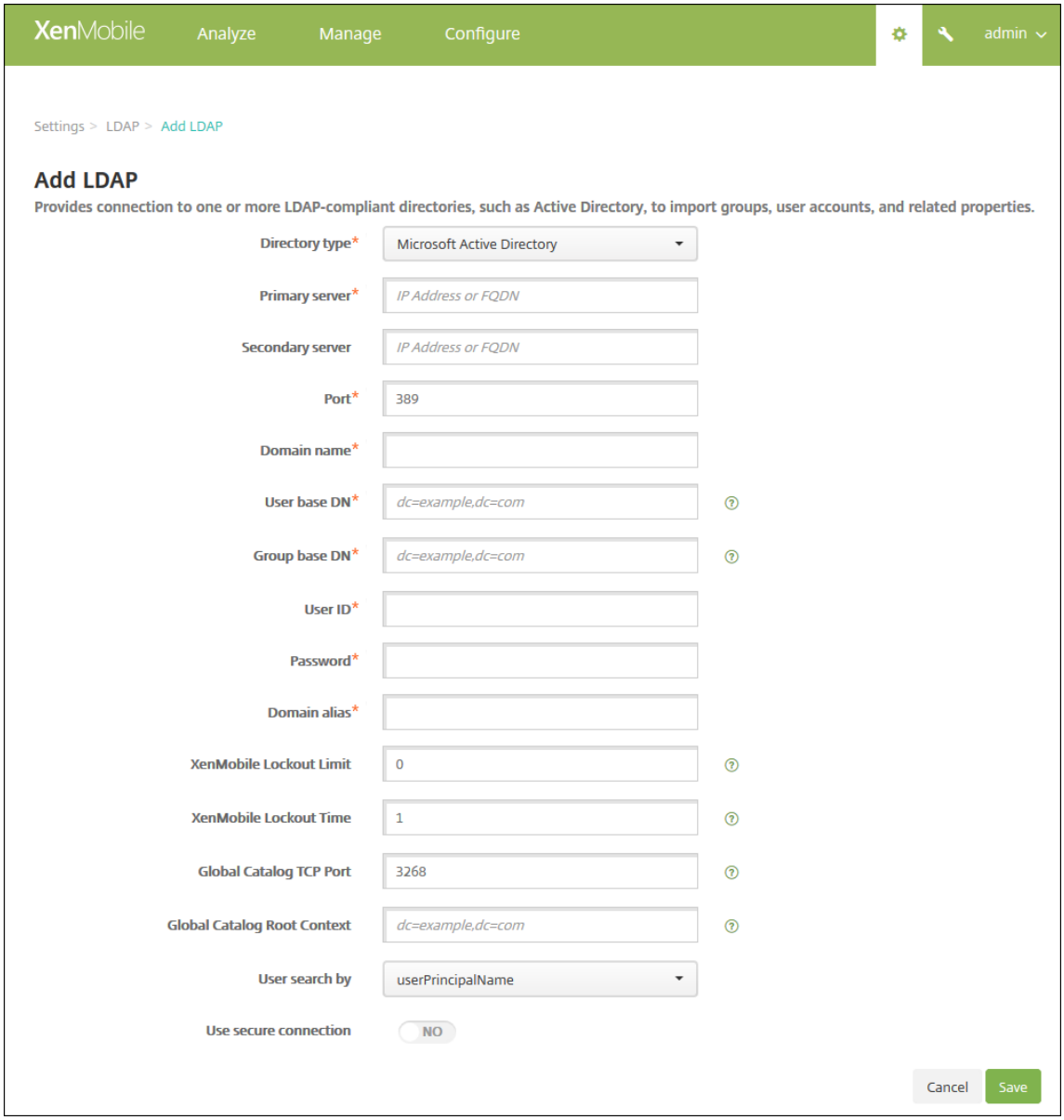
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **LDAP**. A página **LDAP** é exibida. Você pode adicionar, editar ou excluir diretórios compatíveis com LDAP, conforme descrito neste artigo.



Para adicionar um diretório compatível com LDAP

1. Na página **LDAP**, clique em **Adicionar**. A página **Adicionar LDAP** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

   - **Tipo de diretório:** na lista, clique no tipo de diretório adequado. O padrão é **Microsoft Active Directory**.
   - **Servidor primário:** digite o servidor primário usado para o 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, digite o endereço IP ou o FQDN do servidor secundário. Esse servidor é um failover usado se o servidor primário não pode ser acessado.
   - **Porta:** digite o número da porta usada pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número de porta **636** para conexões LDAP seguras, **3268** para conexões LDAP não seguras da Microsoft ou **3269** para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

conexões LDAP seguras da Microsoft.
- **Nome de domínio:** digite o nome de domínio.
- **DN base de usuário:** digite a localização dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users`, `dc=example` ou `dc=com`.
- **DN base de grupo:** digite a localização 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 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.
- **Limite de bloqueio do XenMobile:** digite um número entre **0** e **999** para ser o número de tentativas de login com falha. Um valor **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de login com falha.
- **Tempo de bloqueio do XenMobile:** digite um número entre **0** e **99999** para representar o número de minutos que um usuário deve esperar depois de ultrapassar o limite de bloqueio. Um valor **0** significa que o usuário não é forçado a esperar após um bloqueio.
- **Porta TCP do catálogo global:** digite o número da porta TCP do servidor do Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número de porta **3269**.
- **Contexto raiz do catálogo global:** opcionalmente, digite o valor do Contexto Raiz Global usado para ativar uma pesquisa do catálogo global no Active Directory. Essa pesquisa é 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**.
- **Usar conexão segura:** selecione se devem ou não ser usadas conexões seguras. O padrão é **NÃO**.

3. Clique em **Salvar**.

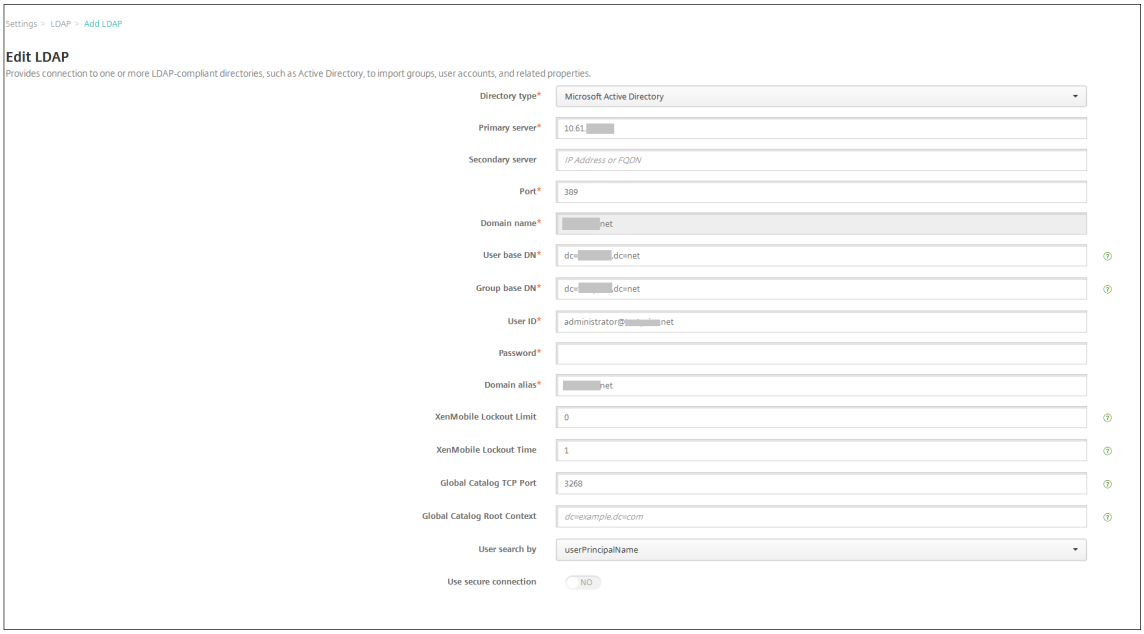
Para editar um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório a editar.

   Quando você marca a caixa de seleção ao lado de um diretório, o menu de opções é exibido acima da lista LDAP. Clique em qualquer outro lugar na lista e o menu de opções é exibido no lado direito da listagem.

2. Clique em **Editar**. A página **Editar LDAP** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Altere as seguintes informações conforme apropriado:

   - **Tipo de diretório:** na lista, clique no tipo de diretório adequado.
   - **Servidor primário:** digite o servidor primário usado para o LDAP; você pode inserir o endereço IP ou o nome de domínio totalmente qualificado (FQDN).
   - **Servidor secundário:** opcionalmente, digite o endereço IP ou o FQDN do servidor secundário (se um tiver sido configurado).
   - **Porta:** digite o número da porta usada pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número de porta **636** para conexões LDAP seguras, **3268** para conexões LDAP não seguras da Microsoft ou **3269** para conexões LDAP seguras da Microsoft.
   - **Nome de domínio:** você não pode alterar esse campo.
   - **DN base de usuário:** digite a localização dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users`, `dc=example` ou `dc=com`.
   - **DN base de grupo:** digite o nome de grupo DN base de 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 está executando o Active Directory.
   - **ID do 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.
   - **Limite de bloqueio do XenMobile:** digite um número entre **0** e **999** para ser o número de tentativas de login com falha. Um valor **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de login com falha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Tempo de bloqueio do XenMobile:** digite um número entre **0** e **99999** para representar o número de minutos que um usuário deve esperar depois de ultrapassar o limite de bloqueio. Um valor **0** significa que o usuário não é forçado a esperar após um bloqueio.
- **Porta TCP do catálogo global:** digite o número da porta TCP do servidor do Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número de porta **3269**.
- **Contexto raiz do catálogo global:** opcionalmente, digite o valor do Contexto Raiz Global usado para ativar uma pesquisa do catálogo global no Active Directory. Essa pesquisa é 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**.
- **Usar conexão segura:** selecione se devem ou não ser usadas 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 desejar 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 a 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 a autenticação para vários domínios. As etapas são as mesmas na versão local do XenMobile Server e na versão na nuvem do Endpoint Management.

Configurar autenticação de domínio e de token de segurança

Você pode configurar o XenMobile para exigir que os usuários autentiquem com as suas credenciais LDAP mais uma senha de uso único, usando o protocolo RADIUS.

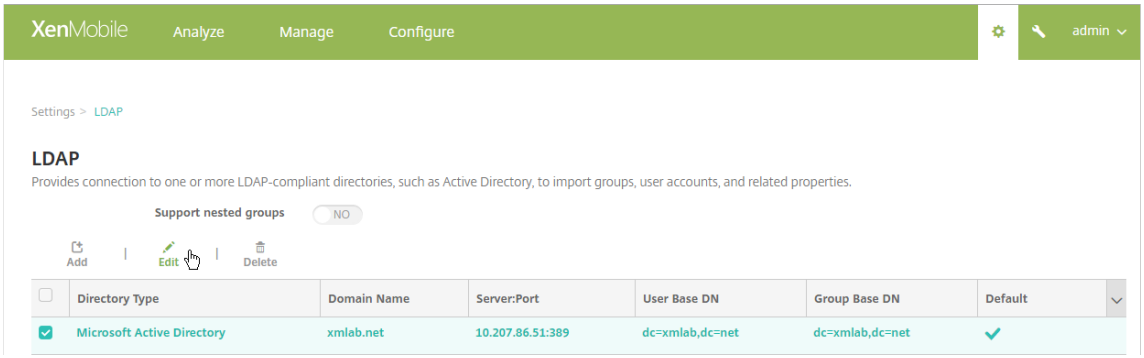
Para melhor usabilidade, você pode combinar essa configuração com o Citrix PIN e armazenamento em cache de senha do Active Directory. Com essa configuração, os usuários não precisam digitar seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem seus nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

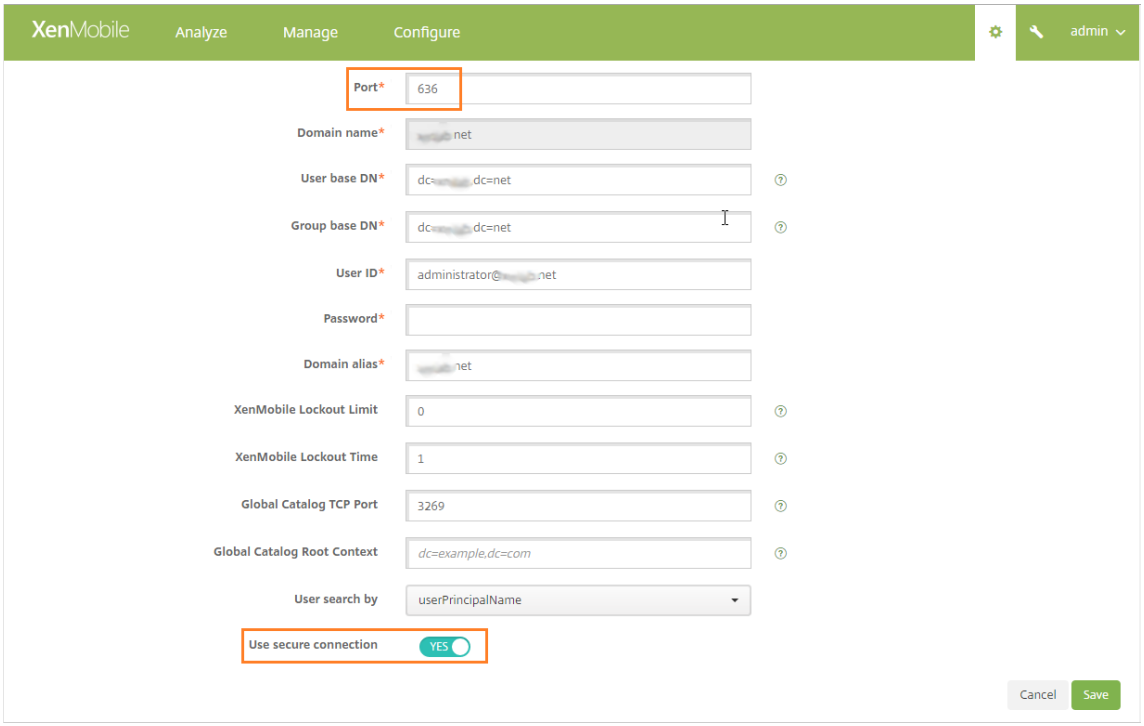
Definir as configurações do LDAP

O uso de LDAP para autenticação requer 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, em seguida, 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**.

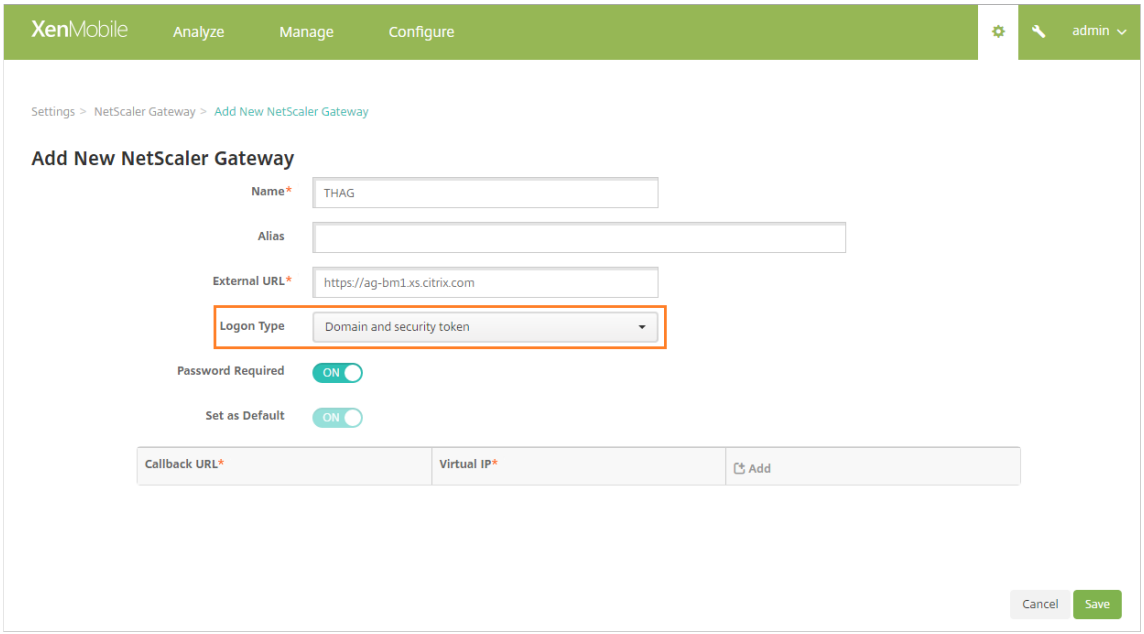


© 1999-2019 Citrix Systems, Inc. All rights reserved.

Definir as configurações do NetScaler Gateway

As seguintes etapas pressupõem que você já tenha adicionado uma instância do NetScaler Gateway ao XenMobile. Para adicionar uma instância do NetScaler Gateway instance, consulte Adicionar uma instância do NetScaler Gateway.

1. Em **Configurações**, clique em **NetScaler Gateway**.
2. Selecione o **NetScaler Gateway** e clique em **Editar**.
3. Em **Tipo de logon**, selecione **Domínio e token de segurança**.



Ativar o PIN da Citrix e o cache de senha de usuário

Para ativar o PIN da Citrix e a senha do usuário em cache, vá para **Configurações > Propriedades do Cliente** e assinale as caixas de seleção para **Ativar PIN da Citrix** e **Ativar armazenamento em cache da senha do usuário**. Para obter mais informações, consulte Propriedades do cliente.

Configurar o NetScaler Gateway para autenticação de domínio e de token de segurança

Configure perfis de sessão do NetScaler Gateway e as políticas de seus servidores virtuais usados com o XenMobile. Para obter mais informações, consulte a documentação do Citrix NetScaler Gateway.

Autenticação de certificado cliente ou certificado e domínio

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A configuração padrão para o XenMobile é autenticação de nome de usuário e senha. Para adicionar outra camada de segurança para registro e acesso ao ambiente do XenMobile, considere usar a autenticação baseada em certificado. No ambiente XenMobile, essa configuração é a melhor combinação de segurança e experiência do usuário. O certificado mais a autenticação de domínio tem as melhores possibilidades de SSO, juntamente com a segurança fornecida pela autenticação de dois fatores no NetScaler.

Para melhor usabilidade, você pode combinar autenticação de certificado mais domínio com o Citrix PIN e a senha em cache do Active Directory. Como resultado, os usuários não precisam digitar seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem seus nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

> Importante:
>
> O XenMobile não dá 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 similar métodos, a configuração de certificados permite a você representar um cartão inteligente para o XenMobile. Em seguida, os usuários se registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que o usuário pode acessar, o XenMobile cria e implanta o certificado usado para autenticar no ambiente XenMobile.

Você pode usar o assistente NetScaler para o XenMobile para executar a configuração necessária para o XenMobile ao usar autenticação de NetScaler de certificate apenas ou autenticação de certificado mais domínio. Você pode executar o NetScaler para o assistente do 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, uma opção é a autenticação de dois fatores que usa um certificado de cliente e um token de segurança. Para obter informações, consulte Configuração do XenMobile para autenticação de certificado e token de segurança.

Autenticação de certificado de cliente está disponível para o modo MAM do XenMobile (somente MAM) e o modo ENT (quando os usuários se registram no MDM). A autenticação de certificado cliente não está disponível para o modo ENT do XenMobile quando os usuários se registram no modo MAM legado. Para usar a autenticação de certificado de cliente para os modos ENT e MAM do XenMobile, você deve configurar o servidor Microsoft, o XenMobile Server e o NetScaler Gateway. Siga os seguintes procedimentos gerais, como detalhado neste artigo.

No servidor Microsoft:

1. Adicione um snap-in de certificado ao Console de Gerenciamento Microsoft.
2. Adicione o modelo à Autoridade de Certificação (AC).
3. Crie um certificado PFX do servidor de AC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

No XenMobile Server:

1. Carregue o certificado no XenMobile.
2. Crie a entidade PKI de autenticação baseada em certificado.
3. Configure os provedores de credenciais.
4. Configure o NetScaler Gateway para fornecer um certificado de usuário para autenticação.

   Para obter informações sobre a configuração do NetScaler Gateway, consulte estes artigos na documentação do Citrix ADC: Autenticação de cliente, Infraestrutura de perfil SSL e Configuração e vinculação de uma política de autenticação de certificado cliente.

Pré-requisitos

- Ao criar um modelo de Entidade de Serviços de Certificado Microsoft, evite possíveis problemas de autenticação com dispositivos tegistrados excluindo caracteres especiais. Por exemplo, não use esses caracteres no nome do modelo: `: ! $ ()## % + * ~ ? | { } []`
- Para dispositivos Windows Phone 8.1 que usam autenticação de certificado e a descarga de SSL, desabilite a reutilização de sessão SSL para a porta 443 nos servidores virtuais de balanceamento de carga e no NetScaler. Para fazer isso, execute o seguinte comando nos vservers para a porta 443:

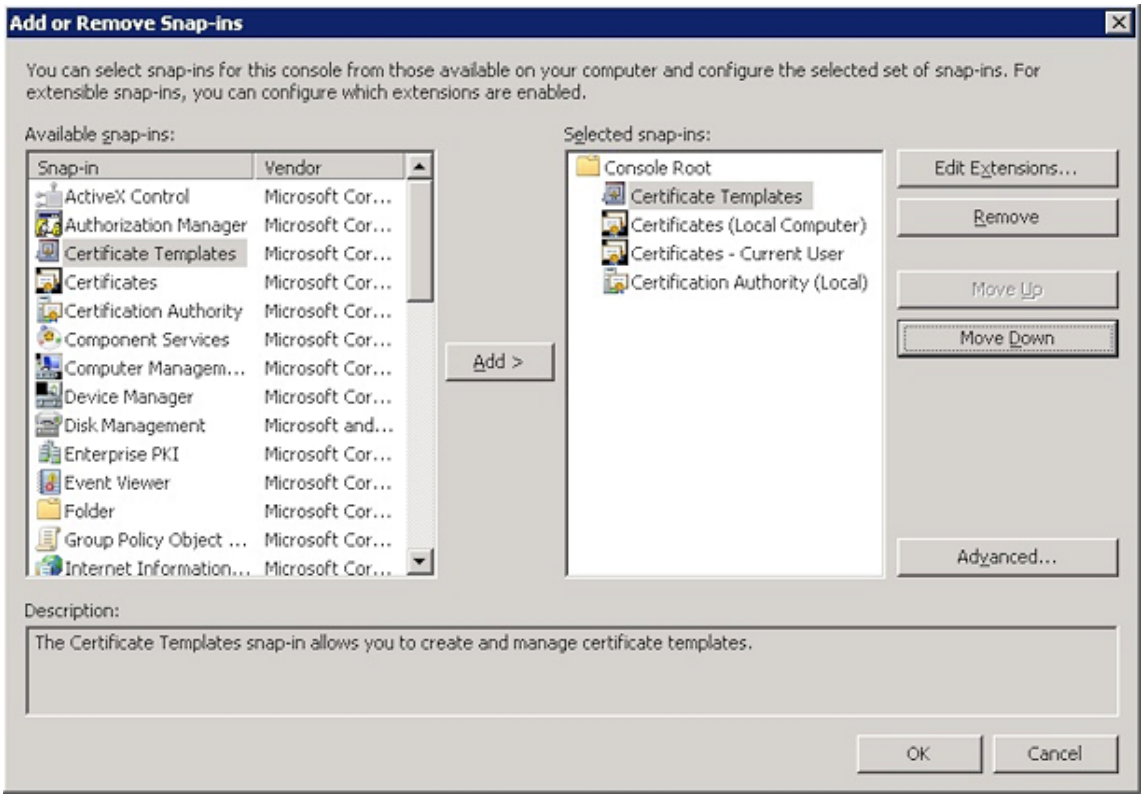
  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```

  A desativação da reutilização da sessão SSL desativa algumas das otimizações que o NetScaler oferece, o que pode resultar em uma redução no desempenho no NetScaler.
- Para configurar a autenticação baseada em certificado para o Exchange ActiveSync, consulte este Blog da Microsoft.
- Se você usa certificados de servidor privados para proteger o tráfego do ActiveSync ao Exchange Server, verifique se os dispositivos móveis têm todos os certificados raiz e intermediários. Caso contrário, a autenticação baseada em certificado não ocorrerá durante a instalação da caixa de correio no Secure Mail. No console do IIS do Exchange, você deve:
  - Adicione um site para uso do XenMobile com o Exchange e associe o certificado de servidor Web.
  - Use a porta 9443.
  - Para esse site, você deve adicionar dois aplicativos, um para “Microsoft-Server-ActiveSync” e um para “EWS”. Por ambos os aplicativos, em **Configurações de SSL**, selecione **Exigir SSL**.
- Assegure que o Secure Mail esteja preparado com o MDX Toolkit mais recente, se necessário para o seu método de implantação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

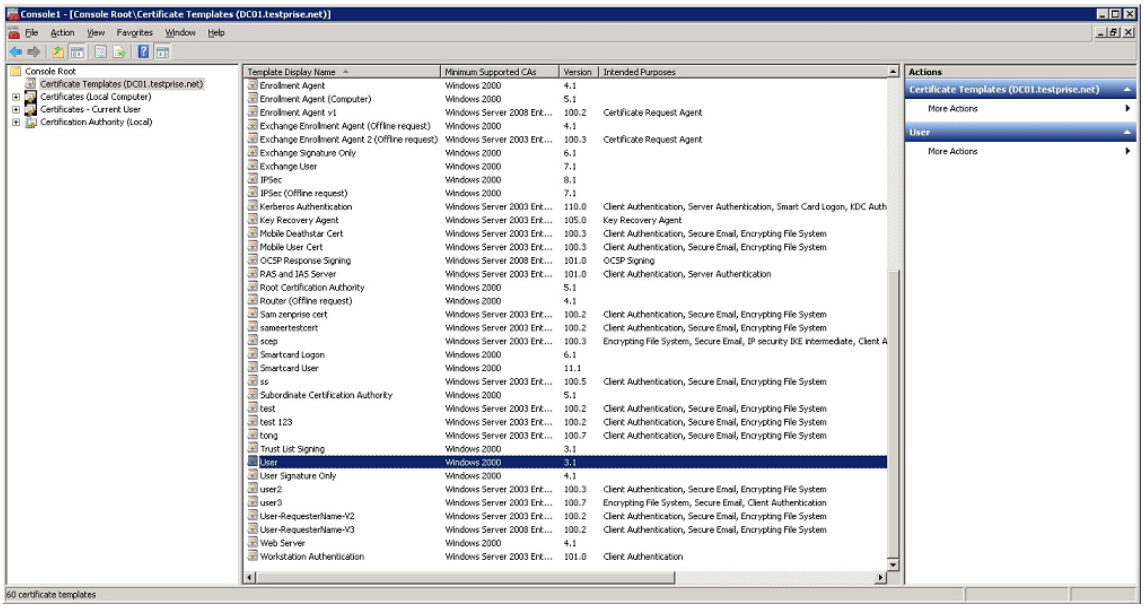
Adicionar um snap-in de certificado ao Console de Gerenciamento Microsoft

1. Abra o console e, em seguida, clique em **Adicionar ou remover snap-ins**.
2. Adicione os seguintes snap-ins:
   - Modelos de Certificado
   - Certificados (Computador Local)
   - Certificados - Usuário Atual
   - Autoridade de Certificação (Local)

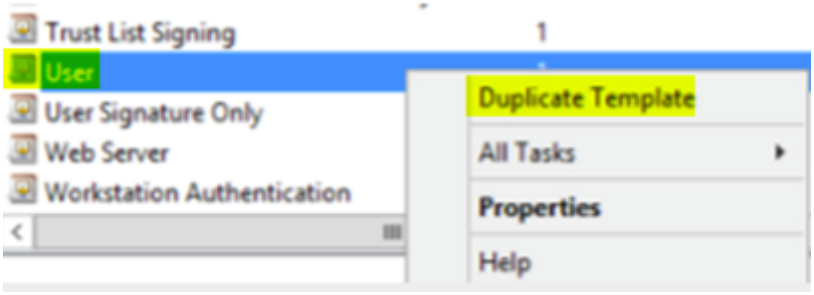


3. Expanda **Modelos de certificado**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Selecione o modelo **Usuário** e **Modelo Duplicado**.

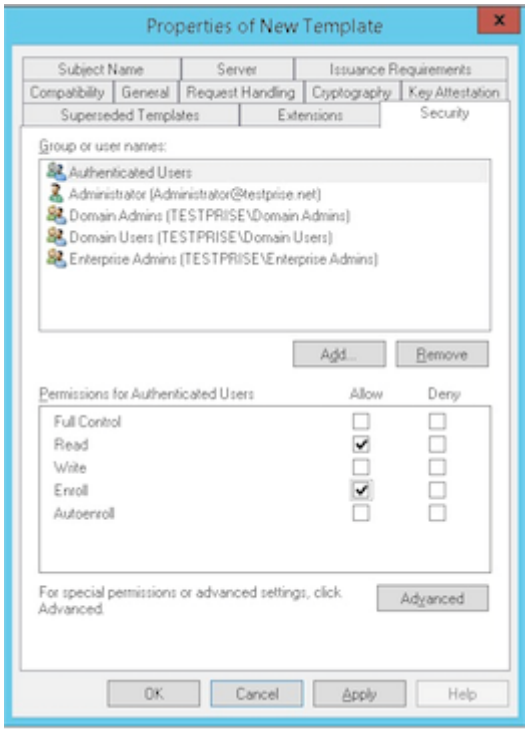


5. Forneça o nome para exibição do Modelo.

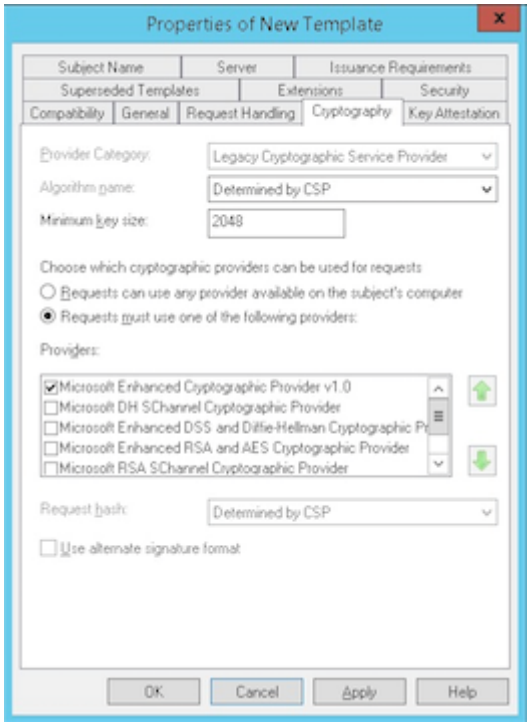
> Importante:
>
> Marque a caixa de seleção **Publicar certificado no Active Directory** somente se necessário. Se essa opção estiver marcada, todos os certificados cliente do usuário serão criados no Active Directory, o que pode atravancar o banco de dados do Active Directory.

6. Selecione **Windows 2003 Server** como 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**, selecione a opção **Registrar** na coluna **Permitir** dos usuários autenticados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

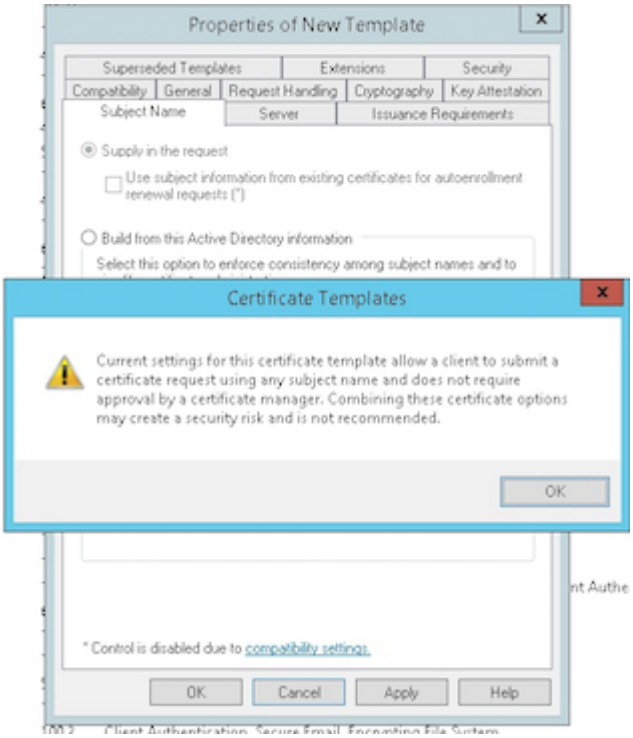


8. Em **Criptografia**, assegure-se de fornecer o tamanho da chave. Você depois insere o tamanho da chave durante a configuração do XenMobile.



9. Em **Nome da entidade**, selecione **Fornecer na solicitação**. Aplique as alterações e, em seguida, salve.

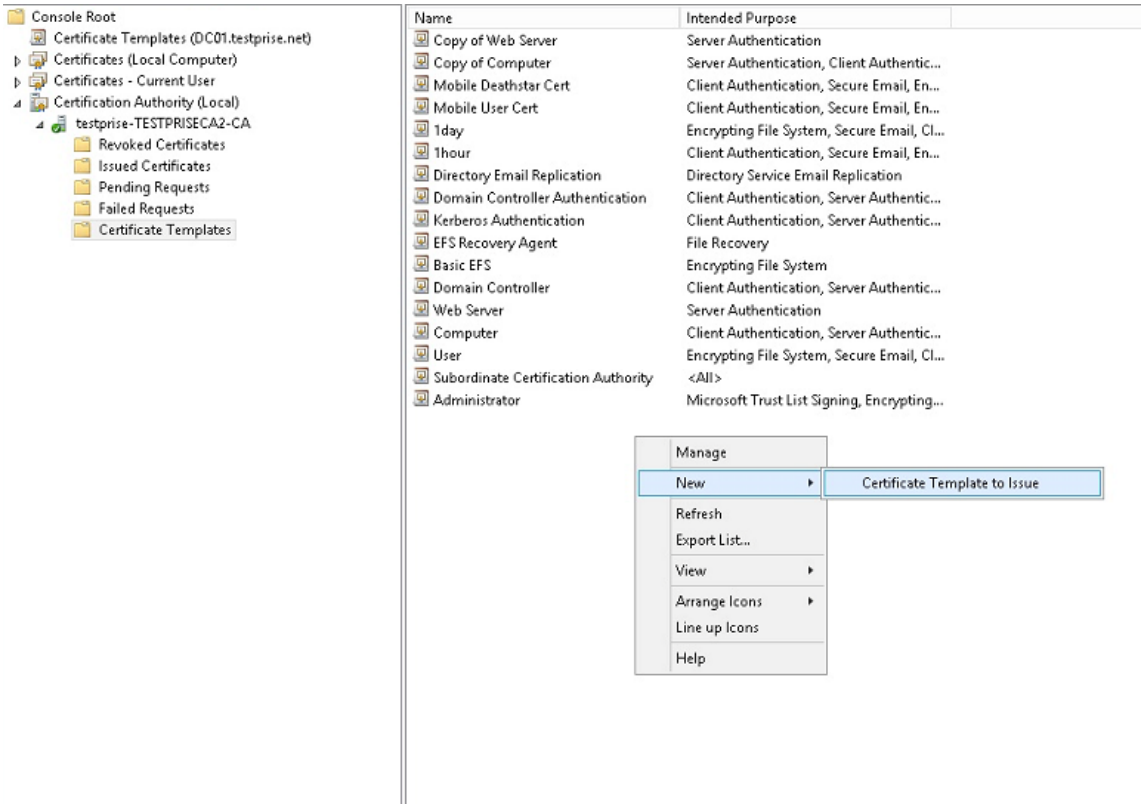
© 1999-2019 Citrix Systems, Inc. All rights reserved.



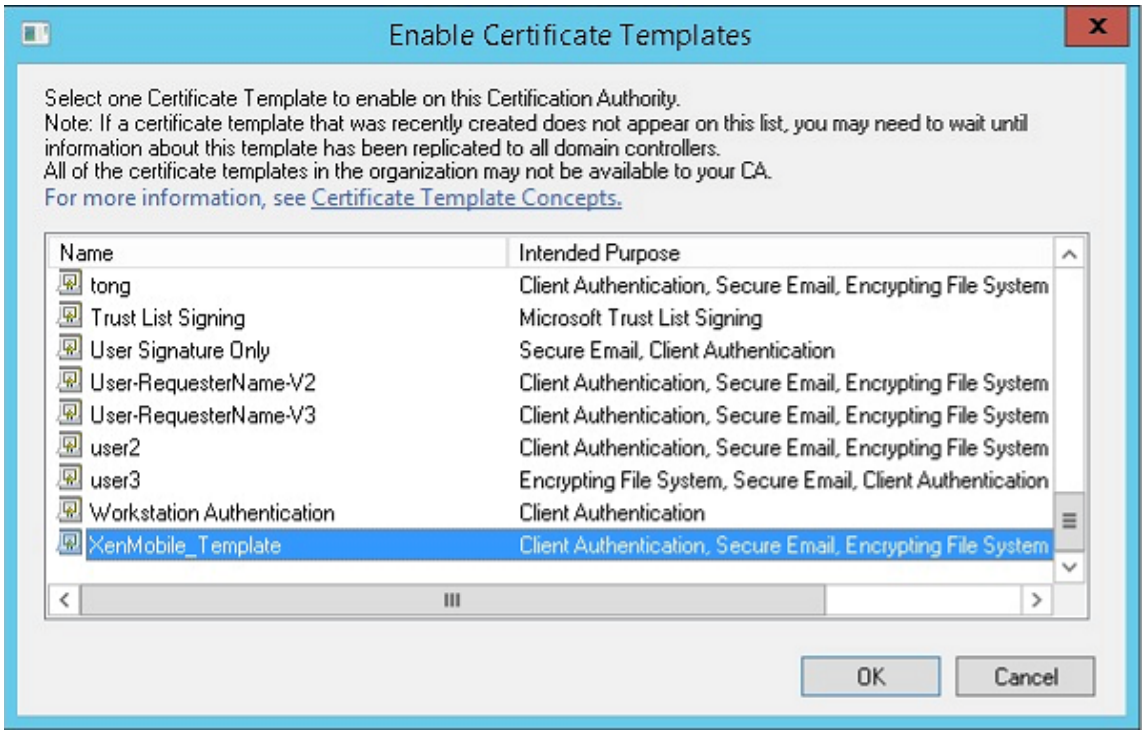
Adição de um modelo à Autoridade de Certificação

1. Vá para **Autoridade de certificação** e selecione **Modelos de certificado**.
2. Clique com o botão direito do mouse no painel direito e selecione **Novo > Modelo de certificado a ser emitido**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



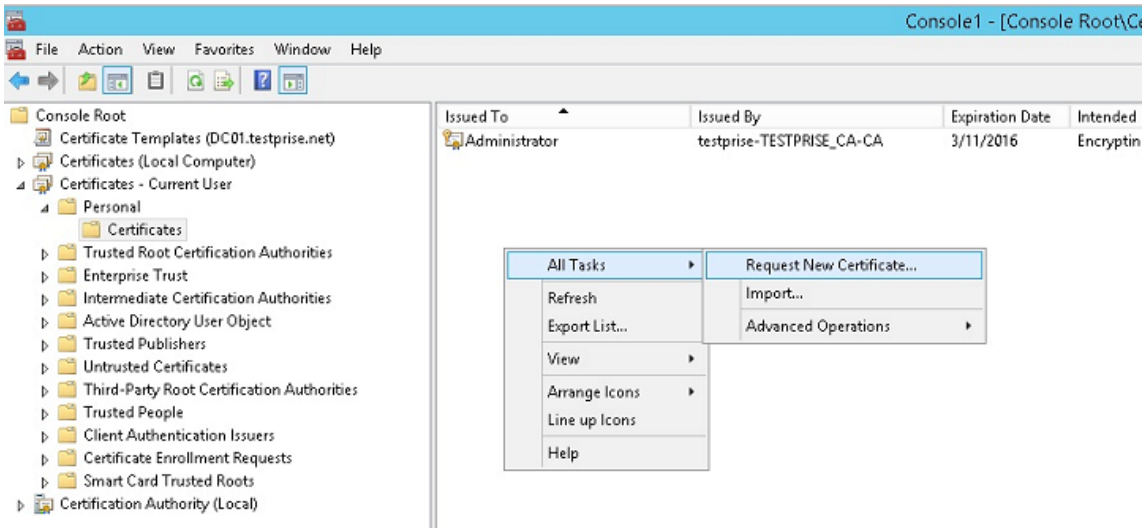
3. Selecione o modelo que você criou na etapa anterior e clique em **OK** para adicioná-lo à **Autoridade de certificação**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

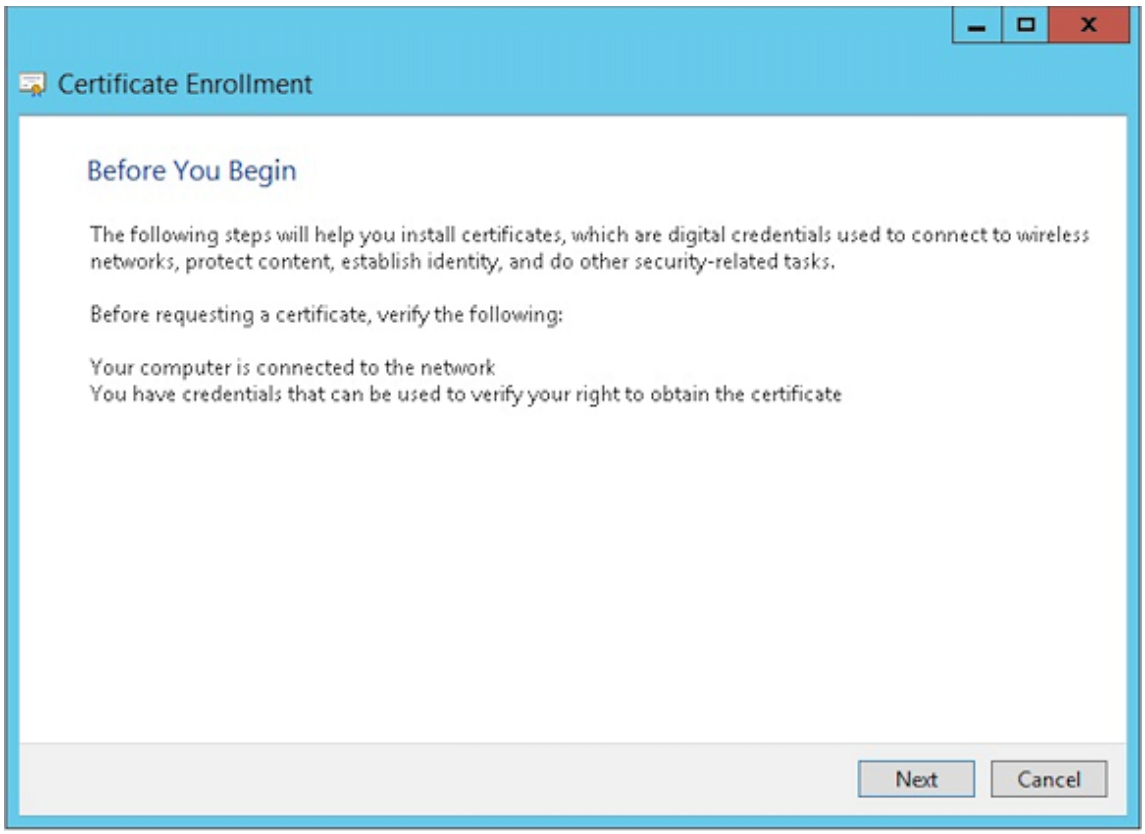
Criação de um certificado PFX do servidor de AC

1. Crie um certificado .pfx de usuário usando a conta de serviço com a qual você fez login. O .pfx é carregado no XenMobile, que 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 do mouse no painel direito e clique em **Solicitar novo certificado**.



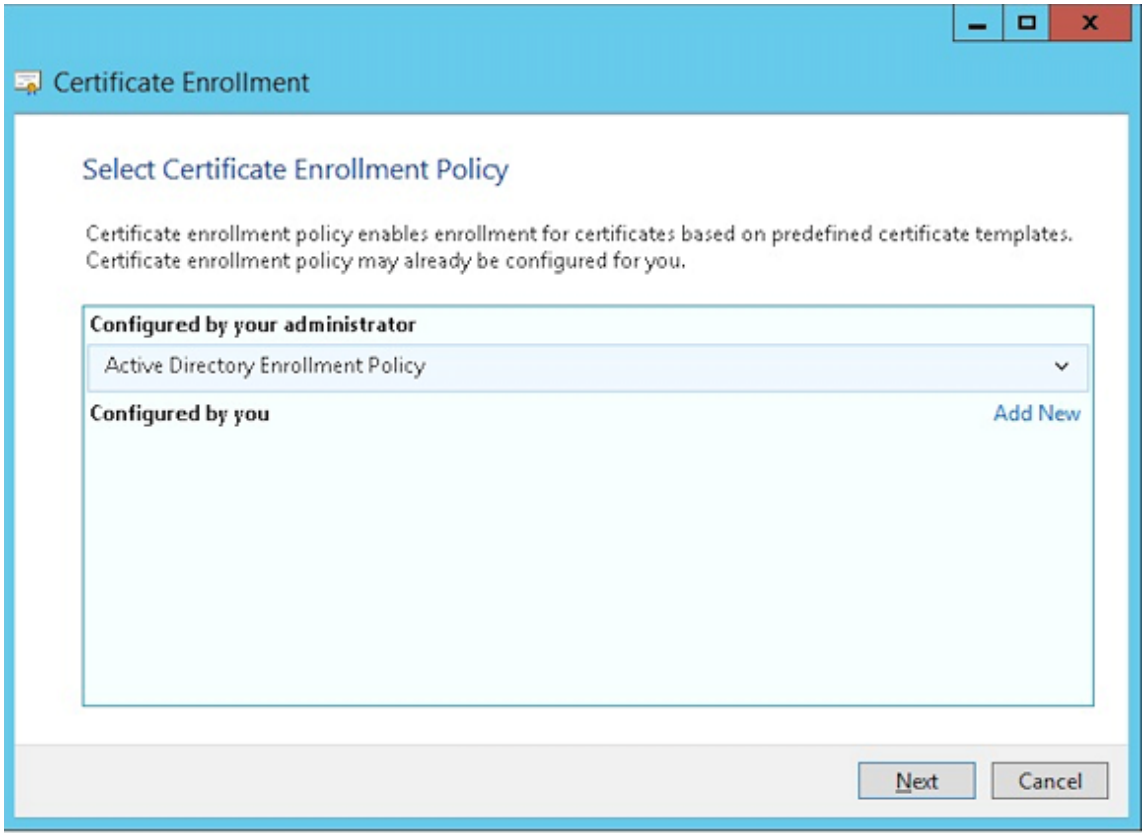
4. A tela **Registro de certificado** é exibida. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



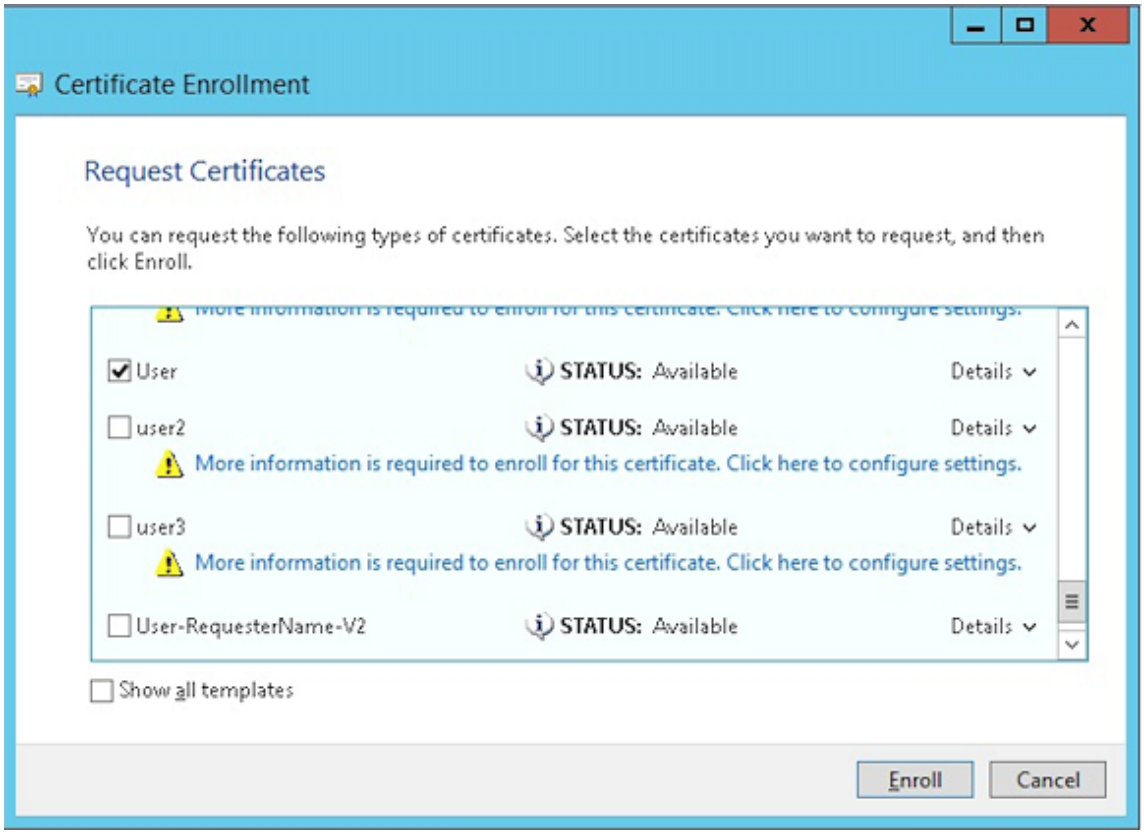
5. Selecione **Política de registro do Active Directory** e clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

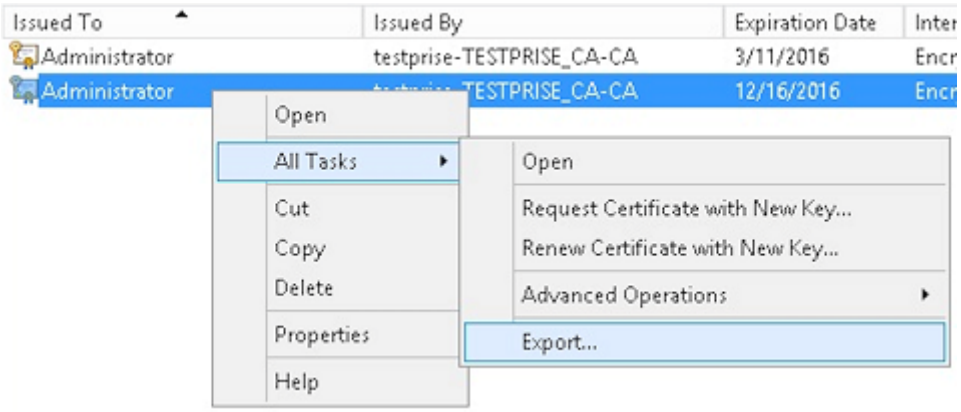


6. Selecione o modelo **Usuário** e clique em **Registrar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

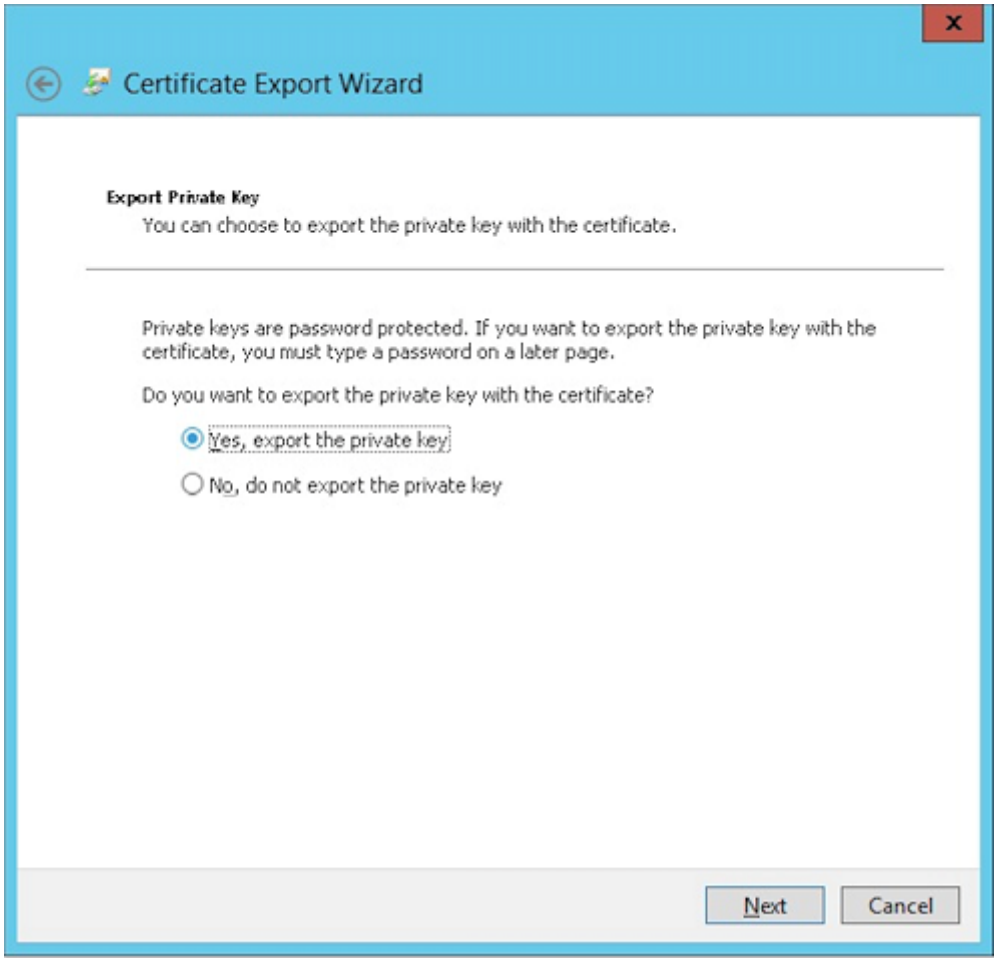


7. Exporte o arquivo .pfx criado na etapa anterior.



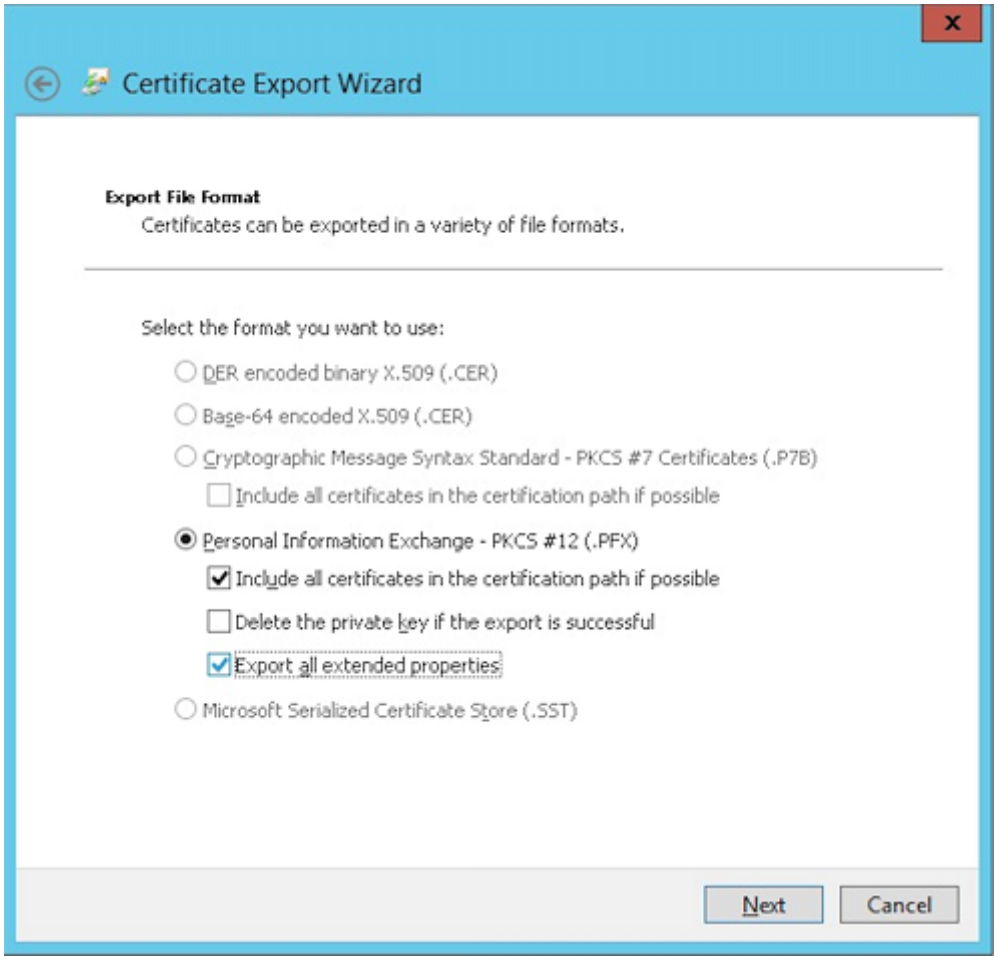
8. Clique em **Sim, exportar a chave privada**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



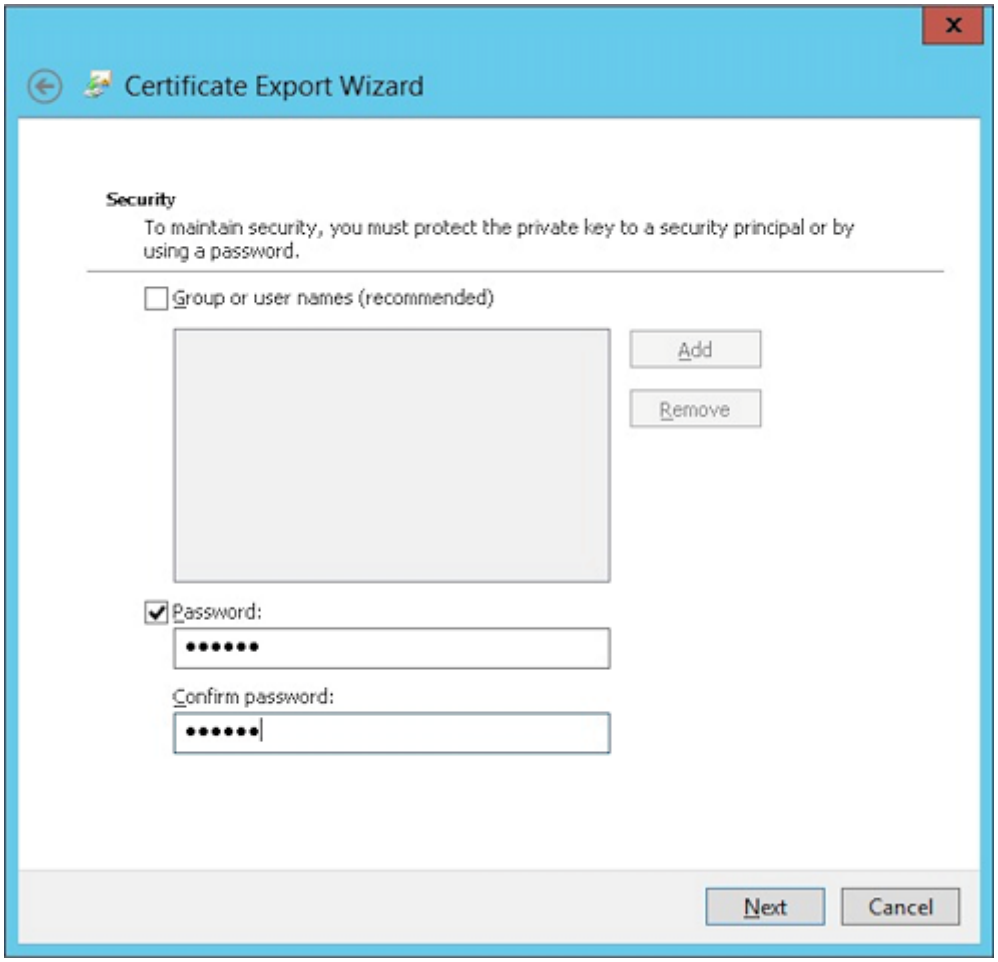
9. Selecione **Incluir todos os certificados no caminho de certificação, se possível** e marque a caixa de seleção **Exportar todas as propriedades estendidas**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



10. Defina uma senha para usar quando carregar o certificado para o XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

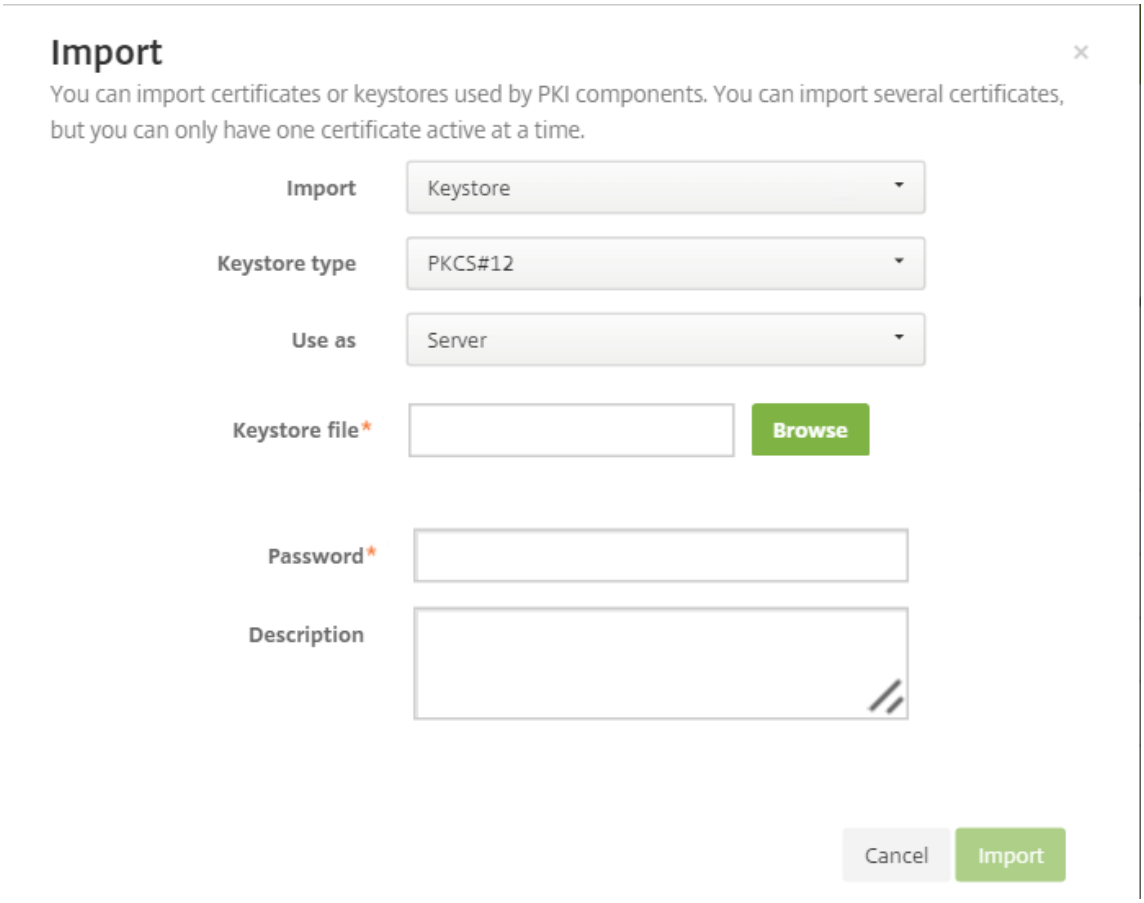


11. Salve o certificado no seu disco rígido.

Upload do certificado no XenMobile

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Clique em **Certificados** e em **Importar**.
3. Insira os seguintes parâmetros:
   - **Importar:** Keystore
   - **Tipo de Keystore:** PKCS #12
   - **Usar como:** Servidor
   - **Arquivo de keystore**: clique em Procurar para selecionar o certificado .pfx que você acabou de criar.
   - **Senha:** insira a senha criada para esse certificado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



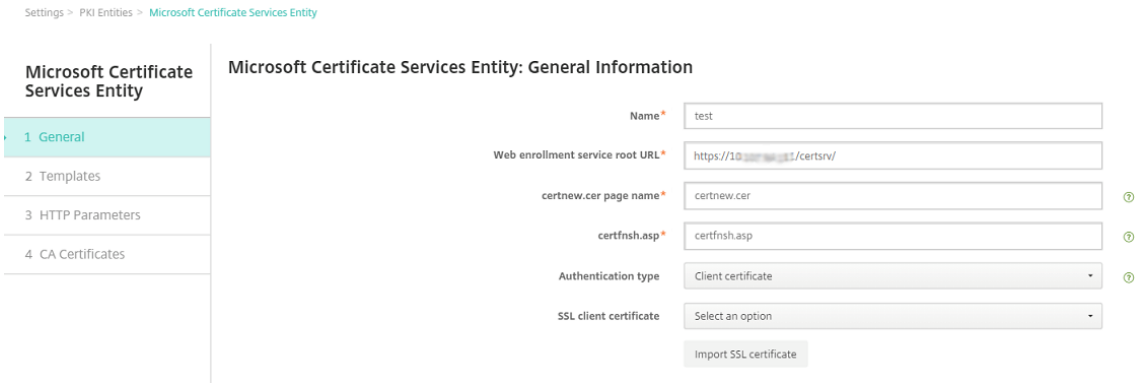
4. Clique em **Importar**.
5. Verifique se o certificado foi instalado corretamente. Um certificado instalado corretamente é exibido como um certificado de usuário.

Criação da entidade PKI de autenticação baseada em certificado

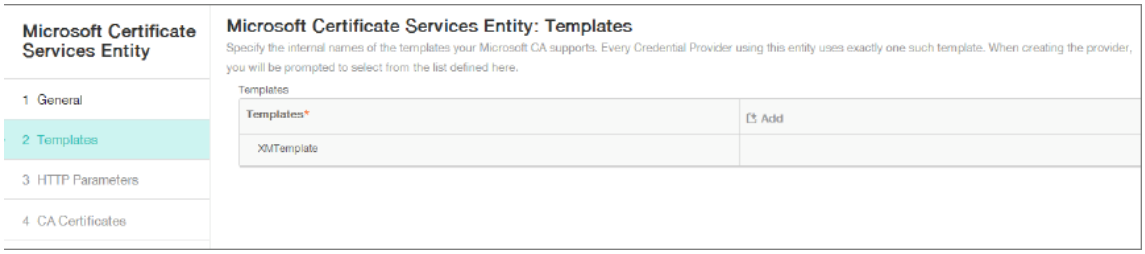
1. Em **Configurações**, vá para **Mais > Gerenciamento de certificados > Entidades PKI**.
2. Clique em **Adicionar** e em **Entidade de serviços de certificado da Microsoft**. A tela **Entidade de serviços de certificado da Microsoft: informações gerais** é exibida.
3. Insira os seguintes parâmetros:
   - **Nome:** digite qualquer nome.
   - **URL raiz do serviço de registro na Web:** `https://RootCA-URL/certsrv/` (Lembre-se de adicionar a última barra (/) ao caminho da URL.)
   - **Nome da página certnew.cer:** certnew.cer (valor padrão)
   - **certfnsh.asp:** certfnsh.asp (valor padrão)
   - **Tipo de autenticação:** certificado cliente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

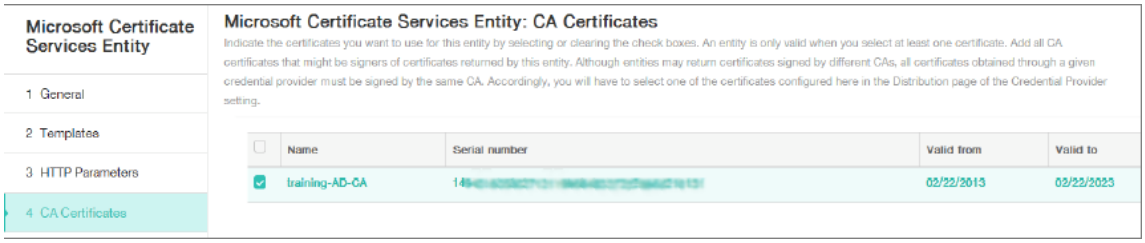
- **Certificado de cliente SSL:** Selecione o certificado de usuário a ser usado para emitir o certificado cliente do XenMobile.



4. Em **Modelos**, adicione o modelo que você criou ao configurar o certificado da Microsoft. Não adicione espaços.



5. Ignore os Parâmetros HTTP e, em seguida, clique em **Certificados de CA**.
6. Selecione o nome da AC raiz que corresponde ao seu ambiente. Essa AC raiz é parte da cadeia importada do certificado cliente do XenMobile.



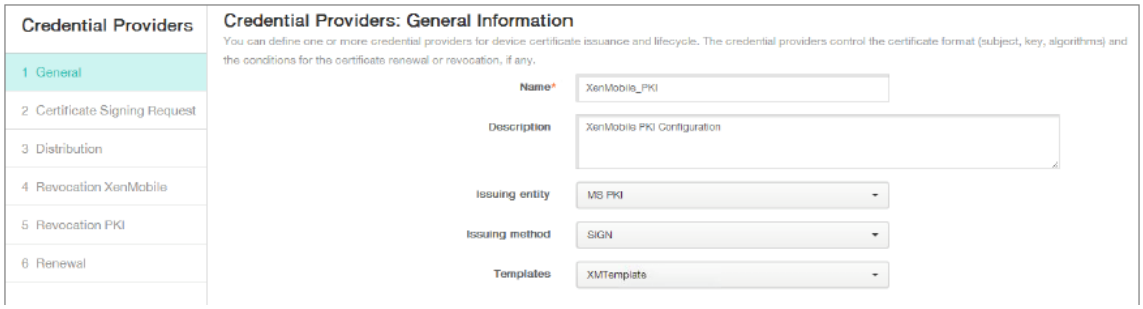
7. Clique em **Salvar**.

Configuração dos 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Nome:** digite qualquer nome.
- **Descrição:** digite uma descrição
- **Entidade de emissão:** selecione a entidade PKI criada anteriormente.
- **Método de emissão:** SIGN
- **Modelos:** selecione o modelo adicionado sob a 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:** SHA1withRSA
   - **Nome de entidade:** `cn=$user.username`

   Para **Nomes de entidade alternativos**, clique em **Adicionar** e insira os seguintes parâmetros:

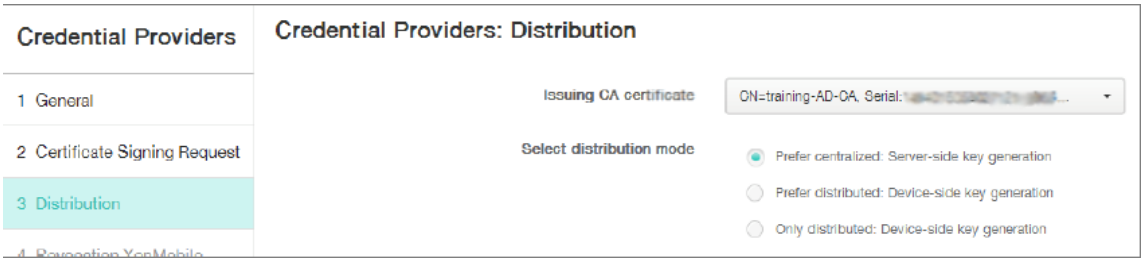
   - **Tipo:** nome UPN
   - **Valor:** `$user.userprincipalname`



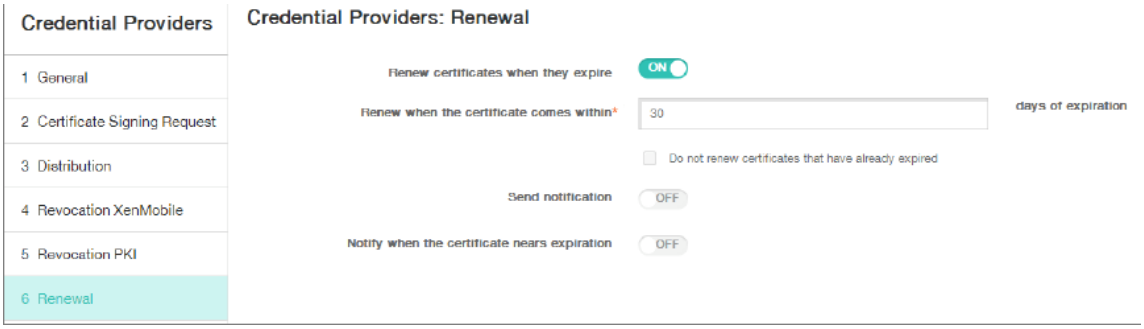
5. Clique em **Distribuição** e insira os seguintes parâmetros:

   - **Emissão de certificado de CA:** selecione a CA emissora que assinou o Certificado cliente do XenMobile.
   - **Selecionar modo de distribuição:** selecione **Preferir modo centralizado: geração de chaves do lado do servidor**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



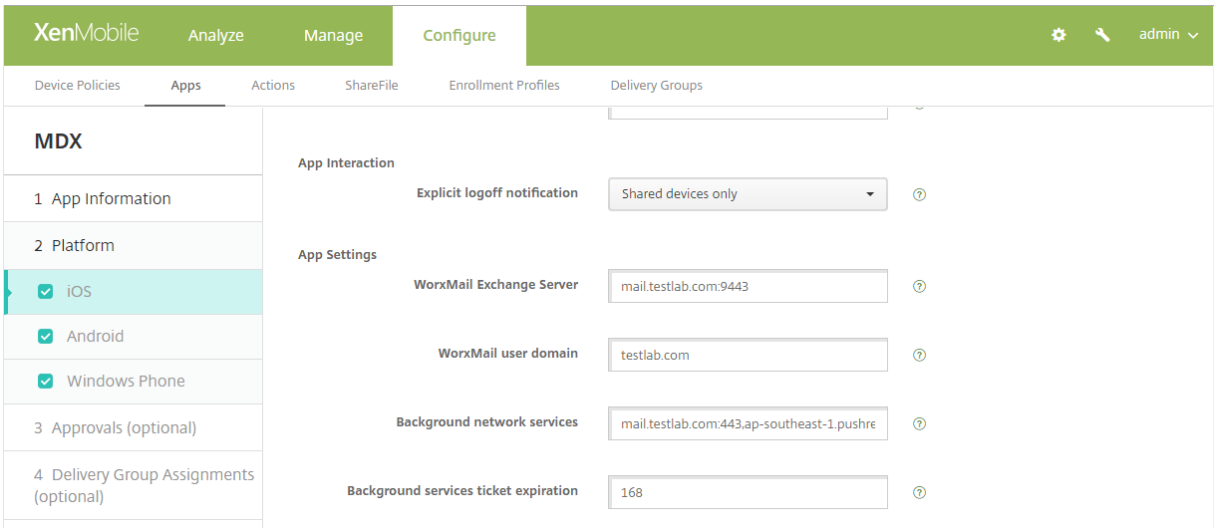
6. Para as duas próximas seções, **Revogação XenMobile** e **Revogação PKI**, defina os parâmetros conforme necessário. Neste exemplo, as duas opções são ignoradas.
7. Clique em **Renovação**.
8. Para **Renovar os certificados quando eles expirarem**, selecione **I**.
9. Deixe todas as outras configurações como o padrão ou altere-as conforme necessário.



10. Clique em **Salvar**.

Configuração do Secure Mail para usar a autenticação baseada em certificado

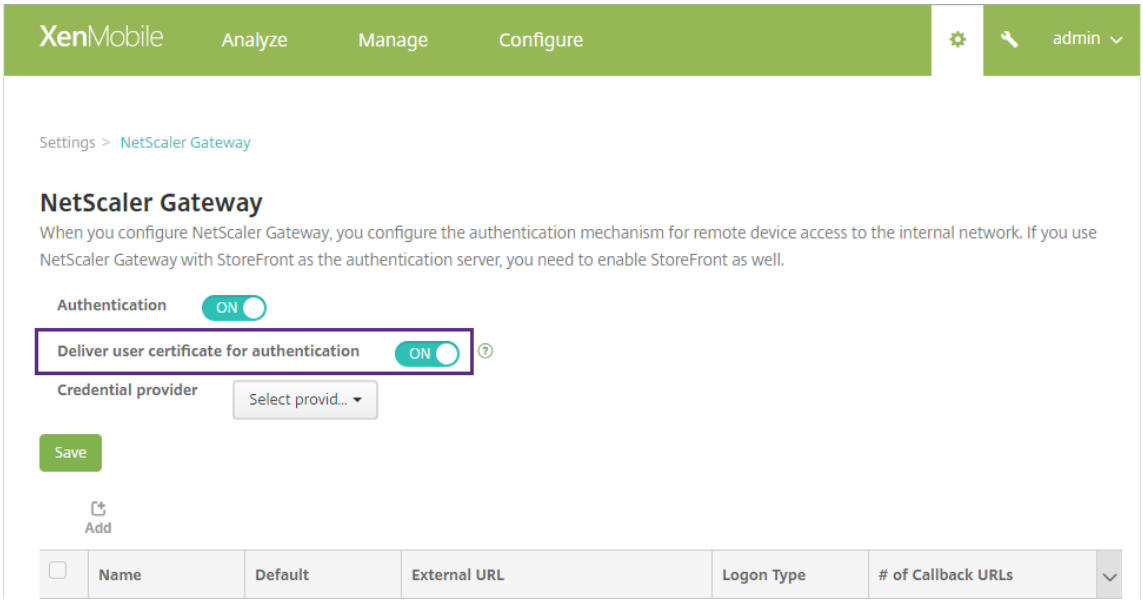
Quando você adicionar o Secure Mail ao XenMobile, defina as configurações do Exchange em **Configurações de Aplicativo**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

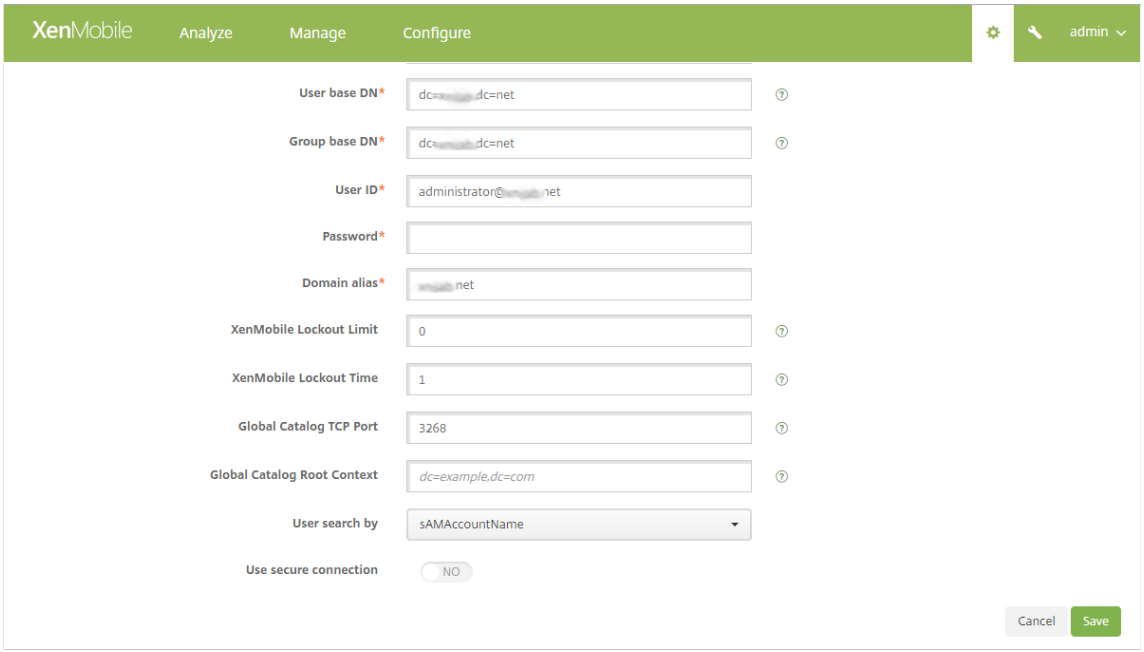
Configuração da entrega de certificado do NetScaler no XenMobile

1. Faça login no console XenMobile e clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Em **Servidor**, clique em **NetScaler Gateway**.
3. Se o NetScaler Gateway ainda não foi adicionado, clique em **Adicionar** e especifique as configurações:
   - **URL externa:** `https://YourNetScalerGatewayURL`
   - **Tipo de login:** Certificado
   - **Senha obrigatória**: desativado
   - **Definir como padrão:** ativado
4. Para **Entregar certificado de usuário para autenticação**, selecione **I**.



5. Para **Provedor de credenciais**, selecione um provedor e clique em **Salvar**.
6. Para usar atributos de sAMAccount nos certificados de usuário como alternativa para o nome UPN, configure o conector LDAP no XenMobile da seguinte maneira: vá para **Configurações > LDAP**, selecione o diretório e clique em **Editar** e selecione **sAMAccountName** em **Pesquisa de usuário por**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Ativar o PIN da Citrix e o cache de senha de usuário

Para ativar o PIN da Citrix e a senha do usuário em cache, vá para **Configurações > Propriedades do Cliente** e assinale as caixas de seleção para **Ativar PIN da Citrix** e **Ativar armazenamento em cache da senha do usuário**. Para obter mais informações, consulte Propriedades do cliente.

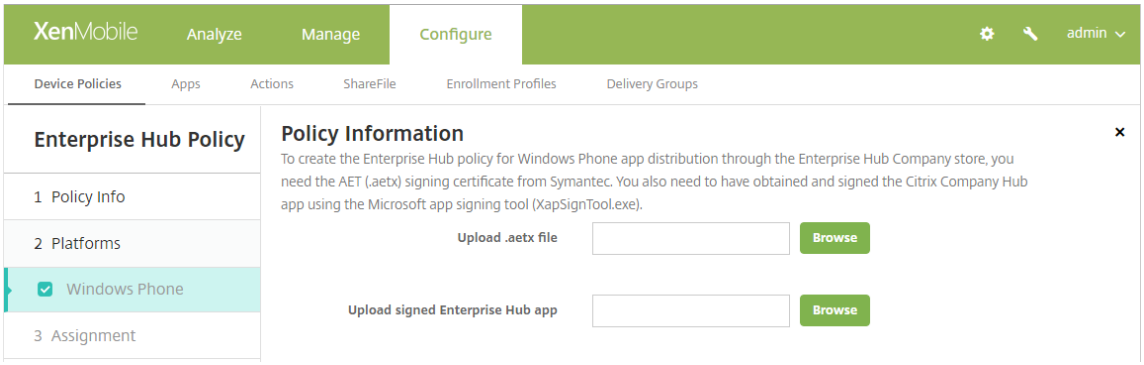
Criação de uma política de Hub Empresarial para o Windows Phone

Para dispositivos Windows Phone, você deve criar uma política de dispositivo de Hub Empresarial para fornecer o arquivo AETX e o Secure Hub cliente.

> Nota:
>
> Certifique-se de que os arquivos AETX e Secure Hub usem:
>
> - O mesmo certificado corporativo do provedor de certificados.
> - Mesmo ID de Fornecedor da conta de desenvolvedor da Windows Store.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.
2. Clique em **Adicionar** e, em **Mais > Agente XenMobile**, clique em **Hub empresarial**.
3. Após atribuir um nome à política, selecione o arquivo .AETX correto e o aplicativo Secure Hub assinado para o hub empresarial.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Atribua a política a grupos de entrega e salve-a.

Solução de problemas da sua configuração de certificado cliente

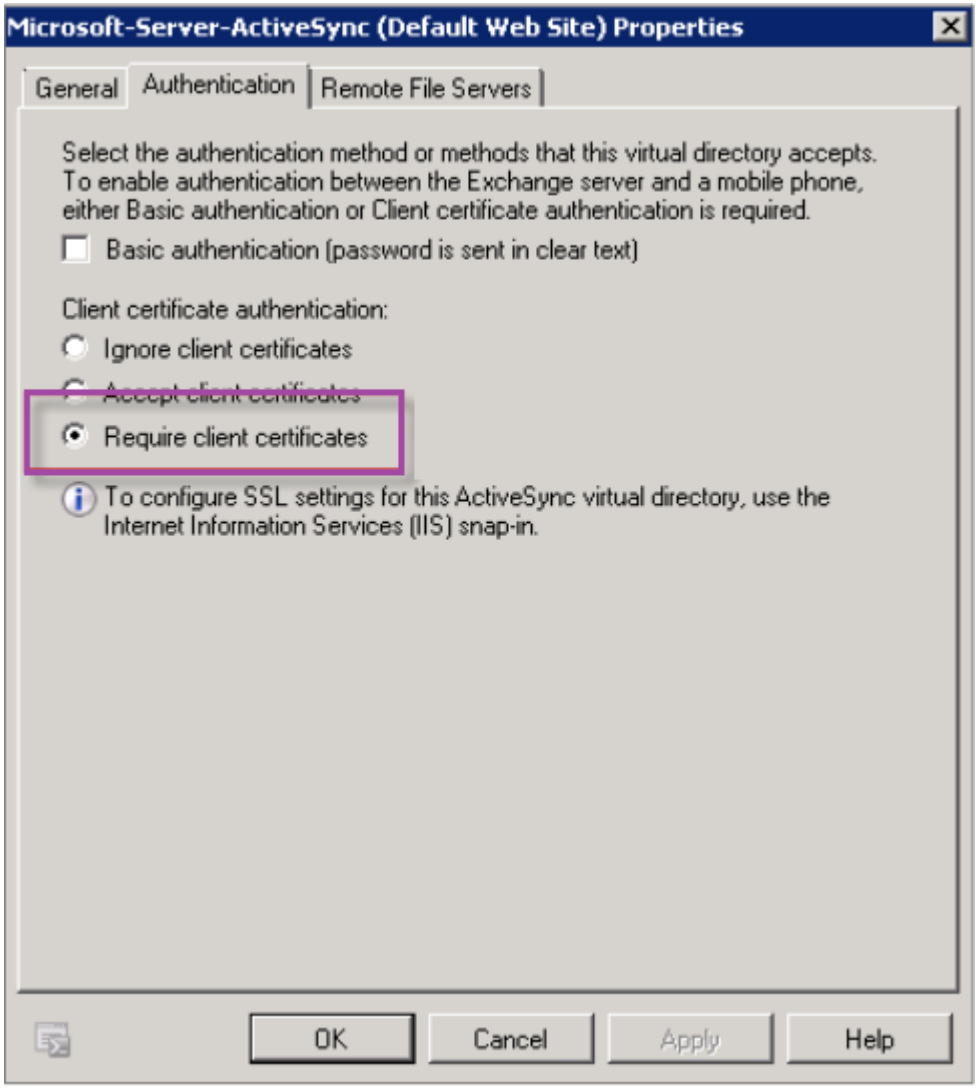
Após uma configuração com êxito da configuração anterior mais a configuração do NetScaler Gateway, o usuário fluxo de trabalho é o seguinte:

1. Os usuários registram seus dispositivos móveis.
2. O XenMobile solicita que os usuários criem um PIN da Citrix.
3. Os usuários são redirecionados para a XenMobile Store.
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 de 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 a sua configuração.

Se os usuários puderem baixar e instalar o Secure Mail, mas durante a configuração da caixa de correio o Secure Mail não termina a configuração:

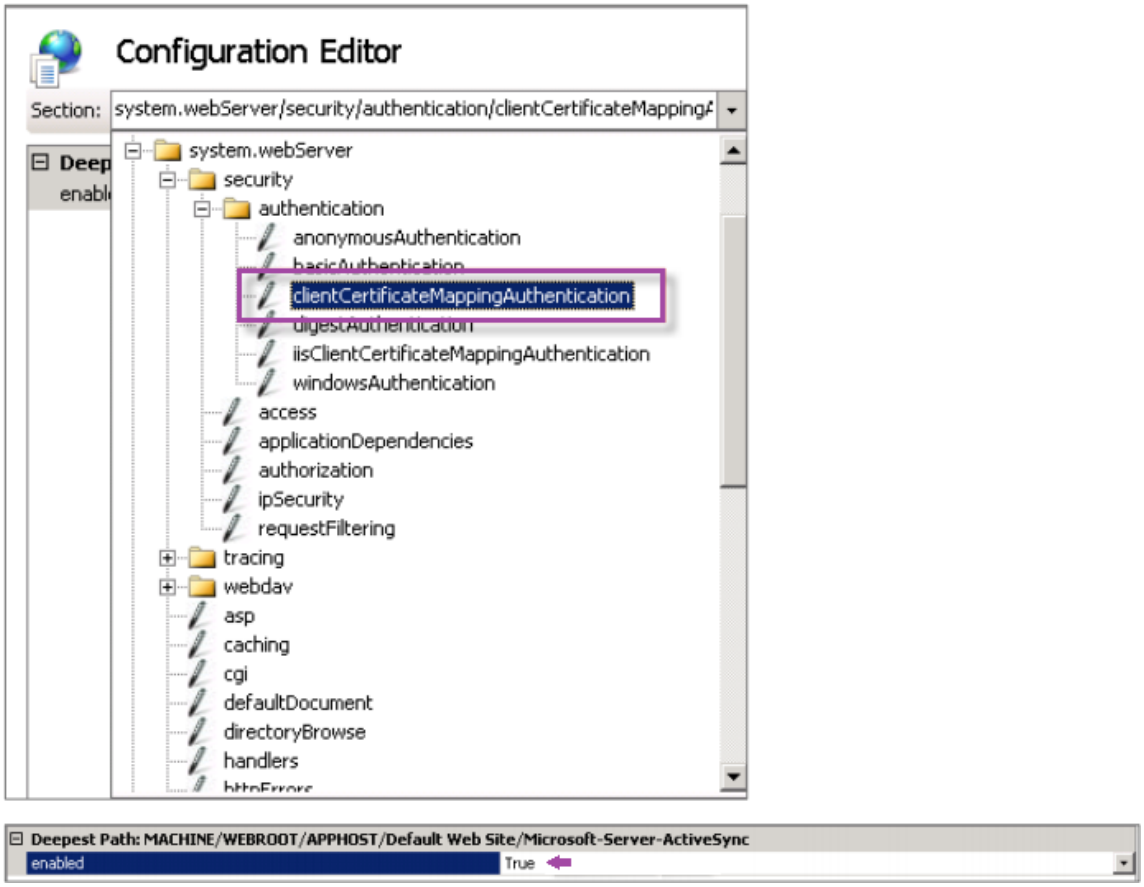
1. Se o Microsoft Exchange Server ActiveSync usa certificados de servidor SSL privados para proteger o tráfego, verifique se os certificados raiz/intermediário estão instalados no dispositivo móvel.
2. Verifique se o tipo de autenticação selecionado para o ActiveSync é **Exigir certificados de cliente**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. No Microsoft Exchange Server, verifique o site **Microsoft-Server-ActiveSync** para confirmar que a autenticação de mapeamento de certificado de cliente esteja ativada. Por padrão, a autenticação de mapeamento de certificado de cliente está desativada. A opção está sob **Editor de Configurações > Segurança > Autenticação**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Nota: depois de selecionar **True**, clique em **Aplicar** para que as alterações tenham efeito.

4. Verifique as configurações do NetScaler 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 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 esta entrada:

   Credenciais do NetScaler Gateway: credencial solicitada, CertId=

Para validar se a negociação do certificado de cliente está habilitada

1. Execute este comando `netsh` para mostrar a configuração de certificado SSL que está vinculada ao website do IIS:

   ```
   netsh http show sslcert
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Se o valor de **Negociar certificado de cliente** for **Desativado**, execute o seguinte comando para ativá-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=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

Se não for possível fornecer certificados raiz/intermediários a um dispositivo Windows Phone 8.1 por meio do XenMobile:

- Envie arquivos de certificados raiz/intermediário (.cer) por email ao dispositivo Windows Phone 8.1 e instale-os diretamente.

Se o Secure Mail não for instalado com êxito no Windows Phone 8.1, verifique o seguinte:

- O arquivo Application Enrollment Token (.AETX) é entregue por meio do XenMobile usando a política de dispositivo de hub empresarial.
- O arquivo Application Enrollment Token foi criado usando o mesmo certificado empresarial do provedor de certificados usado para preparar o Secure Mail e assinar aplicativos do Secure Hub.
- O mesmo ID de Fornecedor é usado para assinar e preparar o Secure Hub, o Secure Mail e o Application Enrollment Token.

Entidades PKI

April 15, 2019

Uma configuração de entidade Infraestrutura de Chave Pública (PKI) do XenMobile representa um componente que realiza operações reais da PKI (emissão, revogação e informações de status). Esses componentes são internos ou externos ao XenMobile. Os componentes internos são conhecidos como discricionários. Os componentes externos fazem parte da sua infraestrutura corporativa.

O XenMobile é compatível com os seguintes tipos de entidades PKI:

- PKIs Genéricas (GPKIs)

O suporte do XenMobile Server GPKI inclui PKI gerenciada da Symantec.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Serviços de Certificado da Microsoft
- Autoridades de Certificação (CAs) Discricionárias

O XenMobile é compatível com os seguintes servidores de AC:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Conceitos de PKI comuns

Independentemente do tipo, cada entidade PKI tem um subconjunto dos seguintes recursos:

- **Assinar:** emitir um novo certificado com base em uma Solicitação de Assinatura de Certificado (CSR).
- **Obter:** recuperar um certificado e um par de chaves existentes.
- **Revogar:** revogar um certificado cliente.

Sobre certificados AC

Quando você configura uma entidade PKI, indique ao XenMobile qual certificado AC será o signatário dos certificados emitidos por (ou recuperados de) essa entidade. Essa entidade PKI pode retornar certificados (obtidos ou assinados recentemente) assinados por qualquer número de ACs diferentes.

Forneça o certificado de cada uma dessas CAs como parte da configuração da entidade PKI. Para fazer isso, carregue os certificados no XenMobile e faça referência a eles na entidade PKI. Para CAs discricionárias, o certificado é, implicitamente, o certificado de AC de assinatura. Para entidades externas, você deve especificar o certificado manualmente.

> Importante:
>
> Quando você cria 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: `! : $ ( )## % + * ~ ? | { } [ ]`

PKI Genérica

O protocolo PKI Genérica (GPKI) é um protocolo proprietário do XenMobile em execução em uma camada do Serviço Web SOAP para fins de interface uniforme com várias soluções de PKI. O protocolo GPKI define as três operações de PKI fundamentais:

- **Assinar:** o adaptador pode receber CSRs, transmiti-las para a PKI e retornar os certificados recém-assinados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Obter:** o adaptador pode recuperar (restaurar) certificados e pares de chaves existentes (dependendo dos parâmetros de entrada) da PKI.
- **Revogar:** o adaptador pode fazer com que a PKI revogue um determinado certificado.

O receptor do protocolo GPKI é o adaptador GPKI. O adaptador converte as operações fundamentais no tipo específico de PKI para o qual foi criado. Por exemplo, há adaptadores GPKI para RSA e Entrust.

O adaptador GPKI, como um ponto de extremidade dos Serviços da Web SOAP, publica uma definição de Linguagem de Descrição de Serviços da Web (WSDL) autodescritiva. Criar uma entidade PKI GPKI equivale a fornecer ao XenMobile essa definição WSDL, por meio de uma URL ou mediante o carregamento do arquivo em si.

O suporte a cada uma das operações de PKI em um adaptador é opcional. Se um adaptador der suporte a uma determinada operação, considera-se que tem a capacidade correspondente (assinar, obter ou revogar). Cada um desses recursos pode ser associado a um conjunto de parâmetros de usuário.

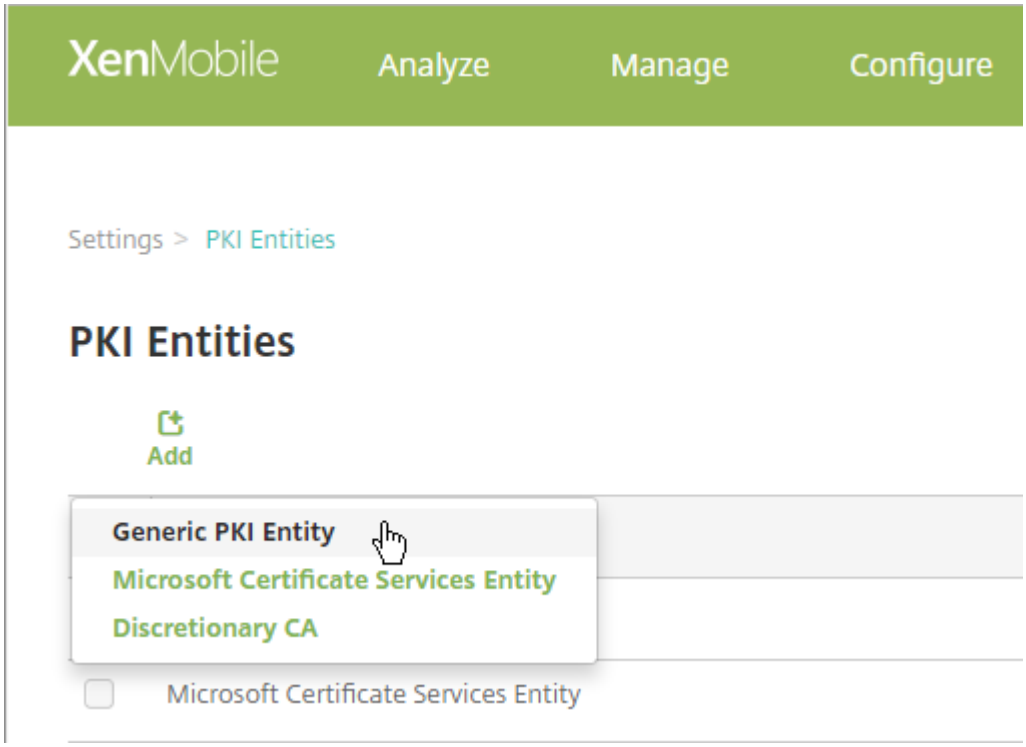
Os parâmetros de usuário são parâmetros que o adaptador GPKI define para uma operação específica e cujos valores você precisa fornecer ao XenMobile. O XenMobile analisa o arquivo WSDL para determinar quais operações o adaptador tem e quais parâmetros o adaptador exige para cada uma dessas operações. Se você preferir, use a autenticação de cliente SSL para proteger a conexão entre o XenMobile e o adaptador GPKI.

Para adicionar uma PKI genérica

1. No console XenMobile, clique em **Configurações > Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

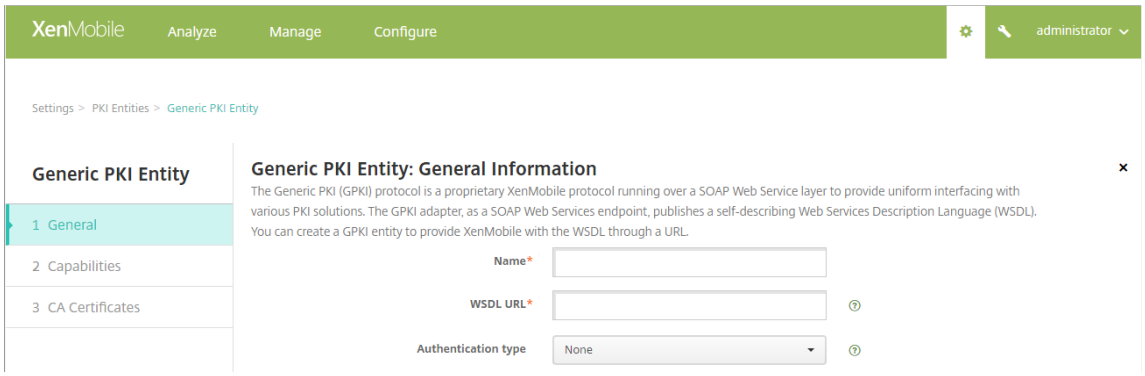
   É exibido um menu de tipos de entidade PKI.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Clique em **Entidade PKI genérica**.

   A página Entidade PKI genérica: Informações gerais é exibida.



4. Na página **Entidade PKI genérica: Informações gerais**, faça o seguinte:

   - **Nome:** digite um nome descritivo para a entidade PKI.
   - **URL WSDL:** digite a localização do WSDL que descreve o adaptador.
   - **Tipo de autenticação:** clique no método de autenticação que você deseja usar.
   - **Nenhum**
   - **HTTP básico:** forneça o nome do usuário e a senha necessários para se conectar ao adaptador.
   - **Certificado cliente:** selecione o certificado de cliente SSL correto.

5. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A página Entidade PKI genérica: Recursos do adaptador é exibida.

6. Na página **Entidade PKI genérica: Recursos do adaptador**, revise as capacidades e os parâmetros associados ao adaptador e clique em **Avançar**.

   A página **Entidade PKI genérica: Emissão de certificados AC** é exibida.

7. Na página Entidade PKI genérica: Emissão de certificados AC, selecione os certificados que você deseja usar para a entidade.

   Embora as entidades possam retornar certificados assinados por diferentes ACs, a mesma AC deve assinar todos os certificados obtidos por meio de um determinado provedor de certificados. Da mesma forma, quando você configurar a definição **Provedor de credenciais**, na página **Distribuição**, selecione um dos certificados configurados aqui.

8. Clique em **Salvar**.

   A entidade é exibida na tabela Entidades PKI.

PKI gerenciada pela Symantec

O suporte do XenMobile Server GPKI inclui PKI gerenciada da Symantec, também chamada MPKI. Esta seção descreve como configurar o Windows Server e o XenMobile Server para PKI gerenciada da Symantec.

Pré-requisitos

- Acesso a infraestrutura de PKI gerenciada da Symantec
- Windows Server 2012 R2 com os seguintes componentes instalados, conforme descrito neste artigo:
  - Java
  - Apache Tomcat
  - Cliente PKI da Symantec
  - Portecle
- Acesso ao site de downloads do XenMobile

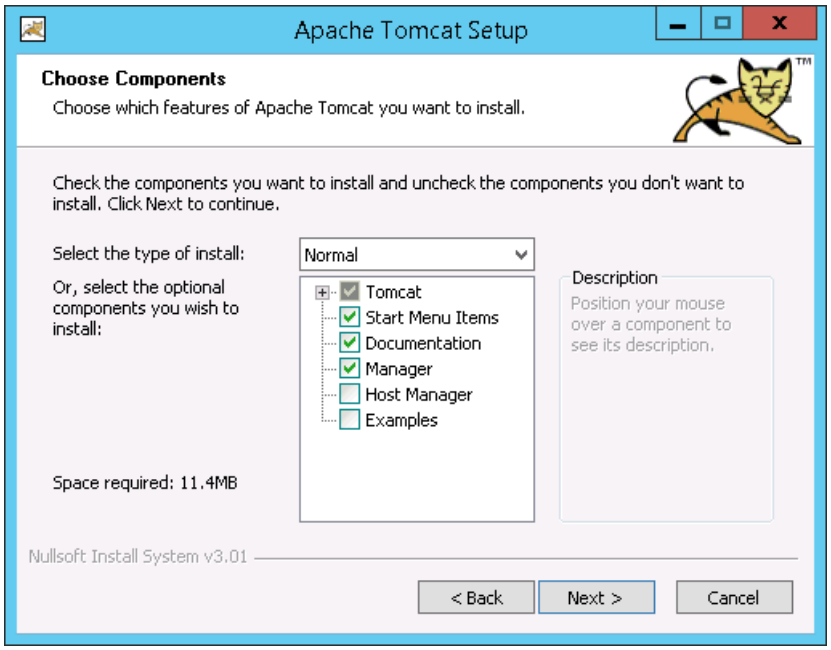
Instalar o Java no Windows Server

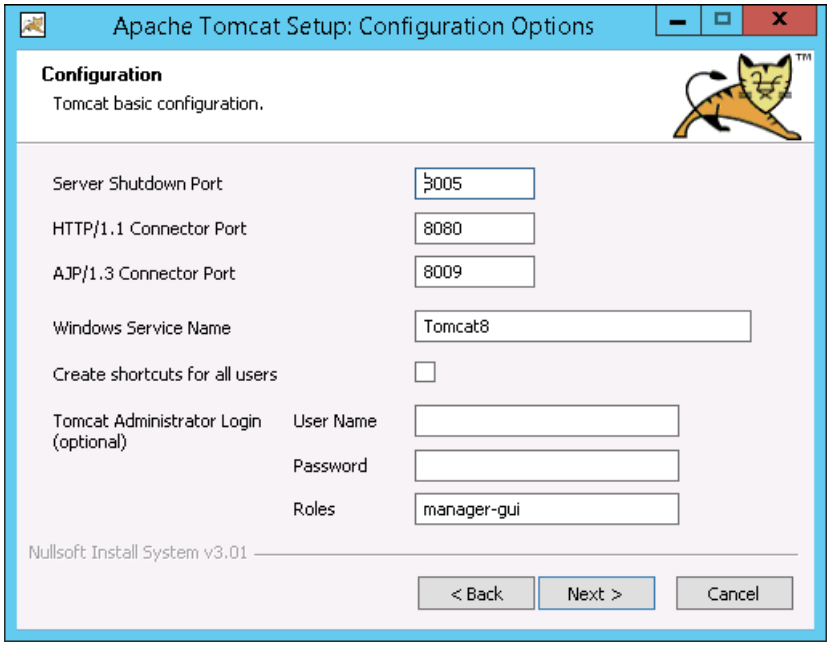
Faça o download do Java em https://java.com/en/download/faq/java_win64bit.xml e instale-o. Na caixa de diálogo Aviso de segurança, clique em **Executar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

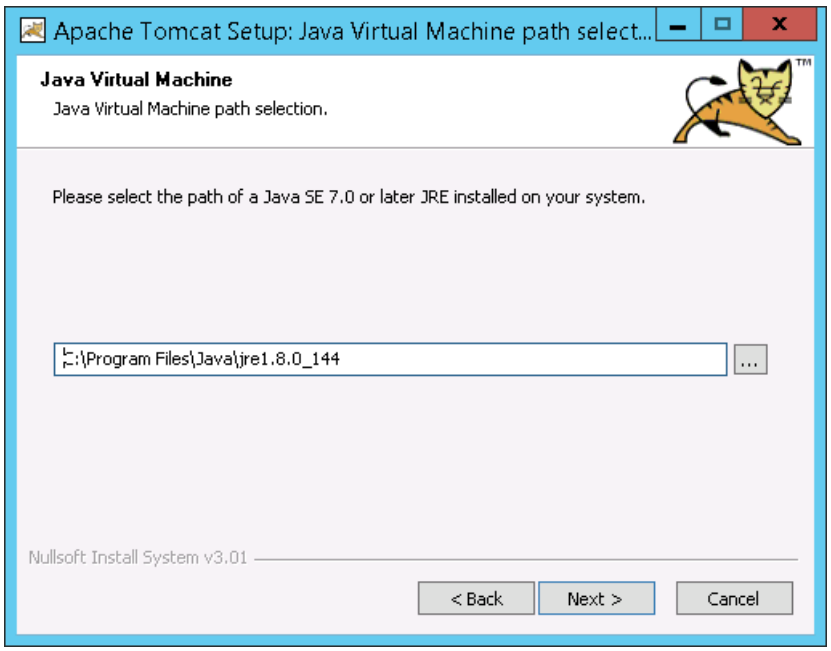
Instalar o Apache Tomcat no Windows Server

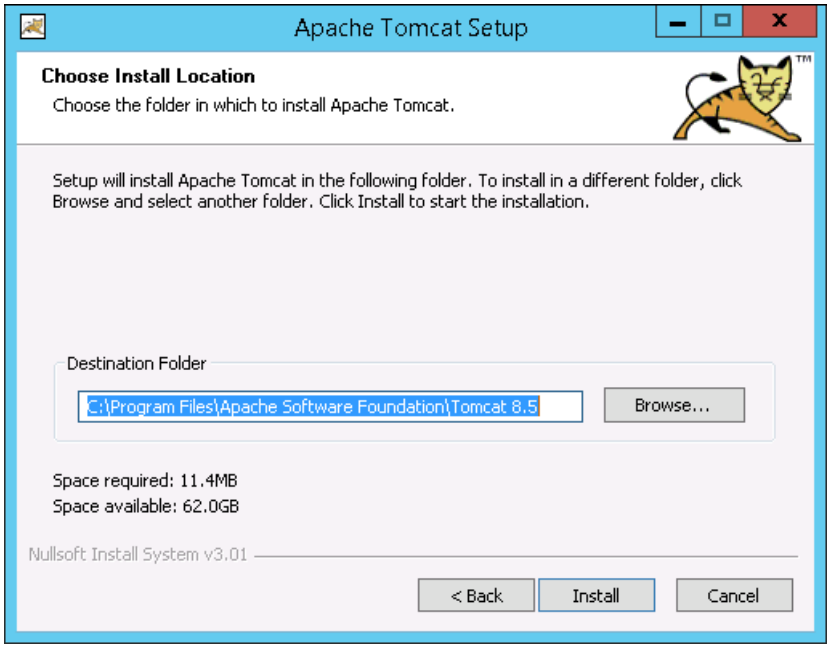
Baixe o instalador de serviços do Windows Apache Tomcat de 32/64 bits em https://tomcat.apache.org/download-80.cgi e depois instale-o. Na caixa de diálogo Aviso de segurança, clique em **Executar**. Complete a configuração do Apache Tomcat, usando os seguintes exemplos como um guia.



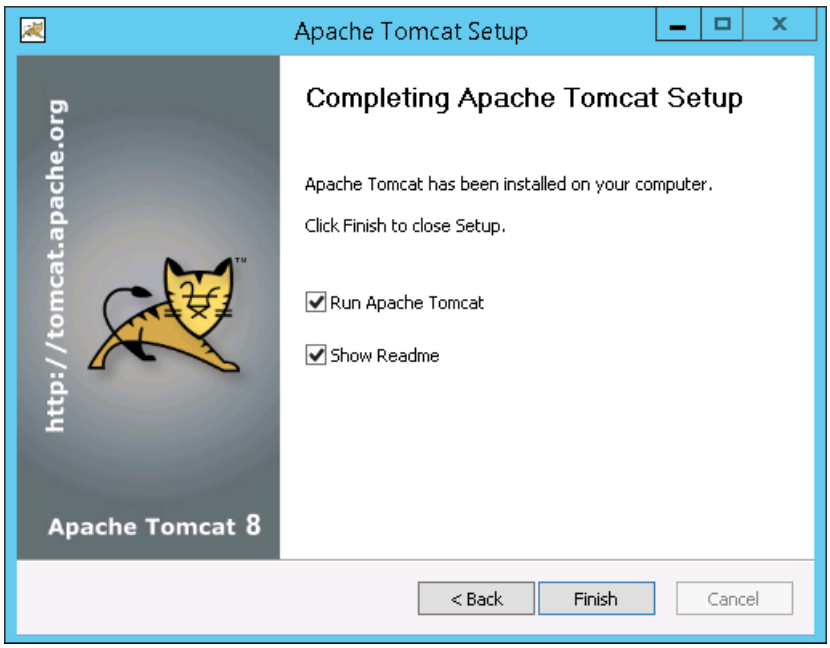


© 1999-2019 Citrix Systems, Inc. All rights reserved.

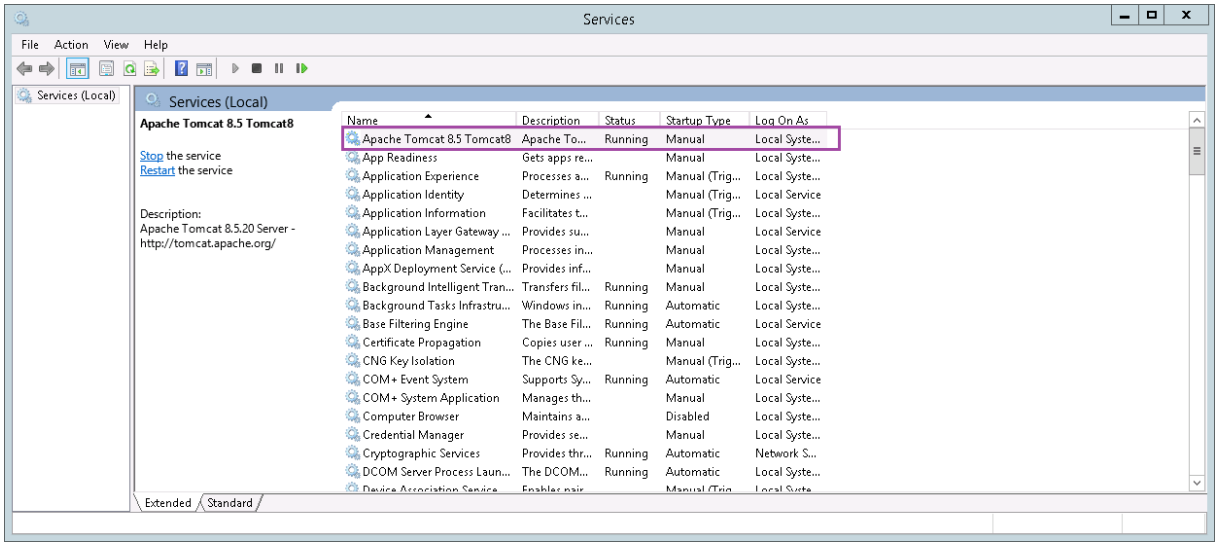




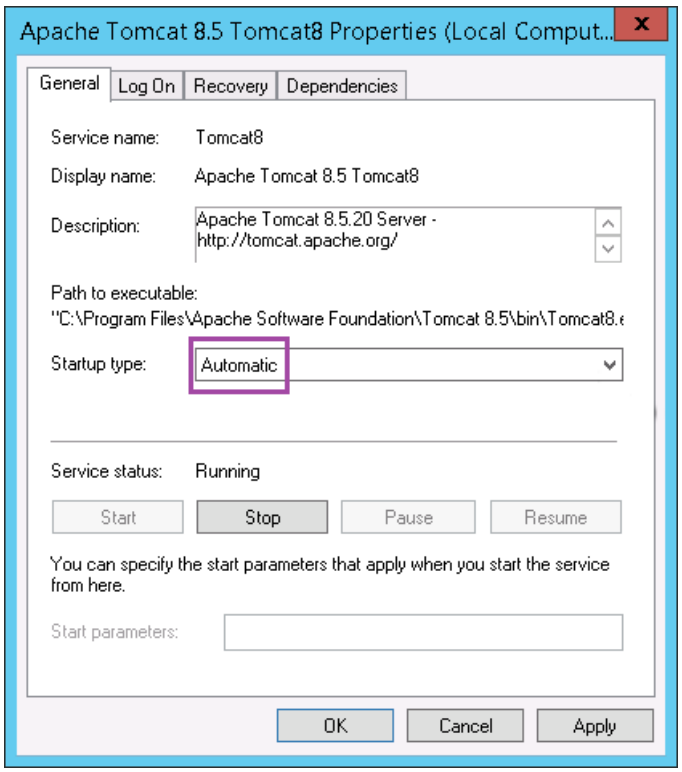
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Em seguida, vá até Windows Services e altere o **Tipo de inicialização** de **Manual** para **Automático**.

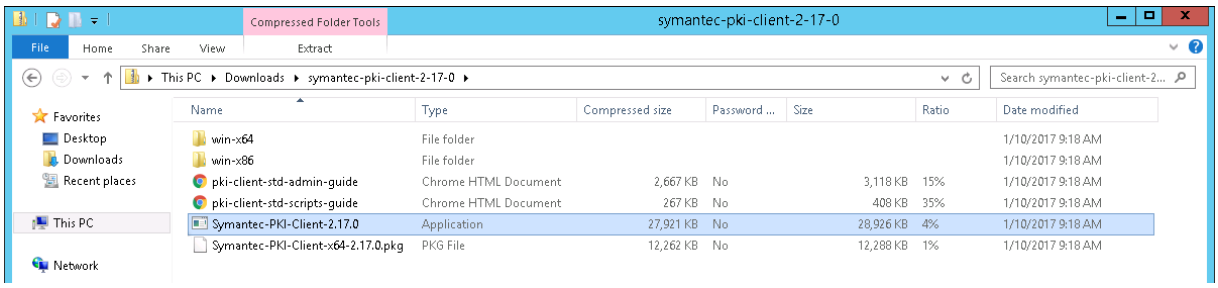


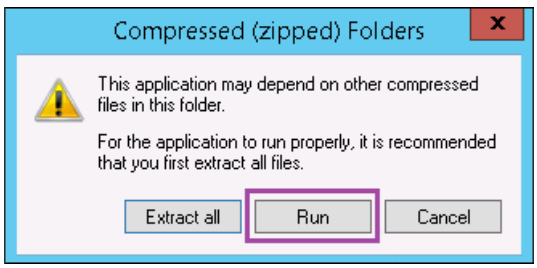
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Instalar o cliente Symantec PKI no Windows Server

Baixe o instalador a partir do console do PKI Manager. Se você não tem acesso ao console, baixe o instalador a partir da página de suporte da Symantec How to download Symantec PKI Client. Descompacte e execute o instalador.





Na caixa de diálogo Aviso de segurança, clique em **Executar**. Siga as instruções no instalador para concluir a instalação. Quando a instalação for concluída, ele solicitará que você reinicie.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Instalar o Portecle no Windows Server

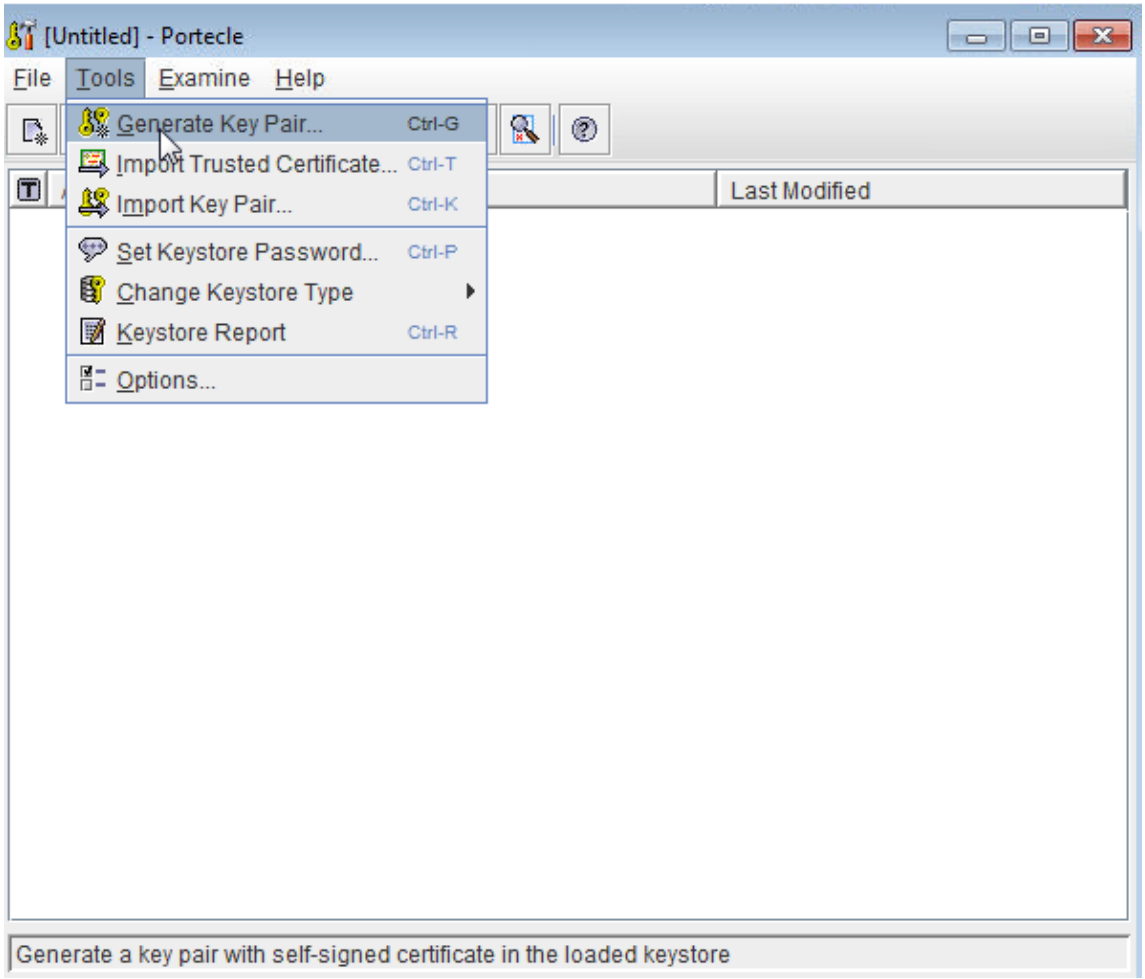
Baixe o instalador de https://sourceforge.net/projects/portecleinstall/files/ e depois descompacte e execute o instalador.

Gere o certificado de autoridade de registro (RA) para o PKI gerenciado da Symantec

O keystore para autenticação de certificado de cliente está contido em um certificado de autoridade de registro (RA), chamado RA.jks. As etapas a seguir descrevem como gerar esse certificado usando Portecle. Você também pode gerar o certificado de RA usando a interface de linha de comando Java.

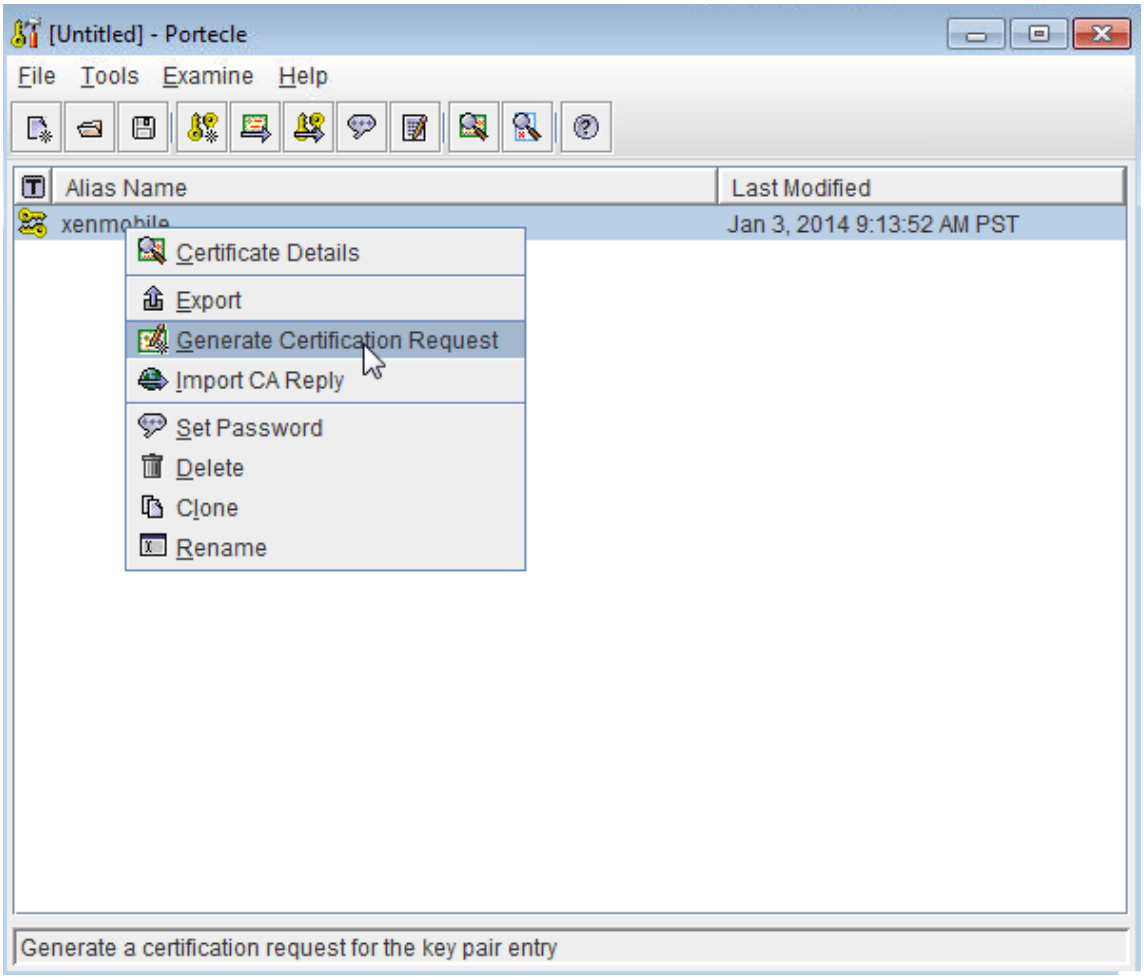
Este artigo também descreve como carregar o RA e os certificados públicos.

1. No Portecle, vá para **Tools > Generate Key Pair**, forneça as informações necessárias e gere um par de chaves.

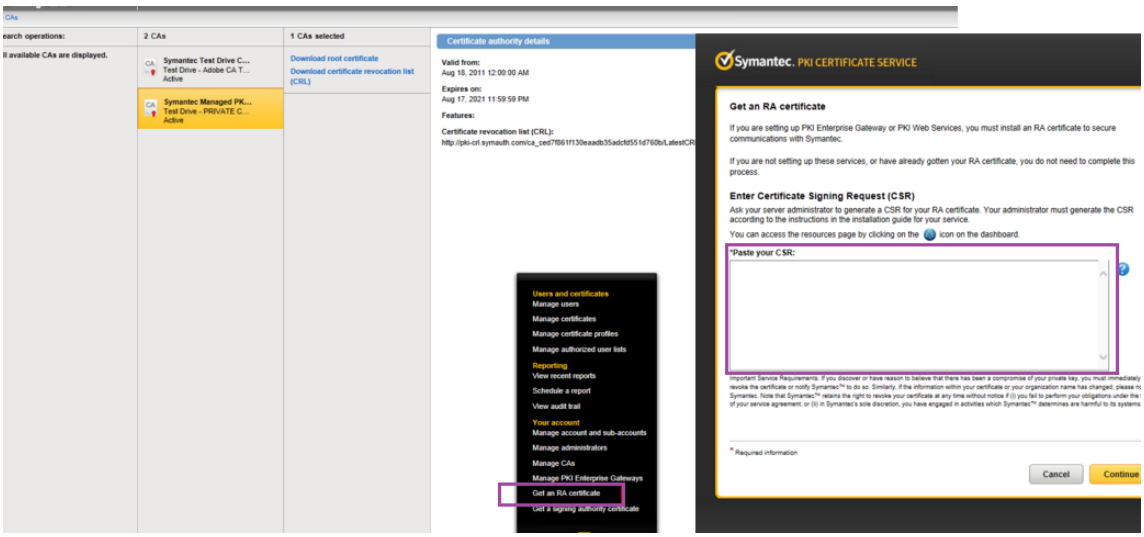


2. Clique com o botão direito do mouse no par de chaves e clique em **Generate Certification Request**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

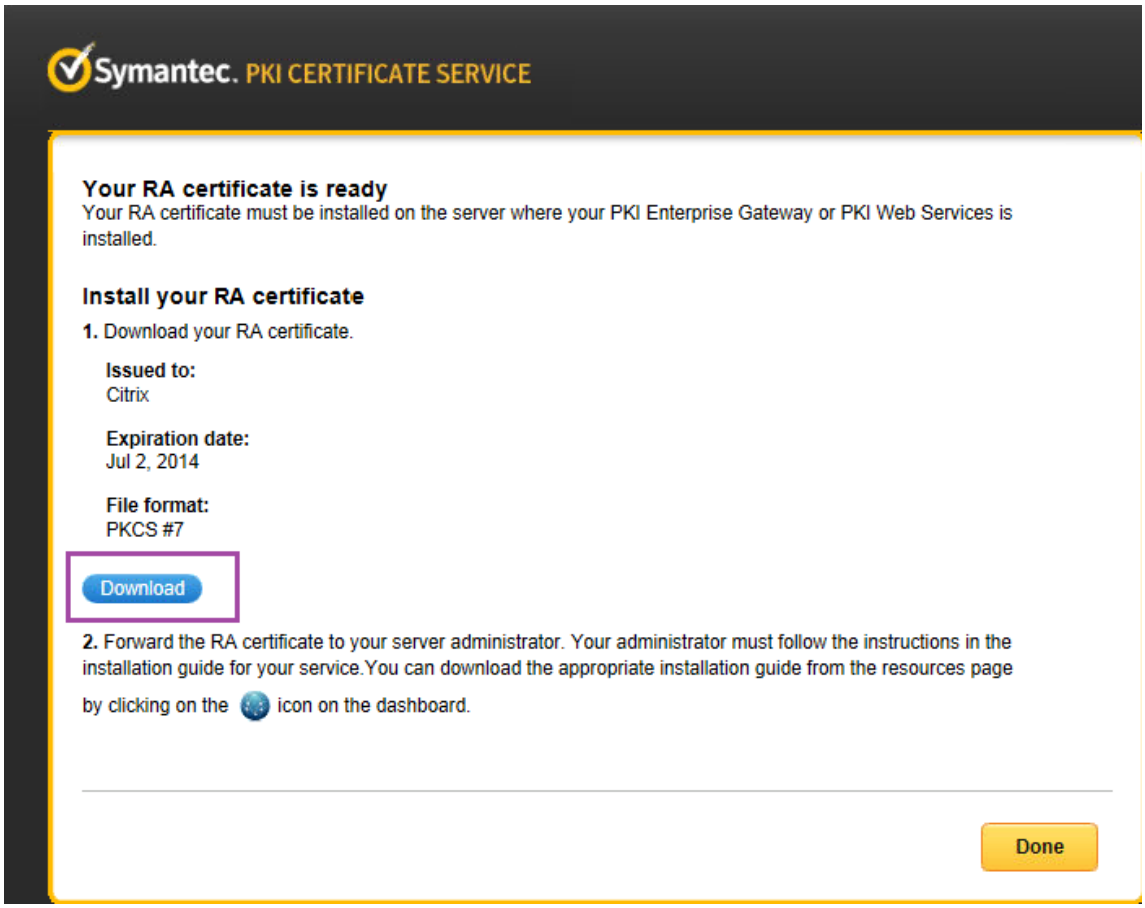


3. Copie o CSR.
4. No Symantec PKI Manager, gere um certificado de RA: clique em **Settings**, clique em **Get a RA Certificate**A, cole a CSR e clique em **Continue**.



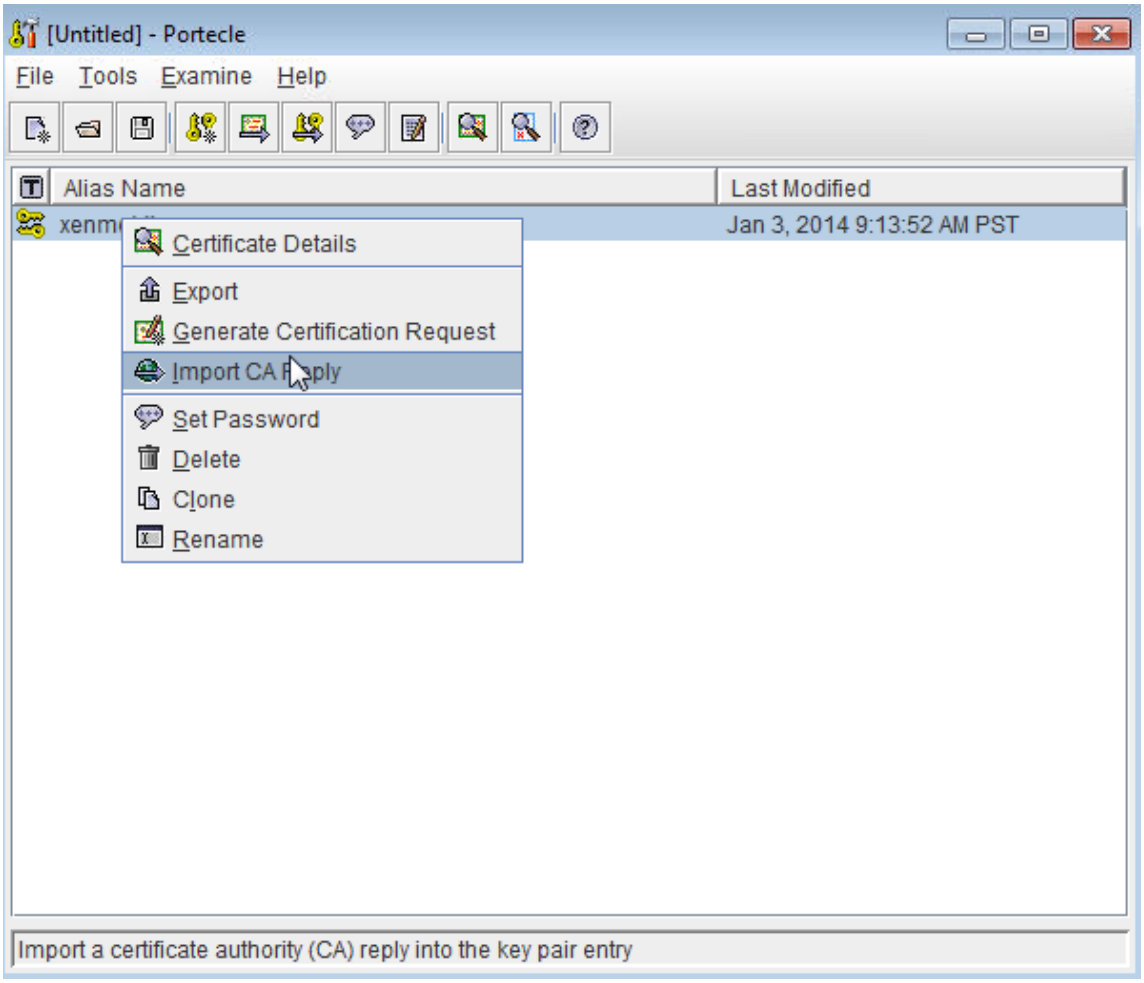
© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Clique em **Download** para baixar o certificado de RA gerado.



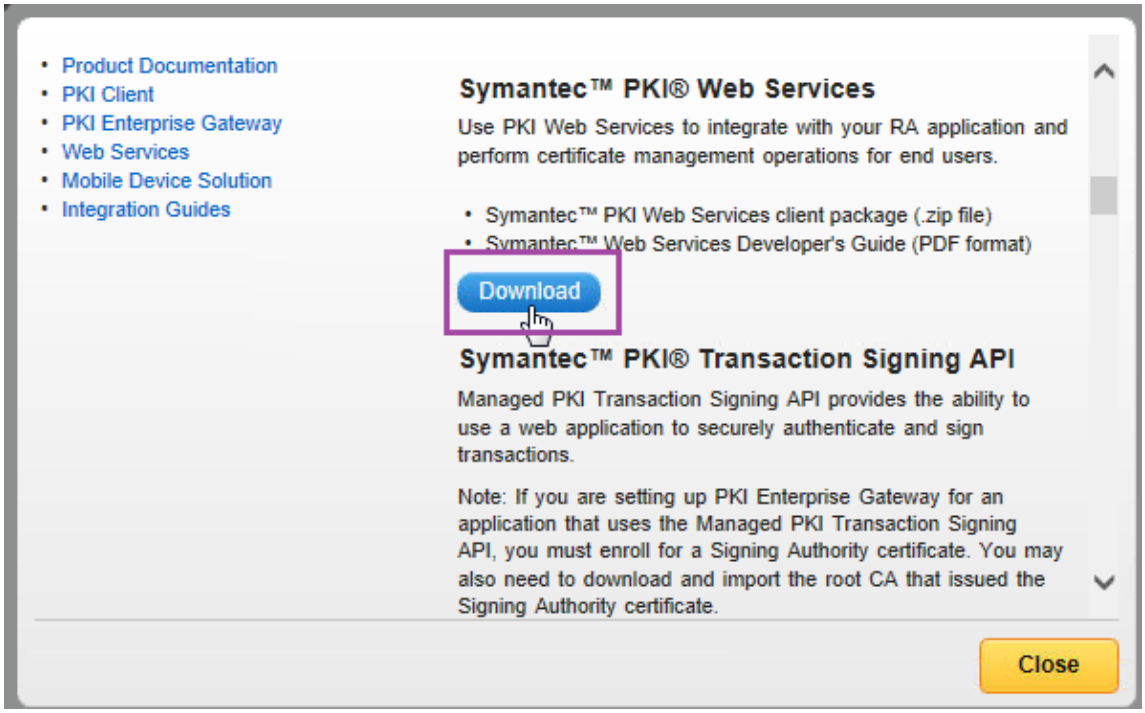
6. No Portecle, importe o certificado RA: clique com o botão direito do mouse no par de chaves e depois clique em **Import CA Reply**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



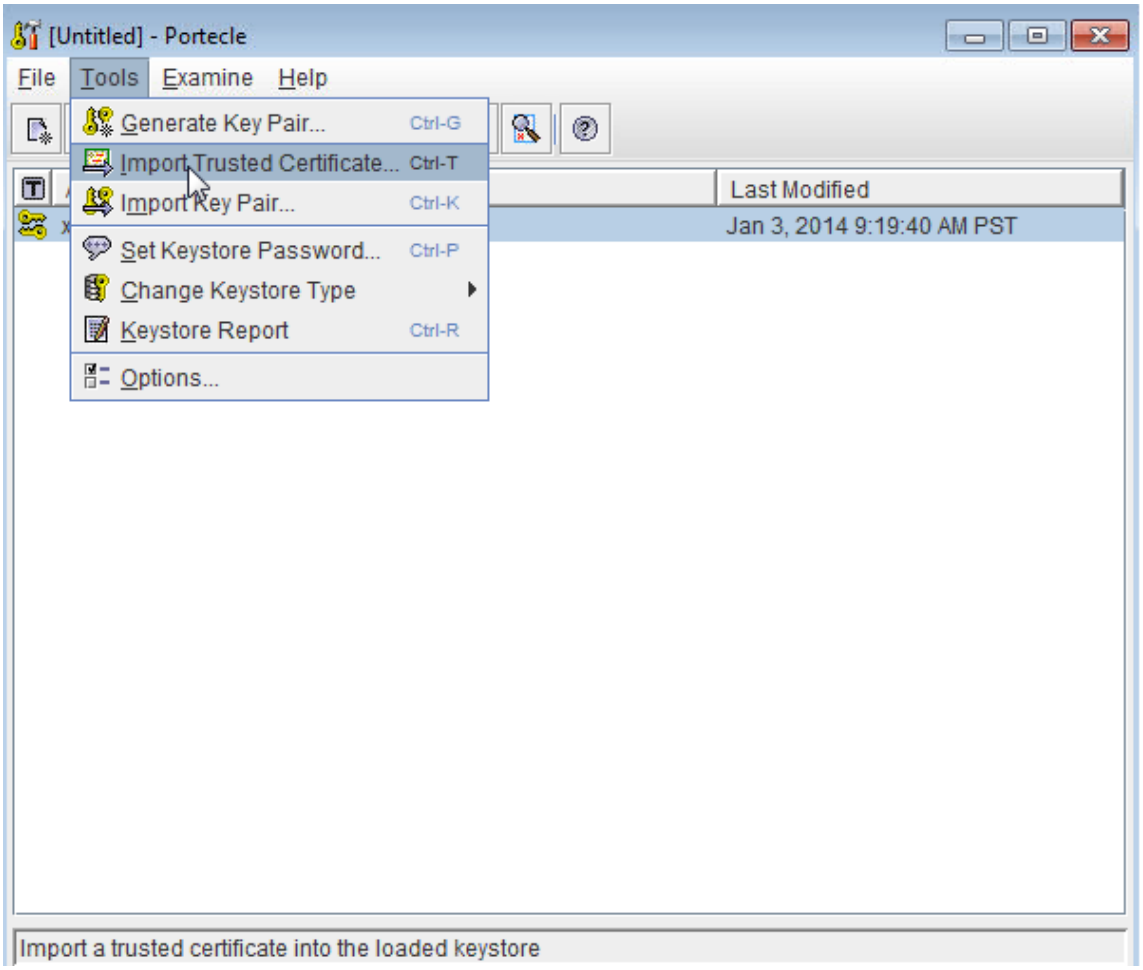
7. No Symantec PKI Manager: vá para **Resources > Web Services** e, em seguida, baixe os certificados da CA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



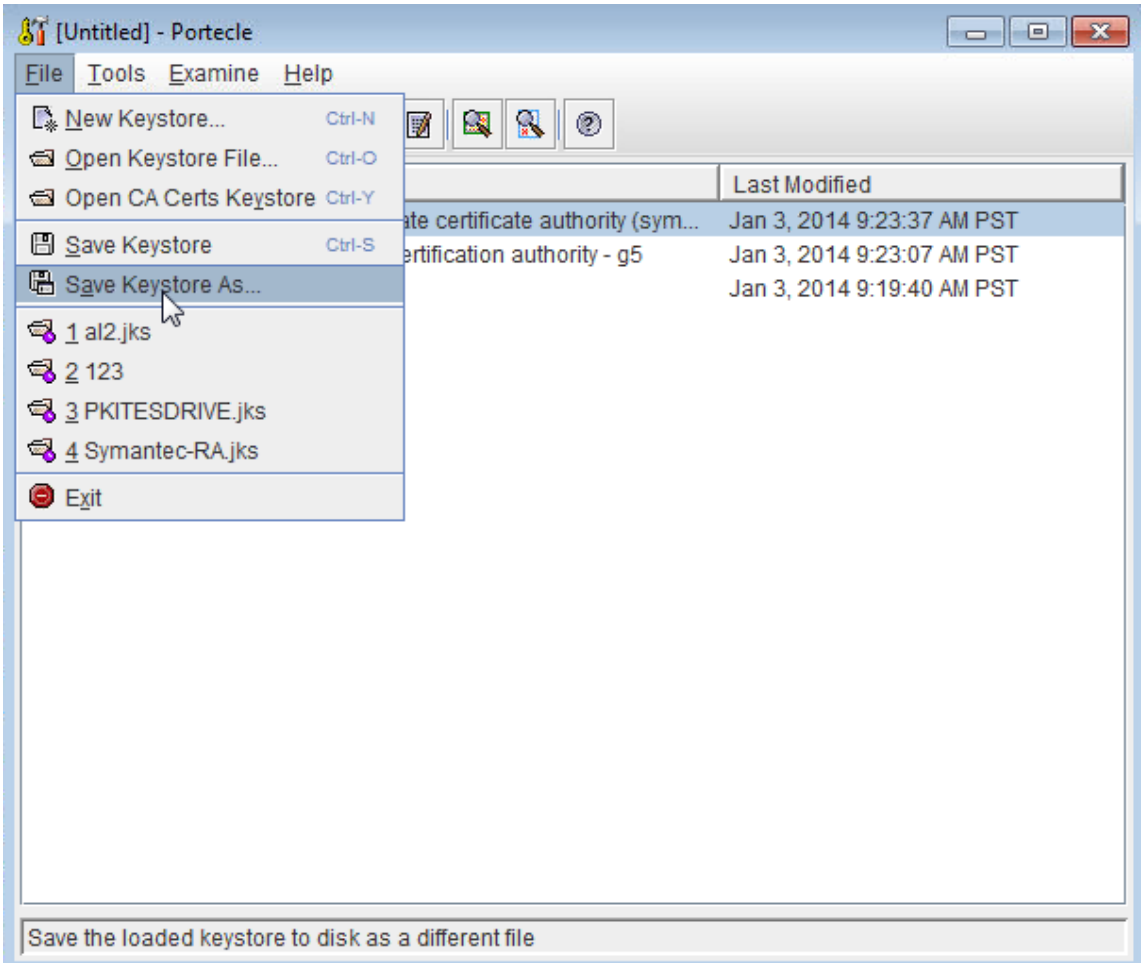
8. No Portecle, importe os certificados de RA intermediário e raiz para o keystore: vá para **Tools > Import Trusted Certificates**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



9. Depois de importar os CAs, salve o keystore como RA.jks na pasta C:\Symantec no Windows Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Configurar o Symantec PKI Adapter no Windows Server

1. Faça login no Windows Server como administrador.
2. Carregue o arquivo RA.jks que você gerou na seção anterior. Carregue também os certificados públicos (cacerts.jks) para o seu servidor Symantec MPKI.
3. Na página de Download do XenMobile Server 10, expanda **Ferramentas** e baixe o arquivo do Symantec PKI Adapter. O nome do arquivo é XenMobile_Symantec_PKI_Adapter.zip. Descompacte o arquivo .zip e copie os arquivos para a unidade C: do Windows Server:
   - custom_gpki_adapter.properties
   - Symantec.war
4. Abra custom_gpki_adapter.properties no Bloco de Notas e edite os seguintes valores:

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth
```

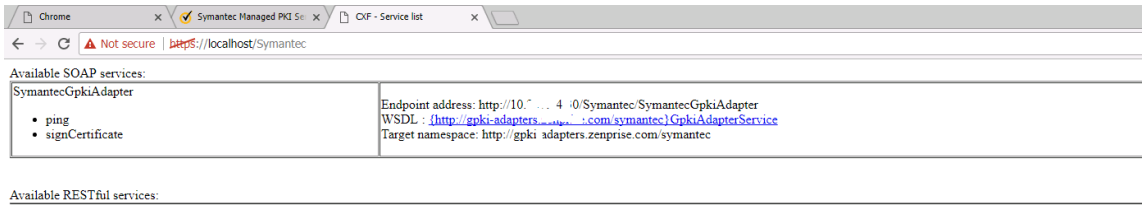
© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
4
5 keyStore=C:\Symantec\RA.jks
6
7 # truststore for server with self-signed root CA
8
9 trustStore=C:\Symantec\cacerts.jks
```

5. Copie o Symantec.war para a pasta `<tomcat dir>\webapps` e inicie o Tomcat.
6. Verifique se o aplicativo foi implantado: abra um navegador da Web e vá até `https://localhost/Symantec`.
7. Navegue até a pasta `<tomcat dir>\webapps\Symantec\WEB-INF\classes` e edite gpki_adapter.properties. Modifique a propriedade **CustomProperties** para apontar para o arquivo custom_gpki_adapter na pasta C:\Symantec:

   ```
   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
   ```

8. Reinicie o Tomcat, navegue até `https://localhost/Symantec` e copie o endereço de ponto de extremidade. Na próxima seção, você cola esse endereço ao configurar o adaptador PKI.



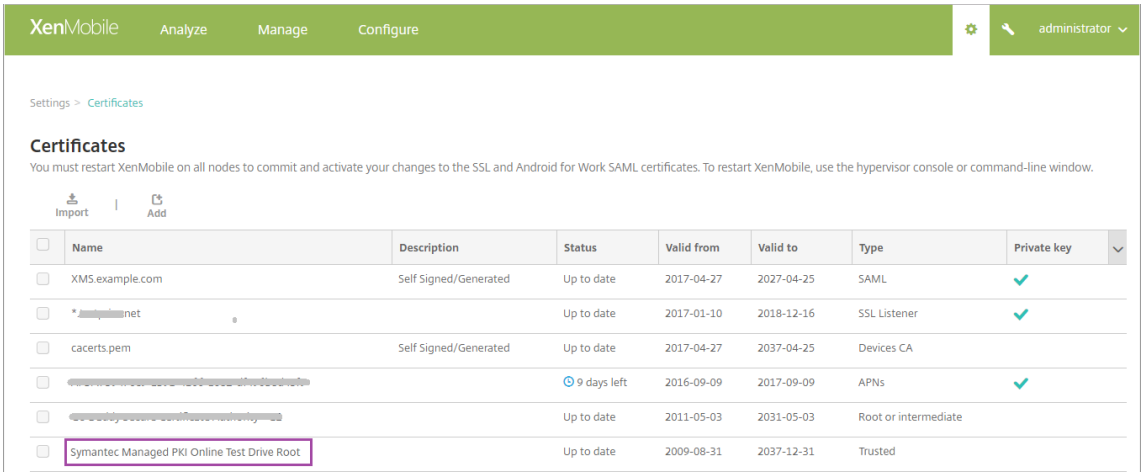
Configurar o XenMobile Server para PKI gerenciado da Symantec

Conclua a instalação do Windows Server antes de executar a configuração de XenMobile Server a seguir.

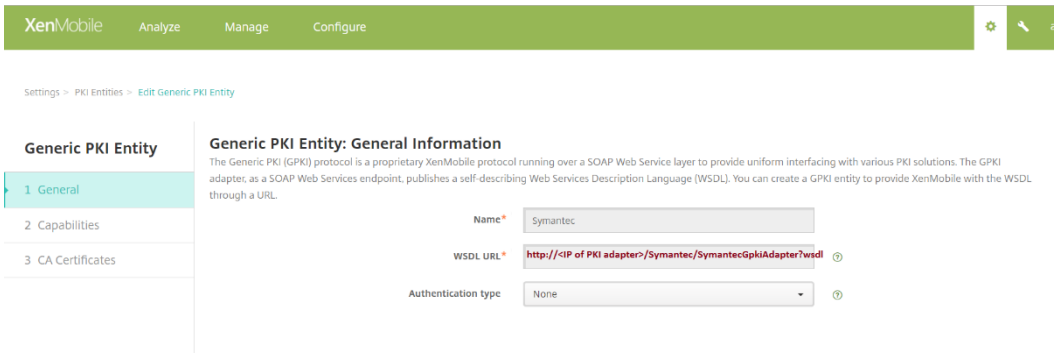
Para importar os certificados de AC da Symantec e configurar a entidade PKI

1. Importe os certificados de AC da Symantec que emitem o certificado do usuário final: no console do XenMobile Server, vá para **Configurações > Certificados** e clique em **Importar**.

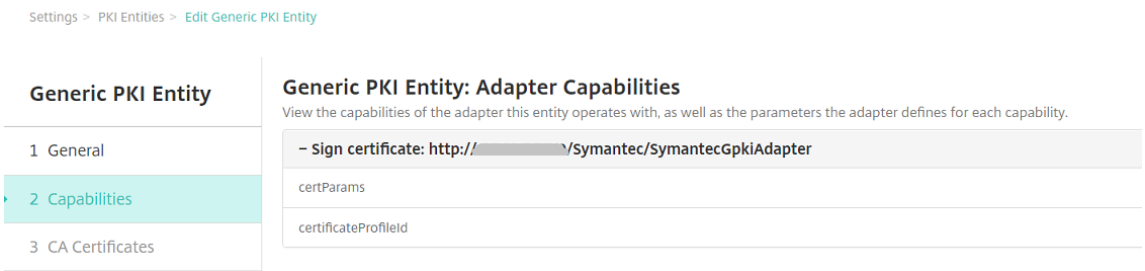
© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Adicione e configure a Entidade PKI: vá para **Configurações > Entidades PKI**, clique em **Adicionar** e, em seguida, escolha **Entidade Genérica PKI**. Em **URL WSDL**, cole o endereço do ponto de extremidade que você copiou quando configurou o adaptador PKI na seção anterior e, em seguida, acrescente `?wsdl`, conforme mostrado abaixo.

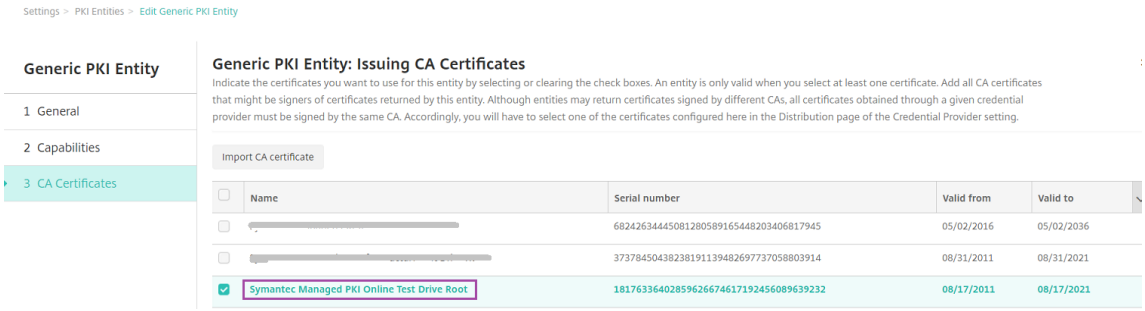


3. Clique em **Avançar**. O XenMobile preenche os nomes dos parâmetros do WSDL.

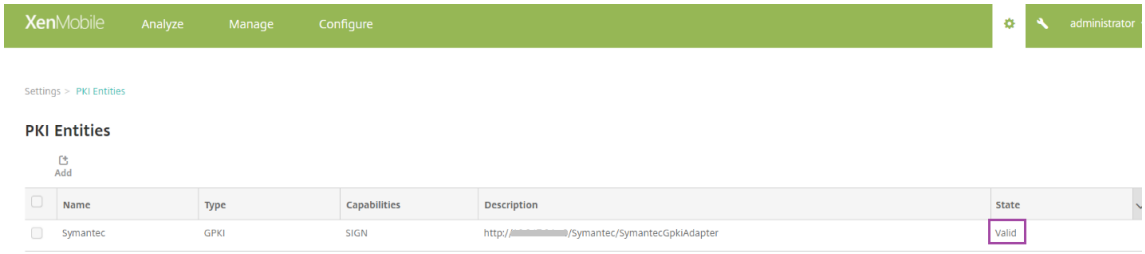


4. Clique em **Avançar**, selecione o certificado da autoridade de certificação correto e clique em **Salvar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

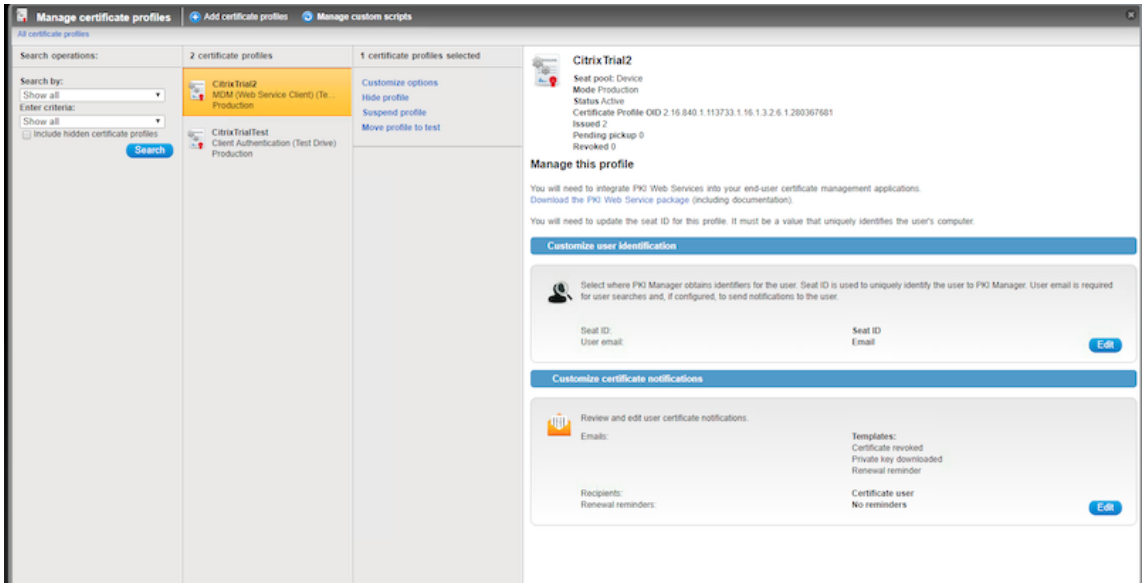


5. Na página **Configurações > Entidades de PKI**, verifique se o **Estado** da Entidade PKI que você adicionou é **Válido**.



Para criar o provedor de credenciais para PKI gerenciado da Symantec

1. No console do Symantec PKI Manager, copie o **Certificate Profile OID** em Certificate Template.

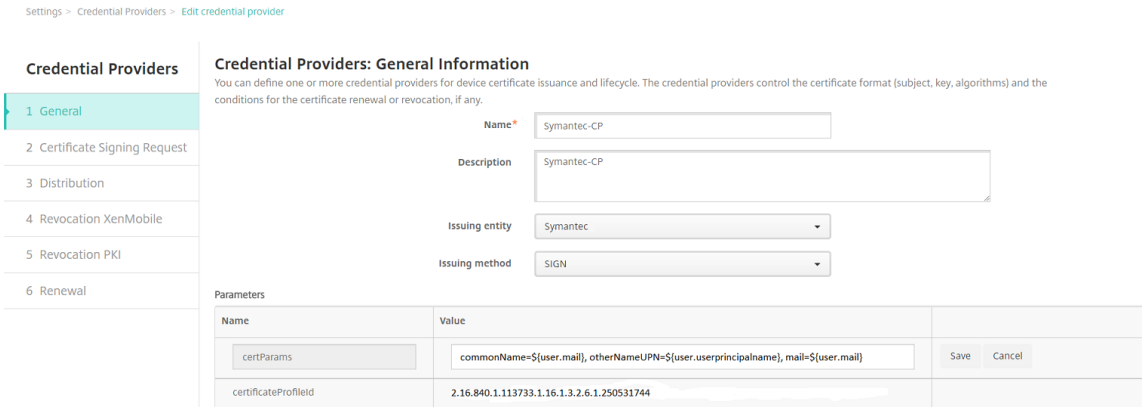


2. No console do XenMobile Sever, vá para **Configurações > Provedores de credenciais**, clique em **Adicionar** e defina as configurações da seguinte maneira.

    - **Nome:** digite um nome exclusivo para a nova configuração do provedor. Este nome é usado para referir-se à configuração em outras partes do console XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Descrição:** descreva o provedor de credenciais. Embora esse campo seja opcional, uma descrição pode ser útil para quando você precisar de detalhes sobre esse provedor de credenciais.
- **Entidade de emissão:** escolha a entidade de emissão do certificado.
- **Método de emissão:** escolha **Assinar** como o método que o sistema utiliza para obter certificados cliente da entidade configurada.
- **certParams:** Adicione o seguinte valor: **commonName=${user.mail},otherNameUPN=${user.userpr**
- **certificateProfileid:** cole o OID de perfil de certificado que você copiou na etapa 1.

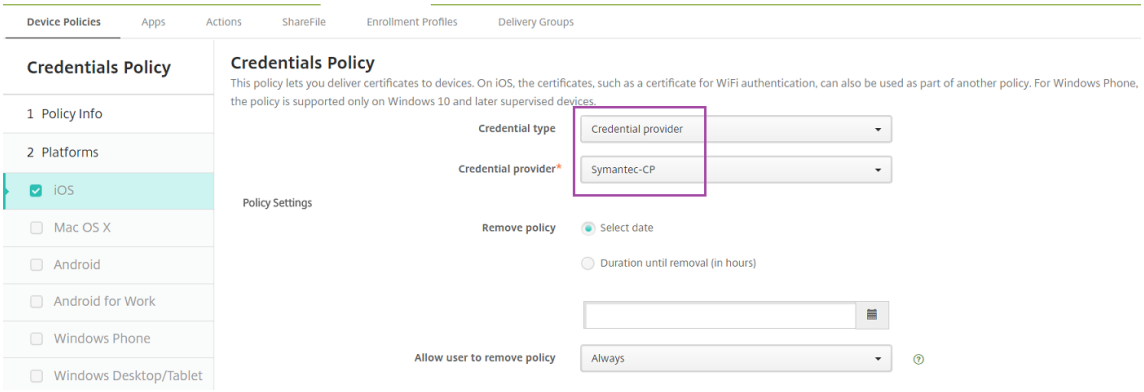


3. Clique em **Avançar**. Em cada uma das páginas restantes (solicitação de assinatura do certificado por meio de renovação), aceite as configurações padrão. Quando terminar, clique em **Salvar**.

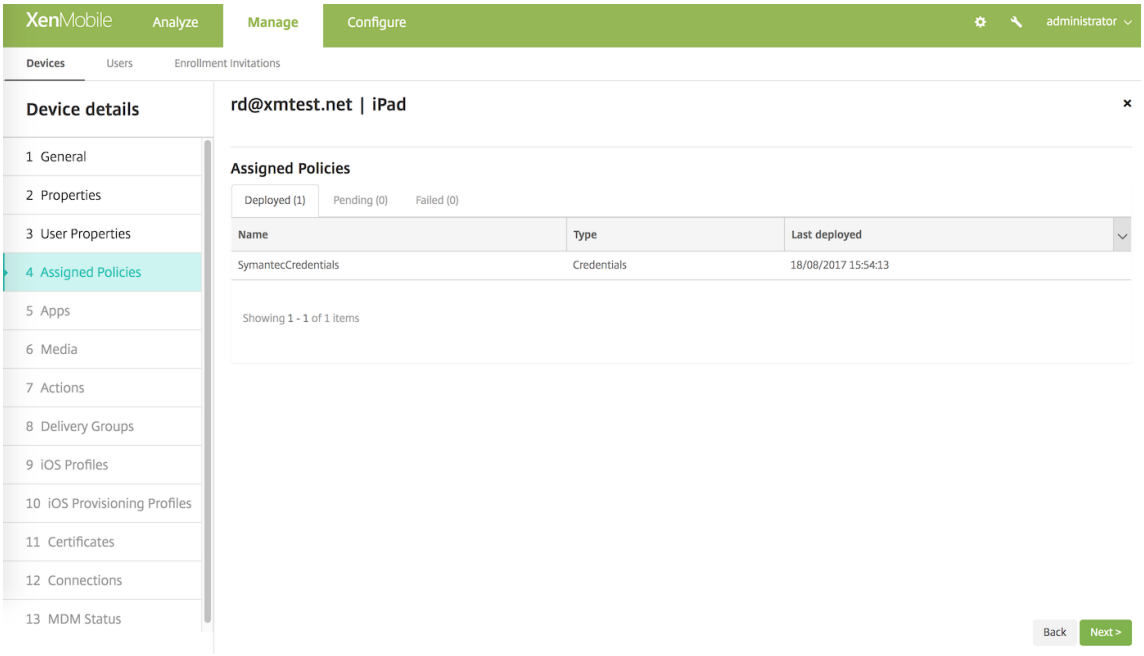
Para testar e solucionar problemas de configuração

1. Criar uma política de dispositivo de credenciais: vá para **Configurar > Políticas de dispositivo**, clique em **Adicionar**, comece a digitar **Credenciais** e clique em **Credenciais**.
2. Especifique o **Nome da Política**.
3. Defina as configurações da plataforma, como se seguem:
   - **Tipo de credencial:** escolha **Provedor de credenciais**.
   - **Provedor de credenciais:** escolha o provedor Symantec.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

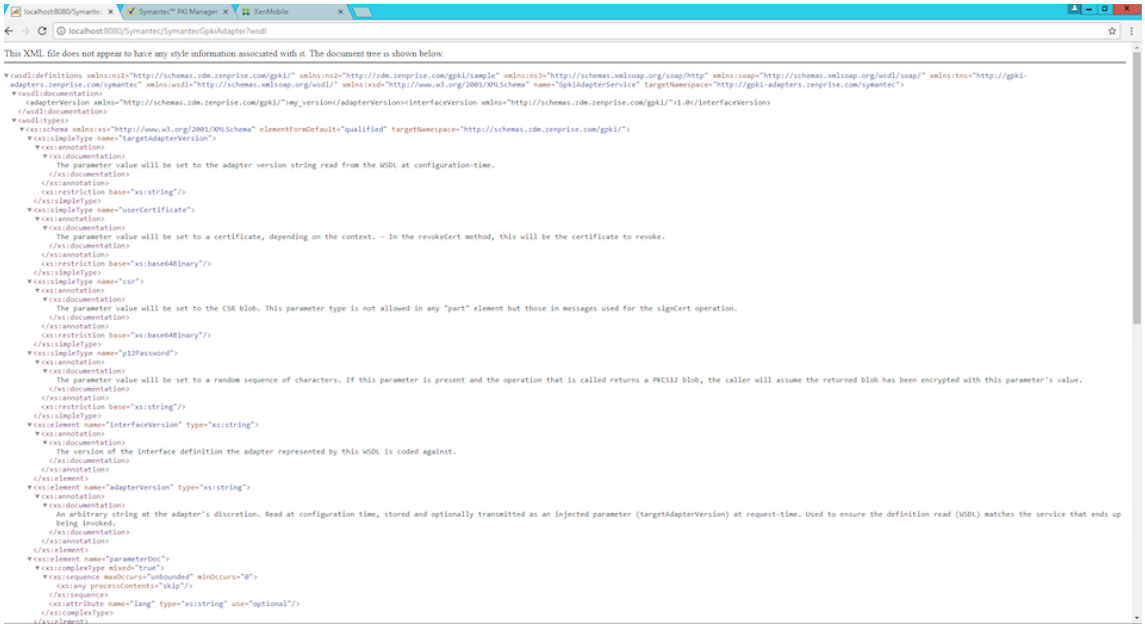


4. Depois de completar as configurações da plataforma, vá para a página **Atribuição**, atribua a política aos grupos de entrega e clique em **Salvar**.
5. Para verificar se a política foi implantada no dispositivo, vá para **Gerenciar > Dispositivos,** selecione o dispositivo, clique em **Editar** e clique em **Políticas atribuídas**. O exemplo a seguir mostra uma implantação com êxito de uma política.



Se a política não foi implantada, faça login no Windows Server e verifique se o WSDL está sendo carregado corretamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para mais informações sobre solução de problemas, verifique os logs do Tomcat em <tomcat dir>\logs\catalina.<current date>.

Serviços de Certificado da Microsoft

O XenMobile faz interface com os Serviços de Certificado da Microsoft por meio da respectiva interface de registro na Web. O XenMobile é compatível com a emissão de novos certificados somente por meio dessa interface (o equivalente ao recurso assinar da GPKI). Se a AC da Microsoft gerar um certificado de usuário do NetScaler Gateway, o NetScaler Gateway oferece a renovação e revogação para esses certificados.

Para criar uma entidade PKI da AC da Microsoft no XenMobile, você deve especificar a URL base da interface da Web dos Serviços de Certificado. Se você preferir, use a autenticação de cliente SSL para proteger a conexão entre o XenMobile e a interface da Web dos Serviços de Certificado.

Adicionar uma entidade dos Serviços de Certificado da Microsoft

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

   É exibido um menu de tipos de entidade PKI.
3. Clique em **Entidade de serviços de certificado da Microsoft**.

   A página **Entidade de serviços de certificado da Microsoft: Informações gerais** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Na página **Entidade de serviços de certificado da Microsoft: Informações gerais**, defina estas configurações:
   - **Nome:** digite um nome para a nova entidade que você usará mais tarde para se referir a ela. Os nomes de entidade devem ser exclusivos.
   - **URL raiz do serviço de registro na Web:** digite a URL base do seu serviço de registro na Web da AC da Microsoft, por exemplo, `https://192.0.2.13/certsrv/`. A URL pode usar HTTP simples ou HTTP sobre SSL.
   - **certnew.cer page name:** 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 no método de autenticação que você deseja usar.
     - **Nenhum**
     - **HTTP básico:** digite o nome do usuário e a senha necessários para se conectar.
     - **Certificado cliente:** escolha o certificado cliente SSL correto.
5. Clique em **Testar conexão** para garantir que o servidor esteja acessível. Se ele não estiver acessível, será exibida uma mensagem informando que a conexão falhou. Verifique as definições de configuração.
6. Clique em **Avançar**.

   A página **Entidade de serviços de certificado da Microsoft: modelos** é exibida. Nessa página, especifique os nomes internos dos modelos com os quais a sua AC da Microsoft é compatível. Quando você criar provedores de credenciais, selecione um modelo na lista definida aqui. Cada provedor de credenciais que usa essa entidade usa exatamente um desses modelos.

   Para os requisitos de modelo dos Serviços de Certificado da Microsoft, consulte a documentação da Microsoft relativa à versão do Microsoft Server. O XenMobile não tem requisitos para os certificados que distribui além dos formatos de certificado indicados em Certificados.
7. Na página **Entidade de serviços de certificado da Microsoft: Modelos** clique em **Adicionar**, digite o nome do modelo e clique em **Salvar**. Repita essa etapa para cada modelo que você desejar 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 na Web da Microsoft. Parâmetros personalizados são úteis somente para scripts personalizados em execução na autoridade de certificação.
9. Na página **Entidade de serviços de certificado da 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

É exibida a página **Entidade de serviços de certificado da Microsoft: certificados AC**. Nessa página, você deve informar ao XenMobile sobre os signatários dos certificados que o sistema obtém por meio dessa entidade. Quando seu certificado de CA for renovado, atualize-o no XenMobile. O XenMobile aplica a mudança à entidade de forma transparente.

10. Na página **Entidade de serviços de certificado da Microsoft: Certificados AC**, selecione os certificados que você deseja usar para esta entidade.
11. Clique em **Salvar**.

    A entidade é exibida na tabela Entidades PKI.

Lista de certificados revogados (CRL) de NetScaler

O XenMobile dá suporte a lista de certificados revogados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o NetScaler para gerenciar a revogação.

Quando você configura a autenticação baseada em certificado de cliente, decida se você precisa configurar a opção lista de certificados revogados (CRL) **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 emite novamente um novo certificado porque ele não impede que um usuário gere um certificado de usuário depois que um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

CAs discricionárias

Uma AC discricionária é criada quando você fornece ao XenMobile um certificado de AC e a chave privada associada. O XenMobile manipula a emissão, a revogação e as informações de status do certificado internamente, de acordo com os parâmetros que você especificar.

Quando você configura uma AC discricionária, pode ativar o suporte do Protocolo OCSP (Online Certificate Status Protocol) para essa AC. Se, e somente se, você ativar o suporte do OCSP, a AC adicionará uma extensão `id-pe-authorityInfoAccess` aos certificados que a AC emitir. A extensão aponta para o respondente OCSP interno do XenMobile na seguinte localização:

```
https://<server>/<instance>/ocsp
```

Quando você configurae o serviço OCSP, especifique um certificado de assinatura OCSP para a entidade discricionária em questão. Você pode usar o próprio certificado de AC como signatário. Para evitar a exposição desnecessária da chave privada de AC (recomendado): crie um certificado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de assinatura OCSP assinado pelo certificado de AC e inclua a extensão: `id-kp-OCSPSigning extendedKeyUsage`.

O serviço do respondedor OCSP do XenMobile é compatível com respostas OCSP básicas e com os 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 ACs discricionárias

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Mais > Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

   É exibido um menu de tipos de entidade PKI.
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 de AC para assinar solicitações de certificado:** clique no certificado da CA discricionária a ser usado para assinar solicitações de certificado.

     Essa lista de certificados é gerada com base nos certificados de AC com chaves privadas que você carregou para o 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 ela emite. Nessa lista, clique em **Sequencial** ou **Não sequencial** para determinar como os números serão gerados.
   - **Próximo número de série:** digite um valor para determinar o próximo número emitido.
   - **Certificado válido para:** digite o número de dias durante os quais o certificado é válido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Uso da chave:** identifique o propósito dos certificados emitidos pela CA discricionária definindo as chaves adequadas como **Ativado**. Depois de definida, a AC é limitada a emitir certificados para esses fins.
- **Uso de chave estendido:** para adicionar mais parâmetros, clique em **Adicionar**, escreva o nome da chave e 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 do 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 do lado do dispositivo**. As chaves privadas são geradas nos dispositivos do usuário. Esse modo distribuído usa o 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 autenticação e criptografia.

9. Clique em **Avançar**.

   A página **CA discricionária: Protocolo OCSP (Online Certificate Status Protocol)** é exibida.

   Na página **CA discricionária: Protocolo OCSP (Online Certificate Status Protocol)**, faça o seguinte:

   - Se você desejar adicionar uma extensão `AuthorityInfoAccess` (RFC2459) aos certificados assinados por essa AC, defina **Ativar suporte a OCSP para esta AC** como **Ativado**. Essa extensão aponta para o respondente OCSP da AC em `https://<server>/<instance>/ocsp`.
   - Se você tiver ativado o suporte do OCSP, selecione um certificado de AC de assinatura OSCP. Essa lista de certificados é gerada com base nos certificados de AC que você carregou no XenMobile.

10. Clique em **Salvar**.

    A AC discricionária é exibida na tabela Entidades PKI.

Provedores de credenciais

April 15, 2019

Os provedores de credenciais são as configurações reais de certificado que você usa em várias partes do sistema XenMobile. Provedores de credenciais definem as origens, parâmetros e ciclos de vida

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de seus certificados. Essas operações ocorrem se os certificados fizerem parte das configurações do dispositivo ou se forem independentes (isto é, 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 ele possa emitir alguns certificados como parte do processo de registro. Além disso, os certificados emitidos da PKI interna no contexto de um registro são revogados quando o processo de registro é revogado. Depois que o relacionamento de gerenciamento é encerrado, nenhum certificado válido permanece.

Você pode usar uma configuração de provedor de credenciais em vários locais para que uma configuração possa reger qualquer número de certificados ao mesmo tempo. A unidade está no recurso de implantação e na implantação. Por exemplo, se o provedor de credenciais P for implantado para o 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 de D se aplicam quando C é atualizada. E as configurações de revogação de D também se aplicam quando C é excluída ou quando D é revogado.

De acordo com essas regras, a configuração do provedor de credenciais no XenMobile determina o seguinte:

- A origem de certificados.
- O método pelo qual os certificados são obtidos: assinando um novo certificado ou obtendo (recuperando) um certificado e um par de chaves existentes.
- Os parâmetros para emissão ou recuperação. Por exemplo, os parâmetros de CSR (Solicitação de Assinatura de Certificado), como tamanho da chave, algoritmo de chave e extensões de certificado.
- A forma como os certificados são entregues ao dispositivo.
- Condições de revogação. Embora todos os certificados sejam revogados no XenMobile quando o relacionamento de gerenciamento é interrompido, 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 certificados no XenMobile pode causar a revogação de certificados na PKI.
- Configurações de renovação. Os certificados obtidos por meio de um determinado provedor de credenciais podem ser renovados automaticamente quando estão próximos do vencimento. Ou, separadamente dessa situação, as notificações podem ser emitidas quando essa expiração se aproximar.

A disponibilidade das opções de configuração depende principalmente do tipo de Entidade PKI e do método de emissão que você selecionar para um provedor de credenciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Métodos de emissão de certificado

Você pode obter um certificado, conhecido como métodos de emissão, de duas maneiras:

- **Assinar:** Com esse método, a emissão envolve a criação de uma nova chave privada, a criação de uma CSR e o envio da CSR para uma Autoridade de Certificação (CA) para assinatura. O XenMobile é compatível com o método de assinar para as três entidades PKI (Entidade de serviços de certificado da Microsoft, PKI genérica e CA discricionária).
- **Obter:** Com esse método, a emissão, para fins do XenMobile, é a recuperação de um par de chaves existente. O XenMobile é compatível com o método obter somente para PKI Genérica.

Um provedor de credenciais usa o método de emissão Assinar ou Obter. O método selecionado afeta as opções de configuração disponíveis. Em especial, a configuração de CSR e a entrega distribuída estarão disponíveis somente se o método de emissão for assinar. Um certificado obtido é sempre enviado para o dispositivo como um PKCS #12, o equivalente ao modo de entrega centralizado do método de assinatura.

Entrega de certificado

Dois modos de entrega de certificado estão disponíveis no XenMobile: centralizado e distribuído. O modo distribuído usa o Protocolo de Registro de Certificado Simples (SCEP) e está disponível somente nas situações em que o cliente é compatível com o protocolo (somente iOS). O modo distribuído é obrigatório em algumas situações.

Para que um provedor de credenciais seja compatível com a entrega distribuída (assistida por SCEP), é necessária uma etapa de configuração especial: Configurar certificados de Autoridade de Registro (RA). Os certificados de RA são necessários porque, ao usar o protocolo SCEP, o XenMobile age como um representante (um registrador) da AC real. O XenMobile precisa comprovar para o cliente que ele tem autoridade para agir como tal. Essa autoridade é estabelecida fazendo o upload para o XenMobile dos certificados anteriormente mencionados.

São necessárias duas funções de certificado diferentes (embora um único certificado possa atender a ambos os requisitos): assinatura de RA e criptografia de RA. As restrições dessas funções são as seguintes:

- O certificado de assinatura RA deve ter a assinatura digital de uso de chave X.509.
- O certificado de criptografia RA deve ter a codificação de chave de uso de chave X.509.

Para configurar os certificados de RA do provedor de credenciais, você carrega os certificados para o XenMobile e cria links para eles no provedor de credenciais.

Um provedor de credenciais é considerado como compatível com entregas distribuídas somente se ele tiver um certificado configurado para funções de certificado. Você pode configurar cada provedor de credenciais para dar preferência ao modo centralizado, ao modo distribuído ou para exigir o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

modo distribuído. O resultado real depende do contexto: se o contexto não for compatível com o modo distribuído, mas o provedor de credenciais exigir esse modo, a implantação não será realizada. Da mesma forma, quando o contexto exige o modo distribuído, mas o provedor de credenciais não é compatível com ele, a implantação não é realizada. Em todos os outros casos, a configuração preferencial é respeitada.

A seguinte tabela mostra a distribuição SCEP em todo o XenMobile:

Contexto	SCEP com suporte	SCEP necessário
Serviço de Perfil do iOS	Sim	Sim
Registro do gerenciamento de dispositivo móvel do iOS	Sim	Não
Perfis de configuração do iOS	Sim	Não
Registro SHTP	Não	Não
Configuração SHTP	Não	Não
Registro de telefone e tablet com Windows	Não	Não
Configuração de telefone e tablet com Windows	Não, exceto para a política de dispositivo de Wifi, que é compatível com Windows Phone 8.1 e a versão mais recente do Windows 10	Não

Revogação de certificados

Há 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 o 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 conhecido como Revogação XenMobile, esse tipo de revogação se aplica aos certificados obtidos de uma PKI externa. O certificado foi revogado na PKI quando o XenMobile o revogou internamente, sob as condições definidas pela configuração do provedor de credenciais. A chamada para realizar a revogação exige uma entidade PKI Geral (GPKI) com capacidade de revogação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Revogação induzida externamente:** Também conhecida como Revogação PKI, esse tipo de revogação também se aplica somente aos certificados obtidos de uma PKI externa. Sempre que o XenMobile avalia um determinado status de certificado, ele consulta a PKI quanto a esse status. Se o certificado tiver sido revogado, o XenMobile revoga-o internamente. Esse mecanismo usa o protocolo OCSP.

Esses três tipos não são exclusivos, mas aplicam-se juntos. Uma revogação externa ou descoberta independente pode causar uma revogação interna. Uma revogação interna afeta potencialmente uma revogação externa.

Renovação de certificado

A 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 quando a emissão falhar. Para entrega distribuída (suportada pelo SCEP), a revogação também ocorre somente após o certificado ter sido instalado com êxito 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 determinada 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 tentará renovar o certificado.

Criar um provedor de credenciais

Configurar um provedor de credenciais varia principalmente como um fator de qual entidade e método de emissão você seleciona para o provedor de credenciais. Você pode distinguir entre os provedores de credenciais que usam uma entidade interna ou uma entidade externa:

- Uma entidade discricionária, que é interna para o XenMobile, é uma entidade interna. O método de emissão para uma entidade discricionária é sempre Assinar. Assinar significa que, a cada operação de emissão, o XenMobile assina um novo par de chaves com o certificado de CA selecionado para a entidade. A geração do par de chaves no dispositivo ou no servidor depende do método de distribuição selecionado.
- Uma entidade externa, que faz parte de sua infraestrutura corporativa, inclui AC da Microsoft ou uma GPKI.

Para obter informações detalhadas sobre a configuração do PKI gerenciado da Symantec, incluindo a criação do provedor de credenciais, consulte “Symantec Managed PKI” em Entidades PKI.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito e 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. Este nome é usado mais tarde para identificar a configuração em outras partes do console XenMobile.
   - **Descrição:** descreva o provedor de credenciais. Embora esse campo seja opcional, uma descrição pode fornecer detalhes úteis sobre esse provedor de credenciais.
   - **Entidade de emissão:** clique na entidade de emissão do certificado.
   - **Método de emissão:** clique em **Assinar** ou **Obter** para servir como o método que o sistema utiliza para obter certificados da entidade configurada. Para usar a autenticação de certificado de cliente, **Assinar**.
   - Se a lista de **Modelos** estiver disponível, selecione o modelo que você adicionou sob a entidade PKI para o provedor de credenciais.

     Esses modelos são disponibilizados 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 **Credenciais de Fornecedores: solicitação de assinatura de certificado**, configure o seguinte de acordo com a configuração do seu 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, o que depende do hardware e do 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-lo em produção.
   - **Algoritmo de assinatura:** clique em um valor para o novo certificado. Os valores dependem do algoritmo de chave.
   - **Nome de entidade:** necessário. Digite o Nome Diferenciado (DN) da entidade do novo certificado. Por exemplo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
CN=${ user.username } , OU=${ user.department } , O=${ user.companyname
 } ,C=${ user.c } \endquotation
```

Por exemplo, para a autenticação de certificado de cliente, use estas configurações:

- **Algoritmo de chave:** RSA
- **Tamanho da chave:** 2048
- **Algoritmo de assinatura:** SHA1withRSA
- **Nome de entidade:** `cn=$user.username`

- Para adicionar uma entrada à tabela **Nomes alternativos de entidade**, clique em **Adicionar**. Selecione o tipo de nome alternativo e digite um valor na segunda coluna.

  Para autenticação de certificado de cliente, especifique:

  - **Tipo:** nome UPN
  - **Valor:** `$user.userprincipalname`

    Assim como para o nome de entidade, 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 **Emissão de certificado de CA**, clique no certificado de CA oferecido. Como o provedor de credenciais usa uma entidade de CA discricionária, o certificado de CA do provedor de credenciais é sempre o certificado de CA configurado na própria entidade. O certificado de CA é apresentado aqui para consistência com configurações que usam entidades externas.
   - Em **Selecionar modo de distribuição**, clique em uma das seguintes formas de gerar e distribuir chaves:
     - **Preferir modo centralizado: geração de chaves do lado do servidor:** a Citrix recomenda essa opção centralizada. Ela é compatível com todas as plataformas compatíveis com o XenMobile e é exigida quando a autenticação do NetScaler Gateway é usada. As chaves privadas são geradas e armazenadas no servidor e distribuídas para os dispositivos do usuário.
     - **Preferir modo distribuído: geração de chaves do lado do dispositivo:** as chaves privadas são geradas e armazenadas nos dispositivos do usuário. Esse 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 autenticação e criptografia.
     - **Somente distribuído: geração de chaves do lado do dispositivo:** Essa opção funciona da mesma forma que Preferir modo distribuído: geração de chaves do lado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

do dispositivo, exceto que, como é “Somente” em vez de “Preferir”, nenhuma opção estará disponível se a geração de chave do lado do dispositivo falhar ou não estiver disponível.

Se você tiver selecionado **Preferir modo distribuído: geração de chaves do lado do dispositivo** ou **Somente distribuído: geração de chaves do 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 são exibidos para esses certificados.

8. Clique em **Avançar**.

   A página **Provedores de credenciais: revogação XenMobile** é exibida. Nessa página, você pode configurar as condições sob as quais o XenMobile sinaliza internamente como revogados os certificados emitidos por essa configuração de provedor.

9. Na página **Provedores de credenciais: revogação XenMobile**, faça o seguinte:

   - Em **Revogar certificados emitidos**, selecione uma das opções que indicam quando revogar os certificados.
   - Para que o XenMobile envie 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 ele tiver sido revogado do XenMobile, defina **Revogar certificado na PKI** como **Ativado** e, na **lista Entidade**, clique em um modelo. A lista Entidade mostra todas as entidades GPKI disponíveis com capacidades de revogação. Quando o certificado é revogado do XenMobile, uma chamada de revogação é enviada para a PKI selecionada da lista Entidade.

10. Clique em **Avançar**.

    A página **Provedores de credenciais: revogação PKI** é exibida. Nessa página, identifique as ações a serem tomadas na PKI se o certificado for revogado. Você também tem a opção de criar uma mensagem de notificação.

11. Na página **Provedores de credenciais: revogação PKI**, faça o seguinte se você deseja revogar os certificados da PKI:

    - Altere a configuração de **Ativar verificações de revogação externa** para **Ativado**. São exibidos mais campos relacionados à revogação PKI.
    - Na lista **Certificado de AC do respondedor OCSP**, clique no nome distinto (DN) da entidade do certificado.

      Você pode usar macros do XenMobile para os valores de campo de DN. Por exemplo: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Na lista **Quando o certificado for revogado**, clique em uma das seguintes ações a serem tomadas em relação à entidade PKI quando o certificado é revogado:
  - Não fazer nada.
  - Renovar o certificado.
  - Revogar e apagar o dispositivo.
- Para que o XenMobile envie 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 escolher **Selecionar modelo de notificação**, poderá selecionar uma mensagem de notificação previamente escrita que poderá personalizar. Esses modelos estão na lista Modelo de notificação.
- Se você selecionar **Inserir detalhes da notificação**, poderá escrever sua própria mensagem de notificação. Além de fornecer endereço de email 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. Nessa página, você pode configurar o XenMobile para fazer o seguinte:

    - Renovar o certificado. Você pode, opcionalmente, enviar uma notificação sobre a renovação e, opcionalmente, excluir certificados já expirados da operação.
    - Emitir uma notificação para os certificados que estão perto do vencimento (notificação antes da renovação).

13. Na página **Provedores de Credenciais: renovação**, faça o seguinte se desejar renovar os certificados quando eles expirarem:

    Defina **Renovar certificados** quando eles expirarem para **Ativado**. Mais campos aparecem.

    - No campo **Renovar quando o certificado expirar em**, digite quantos dias antes da expiração para renovar o certificado.
    - Opcionalmente, selecione **Não renovar certificados que já expiraram**. Nesse caso, "já expiraram" significa que a data `NotAfter` está no passado, não que tenha sido revogada. O XenMobile não renova certificados depois que eles são revogados internamente.

    Para que o XenMobile envie uma notificação quando o certificado tiver sido renovado, defina **Enviar notificação** como **Ativado**. Para que o XenMobile envie uma notificação quando o certificado estiver prestes a expirar, defina **Notificar quando o certificado estiver prestes a expirar** como **Ativado**.
    Para qualquer uma dessas opções, você pode escolher entre duas opções de notificação:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Selecionar modelo de notificação:** selecione uma mensagem de notificação previamente escrita que você pode personalizar. Esses modelos estão na lista Modelo de notificação.
- **Inserir detalhes da notificação:** escreva a sua própria mensagem de notificação. Forneça o endereço de e-mail do destinatário, uma mensagem e uma frequência para enviar a notificação.

No campo **Notificar quando o certificado expira em**, digite quantos dias antes da expiração do certificado a notificação deve ser enviada.

14. Clique em **Salvar**.

    O provedor de credenciais é exibido na tabela Provedor de Credenciais.

Certificados APNs

April 15, 2019

Para registrar e gerenciar dispositivos iOS no XenMobile, configure um certificado de serviço de Notificação por Push(APNs) da Apple.

> Nota:
>
> - O certificado de APNs da Apple permite o gerenciamento de dispositivo móvel por meio da Rede Push da Apple. Se você acidentalmente ou intencionalmente revogar o certificado, perderá a capacidade de gerenciar os seus dispositivos.
> - O XenMobile também requer um certificado APNs se você planeja usar notificações por push para o Secure Mail para iOS.
> - Se você estiver usado o iOS Developer Enterprise Program para criar um certificado de envio por push do gerenciador de dispositivos móveis, talvez você precise tomar uma ação devido à migração dos certificados existentes para o Apple Push Certificates Portal.

Os tópicos que descrevem os procedimentos passo a passo estão listados em ordem nesta seção: Aqui está um resumo do processo.

Etapa 1: Para Windows, gere uma CSR usando o Windows Server 2012 R2 ou o Windows 2008 R2 Server, e o Microsoft IIS. Para Mac, gere uma CSR em um computador Mac. A Citrix recomenda esse método.

Etapa 2: Envie a CSR para a Citrix. A Citrix assina a CSR com o respectivo certificado de assinatura de gerenciamento de dispositivo móvel e retorna o arquivo assinado em um formato .plist.

Etapa 3: Envie a CSR assinada para a Apple e faça o download do certificado de APNs da Apple.

Etapa 4: Exporte o certificado de APNs como um certificado PCKS #12 (.pfx) (no IIS, Mac ou SSL).

Etapa 5: Importe um certificado de APNs para o XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Informações de migração de certificado de envio por push do Apple MDM

Os certificados de envio por push do gerenciamento de dispositivo móvel (MDM) criados no iOS Developer Enterprise Program foram migrados para o Apple Push Certificates Portal. Essa migração afeta a criação de novos certificados de envio por push do MDM e a renovação, a revogação e o download de certificados de envio por push do MDM existentes. A migração não afeta outros certificados de APNs (não MDM).

Se o seu certificado de envio por push do MDM tiver sido criado no iOS Developer Enterprise Program, as seguintes situações se aplicarão:

- O certificado foi migrado automaticamente para você.
- Você pode renovar o certificado no Apple Push Certificates Portal sem afetar os seus usuários.
- Você precisa usar o iOS Developer Enterprise Program para revogar ou baixar um certificado preexistente.

Se seus certificados de envio por push do MDM não estiverem perto de expirar, não será necessária nenhuma ação. Se você tiver um certificado de envio por push do MDM que está perto de expirar, entre em contato com seu provedor de soluções de MDM. Em seguida, faça com que o seu iOS Developer Program Agent faça login no Apple Push Certificates Portal com o ID Apple dele.

Todos os novos certificados de envio por push do MDM devem ser criados no Apple Push Certificates Portal. O iOS Developer Enterprise Program não permitirá mais a criação de um ID de Aplicativo com um Identificador de Pacote (tópico de APNs) que contenha `com.apple.mgmt`.

> Importante:
>
> Mantenha um controle do ID Apple usado para criar o certificado. Além disso, o ID Apple deve ser um ID corporativo, e não um ID pessoal.

Para criar uma CSR usando o Microsoft IIS

A primeira etapa para gerar uma solicitação de certificado de APNs para dispositivos iOS é criar uma Solicitação de Assinatura de Certificado (CSR). Em um Windows 2012 R2 ou Windows 2008 R2 Server, você pode gerar uma CSR usando o Microsoft IIS.

1. Abra o Microsoft IIS.
2. Clique duas vezes no ícone Certificados do Servidor do IIS.
3. Na janela Certificados do Servidor, clique em **Criar Solicitação de Certificado**.
4. Digite as informações adequadas de Nome Diferenciado (DN) e clique em **Avançar**.
5. Selecione **Microsoft RSA SChannel Cryptographic Provider** como o Provedor de Serviços de Criptografia e **2048** como o comprimento de bit e, em seguida, clique em **Avançar**.
6. Insira um nome do arquivo, especifique uma localização para salvar a CSR e clique em **Concluir**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para criar uma CSR em um computador Mac

1. Em um computador Mac que executa o macOS, em **Aplicativos > Utilitários**, inicie o aplicativo Keychain Access.
2. Abra o menu de **Keychain Access** e clique em **Preferences**.
3. Clique na guia **Certificates**, altere as opções **OCSP** e **CRL** para **Off** e feche a janela Preferences.
4. No menu **Keychain Access**, clique em **Certificate Assistant > Request a Certificate From a Certificate Authority**.
5. O Certificate Assistant solicita que você insira as seguintes informações:
   - **Email Address:** o endereço de email do indivíduo ou da conta de função responsável por gerenciar o certificado.
   - **Common Name:** o nome comum em Common Name composto pelo nome de host e nome de domínio. Isso normalmente se parece com “www.website.com” ou “website.com”. O nome em Common Name deve ser o mesmo que o endereço da Web que você acessa ao se conectar a um site.
   - **CA Email Address:** o endereço de email da autoridade de certificação.
6. Selecione as opções **Saved to disk** e **Let me specify key pair information**e clique em **Continue**.
7. Insira um nome para o arquivo da CSR, salve o arquivo no seu computador e depois clique em **Save**.
8. Especifique as informações de par de chaves: selecione o **Key Size** de 2048 bits e o **RSA algorithm** e clique em **Continue**. O arquivo da CSR está pronto para que você o carregue como parte do processo de certificado de APNs.
9. Clique em **Done** quando o Certificate Assistant concluir o processo da CSR.

Para criar uma CSR usando o OpenSSL

Se você não pode usar um computador Mac ou um Windows Server e Microsoft IIS suportados para gerar uma CSR, poderá usar o OpenSSL.

Para usar o OpenSSL para criar uma CSR, primeiro baixe e instale o OpenSSL no site do OpenSSL.

1. No computador no qual você instalou o OpenSSL, execute o seguinte comando de um prompt de comando ou shell.

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.
   csr -newkey rsa:2048
   ```

2. A mensagem de informações de nomenclatura de certificado a seguir é exibida. Insira as informações conforme solicitado.

   ```
   1 You are about to be asked to enter information that will be
       incorporated into your certificate request.
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
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 mensagem seguinte, insira uma senha para a chave privada da CSR.

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Para assinar a CSR

Antes de enviar o certificado à Apple, envie o certificado para a Citrix para assinatura, para que ele possa ser usado com o XenMobile.

1. No seu navegador, acesse o site XenMobile APNs CSR Signing.
2. Clique em **Upload the CSR**.
3. Procure e selecione o certificado.

   O certificado deve estar no formato .pem/txt.
4. Na página **XenMobile APNs CSR Signing**, clique em **Sign**. A CSR é assinada e salva automaticamente na sua pasta configurada de downloads.

Para enviar a CSR assinada para a Apple para obter o certificado de APNs

Depois de receber a sua Solicitação de Assinatura de Certificado (CSR) assinada da Citrix, você precisará enviá-la para a Apple para obter o certificado de APNs.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Alguns usuários relataram problemas ao fazer login no Apple Push Portal. Como alternativa, você pode fazer login no Apple Developer Portal antes de seguir o link para identity.apple.com na Etapa 1.

1. Em um navegador, vá para https://identity.apple.com/pushcert.
2. Clique em **Create a Certificate**.
3. Na primeira vez em que você cria um certificado junto à Apple, marque a caixa de seleção **I have read and agree to these terms and conditions** e clique em **Accept**.
4. Clique em **Choose File**, navegue até a CSR assinada no seu computador e clique em **Upload**. Uma mensagem de confirmação indica que o carregamento foi bem-sucedido.
5. Clique em **Download** para recuperar o certificado .pem.

   Se você estiver usando o Internet Explorer e a extensão do arquivo estiver ausente, clique em **Cancel** duas vezes e baixe da janela seguinte.

Para criar um certificado de APNs .pfx usando o Microsoft IIS

Para usar o certificado de APNs da Apple com o XenMobile, preencha a solicitação de certificado no Microsoft IIS, exporte o certificado como um arquivo de PCKS #12 (.pfx) e importe o certificado de APNs para o XenMobile.

> Importante:
>
> Para essa tarefa, use o mesmo servidor IIS que você usou para gerar a CSR.

1. Abra o Microsoft IIS.
2. Clique no ícone Certificados do Servidor.
3. Na janela **Certificados do Servidor**, clique em **Concluir Solicitação de Certificado**.
4. Procure 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 uma localização e um nome do arquivo para o certificado .pfx, além de uma senha e clique em **OK**.

   Você precisa da senha do certificado durante a instalação do XenMobile.
7. Copie o certificado .pfx para o servidor no qual planeja instalar o XenMobile.
8. Faça logon no console XenMobile como um administrador.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

9. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
10. Clique em **Certificados**. A página **Certificados** é exibida.
11. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
12. No menu **Importar**, selecione **Keystore**.
13. Em **Usar como**, selecione **APNs**.
14. No arquivo **Keystore**, selecione o arquivo de keystore a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
15. Em **Senha**, digite a senha atribuída ao certificado.
16. Clique em **Importar**.

Para criar um certificado de APNs .pfx em um computador Mac

1. No mesmo computador Mac que executa o macOS que você usou para gerar a CSR, localize o certificado de Identidade de produção (PEM) que você recebeu da Apple.
2. Clique duas vezes no arquivo de certificado para importá-lo para as chaves.
3. Se você for solicitado a adicionar o certificado a chaves específicas, mantenha as chaves de login padrão selecionadas e clique em **OK**. O certificado recém-adicionado é exibido na sua lista de certificados.
4. Clique no certificado e, no menu **File**, clique em **Export** para iniciar a exportação do certificado para um certificado PCKS #12 (.pfx).
5. Dê ao arquivo de certificado um nome exclusivo para uso com o XenMobile Server. Não inclua espaços no nome. Em seguida, escolha o local da 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, mantenha o certificado e a senha protegidos para uso e referência posteriores.
7. O aplicativo Keychain Access solicitará a senha de login ou as chaves selecionadas. Insira a senha e clique em **OK**. O certificado salvo agora está pronto para ser usado com o XenMobile Server.

   > Nota:
   >
   > Se você não pretende manter o computador e a conta de usuário que usou originalmente para gerar a CSR e concluir o processo de exportação de certificado, a Citrix recomenda salvar ou exportar as Chaves Pública e Pessoal do sistema local. Caso contrário, o acesso

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> aos certificados de APNs para reutilização será anulado e você precisará repetir todo o processo de CSR e APNs.

Para criar um certificado de APNs .pfx usando o OpenSSL

Depois de usar o OpenSSL para criar uma Solicitação de Assinatura de Certificado (CSR), você também poderá usar o OpenSSL para criar um certificado de APNs .pfx.

1. Em um prompt de comando ou shell, execute o comando a seguir.

   ```
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer
   .key.pem -out apns_identity.p12
   ```

2. Insira uma senha para o arquivo de certificado .pfx. Guarde essa senha, pois você a usará novamente quando carregar o certificado para o XenMobile.
3. Anote a localização do arquivo de certificado .pfx. Depois copie o arquivo para o XenMobile Server para que você possa usar o console para carregar o arquivo.

Para importar um certificado de APNs para o XenMobile

Depois de solicitar e receber um novo certificado de APNs, importe-o para o XenMobile para adicioná-lo pela primeira vez ou para substituir um certificado existente.

1. No console 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. No menu **Importar**, selecione **Keystore**.
5. Em **Usar como**, selecione **APNs**.
6. Navegue até o arquivo .p12 no seu computador.
7. Insira uma senha e clique em **Importar**.

Para obter mais informações sobre certificados no XenMobile, consulte Certificados.

Para renovar um certificado de APNs

Para renovar um certificado de APNs, realize as mesmas etapas que usaria para criar um certificado. Em seguida, visite o Apple Push Certificates Portal e carregue o novo certificado. Depois de fazer login, você vê o seu certificado existente, ou talvez veja um certificado que foi importado da sua conta anterior do Apple Developers.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

No Certificates Portal, a única diferença durante a renovação do certificado é que você clica em **Renew**. Você deve ter uma conta de desenvolvedor no Certificates Portal para acessar o site. Quando renovar seu certificado, lembre-se de usar o mesmo nome da organização e ID Apple.

Para determinar quando o certificado de APNs expira, no console XenMobile, clique em **Configurar > Configurações > Certificados**. No entanto, se o certificado tiver expirado, não o revogue.

1. Gere uma CSR usando o IIS (Microsoft), o OpenSSL ou o Keychain Access (macOS).
2. No site XenMobile APNs CSR Signing, selecione **Solicitar assinatura de certificado de notificação por push**.
3. Clique em **+ Upload the CSR**. Em seguida, na caixa de diálogo, navegue até a CSR, clique em **Abrir** e clique em **Login**.
4. Quando você receber um arquivo .plist, salve-o.
5. Clique em **Apple Push Certificates Portal** e faça logon.
6. Selecione o certificado que deseja renovar e clique em **Renovar**.
7. Carregue o arquivo .plist. Você receberá um arquivo .pem como resultado. Salve o arquivo .pem.
8. Usando esse arquivo .pem, preencha o CSR (de acordo com o método usado para criar o CSR na Etapa 1).
9. Exporte o certificado como um arquivo .pfx.

No console XenMobile, importe o arquivo .pdx e conclua a configuração da seguinte maneira:

1. Vá para **Configurações > Gerenciamento de certificados**.
2. Na página **Certificados**, clique em **Importar**.
3. No **menu Importar**, selecione **Keystore**.
4. No **Tipo de Keystore**, escolha **PKCS#12**.
5. Em **Usar como**, selecione **APNs**.
6. Em **Arquivo de keystore**, clique em **Procurar** e navegue até o arquivo.
7. Em **Senha**, digite a senha do certificado.
8. Digite uma **Descrição** opcional.
9. Clique em **Importar**.

O XenMobile redireciona você de volta à página **Certificados**. Os campos **Nome**, **Status**, **Válido de** e **Válido até** são atualizados.

SAML para login único com o ShareFile

April 15, 2019

Você pode configurar o XenMobile e o ShareFile para usar a SAML (Security Assertion Markup Language) para fornecer acesso via logon único (SSO) a aplicativos do ShareFile Mobile. Essa funcionali-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dade inclui aplicativos do ShareFile preparados com o MDX Toolkit e clientes ShareFile não preparados, como o site da Web, o plug-in do Outlook ou os clientes de sincronização.

- **Para aplicativos ShareFile preparados**. Os usuários que fazem login no ShareFile por meio do aplicativo móvel do ShareFile são redirecionados para o Secure Hub para autenticação do usuário e para obter um token SAML. Após a autenticação bem-sucedida, o aplicativo móvel do ShareFile envia o token SAML para o ShareFile. Após o logon inicial, os usuários podem acessar o aplicativo móvel do ShareFile por meio de SSO. Eles também podem anexar documentos do ShareFile a emails do Secure Mail sem fazer login todas as vezes.
- **Para clientes ShareFile não preparados**. Os usuários que fazem login no ShareFile usando um navegador da Web ou outro cliente ShareFile são redirecionados para o XenMobile. O XenMobile autentica os usuários, que então adquirem um token SAML que é enviado para o ShareFile. Após o login inicial, os usuários podem acessar os clientes ShareFile por meio de SSO sem fazer login toda vez.

Para usar o XenMobile como um provedor de identidade de SAML (IdP) para o ShareFile, você deve configurar o XenMobile para usar o ShareFile Enterprise, conforme descrito neste artigo. Como alternativa, você pode configurar o XenMobile para funcionar apenas com os StorageZone Connectors. Para obter mais informações, consulte Uso do ShareFile com o XenMobile.

Para um diagrama da arquitetura de referência detalhada, consulte Arquitetura.

Pré-requisitos

Conclua os pré-requisitos antes de configurar o SSO com aplicativos XenMobile e ShareFile:

- O MDX Service ou uma versão compatível do MDX Toolkit (para aplicativos do ShareFile Mobile).

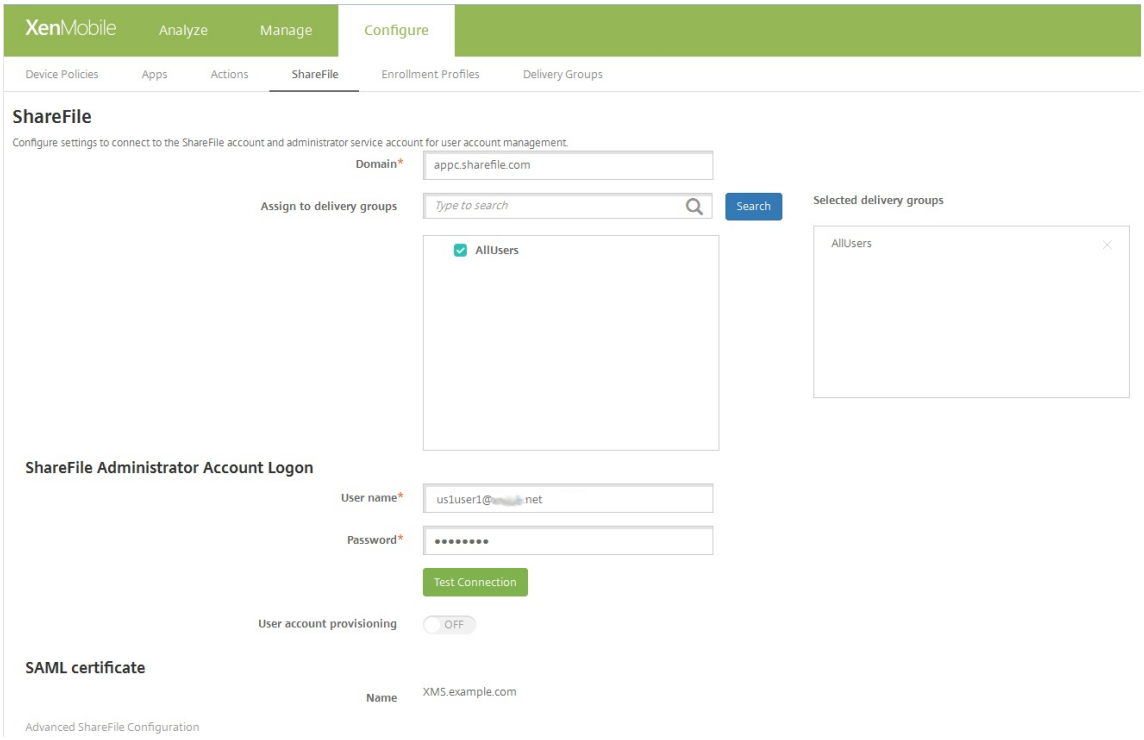
  Para obter mais informações, consulte Compatibilidade do XenMobile.
- Uma versão compatível de aplicativos do ShareFile Mobile e do Secure Hub.
- Conta de administrador do ShareFile.
- Conectividade verificada entre o XenMobile e o ShareFile.

Configurar o acesso ao ShareFile

Antes de configurar SAML para ShareFile, forneça as informações de acesso ao ShareFile da seguinte maneira:

1. No console da Web do XenMobile, clique em **Configurar > ShareFile**. A página de configuração do **ShareFile** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

   - **Domínio:** digite seu nome de subdomínio do ShareFile. Por exemplo: `example.sharefile.com`.
   - **Atribuir a grupos de entrega:** selecione ou pesquise os grupos de entrega nos quais você deseja usar o SSO com o ShareFile.
   - **Login de conta de administrador do ShareFile**
   - **Nome de usuário:** digite o nome de usuário do administrador do ShareFile. Esse usuário deve ter privilégios de administrador.
   - **Senha:** digite a senha de administrador do ShareFile.
   - **Provisionamento de conta de usuário:** para habilitar o provisionamento de usuário no XenMobile, ative essa configuração. Para usar a ShareFile User Management Tool para provisionamento de usuários, deixe esta configuração desabilitada.

   > Nota:
   >
   > Se um usuário sem uma conta do ShareFile for incluído nas funções selecionadas, e você habilitar o Provisionamento de conta de usuário, o XenMobile provisionará automaticamente uma conta do ShareFile para o usuário. A Citrix recomenda que você use uma função com uma pequena associação para testar a configuração. Isso evita a presença de muitos usuários sem contas do ShareFile.

3. Clique em **Testar conexão** para verificar se o nome de usuário e a senha para a conta de administrador do ShareFile autenticam a conta especificada do ShareFile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Clique em **Salvar**. O XenMobile sincroniza com o ShareFile e atualiza as configurações do ShareFile **Emissor de ShareFile/ID de entidade** e **URL de Login**.

Configurar SAML para aplicativos ShareFile MDX preparados

As etapas a seguir se aplicam aos aplicativos e dispositivos iOS e Android.

1. Com o MDX Toolkit, prepare o aplicativo do ShareFile Mobile. Para obter mais informações sobre como preparar aplicativos com o MDX Toolkit, consulte Preparação de aplicativos com o MDX Toolkit.
2. No console XenMobile, carregue o aplicativo preparado do ShareFile Mobile. Para obter informações sobre como carregar aplicativos MDX, consulte Para adicionar um aplicativo MDX ao XenMobile.
3. Verifique as configurações de SAML: faça login no ShareFile com o nome de usuário e a senha do administrador que você configurou acima.
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 do ShareFile

1. No dispositivo do usuário, instale e configure o Secure Hub.
2. Na XenMobile Store, baixe e instale o aplicativo do ShareFile Mobile.
3. Inicie o aplicativo do ShareFile Mobile. O ShareFile é iniciado sem a necessidade de informar o nome do usuário ou a senha.

Validar com Secure Mail

1. No dispositivo do usuário, caso ainda não tenha sido feito, instale e configure o Secure Hub.
2. Na XenMobile Store, baixe, instale e configure o Secure Mail.
3. Abra um novo formulário de email e toque em **Anexar do ShareFile**. Os arquivos disponíveis para serem anexados ao email são mostrados sem a necessidade de informar nome do usuário ou senha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o NetScaler Gateway para outros clientes do ShareFile

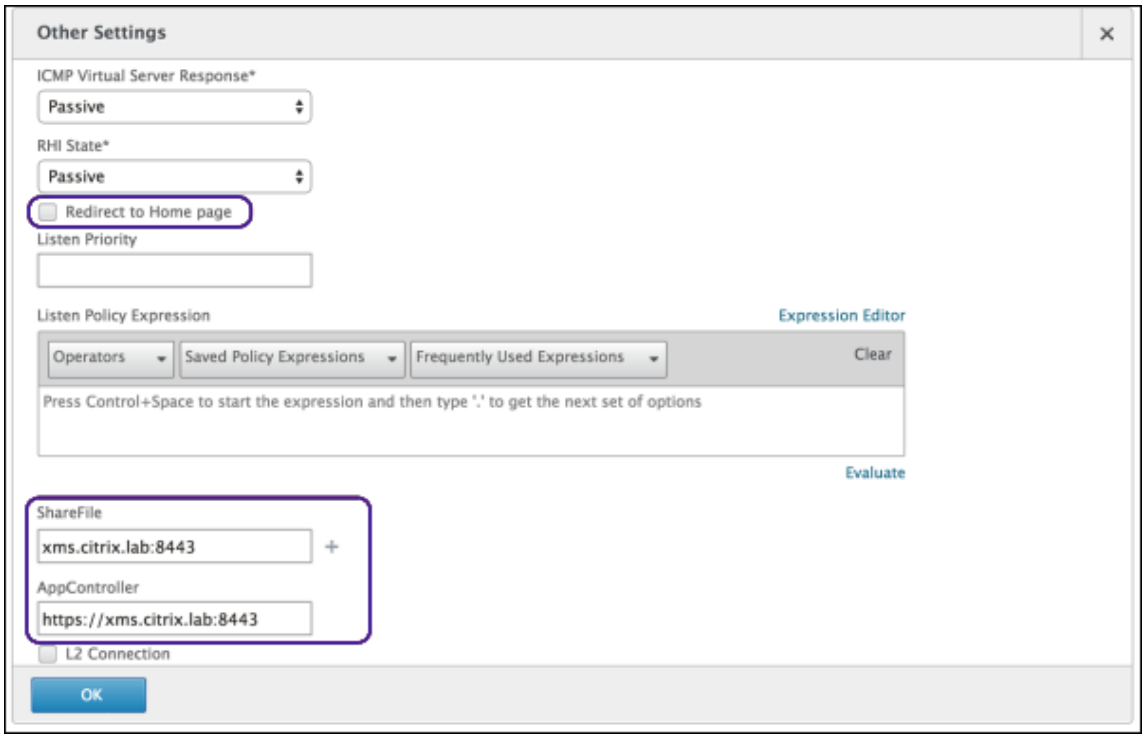
Para configurar o acesso aos clientes do ShareFile não preparados, como site da Web, plug-in do Outlook ou clientes de sincronização, configure o NetScaler Gateway para dar suporte ao uso do XenMobile como um provedor de identidade SAML da seguinte maneira:

- Desative o redirecionamento de página inicial.
- Crie uma política de sessão e um perfil do ShareFile.
- Configure políticas no servidor virtual do NetScaler Gateway.

Desative o redirecionamento de página inicial

Desative o comportamento padrão para solicitações que chegam pelo caminho /cginfra. Essa ação permite que os usuários vejam a URL interna solicitada original em vez da página inicial configurada.

1. Edite as configurações do servidor virtual do NetScaler Gateway usado para logins no XenMobile. No NetScaler, acesse **Other Settings** e desmarque a caixa de seleção **Redirect to Home Page**.



2. Em **ShareFile**, digite o nome e o número da porta do servidor interno do XenMobile.
3. Em **AppController**, digite sua URL do XenMobile.

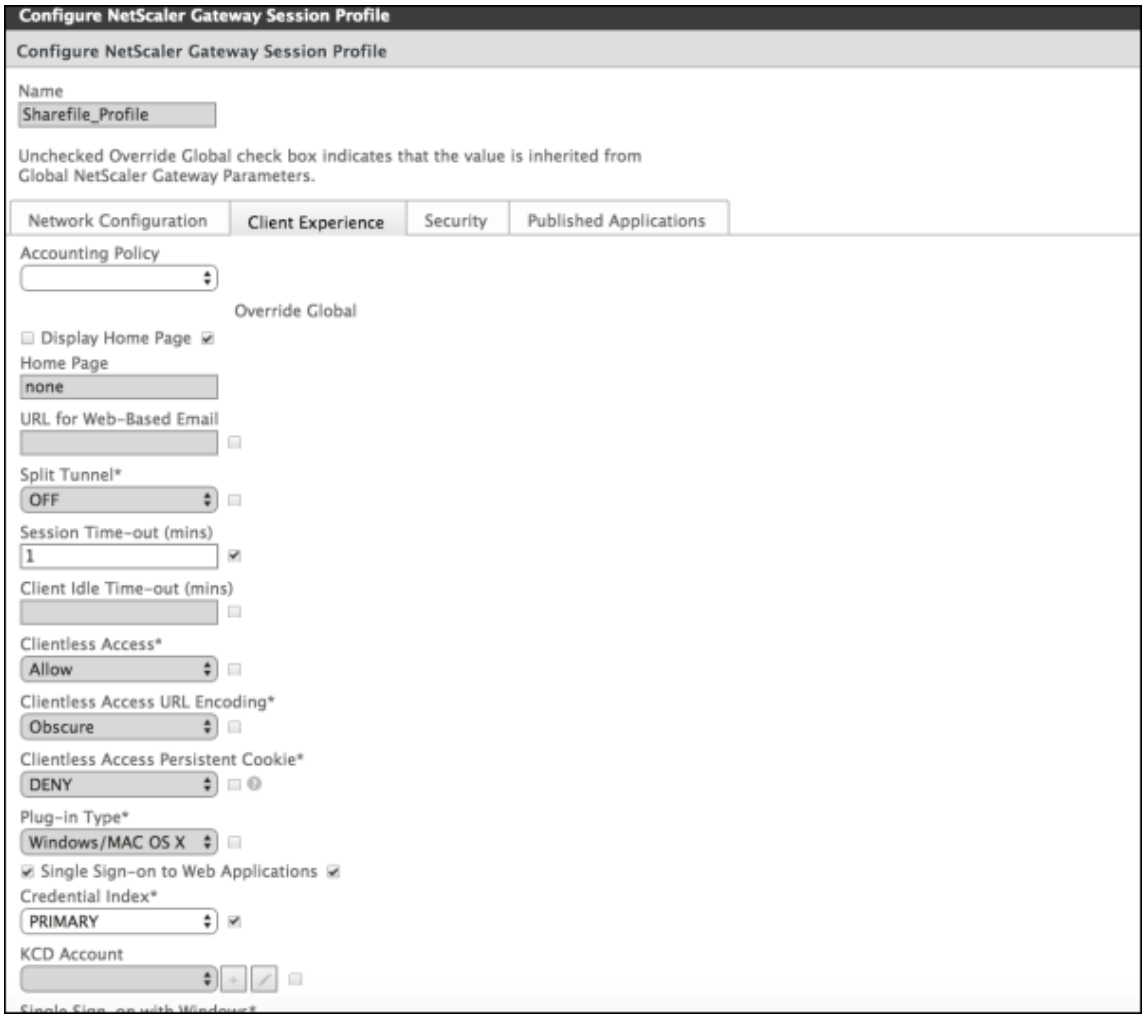
   Essa configuração autoriza as solicitações da URL inserida por meio do caminho /cginfra.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Criar uma política de sessão e um perfil de solicitação do ShareFile

Defina estas configurações para criar uma política de sessão e um perfil de solicitação do ShareFile:

1. No utilitário de configuração do NetScaler Gateway, no painel de navegação esquerdo, clique em **NetScaler 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 NetScaler Gateway Session Profile** é exibida.



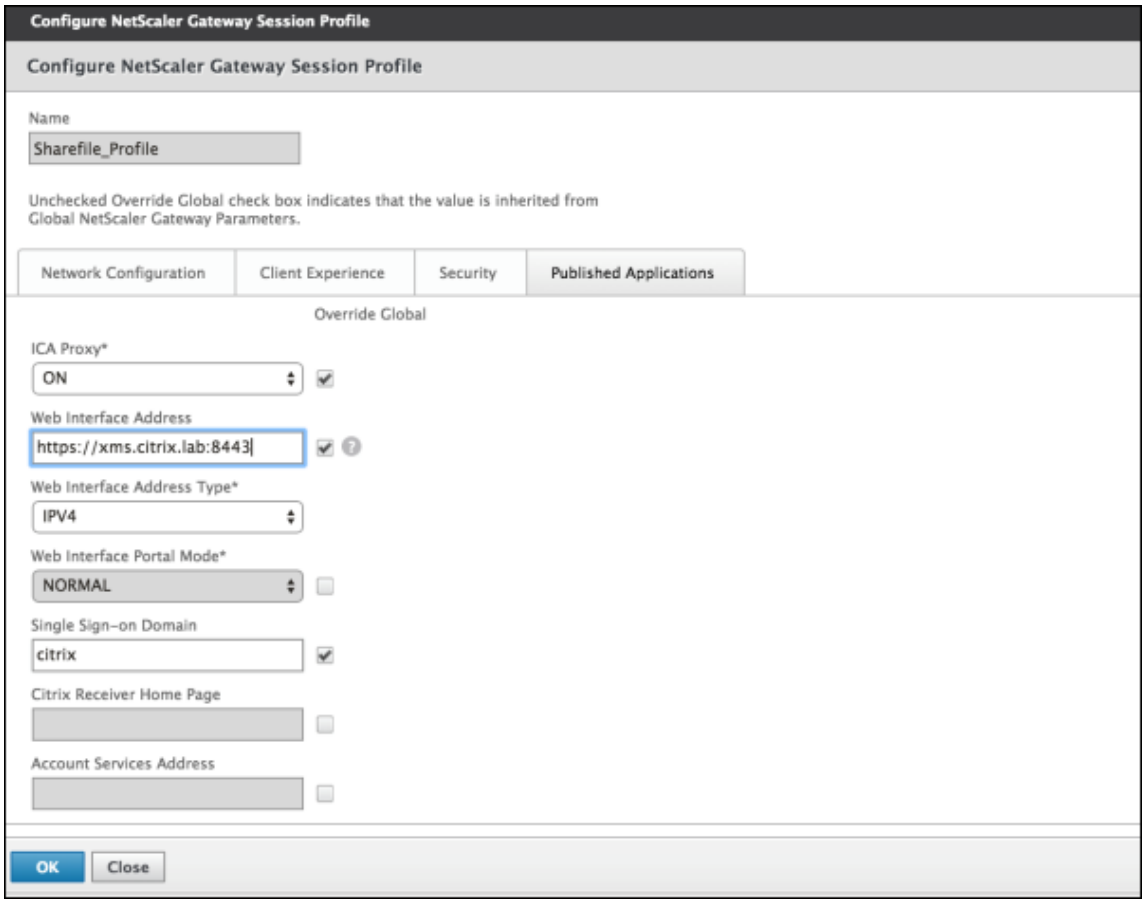
Defina estas configurações:

- **Name:** digite **ShareFile_Profile**.
- Clique na guia **Client Experience** e defina estas configurações:
  - **Home Page:** digite **none**.
  - **Session Time-out (mins):** digite **1**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Single Sign-on to Web Applications:** selecione esta configuração.
- **Credential Index:** clique em **PRIMARY**.

- Clique na guia **Published Applications**.



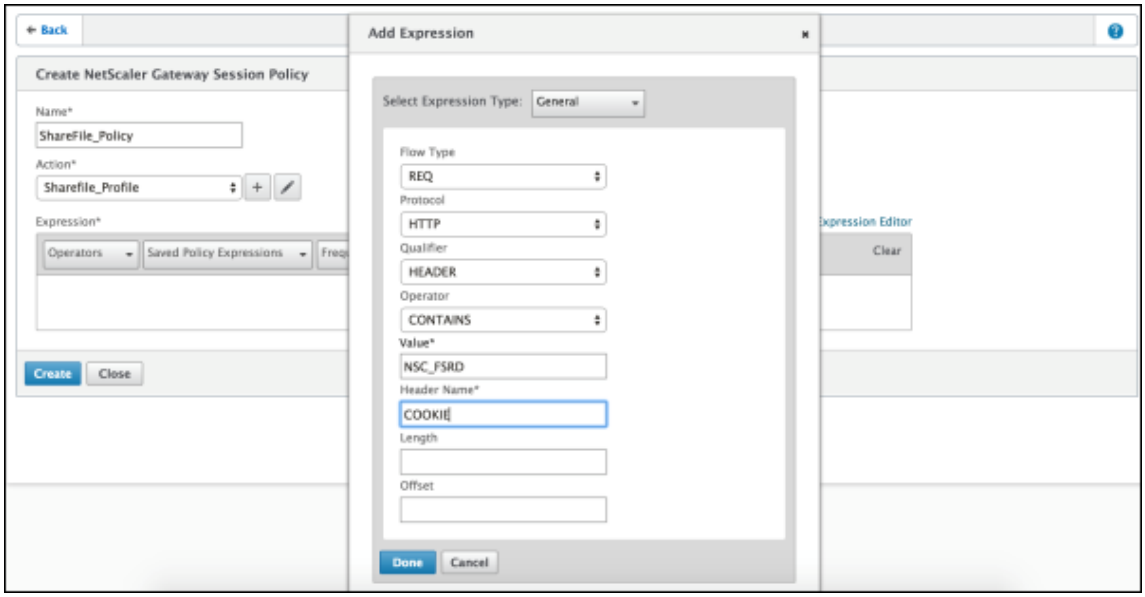
Defina estas configurações:

- **ICA Proxy:** clique em **ON**.
- **Web Interface Address:** digite sua URL do XenMobile Server.
- **Single Sign-on Domain:** digite o nome do domínio do Active Directory.

  Durante a configuração do NetScaler Gateway Session Profile, o sufixo de domínio para **Single Sign-on Domain** deve corresponder ao alias de domínio do XenMobile definido no LDAP.

5. Clique em **Create** para definir o perfil de sessão.
6. Clique em **Expression Editor**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **Value:** digite **NSC_FSRD**.
- **Header Name:** digite **COOKIE**.

7. Clique em **Create** e em **Close**.



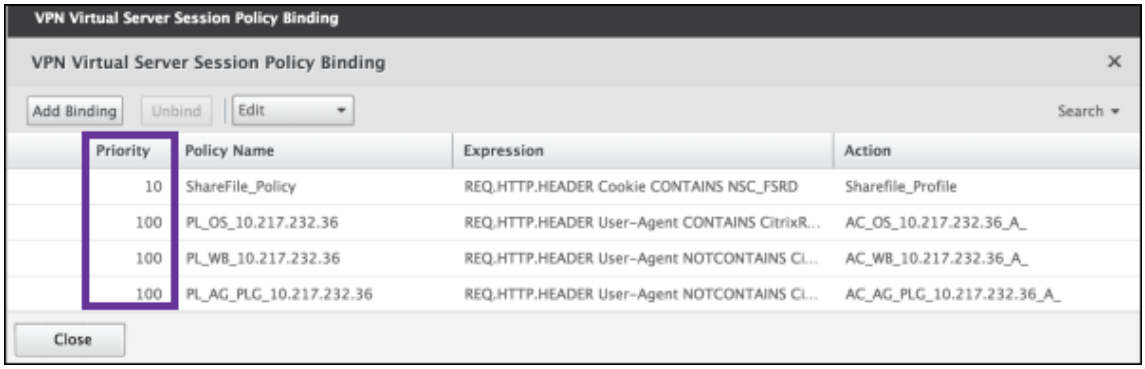
Configure políticas no servidor virtual do NetScaler Gateway

Defina estas configurações no servidor virtual do NetScaler Gateway.

1. No utilitário de configuração do NetScaler Gateway, no painel de navegação esquerdo, clique em **NetScaler Gateway > Virtual Servers**.
2. No painel **Details**, clique em seu servidor virtual do NetScaler Gateway.
3. Clique em **Edit**.
4. Clique em **Configured policies > Session policies** e em **Add binding**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Selecione **ShareFile_Policy**.
6. Edite o número de **Priority** gerado automaticamente para a política selecionada, para que ele tenha a prioridade mais alta (o menor número) em relação às outras políticas listadas. Por exemplo:



7. Clique em **Done** e salve a configuração do NetScaler em execução.

Configurar SAML para aplicativos ShareFile não MDX

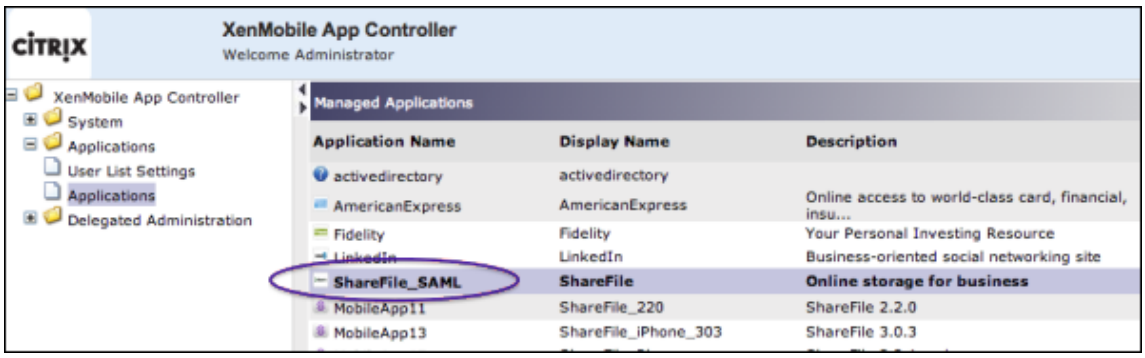
Use as etapas abaixo para encontrar o nome do aplicativo interno para sua configuração do ShareFile.

1. Faça login na ferramenta de administrador do XenMobile usando a URL `https://<XenMobile server>:4443/OCA/admin/`. Não se esqueça de inserir “OCA” em letras maiúsculas.
2. Na lista **Exibir**, clique em **Configuração**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Clique em **Aplicativos > Aplicativos** e anote o **Nome do aplicativo** com o **Nome de exibição ShareFile**.



Modificar as configurações de SSO do ShareFile.com

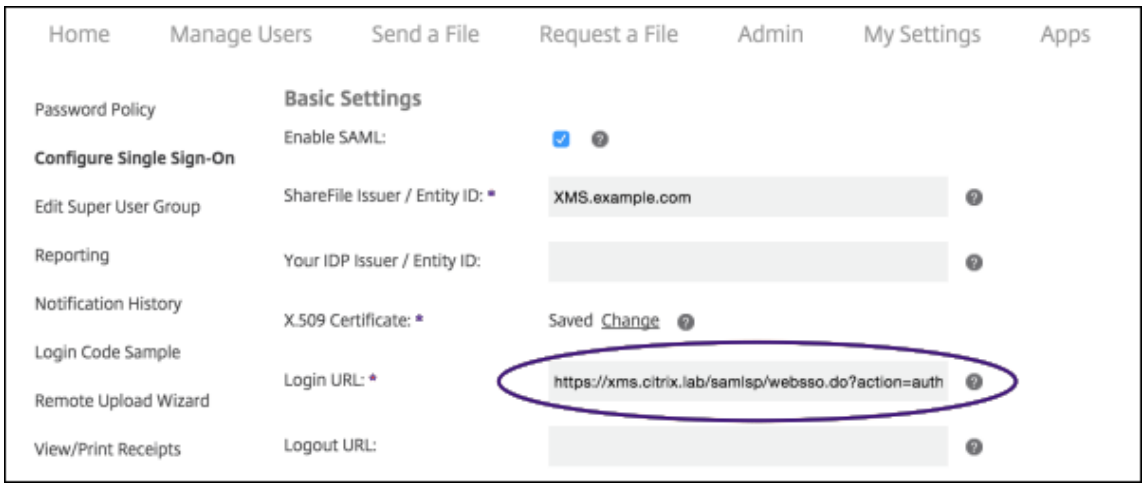
Faça as seguintes alterações para aplicativos ShareFile MDX e não-MDX.

> Importante:
>
> Toda vez que você edita ou recria o aplicativo ShareFile ou altera as configurações do ShareFile no XenMobile, um novo número é anexado ao nome do aplicativo interno. Como resultado, você também deve atualizar a URL de Login no site do ShareFile para refletir o nome do aplicativo atualizado.

1. Faça login na sua conta do ShareFile (`https://<subdomain>.sharefile.com`) como administrador do ShareFile.
2. Na interface da Web do ShareFile, clique em **Administrador** e selecione **Configurar logon único**.
3. Edite a **URL de login** da seguinte maneira:

   Aqui está um exemplo de **URL de login** antes das edições: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Insira o FQDN externo do servidor virtual do NetScaler Gateway mais **/cginfra/https/** na frente do FQDN do XenMobile Server e adicione **8443** após o FQDN do XenMobile.

  Aqui está uma amostra de uma 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 do aplicativo interno do ShareFile. 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).

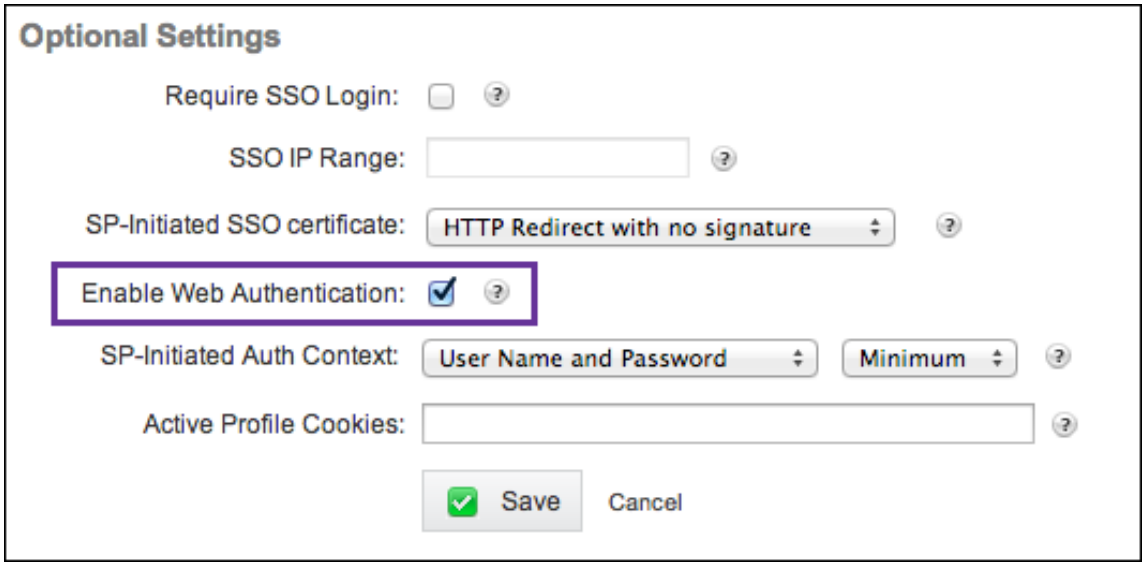
  Aqui está uma amostra de um URL editado: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- Adicione `&nssso=true` ao final da URL.

  Aqui está uma amostra 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**, marque a caixa de seleção **Ativar autenticação da Web**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Validar a configuração

Siga os procedimentos a seguir para validar a configuração.

1. Aponte seu navegador para `https://<subdomain>sharefile.com/saml/login`.

   Você será redirecionado para o formulário de logon do NetScaler Gateway. Se você não for redirecionado, verifique as definições de configuração anteriores.

2. Insira o nome do usuário e a senha do NetScaler Gateway e do ambiente do XenMobile configurado.

   Suas pastas do ShareFile em `<subdomain>.sharefile.com` aparecem. Se você não vir as pastas do ShareFile, verifique se inseriu as credenciais de login corretas.

Azure Active Directory como IDP

April 15, 2019

Configurar o Azure Active Directory (AD) como seu provedor de identidade (IDP) permite que os usuários se registram no XenMobile usando suas credenciais do Azure.

iOS, Android e Windows 10 dispositivos são compatíveis. Dispositivos iOS e Android são registrados por meio do Secure Hub.

Configure o Azure como seu IDP em **Configurações > Autenticação > IDP**. A página **IDP** é nova nesta versão do XenMobile. Em versões anteriores do XenMobile, você configurava o Azure em **Configurações > Microsoft Azure**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos

- Versões e licenças
  - Para registrar dispositivos Android ou iOS, você precisa do Secure Hub 10.5.5.
  - Para registrar dispositivos Windows 10, você precisa de licenças do Microsoft Azure Premium.
- Serviços e autenticação de diretório
  - O XenMobile Server deve ser configurado para a autenticação baseada em certificado.
  - Se você estiver usando o NetScaler para autenticação, o NetScaler deverá 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 o LDAP. Configure o servidor LDAP local para sincronizar com o Azure AD.

Fluxo de autenticação

Quando o dispositivo se registra por meio do Secure Hub e o XenMobile está configurado para usar o Azure como seu IDP:

1. Os usuários inserem um nome de usuário e uma senha em seus dispositivos, na tela de logon 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 nesse token. O XenMobile retorna um ID de sessão.

Configuração da conta do Azure

Para usar o Azure AD como seu IDP, primeiro faça login na sua conta do Azure e faça estas alterações:

1. Registre o seu domínio personalizado e verifique esse domínio. Para obter detalhes, consulte Adicionar seu próprio nome de domínio ao Active Directory do Azure.
2. Estenda seu diretório local para o Active Directory do Azure usando ferramentas de integração de diretório. Para obter detalhes, consulte Integração de Diretórios.

Para usar o AD do Azure para registrar dispositivos Windows 10, faça as seguintes alterações na sua conta do Azure:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Torne o MDM uma parte confiável de AD do Azure. Para fazer isso, clique em **Active Directory do Azure > Aplicativos** e clique em **Adicionar**.
2. Selecione **Adicionar um aplicativo** na galeria. Acesse **MOBILE DEVICE MANAGEMENT** e selecione **Aplicativo MDM no local**. Salve as configurações.

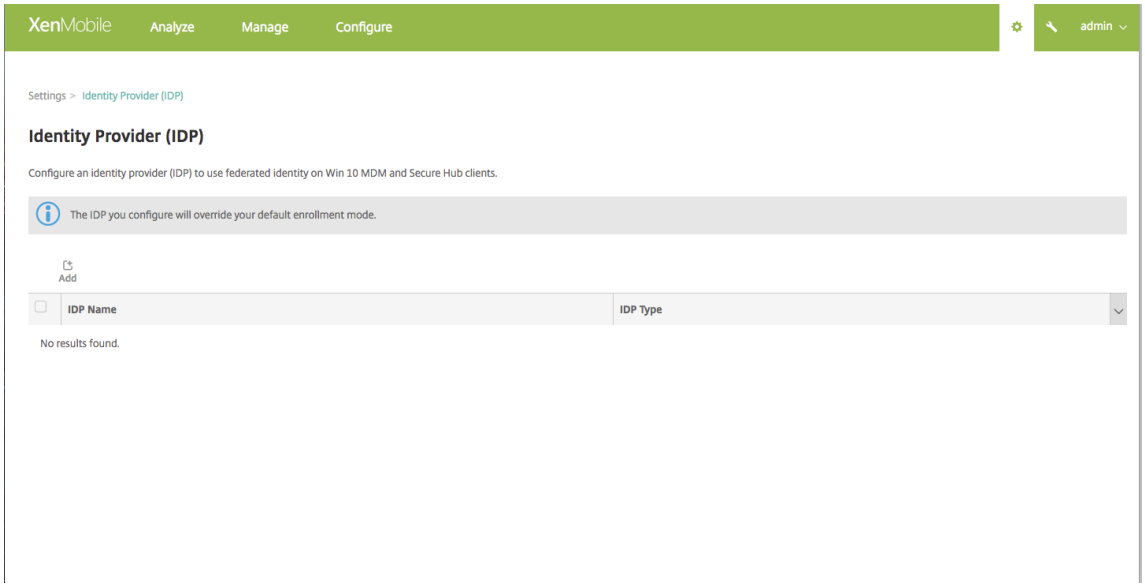
   Você escolhe o aplicativo local mesmo se tiver se inscrito na nuvem do Citrix XenMobile. Na terminologia da Microsoft, qualquer aplicativo não multilocatário é um aplicativo MDM local.
3. No aplicativo, configure a descoberta do XenMobile Server, os pontos de extremidade dos termos de uso e a URI do ID de aplicativo, da seguinte forma:
   - **URL de descoberta do MDM:** `https://<FQDN>:8443/<instanceName>/wpe`
   - **URL dos Termos de Uso do MDM:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **URI de ID do aplicativo** `https://<FQDN>:8443/`
4. Selecione o aplicativo MDM local que você criou na etapa 2. Ative a opção **Gerenciar dispositivos para estes usuários** para permitir o gerenciamento de MDM para todos os usuários ou para qualquer grupo específico de usuários.

   Para obter mais informações sobre como usar o Azure AD com dispositivos Windows 10, consulte o artigo da Microsoft Azure Active Directory integration with MDM.

Configurar o AD do Azure como seu IDP

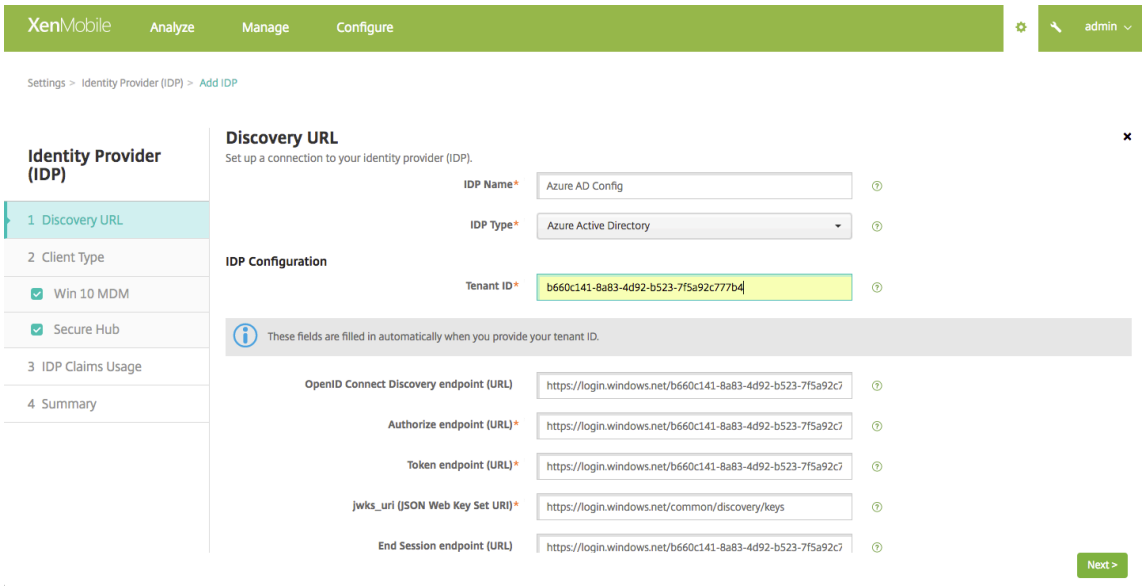
1. Localize ou anote as informações necessárias da sua conta do Azure:
   - ID de locatário, na página de configurações do aplicativo Azure.
   - Se quiser usar o Azure AD para registrar dispositivos Windows 10, você também precisará do seguinte:
     - **URI do ID de aplicativo:** a URL do servidor que executa o XenMobile.
     - **ID do cliente:** o identificador exclusivo do seu aplicativo, na página de configuração do Azure.
     - **Chave:** na página de configurações do aplicativo Azure.
2. No console 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Clique em **Adicionar**. A página **Configuração IDP** é exibida.
5. Configure as seguintes informações sobre seu IDP:
   - **Nome do IDP:** digite um nome para a conexão com o IDP que você está criando.
   - **Tipo de IDP:** escolha Azure Active Directory como tipo de IDP.
   - **ID do locatário:** copie esse valor da página de configurações do aplicativo Azure. Na barra de endereços 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`.



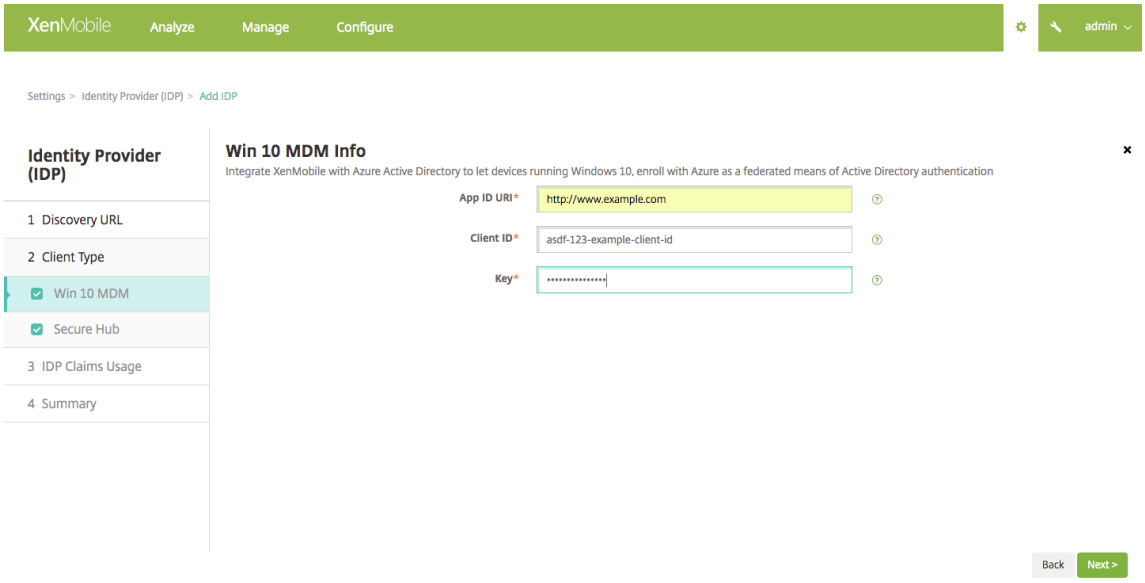
6. O restante dos campos é preenchido automaticamente. Quando eles estiverem preenchidos,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

clique em **Avançar**.

7. Para configurar o XenMobile para registrar dispositivos Windows 10 usando o AD do Azure para registro do MDM, defina as seguintes configurações. Para ignorar essa etapa opcional, desmarque **Win 10 MDM**.

   - **URI do ID de aplicativo:** digite a URL do XenMobile Server inserido quando você definiu as configurações do Azure.
   - **ID do cliente:** copie e cole esse valor da página Configurar do Azure. O ID do cliente é o identificador exclusivo do seu aplicativo.
   - **Chave:** copie esse valor da página de configurações do aplicativo Azure. Em chaves, selecione uma duração na lista e salve a configuração. Você pode copiar a chave e colá-la nesse campo. Uma chave é necessária para a leitura e a gravação de dados no AD do Microsoft Azure.

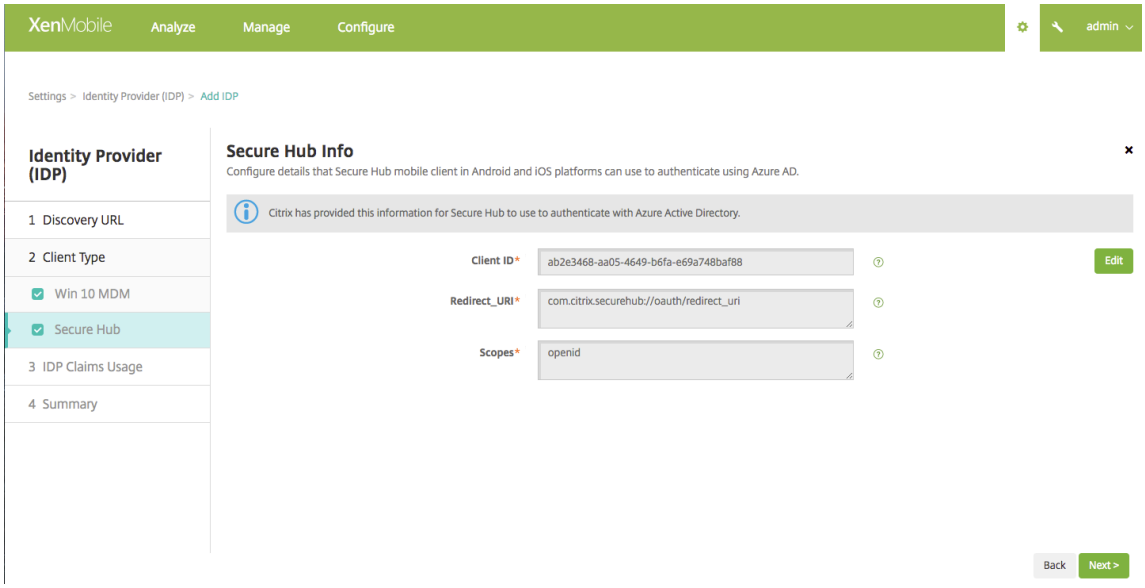


8. Clique em **Avançar**.

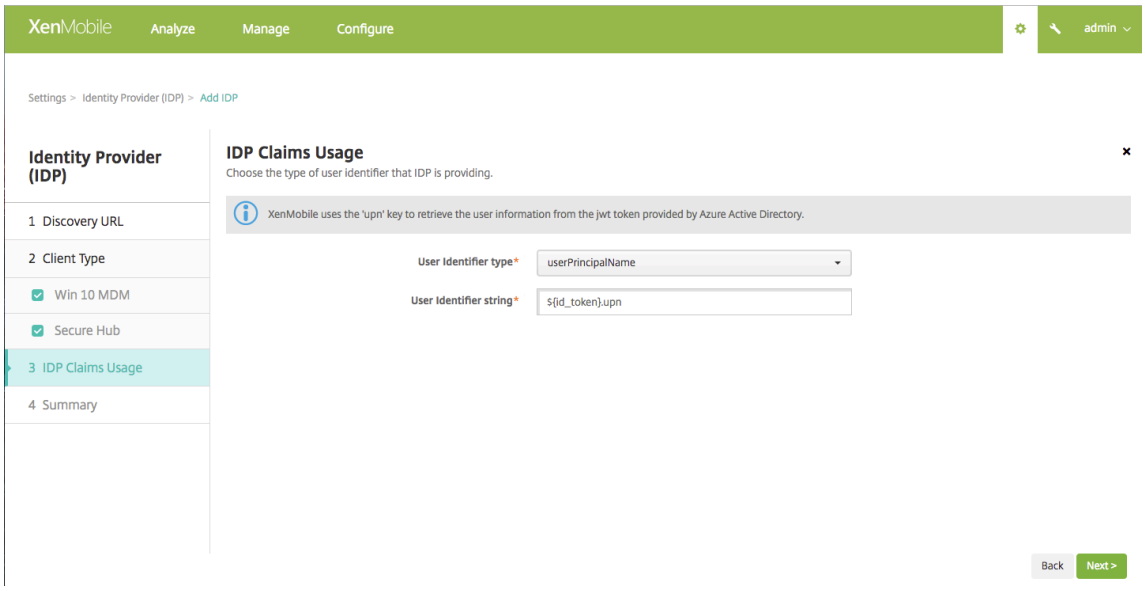
   A Citrix registrou o Secure Hub no Microsoft Azure e mantém as informações. Essa tela mostra os detalhes usado pelo Secure Hub para se comunicar com o Azure Active Directory. Essa página será usada no futuro se essas informações precisarem de alteração. Edite essa página apenas se recomendado pela Citrix.

9. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

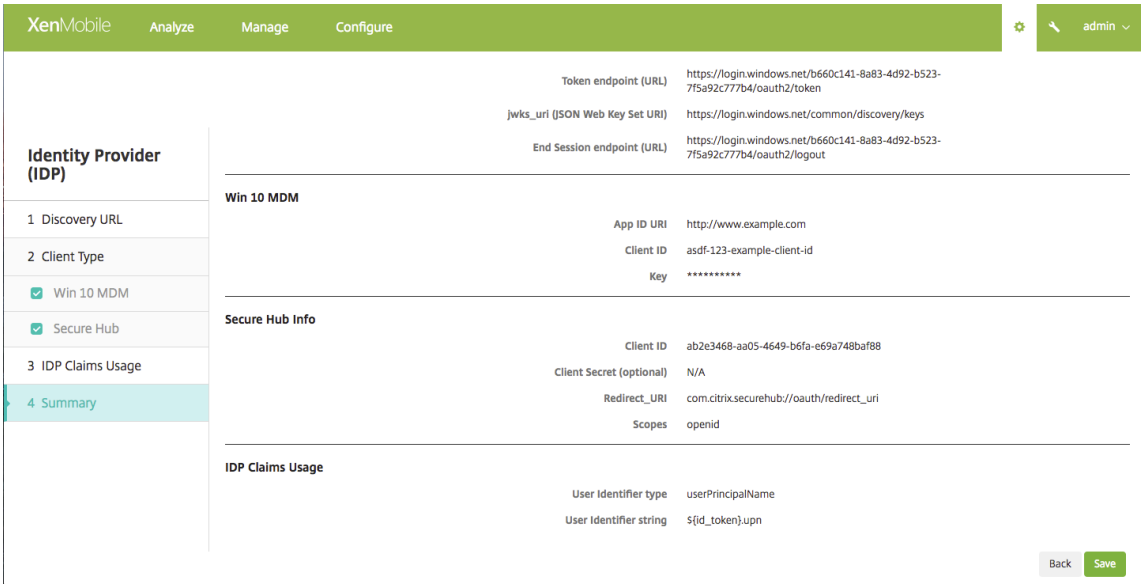


10. Configure o tipo de identificador de usuário que seu IDP fornece:
    - **Tipo de identificador do usuário:** escolha **userPrincipalName** na lista.
    - **Sequência de caracteres do identificador do usuário:** esse campo é preenchido automaticamente.
11. Clique em **Avançar**.



12. Revise a página **Resumo** e clique em **Salvar**.

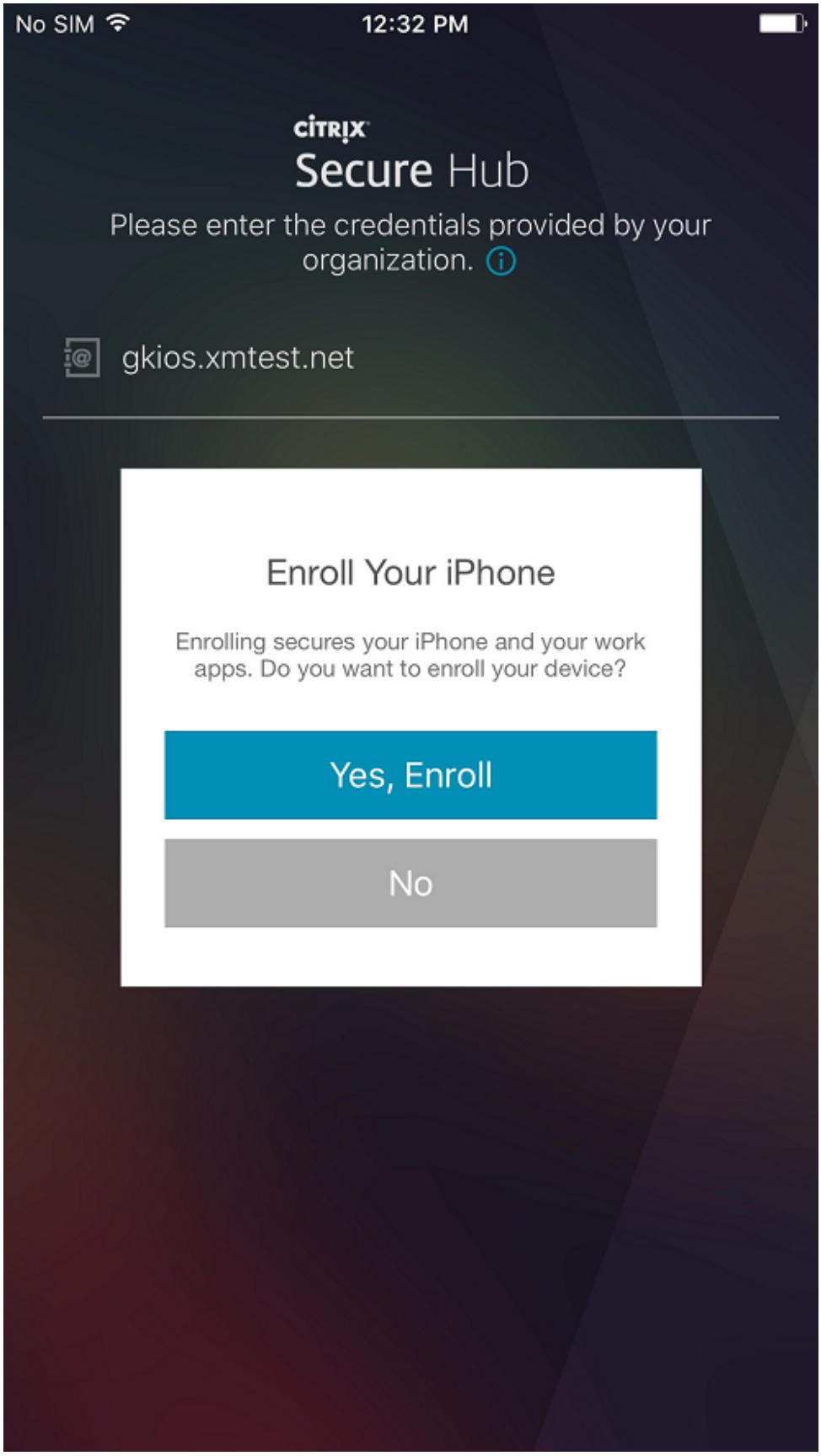
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Experiência dos usuários

1. Os usuários iniciam o Secure Hub. Em seguida, eles inserem o nome de domínio totalmente qualificado (FQDN) do XenMobile Server, nome UPN ou endereço de email.

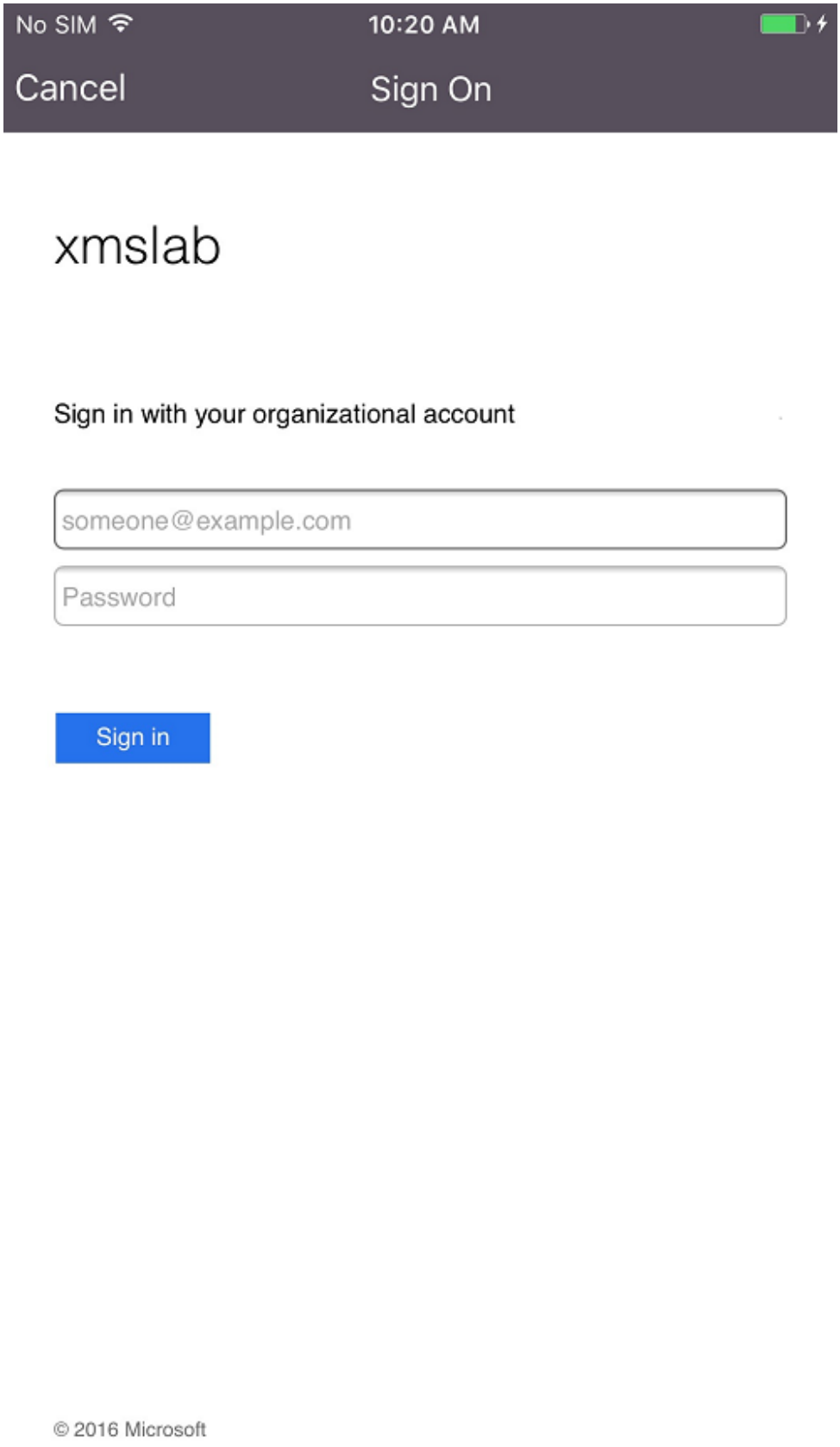
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em seguida, os usuários clicam em **Sim, registrar**.

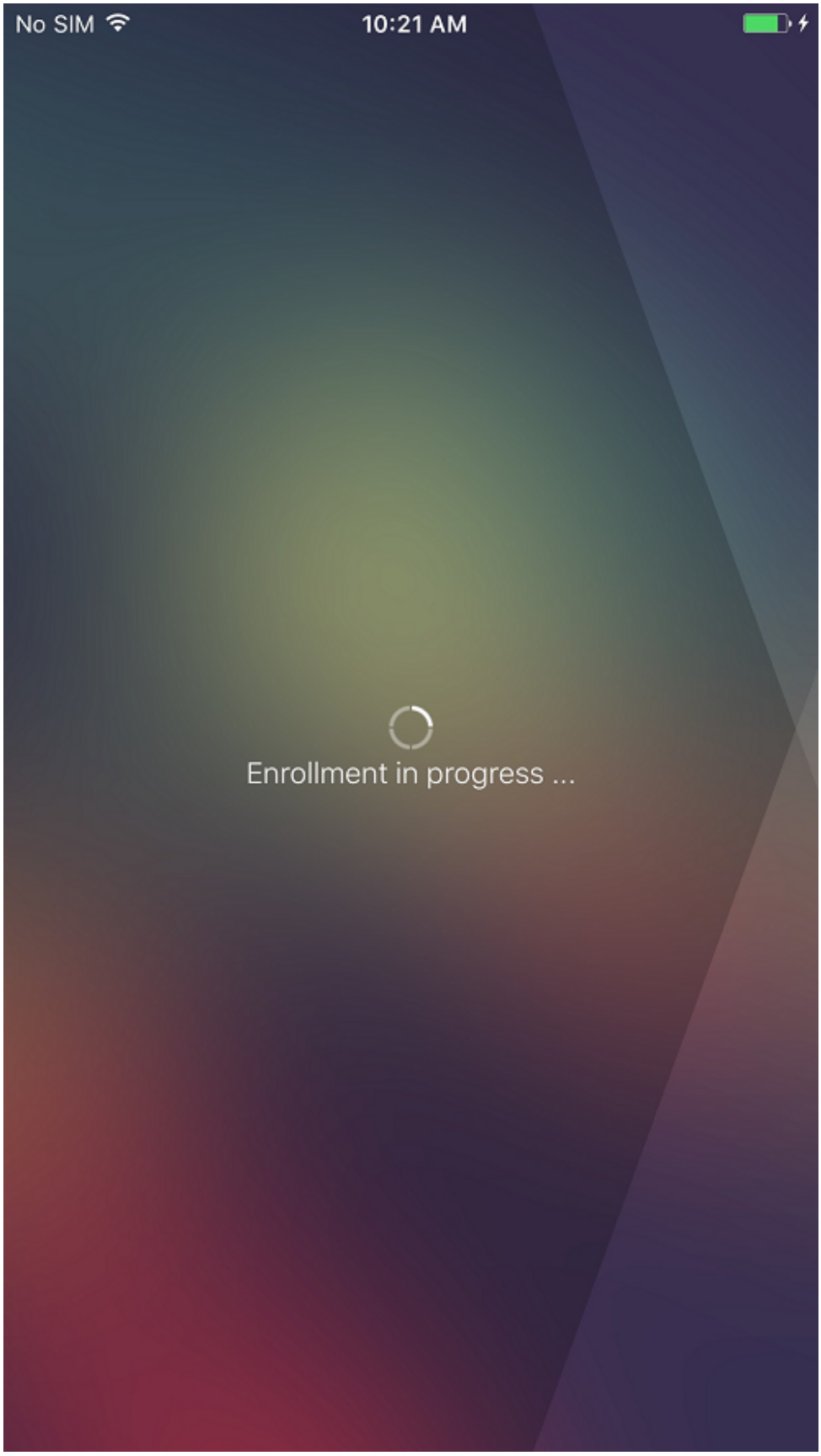
© 1999-2019 Citrix Systems, Inc. All rights reserved.



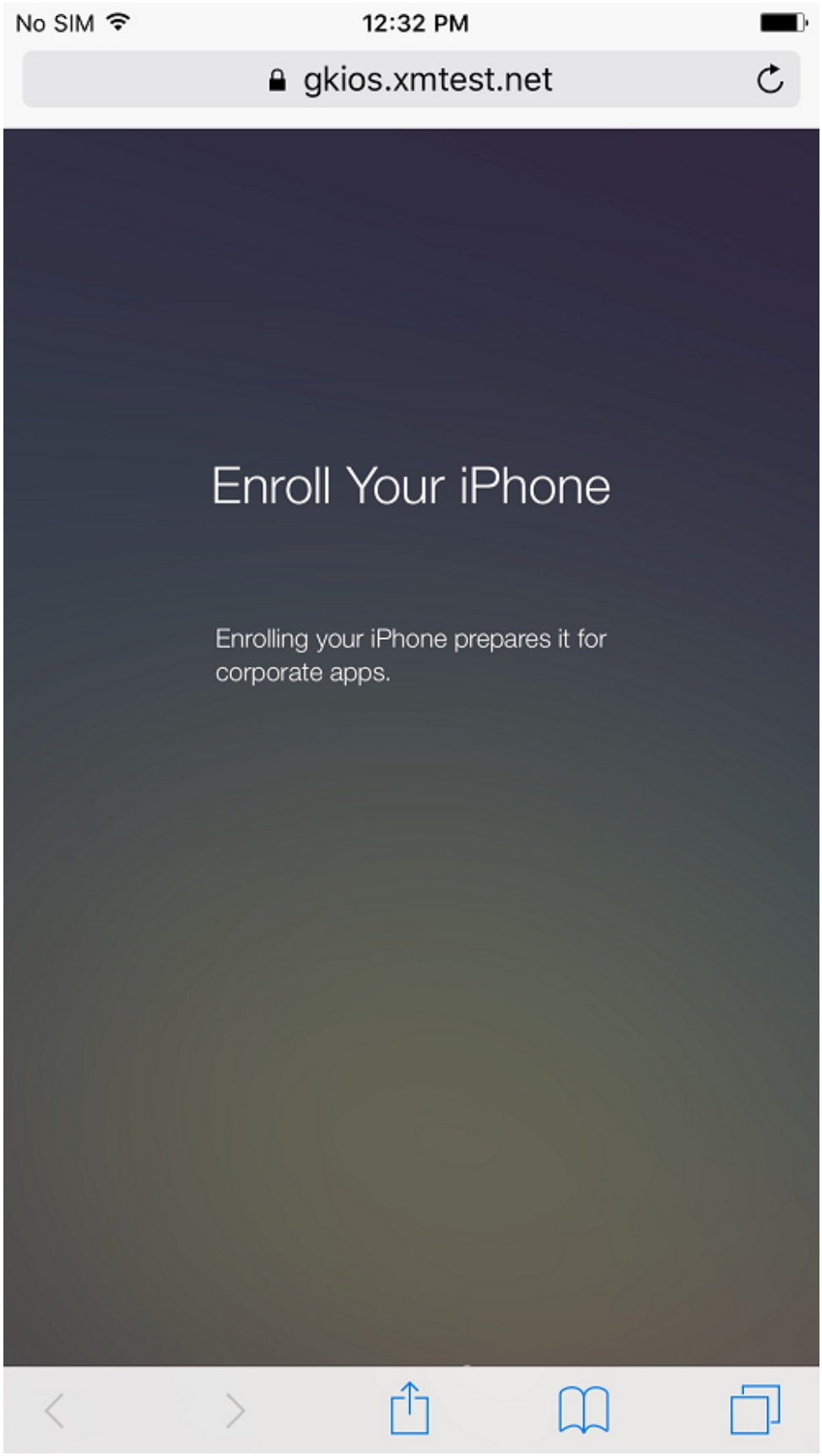
© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Os usuários fazem logon usando suas credenciais do AD do Azure.

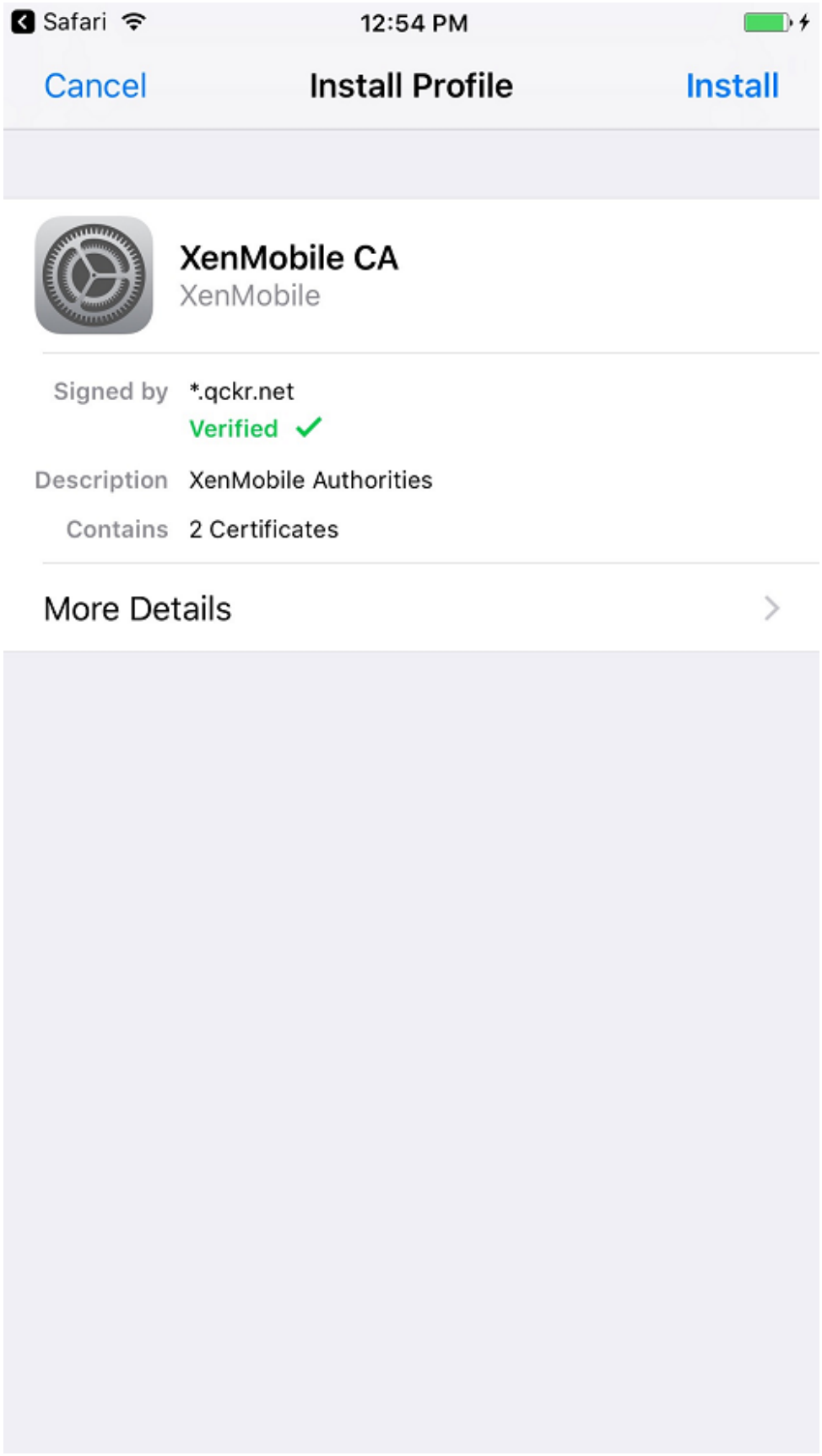
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Os usuários concluem as etapas de registro da mesma forma que qualquer outro registro por meio do Secure Hub.

> Nota:
>
> O XenMobile não dá suporte à autenticação por meio do AD do Azure a convites para registro. Se você enviar um convite para registro que contém uma URL de registro de usuários, os usuários se autenticarão por meio do LDAP em vez do AD do Azure.

Credenciais derivadas

April 15, 2019

As credenciais derivadas fornecem autenticação forte para dispositivos móveis. As credenciais, derivadas de um cartão inteligente, residem em um dispositivo móvel em vez do cartão. O cartão inteligente é um cartão de verificação de identidade pessoal (Personal Identity Verification - PIV).

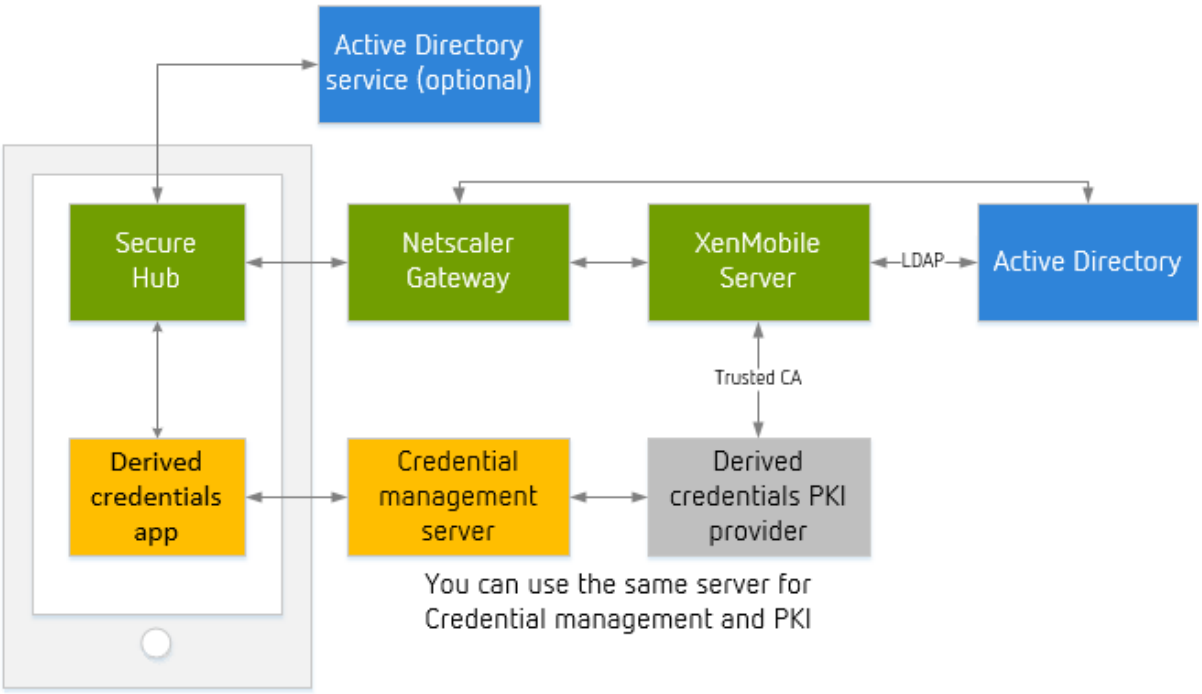
As credenciais derivadas são um certificado de registro que contém o identificador de usuário, como UPN. O XenMobile salva as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

O XenMobile pode usar credenciais derivadas para registro e autenticação do dispositivo. Se configurado para credenciais derivadas, o XenMobile não dá suporte a convites de registro ou outros modos de registro. A Citrix suporta o uso de um aplicativo de credenciais derivadas durante o registro do iOS.

Arquitetura

Para o registro, o XenMobile Server se conecta aos componentes, conforme mostrado no diagrama a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

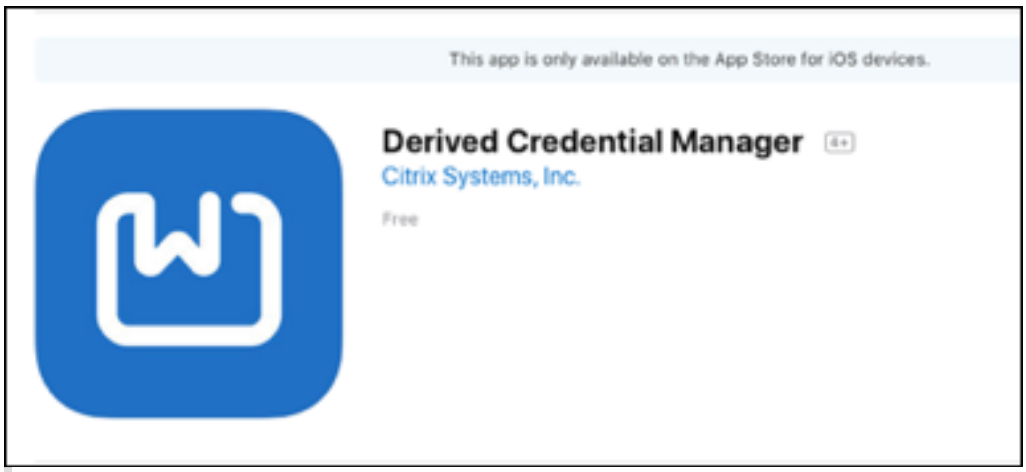


- Durante o registro de dispositivos, o Secure Hub obtém certificados do aplicativo de credenciais derivadas.
- O aplicativo de credenciais derivadas se comunica com o servidor de gerenciamento de credenciais durante o registro.
- Você pode usar o mesmo servidor ou um servidor diferente para o servidor de gerenciamento de credenciais e um provedor de PKI de terceiros.
- O XenMobile Server se conecta ao seu servidor de PKI de terceiros para obter certificados.

Requisitos

- Baixe e instale o Citrix Secure Hub.
- Com base na sua solução de credencial derivada, baixe e configure o aplicativo:
  - **Para Entrust Datacard:**
    * Baixe e instale o aplicativo Citrix Derived Credential Manager em seus dispositivos *antes* de se registrar no XenMobile. O aplicativo Derived Credentials Manager é o aplicativo provedor de identidade da Citrix. Segue o logotipo desse aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
> O aplicativo Citrix Derived Credential Manager suporta apenas novos registros. Os usuários do dispositivo devem se registrar novamente.

  * XenMobile Server versão 10.8 ou posterior.
  * O XenMobile Server deve ser configurado no modo Empresarial.
- **Para outros provedores de credenciais derivadas:** embora seja provável que a maioria das outras soluções de credenciais seja compatível com o XenMobile, teste a integração antes de colocá-la em produção.

- Deve ter o certificado raiz da autoridade que emite certificados ao servidor do Provedor de credenciais. Essa configuração permite que o XenMobile aceite os certificados assinados digitalmente durante o registro. Para obter informações sobre como adicionar certificados, consulte Certificados e autenticação.
  - Se o domínio de email de usuário for diferente do domínio LDAP, inclua o domínio de email na configuração **Alias de domínio**, em **Configurações > LDAP**. Por exemplo, se o domínio de endereços de email for `citrix.com` e o nome do domínio LDAP for `sample.com`, defina **Alias de domínio** como **`sample.com, citrix.com`**.
  - O XenMobile não suporta o uso de credenciais derivadas com dispositivos compartilhados.
- Certificados de identidade de usuário:
  - O nome de usuário no campo Nome de entidade alternativo deve ser formatado como o campo otherName, rfc822Name ou dNSName da extensão SubjectAltName. Não há suporte para outros campos. Para obter mais informações sobre o Nome de entidade alternativo, consulte a RFC, https://www.ietf.org/rfc/rfc5280.txt.
  - Não há suporte para o campo Entidade em Email ou CN.
- Citrix Gateway configurado para autenticação de certificado ou autenticação de certificado mais token de segurança

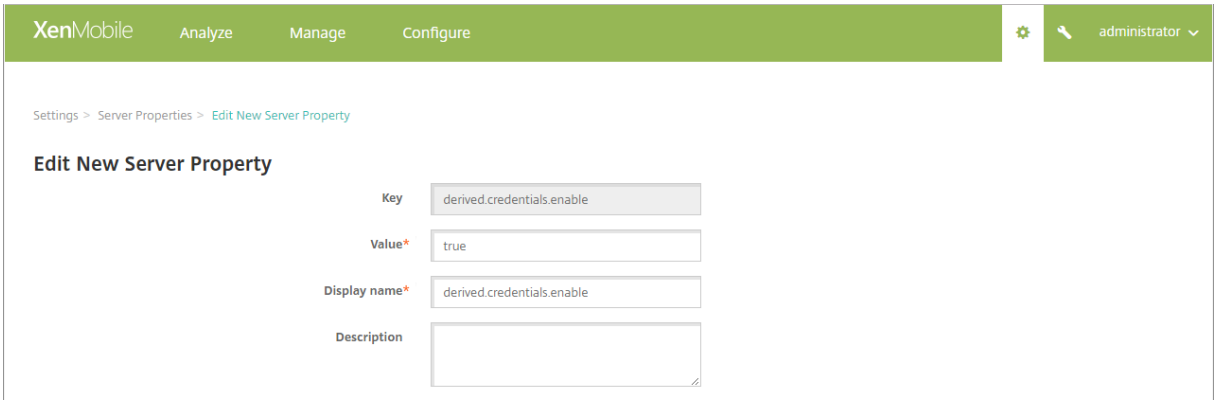
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ativar credenciais derivadas

Por padrão, o console XenMobile não inclui a página **Configurações > Credenciais derivadas**.

Para ativar a interface para credenciais derivadas:

- Vá até **Configurações > Propriedades do servidor**, adicione **derived.credentials.enable** como a propriedade de servidor e defina o valor da propriedade como **true**.



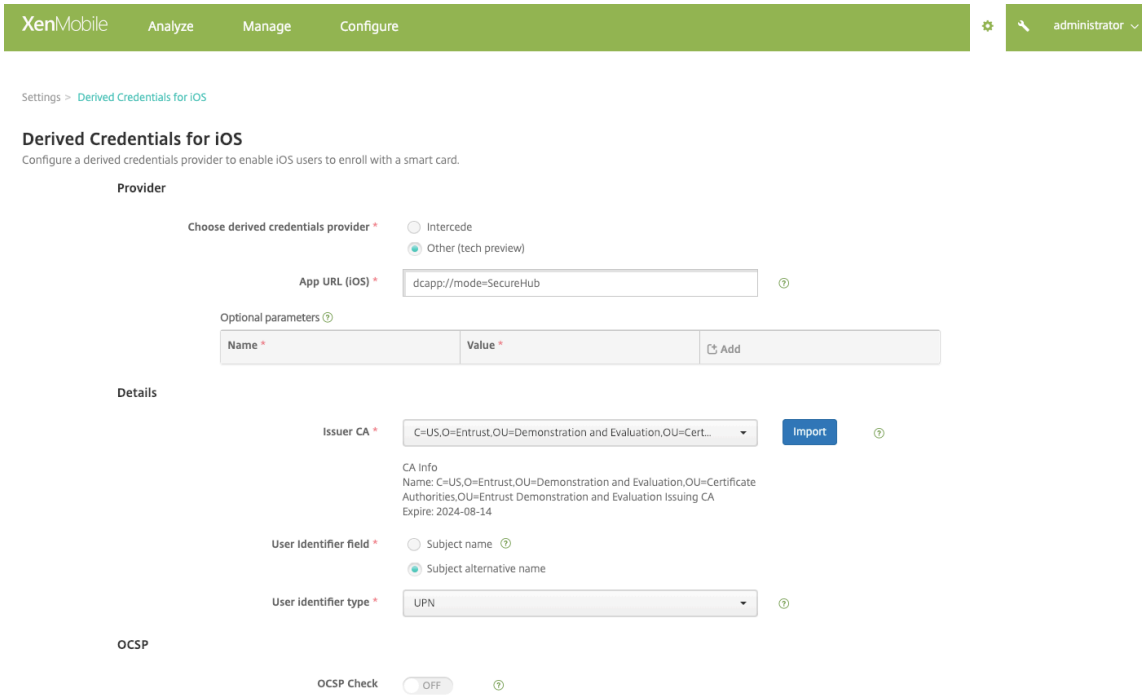
Configurar credenciais derivadas

Parte-se do pressuposto que você tenha uma configuração funcional para o provedor de credenciais derivadas que planeja integrar com o XenMobile. Você poderá configurar o XenMobile para se comunicar com esse servidor. Você também pode escolher um certificado de CA de credenciais derivadas já adicionado ao XenMobile ou importar o certificado.

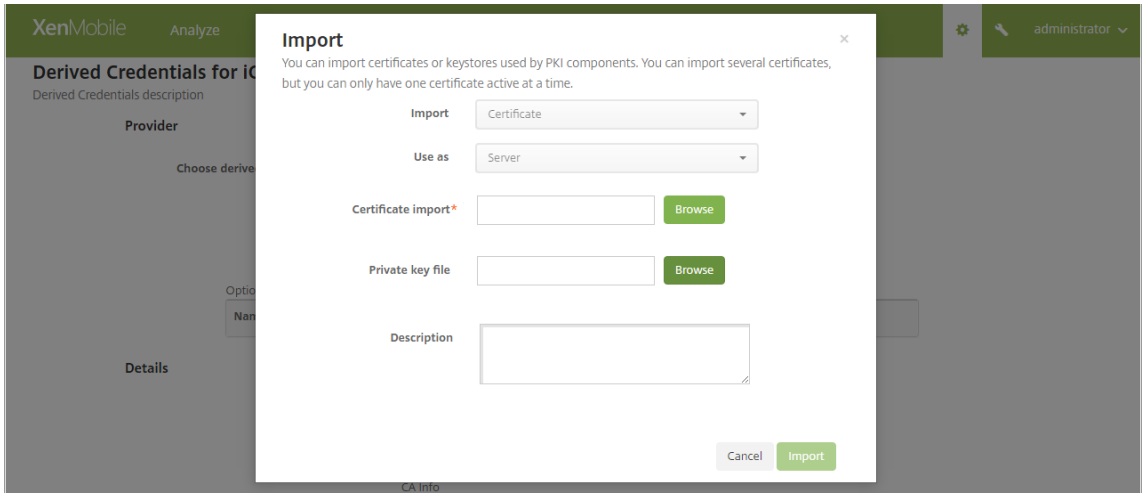
É possível ativar o suporte ao protocolo OCSP para esse certificado de CA. Para obter mais informações sobre o protocolo OCSP, consulte “CAs discricionárias”, em Entidades PKI.

1. No console XenMobile, vá até **Configurações > Credenciais derivadas para iOS**.
2. Em **Escolher o provedor de credenciais derivadas**, escolha **Outro** para Entrust Datacard. Digite `dcapp://mode=SecureHub` em **URL de aplicativo (iOS)**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. **Parâmetros opcionais:** alguns provedores de credenciais derivadas podem exigir que você forneça parâmetros para a conexão. Por exemplo, um fornecedor pode exigir que você especifique as URLs de um servidor back-end. Clique em **Adicionar** para fornecer parâmetros.
4. Especifique um certificado para credenciais derivadas: se o certificado já estiver carregado no XenMobile, escolha-o em **AC emissora**. Caso contrário, clique em **Importar** para adicionar um certificado. A caixa de diálogo **Importar certificado** é exibida.
5. Na caixa de diálogo **Importar certificado**, clique em **Procurar** para navegar até o certificado. Em seguida, clique em **Procurar** para navegar até o arquivo de chave privada.

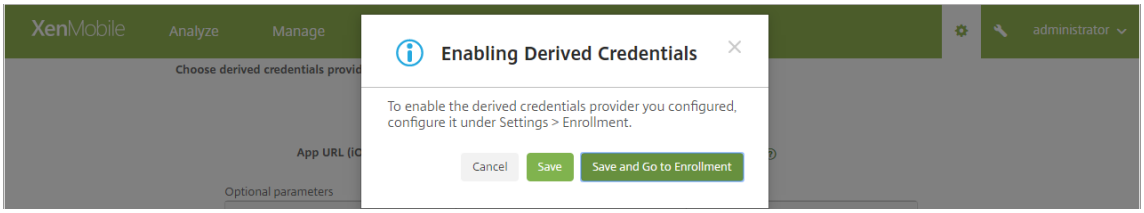


6. Defina as configurações.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

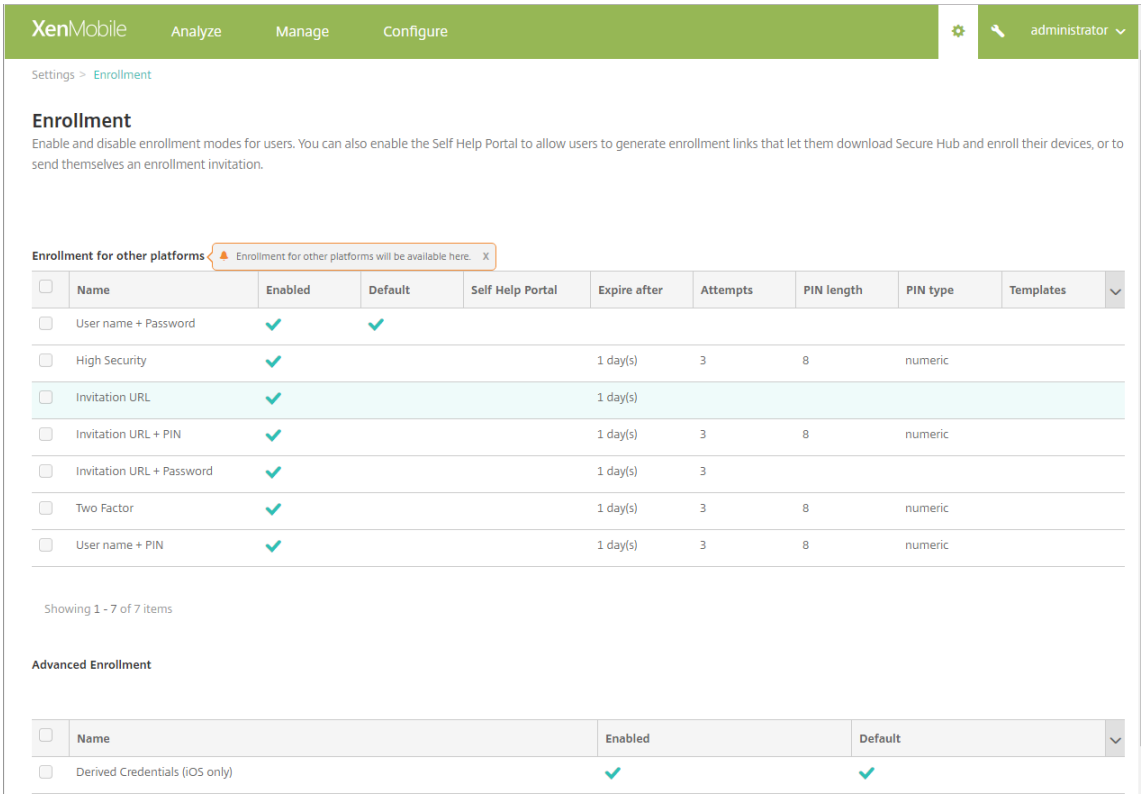
- No aplicativo Citrix Derived Credentials Manager: o **Campo de identificador do usuário** é o **Nome de entidade alternativo**, e o **Tipo de identificador do usuário** é **userPrincipalName**.
- Entre em contato com outros provedores de credenciais derivadas para obter suas informações.

7. Você tem a opção de usar um respondedor OCSP para verificação da revogação de certificados. A Citrix recomenda o uso de um respondedor OCSP para fins de segurança. Por padrão, a verificação OSP é **Desativado**.
   - Se você ativar o suporte OCSP para o certificado de CA, escolha uma opção para **Use o URL de OCSP personalizada**. Por padrão, o XenMobile extrai a URL OCSP do certificado (a opção **Usar definição de certificado para revogação**). Para especificar uma URL de respondedor, clique em **Usar definido pelo usuário** e digite a URL.
   - **AC respondedora:** em **AC respondedora**, escolha um certificado. Ou clique em **Importar** e use a caixa de diálogo **Importar certificado** para localizar o certificado.
8. Clique em **Salvar**. A caixa de diálogo **Ativação de credenciais derivadas** é exibida.

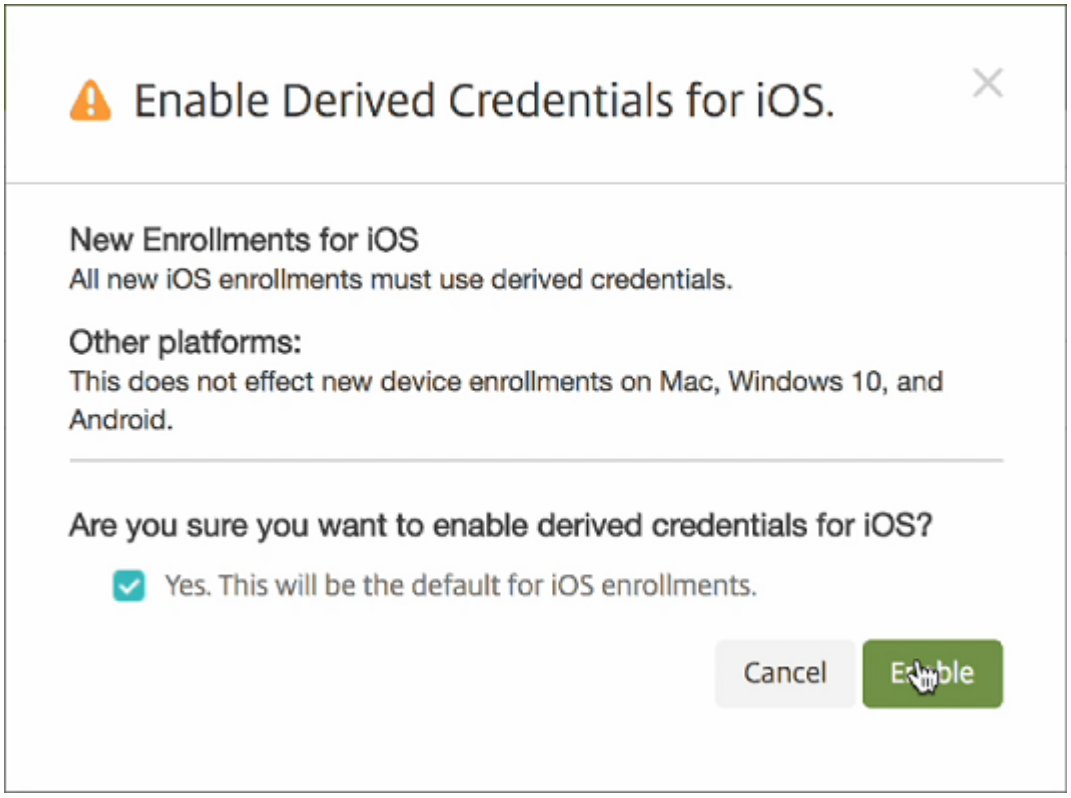


   - Para ativar a configuração de credenciais derivadas, clique em **Salvar**. Para usar credenciais derivadas, você também deve definir as configurações de registro.
   - Para ativar a configuração de credenciais derivadas e ir imediatamente para **Configurações > Registro**, clique em **Salvar e Ir para Registro**.
9. Para ativar credenciais derivadas para registro: na página **Configurações > Registro**, em **Registro avançado**, selecione **Credenciais derivadas** (apenas iOS) e clique em **Ativar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



10. Uma caixa de diálogo de confirmação é exibida. Para ativar credenciais derivadas, marque a caixa de seleção e clique em **Ativar**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

11. Para editar opções de registro de credenciais derivadas, acesse **Configurações > Registro**, selecione **Credenciais derivadas (apenas iOS)** e clique em **Editar**.

Depois que você ativar credenciais derivadas, no relatório **Registro de dispositivos**, a coluna **Modo de registro** mostrará **derived_credentials**.

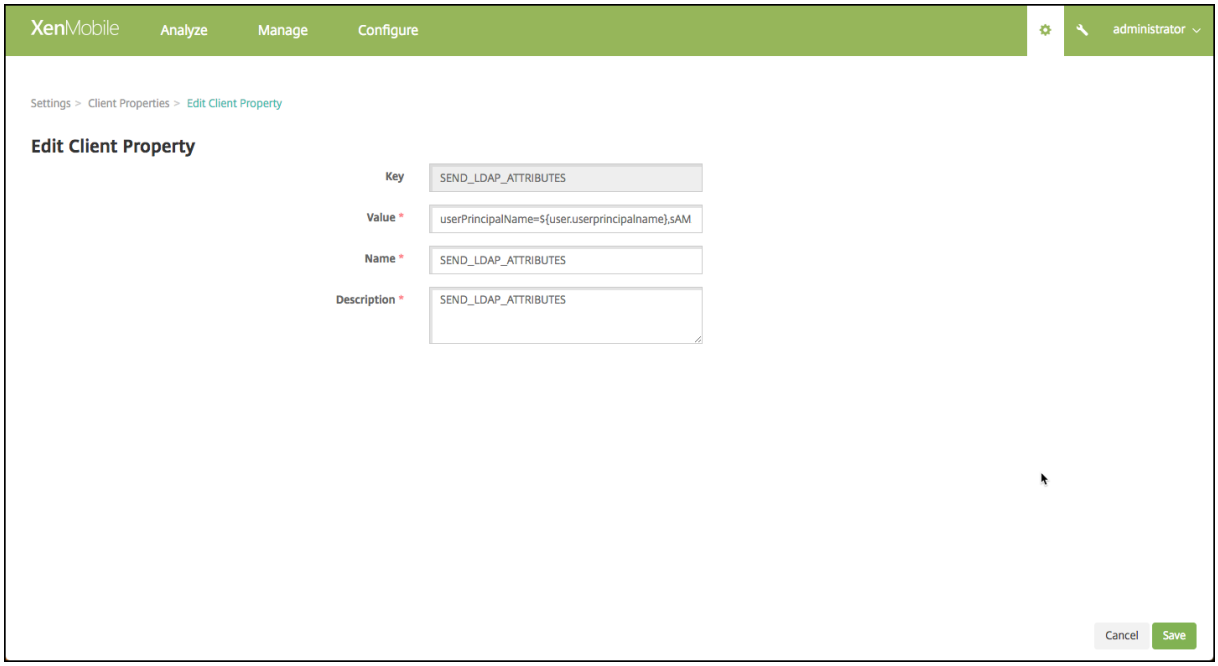
> **Importante:**
>
> Depois de adicionar o provedor de credenciais derivadas, reinicie o XenMobile Server.

Configurar o XenMobile Server para Secure Mail

Para que o Secure Mail funcione com credenciais derivadas, adicione a propriedade do cliente LDAP Attributes. Para obter informações sobre como adicionar uma propriedade de cliente, consulte Propriedades do cliente.

Use as seguintes informações para a propriedade do cliente:

- **Chave:** `SEND_LDAP_ATTRIBUTES`
- **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



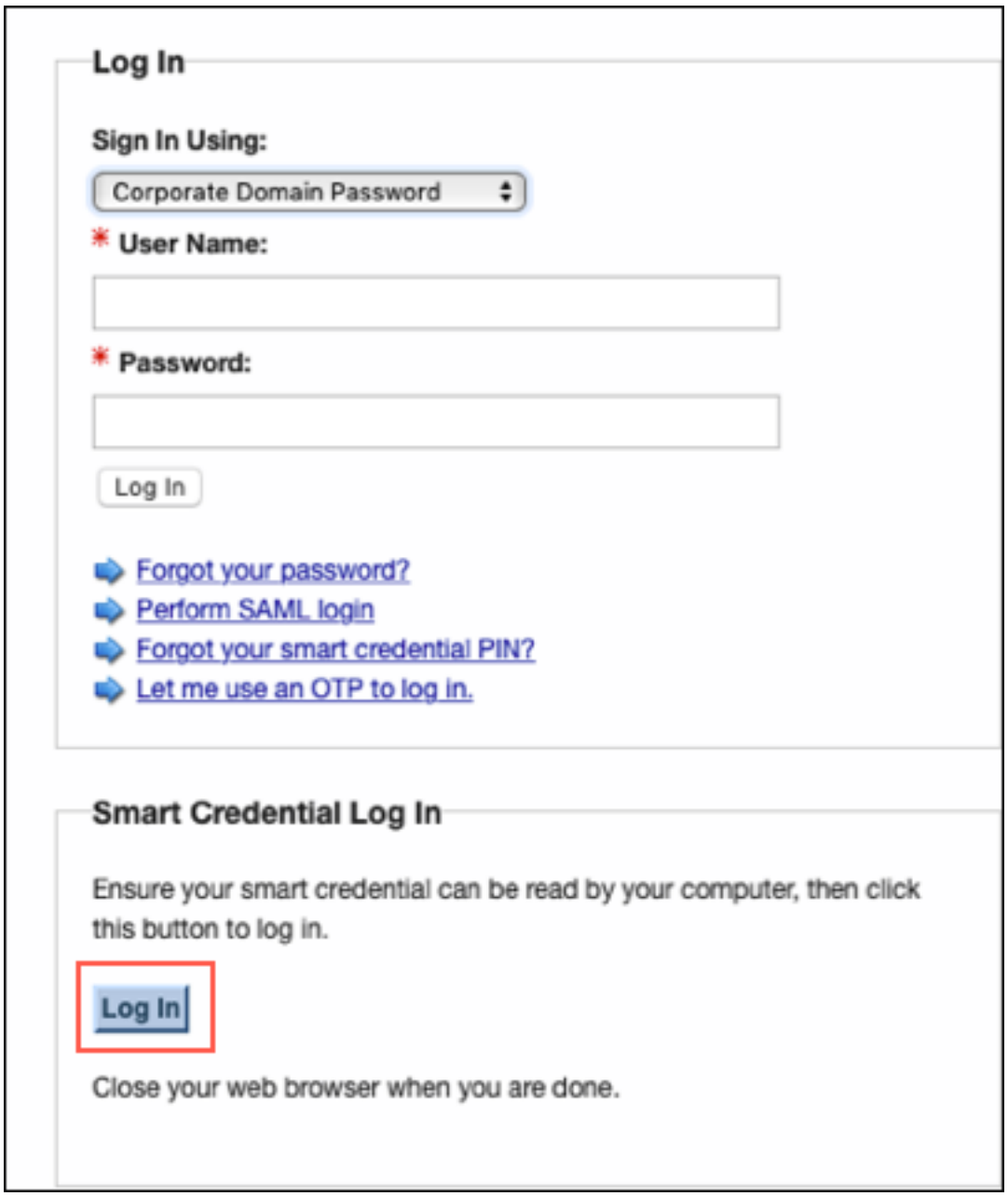
Ativação de credenciais derivadas do Entrust Datacard em dispositivos iOS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Ao utilizar o site da Entrust:
>
> - Certifique-se de que o navegador Internet Explorer esteja habilitado para Java quando você programar o cartão PIV.
> - Limpe o cache do navegador quando trocar de cartão PIV.

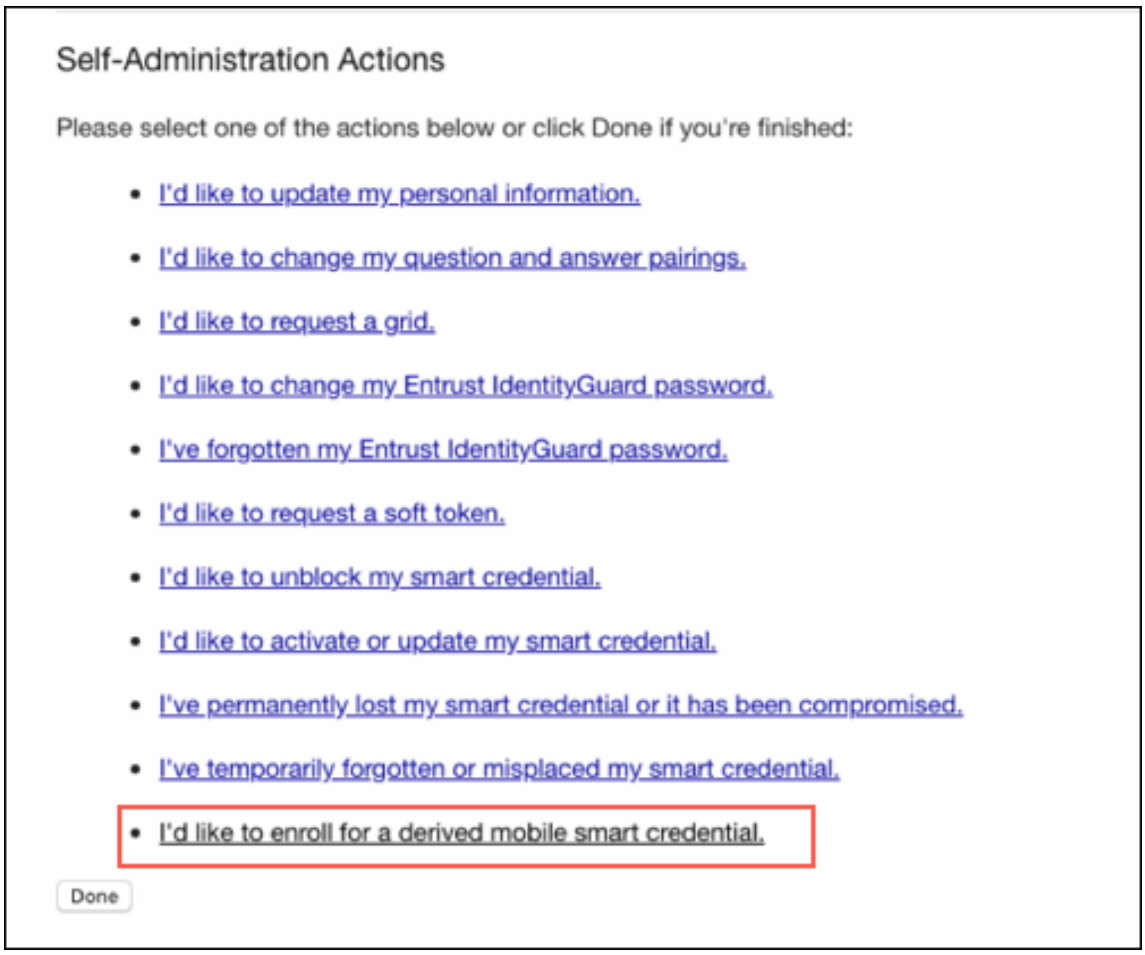
1. Para solicitar novas credenciais inteligentes, utilize um computador ou outro dispositivo para iniciar uma sessão no site da Entrust. Faça login usando o botão em **Smart Credential Log In**, na parte inferior da página. Os usuários inserem o cartão inteligente em um leitor acoplado ao computador.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

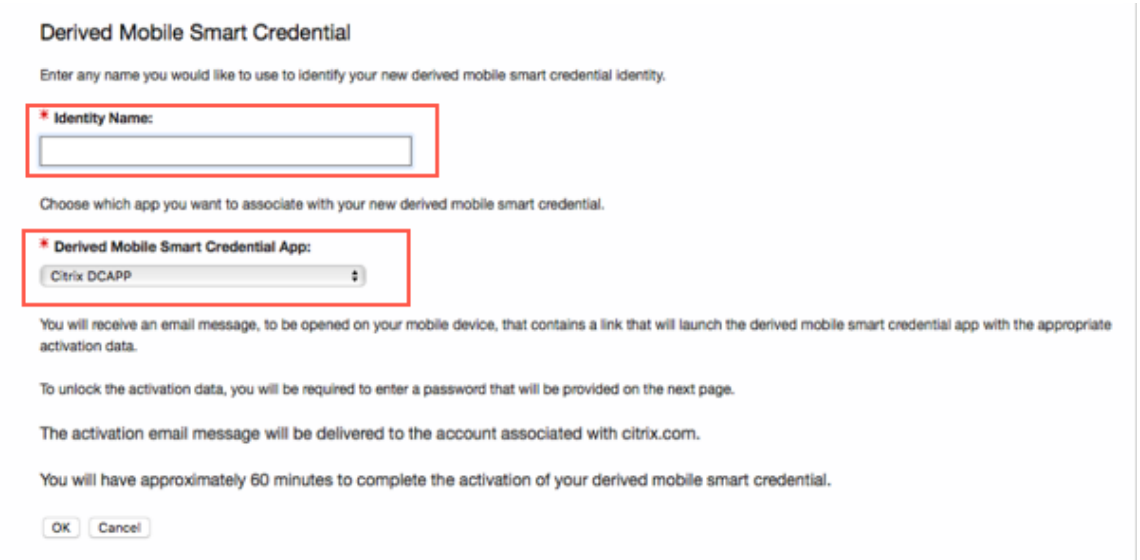


2. Em **Self-Administration Actions**, selecione **I'd like to enroll for a derived mobile smart credential** e clique em **Done**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Na tela **Derived Mobile Smart Credential**, forneça o nome de identidade em **Identity Name**. O usuário pode escolher um nome exclusivo, como um nome de usuário ou números de ID.
4. Selecione **Citrix DCAPP** no menu aplicativo de credenciais derivadas e clique em **Ok**.

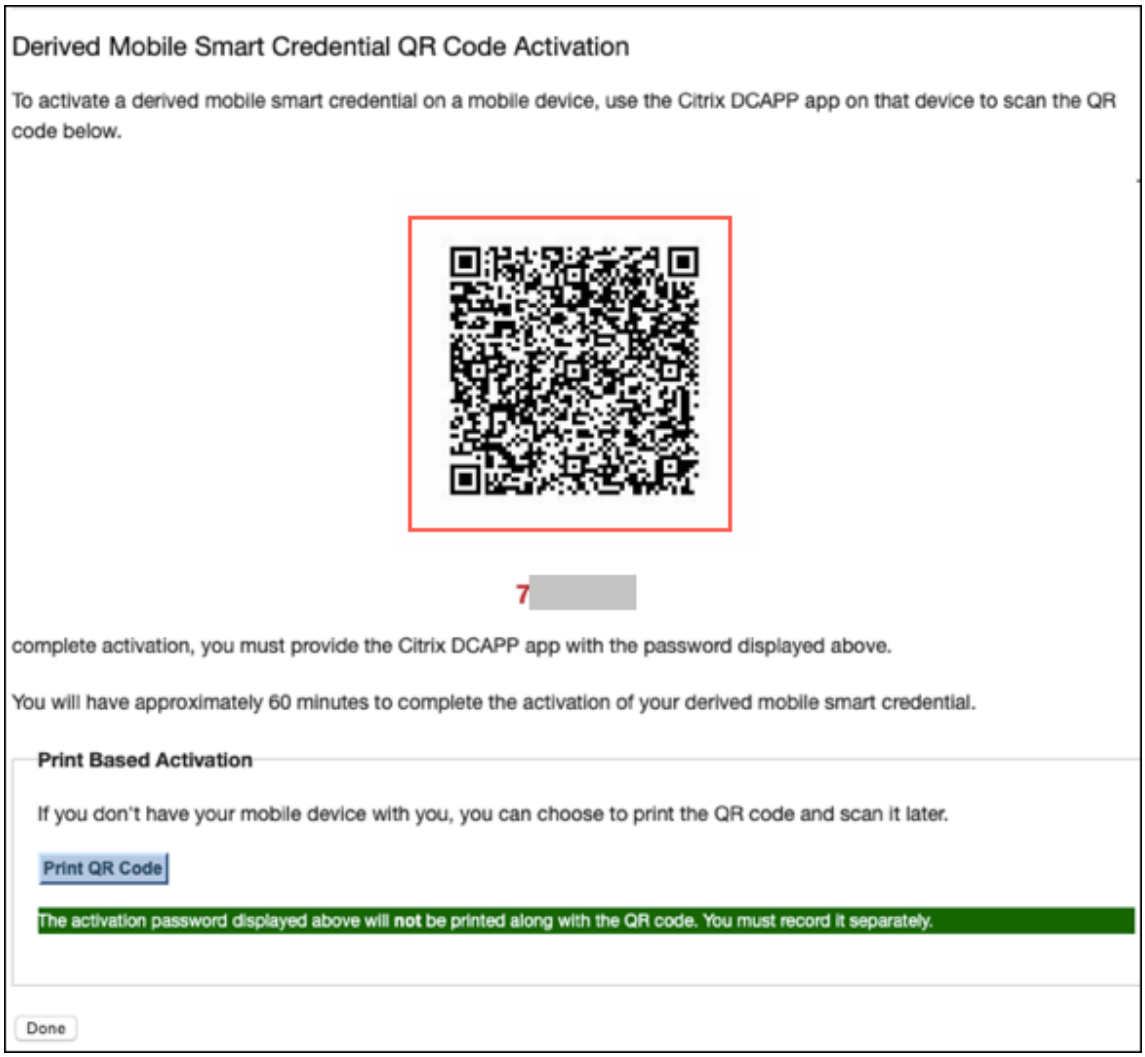


© 1999-2019 Citrix Systems, Inc. All rights reserved.

A tela de ativação de código QR aparece e solicita ao usuário que escaneie o código com o dispositivo móvel.

> Nota:
>
> Por padrão, o código QR de credenciais derivadas expira em 3 minutos.

5. Escaneie o código QR usando o aplicativo **Derived Credential Manager** no dispositivo para concluir a ativação.



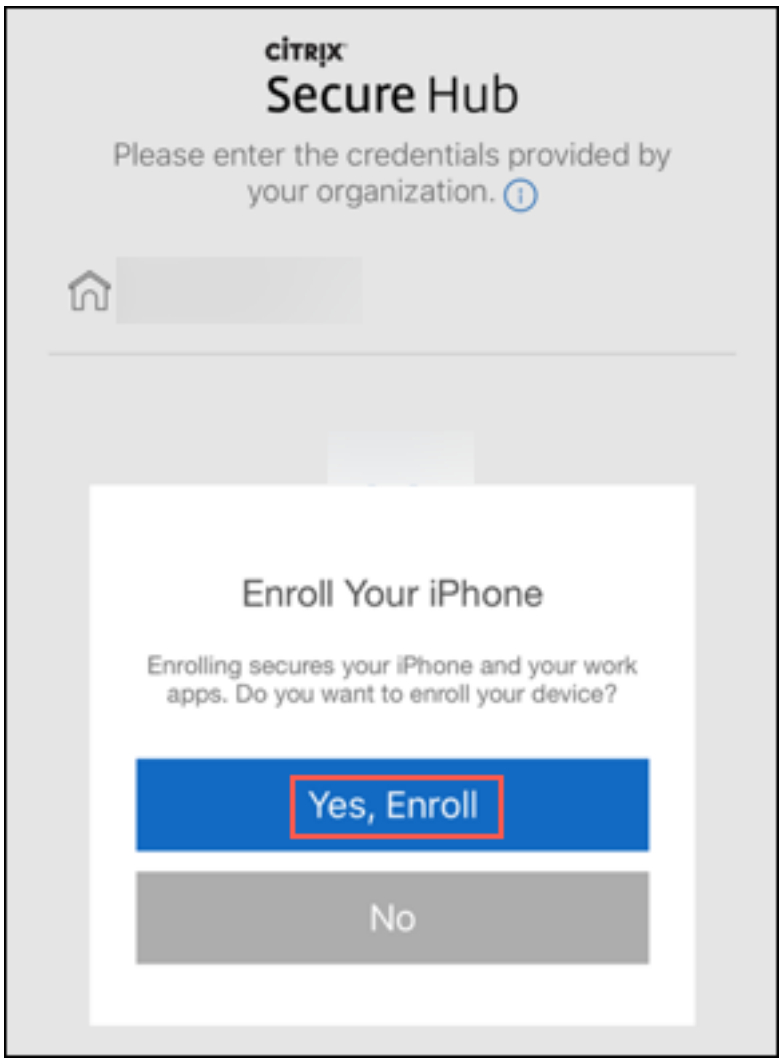
Registro do dispositivo

Depois de concluir a instalação descrita anteriormente neste artigo, os usuários podem registrar seus dispositivos usando credenciais derivadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> As capturas de tela desta seção usam o Entrust Datacard como exemplo.

1. Toque para abrir o **Secure Hub**. Quando solicitado, digite o nome de domínio totalmente qualificado do XenMobile Server e clique em **Avançar**.
2. Clique em **Sim, registrar**. O registro do dispositivo no Secure Hub é iniciado.



Se o XenMobile Server oferecer suporte a credenciais derivadas, o Secure Hub solicita ao usuário que crie e confirme o PIN da Citrix.

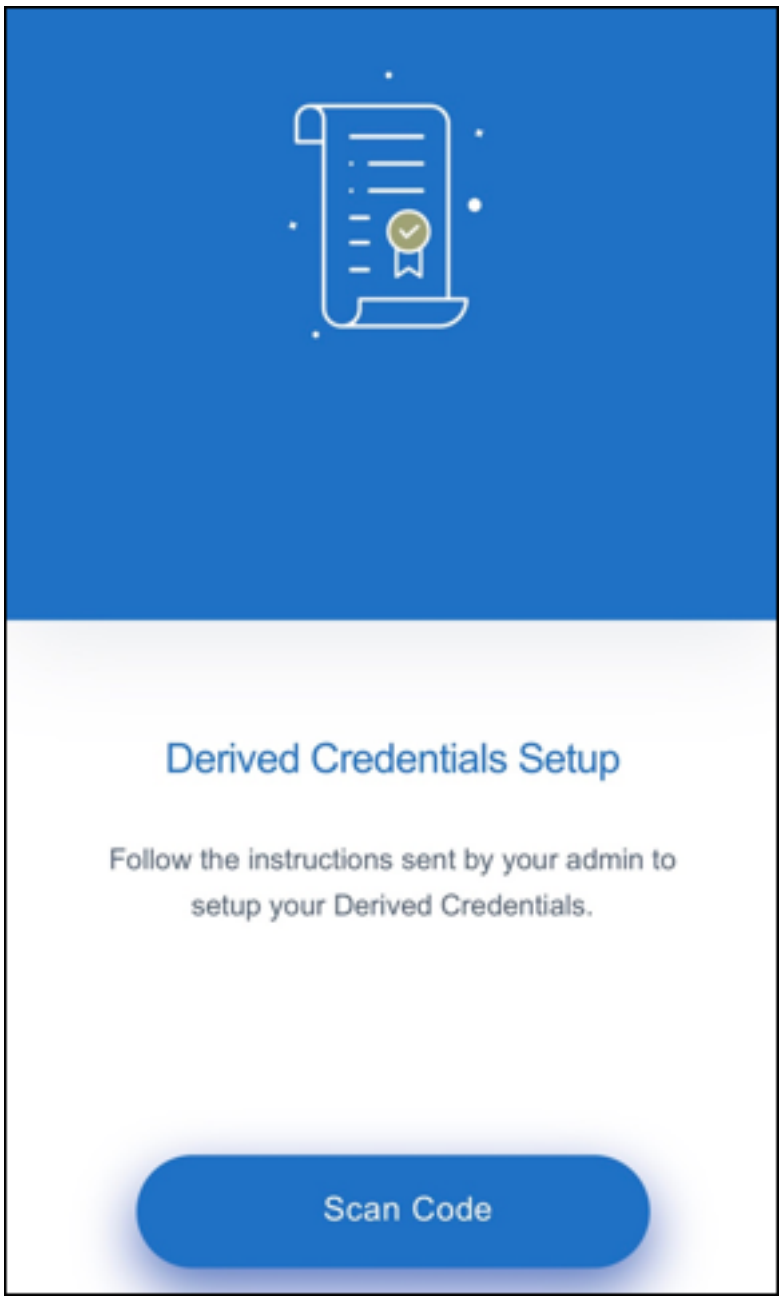
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Depois de confirmar o PIN da Citrix, aparece a tela de abertura de configuração de Credenciais Derivadas. Siga as instruções para ativar as credenciais inteligentes.

3. Toque em **Escanear código**. A câmera do telefone celular é ativada.

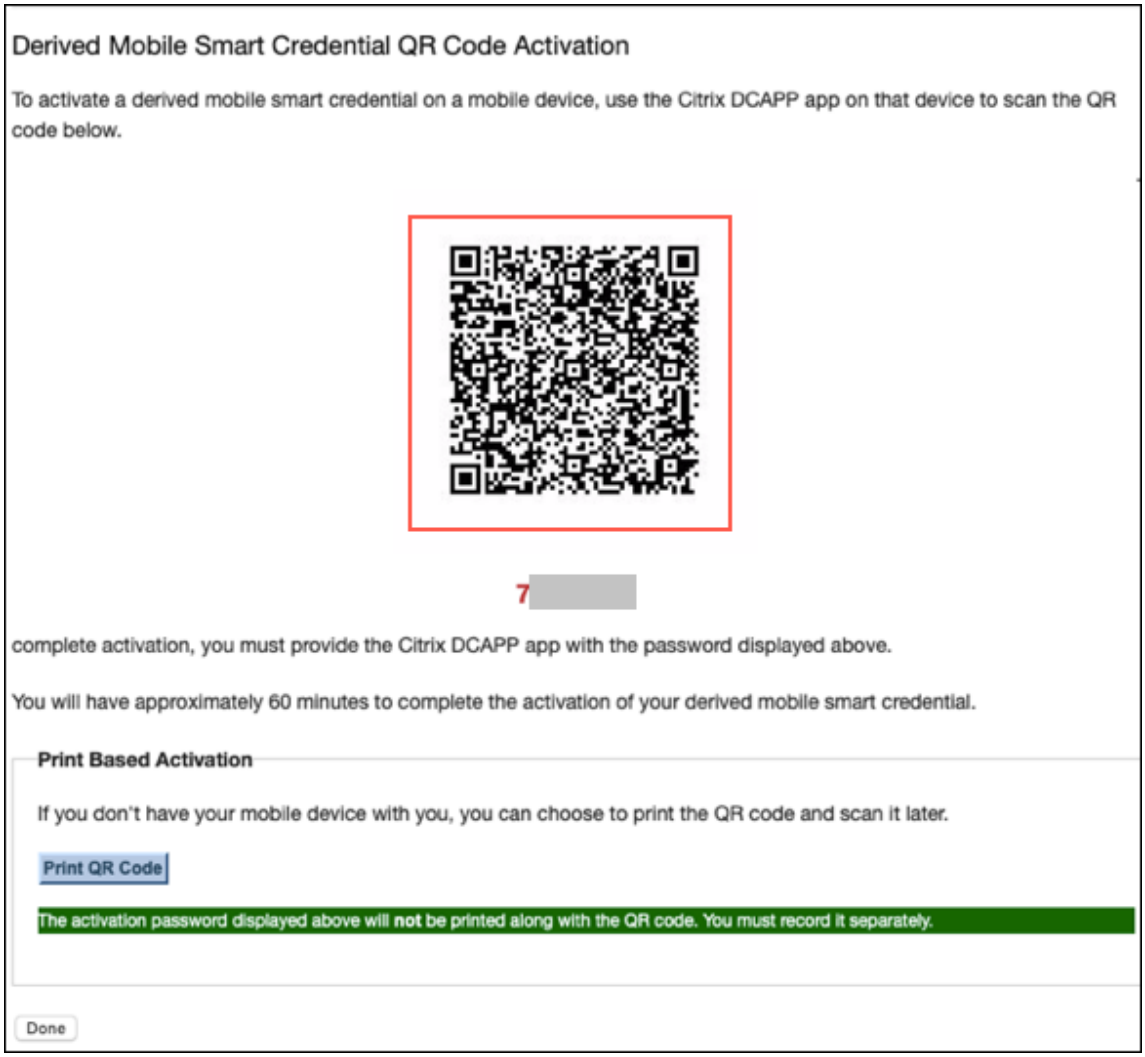
© 1999-2019 Citrix Systems, Inc. All rights reserved.



> **Nota:**
>
> Para escanear o código QR, certifique-se de que sua câmera e microfone estão ativados e têm as permissões de acesso necessárias.

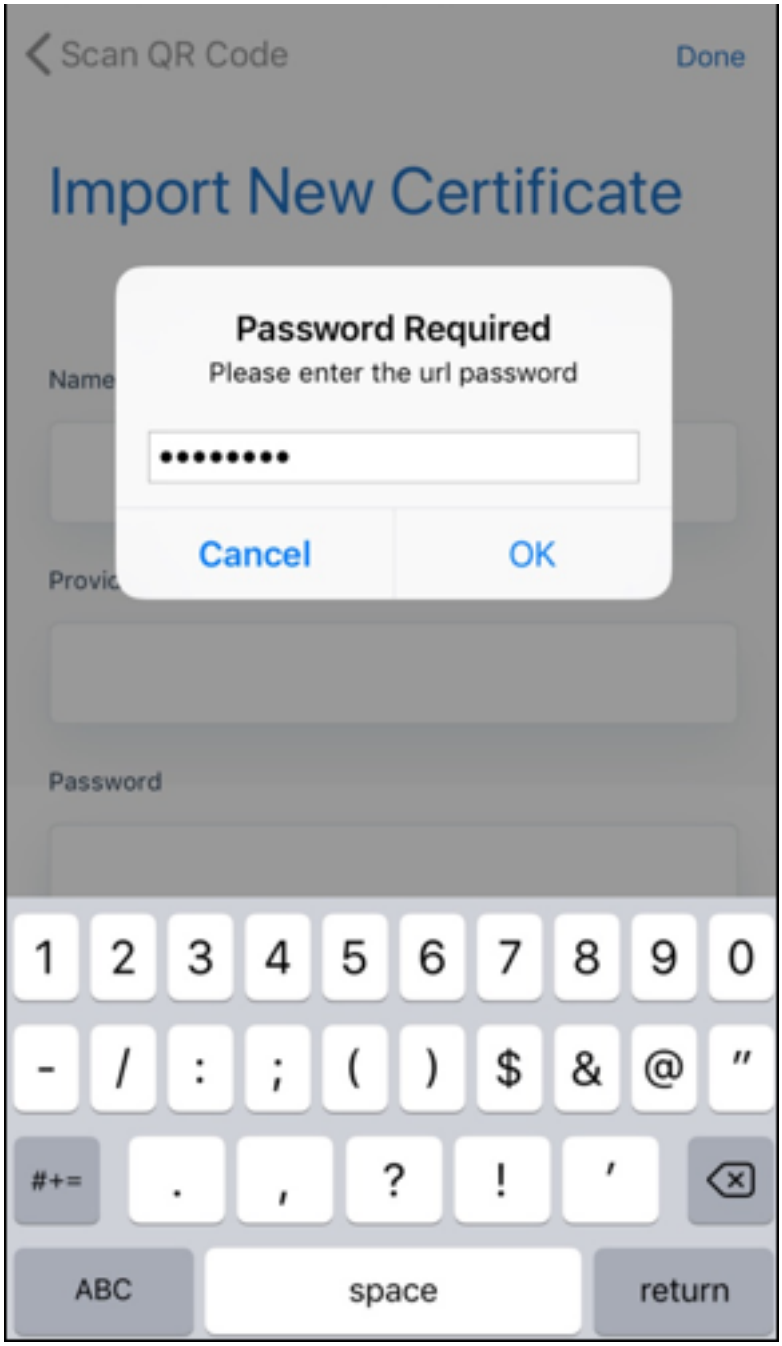
4. No aplicativo de credenciais derivadas, escaneie o código QR que foi criado em etapas anteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



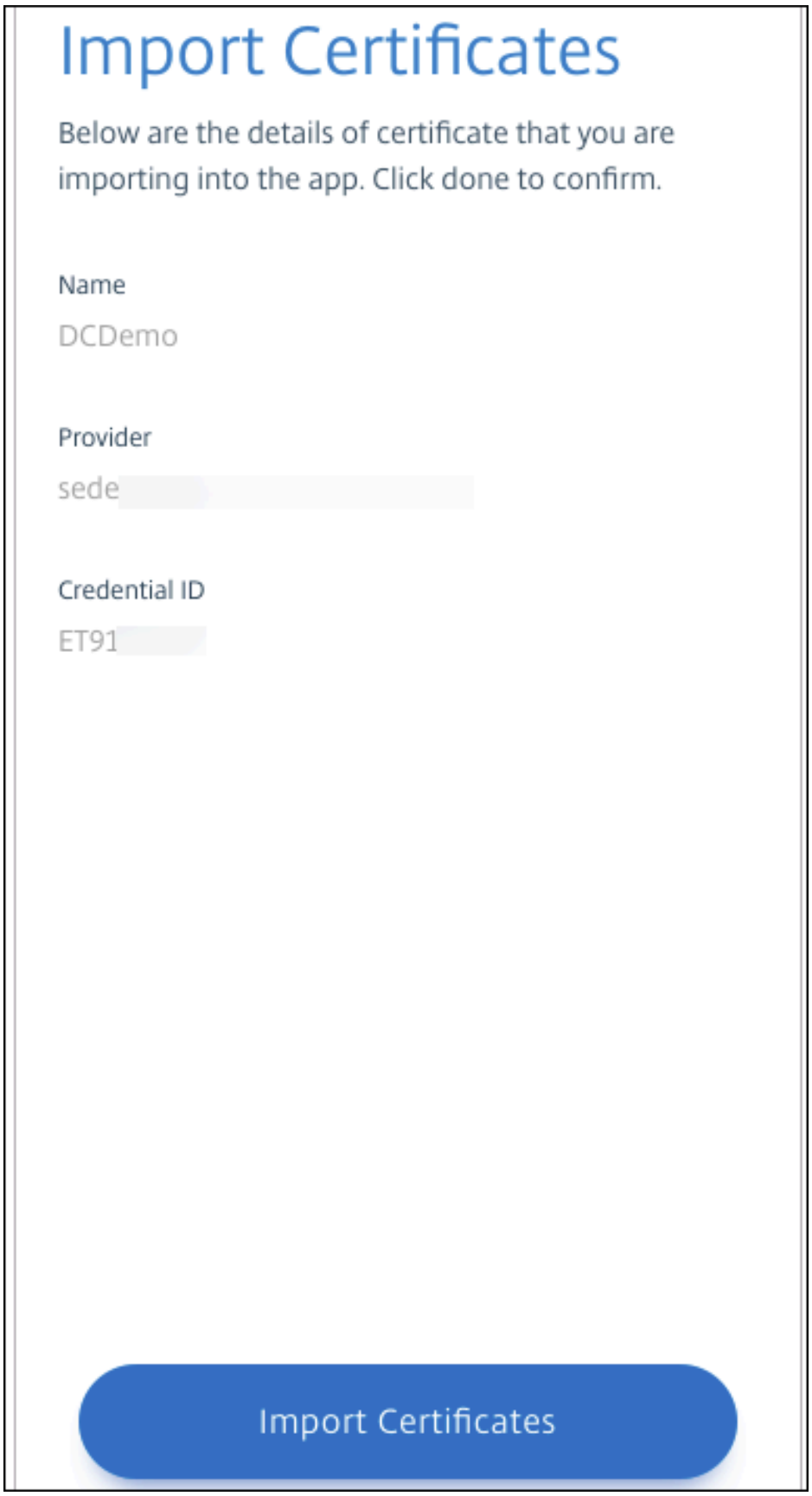
5. Depois de escanear o código QR, na tela **Importar novo certificado** aparece uma caixa de diálogo de senha: digite a senha e clique em **OK**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A tela **Importar novo certificado** é exibida com os campos preenchidos automaticamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Depois que os certificados forem adicionados com êxito, na tela de **Credenciais derivadas**, clique em **Continue to Secure Hub**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. No Secure Hub, insira um novo PIN quando solicitado.

   Depois de autenticar o PIN, o Secure Hub baixa os certificados. Siga os prompts para concluir o registro.

Para exibir informações do dispositivo no console XenMobile:

- Vá para **Gerenciar** > **Dispositivos** e selecione um dispositivo para exibir uma caixa de comando. Clique em **Mostrar mais**.
- Vá para **Analisar** > **Painel**.

Atualização

April 15, 2019

> Importante:
>
> **Antes de atualizar para o XenMobile 10.9:**
>
> 1. Atualize o seu Citrix License Server para 11.15 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.9.
>   A versão mais recente do XenMobile exige o Citrix License Server 11.15 (versão mínima).
>   Nota: Esteja ciente de que a data de Subscription Advantage (SA) no XenMobile 10.9 é 14 de setembro de 2018. A data de Subscription Advantage (SA) em sua licença Citrix deve ser posterior a essa data. Você pode ver sua data de SA ao lado da licença do 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 as em sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte https://support.citrix.com/article/CTX209580.
> 2. Para um ambiente em cluster: as implantações de aplicativos e políticas do iOS para dispositivos que executam o iOS 11 e posterior têm o seguinte requisito. Se o NetScaler Gateway estiver configurado para persistência de SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
> 3. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a quantidade mínima de RAM recomendada é de 8 GB para ambientes de produção.
> 4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Depois de atualizar para o XenMobile 10.9:**
>
> Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: "Não é possível se conectar ao servidor VPP: o nome do host '192.0.2.0' não corresponde à entidade 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. Como padrão, a verificação do nome do host está ativada nas 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**.

A Citrix publica novas versões ou atualizações importantes do XenMobile no site Citrix.com. Ao mesmo tempo, uma notificação é enviada ao contato registrado para cada cliente.

Você pode atualizar diretamente do XenMobile 10.7.x ou 10.8.x para o XenMobile 10.9 Para executar a atualização, use o binário 10.9 mais recente disponível na página de Download da Citrix. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Gerenciamento de Versão**.

Para atualizar do XenMobile 10.6 para o 10.9, primeiro atualize do XenMobile 10.6 para o 10.7 ou 10.8 e, em seguida, atualize para o 10.9.

Para atualizar de versões mais antigas do XenMobile, consulte o artigo sobre Atualização no PDF do XenMobile Server 10.8.

> Dica: Serviço de migração do XenMobile
>
> Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.
>
> Para obter mais informações, entre em contato com o pessoal de vendas local da Citrix, com um engenheiro de sistemas ou com um parceiro Citrix. Estes blogs discutem o Serviço de Migração do XenMobile:
>
> Novo serviço de migração do XenMobile
>
> Criando o cenário para o XenMobile na Nuvem

Este artigo descreve como usar a página **Gerenciamento de versão**, atualizar implantações do XenMobile em cluster e atualizar do MDM para o Enterprise Edition.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para atualizar usando a página Gerenciamento de versão

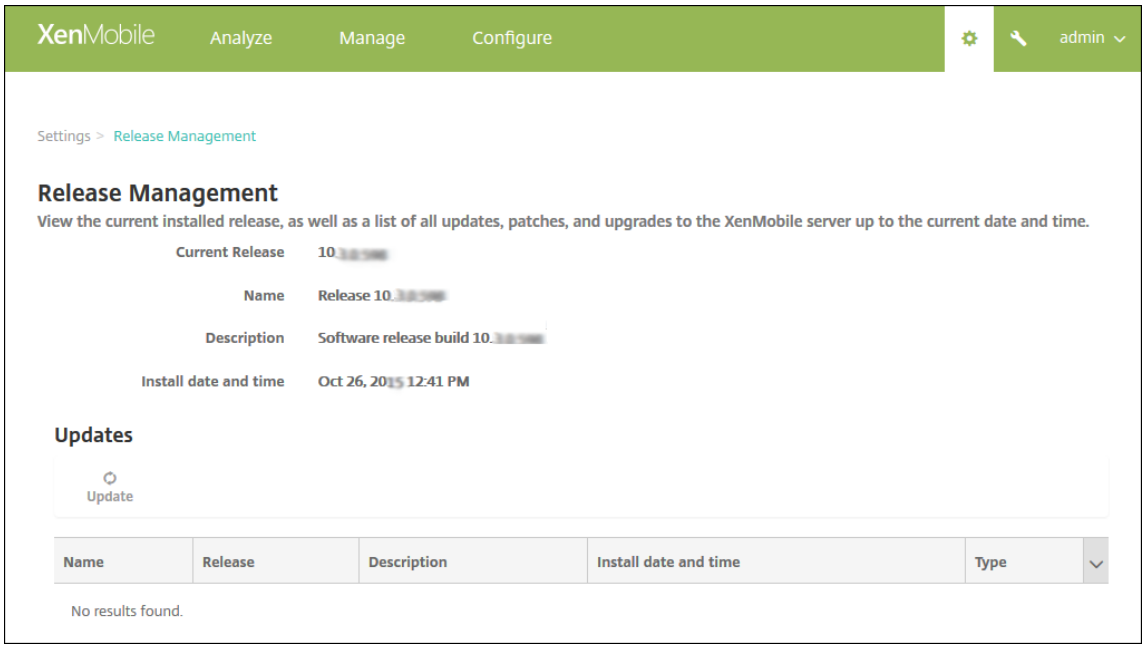
Use a página **Gerenciamento de versão** para atualizar do XenMobile 10.7.x ou 10.6.x para a versão mais recente do XenMobile Server.

Pré-requisitos:

- Leia os Requisitos do sistema.

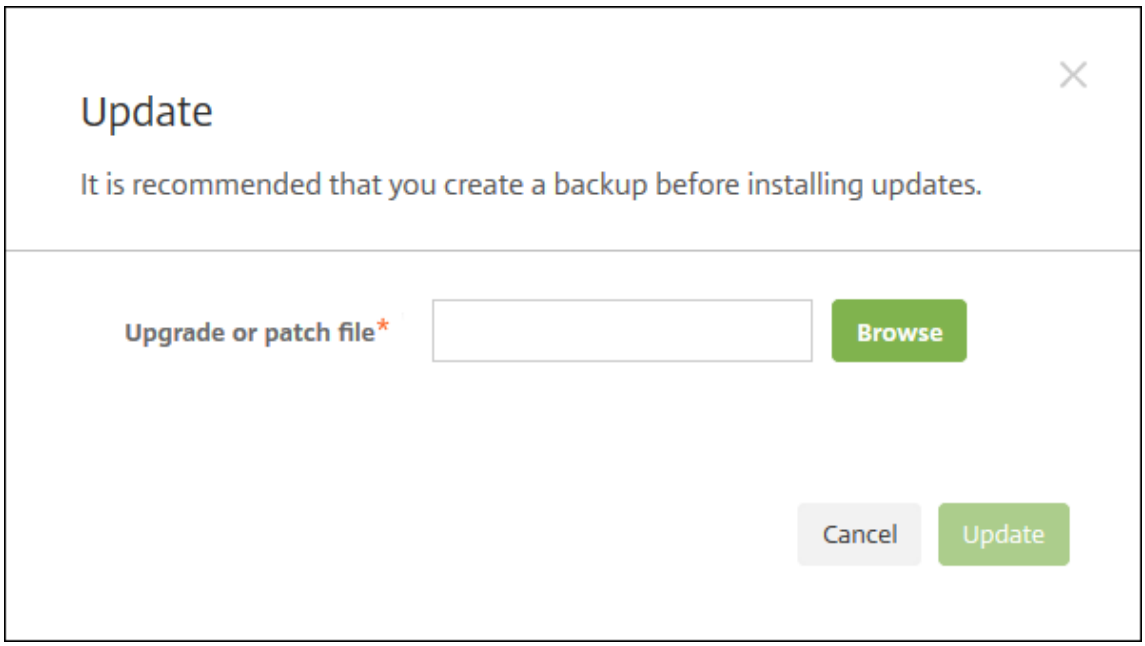
Se você tem uma implantação em cluster, consulte as instruções no final deste artigo.

1. Faça logon na sua conta no site da Citrix e vá para a página de Download. Baixe o arquivo de atualização do XenMobile (.bin) para uma localização apropriada.
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
3. Clique em **Gerenciamento de versão**. A página **Gerenciamento de Versão** é exibida.



4. Em **Atualizações**, clique em **Atualizar**. A caixa de diálogo **Atualizar** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Selecione o arquivo de atualização do XenMobile que você baixou do site Citrix.com clicando em **Procurar** e navegando até a localização do arquivo.
6. Clique em **Atualizar** e, se solicitado, reinicie o XenMobile.

   Se por algum motivo a atualização não puder ser concluída com sucesso, uma mensagem de erro será exibida indicando o problema. O sistema é revertido ao estado anterior à tentativa de atualização.

   > Nota:
   >
   > Após uma atualização, o XenMobile exige a reinicialização. Use a interface de linha de comando do XenMobile para reiniciar o XenMobile Server. É importante que você limpe o cache do navegador depois que o sistema for reiniciado.

Para atualizar implantações XenMobile em cluster

> Importante:
>
> Antes de instalar uma atualização do XenMobile, use a funcionalidade na 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 tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Se o seu sistema estiver configurado no modo de cluster, siga estas etapas para atualizar cada nó de uma versão do XenMobile 10:

1. Carregue o arquivo .bin em todos os nós, acessando **Configurações > Gerenciamento de versão**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Desligue todos os nós no **Menu Sistema** na interface de linha de comando.
3. Ative um único nó, no **Menu Sistema** na interface de linha de comando e verifique se o serviço está em execução.
4. Abra os outros nós, um após o outro.

   Se o XenMobile não conseguir concluir a atualização com sucesso, uma mensagem de erro será exibida indicando o problema. O XenMobile reverte o sistema ao seu estado anterior à tentativa de atualização.

Atualize do XenMobile 10.8 MDM Edition para Enterprise Edition

Você pode atualizar do XenMobile 10.8 MDM Edition para o XenMobile 10.8 Enterprise Edition para dispositivos iOS e Android.

Pré-requisitos

- A licença Enterprise correta.
- O NetScaler Gateway está configurado.

Para atualizar

1. Vá para **Configurações > Licenciamento** e verifique se o tipo de licença Enterprise Edition correto está carregado.
2. Vá para **Configurações > Propriedades do Servidor** e mude a propriedade do **Modo Servidor** de **MDM** para **ENT**.
3. Vá para **Configurações > NetScaler Gateway** e configure os detalhes do NetScaler Gateway. Defina o modo de autenticação para o mesmo que o MDM Edition, ou seja, a autenticação de domínio (Active Directory). O XenMobile não dá suporte à alteração para o modo de autenticação após o registro de usuário.
4. Opcional: vá para **Configurações > Propriedades do Cliente** e habilite a autenticação do PIN da Citrix.

Depois de concluir essas etapas, os usuários devem executar as seguintes etapas para alternar um dispositivo para o modo Enterprise.

Usuários do iOS

1. Fechar o Secure Hub: toque no botão de página inicial do dispositivo duas vezes (rapidamente) e deslize no aplicativo Secure Hub.
2. Abra o Secure Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usuários do Android

1. Abra o Secure Hub.
2. Vá para **Preferências > Informações do dispositivo**.
3. Clique em **Atualizar política**.

Se você ativou a autenticação do PIN da Citrix, o Secure Hub solicita aos usuários que criem um PIN. Depois que um usuário cria um PIN, o XenMobile configura o dispositivo no modo Enterprise. No console XenMobile, a página **Gerenciar > Dispositivos** mostra ambos, MDM e MAM, como ativos para o dispositivo.

Contas de usuário, funções e registro

April 15, 2019

Você configura contas de usuário, funções e inscrições no console XenMobile na guia **Gerenciar** e na página **Configurações**. Salvo indicação em contrário, as etapas para as seguintes tarefas são fornecidas neste artigo.

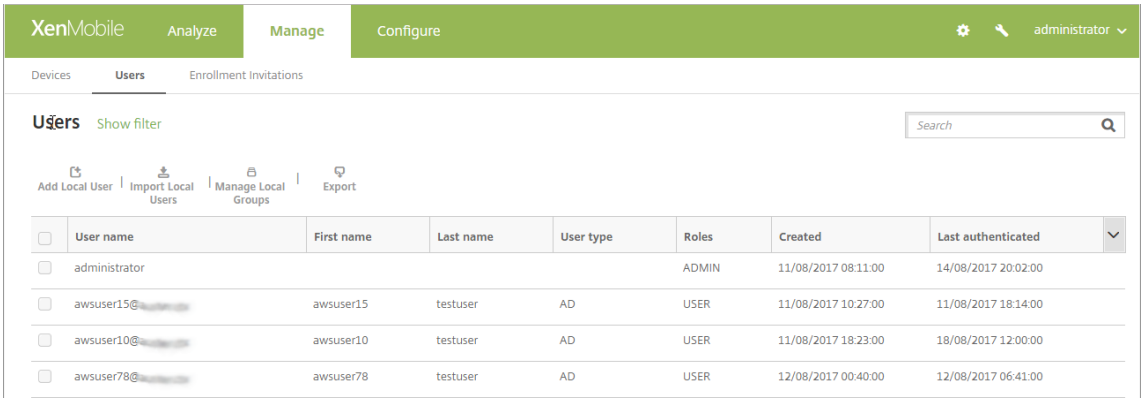
- Contas de usuário e grupos:
  - Em **Gerenciar > Usuários**, adicione contas de usuário manualmente ou use um arquivo de provisionamento .csv para importar as contas e gerenciar os grupos locais.
  - Em **Configurações > Fluxos de trabalho**, use fluxos de trabalho para gerenciar a criação e a remoção de contas de usuário.
- Funções para contas de usuário e grupos
  - Clique em **Configurações > Controle de acesso baseado em função** para 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. Para obter mais informações, consulte Configurar funções com RBAC.
  - Em **Configurações> Modelos de notificação**, para criar ou atualizar modelos de notificação para usar em ações automatizadas, registros e mensagens de notificação padrão enviadas para os usuários. Configure 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 registro e convites.
  - Em **Configurações > Registro**, configure até sete modos de registro e envie convites para registro. Cada modo de registro tem seu próprio nível de segurança e o número de etapas que os usuários deve seguir para registrar seus dispositivos.
  - Ativar a detecção automática no XenMobile para o registro de usuário

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar, editar ou excluir contas de usuários

Você pode adicionar contas de usuário locais ao XenMobile manualmente ou pode usar um arquivo de provisionamento para importar as contas. Para as etapas para importar contas de usuário de um arquivo de provisionamento, consulte Importar contas de usuário.

1. No console XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.

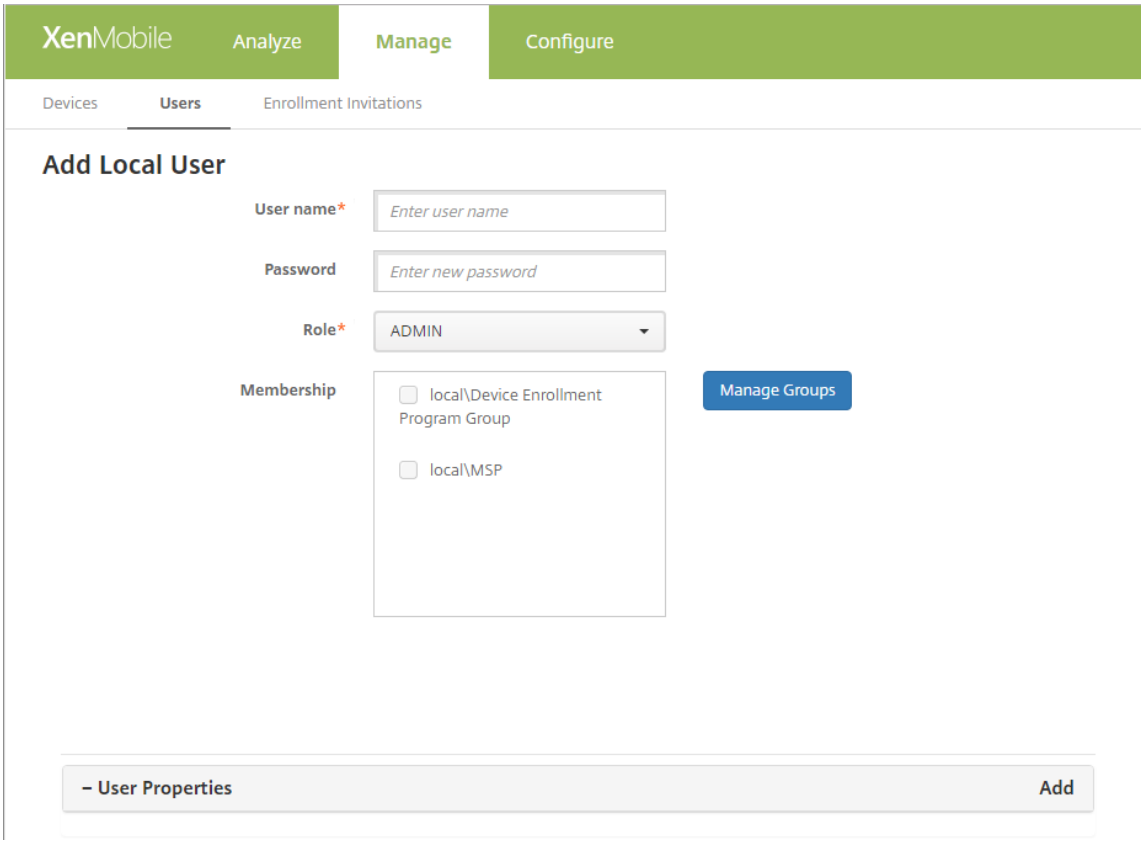


2. Clique em **Mostrar filtro** para filtrar a lista.

Para adicionar uma conta de usuário local

1. Na página **Usuários**, clique em **Adicionar usuário local**. A página **Adicionar usuário local** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

   - **Nome de usuário:** digite o nome, um campo obrigatório. Você pode incluir espaços em nomes, bem como letras maiúsculas e minúsculas.
   - **Senha:** digite uma senha de usuário opcional.
   - **Função:** Na lista, clique na função do usuário. Para obter mais informações sobre as funções, consulte Configurar funções com RBAC. As opções possíveis são:
     - ADMIN
     - DEVICE_PROVISIONING
     - SUPPORT
     - USER
   - **Participação:** na lista, clique nos grupos aos quais deseja adicionar o usuário.
   - **Propriedades de usuário:** adicione as propriedades de usuário opcionais. Para cada propriedade de usuário que você deseja adicionar, clique em **Adicionar** e siga os procedimentos:
     - **Propriedades de usuário:** Na lista, clique em uma propriedade e digite o atributo de 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 do usuário existente, passe o mouse sobre a linha que contém a propriedade e clique no X à direita. A propriedade é excluída imediatamente.

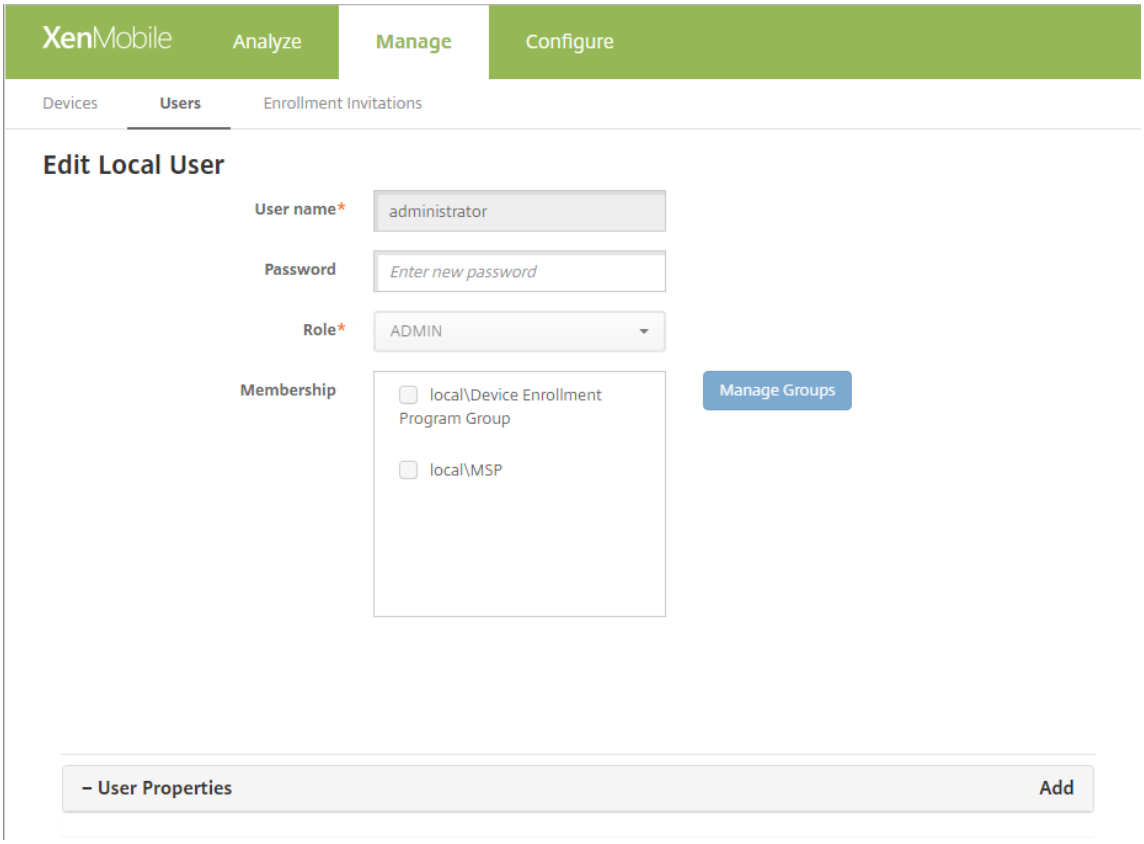
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para editar uma propriedade do usuário existente, clique na propriedade e faça 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 clique em **Editar**. A página **Editar usuário local** é exibida.



2. Altere as seguintes informações conforme apropriado:

   - **Nome de usuário:** Não é possível alterar o nome do usuário.
   - **Senha:** Altere ou adicione uma senha de usuário.
   - **Função:** Na lista, clique na função do usuário.
   - **Participação:** Na lista, clique nos grupos aos quais deseja adicionar o usuário. Para remover a conta de usuário de um grupo, desmarque a caixa de seleção ao lado do nome do grupo.
   - **Propriedade do usuário:** Você pode optar por um dos seguintes procedimentos:
     - Para cada propriedade de usuário que você deseja alterar, clique na propriedade e

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 siga os procedimentos:
  * **Propriedades de usuário:** Na lista, clique em uma propriedade e digite o atributo de 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 clique no **X** à direita. A propriedade é excluída imediatamente.

3. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar o usuário inalterado.

Para excluir uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuários, clique para selecionar uma conta de usuário.

Você pode selecionar mais de um usuário a ser excluído marcando a caixa de seleção ao lado de cada usuário.

1. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.
2. Clique em **Excluir** para excluir o usuário ou 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 excluir tiver os dispositivos registrados e você desejar registrar novamente esses dispositivos, exclua os dispositivos antes de registrá-los. Para excluir um dispositivo, vá até **Gerenciar > Dispositivos**, selecione o dispositivo e, em seguida, clique em **Excluir**.

Importar contas de usuário

Você pode importar contas de usuário locais e propriedades de um arquivo .csv, chamado de arquivo de provisionamento, que pode ser criado manualmente. Para obter mais informações sobre arquivos de provisionamento, consulte Formatos de arquivo de provisionamento.

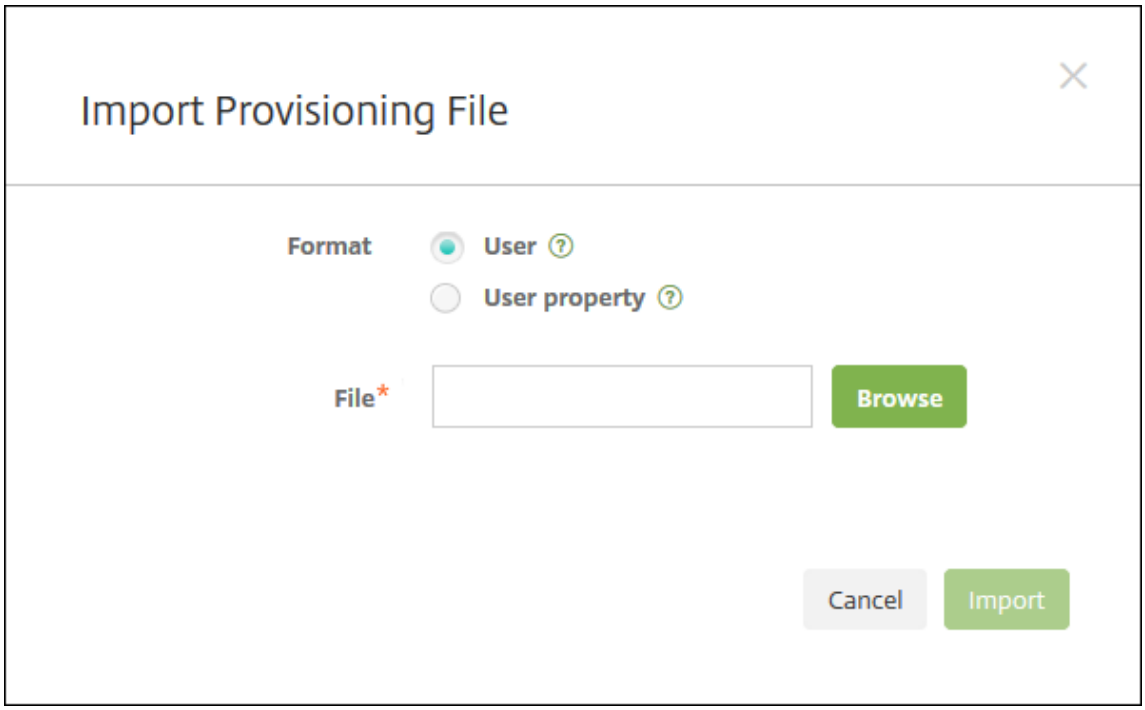
> Nota:
>
> - Para usuários locais, use o nome de domínio junto com o nome do usuário no arquivo de importação. Por exemplo, especifique nome_usuário@domínio. Se o usuário local que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> você criar ou importar for um domínio gerenciado no XenMobile, o usuário não poderá fazer o registro usando as credenciais LDAP correspondentes.
> - Se você estiver importando contas de usuários para o diretório de usuário interno do XenMobile, desative o domínio padrão para acelerar o processo de importação. Lembre-se que desativar o domínio afeta os registros, portanto, você deve reativar o domínio padrão após a conclusão da importação de usuários internos.
> - Os usuários locais podem estar no formato de nome UPN. No entanto, a Citrix recomenda que você não use o domínio gerenciado. Por exemplo, se exemplo.com for gerenciado, não crie um usuário local com este formato de UPN: user@example.com.

Depois que você preparar um arquivo de provisionamento, siga estas etapas para importá-lo para o XenMobile.

1. No console 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 usada clicando em **Procurar** e navegando até a localização do arquivo.
5. Clique em **Importar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Formatos de arquivo de provisionamento

Um arquivo de provisionamento que você cria manualmente e usa para importar contas de usuário e propriedades para o XenMobile deve estar em um dos seguintes formatos:

- **Campos do arquivo de provisionamento de usuário:** user;password;role;group1;group2
- **Campos do arquivo de provisionamento de atributo de usuário:** user;propertyName1;propertyValue1;pro

> Nota:
>
> - Separe os campos no arquivo de provisionamento com um ponto e vírgula (;). Se parte de um campo contiver um ponto e vírgula, ele deverá ser antecedido por 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 outras funções que você definiu.
> - Use o caractere de ponto (.) como um separador para criar a hierarquia de grupo. Não use um ponto nos nomes de grupo.
> - Use letras minúsculas para atributos de propriedade nos arquivos de provisionamento de atributo. O banco de dados diferencia maiúsculas de minúsculas.

Exemplo de conteúdo de fornecimento 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.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 fornecimento de atributo do usuário

A entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Usuário:** user01
- **Propriedade 1**
  - **nome:** propertyN
  - **valor:** propertyV;test;1;2
- **Propriedade 2:**
  - **nome:** prop 2
  - **valor:** prop2 value

Para configurar modos de registro

Configure os modos de registro de dispositivo para permitir que os usuários registrem seus dispositivos no XenMobile. O XenMobile oferece sete modos, cada um com seu próprio nível de segurança e etapas que os usuários devem seguir para registrar os dispositivos. Você pode disponibilizar alguns modos no Portal de Autoajuda. Os usuários podem fazer login no portal e gerar links de registro que lhes permitem registrar os dispositivos ou optar por enviar um convite de registro para si mesmos. Configure modos de registro no console XenMobile da página **Configurações > Registro**.

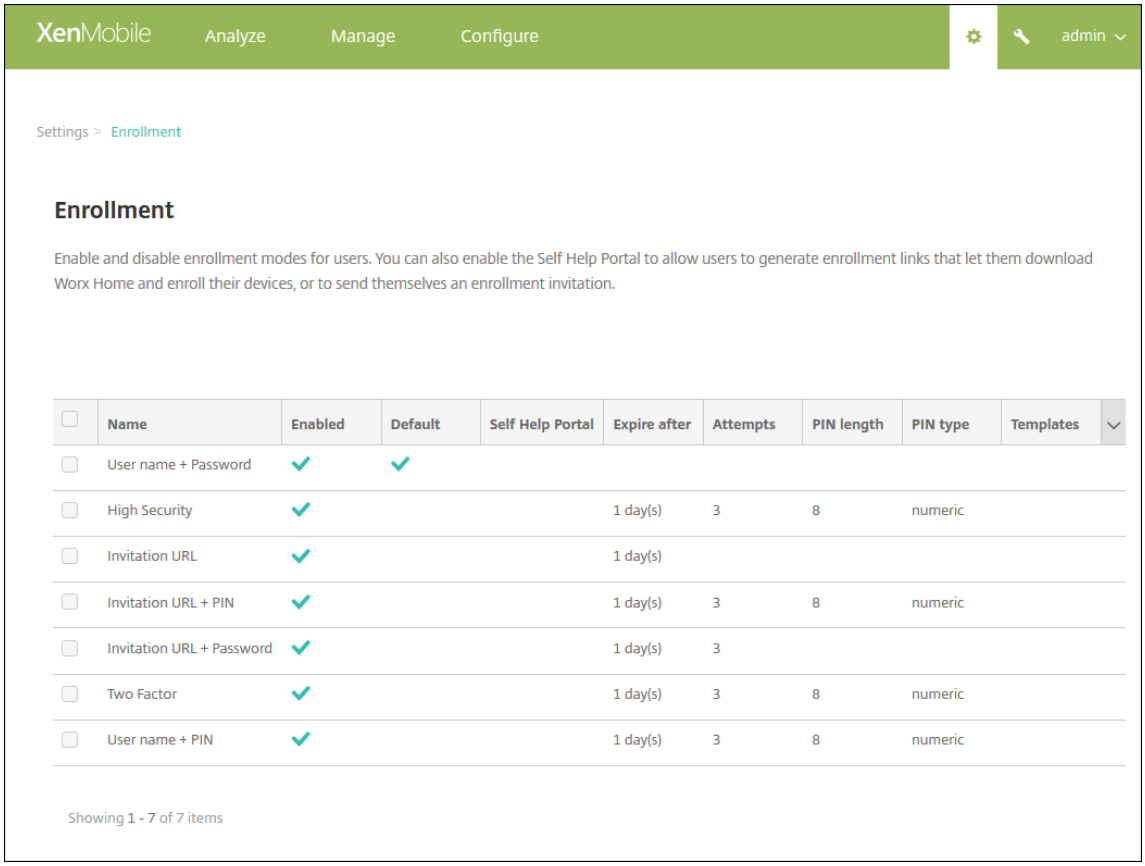
Envie convites de registro na página **Gerenciar > Convites de registro**. Para obter informações, consulte Envie um convite para registro.

> Nota:
>
> Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de você configurar os modos de registro. Para obter mais informações sobre modelos de notificação, consulte Criando ou atualizando modelos de notificação.

1. No console 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 registro disponíveis. Por padrão, todos os modos de registro estão ativados.
3. Selecione um modo de registro na lista para editá-lo. Em seguida, defina o modo como padrão, desative o modo ou permita o acesso de usuários ao Portal de Autoajuda.

   > Nota:
   >
   > Quando você marca a caixa de seleção ao lado de um modo de registro, o menu de opções é exibido acima da lista de modos de registro. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Escolha entre os modos de registro:

- Nome de usuário + Senha
- Alta Segurança
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Dois Fatores
- Nome de usuário + PIN

Você pode usar convites de registro para restringir o registro para os usuários com apenas um convite.

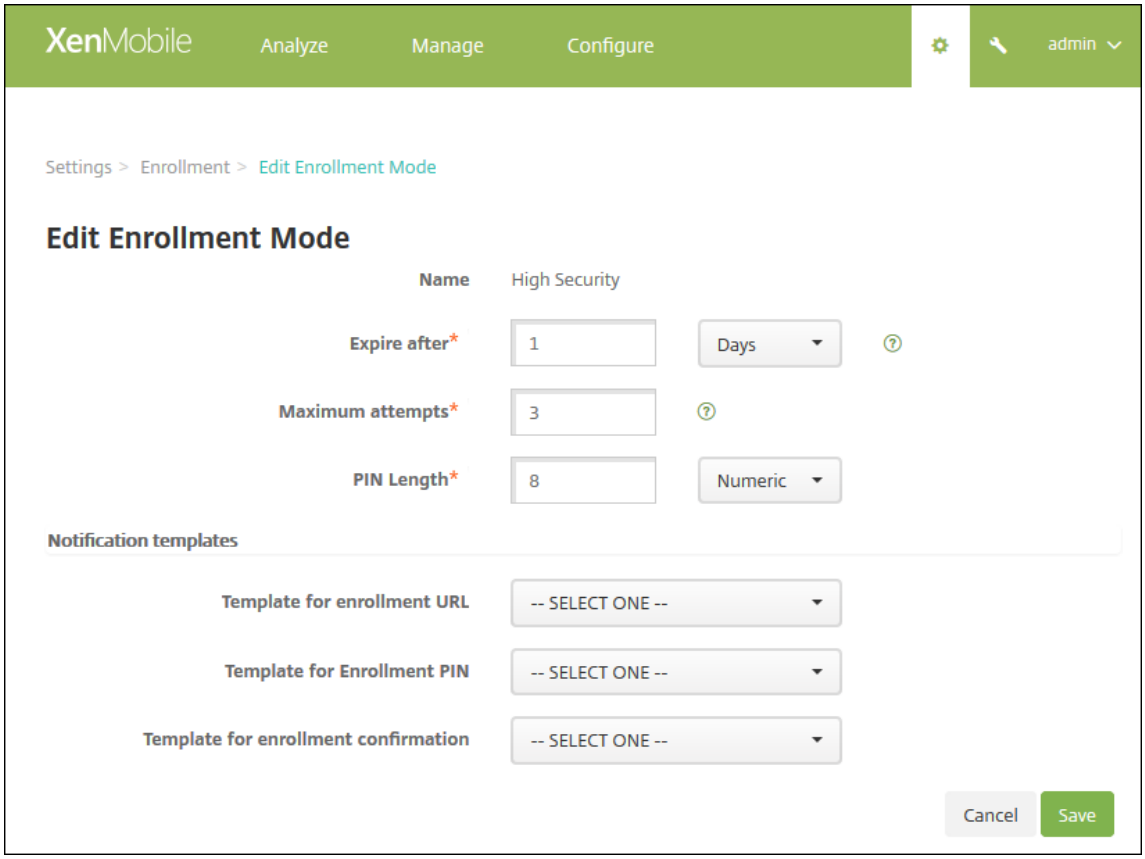
Você pode usar convites de registro de PIN de uso único (OTP) como uma solução de dois fatores. Os convites de registro OTP controlam o número de dispositivos que um usuário pode registrar.

Para ambientes com requisitos de segurança, você pode associar convites de registro a um dispositivo por UDID/SN/EMEI. Uma opção de dois fatores também está disponível para exigir senha do Active Directory e OTP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para editar um modo de registro

1. Na lista **Registro**, selecione um modo de registro e clique em **Editar**. A página **Editar Modo de Registro** é exibida. Dependendo do modo selecionado, você pode ver opções diferentes.



2. Altere as seguintes informações conforme apropriado:

   - **Expira após:** digite um prazo de expiração após o qual os usuários não poderão registrar dispositivos. Este valor aparece nas páginas de configuração de convite de registro de usuário e de grupo.

     Digite **0** para impedir que o convite expire.

   - **Dias:** na lista, clique em **Dias** ou **Horas** para corresponder ao prazo de expiração inserido em **Expira após**.

   - **Máximo de tentativas:** digite o número de tentativas para registrar que um usuário pode fazer antes que o processo de registro fique bloqueado para ele. Este valor aparece nas páginas de configuração de convite de registro de usuário e de grupo.

     Digite **0** para permitir tentativas ilimitadas.

   - **Comprimento do PIN:** digite um numeral para definir o comprimento do PIN gerado.

   - **Numérico:** na lista, clique em **Numérico** ou **Alfanumérico** para o tipo de PIN.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Modelos de notificação:**
  - **Modelo de URL de registro:** na lista, clique em um modelo a ser usado para o URL de registro. Por exemplo, o modelo de convite de registro envia aos usuários um email ou SMS. O método depende de como você configurou o modelo que permite registrar seus dispositivos no XenMobile. Para obter mais informações sobre modelos de notificação, consulte Criando ou atualizando modelos de notificação.
  - **Modelo de PIN de registro:** na lista, clique em um modelo a ser usado para o PIN de registro.
  - **Modelo de confirmação de registro:** na lista, clique em um modelo a ser usado para informar um usuário que ele foi registrado com sucesso.

3. Clique em **Salvar**.

Para definir um modo de registro como padrão

Quando você define um modo de registro como padrão, o modo é usado para todas as solicitações de registro de dispositivo, a menos que você selecione um modo de registro diferente. Se nenhum modo de registro for definido como padrão, você deverá criar uma solicitação de registro para cada dispositivo.

> Nota:
>
> Os únicos modos de registro que você pode usar como padrão são **Somente nome de usuário + senha**, **Dois fatores** ou **Nome de usuário + PIN**.

1. Selecione o modo de registro, **Nome de usuário + senha**, **Dois fatores** ou **Nome de usuário + PIN**.

   Para usar um modo como padrão, é preciso ativá-lo primeiramente.

2. Clique em **Padrão**. O modo selecionado agora é o padrão. Se qualquer outro modo de registro tiver sido definido como padrão, o modo não será mais o padrão.

Para desabilitar um modo de registro

Desativar um modo de registro o torna indisponível para uso nos convites de registro de grupo e no Portal de Autoajuda. Você pode alterar como permite que usuários registrem seus dispositivos desativando um modo de registro e permitindo outro.

1. Selecione um modo de registro.

   Você não pode desativar o modo de registro padrão. Se você desejar desativar o modo de registro padrão, deverá primeiro remover o status padrão.

2. Clique em **Desativar**. O modo de registro não está mais ativado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para habilitar um modo de registro no Portal de Autoajuda

Permitir um modo de registro no Portal de Autoajuda permite que os usuários registrem seus dispositivos no XenMobile individualmente.

> Nota:
>
> - O modo de registro deve ser ativado e estar limitado aos modelos de notificação a serem disponibilizados no Portal de Autoajuda.
> - Você só pode ativar um modo de registro no Portal de Autoajuda por vez.

1. Selecione um modo de registro.
2. Clique em **Portal de Autoajuda**. O modo de registro selecionado está disponível para os usuários do Portal de Autoajuda. Qualquer modo que já estiver ativado no Portal de Autoajuda não estará mais disponível para os usuários.

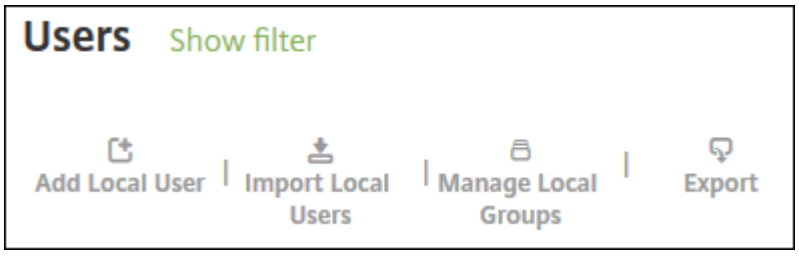
Adição ou remoção de grupos

Gerencie grupos na caixa de diálogo **Gerenciar grupos** no console XenMobile nestas páginas: **Usuários**, **Adicionar usuário local** ou **Editar usuário local**. Não há nenhum comando de edição de grupo.

Se você remover um grupo, esteja ciente de que a remoção do grupo não afeta as contas de usuário. Remover um grupo simplesmente remove a associação dos usuários àquele grupo. Os usuários também perdem acesso aos aplicativos ou aos perfis fornecidos pelos Grupos de Entrega que são associados a esse grupo; todas as outras associações de grupo, no entanto, permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles estarão associados ao nível superior.

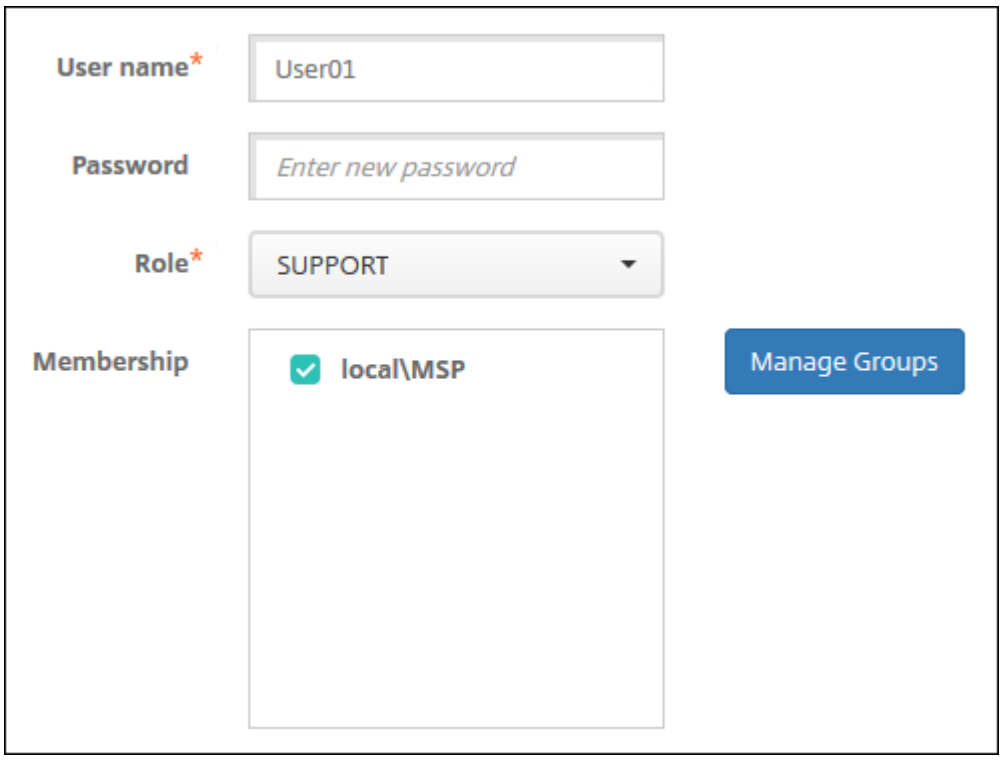
Para adicionar um grupo local

1. Você pode optar por um dos seguintes procedimentos:
   - Na página **Usuários**, clique em **Gerenciar grupos locais**.



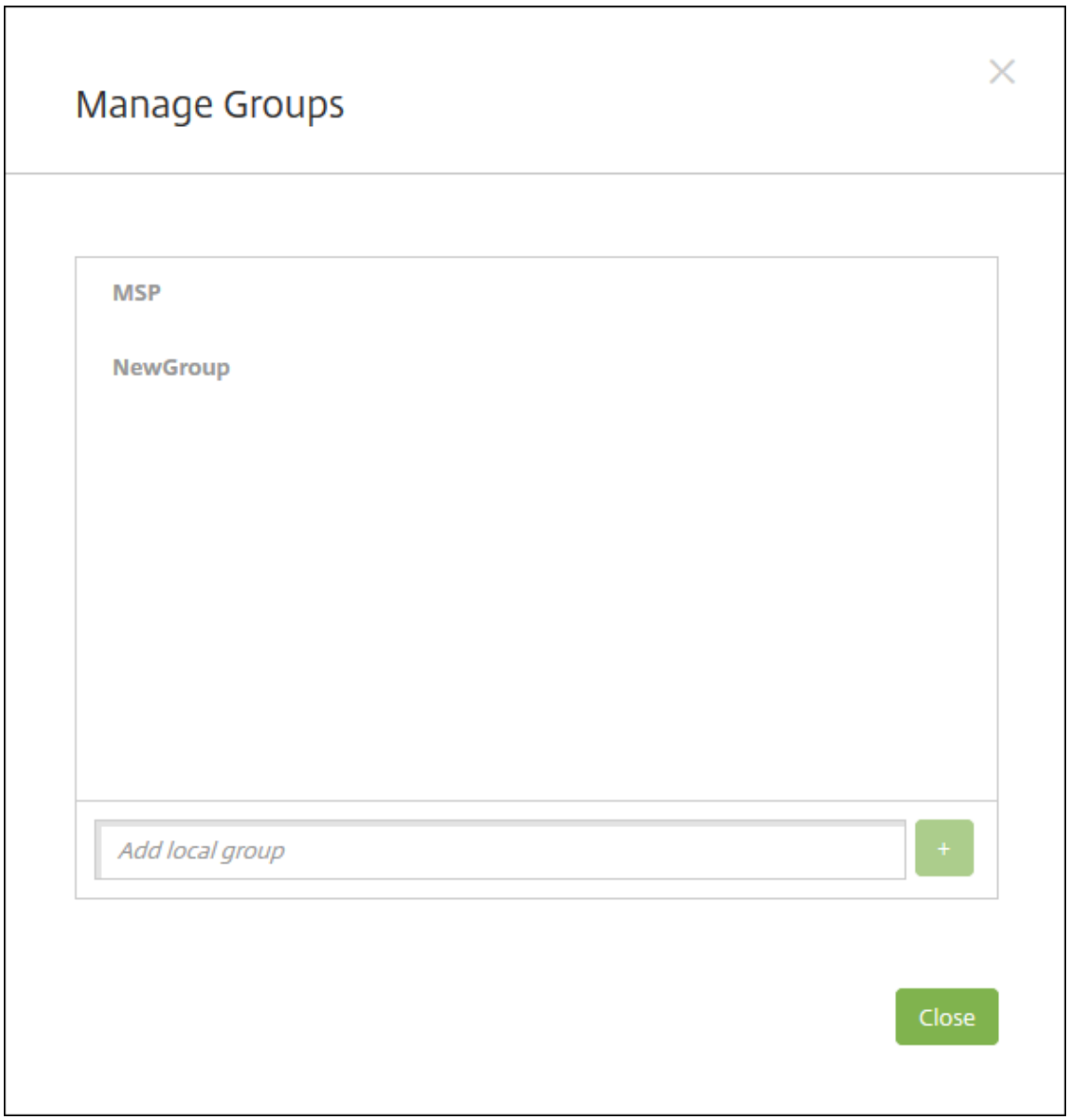
   - Na página **Adicionar usuário local** ou na página **Editar usuário local**, clique em **Gerenciar grupos**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A caixa de diálogo **Gerenciar grupo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Abaixo da lista de grupos, digite um novo nome de grupo e, em seguida, clique no sinal de mais (**+**). O grupo de usuário é adicionado à lista.
3. Clique em **Fechar**.

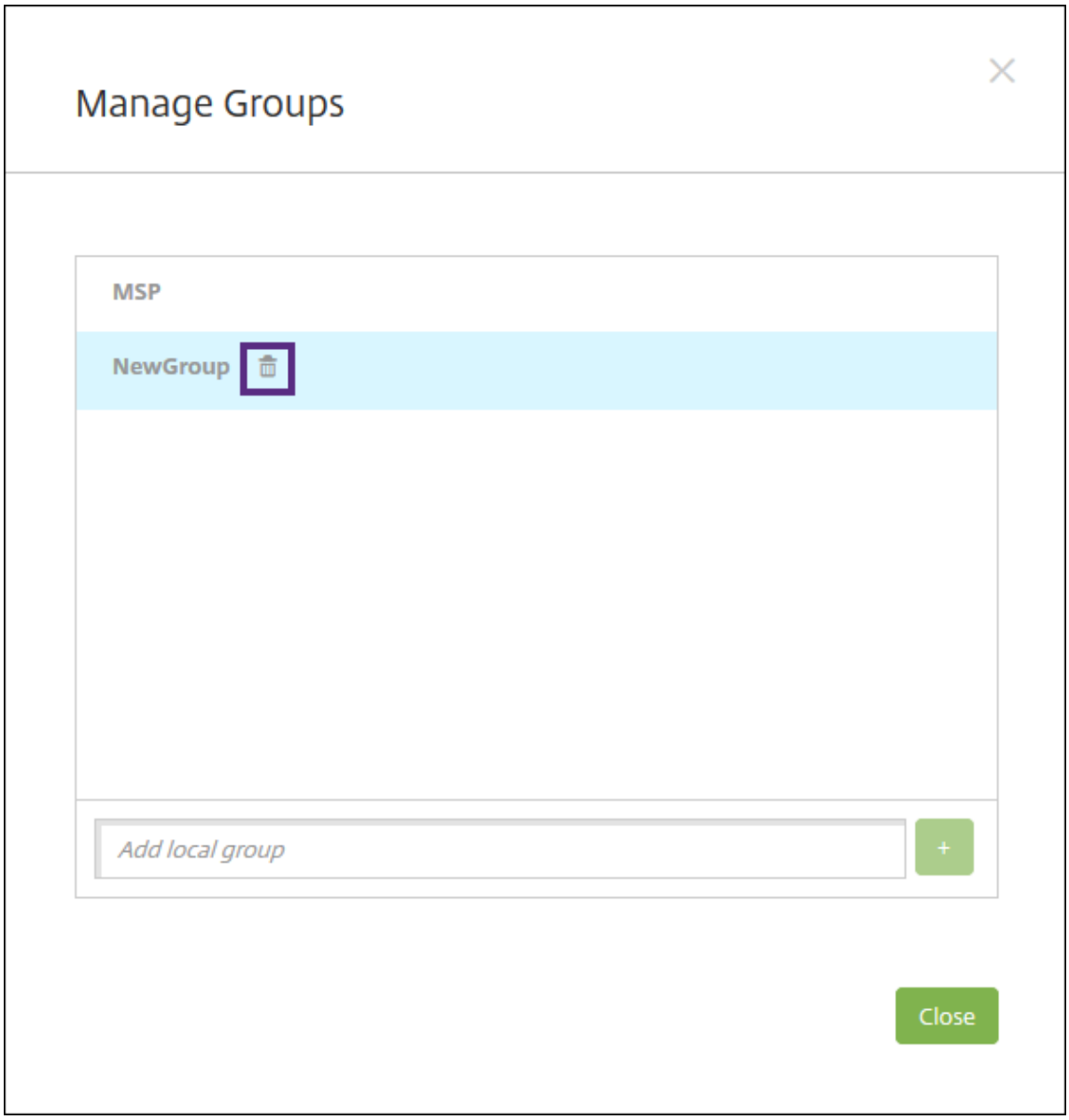
Para remover um grupo

Remover um grupo não afeta as contas de usuário. Remover um grupo simplesmente remove a associação do usuário àquele grupo. Os usuários também perdem acesso aos aplicativos ou aos perfis fornecidos pelos Grupos de Entrega que são associados a esse grupo. No entanto, todas as outras associações de grupo permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles estarão associados ao nível superior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Você pode optar por um dos seguintes procedimentos:
   - 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 desejar excluir.
3. Clique no ícone de 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Importante:
>
> Você não pode desfazer essa 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 a remoção de contas de usuário. Antes de poder usar um fluxo de trabalho, identifique as pessoas em sua organização que têm a autoridade para aprovar solicitações de conta de usuário. Em seguida, você pode usar o modelo de fluxo de trabalho para criar e aprovar solicitações de conta de usuário.

Quando você configura o XenMobile pela primeira vez, define as configurações de email de fluxo de trabalho, o que deve ocorrer antes de você poder usar os fluxos de trabalho. Você pode alterar as configurações de email de fluxo de trabalho a qualquer momento. Essas configurações incluem o servidor de email, a porta, o endereço de email, e se a solicitação para criar a conta de usuário requer aprovação.

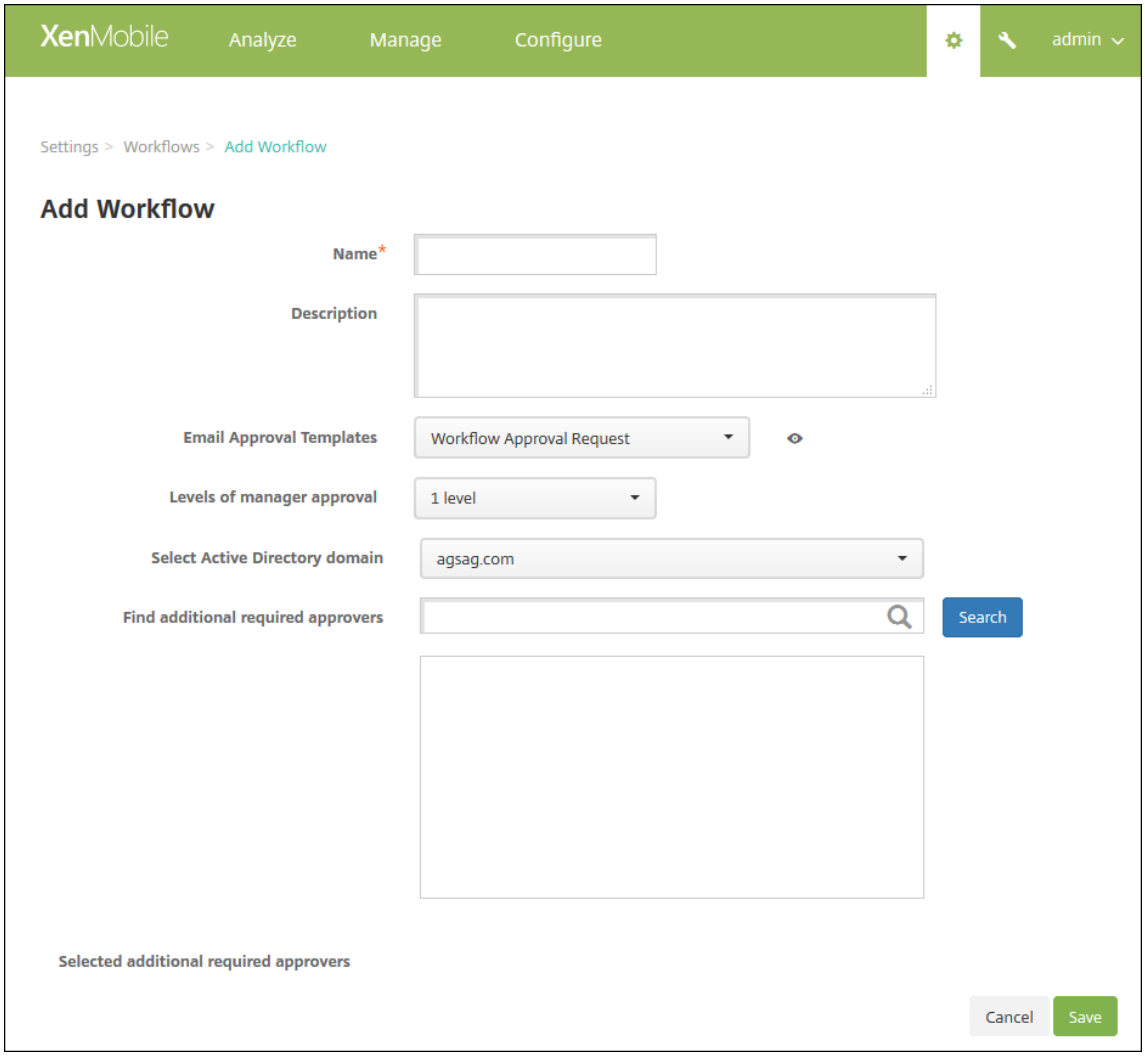
Você pode configurar os fluxos de trabalho em dois lugares no XenMobile:

- Na página **Fluxos de trabalho** no console XenMobile. Na página **Fluxos de trabalho**, você pode configurar vários fluxos de trabalho para serem usados com as configurações do aplicativo. Ao configurar fluxos de trabalho na página Fluxos de trabalho, você pode selecionar o fluxo de trabalho durante a configuração do aplicativo.
- Ao configurar um conector de aplicativo, forneça um nome de fluxo de trabalho e configure os indivíduos que podem aprovar a solicitação de conta de usuário. Veja Adição de aplicativos ao XenMobile.

Você pode atribuir até três níveis à aprovação do gerente de contas de usuário. Se você precisar que outras pessoas aprovem a conta de usuário, poderá procurar e selecionar essas pessoas usando o respectivo nome ou endereço de email. Quando o XenMobile encontrar a pessoa, adicione-a ao fluxo de trabalho. Todos os indivíduos do fluxo de trabalho recebem emails para aprovar ou negar a nova conta de usuário.

1. No console 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Defina 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 email:** na lista, selecione o modelo de aprovação a ser atribuído. Você pode criar modelos de emails na seção **Modelos de notificação** sob **Configurações** no console XenMobile. Quando você clica no ícone de olho à direita deste campo, é exibida uma visualização do modelo que você está configurando.
   - **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
     - Não é Necessário
     - 1 nível
     - 2 níveis
     - 3 níveis

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome no campo de busca e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
  - Para remover um nome da lista, proceda de um dos seguintes modos:
    * Clique em **Pesquisar** para ver uma lista de todos no domínio selecionado.
    * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
    * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

5. Clique em **Salvar**. O fluxo de trabalho criado é exibido na página **Fluxos de trabalho**.

Depois de criar o fluxo de trabalho, você pode exibir os detalhes do fluxo de trabalho, exibir os aplicativos associados a ele ou excluí-lo. Você não pode editar um fluxo de trabalho depois de tê-lo criado. Se você precisar de um fluxo de trabalho com níveis diferentes de aprovação ou aprovadores diferentes, crie outro fluxo de trabalho.

Para ver 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 tanto, 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:
   >
   > Você não pode desfazer essa operação.

Configurar funções com RBAC

April 15, 2019

Cada função de controle de acesso baseado em função (RBAC) predefinida tem acesso a determinados recursos e permissões associados. Este artigo descreve o que cada uma dessas permissões faz. Para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

obter uma lista completa das permissões padrão de cada função interna, baixe Padrões de Controle de Acesso Baseado em Funções.

Quando você *aplicar permissões*, você define os grupos de usuários que a função RBAC tem a permissão para gerenciar. Observe que o administrador padrão não pode alterar as configurações de permissões aplicadas. Como padrão, as permissões aplicadas se aplicam a todos os grupos de usuários.

Quando você faz uma *atribuição*, você atribui a função RBAC a um grupo, de modo que o grupo de usuários detém os direitos de administrador RBAC.

Este artigo contém as seguintes seções:

- Função de Administrador
- Função de provisionamento de dispositivos
- Função de suporte
- Função de Usuário
- Configurar funções com RBAC

Função de Administrador

Os usuários com a função Administração predefinida têm acesso ou não aos recursos a seguir no XenMobile. Como padrão, **Acesso autorizado** (exceto Portal de Autoajuda e Suporte Remoto), **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 XenMobile.
Acesso ao Portal de Autoajuda	Os administradores não têm acesso ao Portal de Autoajuda.
Assistente de registro de dispositivos compartilhados	Os administradores não têm acesso ao assistente de registro de dispositivos compartilhados. Esse recurso é destinado aos usuários que precisam registrar dispositivos compartilhados.
Acesso ao suporte remoto	Os administradores têm acesso ao suporte remoto.*

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Acesso à API pública	Os administradores têm acesso à API pública para realizar, de forma programática, ações que estão disponíveis no console XenMobile. As ações incluem administrar certificados, aplicativos, dispositivos, grupos de entrega e usuários locais.

* O suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível somente com dispositivos Samsung KNOX. O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

Recursos do console

Os administradores têm acesso irrestrito ao console XenMobile.

Painel	O **painel** é a primeira página que os administradores veem depois de fazer login no console XenMobile. O **painel** mostra informações básicas sobre as notificações e os dispositivos.
Criação de relatórios	A página **Analisar > Relatórios** fornece relatórios predefinidos que permitem analisar as implantações de aplicativo e dispositivo.
Dispositivos	A página **Gerenciar > Dispositivos** é o local em que 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 ao mesmo tempo.
Usuários locais e grupos	A página **Gerenciar > Dispositivos** é o local em que você pode adicionar, editar ou excluir usuários locais e grupos de usuários locais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registro	A página **Gerenciar > Convites de Registro** é o local em que você gerencia como os usuários são convidados para registrar seus dispositivos no XenMobile.
Políticas	A página **Configurar > Políticas de dispositivo** é o local em que você gerencia as políticas de dispositivo, como VPN e WiFi.
Aplicativos	A página **Configurar > Aplicativos** é o local em que você gerencia os vários aplicativos que os usuários podem instalar nos seus dispositivos.
Mídia	A página **Configurar > Mídia** é o local em que você gerencia as várias mídias que os usuários podem instalar nos seus dispositivos.
Ação inteligente	A página **Configurar > Ações** é o local em que você gerencia as respostas a eventos de disparo.
Perfis de registro	A página **Configurar > Perfis de registro** é o local em que você configura perfis (modos) de registro para permitir que os usuários registrem seus dispositivos.
Grupos de entrega	A página **Configurar > Grupos de Entrega** é o local em que você gerencia os grupos de entrega e os recursos associados a eles.
Configurações	A página **Configurações** é o local em que você administra as configurações do sistema, como propriedades do cliente e servidor, certificados e provedores de credenciais.
Suporte	A página **Solução de problemas e suporte** é o local em que você executa atividades de solução de problemas, como realizar diagnósticos e gerar logs.

Dispositivos

Os administradores acessam recursos de dispositivo em todo o console definindo restrições de dis-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

positivo, configurando e enviando notificações para dispositivos, administrando os aplicativos nos dispositivos e assim por diante.

Apagamento completo do dispositivo	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, caso o dispositivo os tenha.
Apagar Restrição	Remover uma ou mais restrições de dispositivo.
Apagamento seletivo do dispositivo	Apagar todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local.
Exibir localizações	Ver a localização de e definir as 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 o dispositivo, de forma que os usuários não possam usá-lo.
Desbloquear dispositivo	Desbloquear remotamente o dispositivo, de forma que os usuários não 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 desvio de bloqueio de ativação DEP ASM	Armazene um código de desvio em um dispositivo iOS supervisionado, quando o bloqueio de ativação estiver ativado. Se você precisar apagar o dispositivo, use esse código para limpar o bloqueio de ativação automaticamente.
Chama o dispositivo	Chamar remotamente um dispositivo Windows no volume mais alto durante cinco minutos.
Reinicializar o dispositivo	Reinicie os dispositivos Windows no console XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Implantar no dispositivo	Enviar aplicativos, notificações, restrições e assim por diante para um dispositivo.
Editar dispositivo	Alterar as configurações do dispositivo.
Notificação para o dispositivo	Enviar uma notificação para um dispositivo.
Adicionar/excluir dispositivo	Adicionar ou remover dispositivos no XenMobile.
Importação de dispositivos	Importar um grupo de dispositivos de um arquivo para o XenMobile.
Exportar tabela do dispositivo	Coletar informações do dispositivo na página Dispositivo e exportá-las para um arquivo .csv.
Revogar dispositivo	Proibir um dispositivo de se conectar ao XenMobile.
Bloqueio de aplicativo	Negar acesso a todos os aplicativos em um dispositivo. No Android, os usuários não poderão fazer logon para o XenMobile de modo nenhum. No iOS, os usuários poderão continuar a fazer logon, mas elas não poderão acessar aplicativos.
Apagamento de aplicativos	No Android, esta opção exclui a conta do XenMobile. No iOS, essa opção exclui a chave de criptografia de que os usuários precisam para ter acesso aos recursos do XenMobile.
Exibir inventário de software	Ver quais softwares estão instalados em um dispositivo.
Solicitar espelhamento de AirPlay	Solicitar o início do streaming do AirPlay.
Parar espelhamento de AirPlay	Parar o streaming do AirPlay.
Ativar o modo perdido	Na página Gerenciar, em dispositivos, você pode colocar um dispositivo supervisionado no modo perdido para bloquear um dispositivo supervisionado na tela de bloqueio e localize o dispositivo quando o dispositivo seja perdido ou roubado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Desativar o modo perdido	Na página Gerenciar dispositivos, você pode desativar o modo perdido para um dispositivo está configurado para modo perdido.
Dispositivo de atualização de SO	Você pode implantar uma política de dispositivo de Controle de atualizações de sistema operacional para dispositivos.
Desligar o dispositivo	Desligue os dispositivos iOS no console XenMobile.
Reinicializar o dispositivo	Reinicie os dispositivos iOS no console XenMobile.

Usuários locais e grupos

Os administradores gerenciam usuários locais e grupos de usuários locais na página **Gerenciar > Usuários** no XenMobile.

Adicionar/excluir usuários locais
Editar usuários locais
Importar usuários locais
Exportar usuários locais
Grupos de usuários locais

Registro

Os administradores podem adicionar e excluir convites para registro, enviar notificações para os usuários e exportar a tabela de registro para um arquivo .csv.

Adicionar/excluir registro	Adicionar ou remover um convite para registro de um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite para registro para um usuário ou um grupo de usuários.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exportar tabela de convites de registro	Coletar informações de registro na página Registro e exportá-las para um arquivo .csv.

Políticas

Adicionar/excluir política	Adicionar ou remover um dispositivo ou uma política de aplicativo.
Editar política	Alterar um dispositivo ou uma política de aplicativo.
Carregar Política	Carregar uma política de dispositivo ou de aplicativo.
Clonar Política	Copiar uma política de dispositivo ou de aplicativo.
Desativar Política	Desativar uma política de aplicativo existente.
Exportar política	Coletar informações de política de dispositivo na 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 não preparado com o MDX Toolkit.
Editar loja de aplicativos ou aplicativo empresarial	Fazer alterações em um aplicativo de loja de aplicativos pública ou um aplicativo não preparado com o MDX Toolkit.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar/excluir aplicativo MDX, Web e SaaS	Adicionar ou remover um aplicativo preparado com o MDX Toolkit (aplicativo 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	Fazer alterações em um aplicativo preparado com o MDX Toolkit (aplicativo 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 no XenMobile Store.
Atribuir aplicativo público/empresarial ao grupo de entrega	Atribuir um aplicativo de loja de aplicativos pública ou um aplicativo não preparado com o MDX Toolkit a um grupo de entrega para implantação.
Atribuir aplicativo MDX/WebLink/SaaS ao grupo de entrega	Atribuir um aplicativo preparado com o MDX Toolkit (aplicativo MDX), um aplicativo que não exige logon único (WebLink) ou um aplicativo de uma rede pública (SaaS) a um grupo de entrega para implantação nos dispositivos do usuário.
Exportar tabela de aplicativos	Coletar informações do aplicativo na página Aplicativo e exportá-las para um arquivo .csv.

Mídia

Gerencie mídias obtidas de uma loja de aplicativos pública ou por meio de uma licença VPP.

Adicionar/excluir loja de aplicativos ou livros empresariais
Atribuir livros públicos/empresariais ao grupo de entrega
Editar loja de aplicativos ou livros empresariais

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ação inteligente

Adicionar/excluir ação inteligente	Adicionar ou remover uma ação definida por um gatilho (evento, propriedade do dispositivo ou usuário, ou nome do aplicativo instalado) e a resposta associada.
Editar ação inteligente	Alterar uma ação definida por um gatilho (evento, propriedade do dispositivo ou usuário, ou nome do aplicativo instalado) e a resposta associada.
Atribuir ação inteligente ao grupo de entrega	Atribuir uma ação a um grupo de entrega para implantação nos dispositivos do usuário.
Exportar ação inteligente	Coletar informações sobre a ação na 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 os usuários especificados e políticas, aplicativos e ações opcionais.
Editar grupo de entrega	Alterar um grupo de entrega, que modifica os usuários e políticas opcionais, aplicativos e ações.
Implantar grupo de entrega	Disponibilizar o grupo de entrega para uso.
Exportar grupo de entrega	Coletar informações de grupo de entrega da página Grupo de Entrega e exportá-las para um arquivo .csv.

Perfil de registro

Gerenciar perfis de registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar/apagar perfil de registro
Editar perfil de registro
Atribuir o perfil de registro para o grupo de entrega

Configurações

Os administradores definem várias configurações nas páginas de **Configurações**.

RBAC	Atribuição de RBAC, atribuir funções
LDAP	Administrar um ou mais diretórios em conformidade com o LDAP, como o Active Directory, para importar grupos, contas de usuário e propriedades relacionadas.
Licença	Para o XenMobile Server local. Administrar as licenças da Citrix.
Registro	Ativar os modos de registro dos usuários, bem como o Portal de Autoajuda.
Gerenciamento de Versão	Exibir a versão instalada atual. Inclui: atualização do gerenciamento de versões
Certificados	Editar certificado APNS, certificados de ouvinte SSL
Modelos de notificação	Crie modelos de notificação para usar em ações automatizadas, registros e entregas de mensagens de notificação padrão para os usuários.
Fluxos de Trabalho	Gerenciar a criação, a aprovação e a remoção de contas de usuário para uso com as configurações do aplicativo.
Provedores de credenciais	Adicionar um ou mais provedores de credenciais autorizados a emitir certificados do dispositivo. Os provedores de credenciais controlam o formato do e as condições certificado para renová-lo ou revogá-lo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Entidades PKI	Gerenciar entidades de infraestrutura de chave pública (genéricas, Serviços de Certificado da Microsoft ou AC discricionária).
Testar conexão PKI	Use o botão Testar Conexão na página **Configurações > Entidades PKI** para garantir que o servidor esteja acessível.
Propriedades do cliente	Gerenciar várias propriedades nos dispositivos do usuário, como o tipo de código secreto, a segurança, a expiração e assim por diante.
Suporte ao cliente	Defina como os usuários podem entrar em contato com os seus serviços de suporte (email, telefone ou email de tíquete de suporte).
Identidade visual do cliente	Crie um nome de armazenamento personalizado e exibições de armazenamento padrão para o XenMobile Store. Adicione um logotipo personalizado para ser exibido no XenMobile Store ou no Secure Hub.
Gateway de SMS da operadora	Instalar gateways de SMS da operadora para configurar as notificações que o XenMobile envia pelos gateways de SMS da operadora.
Servidor de notificação	Configurar um servidor de gateway SMTP para enviar emails aos usuários.
ActiveSync Gateway	Gerenciar o acesso do usuário aos usuários e dispositivos por meio de regras e propriedades.
Device Enrollment Program (DEP) da Apple	Adicione uma conta do Apple DEP ao XenMobile.
Registro de dispositivo do Apple Configurator	Definir configurações do Apple Configurator no XenMobile.
Configurações iOS/VPP	Adicionar contas do Apple Volume Purchase Program.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Provedor de serviços móveis	Usar a interface de Provedor de Serviços Móveis para consultar o BlackBerry e outros dispositivos do Exchange ActiveSync e para emitir operações.
NetScaler Gateway	Para o XenMobile Server local. Adicionar um NetScaler Gateway. Escolha se deseja ativar a autenticação e se deseja enviar o certificado de usuário para autenticação. Escolha um provedor de credenciais.
Controle de Acesso da Rede	Definir as condições que determinam que um dispositivo não está em conformidade e, portanto, tem acesso negado à rede.
Samsung KNOX	Ativar ou desativar o XenMobile para consultar as APIs REST do servidor de atestado do Samsung KNOX.
Propriedades do servidor	Adicionar ou modificar as propriedades do servidor. Exige a reinicialização do XenMobile em todos os nós.
Syslog	Para o XenMobile Server local. Enviar arquivos de log para um servidor (syslog) de logs do sistema usando o nome de host ou o endereço IP do servidor.
XenApp/XenDesktop	Permitir que os usuários adicionem XenApp e XenDesktop via Secure Hub.
ShareFile	Ao usar o XenMobile com ShareFile Enterprise: defina configurações para conexão com a conta do ShareFile e a conta de serviço do administrador para gerenciar contas de usuário. Exige um domínio do ShareFile existente e credenciais de administrador. Ao usar o XenMobile com Conectores do StorageZone: configure o XenMobile para apontar para compartilhamentos de rede e SharePoint locais definidos nos Conectores do ShareFile StorageZones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Programa de melhoria de experiência	Para o XenMobile Server local. Aceitar ou recusar o envio de estatísticas anônimas e informações de uso para a Citrix.
Microsoft Azure	Para o XenMobile Server local. Integre o XenMobile ao Microsoft Azure.
Android for Work	Definir as configurações de servidor do Android for Work.
Provedor de identidade (IDP)	Configure um provedor de identidade.
Credenciais derivadas	Configure credenciais derivadas para o registro de dispositivo iOS.
XenMobile Tools	Acesse a página do XenMobile Tools.
Configuração de SNMP	Ative SNMP para os nós do XenMobile Server. Edite ou adicione usuários de monitoramento, configure o SNMP Manger onde as notificações de interceptação aparecem e configure intervalos e limites de interceptação.

Suporte

Os administradores podem executar várias tarefas de suporte.

Verificações de conectividade do NetScaler Gateway	Executar várias verificações de conectividade do NetScaler Gateway por endereço IP. Exige um nome do usuário e uma senha.
Verificações de conectividade XenMobile	Realizar verificações de conectividade dos recursos selecionados do XenMobile, como o banco de dados, o DNS, o Google Plan e assim por diante.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Criar pacotes de suporte	Para o XenMobile Server local. Crie um arquivo a ser enviado para o suporte da Citrix para solução de problemas. Contém as informações do sistema, os logs, as informações do banco de dados, as informações de núcleo, arquivos de rastreamento e as informações de configuração mais recentes do XenMobile ou do NetScaler Gateway.
Documentação de produtos Citrix	Acessar o site público de documentação do Citrix XenMobile.
Citrix Knowledge Center	Acessar o site Suporte da Citrix para pesquisar artigos da base de dados de conhecimento.
Logs	Acessar e analisar detalhes dos arquivos de log de depuração, auditoria do administrador e auditoria do usuário.
Informações de cluster	Para o XenMobile Server local. Acessar informações sobre cada um dos nós em um ambiente clusterizado.
Coleta de lixo	Para o XenMobile Server local. Acessar informações sobre objetos de memória que não são mais usados.
Propriedades de memória Java	Para o XenMobile Server local. Acessar um instantâneo do uso da memória, dos detalhes da memória e dos detalhes do pool de memória Java.
Macros	Preencher os dados de propriedade do usuário ou do dispositivo no campo de texto de um perfil, uma política, uma notificação ou um modelo de registro. Configure uma única política, implante-a em uma grande base de usuários e faça com que os valores específicos do usuário sejam exibidos para cada usuário de destino.
Configuração de PKI	Importar e exportar informações de configuração de PKI.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Utilitário de assinatura APNS	Enviar uma solicitação de certificados de assinatura de Apple Push Network (APNs) ou carregar um certificado de APNs do Secure Mail para o iOS.
Citrix Insight Services	Carregar logs para o Citrix Insight Services (CIS) para obter assistência com vários problemas.
Status do dispositivo com o conector Citrix Gateway para Exchange ActiveSync	Consulte o XenMobile para saber 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 o XenMobile Server local. Quando você cria pacotes de suporte no XenMobile, dados confidenciais do usuário, do servidor e da rede são anonimizados por padrão. Você pode alterar esse comportamento na página Anonimização e desanonimização e, Suporte, sob Avançado.
Configurações de log	Personalize o nível de log ou adicionE um agente de log personalizado.

Restringir Acesso de Grupo

Os usuários administradores podem aplicar permissões a todos os grupos de usuários.

Função de provisionamento de dispositivos

> Importante:
>
> A Função de Provisionamento do Dispositivo se aplica somente aos dispositivos Windows CE.

Os usuários com a função de provisionamento do dispositivo predefinida têm acesso limitado aos recursos do console; Por padrão, sua permissão é definida como todos os grupos de usuários e não podem alterar essa configuração.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Recursos do console

Os usuários de provisionamento de dispositivo têm o acesso restrito a seguir no console XenMobile. Por padrão, cada um dos recursos a seguir está ativado.

Dispositivos

Editar dispositivo	Alterar as configurações do dispositivo.
Adicionar/excluir dispositivo	Adicionar ou remover dispositivos no XenMobile.

Configurações

Os usuários de provisionamento do dispositivo podem acessar a página **Configurações**, mas não têm os direitos para configurar os recursos.

Função de suporte

Os usuários com a função de suporte têm acesso ao suporte remoto; as permissões se aplicam a todos os usuários por padrão e não podem editar essa configuração.

Função de Usuário

Os usuários com a função de Usuário têm o acesso limitado a seguir ao XenMobile.

Acesso autorizado

Portal de Autoajuda	Os usuários têm acesso somente ao Portal de Autoajuda no XenMobile.

Recursos do console

Os usuários têm o acesso restrito a seguir no console XenMobile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dispositivos

Apagamento completo do dispositivo	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, caso o dispositivo os tenha.
Apagamento seletivo do dispositivo	Apagar todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local.
Exibir localizações	Ver a localização de e definir as restrições geográficas em um dispositivo. Incluído: 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 ele não possa ser usado.
Desbloquear dispositivo	Desbloquear remotamente um dispositivo para que ele não possa ser usado.
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 desvio de bloqueio de ativação DEP ASM	Armazene um código de desvio em um dispositivo iOS supervisionado, quando o bloqueio de ativação estiver ativado. Se você precisar apagar o dispositivo, use esse código para limpar o bloqueio de ativação automaticamente.
Chama o dispositivo	Chamar remotamente um dispositivo Windows no volume mais alto durante cinco minutos.
Reinicializar o dispositivo	Reinicie um dispositivo Windows.
Exibir inventário de software	Ver quais softwares estão instalados em um dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registro

Adicionar/excluir registro	Adicionar ou remover um convite para registro de um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite para registro para um usuário ou um grupo de usuários.

Restringir Acesso de Grupo

Para todas as quatro funções padrão, essa permissão é definido como padrão e pode ser aplicada a todos os grupos de usuários. Você não pode editar a função.

Configurar funções com RBAC

O recurso Controle de Acesso Baseado em Função (RBAC) no XenMobile permite que você 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.

O XenMobile implementa quatro funções de usuário padrão para separar logicamente o acesso às funções do sistema:

- **Administrador:** Concede acesso total ao sistema.
- **Provisionamento de dispositivos:** Concede acesso à administração básica de dispositivos para dispositivos Windows CE.
- **Suporte:** Concede acesso ao suporte remoto.
- **Usuário:** Usado pelos usuários que podem registrar dispositivos e acessar o Portal de Autoajuda.

Você também pode usar as funções padrão como modelos que podem ser personalizados para criar novas funções de usuário com permissões para acessar funções do sistema específicas além das funções definidas pelas funções padrão.

As funções podem ser atribuídas a usuários locais (no nível de 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 desse usuário. Por exemplo, se os usuários de ADGroupA podem localizar dispositivos de gerente e os usuários de ADGroupB podem apagar dispositivos de funcionário, um usuário que pertence a ambos os grupos pode localizar e apagar os dispositivos de gerentes e funcionários.

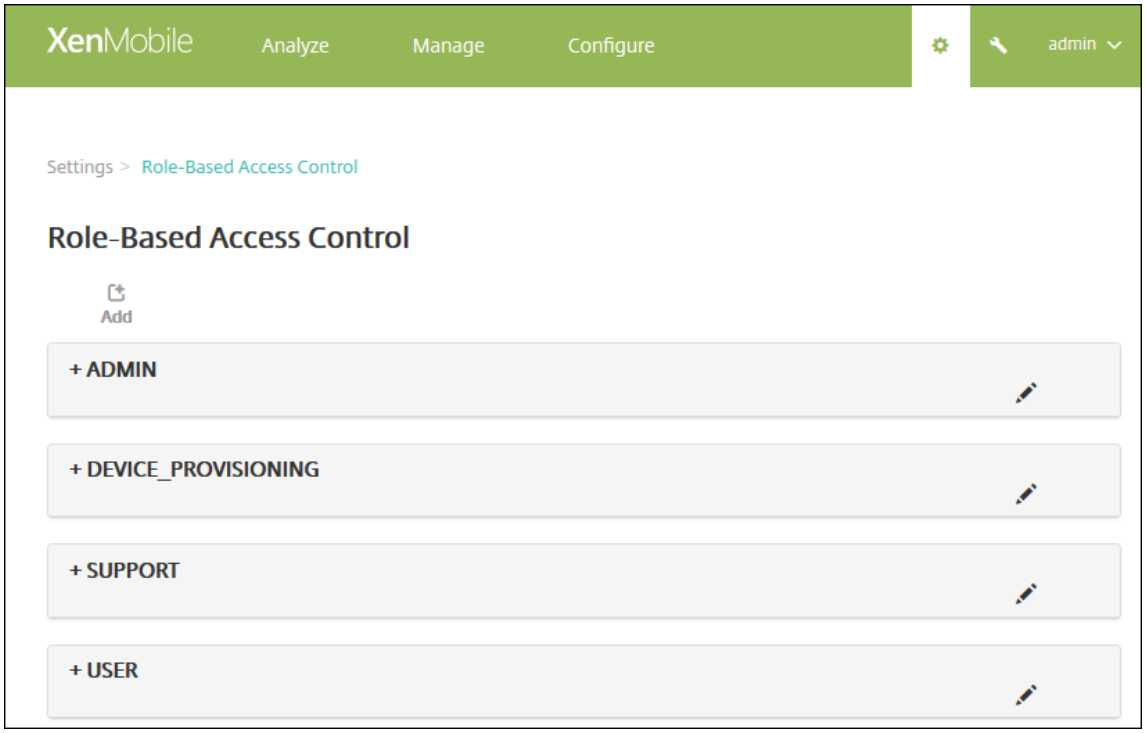
© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Os usuários locais podem ter somente uma função atribuída a eles.

Você pode usar o recurso RBAC no XenMobile para fazer o seguinte:

- Criar uma nova função.
- Adicionar grupos a uma função.
- Associar os usuários locais a funções.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Controle de acesso baseado em função**. A página **Controle de acesso com base na função** é exibida, exibindo as quatro funções de usuário padrão e as funções adicionadas anteriormente.



   Se você clicar no sinal de mais (+) ao lado de uma função, a função se expande para mostrar todas as permissões dessa função, conforme mostrado na figura a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



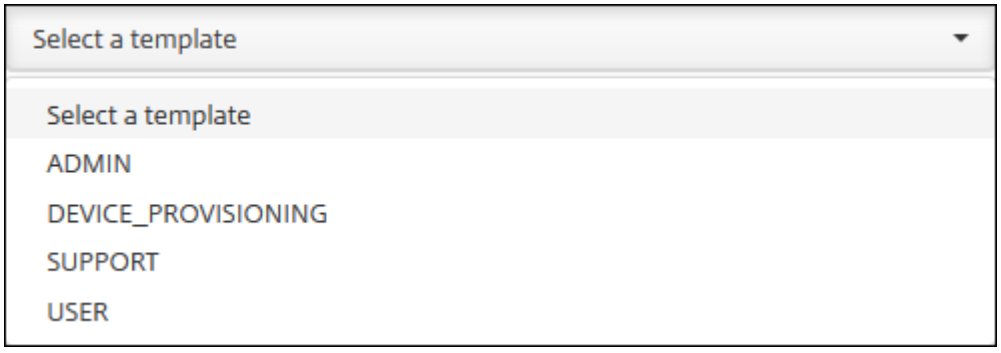
3. Clique em **Adicionar** para adicionar uma nova função do usuário, clique no ícone de caneta à direita de uma função existente para editá-la ou clique no ícone de lixeira à direita de uma função definida anteriormente para excluí-la. Você não pode excluir as funções do usuário padrão.

    - Quando você clica em **Adicionar** ou no ícone de caneta, a página **Adicionar função** ou **Editar função** é exibida.
    - Quando você clica no ícone de lixeira, uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para remover a função selecionada.

4. Insira as seguintes informações para criar uma nova função do usuário ou para editar uma função do usuário existente:

    - **Nome RBAC:** digite um nome descritivo para a nova função do usuário. Você não pode alterar o nome de uma função existente.
    - **Modelo RBAC:** opcionalmente, clique em um modelo como o ponto de partida para a nova função. Você não poderá selecionar um modelo se estiver editando uma função existente.

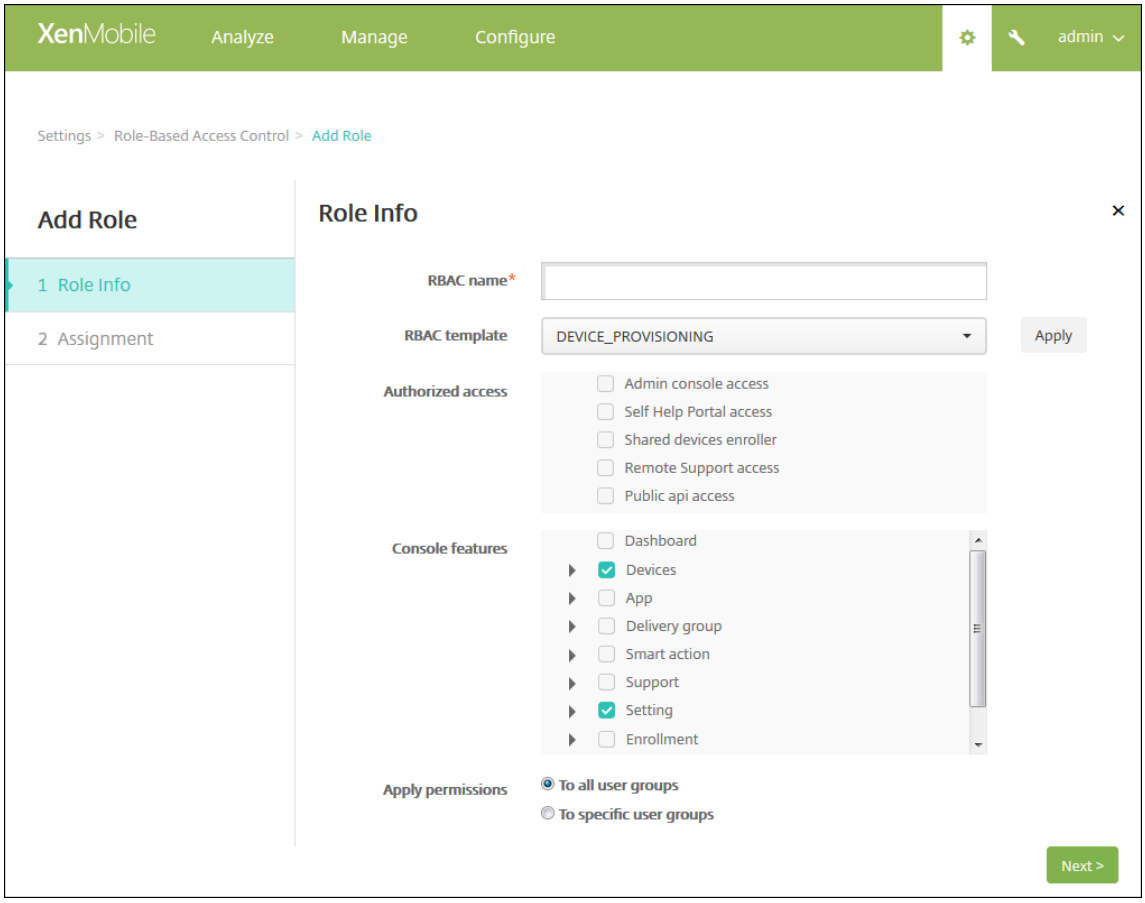
    Os modelos RBAC são as funções do usuário padrão. Eles definem o acesso às funções do sistema que usuários associados a essa função têm. Depois de selecionar um modelo RBAC, você poderá ver todas as permissões associadas a essa função nos campos **Acesso autorizado** e **Recursos do console**. Usando um modelo é opcional; você pode selecionar diretamente as opções que deseja atribuir a uma função nos campos **Acesso autorizado** e **Recursos do console**.



5. Clique em **Aplicar** à direita do campo **Modelo RBAC** para preencher as caixas de seleção **Acesso autorizado** e **Recursos do console** com as permissões de acesso e recurso predefinidas para o

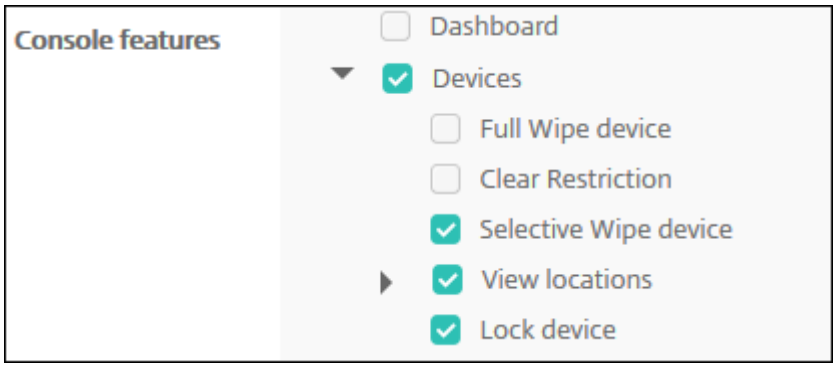
© 1999-2019 Citrix Systems, Inc. All rights reserved.

modelo selecionado.



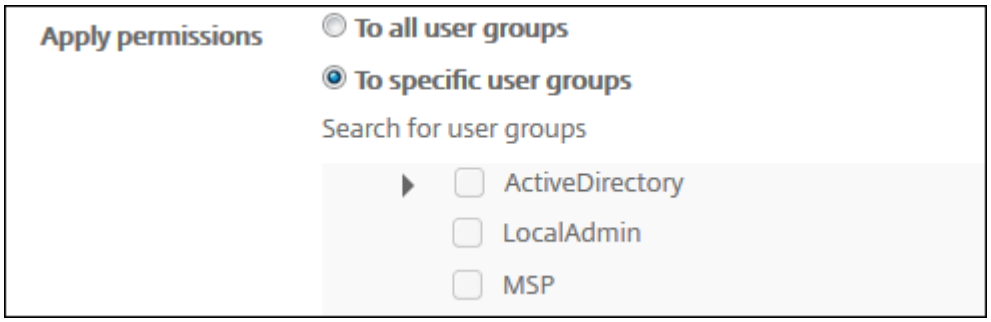
6. Marque e desmarque as caixas de seleção em **Acesso autorizado** e **Recursos do console** para personalizar a função.

   Se você clicar no triângulo ao lado de um recurso do Console, as permissões específicas desse recurso, que você pode selecionar e limpar, serão exibidas. Clicar na caixa de seleção de nível superior proíbe o acesso a essa parte do console; você deve selecionar as opções individuais abaixo do nível superior para ativá-las. Por exemplo, na figura a seguir, as opções **Limpar Dispositivo Total** e **Limpar Restrições** não aparecem no console para usuários atribuídos à função, mas as opções verificadas aparecem.

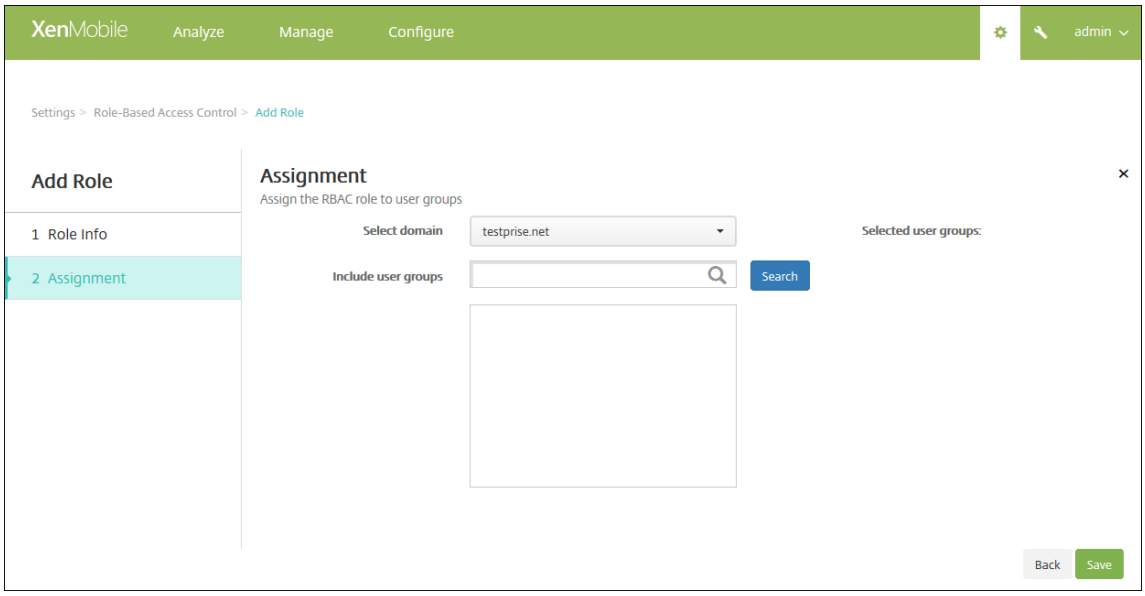


© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. **Aplicar permissões:** selecione os grupos aos quais você deseja aplicar as permissões selecionadas. Se você clicar em **Para grupos de usuários específicos**, será exibida uma lista de grupos a partir da qual você pode selecionar um ou mais grupos.



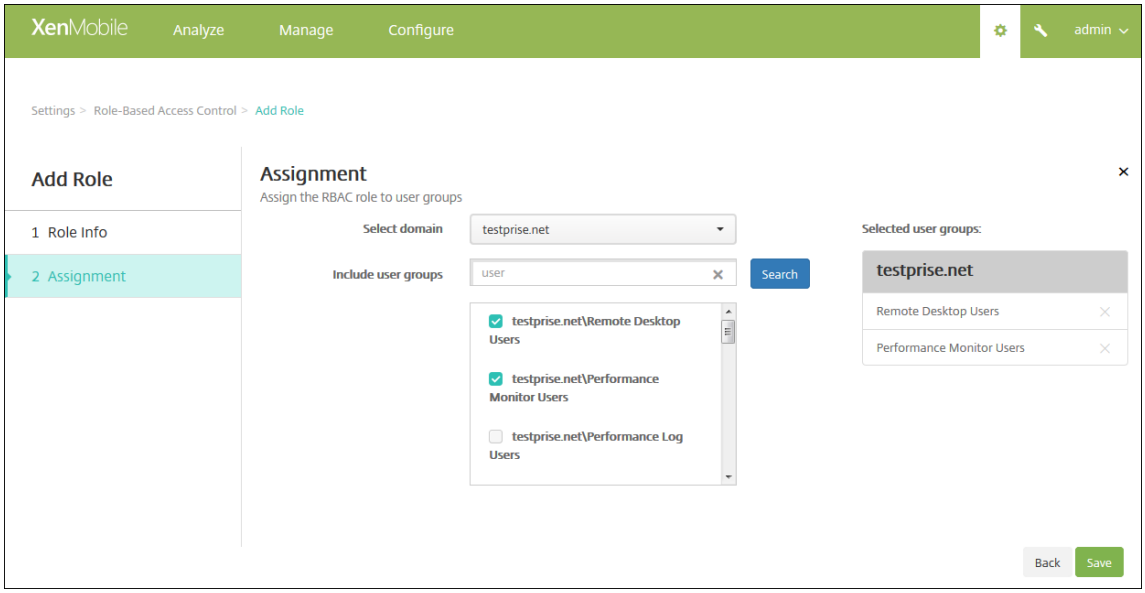
8. Clique em **Avançar**. A página **Atribuições** é exibida.



9. Insira as informações a seguir para atribuir uma função a grupos de usuários.

   - **Selecionar domínio:** na lista, clique em um domínio.
   - **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 a somente grupos com esse nome.
   - Na lista exibida, selecione os grupos de usuários aos quais você deseja atribuir a função. Quando você seleciona um grupo de usuários, o grupo aparece na lista **Grupos de usuários selecionados**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Para remover um grupo de usuários da lista **Grupos de usuários selecionados**, clique no X ao lado do nome do grupo de usuários.

10. Clique em **Salvar**.

Notificações

April 15, 2019

Você pode usar as notificações no XenMobile para os seguintes fins:

- Para se comunicar com grupos selecionados de usuários para uma série de 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 de funcionários etc.
- Para registrar os usuários e os dispositivos deles.
- Para notificar automaticamente os usuários (usando ações automatizadas) quando determinadas condições são atendidas. Por exemplo:
  - Quando o dispositivo de um usuário está prestes a ser bloqueado no domínio corporativo devido a um problema de conformidade.
  - Quando um dispositivo sofreu jailbreak ou root.

Para obter detalhes sobre as ações automatizadas, consulte Ações automatizadas.

Para enviar notificações usando o XenMobile, você deve configurar um gateway e um servidor de notificação. Você pode configurar um servidor de notificação no XenMobile para configurar os servidores

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de gateway de Protocolo SMTP e SMS para enviar notificações de email e mensagem de texto (SMS) aos usuários. Você pode usar as notificações para enviar mensagens por dois canais diferentes: SMTP ou SMS.

- SMTP é um protocolo orientado para conexão e baseado em texto no qual um remetente de email se comunica com um destinatário de email mediante a emissão de cadeias de caracteres de comando e o fornecimento dos dados necessários, geralmente sobre uma conexão de Protocolo TCP. As sessões SMTP consistem em comandos originados de um cliente SMTP (a pessoa que envia a mensagem) e respostas correspondentes do servidor SMTP.
- SMS é um componente do serviço de mensagem de texto de sistemas de comunicação de telefone, Web ou celular. O SMS usa protocolos padronizados de comunicação para possibilitar que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

Você também pode instalar um Gateway de SMS de operadora no XenMobile para configurar notificações que são enviadas por meio de um gateway de SMS de uma operadora. As operadoras usam gateways de SMS para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos padronizados de comunicação para permitir que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

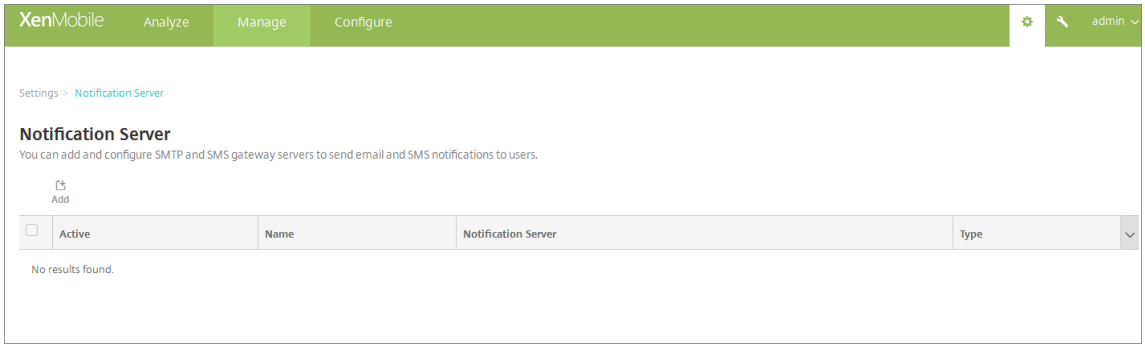
Pré-requisitos

- Antes de configurar o gateway de 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 ele faz parte de um serviço de email hospedado. Nesse caso, você precisa de informações do site do provedor de serviços.
- Configure as notificações do servidor 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 as informações de configuração. Se o servidor for um serviço de email hospedado, localize as informações de configuração adequadas no site do provedor de serviços.
- Somente um servidor SMTP e somente um servidor SMS estão ativos por vez.
- Abra a porta 25 do XenMobile localizado no DMZ da sua rede para apontar de volta para o servidor SMTP na sua rede interna. Isso permite que o XenMobile envie notificações com êxito.

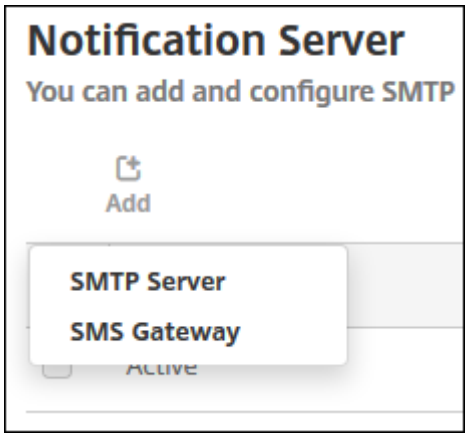
Configurar um servidor SMTP e um gateway de SMS

1. No console 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



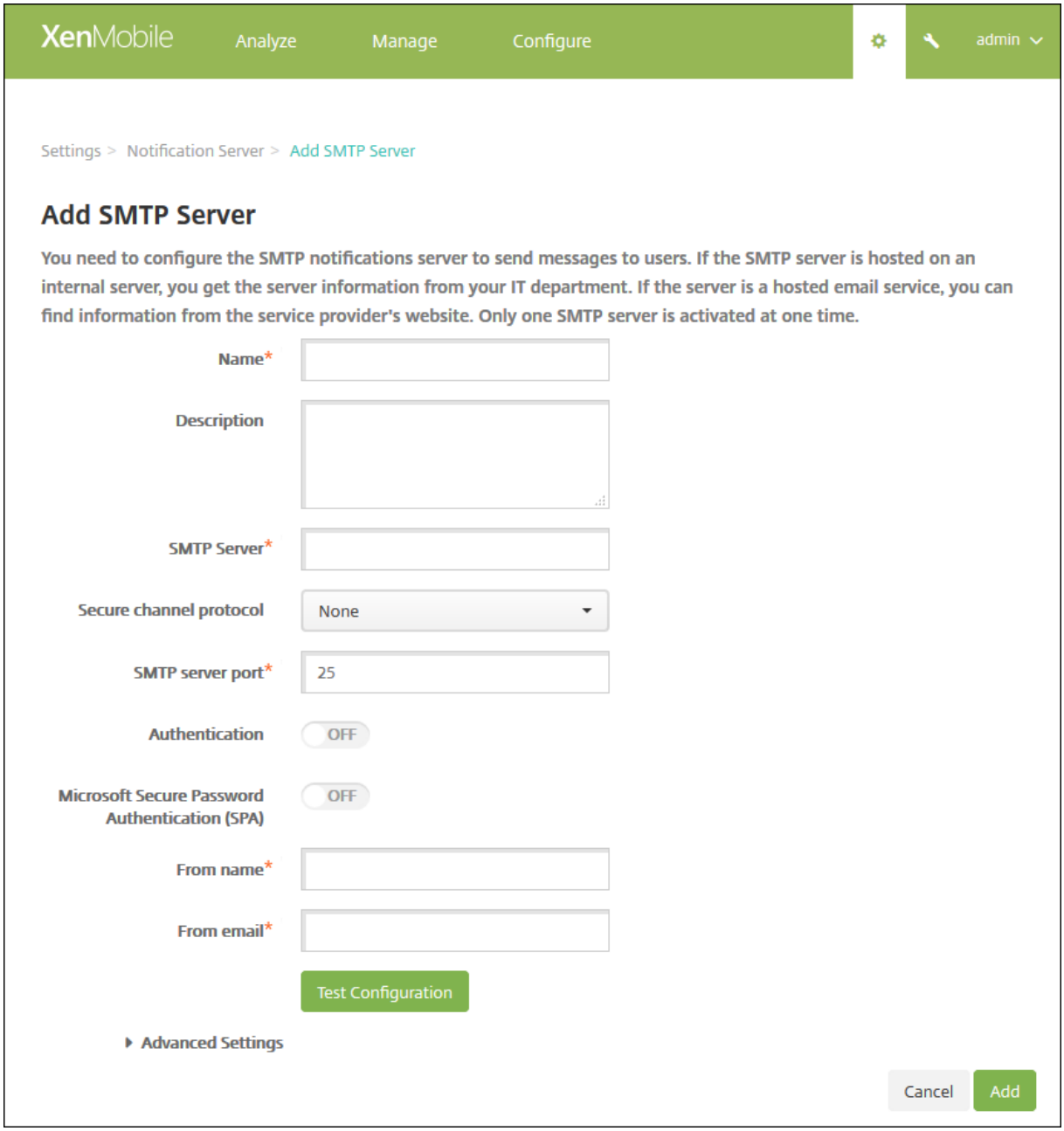
3. Clique em **Adicionar**. Um menu aparece com opções para configurar um servidor SMTP ou um gateway SMS.



- Para adicionar um servidor SMTP, clique em **Servidor SMTP** e, em seguida, consulte Para adicionar um servidor SMTP para ver as etapas para definir essa configuração.
- Para um gateway de SMS, clique em **Gateway de SMS** e consulte Para adicionar um gateway de SMS para ver as etapas para definir essa configuração.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar um servidor SMTP



1. Defina estas configurações:

   - **Nome:** digite o nome associado a essa conta do servidor SMTP.
   - **Descrição:** opcionalmente, insira uma descrição do servidor.
   - **Servidor SMTP:** digite o nome de host do servidor. O nome de host pode ser um nome de domínio totalmente qualificado (FQDN) ou um endereço IP.
   - **Protocolo de canal seguro:** na lista, clique em **SSL**, **TLS** ou **Nenhum** para obter o protocolo de canal seguro usado pelo servidor (se o servidor estiver configurado para usar a

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 canal seguro SSL, a porta será definida como 465.
- **Autenticação:** selecione **I** ou **O**. O padrão é **O**.
- Se você ativar a **Autenticação**, defina estas configurações:
  - **Nome de usuário:** digite o nome do usuário para autenticação
  - **Senha:** insira a senha do usuário de autenticação.
- **Autenticação de senha segura (SPA) da Microsoft:** se o servidor SMTP estiver usando o SPA, clique em **I**. O padrão é **O**.
- **Nome do remetente:** digite o nome exibido na caixa **De** quando um cliente recebe um email de notificação desse servidor. Por exemplo, TI corporativa.
- **Email do remetente:** digite o endereço de email usado se um destinatário de email responder à notificação enviada pelo servidor SMTP.

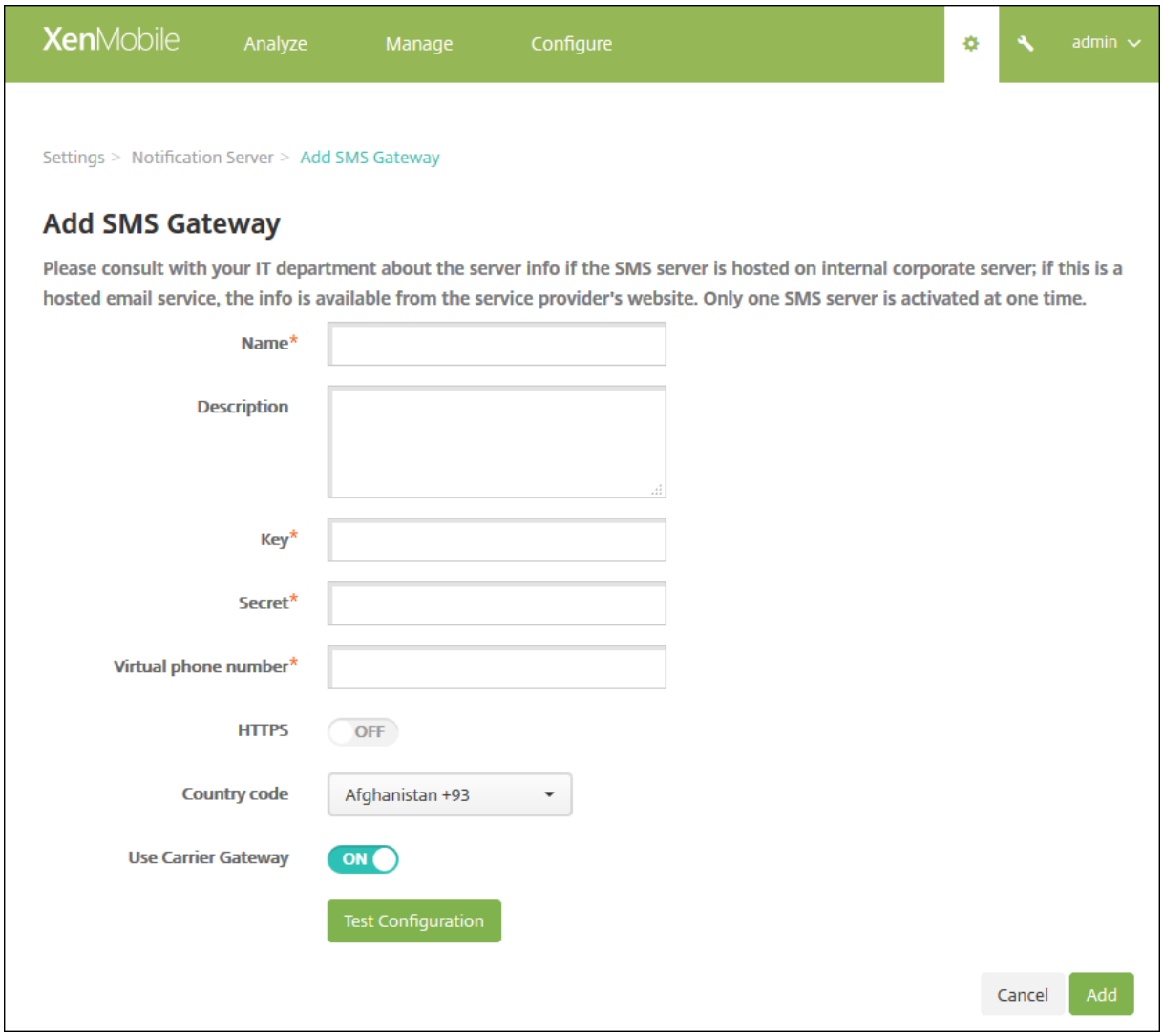
2. Clique em **Testar configuração** para enviar uma notificação de email de teste.
3. Expanda **Configurações avançadas** e defina estas configurações:

   - **Número de novas tentativas de SMTP:** digite o número de novas tentativas para uma mensagem com falha enviada do servidor SMTP. O padrão é 5.
   - **Tempo limite de SMTP:** digite o tempo (em segundos) para aguardar ao enviar uma solicitação SMTP. Aumente esse valor se o envio de mensagens estiver falhando continuamente devido a tempos de espera. Tenha cuidado ao diminuir o valor; ele pode aumentar o número de mensagens não entregues e que atingem o tempo de espera. O padrão é 30 segundos.
   - **Número máximo de destinatários de SMTP:** digite o número máximo de destinatários por mensagem de email enviada pelo servidor SMTP. O padrão é 100.

4. Clique em **Adicionar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar um gateway SMS



> Nota:
>
> O XenMobile é compatível somente com mensagens SMS Nexmo. Se você ainda não tiver uma conta para usar as mensagens Nexmo, visite o site para criar uma.

1. Faça as seguintes configurações:
   - **Nome:** digite um nome para a configuração de Gateway de 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 caso uma senha seja perdida ou roubada. Este campo é obrigatório.
   - **Número de telefone virtual:** esse campo é usado durante o envio para números de tele-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

fone da América do Norte (com o prefixo +1). Você deve digitar um número de telefone virtual Nexmo e você deve usar apenas dígitos neste campo. Você pode comprar números de telefone virtual no site do Nexmo.

- **HTTPS:** selecione se HTTPS deve ser usado para transmitir solicitações SMS para o Nexmo. O padrão é **O**.

> Importante:
>
> Mantenha o HTTPS definido como **I**, a menos que você receba instruções do Suporte Citrix para mantê-lo como **O**.

- **Código do país:** na lista, clique no prefixo padrão do código de país do SMS para os destinatários na sua organização. Esse campo sempre começa com o símbolo +. O padrão é **Afeganistão +93**.

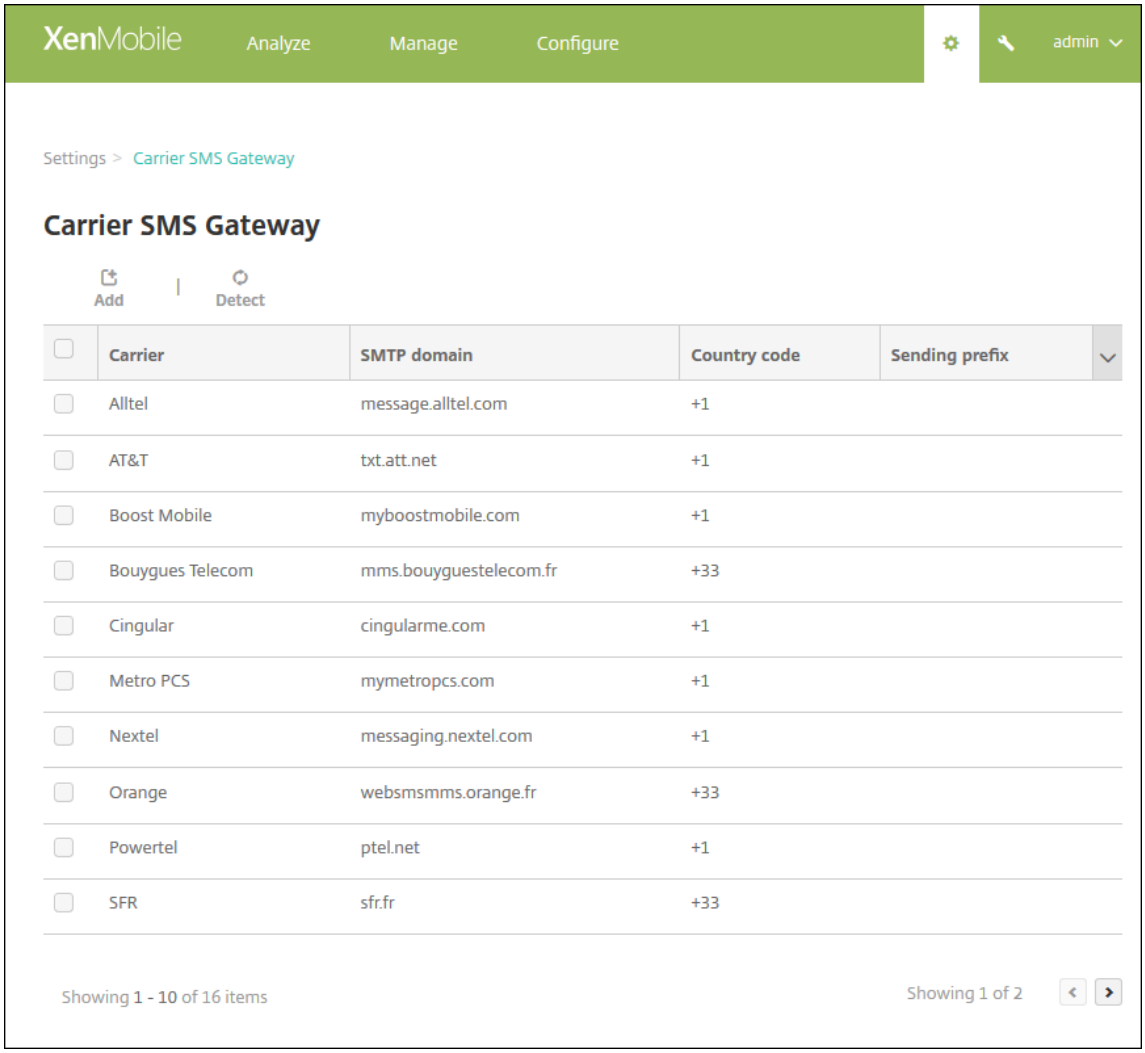
2. Clique em **Testar configuração** para enviar uma mensagem de teste usando a configuração atual. Erros de conexão, como erros de autenticação ou número de telefone virtual, são detectados e exibidos imediatamente. As mensagens são recebidas no mesmo período de tempo que as mensagens enviadas entre celulares.
3. Clique em **Adicionar**.

Adicionar um gateway SMS de operadora

Você pode configurar um Gateway de SMS da Operadora no XenMobile para configurar notificações enviadas usando um gateway de SMS da operadora. As operadoras usam gateways de SMS para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos padronizados de comunicação para permitir que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

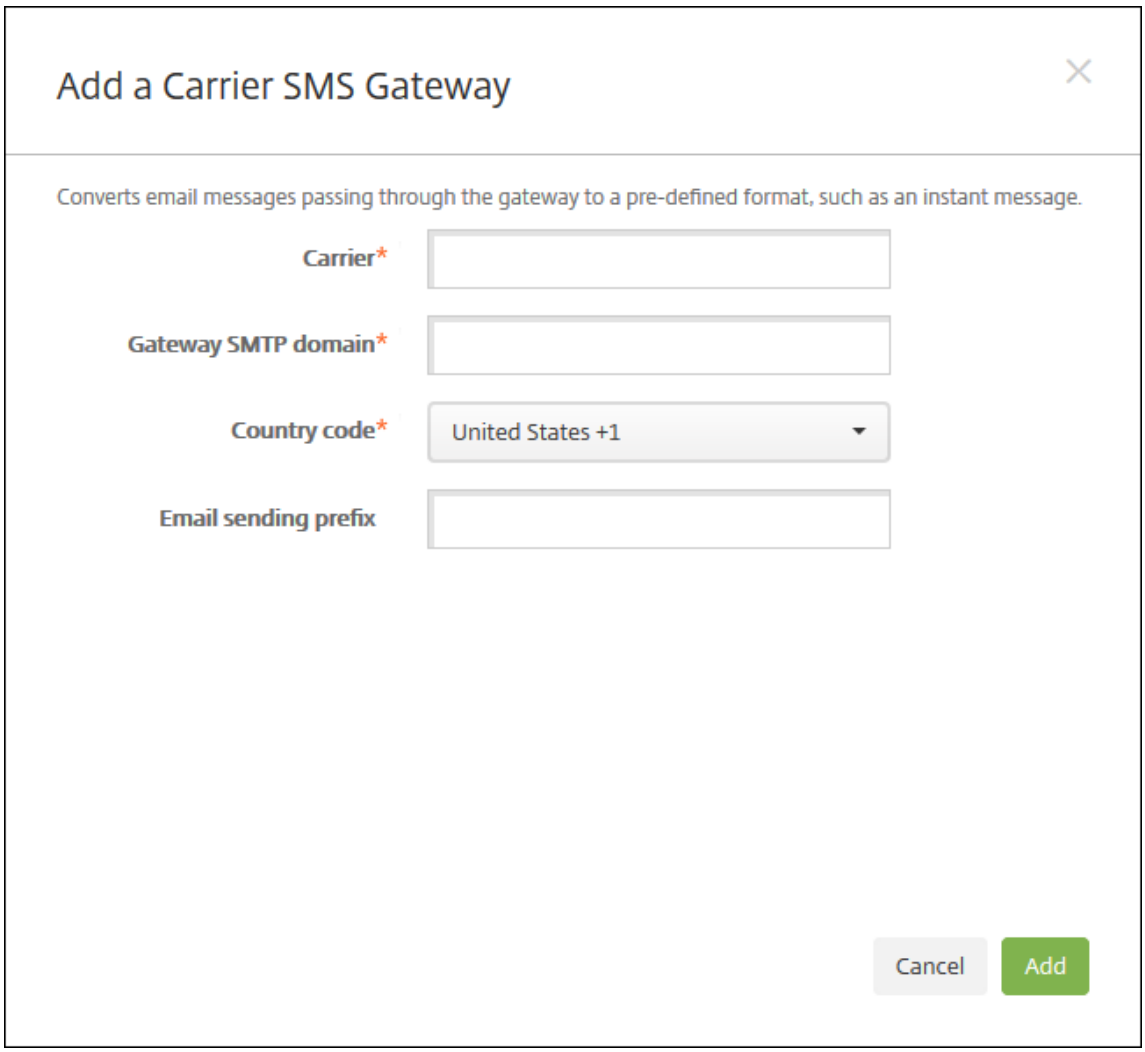
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Notificações**, clique em **Gateway de SMS da operadora**. A página **Gateway de SMS da operadora** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Você pode optar por um dos seguintes procedimentos:
   - Clique em **Detectar** para detectar automaticamente um gateway. Uma caixa de diálogo é exibida para indicar que não há novas operadoras detectadas ou para listar as novas operadoras detectadas entre os dispositivos registrados.
   - Clique em **Adicionar**. A caixa de diálogo **Adicionar um Gateway de SMS de operadora** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> O XenMobile é compatível somente com mensagens SMS Nexmo. Se você ainda não tiver uma conta para usar as mensagens Nexmo, visite o site para criar uma.

4. Defina estas configurações:
   - **Operadora:** digite o nome da operadora.
   - **Domínio SMTP de gateway:** Digite o domínio associado ao gateway de SMTP.
   - **Código do país:** na lista, clique no código do país da operadora.
   - **Prefixo de envio de email:** opcionalmente, especifique um prefixo de envio de email.
5. Clique em **Adicionar** para adicionar a nova operadora ou em **Cancelar** para não adicionar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

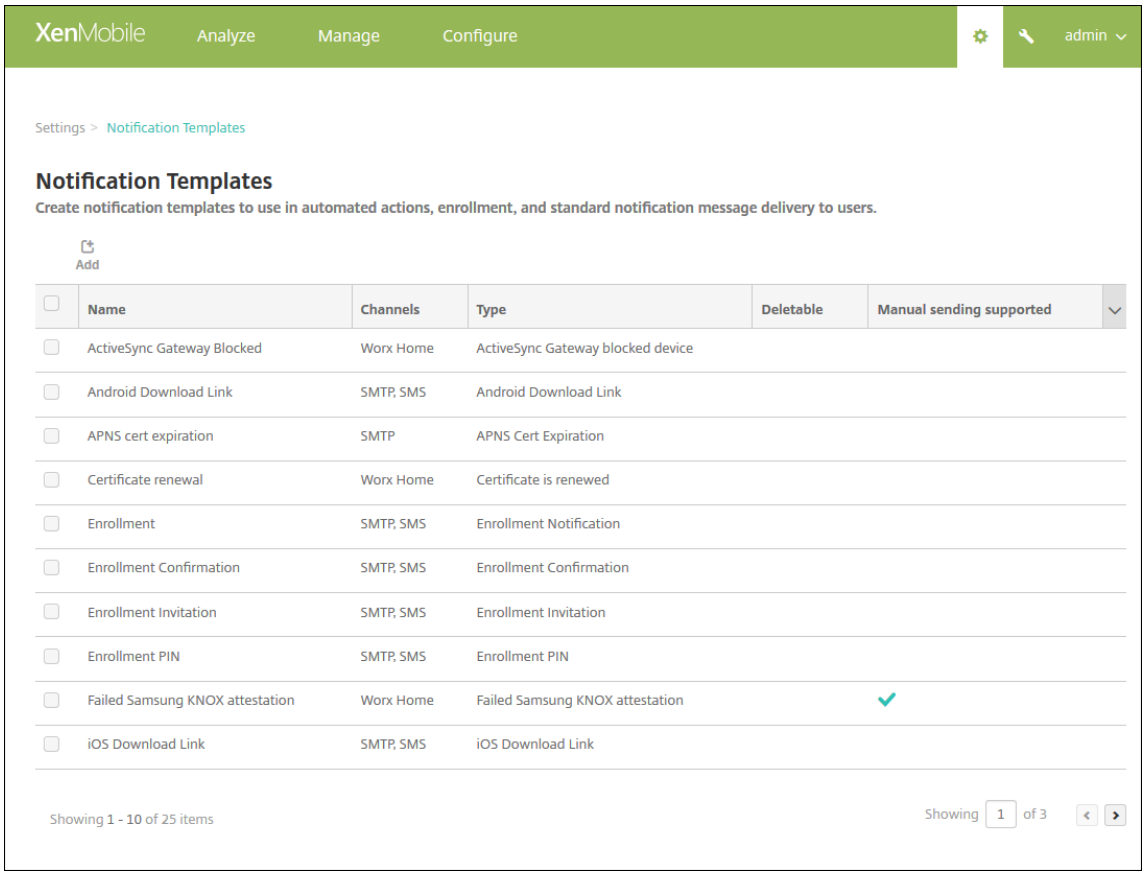
Criar e atualizar modelos de notificação

Você pode criar ou atualizar modelos de notificação no XenMobile para que sejam usados em ações automatizadas, registros e mensagens de notificação padrão enviadas para os usuários. Configure os modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS.

O XenMobile inclui vários modelos de notificação predefinidos que refletem os tipos diferentes de eventos aos quais o XenMobile responde automaticamente para cada dispositivo no sistema.

> Nota:
>
> Se planeja usar canais SMTP ou SMS para enviar notificações aos usuários, você deverá configurar os canais antes que possa ativá-los. O XenMobile solicita que você configure os canais ao adicionar modelos de notificação, se eles já não estiverem configurados.

1. No console 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.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar modelo de notificação

1. Clique em **Adicionar**. Se nenhum gateway de SMS ou servidor SMTP tiver sido configurado, uma mensagem será exibida em relação ao uso de notificações SMS e SMTP. Você pode optar por configurar o servidor SMTP ou o gateway de SMS agora ou mais tarde.

   Se você optar por definir as configurações do servidor SMTP ou SMS agora, será redirecionado para a página **Servidor de notificação** na página **Configurações**. Depois de configurar os canais que desejar usar, você poderá retornar para a página **Modelo de notificação** para continuar adicionando ou modificando modelos de notificação.

   > Importante:
   >
   > Se você optar por definir as configurações do servidor SMTP ou SMS mais tarde, não conseguirá 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 ao usuário.

2. Defina estas configurações:

   - **Nome:** Digite um nome descritivo para o modelo.
   - **Descrição:** Digite uma descrição para o modelo.
   - **Tipo:** Na lista, clique no tipo de notificação. São exibidos somente os canais para o tipo selecionado. Somente um modelo de tipo de Expiração de certificado APNS é permitido, o que é um modelo predefinido. Isso significa que você não pode adicionar um novo modelo desse tipo.

   > Nota:
   >
   > Para alguns tipos de modelo, a frase "Suporte para envio manual" é exibida 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 usa as seguintes macros no campo Assunto ou Mensagem em qualquer canal:

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

3. Em **Canais**, configure as informações de cada canal a ser usado com essa notificação. Você pode escolher qualquer um ou todos os canais. Os canais que você escolher dependem de como você desejar enviar as notificações:

   - Se você escolher **Secure Hub**, somente os dispositivos Android e iOS receberão as notificações, que serão exibidas na bandeja de notificações do dispositivo.
   - Se você escolher **SMTP**, a maioria dos usuários deverá receber a mensagem, pois eles se registraram com os respectivos endereços de email.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Se você escolher **SMS**, somente os usuários que usam dispositivos com um cartão SIM receberão a notificação.

Secure Hub:

- **Ativar:** clique para ativar o canal de notificação.
- **Mensagem:** digite a mensagem a ser enviada ao usuário. Esse campo será obrigatório se você estiver usando o Secure Hub. Para obter informações sobre como usar macros em uma mensagem, consulte Macros.
- **Arquivo de Som**: na lista, clique no som de notificação que o usuário ouvirá quando a notificação for recebida.

SMTP:

- **Ativar:** clique para ativar 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 email ou ambos.
- **Destinatário:** esse campo contém uma macro pré-integrada para todas as notificações, exceto Ad-Hoc, para garantir que elas sejam enviadas para o endereço correto do destinatário de SMTP. A Citrix recomenda que você não modifique as macros em modelos. Você também pode acrescentar destinatários (por exemplo, o administrador corporativo), além do usuário mediante a adição dos respectivos endereços separados por um ponto e vírgula (;). Para enviar notificações Ad Hoc, você pode inserir destinatários específicos nessa página ou selecionar dispositivos na página **Gerenciar> Dispositivos** e enviar as 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 ativar o canal de notificação.

  Você pode ativar a notificação SMTP somente depois de configurar o servidor SMTP.

- **Destinatário:** esse campo contém uma macro pré-integrada para todas as notificações, exceto Ad-Hoc, para garantir que elas sejam enviadas para o endereço correto do destinatário de SMS. A Citrix recomenda que você não modifique as 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Clique em **Adicionar**. Quando todos os canais estiverem corretamente configurados, eles serão exibidos nesta ordem na página **Modelos de Notificação**: SMTP, SMS e Secure Hub. Todos os canais que não estiverem configurados corretamente serão exibidos após os canais configurados corretamente.

Editar um modelo de notificação

1. Selecione um modelo de notificação. É exibida a página de edição específica desse modelo, na qual você pode alterar todos os campos, exceto **Tipo**, bem como ativar ou desativar os 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 em **Cancelar** para cancelar a exclusão.

Dispositivos

April 15, 2019

O banco de dados do servidor XenMobile armazena uma lista de dispositivos móveis. Um único número de série ou International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) define exclusivamente cada dispositivo móvel. Para preencher o console 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 dispositivo, consulte Formatos de arquivo de provisionamento do dispositivo posteriormente neste artigo.

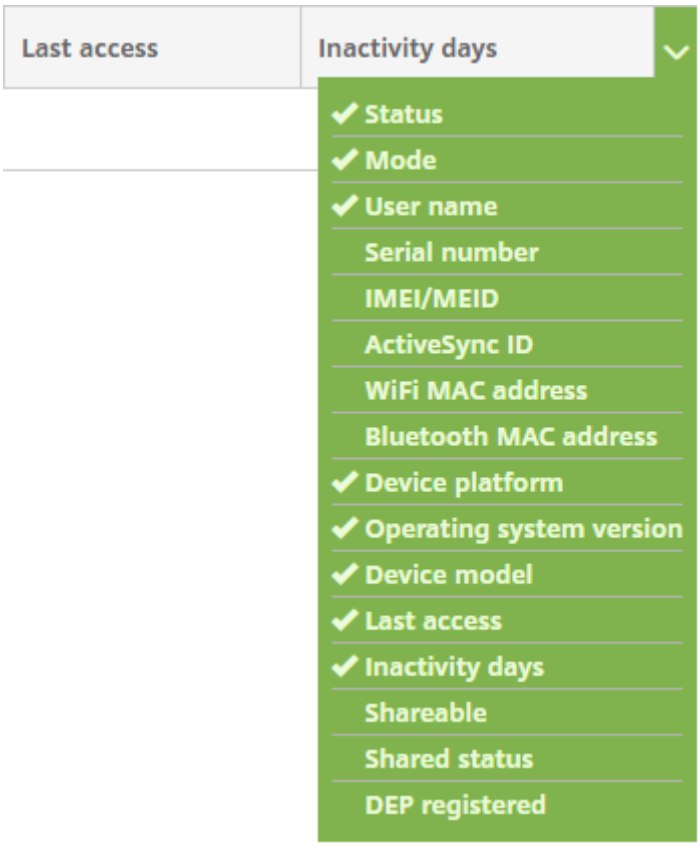
A página **Dispositivos** no console XenMobile lista cada dispositivo e as seguintes informações:

- **Status:** ícones indicam se o dispositivo tiver jailbreak, for gerenciado, se Active Sync Gateway estiver disponível e o estado de implantação.
- **Modo:** se o modo de dispositivo é MDM, MAM ou ambos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Outras informações sobre o dispositivo, como **Nome de usuário**, **Plataforma de dispositivo**, **Versão do sistema operacional**, **Modelo de dispositivo**, **Último acesso** e **Dias de inatividade**. Esses títulos são os padrões mostrados.

Para personalizar a tabela **Dispositivos**, clique na seta para baixo no último cabeçalho. Em seguida, selecione os títulos adicionais que você deseja ver na tabela ou desmarque títulos a serem removidos.



Você pode adicionar dispositivos manualmente, importá-los de um arquivo de provisionamento de dispositivo, editar detalhes do dispositivo, executar ações de segurança e enviar notificações para dispositivos. Você também pode exportar todos os dados da tabela do dispositivo para um arquivo .csv para criar um relatório personalizado. O servidor exporta todos os atributos do dispositivo. Se você aplicar filtros, o XenMobile os usará ao criar o arquivo .csv.

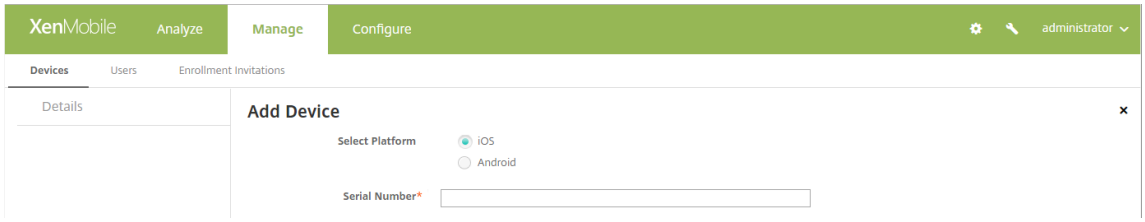
Adicionar um dispositivo manualmente

1. No console XenMobile, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Clique em **Adicionar**. A página **Adicionar dispositivo** é exibida.



3. Defina estas configurações:

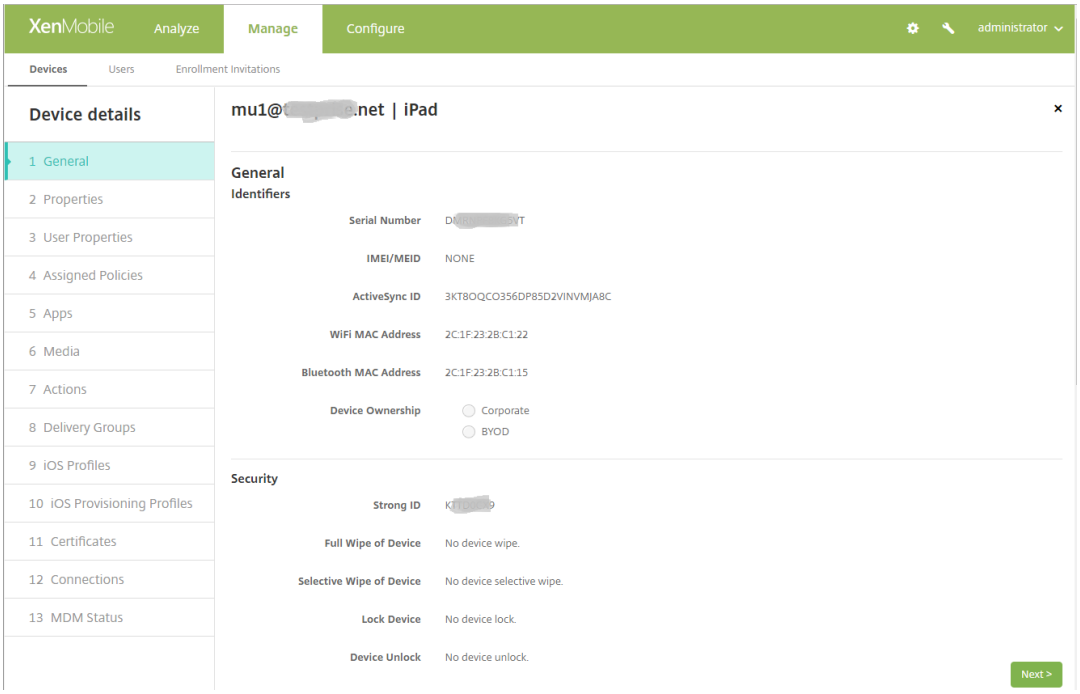
   - **Selecionar plataforma:** Clique em **iOS** ou **Android**.
   - **Número de série:** digite o número de série do dispositivo.
   - **IMEI/MEID:** como opção, somente para dispositivos Android, digite as informações de IMEI/MEID do dispositivo.

4. Clique em **Adicionar**. A tabela **Dispositivos** é exibida com o dispositivo adicionado à parte inferior da lista. Escolha o dispositivo que você adicionou e, no menu exibido, clique em **Editar** para exibir e confirmar os detalhes do dispositivo.

   > Nota:
   >
   > Quando você marca 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 da lista, o menu de opções é exibido no lado direito da listagem.

   - XenMobile Server configurado no modo Empresarial (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 são associados a grupos locais.
   - Se estiver usando o Active Directory:
     - Grupos de entrega são associados a grupos do Active Directory.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. A página **Geral** lista **identificadores** de dispositivo, como o 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 propriedades de **segurança**, como ID forte, Bloquear dispositivo, Ignorar bloqueio de ativação e outras informações, para o tipo de plataforma. O campo de **apagamento completo do dispositivo** inclui o código PIN do usuário. O usuário deve digitar o código depois que o dispositivo for apagado. Se o usuário esquecer o código, você pode procurá-lo aqui.

6. A página **Propriedades** lista as propriedades de dispositivo que o XenMobile provisionará. Esta lista mostra as propriedades de dispositivo incluídas no arquivo de provisionamento usado para adicionar o dispositivo. Para adicionar uma propriedade, clique em **Adicionar** e, em seguida, selecione uma propriedade na lista. Para obter os valores válidos para cada propriedade, consulte o PDF Nomes de propriedade do dispositivo e os valores.

   Quando você adicionar uma propriedade, ela inicialmente aparece na categoria em que você adicionou. Depois de clicar em **Avançar** e voltar para a página **Propriedades**, a propriedade aparece na lista apropriada.

   Para excluir uma propriedade, passe o mouse sobre a listagem e clique no **X** à direita. XenMobile exclui o item imediatamente.

7. As seções restantes de **Detalhes do dispositivo** contêm informações resumidas do dispositivo.

   - **Propriedades do usuário:** exibe funções RBAC, associações de grupo, contas VPP e propriedades do usuário. Você pode desativar uma conta VPP nessa página.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

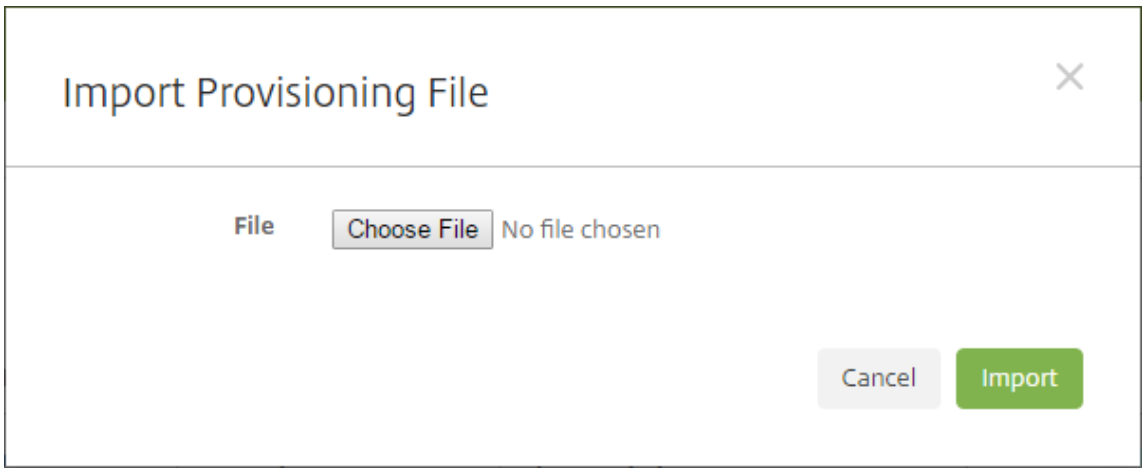
- **Políticas atribuídas:** exibe o número de políticas atribuídas, incluindo o número de políticas implantadas, pendentes e com falha. Fornece o nome da política, tipo e últimas informações de implantação de cada política.
- **Aplicativos:** exibe, para o último inventário, o número de implementações de aplicativo instaladas, pendentes e com falha. Fornece o nome do aplicativo, identificador, tipo e outras informações.
- **Mídia:** exibe, para o último inventário, o número de implementações 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 tempo nome e a implantação do grupo de entrega. Selecione um grupo de entrega para exibir informações mais detalhadas, incluindo status, ação e canal ou usuário.
- **Perfis de iOS:** exibe o último inventário de perfil de iOS, incluindo nome, tipo, organização e descrição.
- **Perfis de provisionamento do iOS:** informações de perfil, como o UUID de provisionamento para distribuição empresarial mostra a data de expiração, e se ele 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 do usuário, penúltimo (próxima ao último) tempo de autenticação e última vez de autenticação.
- **Status de MDM:** exibe informações como o status do MDM, o último envio por push e a hora da última resposta do dispositivo.
- **TouchDown:** (somente dispositivos Android) exibe informações sobre a última autenticação de dispositivo e do último usuário autenticado. Fornece o nome de cada política aplicável valor da política.

Importar dispositivos de um arquivo de provisionamento

Você pode importar um arquivo fornecido por operadoras móveis ou fabricantes de dispositivos, ou pode criar seus próprios arquivos de provisionamento de dispositivo. Para obter detalhes, consulte Formatos de arquivo de provisionamento do dispositivo mais abaixo.

1. Vá até **Gerenciar > Dispositivos** e clique em **Importar**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



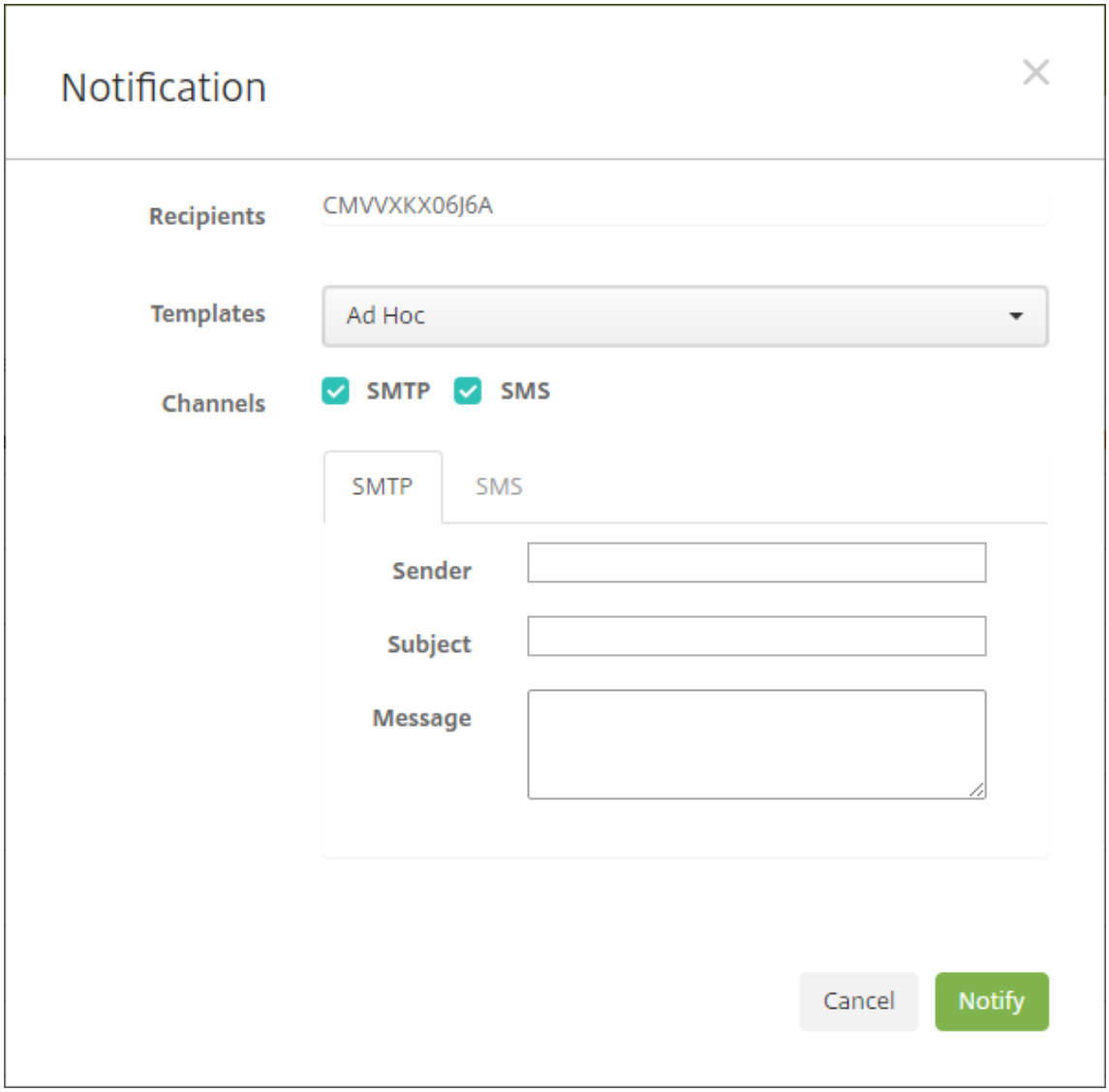
2. Clique em **Escolher Arquivo** e, em seguida, navegue até o arquivo a ser importado.
3. Clique em **Importar**. A tabela de **Dispositivos** contém o arquivo importado.
4. Para editar as informações do dispositivo, selecione-o e, em seguida, clique em **Editar**. Para obter informações sobre as páginas de **Detalhes do dispositivo**, consulte Adicionar um dispositivo manualmente.

Enviar uma notificação para dispositivos

Você pode enviar notificações para os dispositivos da página Dispositivos. Para obter mais informações sobre as 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 devem receber a notificação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Defina 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 guias para ver o formato de mensagem de 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exportar a tabela Dispositivos

1. Filtre a tabela de **Dispositivos** de acordo com o que você deseja exibir no arquivo de exportação.
2. Clique no botão **Exportar** acima da tabela **Dispositivos**. O XenMobile extrai as informações da tabela **Dispositivos** filtrada e converte-as em um arquivo .csv.
3. Quando avisado, abra ou salve o arquivo .csv.

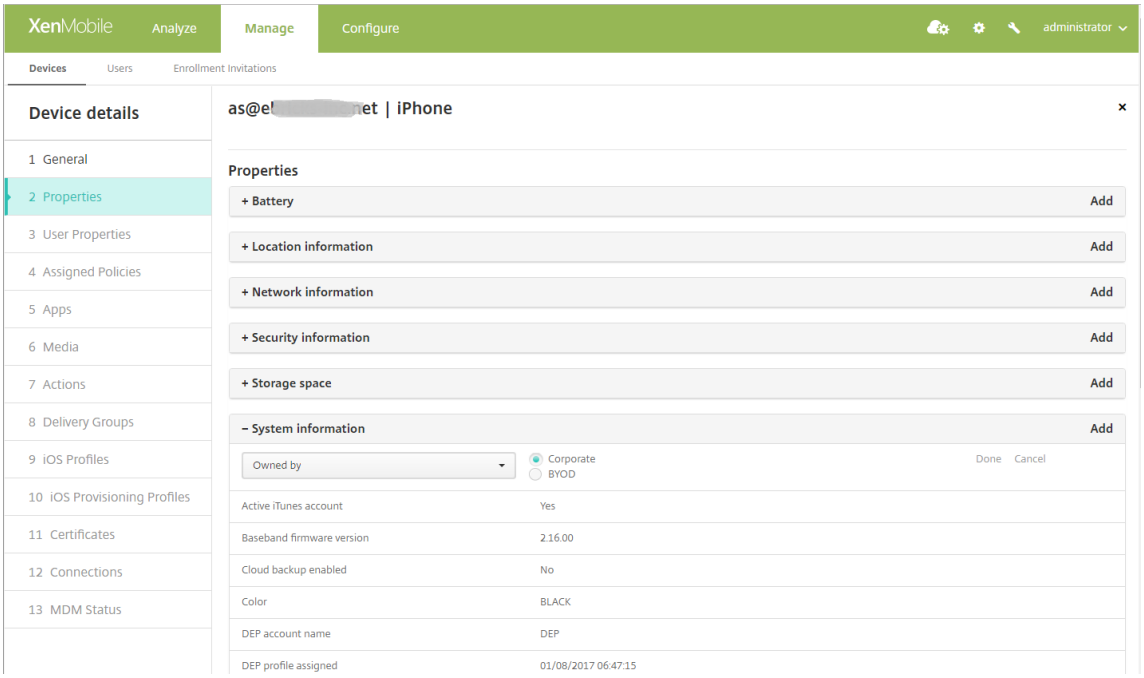
Marcar os dispositivos de usuário manualmente

Você pode marcar manualmente um dispositivo no XenMobile das seguintes maneiras:

- Durante o processo de registro baseado em convite.
- Durante o processo de registro do Portal de Autoajuda.
- Adicionando a propriedade do dispositivo como uma propriedade do dispositivo

Você tem a opção de marcar o dispositivo como de propriedade também da empresa ou do funcionário. Ao usar o Portal de Autoajuda para autorregistrar um dispositivo, você pode marcar o dispositivo como pertencente à empresa ou ao funcionário. Você também pode marcar um dispositivo manualmente, da seguinte maneira.

1. Adicione uma propriedade ao dispositivo da guia **Dispositivos** no console XenMobile.
2. Adicione a propriedade chamada **Propriedade de** e escolha **Empresa** ou **BYOD** (propriedade do funcionário).



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Formatos de arquivo de provisionamento do dispositivo

Muitas operadoras móveis ou fabricantes de dispositivos fornecem listas de dispositivos móveis autorizados. Você pode usar essas listas para evitar a necessidade de inserir manualmente uma longa lista de dispositivos móveis. O XenMobile é compatível com um formato de arquivo de importação que é comum a todos os três tipos de dispositivos compatíveis: 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 obter os valores válidos para cada propriedade, consulte o PDF Nomes de propriedade do dispositivo e os valores.
- Use o conjunto de caracteres UTF-8.
- Use um ponto e vírgula (;) para separar os campos no arquivo de provisionamento. Se parte de um campo contiver um ponto e vírgula, ele deverá ser antecedido por um caractere de barra invertida (\).

  Por exemplo, para esta propriedade:

  ```
  propertyV;test;1;2
  ```

  Faça da seguinte maneira:

  ```
  propertyV\;test\;1\;2
  ```

- O número de série é necessário para dispositivos iOS porque ele 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 do dispositivo:

```
1 ‘1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;
     propertyV\;test\;1\;2;prop 2
2 2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;
     propertyV$*&&éééétest
3 3050BF3F51730108161006551059039l;35244201625379903;iOS;test;
4 4050BF3F51730108161006551059039l;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;‘
```

Cada linha no arquivo descreve um dispositivo. A primeira entrada no exemplo acima significa o seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- ProertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

ActiveSync Gateway

April 15, 2019

O ActiveSync é um protocolo de sincronização de dados móveis desenvolvido pela Microsoft. O ActiveSync sincroniza dados com dispositivos portáteis e computadores desktop (ou laptop).

Você pode configurar as regras do ActiveSync Gateway no XenMobile. Com base nessas regras, você pode permitir ou negar o acesso dos dispositivos a dados do ActiveSync. Por exemplo, se você ativar a regra Aplicativos Obrigatórios Ausentes, o XenMobile verificará a Política de acesso aos aplicativos dos aplicativos obrigatórios e negará o acesso aos dados do ActiveSync se eles estiverem ausentes. Para cada regra, você poderá escolher a **Permitir** ou **Negar**. A configuração padrão é **Permitir**.

Para obter mais informações sobre a política de dispositivo de Acesso aos aplicativos, consulte Política de dispositivo de acesso aos aplicativos.

O XenMobile é compatível com as seguintes regras:

Dispositivos Anônimos: verifica se um dispositivo está no modo anônimo. Essa verificação estará disponível se o XenMobile não conseguir autenticar novamente o usuário quando um dispositivo tentar se reconectar.

Erro de atestado de Samsung KNOX: verifica se um dispositivo falhou em uma consulta do servidor de atestado do Samsung KNOX.

Aplicativos proibidos: verifica se um dispositivo tem aplicativos proibidos, conforme definido em uma política de Acesso aos Aplicativos.

Permissão e negação implícitas: essa ação é o padrão para o ActiveSync Gateway. O gateway cria uma Lista de dispositivos de todos os dispositivos que não atendem a qualquer um dos outros critérios de regra do filtro e permite ou nega conexões com base nessa lista. Se nenhuma regra corresponder, o padrão será Permissão Implícita.

Dispositivos inativos: verifica se um dispositivo está inativo conforme definido pela configuração Limite de Dias de Inatividade do dispositivo em Propriedades do Servidor.

Aplicativos obrigatórios ausentes: verifica se um dispositivo não tem os aplicativos obrigatórios, conforme definido em uma política de Acesso aos aplicativos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Aplicativos não sugeridos: verifica se um dispositivo tem aplicativos não sugeridos, conforme definido em uma Política de acesso aos aplicativos.

Senha não compatível: verifica se a senha de usuário está em conformidade. Nos dispositivos Android e iOS, o XenMobile pode determinar se a senha no dispositivo no momento está em conformidade com a política de código secreto enviada para o dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de código secreto para o dispositivo. Antes que o usuário defina a senha, o código secreto pode não estar em conformidade.

Dispositivos sem conformidade: verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Sem Conformidade. Essa propriedade normalmente é alterada pelas ações automatizadas ou por um terceiro que aproveita as APIs do XenMobile.

Status revogado: verifica se o certificado do dispositivo foi revogado. Um dispositivo revogado não pode se registrar novamente até que tenha autorização novamente.

Dispositivos Android com root e iOS com jailbreak: verifica se um dispositivo Android ou iOS tem jailbreak.

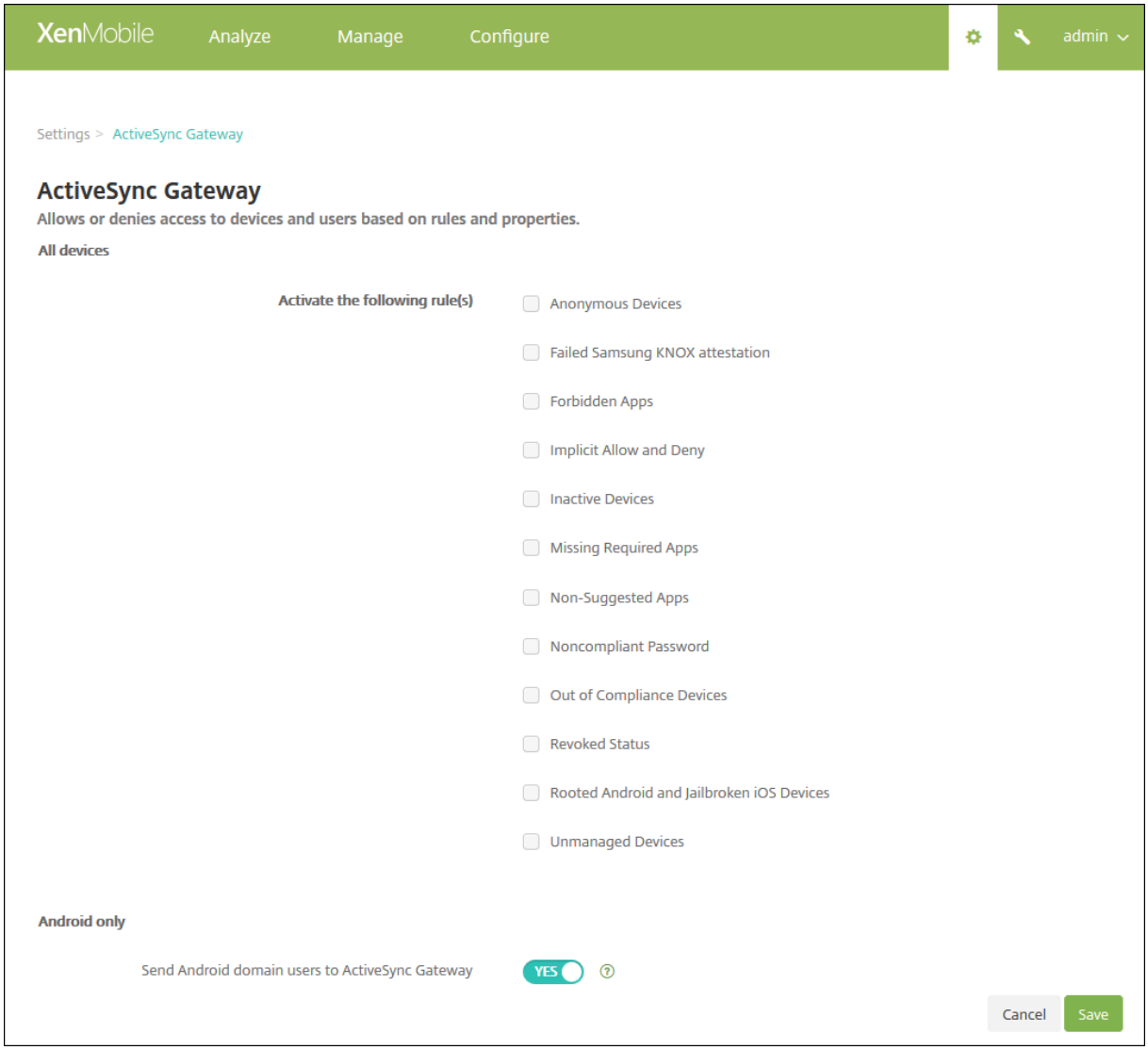
Dispositivos não gerenciados: verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo que está em execução no modo MAM ou um dispositivo não registrado não é gerenciado.

Enviar usuários de domínio do Android para o ActiveSync Gateway: clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o ActiveSync Gateway.

Para definir as configurações do ActiveSync Gateway

1. No console 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



1. Em **Ativar as regras a seguir**, selecione uma ou mais regras que você desejar ativar.
2. Em **Somente Android**, em **Enviar usuários de domínio do Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o ActiveSync Gateway.
3. Clique em **Salvar**.

Android for Work

April 15, 2019

O Android for Work (Android Enterprise) é um espaço de trabalho seguro disponível em dispositivos Android que executam o Android 5.0 e versões posteriores. O espaço de trabalho isola contas comerciais, aplicativos e dados de contas pessoais, aplicativos e dados. No XenMobile, você gerencia

© 1999-2019 Citrix Systems, Inc. All rights reserved.

o seu próprio dispositivo (BYOD) e dispositivos Android de propriedade da empresa solicitando aos usuários que criem um perfil de trabalho separado em seus dispositivos. Ao combinar criptografia de hardware com as políticas que você implanta, você separa com segurança as áreas corporativa e pessoal em um dispositivo. Você pode gerenciar ou apagar todos os dados, aplicativos e políticas corporativas remotamente, sem afetar a área pessoal do usuário. Para obter mais informações sobre os dispositivos Android compatíveis, consulte o site Google Android Enterprise.

Você pode usar o Google Play para adicionar, comprar e aprovar aplicativos para implantação no espaço de trabalho para o Android for Work em um dispositivo. Você pode usar o Google Play para implantar os seus aplicativos Android privados, além de aplicativos públicos e de terceiros. Quando você adiciona um aplicativo pago da loja de aplicativos pública ao XenMobile para Android for Work, você pode verificar o status do licenciamento da compra em massa. Esse status é o número total de licenças disponíveis, o número agora em uso e o endereço de email de cada usuário que consome as licenças. Para obter detalhes sobre como adicionar um aplicativo ao XenMobile, consulte Acrescentar um aplicativo de loja de aplicativos pública.

> Nota:
>
> No XenMobile Server e em nossa documentação, fazemos referência ao Android for Work. A terminologia mais recente é Android Enterprise. Para obter detalhes, consulte a Documentação do Android.

Configurar o Android for Work

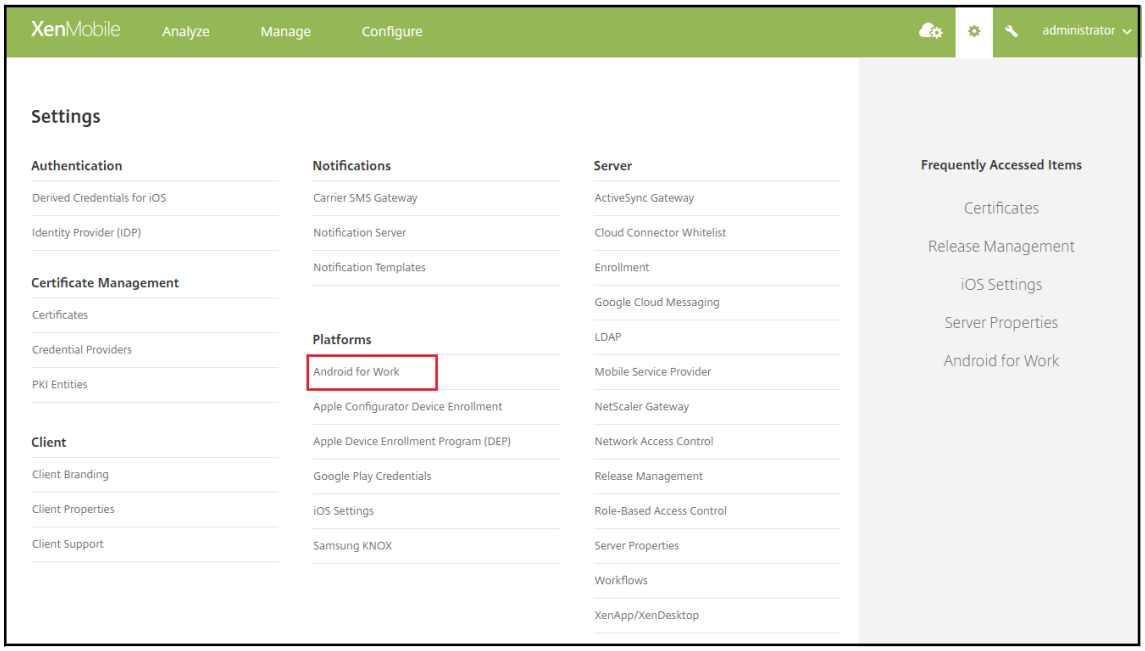
O XenMobile fornece uma maneira simples de configurar o Android for Work para sua organização. Usando as Ferramentas de Gerenciamento do XenMobile, você vincula o XenMobile como seu provedor de gerenciamento de mobilidade empresarial através do Google Play e cria uma empresa para o Android for Work.

> Nota:
>
> Clientes do G Suite, consultem Clientes com Android for Work legado para G Suite, que inclui uma tabela de informações sobre políticas relacionadas.
>
> Você precisará:

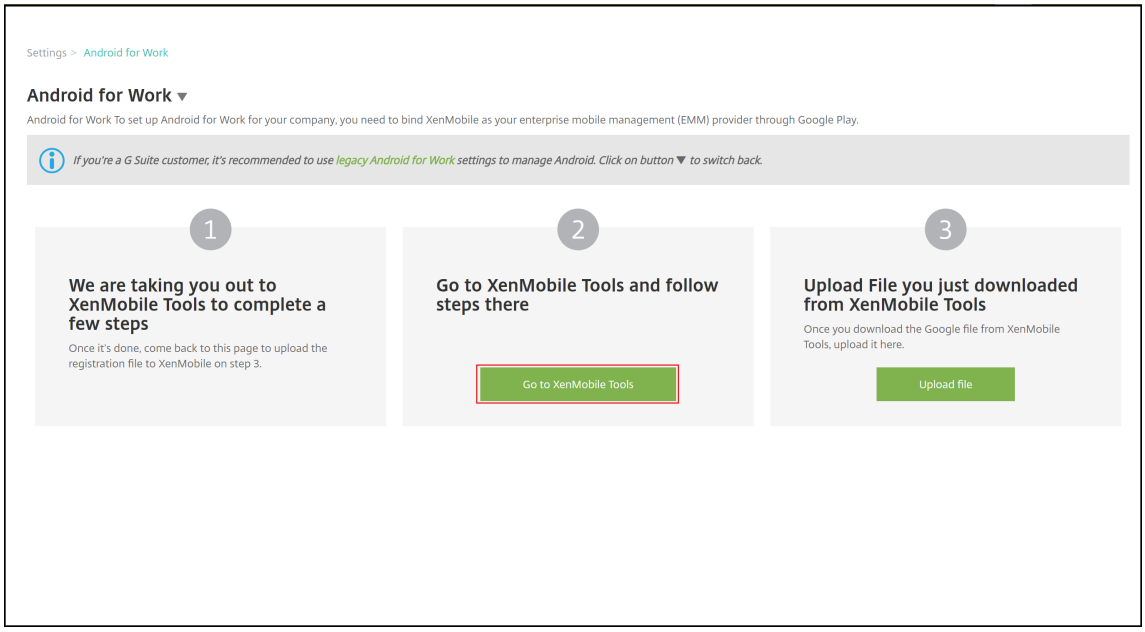
- Suas credenciais de conta da Citrix para fazer logon no XenMobile Tools
- Suas credenciais corporativas de ID do Google para fazer login no Google Play

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Na página **Configurações**, clique em **Android for Work**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

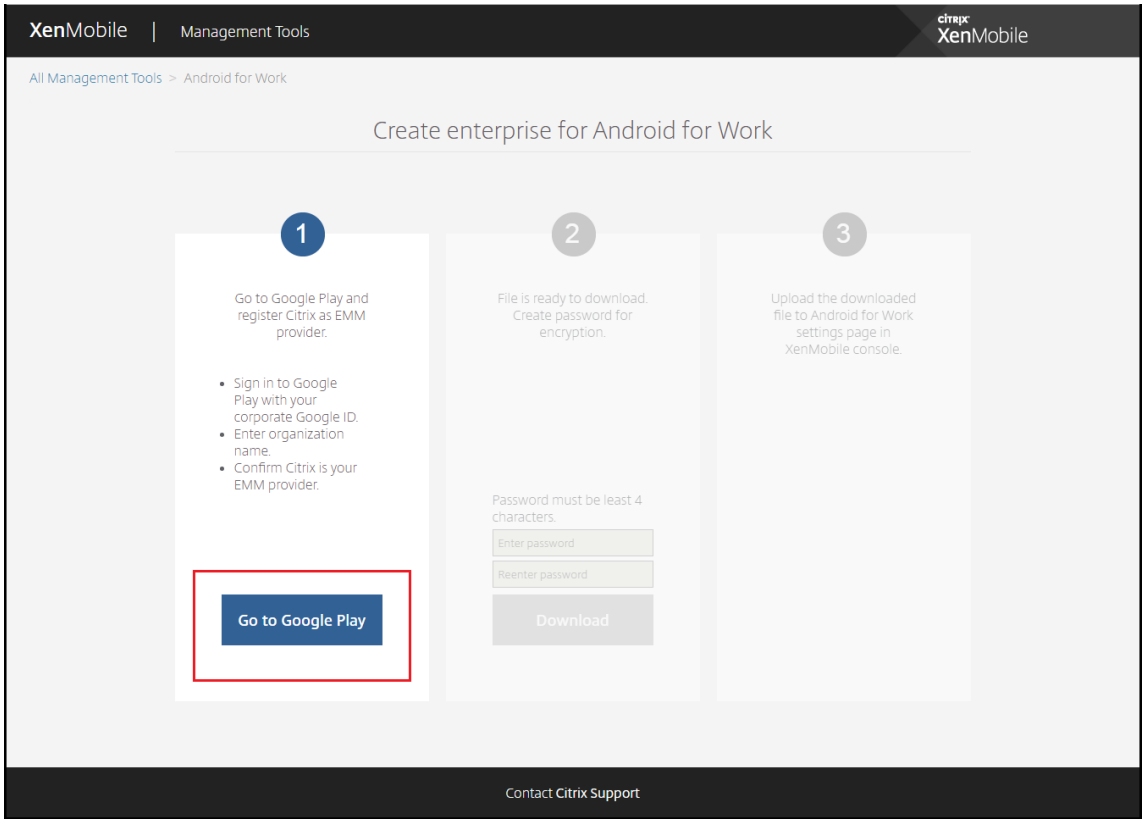


3. Na página **Android for Work**, nas Configurações do XenMobile, clique em **Ir ao XenMobile Tools**.



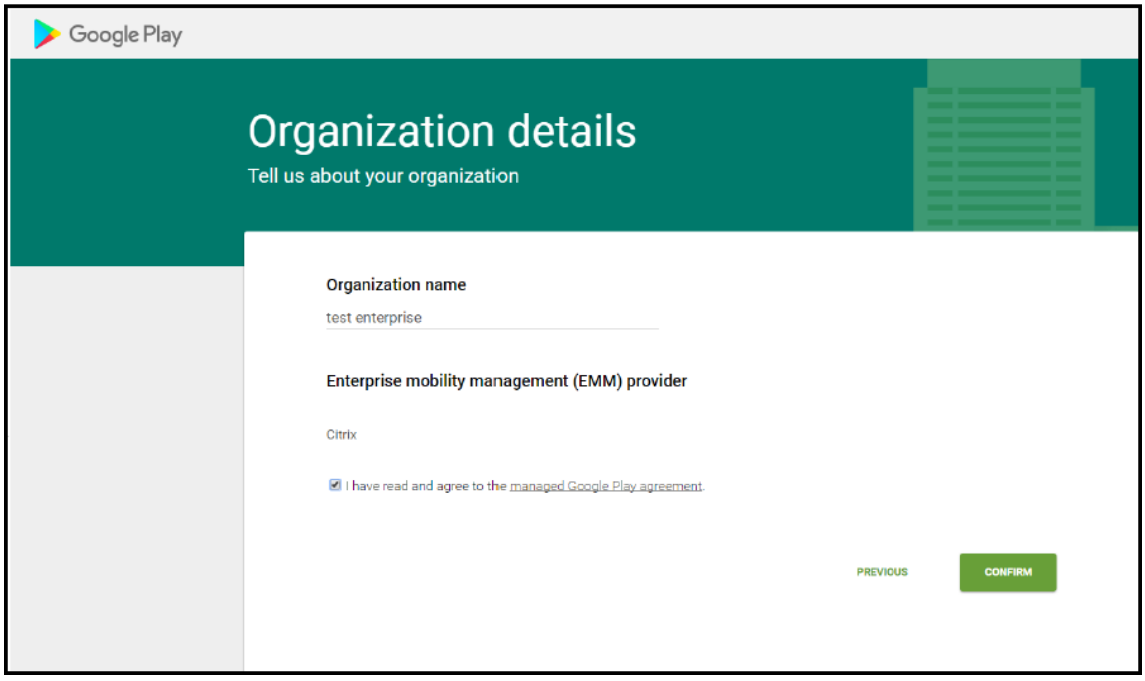
4. Faça logon na sua conta da Citrix, se solicitado.
5. Na página **Android for Work**, no XenMobile Tools Management, clique em **Ir ao Google Play**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. No Google Play, registre a Citrix como o gerenciamento de mobilidade empresarial da sua organização:
    - Digite o nome da sua organização.
    - Verifique se Citrix aparece como o seu gerenciamento de mobilidade empresarial.
    - Aceite os termos e clique em **Confirmar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

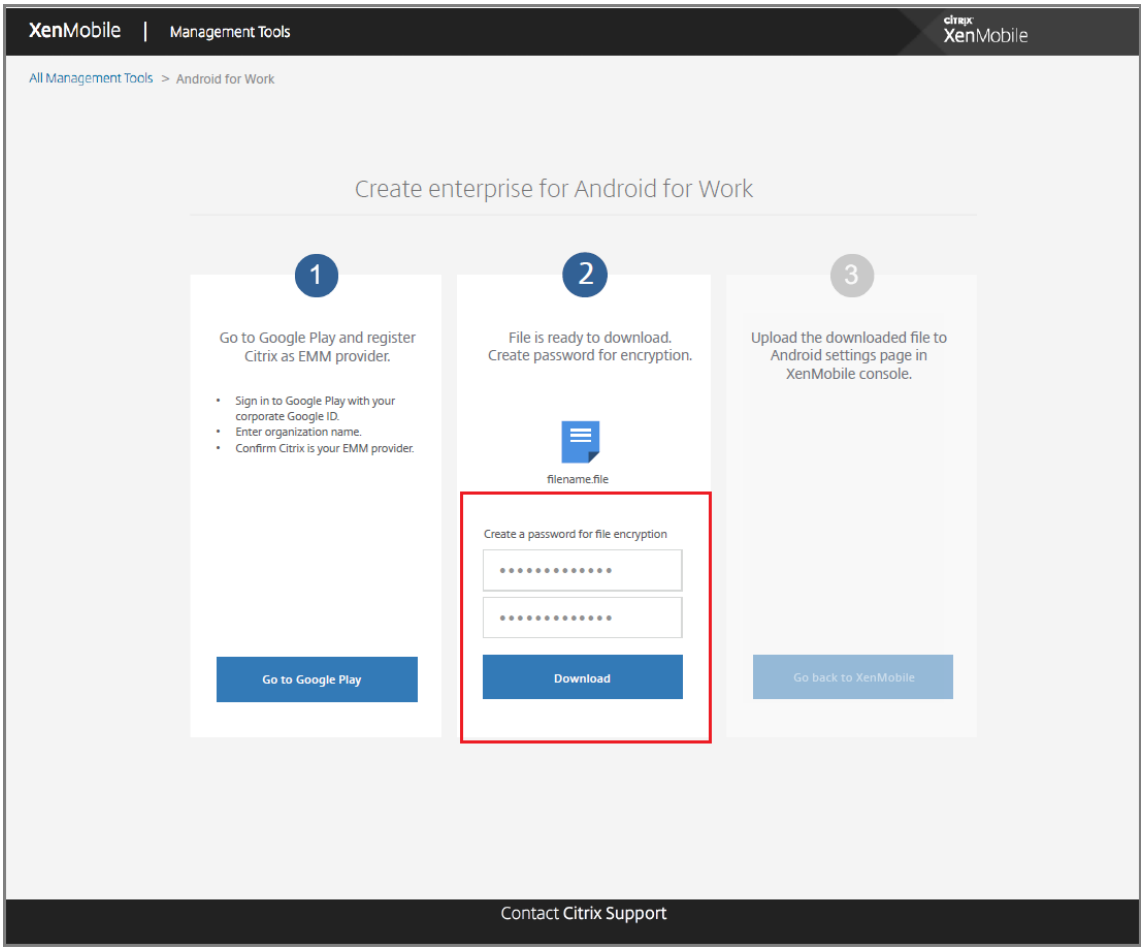


- Na página que é exibida, clique em **Concluir registro**.

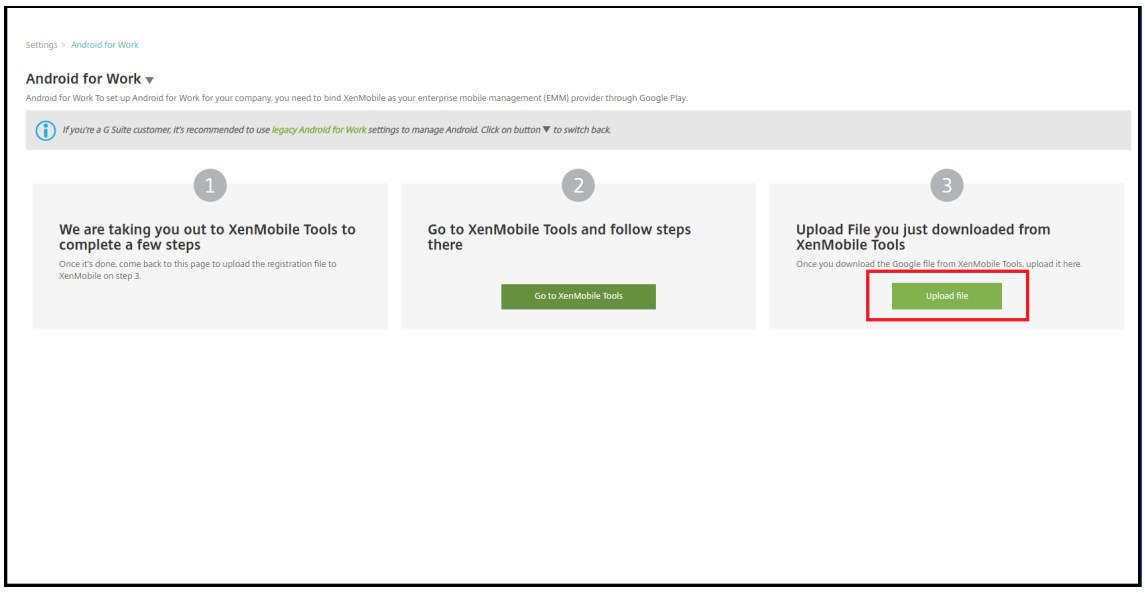
Essa etapa cria um arquivo para você baixar e, em seguida, fazer o upload para o XenMobile.

7. Na página **Android for Work**, no XenMobile Tools Management, clique em **Download**.
8. Crie uma senha para a criptografia de arquivo. Anote a senha para referência ao fazer o upload do arquivo e precisar inserir a senha.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

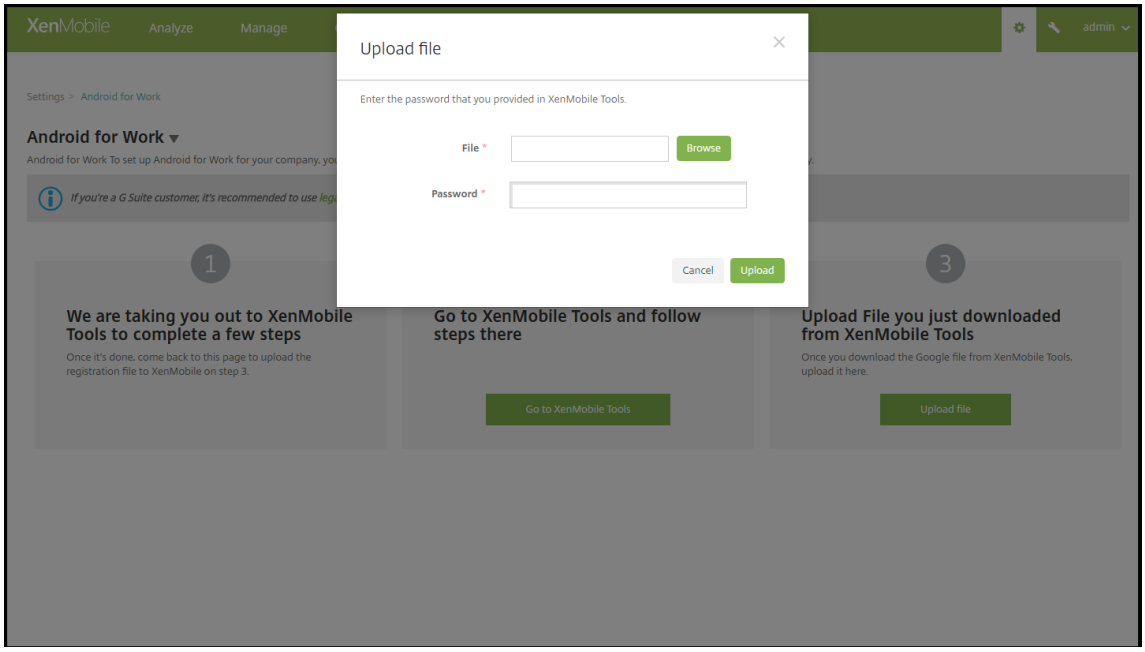


9. Clique em **Voltar ao XenMobile**.
10. Na página Android for Work, nas Configurações do XenMobile, clique em **Carregar arquivo**.

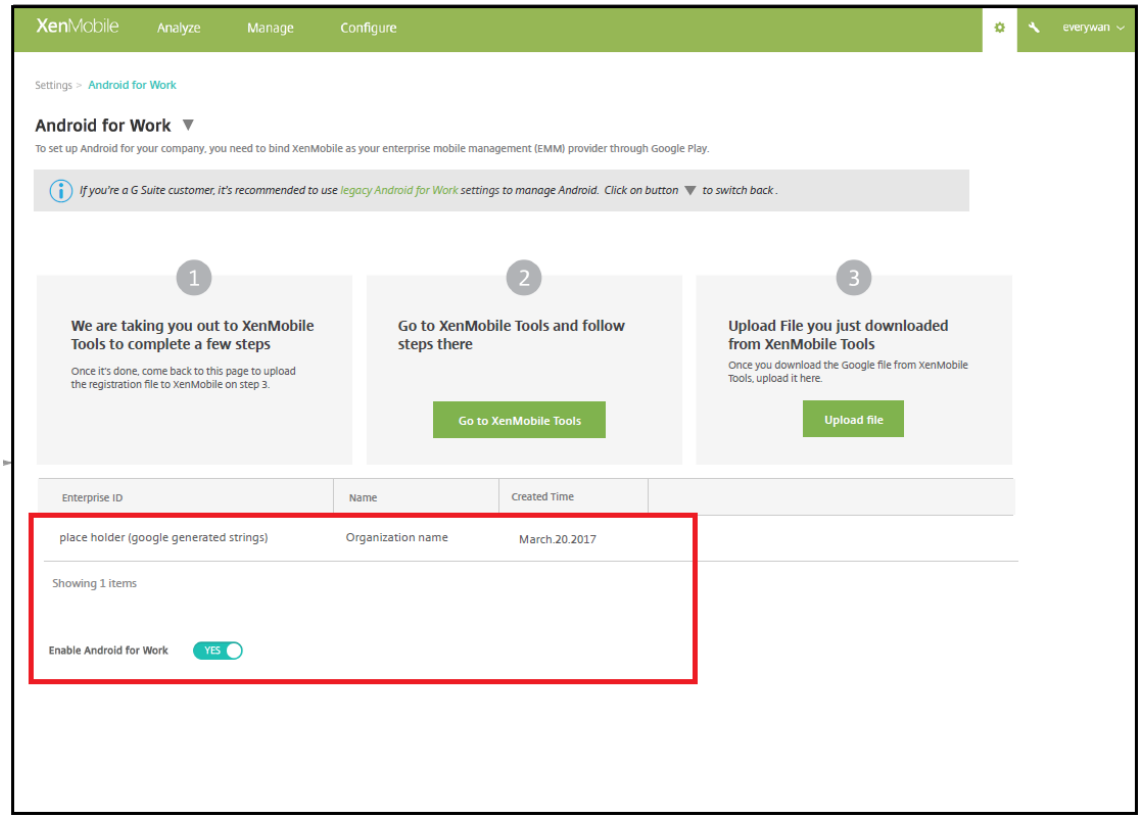


11. Navegue até o arquivo que você baixou e digite a senha criada. Clique em **Carregar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



12. Um ID empresarial é adicionado ao Android for Work. Para ativar o Android for Work, deslize **Ativar Android for Work** para **Sim**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Publicar aplicativos móveis de produtividade para Android for Work

Para publicar aplicativos móveis de produtividade para Android Enterprise, siga as etapas abaixo.

1. Na sua conta gerenciada da Google Play Store, publique os aplicativos que você deseja que seus usuários tenham. Você pode gerenciar sua conta do Google Play em https://play.google.com/work.
2. No console XenMobile, publique os mesmos aplicativos como a seguir:
   a) Selecione aplicativos da loja pública e escolha Android for Work. Para obter mais informações sobre como publicar aplicativos da loja pública, consulte Acrescentar um aplicativo de loja de aplicativos pública.
   b) Publique os aplicativos como aplicativos MDX, para que eles recebam políticas MDX. Para obter mais informações sobre como publicar aplicativos MDX, consulte Acrescentar um aplicativo MDX.

Inscrição de dispositivos Android for Work

Se o processo de inscrição de seu dispositivo exigir que os usuários digitem um nome de usuário ou ID do usuário, o formato aceito depende da forma como o servidor XenMobile está configurado para procurar usuários pelo nome UPN ou pelo nome da conta SAM.

Se o XenMobile Server estiver configurado para procurar usuários por UPN, os usuários devem inserir um UPN no formato:

- *nome de usuário@domínio*

Se o XenMobile Server estiver configurado para procurar usuários por SAM, os usuários devem inserir um SAM em um destes formatos:

- *nome de usuário@domínio*
- *domínio\nome de usuário*

Para determinar para qual tipo de nome de usuário o XenMobile Server está configurado:

1. No console 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, verifique o campo **Pesquisa de usuário por**:
   - Se estiver definido como **userPrincipalName**, o servidor XenMobile estará definido para UPN.
   - Se estiver definido como **sAMAccountName**, o servidor XenMobile estará definido para SAM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cancelar o registro de um Android for Work Enterprise

Você pode cancelar o registro de uma empresa do Android for Work usando o console do XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile Server abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile Server tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista branca de bloqueio de pop-up.

> **Aviso:**
>
> Depois de o registro de um enterprise ser cancelado, os aplicativos Android for Work nos dispositivos já registrados por meio dele são redefinidos para os estados padrão. Os dispositivos não serão mais gerenciados pelo Google. Registrá-los novamente em um enterprise do Android for Workfor pode não restaurar a funcionalidade anterior sem configuração adicional.

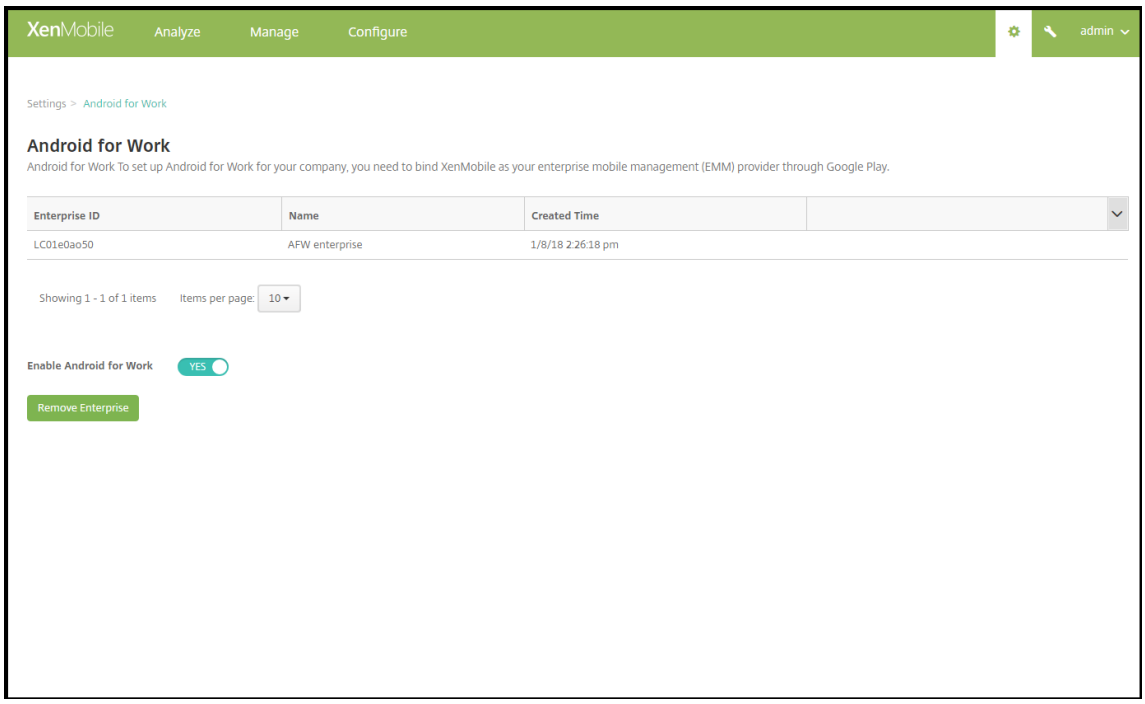
Depois que o registro do enterprise do Android for Work for cancelado:

- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android for Work redefinidos para o estado padrão. As políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work aplicadas anteriormente não afetam mais.
- Os dispositivos registrados por meio do Enterprise são gerenciados pelo XenMobile, mas são não gerenciados pela perspectiva do Google. Nenhum novo aplicativo do Android for Work pode ser adicionado. Não se aplica nenhuma política de Permissões de aplicativos do Android for Work ou de Rrestrições de aplicativos do Android for Work. Outras políticas, como Agendamento, Senha e Restrições, ainda podem ser aplicadas a esses dispositivos.
- Se você tentar registrar dispositivos no Android for Work, eles serão registrados como dispositivos Android, não como dispositivos Android for Work.

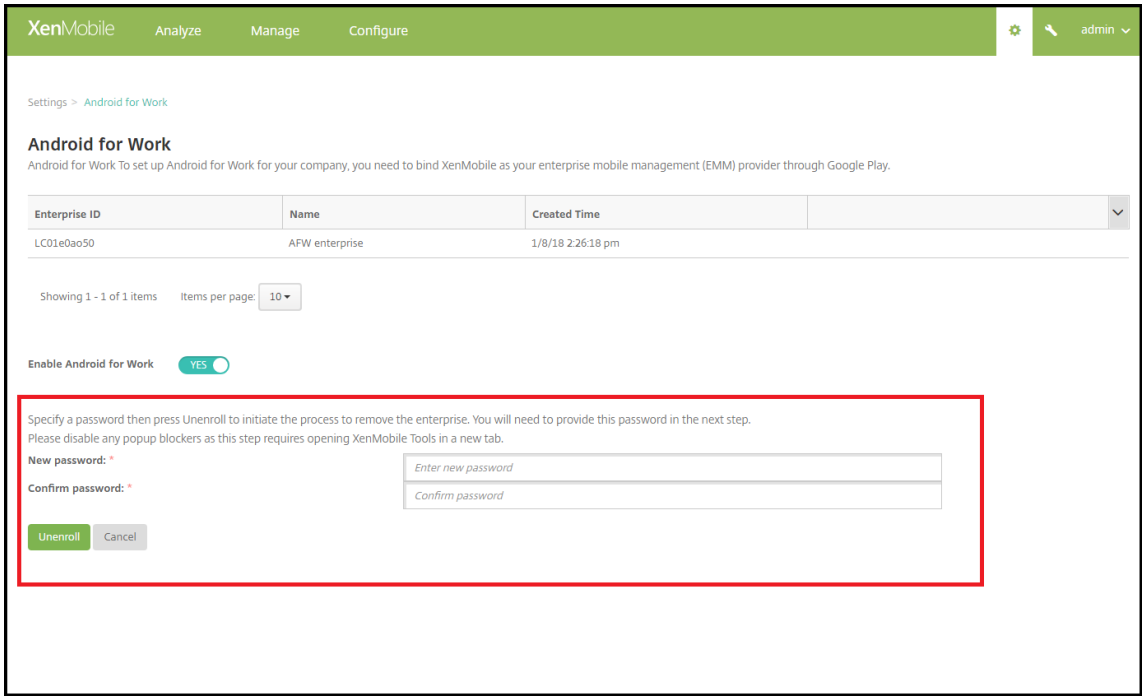
Para cancelar o registro de um Android for Work Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página Configurações é exibida.
2. Na página Configurações, clique em **Android for Work**.
3. Clique em **Remover Enterprise**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

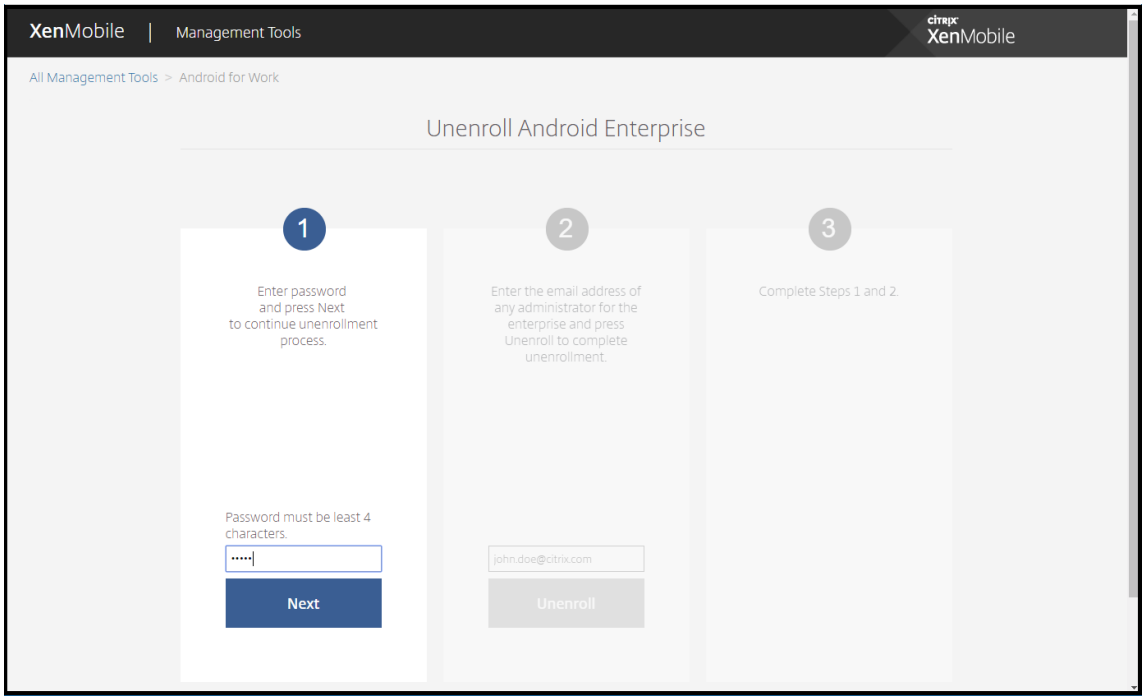


4. Especifique uma senha. Você precisará dela na próxima etapa para concluir o cancelamento do registro. Em seguida, clique em **Cancelar registro**.

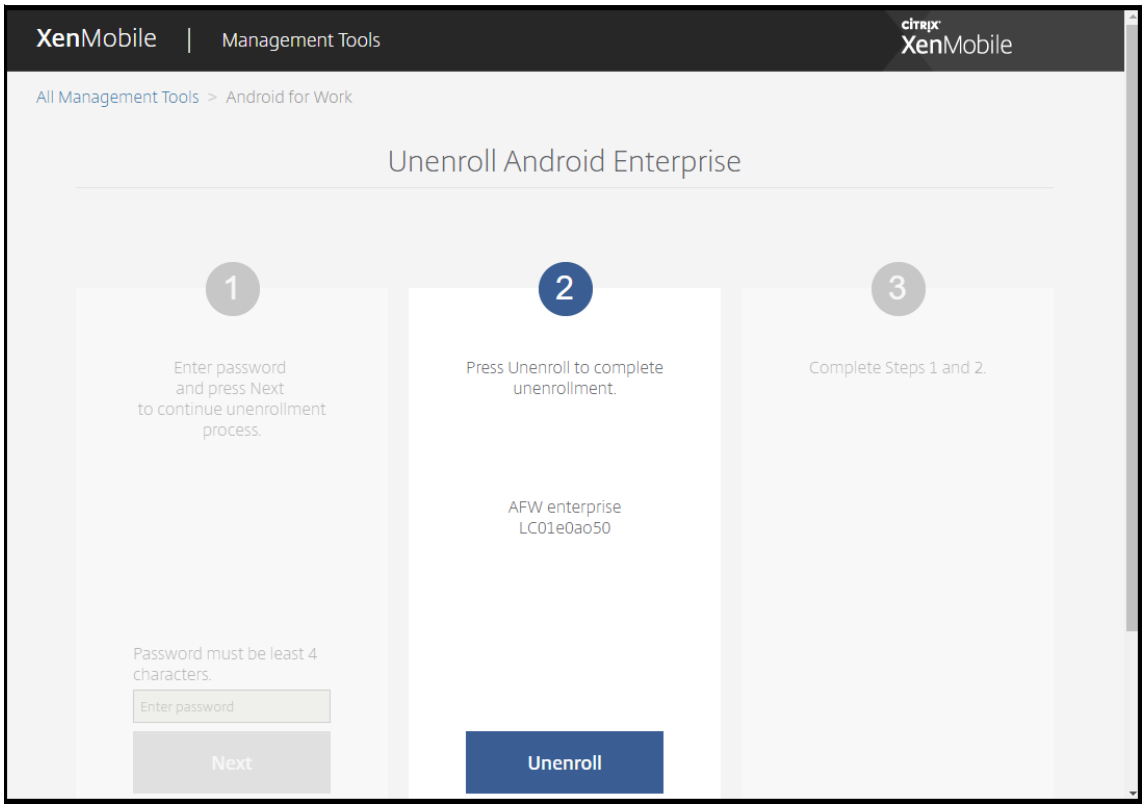


5. Quando a página do XenMobile Tools for aberta, insira a senha que você criou na etapa anterior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Clique em **Cancelar registro**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Provisionar modo de dispositivo de trabalho gerenciado para Android for Work

O modo de dispositivo de trabalho gerenciado para o Android for Work está disponível somente para dispositivos de propriedade da empresa. O XenMobile é compatível com estes métodos de registro no modo de dispositivo de trabalho gerenciado:

- **afw#xenmobile:** com esse método de registro, o usuário insere os caracteres "afw#xenmobile" ao configurar o dispositivo. Esse token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub.
- **Código QR:** o provisionamento de código QR é uma maneira fácil de provisionar uma frota distribuída de dispositivos que não são compatíveis com NFC, como tablets. O método de registro de código QR pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. O método de registro de código QR instala e configura o modo de dispositivo de trabalho gerenciado digitalizando um código QR no Assistente de instalação.
- **Aumento da comunicação a curta distância (NFC):** o método de registro de aumento de NFC pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. Um aumento de NFC transfere dados entre dois dispositivos usando comunicação a curta distância. Bluetooth, Wi-Fi e outros meios de comunicação estão desativados em um dispositivo que sofreu uma redefinição de fábrica. O NFC é o único protocolo de comunicação que o dispositivo pode usar nesse estado.

afw#xenmobile

O método de registro é usado após ligar um novo dispositivo ou dispositivos com a configuração inicial de fábrica redefinida. Os usuários digitam "afw#xenmobile" quando solicitados a inserir uma conta do Google. Essa ação baixa e instala o Secure Hub. Os usuários seguem os prompts de configuração do Secure Hub para concluir o registro.

Esse método de registro é recomendado para a maioria dos clientes, porque a versão mais recente do Secure Hub é baixada da loja Google Play. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download no servidor XenMobile.

Pré-requisitos:

- Suportado em todos os dispositivos Android com Android 5.0 e superior.

Código QR

Para registrar um dispositivo no modo de dispositivo usando um código QR, você pode gerar um código QR criando um JSON e convertendo o JSON em um código QR. A câmera do dispositivo escaneia o código QR para registrar o dispositivo.

Pré-requisitos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Suportado em todos os dispositivos Android com Android 7.0 e superior.

Criar um código QR 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 para o Citrix XenMobile Server como um aplicativo empresarial, ele pode ser baixado de`https://<fqdn>:4443/*instanceName*/worxhome.apk`. O caminho para o Secure Hub APK deve ser acessível através da conexão Wi-Fi em que 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 com duas letras minúsculas (por exemplo, en), conforme definido pela ISO 639-1. Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela ISO 3166-1. Por exemplo, insira en_US para o inglês falado nos Estados Unidos.

- **android.app.extra.PROVISIONING_TIME_ZONE:** o fuso horário em que o dispositivo é executado.

  Insira um nome Olson da área/localização do formulário. 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 (Epoch).

  A época do Unix (ou hora do Unix, hora do POSIX ou carimbo de data/hora do Unix) é o número de segundos decorridos desde 1º de janeiro de 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (in ISO 8601: 1970-01-01T00:00:00Z).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** definido 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 tem esta aparência:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "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 que é criado usando qualquer ferramenta de validação JSON, como https://jsonlint.com. Converta essa sequência JSON em um código QR usando qualquer gerador de código QR on-line, como https://goqr.me.

Este código QR é escaneado por um dispositivo com redefinição de fábrica para registrar o dispositivo no modo de dispositivo de trabalho gerenciado.

Para registrar o dispositivo

Para registrar um dispositivo no modo de dispositivo de trabalho gerenciado, o dispositivo deve estar no estado de redefinição de fábrica.

1. Toque seis vezes na tela de boas-vindas para iniciar o fluxo de registro do 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 através desta rede Wi-Fi.

   Depois que o dispositivo se conecta com êxito a 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 o proprietário do dispositivo.

Para mais informações, consulte este Guia do Google para desenvolvedores de EMM para Android: https://developers.google.com/android/work/prov-devices#qr_code_method.

Compartilhamento por NFC

Registrar um dispositivo no modo de dispositivo usando compartilhamentos por NFC requer dois dispositivos: um cujas configurações de fábrica sejam redefinidas e um que esteja executando a XenMobile Provisioning Tool.

Pré-requisitos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Suportado em todos os dispositivos Android com Android 5.0, Android 5.1, Android 6.0 e superior.
- Um XenMobile Server versão 10.4 que está ativado para o Android For Work.
- Um dispositivo com redefinição de fábrica, provisionado para o Android for Work no modo de dispositivo de trabalho gerenciado. Você pode encontrar as etapas para concluir esse pré-requisito neste artigo.
- Outro dispositivo com recursos NFC executando a Provisioning Tool configurada. A Provisioning Tool está disponível no Secure Hub 10.4 ou na Página de downloads Citrix.

Cada dispositivo pode ter somente um perfil do Android for Work, gerenciado por um aplicativo de gerenciamento de mobilidade empresarial (EMM). No XenMobile, o Secure Hub é o aplicativo EMM. Somente um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo EMM remove o primeiro aplicativo EMM.

Você pode iniciar o modo de dispositivo e trabalho gerenciado em dispositivos novos ou restaurados para as configurações de fábrica. Você administra o dispositivo inteiro usando o XenMobile.

Dados transferidos através do aumento de NFC

Provisionar um dispositivo com redefinição de fábrica requer que você envie os seguintes dados por meio de um aumento de NFC para inicializar o Android for Work:

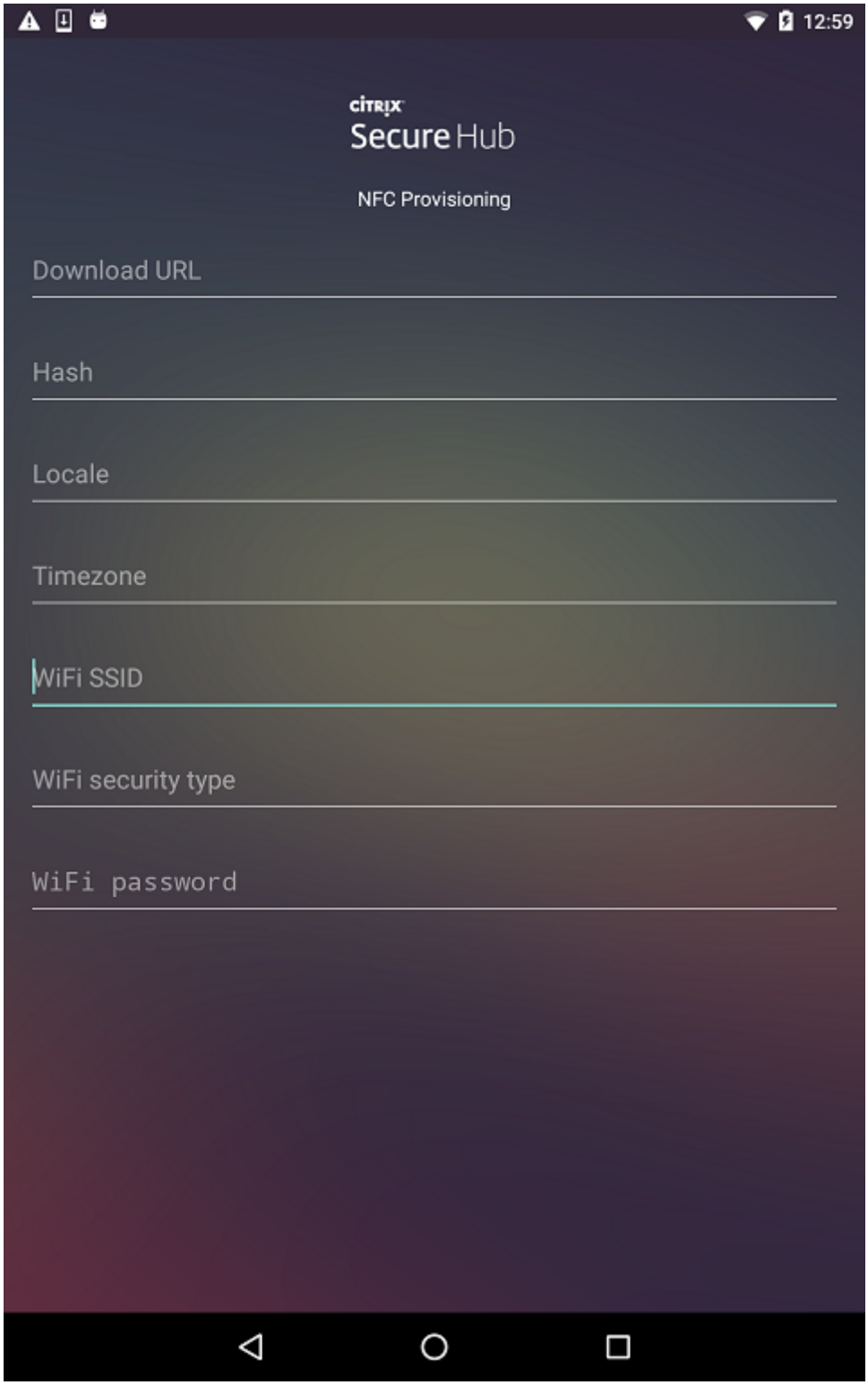
- O nome do pacote do aplicativo do provedor EMM que atua como o proprietário do dispositivo (neste caso, o Secure Hub).
- A localização de Intranet/Internet do qual o dispositivo pode baixar o aplicativo do provedor EMM.
- O hash SHA1 do aplicativo do provedor EMM para verificar se o download é bem-sucedido.
- Os detalhes da conexão WiFi para que um dispositivo com redefinição de fábrica possa se conectar e baixar o aplicativo do provedor EMM. Nota: No momento, o Android não é compatível com WiFi 802.1x para esta etapa.
- O fuso horário do dispositivo (opcional).
- A localização geográfica do dispositivo (opcional).

Quando os dois dispositivos são aumentados, os dados da Provisioning Tool são enviados para o dispositivo com redefinição de fábrica. Esses dados são usados para baixar o Secure Hub com as configurações do administrador. Se você não inserir os valores de localização e fuso horário, o Android os configura automaticamente no novo dispositivo.

Configuração da XenMobile Provisioning Tool

Antes de realizar um aumento de NFC, você deve configurar a Provisioning Tool. Em seguida, essa configuração é transferida para o dispositivo com redefinição de fábrica durante o aumento de NFC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no procedimento a seguir descrevem como configurar o arquivo de texto e contém descrições para cada campo. O aplicativo não salva as informações depois que as digitar, portanto, convém criar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

um arquivo de texto para manter as informações para uso futuro.

Para configurar a Provisioning Tool usando um arquivo de texto

Dê ao arquivo o nome nfcprovisioning.txt e coloque-o na pasta /sdcard/ no cartão SD do dispositivo. Em seguida, o aplicativo poderá ler o arquivo de texto e preencher os valores.

O arquivo de texto deve conter os seguintes dados:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Essa linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo com redefinição de fábrica se conectar a Wi-Fi em seguida ao aumento de NFC, o dispositivo deve ter acesso a esse local para fazer o download. A URL é uma URL regular, sem necessidade de formatação especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

Essa linha é a soma de verificação do aplicativo do provedor EMM. Essa soma de verificação é usada para verificar se o download foi bem-sucedido. As etapas para obter a soma de verificação são discutidas neste artigo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esse é o SSID de Wi-Fi conectado do dispositivo no qual a Provisioning Tool está em execução.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Os valores suportados são WEP e WPA2. Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela ISO 639-1. Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela ISO 3166-1. Por exemplo, digite en_US para o 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 no qual o dispositivo está em execução. Insira um nome Olson da área/localização do formulário. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir nenhum nome, o fuso horário será preenchido automaticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Isso não é necessário, pois o valor é inserido em código fixo no aplicativo, como o Secure Hub. Ele é mencionado aqui somente por uma questão de conclusão.

Se houver um Wi-Fi protegido por WPA2, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
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=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

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 Wi-Fi desprotegida, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
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=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

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 a soma de verificação do Secure Hub

Para obter a soma de verificação de qualquer aplicativo, adicione o aplicativo como um aplicativo empresarial.

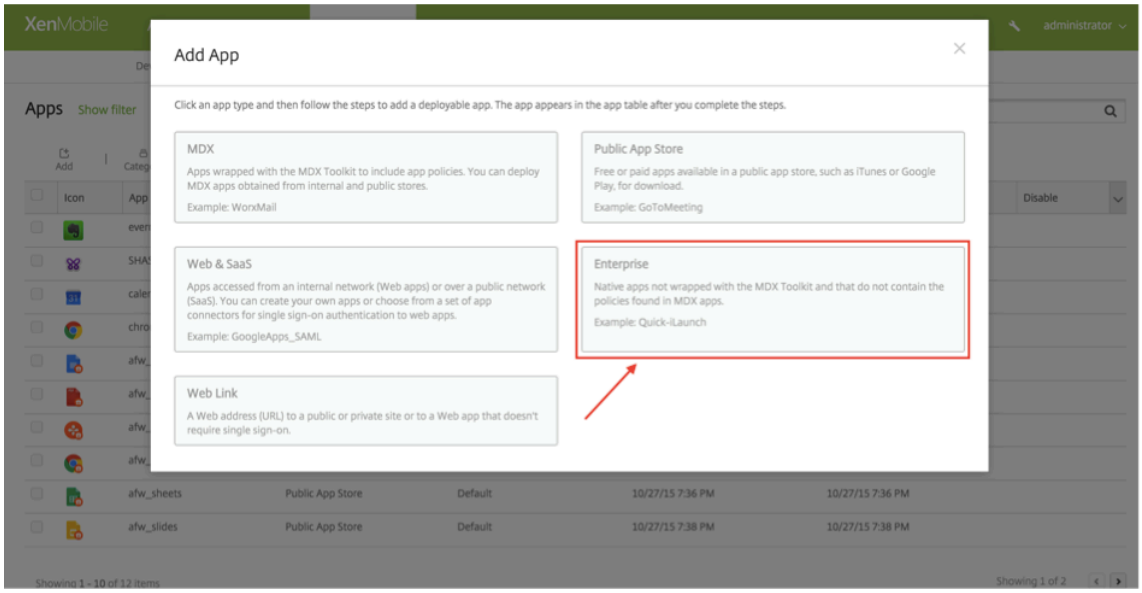
1. No console XenMobile, clique em **Configurar > Aplicativos** e em **Adicionar**.

   A janela **Adicionar aplicativos** é exibida.

2. Clique em **Empresarial**.

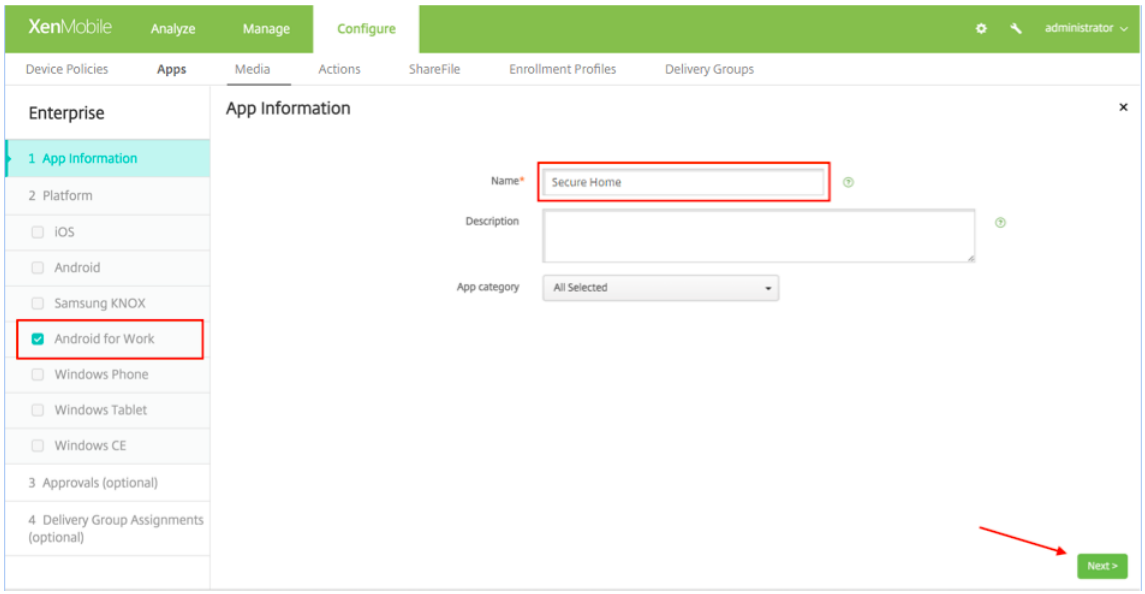
   A página **Informações do Aplicativo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Selecione a configuração a seguir e clique em **Avançar**.

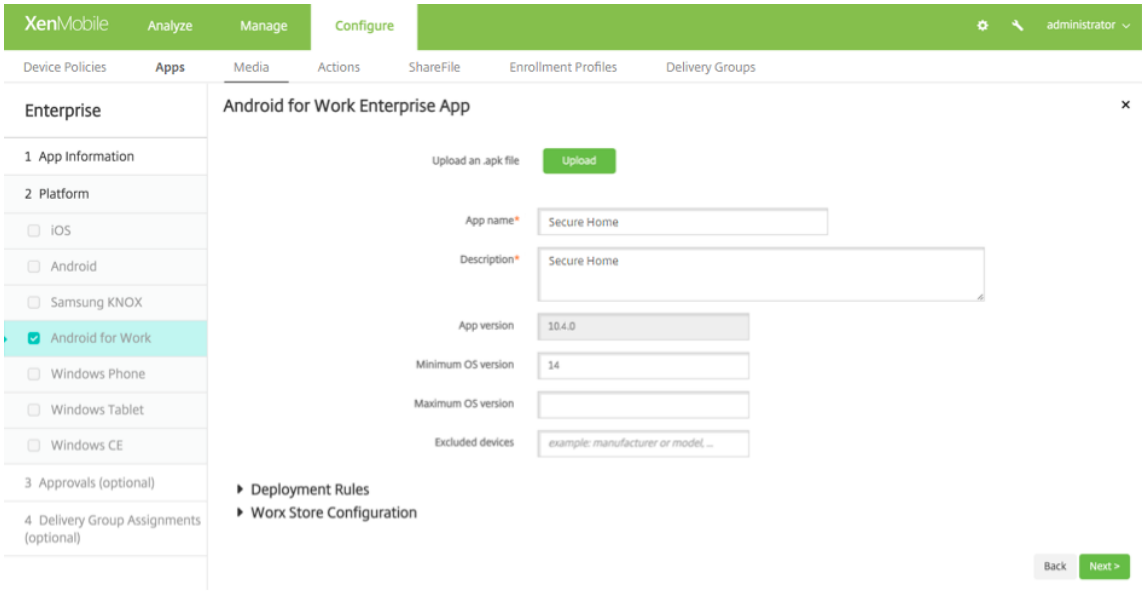
   A tela do **aplicativo Android for Work Enterprise** é exibida.



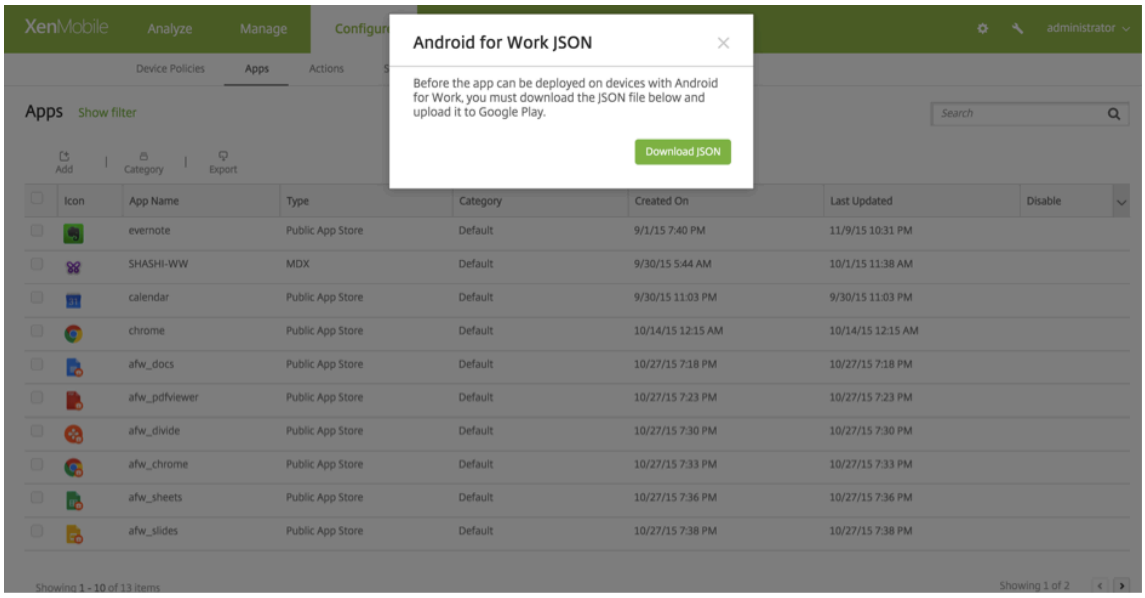
4. Forneça o caminho até o arquivo .apk e clique em **Avançar** para carregá-lo.

   Depois que a instalação for concluída, serão exibidos os detalhes do pacote carregado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Clique em **Avançar** para abrir uma página para baixar o arquivo JSON, que você usará para carregar no Google Play. Para o Secure Hub, não é necessário carregar para Google Play, mas você precisa do arquivo JSON para ler o valor SHA1 dele.



Um arquivo JSON típico tem esta aparência:



6. Copie o **valor file_sha1_base64** e use-o no campo **Hash** na Provisioning Tool.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> O hash deve ser seguro para URLs.

- Converta os símbolos **+** para **-**
- Converta os símbolos **/** para **_**
- Substitua o trailing **\u003d** por **=**

Se você armazenar o hash no arquivo nfcprovisioning.txt no cartão SD do dispositivo, o aplicativo faz a conversão de segurança. No entanto, se você optar por digitar o hash manualmente, será sua responsabilidade garantir a segurança da URL.

Bibliotecas usadas

A Provisioning Tool usa as seguintes bibliotecas no seu código-fonte:

- Biblioteca v7 appcompat, Biblioteca de suporte ao design e biblioteca de paletas v7 do Google sob licença Apache 2.0

  Para obter informações, consulte Guia de Recursos da Biblioteca de Suporte.

- Butter Knife de Jake Wharton sob a licença Apache 2.0

Provisionar o modo de perfil de trabalho no Android for Work

O modo de perfil de trabalho do Android for Work está disponível para dispositivos nos quais você separa as áreas corporativa e pessoal de um dispositivo. Por exemplo, o modo de perfil de trabalho está disponível para dispositivos BYOD. A experiência de registro do modo de perfil de trabalho é semelhante ao registro do Android no XenMobile. Os usuários fazem o download do Secure Hub a partir do Google Play e registram seus dispositivos.

Por padrão, as configurações de Depuração de USB e Fontes desconhecidas são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

> Dica:
>
> Quando for registrar dispositivos no Android for Work no modo de perfil de trabalho, sempre vá para o Google Play. A partir dali, habilite o Hub Secure para aparecer no perfil pessoal do usuário.

Clientes com “Android for Work legado for G Suite”

April 15, 2019

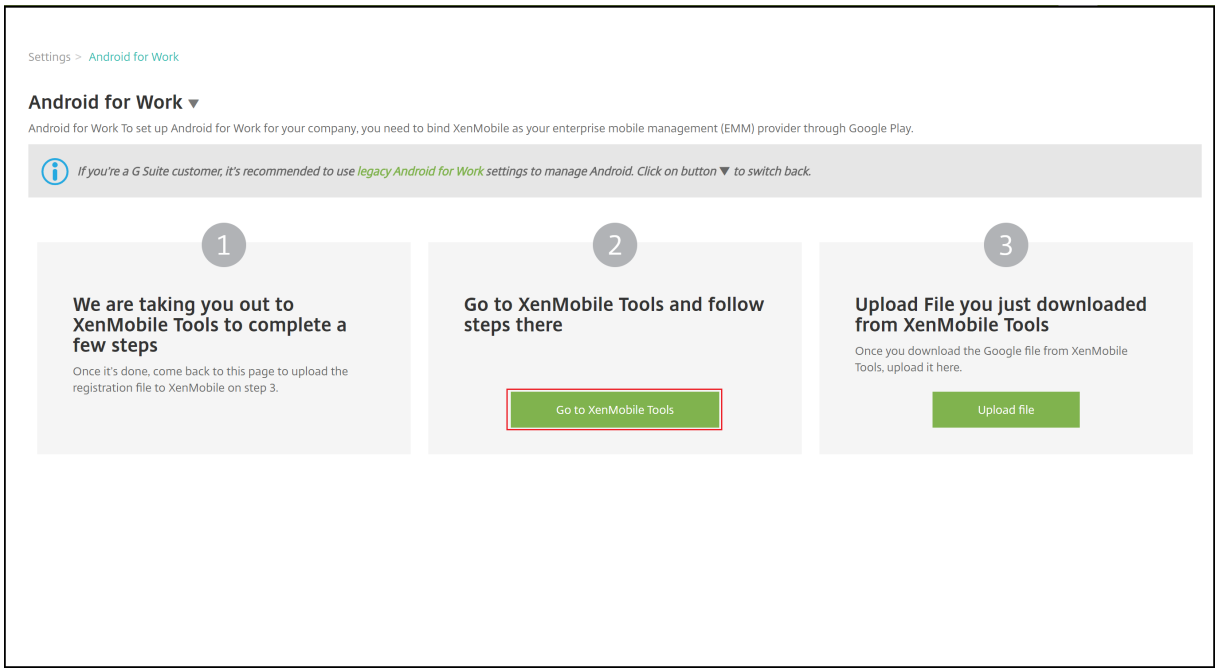
Os clientes do G Suite devem usar as configurações do Android for Work legado para configurar o Android for Work legado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos para o Android for Work legado:

- Um domínio publicamente acessível
- Uma conta de administrador do Google
- Os dispositivos que têm gerenciadas perfis e que executam o Android 5.0 + lollipop compatíveis
- Uma conta do Google que tenha o Google Play instalado
- Um perfil de trabalho configurado no dispositivo

Para iniciar a configuração do Android for Work legado, clique em **Android for Work legado** na página **Android for Work** nas configurações do XenMobile.



Criar uma conta do Android for Work

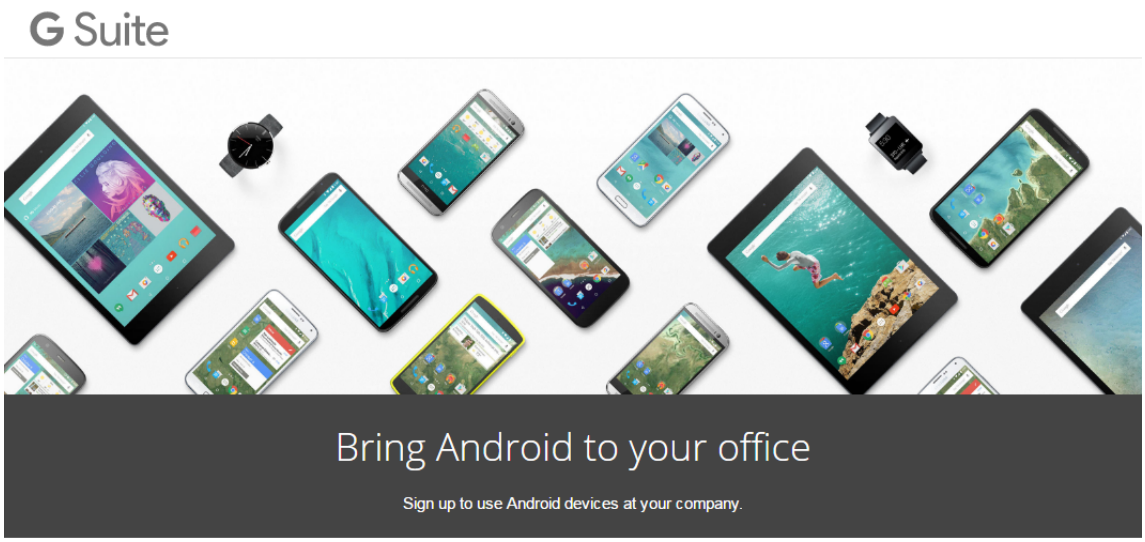
Antes de poder configurar uma conta do Android for Work, você deve confirmar seu nome de domínio com o Google.

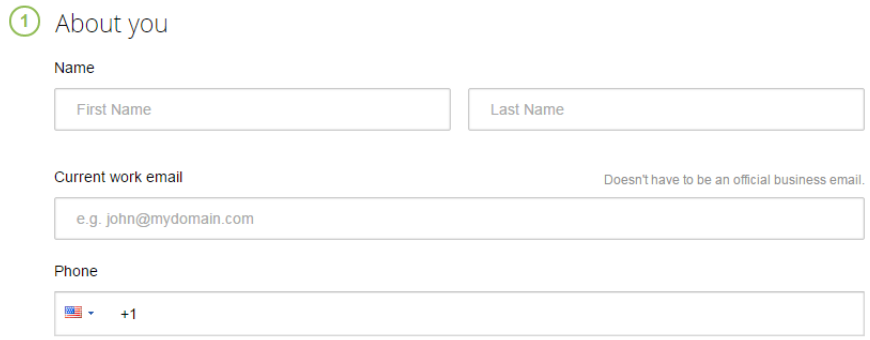
Se você já verificou seu nome de domínio no Google, pode pular para esta etapa: Configurar uma conta de serviço do Android for Work e baixar um certificado do Android for Work.

1. Navegue até https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

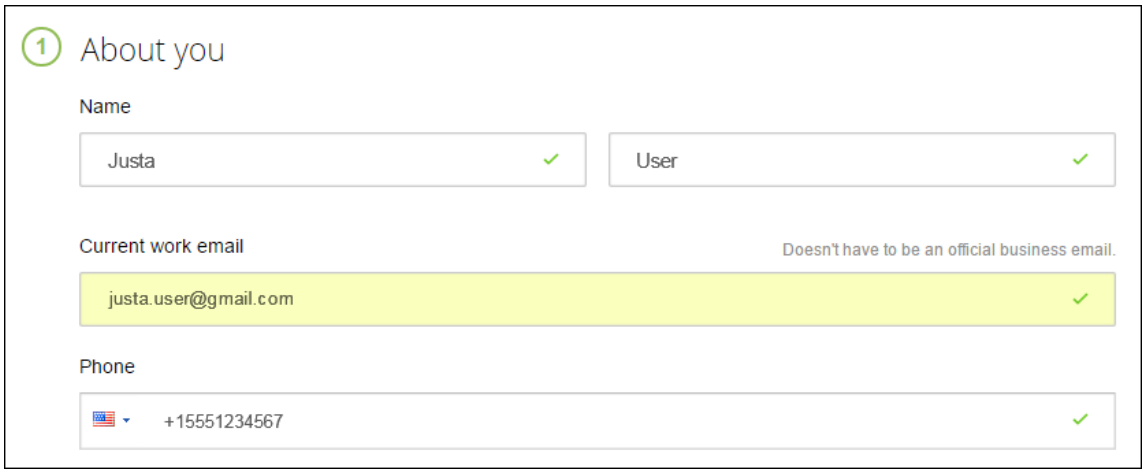
   A seguinte página é exibida, na qual você pode digitar suas informações de administrador e da empresa.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



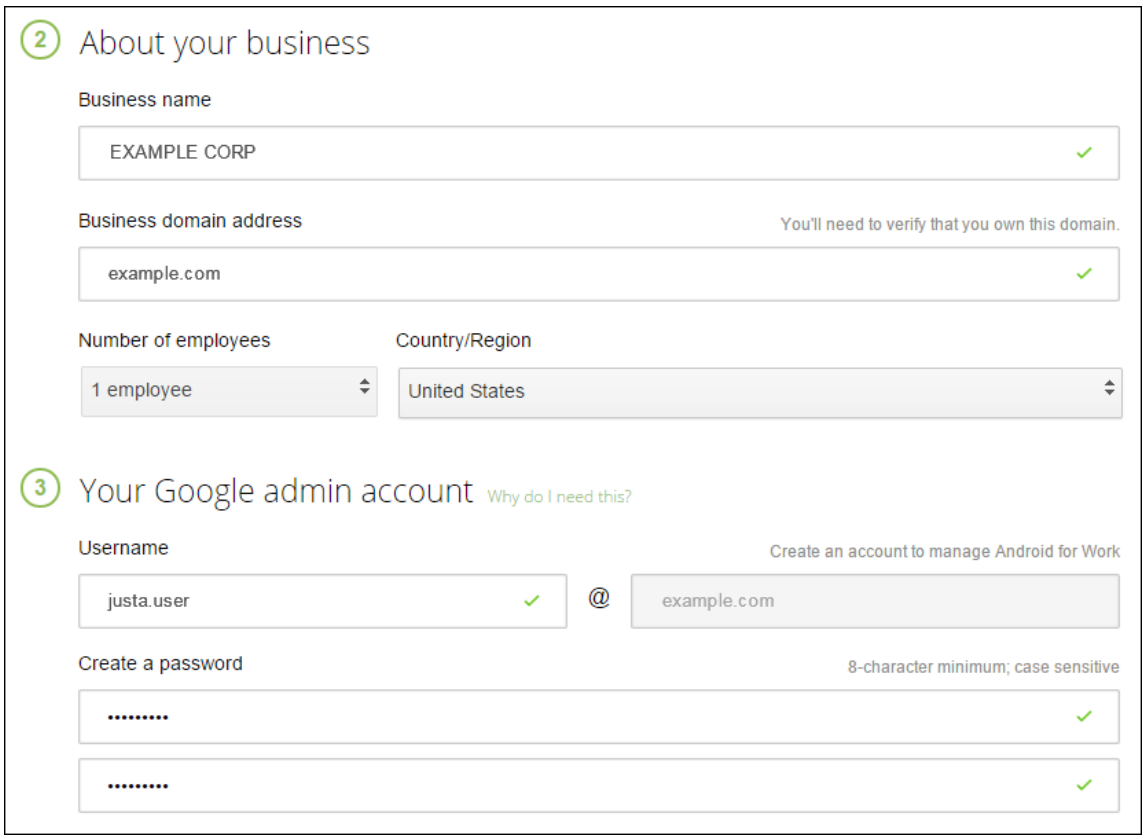


2. Insira as informações de usuário administrador.



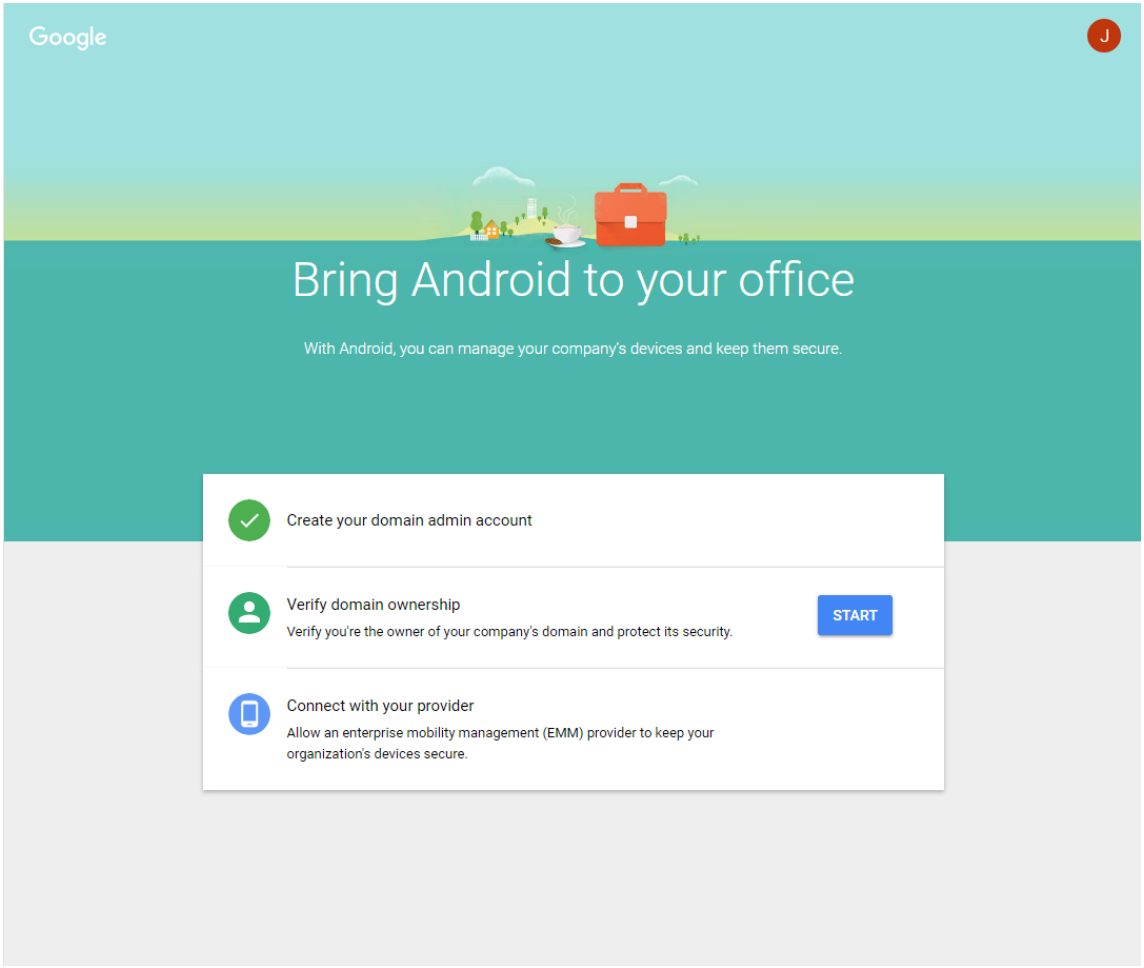
3. Digite as informações da sua empresa, além de informações da sua conta de administrador.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A primeira etapa no processo foi concluída e você vê a página a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Verificar a propriedade do domínio

Permitir que o Google Verifique o seu domínio de uma das seguintes maneiras:

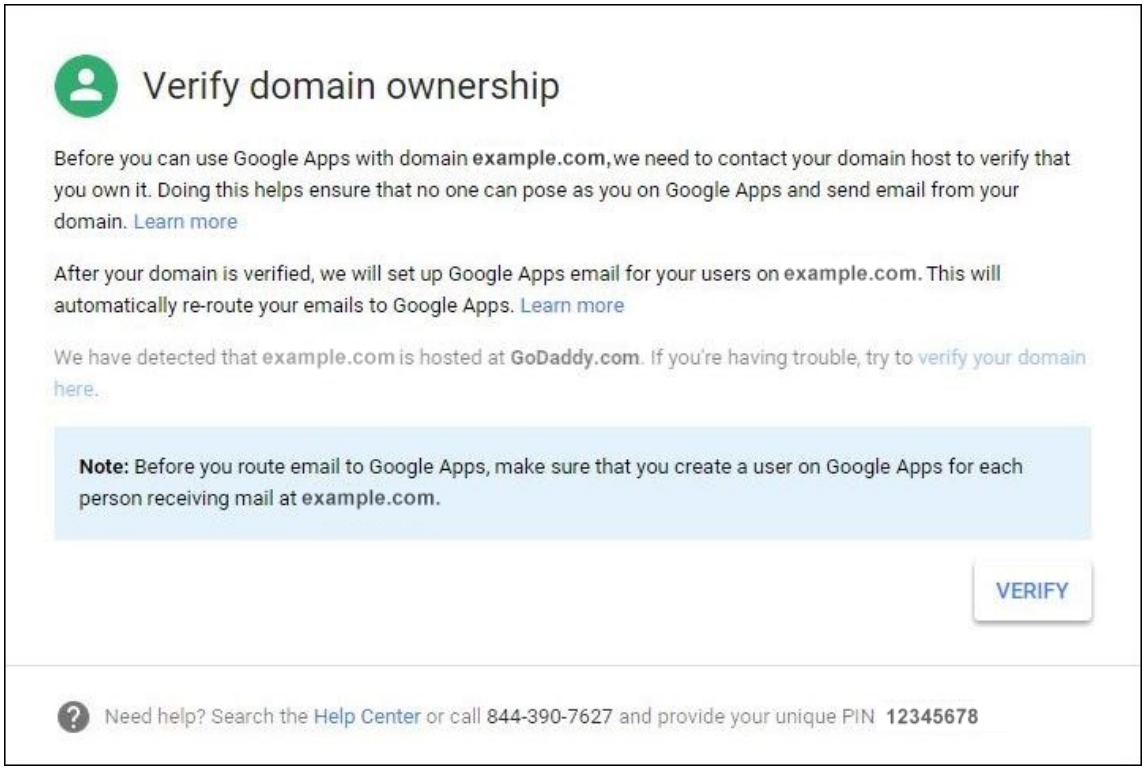
- Adicione um registro TXT ou CNAME no site do host seu domínio.
- Carrega um arquivo HTML para o servidor web do seu domínio.
- Adicione uma marca `<meta>` para a sua página inicial. O Google recomenda o primeiro método. Este artigo não aborda as etapas para verificar a propriedade do seu domínio, mas você pode encontrar as informações de que precisa aqui: https://support.google.com/a/answer/6248925.

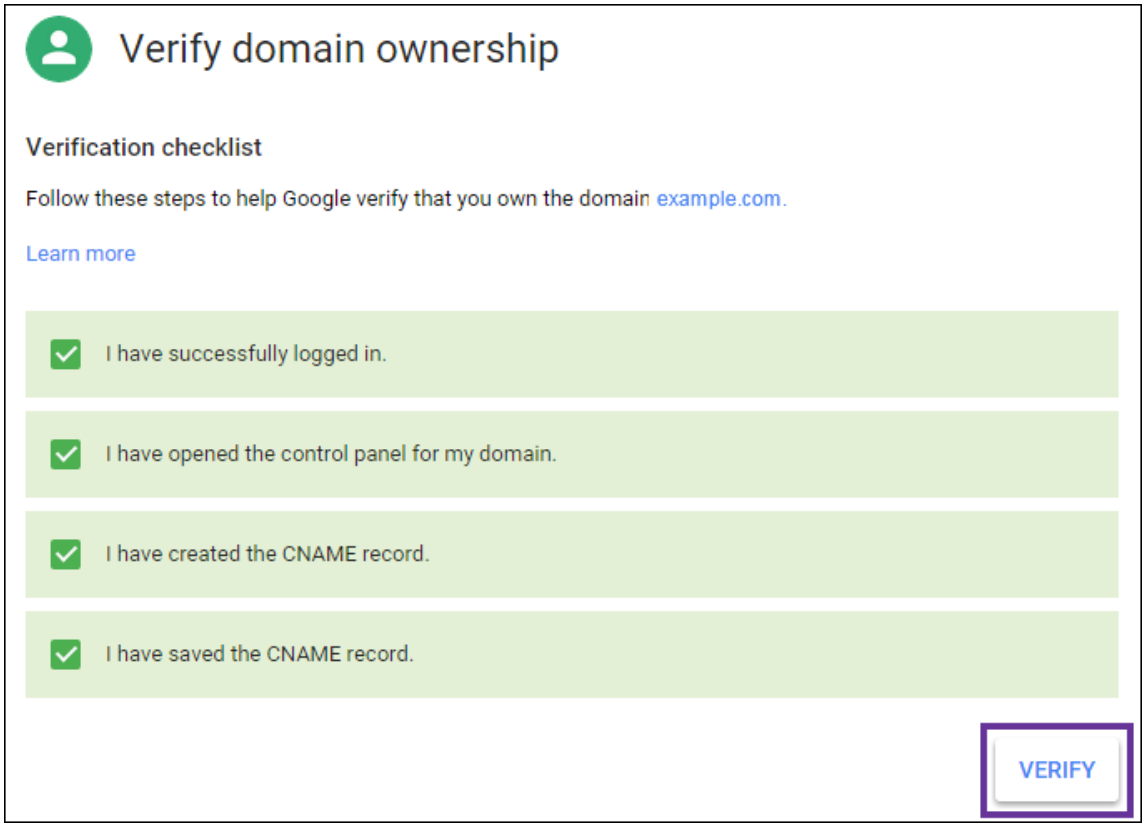
1. Clique em **Start** para iniciar a verificação do seu domínio.

   A página **Verify domain ownership** é exibida. Siga as instruções nessa página para verificar o seu domínio.

2. Clique em **Verify**.

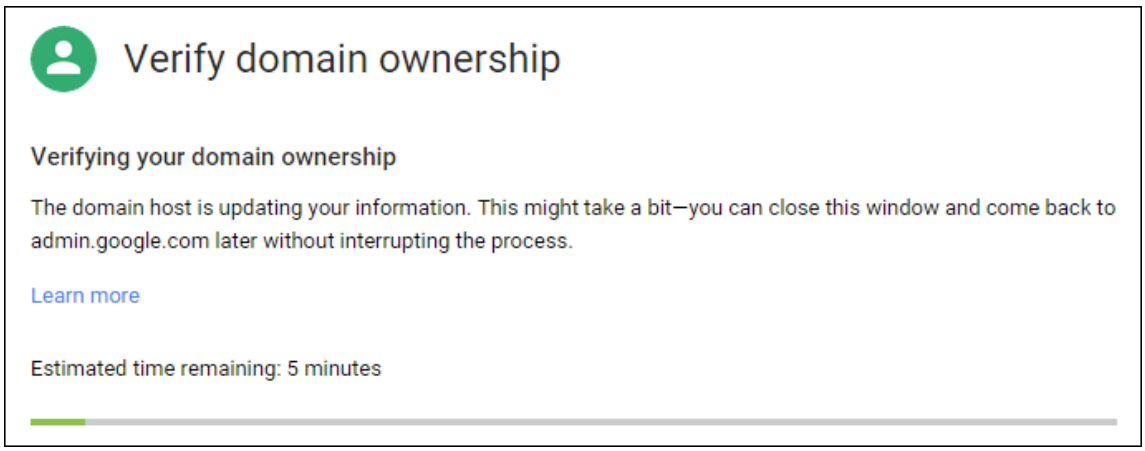
© 1999-2019 Citrix Systems, Inc. All rights reserved.



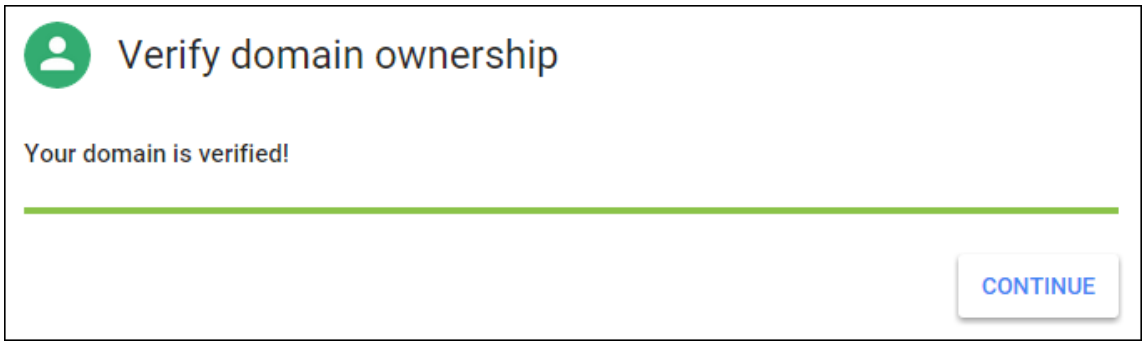


3. O Google verifica a propriedade do domínio.

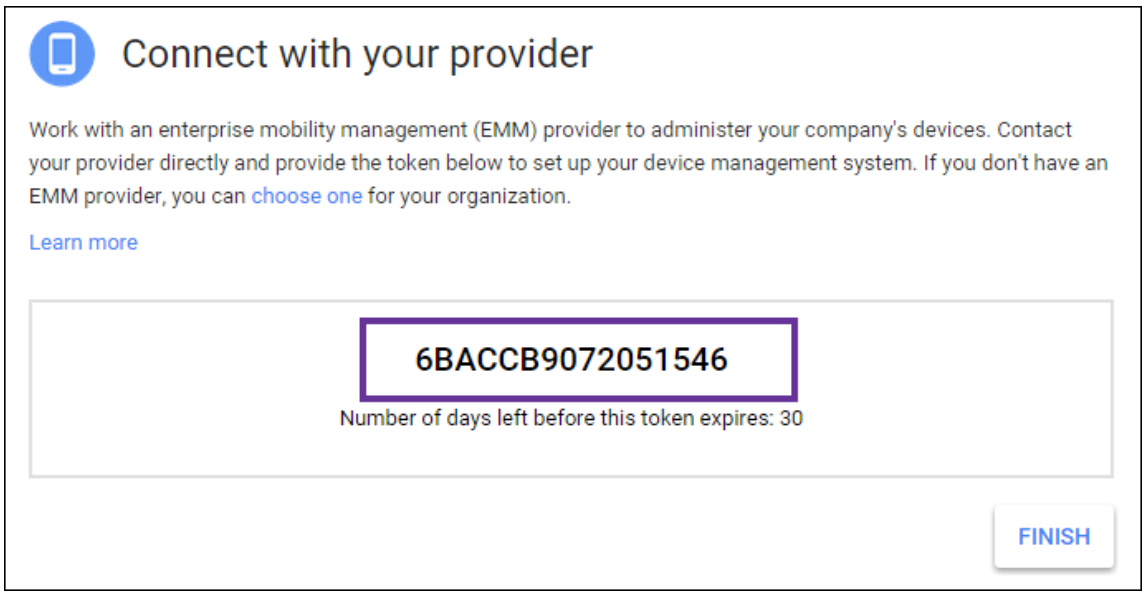
© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Após uma verificação bem-sucedida, a página a seguir é exibida. Clique em **Continue**.



5. O Google cria um token de associação de EMM que você fornece para a Citrix e usa ao definir as configurações do Android for Work. Copie e salve o token; você precisará dele mais tarde no processo de instalação.



6. Clique em **Finish** para concluir a instalação do Android for Work. Uma página será exibida, indicando que com êxito verificar seu domínio.

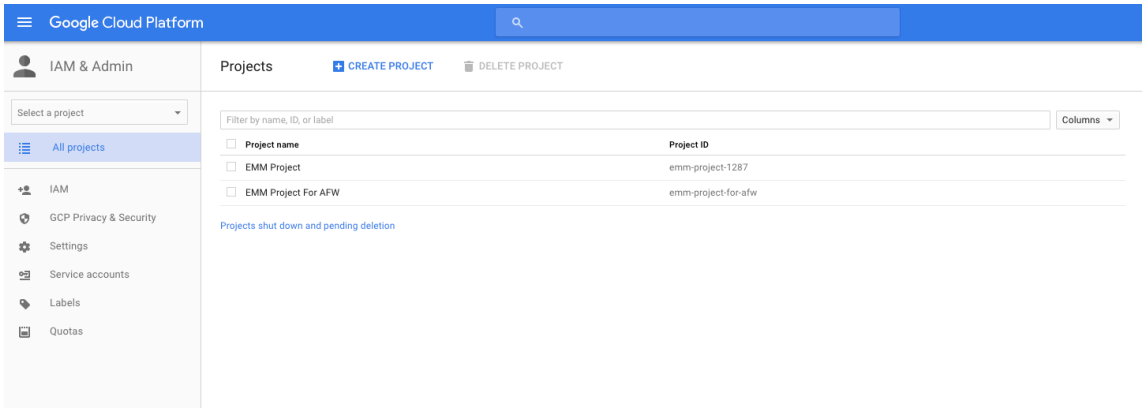
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Depois de criar uma conta de serviço do Android for Work, você poderá fazer logon no console do Google Admin para gerenciar as configurações de gerenciamento de mobilidade.

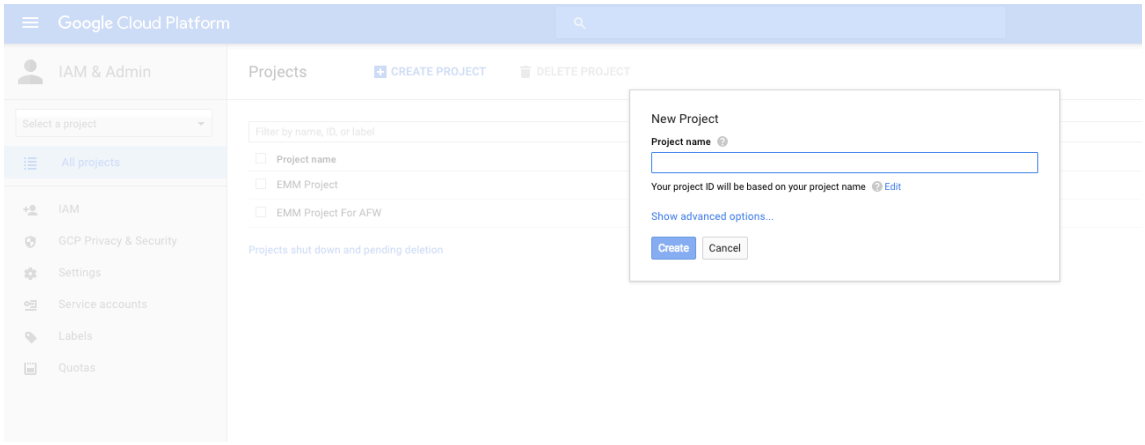
Configurar uma conta de serviço do Android for Work e baixar um certificado do Android for Work

Para permitir que o XenMobile contate os serviços do Google Play e do Directory, você deverá criar uma conta de serviço usando o portal Google Project para desenvolvedores. Essa conta de serviço é usada para a comunicação servidor-a-servidor entre o XenMobile e os serviços do Google para o Android at Work. Para obter mais informações sobre o protocolo de autenticação usado, vá para 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 **Projects**, clique em **Create Project.**

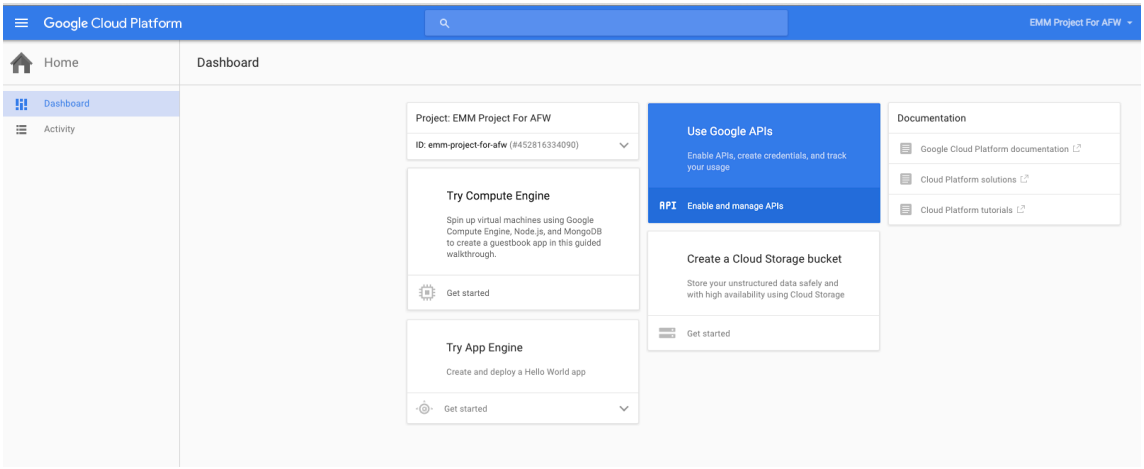


3. Em **Project name**, digite um nome para o projeto.

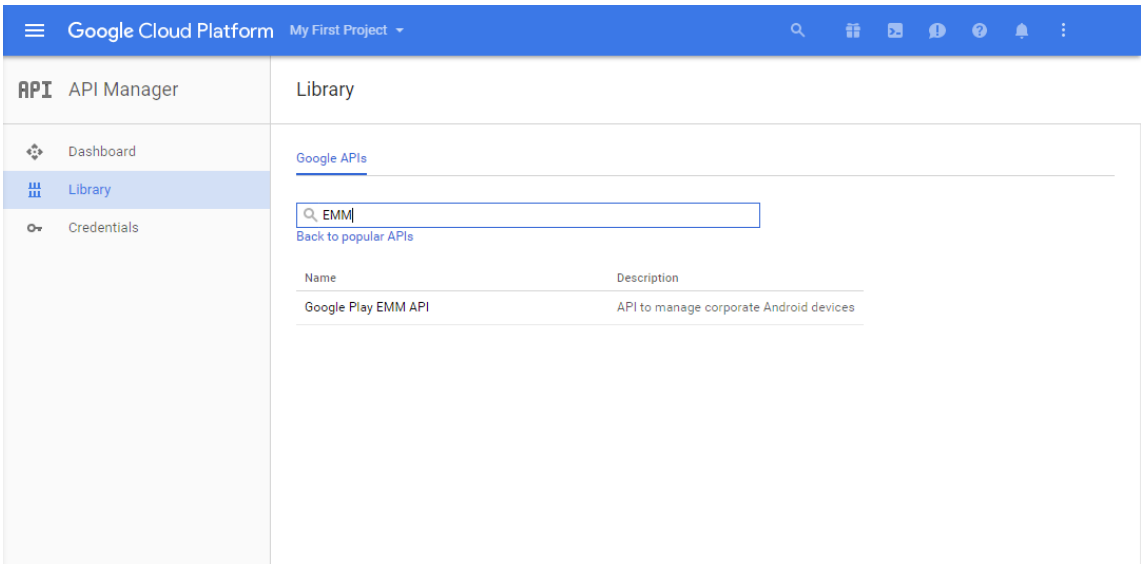


4. Em Dashboard, clique em **Use Google APIs**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

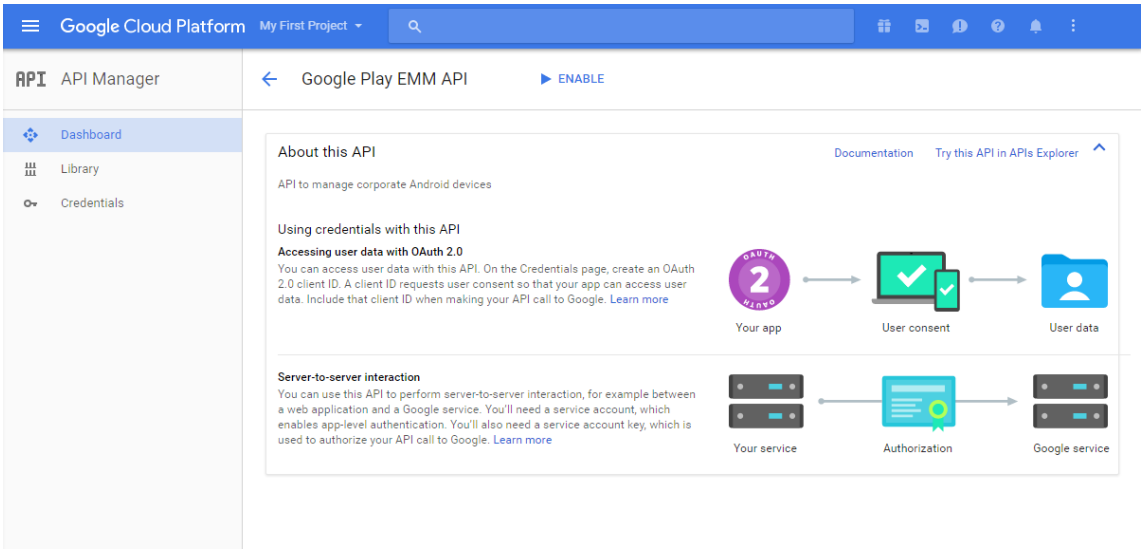


5. Clique em **Library**, em **Search**, tipo **EMM** e, em seguida, clique no resultado da pesquisa.

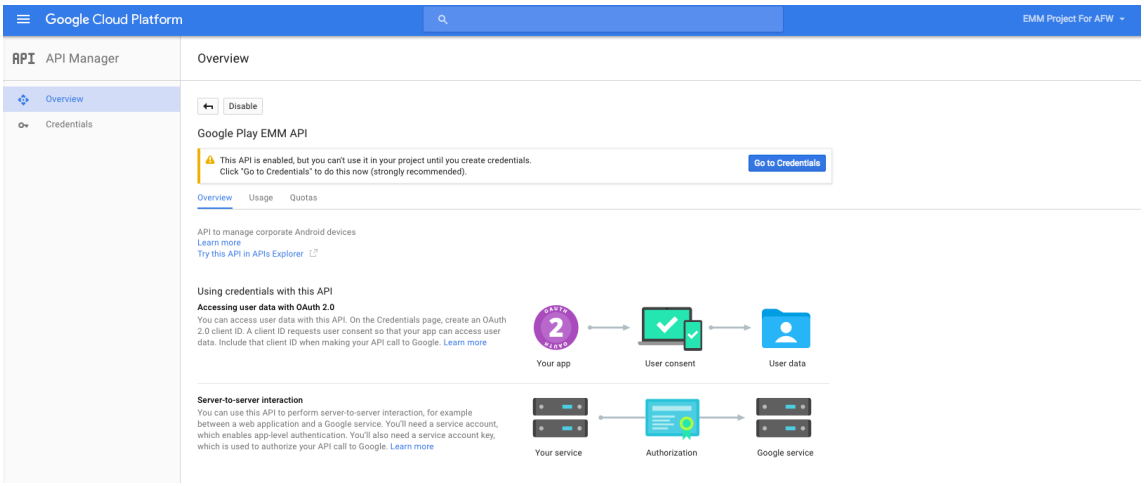


6. Na página **Overview**, clique em **Enable**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

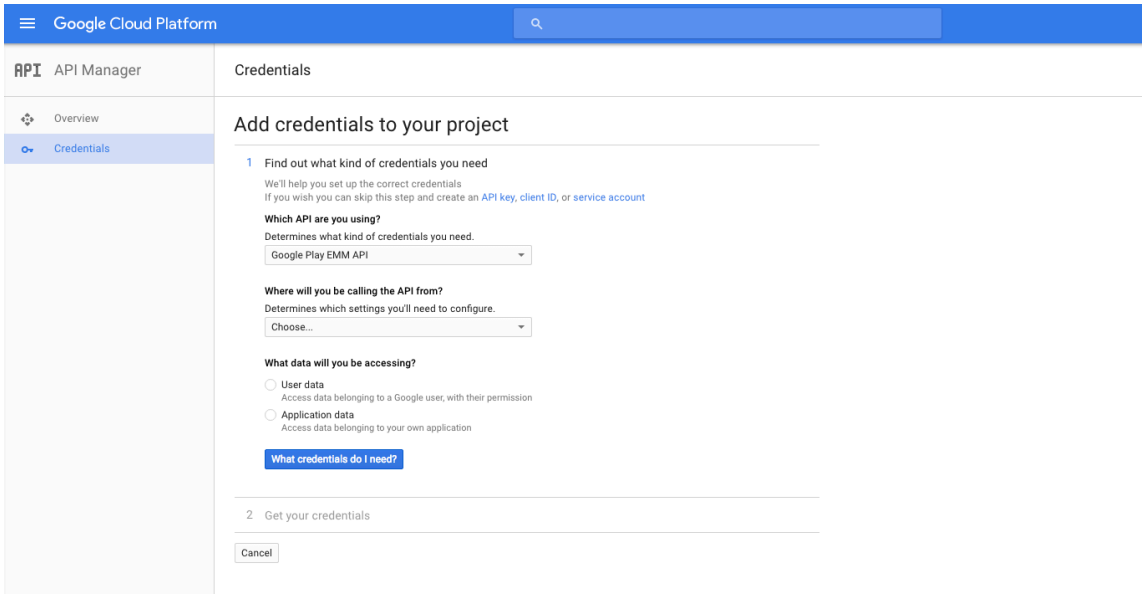


7. Ao lado de **Google Play EMM API**, clique em **Go to Credentials**.

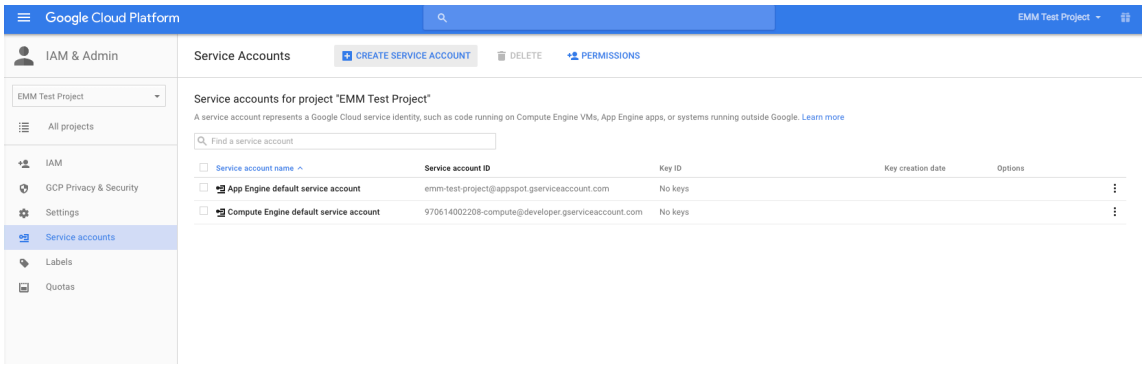


8. Na lista **Add credentials to our project**, na etapa 1, clique em **service account**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

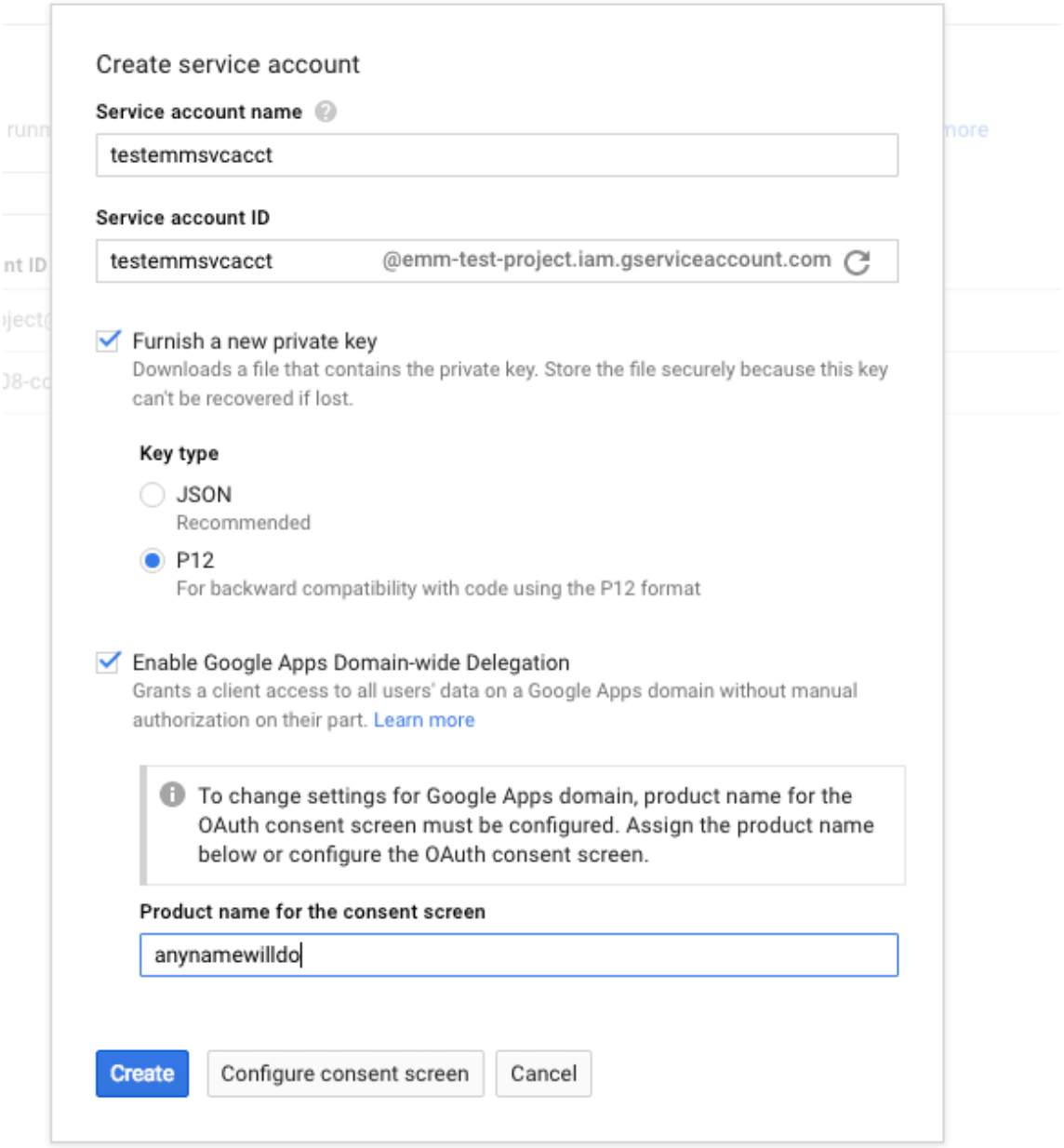


9. Na página **Service Accounts**, clique em **Create Service Account**.



10. Em **Create service account**, dê um nome à conta e marque a caixa de seleção **Furnish a new private key**. Clique em **P12**, marque a caixa de seleção **Enable Google Apps Domain-wide Delegation** e, em seguida, clique em **Create.**

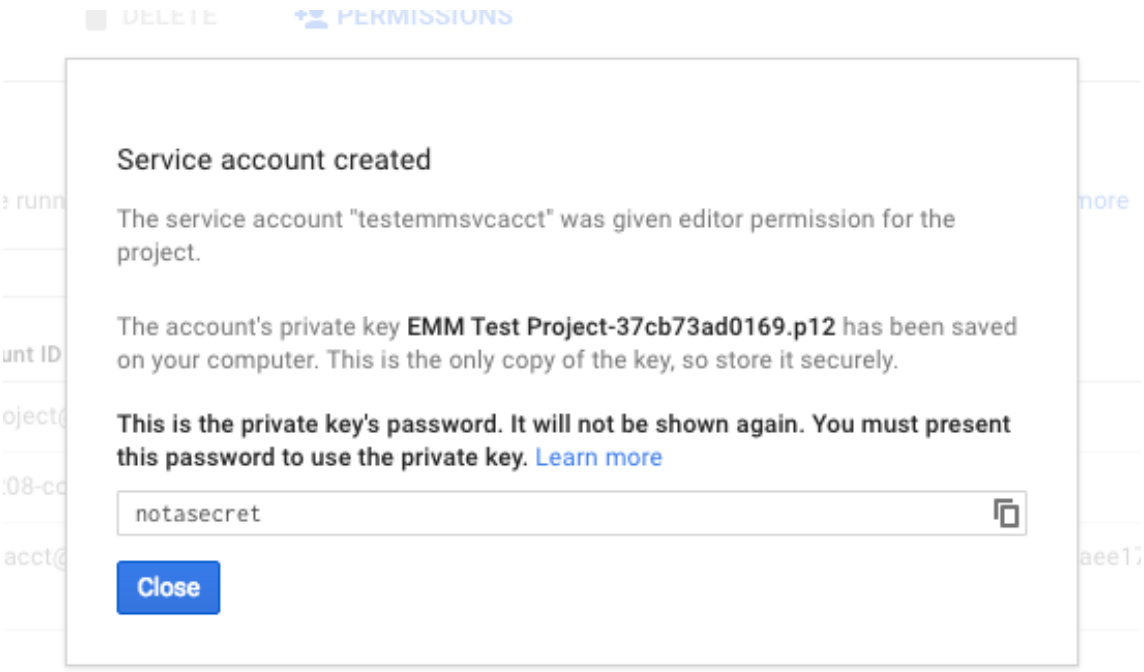
© 1999-2019 Citrix Systems, Inc. All rights reserved.



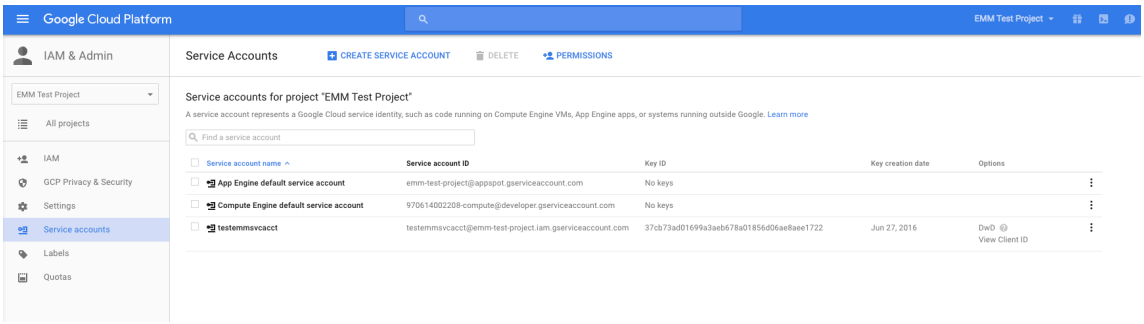
O certificado (arquivo P12) é baixado para o seu computador. Não se esqueça de salvar o certificado em uma localização segura.

11. Na tela de confirmação **Service account created**, clique em **Close**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

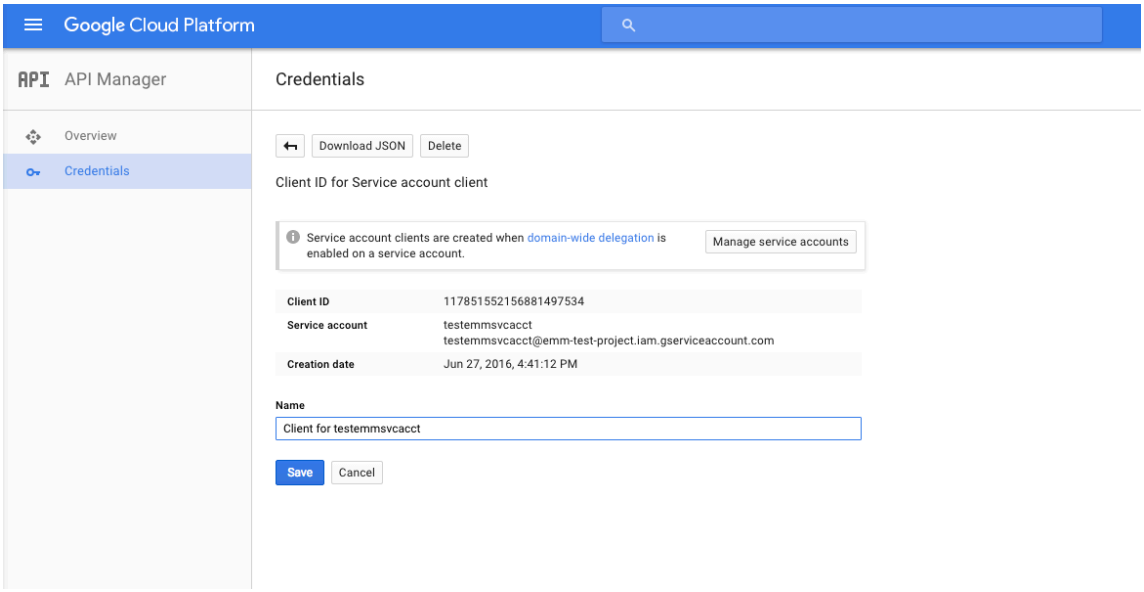


12. Em **Permissions**, clique em **Service accounts** e depois sob **Options** da sua conta de serviço, clique em **View Client ID**.

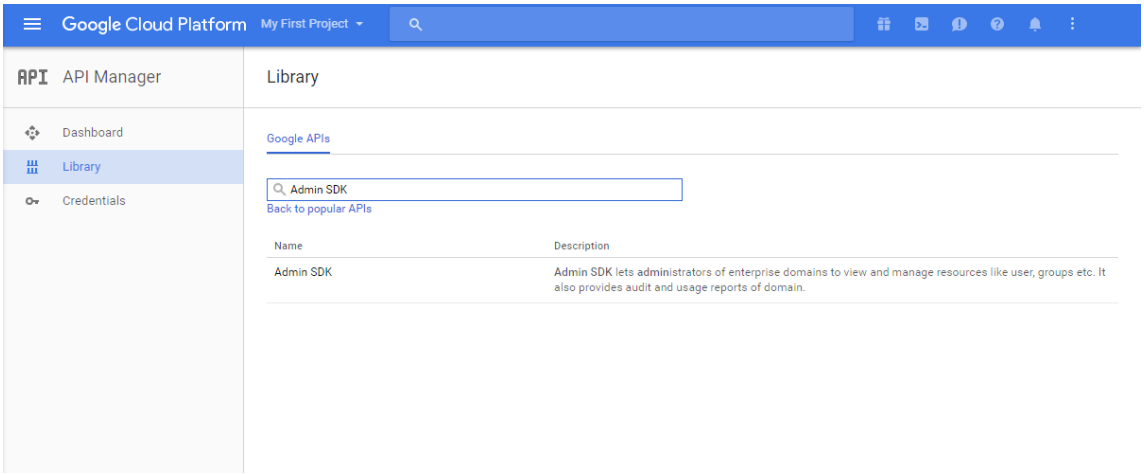


13. Os detalhes necessários para a autorização da conta no console de administração do Google são exibidos. Copie o **Cliente ID** e o **Service account ID** para um local onde você possa recuperar as informações posteriormente. Você precisa dessas informações, juntamente com o nome de domínio, para enviar para o suporte da Citrix para inclusão na lista branca.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

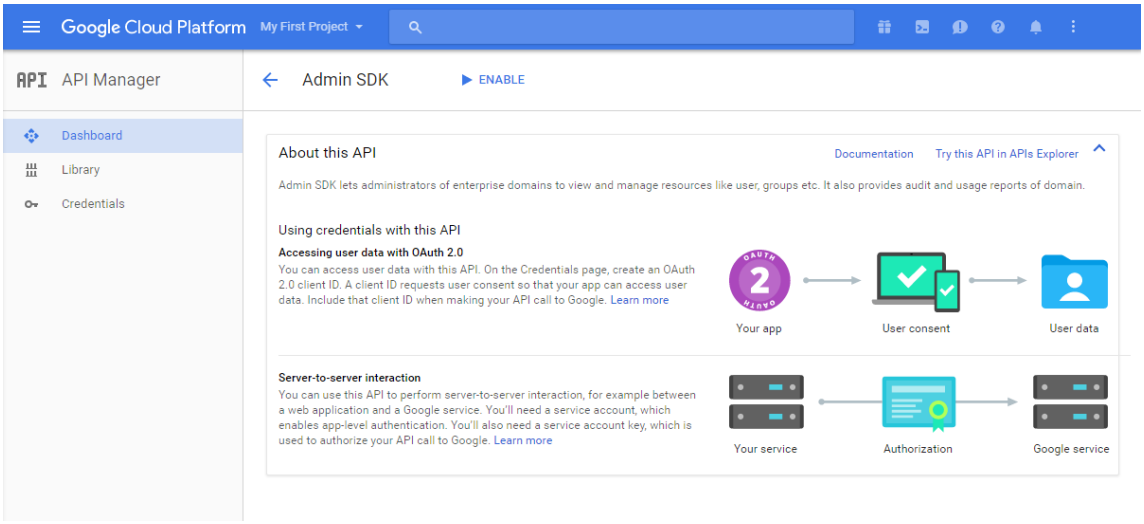


14. Na página **Library**, procure **Admin SDK** e, em seguida, clique no resultado da pesquisa.

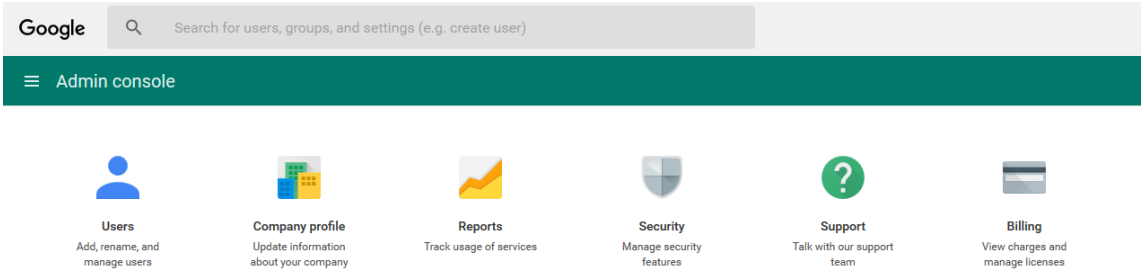


15. Na página **Overview**, clique em **Enable**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

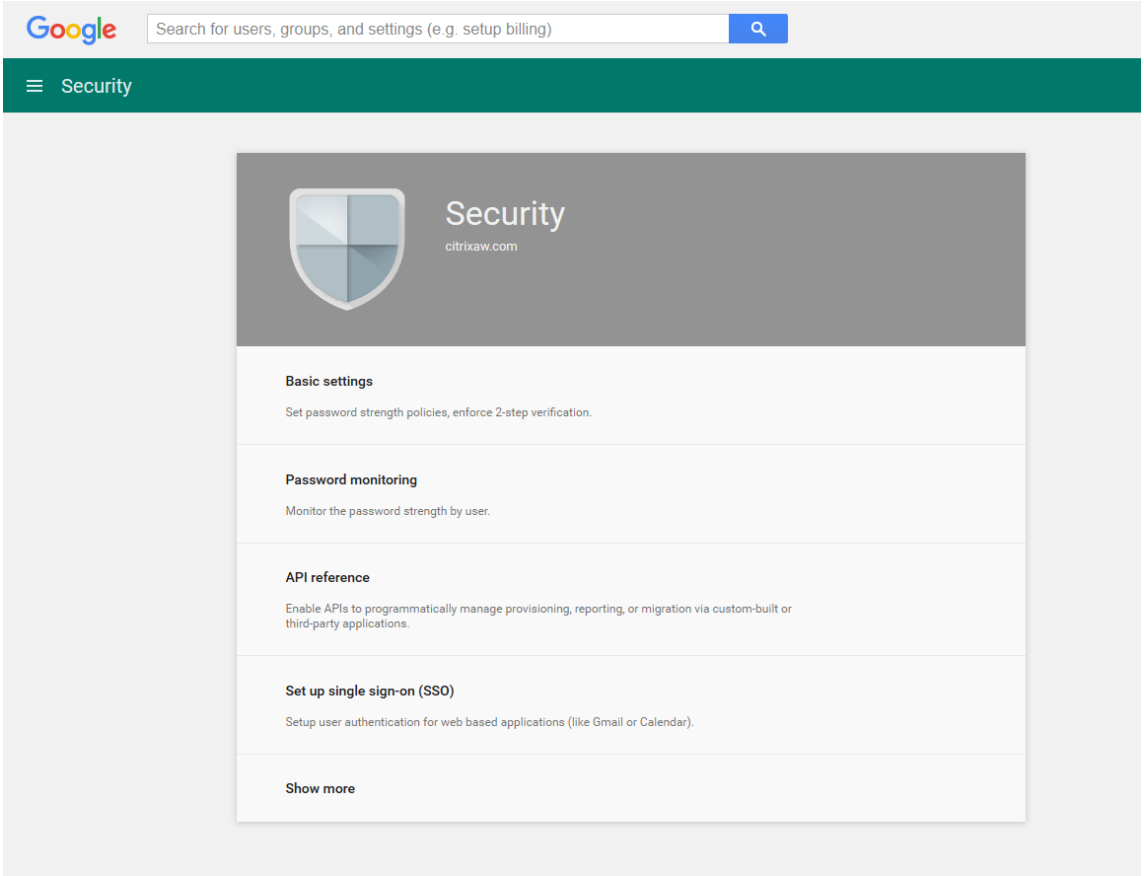


16. Abra o console de administração do Google do seu domínio e clique em **Security**.

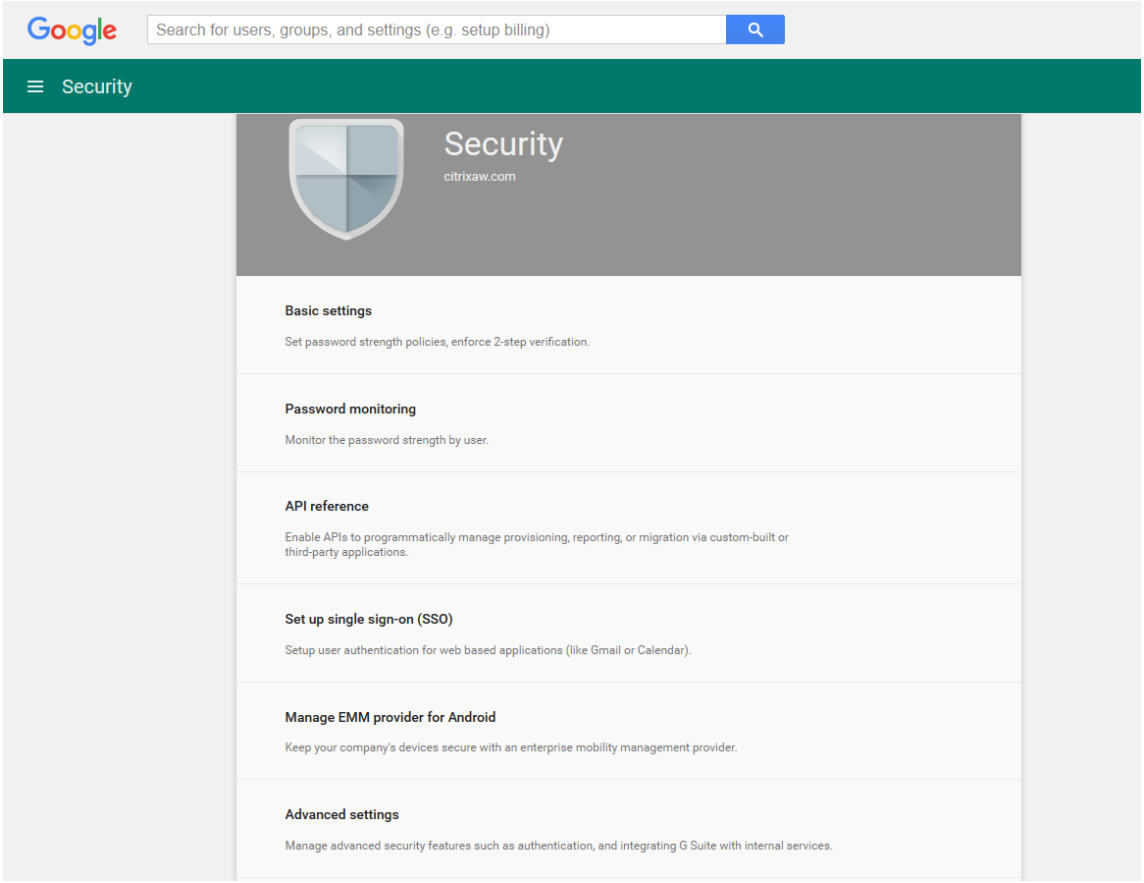


17. Na página **Settings**, clique em **Show more** e, em seguida, clique em **Advanced settings**.

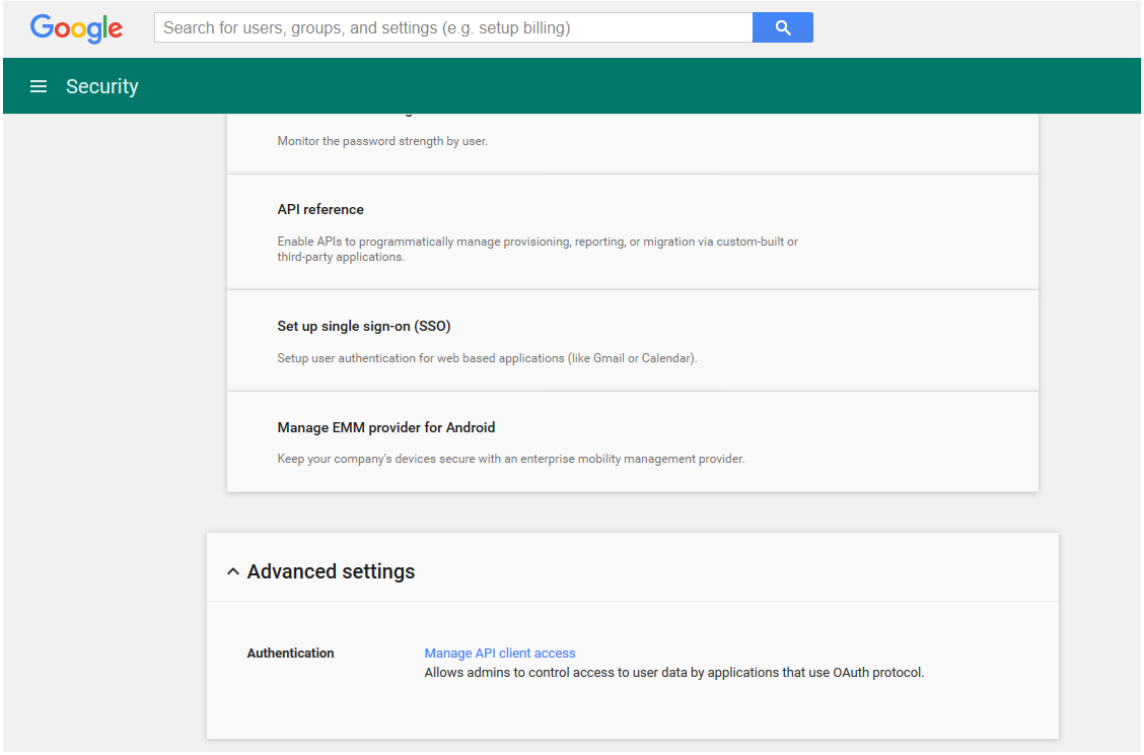
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

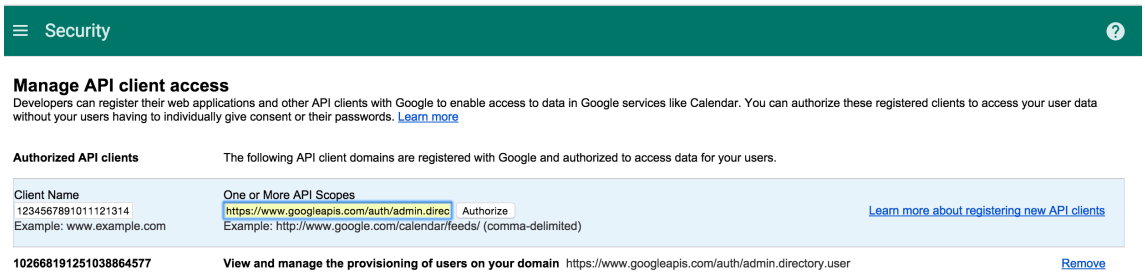


18. Clique em **Manage API client access**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

19. Em **Client Name**, insira o ID de cliente que você salvou anteriormente, em **One or More API Scopes**, insira `https://www.googleapis.com/auth/admin.directory.user` e clique em **Authorize**.



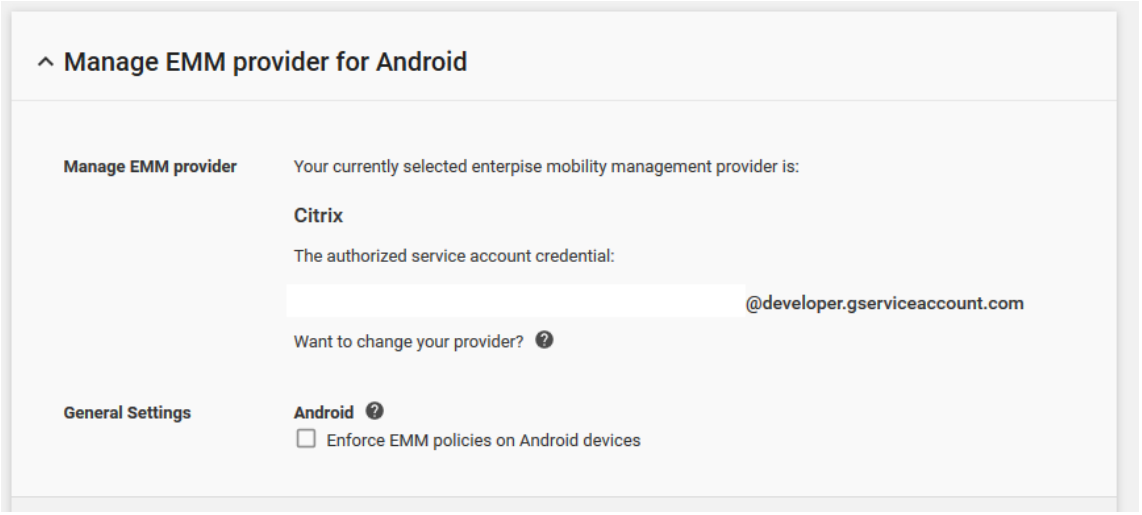
Vinculando ao EMM

Antes de usar o XenMobile para gerenciar os seus dispositivos do Android, você deve contatar o Suporte Técnico da Citrix e fornecer o seu nome de domínio, conta de serviço e token de associação. A Citrix associa o token ao XenMobile como o seu provedor de gerenciamento de mobilidade empresarial (EMM). Para informações de contato para suporte técnico da Citrix, consulte o Suporte Técnico da Citrix..

1. Para confirmar a associação, faça login no portal do Google Admin e clique em **Security**.
2. Clique em **Manage EMM provider for Android**.

   Você verá que a conta do Google Android for Work está associada à Citrix como seu provedor de EMM.

   Depois de confirmar o token de associação, você poderá começar a usar o XenMobile para gerenciar dispositivos Android. Importe o certificado P12 gerado na etapa 14. Defina as configurações do servidor do Android for Work, ativar o logon único baseado em SAML e defina pelo menos uma política de dispositivo do Android for Work.

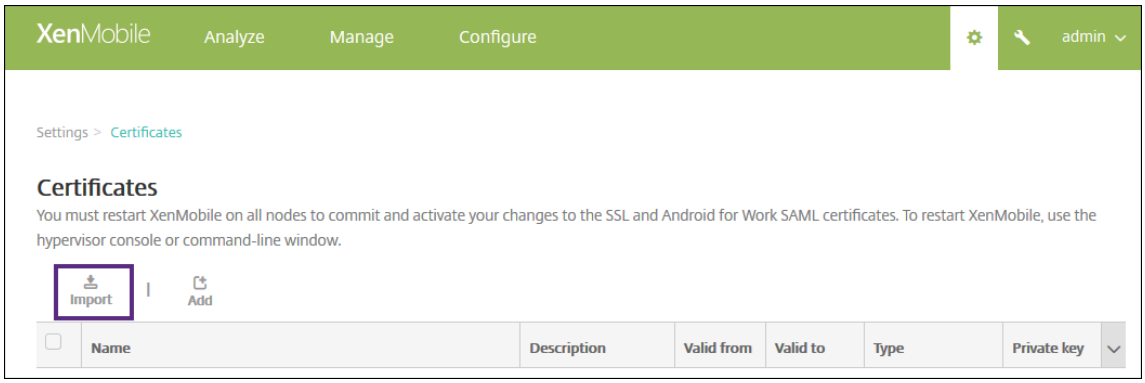


© 1999-2019 Citrix Systems, Inc. All rights reserved.

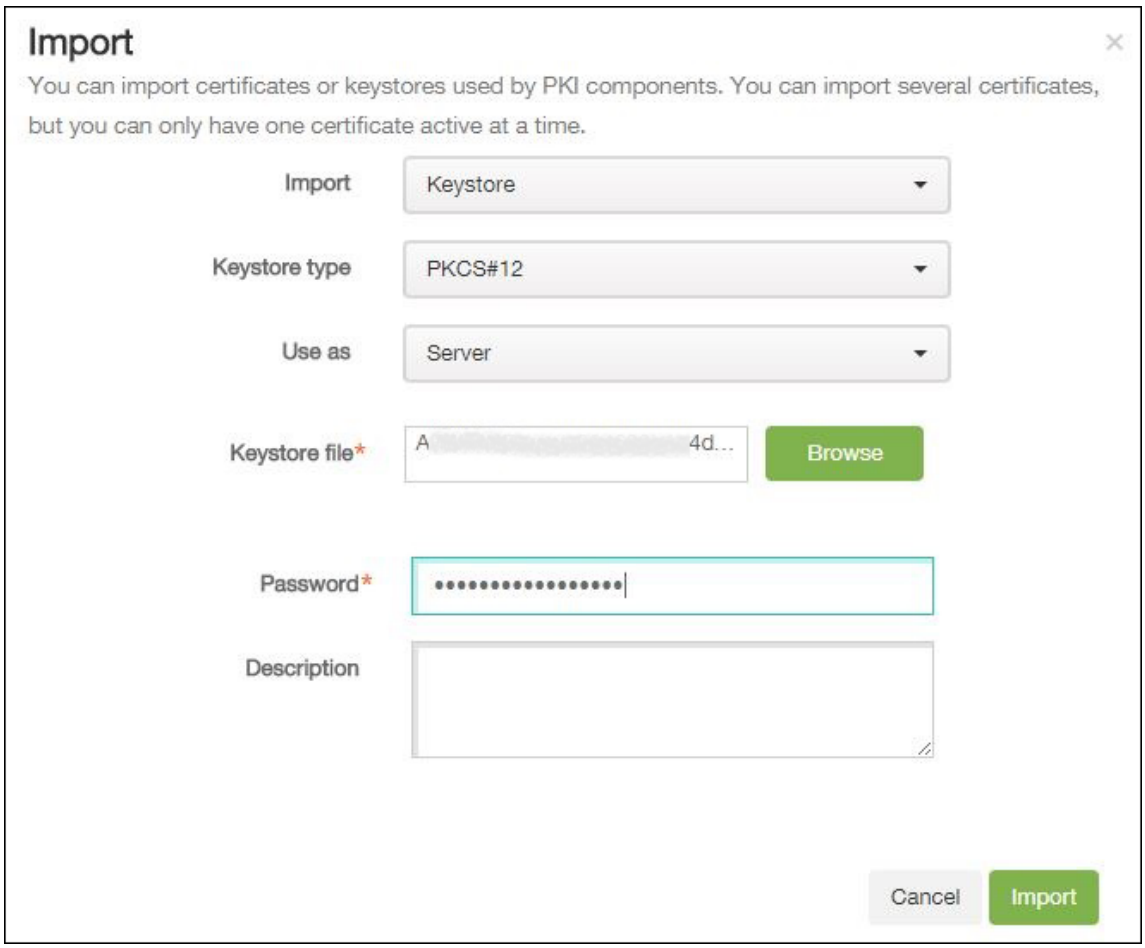
Importe o certificado P12

Siga estas etapas para importar o certificado P12 do Android for Work:

1. Faça login no console XenMobile.
2. Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e clique em **Certificados**. A página **Certificados** é exibida.



3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

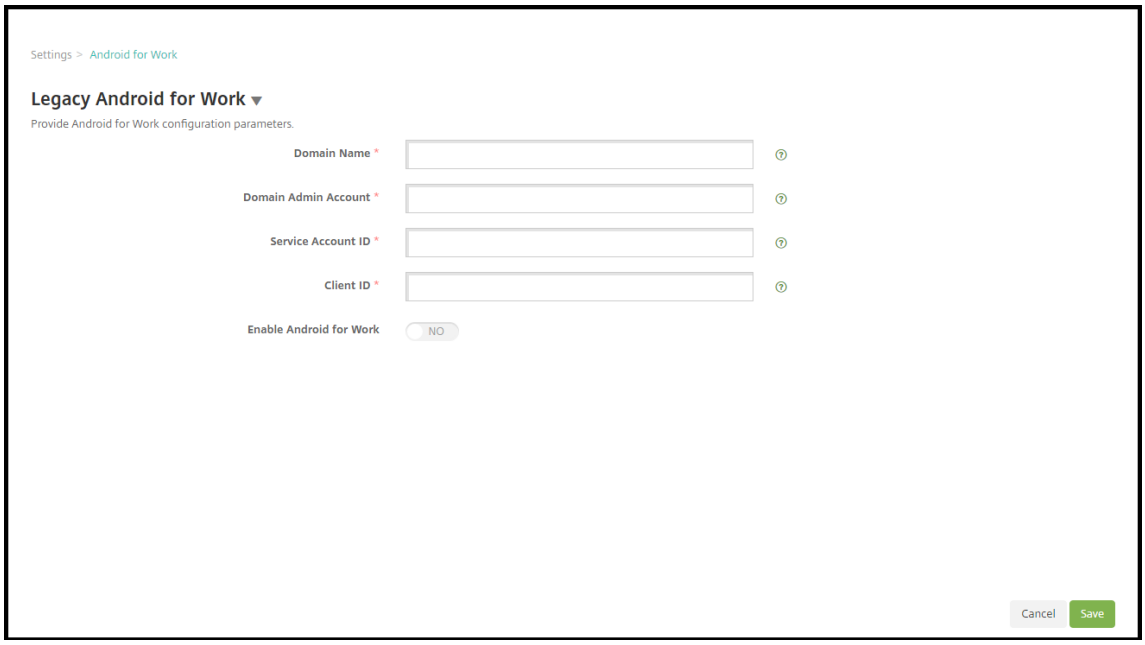
Faça as seguintes configurações:

- **Importar:** na lista, clique em **Keystore**.
- **Tipo de keystore:** na lista, clique em **PKCS#12**.
- **Usar como:** na lista, clique em **Servidor**.
- **Arquivo de keystore:** clique em **Procurar** e navegue até o certificado P12.
- **Senha:** digite a senha do keystore.
- **Descrição:** opcionalmente, digite uma descrição do certificado.

4. Clique em **Importar**.

Definir as configurações de servidor do Android for Work

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Android for Work**. A página **Android for Work** é exibida.



Defina as configurações a seguir e clique em **Salvar**.

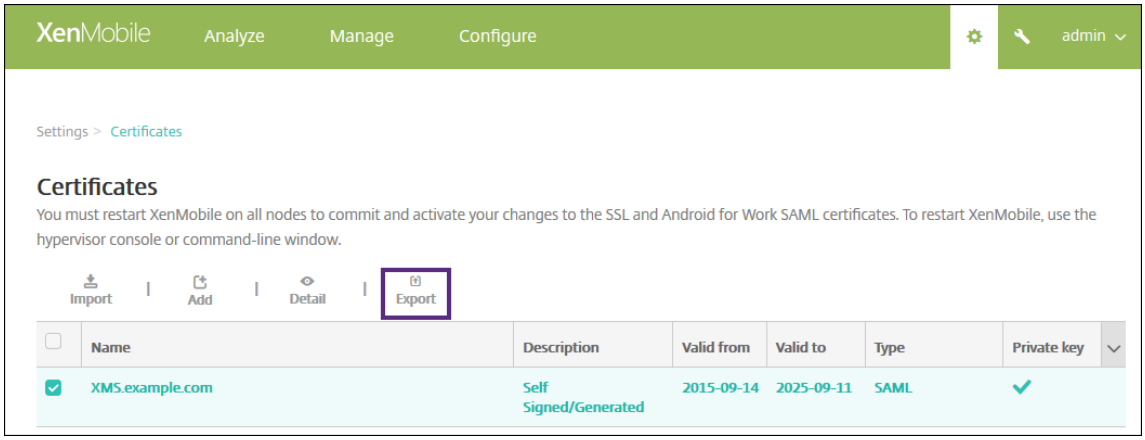
- **Nome de domínio:** digite o nome de domínio do Android for Work; por exemplo, domínio.com.
- **Conta de administrador de domínio:** digite o nome de usuário do administrador de domínio, por exemplo, a conta de email utilizada no Google Developer Portal.
- **ID da conta de serviço:** digite o ID da sua conta de serviço, por exemplo, o e-mail associado à Conta de serviço do Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

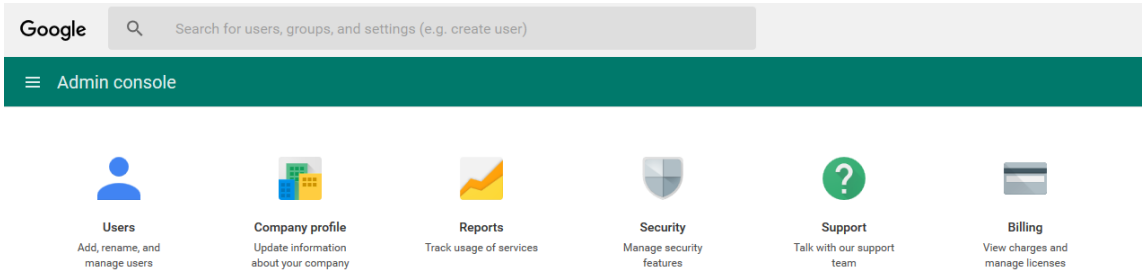
- **ID do cliente:** digite o ID numérico do cliente da sua conta de serviço do Google.
- **Ativar Android for Work:** selecione para ativar ou desativar o Android for Work.

Ativar o logon único baseado em SAML

1. Faça login no console 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.

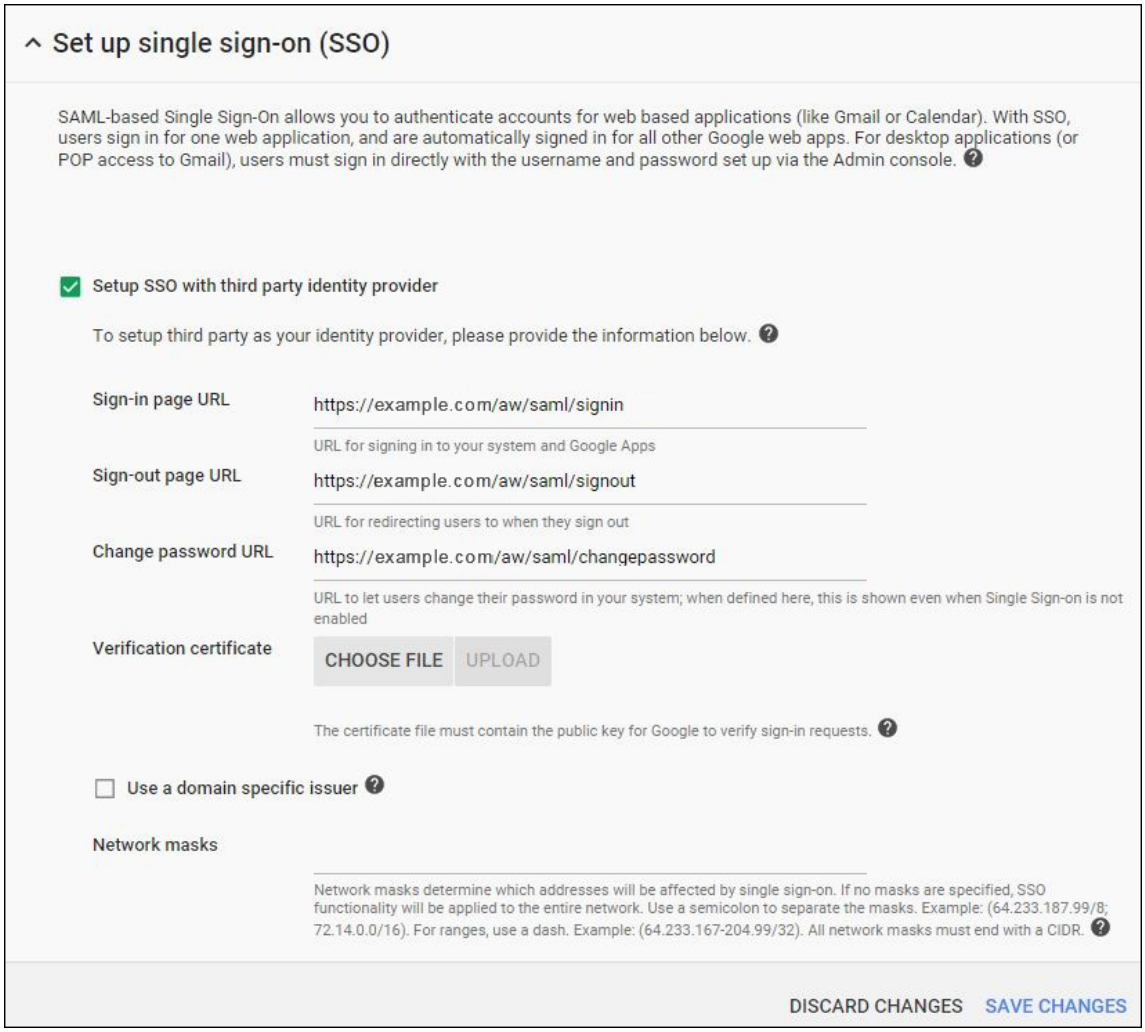


4. Na lista de certificados, clique no certificado SAML.
5. Clique em **Exportar** e salve o certificado no seu computador.
6. Faça login no portal do Google Admin usando as credenciais de administrador do Android for Work. Para acessar o portal, consulte Portal do Google Admin.
7. Clique em **Security**.



8. Em **Security**, clique em **Set up single sign-on (SSO)** e faça as seguintes configurações.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



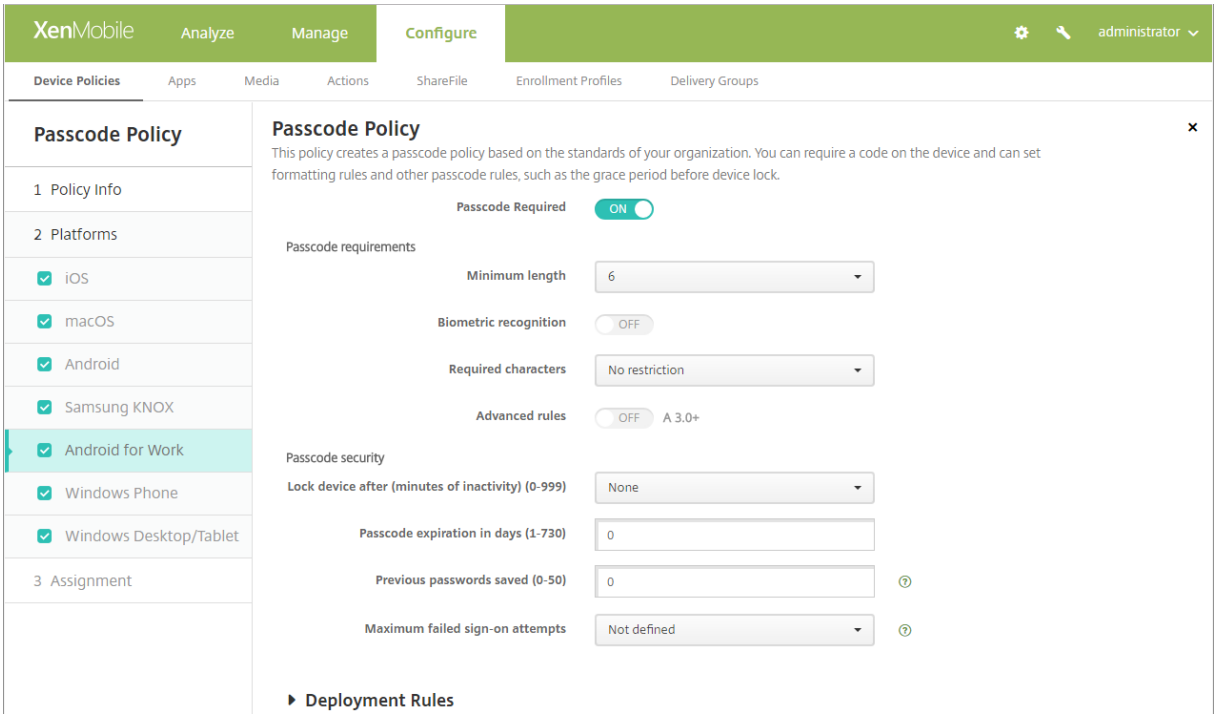
- **Sign-in page URL:** digite a URL para os usuários que estão fazendo login no seu sistema e no Google Apps. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign out page URL:** digite a URL para a qual os usuários são redirecionados quando fazem logoff. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Change password URL**: digite a URL para permitir que os usuários alterem as respectivas senhas no seu sistema. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Se este campo é definido, os usuários veem esse prompt, mesmo quando o SSO não está disponível.
- **Verification certificate:** clique em **CHOOSE FILE** e navegue até o certificado SAML exportado do XenMobile.

9. Clique em **SAVE CHANGES**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar uma política de dispositivo do Android for Work

Configure uma política de código secreto para que os usuários tenham que estabelecer um código secreto 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 XenMobile.
2. Clique **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 você deseja adicionar. Nesse exemplo, você clica em **Código secreto**.
4. Preencha a página **Informações sobre a política**.
5. Clique em **Android for Work** e defina as configurações da política.
6. Atribua a política a um Grupo de Entrega.

Políticas MDX e as políticas de dispositivo com suporte

A tabela a seguir exibe as políticas de dispositivo e as políticas de MDX compatíveis com o contêiner do Android for Work. Para obter mais informações sobre políticas de dispositivos e políticas de MDX, consulte Políticas de dispositivo e Resumo das políticas do MDX, respectivamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de autenticação	Compatível	Valores suportados	Observações
Código secreto do aplicativo	X	Todas	
Sessão online obrigatória		Somente desativado	
Período máximo offline	X	Todas	
NetScaler Gateway alternativo		Somente em branco	

Políticas de acesso à rede do aplicativo	Compatível	Valores suportados	Observações
Acesso à rede	X	Todas	
Etiqueta de certificado		Somente em branco	
Modo VPN preferido	X	Todas	
Permitir mudança de modo VPN	X	Todas	
URL do arquivo PAC ou servidor proxy	X	Todas	
Saída de log padrão	X	Todas	
Nível padrão de log	X	Todas	
Máx. de arquivos de log	X	Todas	
Tamanho máximo de arquivo de log	X	Todas	
Redirecionar logs de aplicativo	X	Todas	
Logs de criptografia	X	Todas	
Redes WiFi em lista branca		Somente em branco	

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de segurança de dispositivos	Compatível	Valores suportados	Observações
Bloquear dispositivos com jailbreak ou root	X	Todas	
Exigir criptografia do dispositivo	X	Todas	
Exigir bloqueio do dispositivo	X	Todas	

Políticas de Requisitos de Rede	Compatível	Valores suportados	Observações
Exigir WiFi	X	Desativado	

Outras Políticas de Acesso	Compatível	Valores suportados	Observações
Período de tolerância de atualização de aplicativo (horas)	X	Todas	
Apagar dados de aplicativo ao bloquear	X	Todas	
Intervalo ativo de sondagem (minutos)	X	Todas	

Políticas de criptografia	Compatível	Valores suportados	Observações
Chaves de criptografia	X	Acesso Offline permitido	Suporte por meio da política do Android Enterprise
Criptografia privada de arquivo	X	Somente desativado	Suporte por meio da política do Android Enterprise

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de criptografia	Compatível	Valores suportados	Observações
Exclusões de criptografia privada de arquivo	X	NA (vazio)	Suporte por meio da política do Android Enterprise
Limites de acesso para arquivos públicos	X	NA (vazio)	Suporte por meio da política do Android Enterprise
Criptografia pública de arquivo	X	Somente desativado	Suporte por meio da política do Android Enterprise
Exclusões de criptografia pública de arquivo	X	NA (vazio)	Suporte por meio da política do Android Enterprise
Migração de arquivo pública	X	Somente desativado	Suporte por meio da política do Android Enterprise

Políticas de interação de aplicativos	Compatível	Valores suportados	Observações
Grupo de Segurança	X	Vazio	Suporte por meio da política do Android Enterprise
Recortar e copiar	X	Somente irrestrita	Suporte por meio da política do Android Enterprise
Colar	X	Somente irrestrita	Suporte por meio da política do Android Enterprise
Troca de documentos (Abrir em)	X	Somente irrestrita	Suporte por meio da política do Android Enterprise
Troca de documentos de entrada (Abrir em)	X	Todas	Suporte por meio da política do Android Enterprise

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de interação de aplicativos	Compatível	Valores suportados	Observações
Lista branca de troca de documentos recebidos	X	Vazio	Suporte por meio da política do Android Enterprise
Lista restrita de exceção de Abrir em	X	Vazio	Suporte por meio da política do Android Enterprise

Políticas de restrições de aplicativos	Compatível	Valores suportados	Observações
Bloquear câmera	X	Somente ativado	Suporte por meio da política do Android Enterprise
Bloquear galeria	X	Somente ativado	Suporte por meio da política do Android Enterprise
Bloquear conexão localhost	X	Todas	
Bloquear gravação de microfone	X	Somente desativado	Suporte por meio da política do Android Enterprise
Bloquear serviços de localização	X	Somente desativado	Suporte por meio da política do Android Enterprise
Bloquear composição de SMS	X	Somente desativado	Suporte por meio da política do Android Enterprise
Bloquear captura de tela	X	Somente desativado	Suporte por meio da política do Android Enterprise
Bloquear sensor de dispositivo	X	Todas	
Bloquear NFC	X	Somente desativado	Suporte por meio da política do Android Enterprise

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de restrições de aplicativos	Compatível	Valores suportados	Observações
Bloquear impressão	X	Todas	
Bloquear logs de aplicativo	X	Todas	

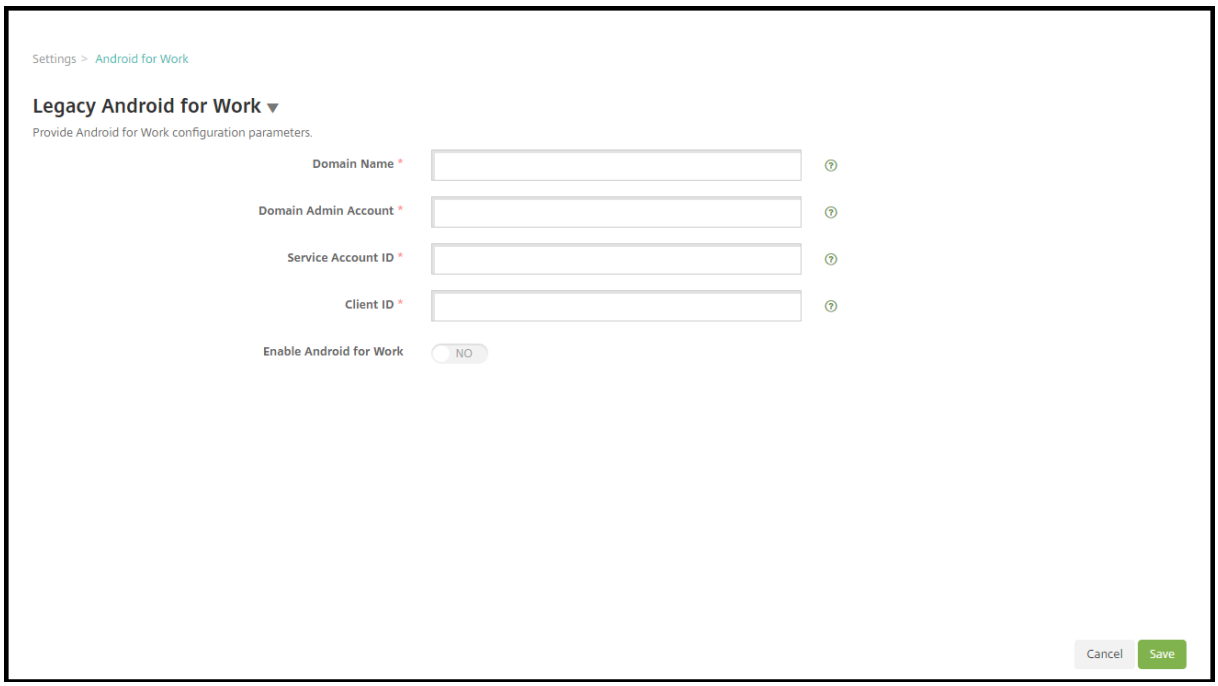
Políticas de geocerca de aplicativos	Compatível	Valores suportados	Observações
Longitude do ponto central	X	Todas	
Latitude do ponto central	X	Todas	
Raio	X	Todas	

Definir as configurações de conta do Android for Work

Antes de começar a gerenciar aplicativos e políticas do Android nos dispositivos, você deverá configurar as informações de domínio e conta do Android for Work no XenMobile. Primeiro, conclua as tarefas de instalação do Android for Work no Google para configurar um administrador de domínio e obter um ID de conta de serviço e um token de associação.

1. No console da Web XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Android for Work**. A página de configuração do **Android for Work** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



1. Na página **Android for Work**, faça as seguintes configurações:
    - **Nome de domínio:** digite seu nome de domínio.
    - **Conta de administrador de domínio:** digite o nome do usuário do seu administrador de domínio.
    - **ID de conta de serviço:** digite o seu ID de Conta de Serviço do Google.
    - **ID do cliente:** digite o ID do cliente da sua conta de serviço do Google.
    - **Ativar Android for Work:** selecione se deseja ativar Android for Work ou não.
2. Clique em **Salvar**.

Configurar o acesso do parceiro do G Suite para o XenMobile

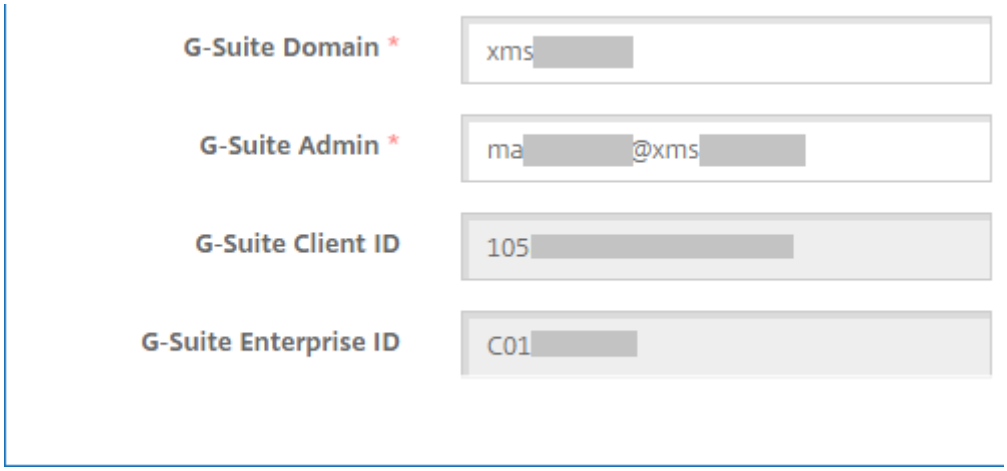
Alguns recursos de gerenciamento de ponto de extremidade do Chrome usam APIs de parceiros do Google para se comunicar entre o XenMobile e seu domínio do G Suite. Por exemplo, o XenMobile exige as APIs para políticas de dispositivos que gerenciam recursos do Chrome, como o modo de navegação Anônima e o modo Visitante.

Para ativar as APIs de parceiros, você configura seu domínio do G Suite no console XenMobile e configura sua conta do G Suite.

Configurar seu domínio do G Suite no XenMobile

Para permitir que o XenMobile se comunique com as APIs no seu domínio do G Suite, acesse **Configurações > Configuração do Google Chrome** e defina as configurações.

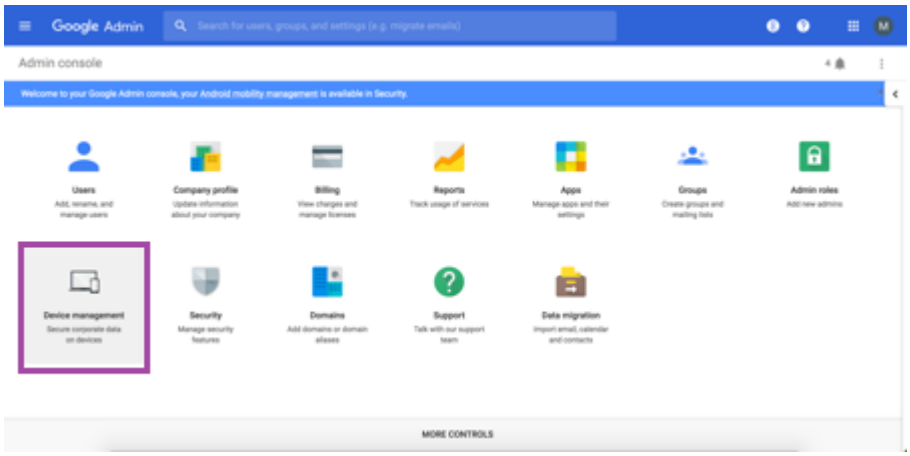
© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Domínio do G Suite:** o domínio do G Suite que hospeda as APIs necessárias ao XenMobile.
- **Conta de administrador do G Suite:** a conta de administrador do seu domínio do G Suite.
- **ID de cliente do G Suite:** o ID de cliente para a Citrix. Use esse valor para configurar o acesso de parceiros para seu domínio do G Suite.
- **ID empresarial do G Suite:** o ID empresarial da sua conta, preenchido a partir da sua conta corporativa do Google.

Ativar o acesso de parceiros para dispositivos e usuários no seu domínio do G Suite

1. Faça login no Admin Console do Google: https://admin.google.com
2. Clique em **Gerenciamento de dispositivos**.

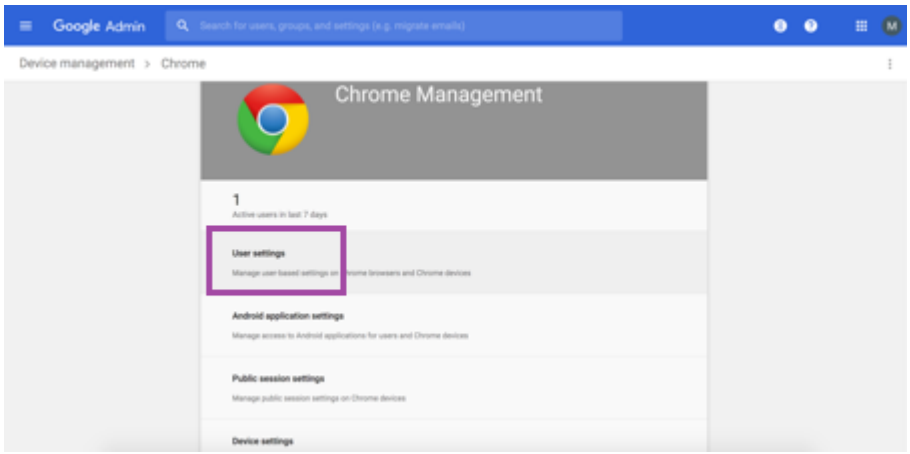


3. Clique em **Gerenciamento do Chrome**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Clique em **Configurações do usuário**.



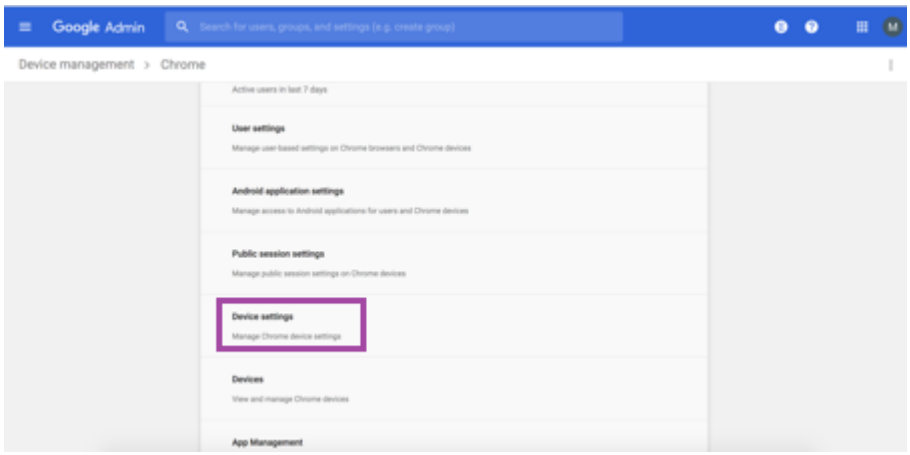
5. Pesquise pelo **Gerenciamento do Chrome - Acesso para parceiros**.



6. Marque a caixa de seleção **Ativar o gerenciamento do Chrome - Acesso para parceiros**.
7. Aceite que você entende e deseja ativar o acesso para parceiros. Clique em **Salvar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

8. Na página de gerenciamento do Chrome, clique em **Configurações do dispositivo**.



9. Pesquise pelo **Gerenciamento do Chrome - Acesso para parceiros**.

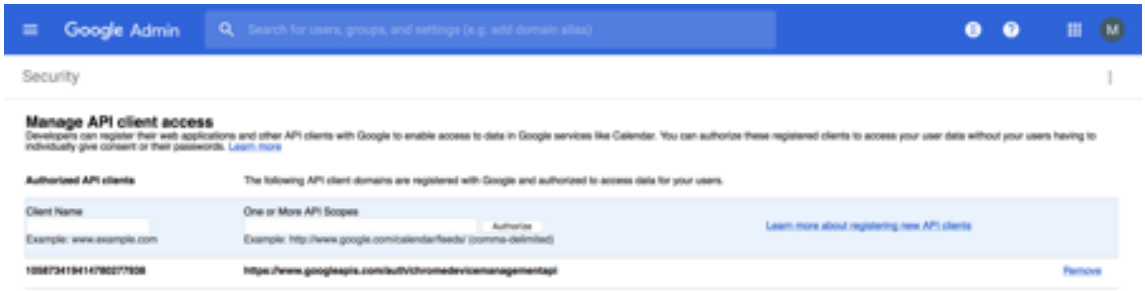


10. Marque a caixa de seleção **Ativar o gerenciamento do Chrome - Acesso para parceiros**.
11. Aceite que você entende e deseja ativar o acesso para parceiros. Clique em **Salvar**.
12. Vá para a página **Segurança** e clique em **Configurações avançadas**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



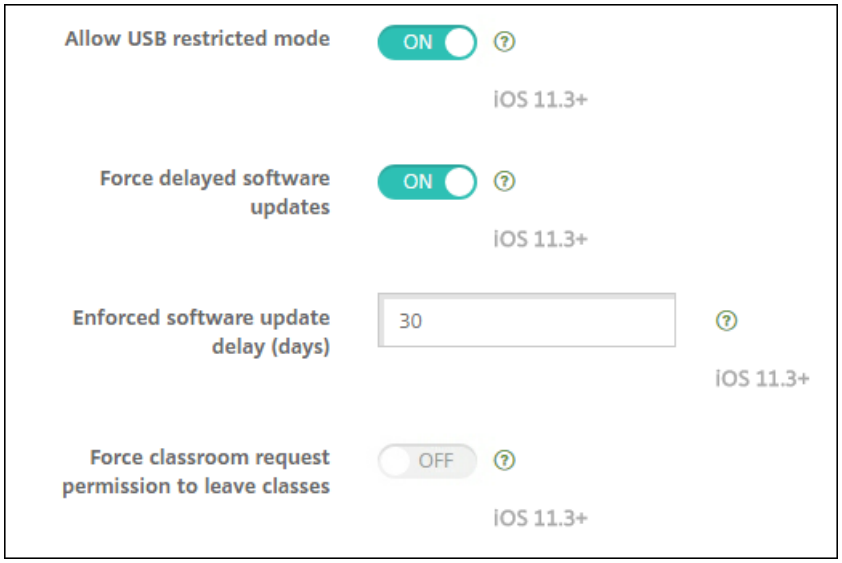
13. Clique em **Gerenciar acesso de cliente de API**.
14. No console XenMobile, acesse **Configurações > Configuração do Google Chrome** e copie o valor do ID do cliente do G Suite. Em seguida, retorne à página **Gerenciar acesso de cliente de API** e cole o valor copiado no campo **Nome do cliente**.
15. Em **Um ou mais escopos de API**, adicione a URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. Clique em **Autorizar**.

    A mensagem “Suas configurações foram salva” é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Inscrição de dispositivos Android for Work

Se o processo de inscrição de seu dispositivo exigir que os usuários digitem um nome de usuário ou ID do usuário, o formato aceito depende da forma como o servidor XenMobile está configurado para procurar usuários pelo nome UPN ou pelo nome da conta SAM.

Se o XenMobile Server estiver configurado para procurar usuários por UPN, os usuários devem inserir um UPN no formato:

- *nome de usuário@domínio*

Se o XenMobile Server estiver configurado para procurar usuários por SAM, os usuários devem inserir um SAM em um destes formatos:

- *nome de usuário@domínio*
- *domínio\nome de usuário*

Para determinar para qual tipo de nome de usuário o XenMobile Server está configurado:

1. No console 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, verifique o campo **Pesquisa de usuário por**:
    - Se estiver definido como **userPrincipalName**, o servidor XenMobile estará definido para UPN.
    - Se estiver definido como **sAMAccountName**, o servidor XenMobile estará definido para SAM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cancelar o registro de um Android for Work Enterprise

Você pode cancelar o registro de uma empresa do Android for Work usando o console do XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile Server abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile Server tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista branca de bloqueio de pop-up.

> **Aviso:**
>
> Depois de o registro de um enterprise ser cancelado, os aplicativos Android for Work nos dispositivos já registrados por meio dele são redefinidos para os estados padrão. Os dispositivos não serão mais gerenciados pelo Google. Registrá-los novamente em um enterprise do Android for Workfor pode não restaurar a funcionalidade anterior sem configuração adicional.

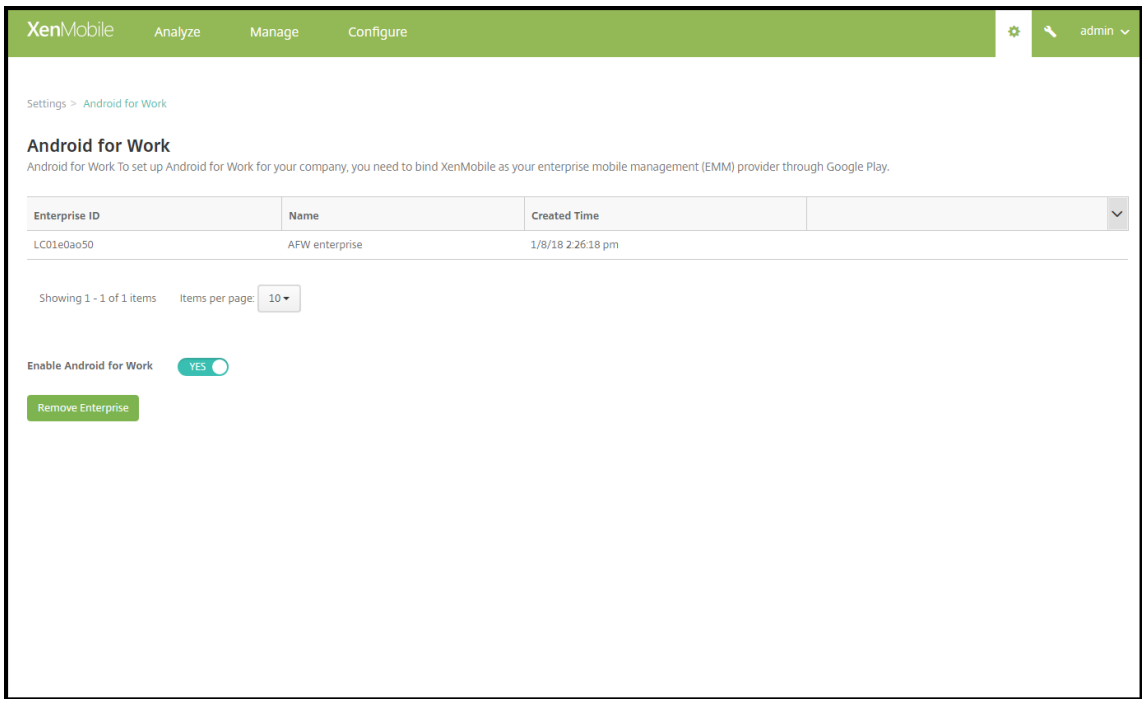
Depois que o registro do enterprise do Android for Work for cancelado:

- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android for Work redefinidos para o estado padrão. As políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work aplicadas anteriormente não afetam mais.
- Os dispositivos registrados por meio do Enterprise são gerenciados pelo XenMobile, mas são não gerenciados pela perspectiva do Google. Nenhum novo aplicativo do Android for Work pode ser adicionado. Não se aplica nenhuma política de Permissões de aplicativos do Android for Work ou de Rrestrições de aplicativos do Android for Work. Outras políticas, como Agendamento, Senha e Restrições, ainda podem ser aplicadas a esses dispositivos.
- Se você tentar registrar dispositivos no Android for Work, eles serão registrados como dispositivos Android, não como dispositivos Android for Work.

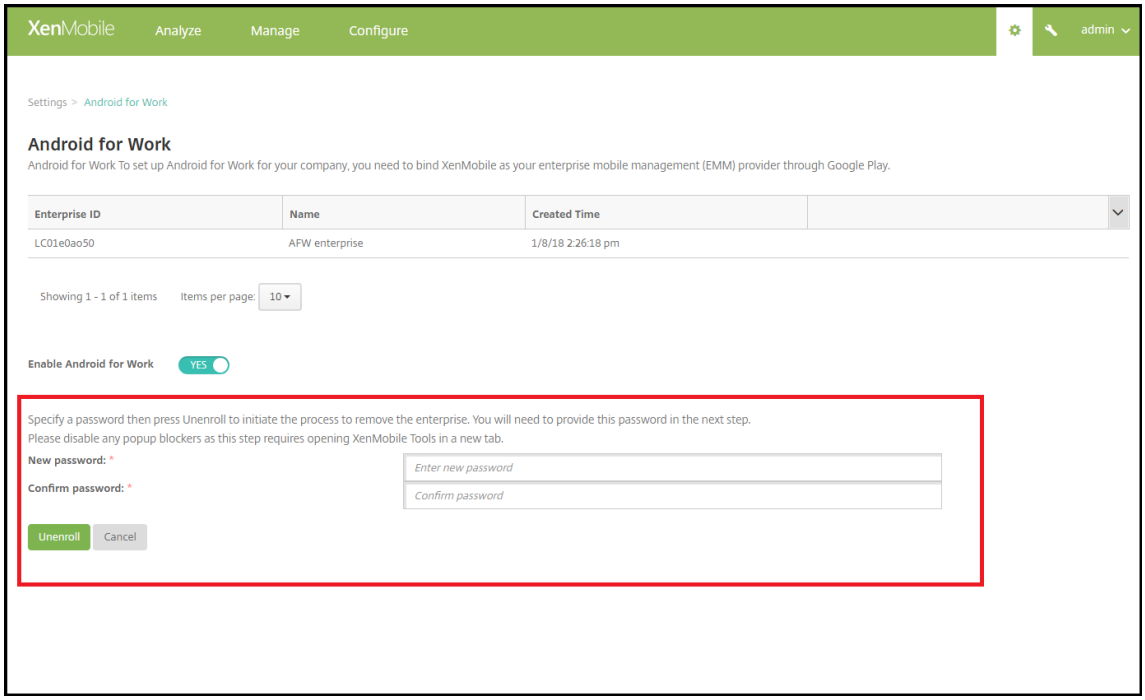
Para cancelar o registro de um Android for Work Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página Configurações é exibida.
2. Na página Configurações, clique em **Android for Work**.
3. Clique em **Remover Enterprise**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

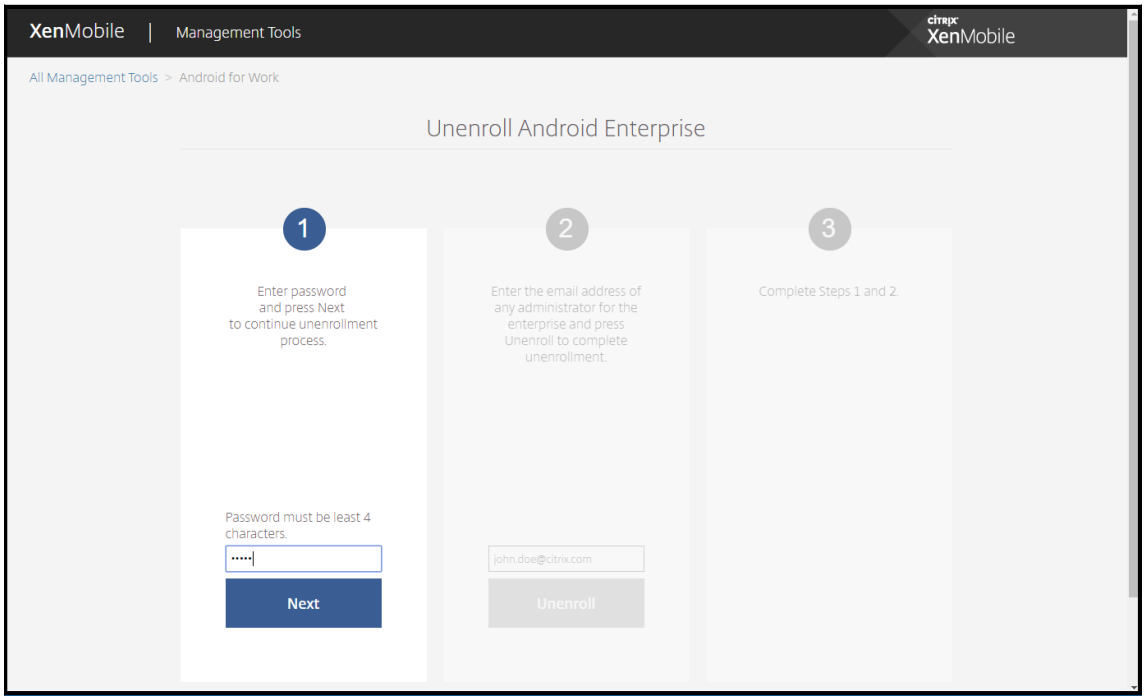


4. Especifique uma senha. Você precisará dela na próxima etapa para concluir o cancelamento do registro. Em seguida, clique em **Cancelar registro**.

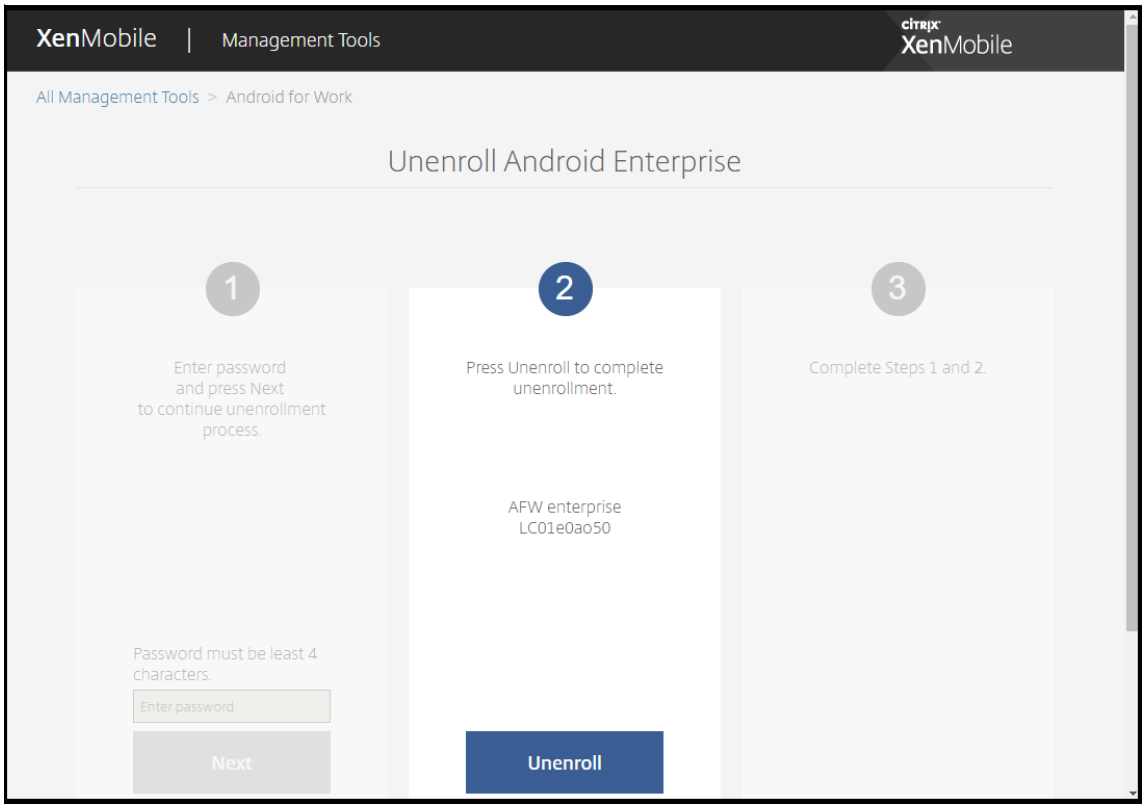


5. Quando a página do XenMobile Tools for aberta, insira a senha que você criou na etapa anterior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Clique em **Cancelar registro**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Provisionamento do modo de dispositivo de trabalho gerenciado no Android for Work

O modo de dispositivo de trabalho gerenciado para o Android for Work está disponível somente para dispositivos de propriedade da empresa. O XenMobile é compatível com estes métodos de registro no modo de dispositivo de trabalho gerenciado:

- **afw#xenmobile:** com esse método de registro, o usuário insere os caracteres "afw#xenmobile" ao configurar o dispositivo. Esse token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub.
- **Código QR:** o provisionamento de código QR é uma maneira fácil de provisionar uma frota distribuída de dispositivos que não são compatíveis com NFC, como tablets. O método de registro de código QR pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. O método de registro de código QR instala e configura o modo de dispositivo de trabalho gerenciado digitalizando um código QR no Assistente de instalação.
- **Aumento da comunicação a curta distância (NFC):** o método de registro de aumento de NFC pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. Um aumento de NFC transfere dados entre dois dispositivos usando comunicação a curta distância. Bluetooth, Wi-Fi e outros meios de comunicação estão desativados em um dispositivo que sofreu uma redefinição de fábrica. O NFC é o único protocolo de comunicação que o dispositivo pode usar nesse estado.

afw#xenmobile

O método de registro é usado após ligar um novo dispositivo ou dispositivos com a configuração inicial de fábrica redefinida. Os usuários digitam "afw#xenmobile" quando solicitados a inserir uma conta do Google. Essa ação baixa e instala o Secure Hub. Os usuários seguem os prompts de configuração do Secure Hub para concluir o registro.

Esse método de registro é recomendado para a maioria dos clientes, porque a versão mais recente do Secure Hub é baixada da loja Google Play. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download no servidor XenMobile.

Pré-requisitos:

- Suportado em todos os dispositivos Android com Android 5.0 e superior.

Código QR

Para registrar um dispositivo no modo de dispositivo usando um código QR, você pode gerar um código QR criando um JSON e convertendo o JSON em um código QR. A câmera do dispositivo escaneia o código QR para registrar o dispositivo.

Pré-requisitos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Suportado em todos os dispositivos Android com Android 7.0 e superior.

Criar um código QR 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 para o Citrix XenMobile Server como um aplicativo empresarial, ele pode ser baixado de`https://<fqdn>:4443/*instanceName*/worxhome.apk`. O caminho para o Secure Hub APK deve ser acessível através da conexão Wi-Fi em que 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 com duas letras minúsculas (por exemplo, en), conforme definido pela ISO 639-1. Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela ISO 3166-1. Por exemplo, insira en_US para o inglês falado nos Estados Unidos.

- **android.app.extra.PROVISIONING_TIME_ZONE:** o fuso horário em que o dispositivo é executado.

  Insira um nome Olson da área/localização do formulário. 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 (Epoch).

  A época do Unix (ou hora do Unix, hora do POSIX ou carimbo de data/hora do Unix) é o número de segundos decorridos desde 1º de janeiro de 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (in ISO 8601: 1970-01-01T00:00:00Z).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** definido 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 tem esta aparência:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "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 que é criado usando qualquer ferramenta de validação JSON, como https://jsonlint.com. Converta essa sequência JSON em um código QR usando qualquer gerador de código QR on-line, como https://goqr.me.

Este código QR é escaneado por um dispositivo com redefinição de fábrica para registrar o dispositivo no modo de dispositivo de trabalho gerenciado.

Para registrar o dispositivo

Para registrar um dispositivo no modo de dispositivo de trabalho gerenciado, o dispositivo deve estar no estado de redefinição de fábrica.

1. Toque seis vezes na tela de boas-vindas para iniciar o fluxo de registro do 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 através desta rede Wi-Fi.

   Depois que o dispositivo se conecta com êxito a 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 o proprietário do dispositivo.

Para mais informações, consulte este Guia do Google para desenvolvedores de EMM para Android: https://developers.google.com/android/work/prov-devices#qr_code_method.

Compartilhamento por NFC

Registrar um dispositivo no modo de dispositivo usando compartilhamentos por NFC requer dois dispositivos: um cujas configurações de fábrica sejam redefinidas e um que esteja executando a XenMobile Provisioning Tool.

Pré-requisitos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Suportado em todos os dispositivos Android com Android 5.0, Android 5.1, Android 6.0 e superior.
- Um XenMobile Server versão 10.4 que está ativado para o Android For Work.
- Um dispositivo com redefinição de fábrica, provisionado para o Android for Work no modo de dispositivo de trabalho gerenciado. Você pode encontrar as etapas para concluir esse pré-requisito neste artigo.
- Outro dispositivo com recursos NFC executando a Provisioning Tool configurada. A Provisioning Tool está disponível no Secure Hub 10.4 ou na Página de downloads Citrix.

Cada dispositivo pode ter somente um perfil do Android for Work, gerenciado por um aplicativo de gerenciamento de mobilidade empresarial (EMM). No XenMobile, o Secure Hub é o aplicativo EMM. Somente um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo EMM remove o primeiro aplicativo EMM.

Você pode iniciar o modo de dispositivo e trabalho gerenciado em dispositivos novos ou restaurados para as configurações de fábrica. Você administra o dispositivo inteiro usando o XenMobile.

Dados transferidos através do aumento de NFC

Provisionar um dispositivo com redefinição de fábrica requer que você envie os seguintes dados por meio de um aumento de NFC para inicializar o Android for Work:

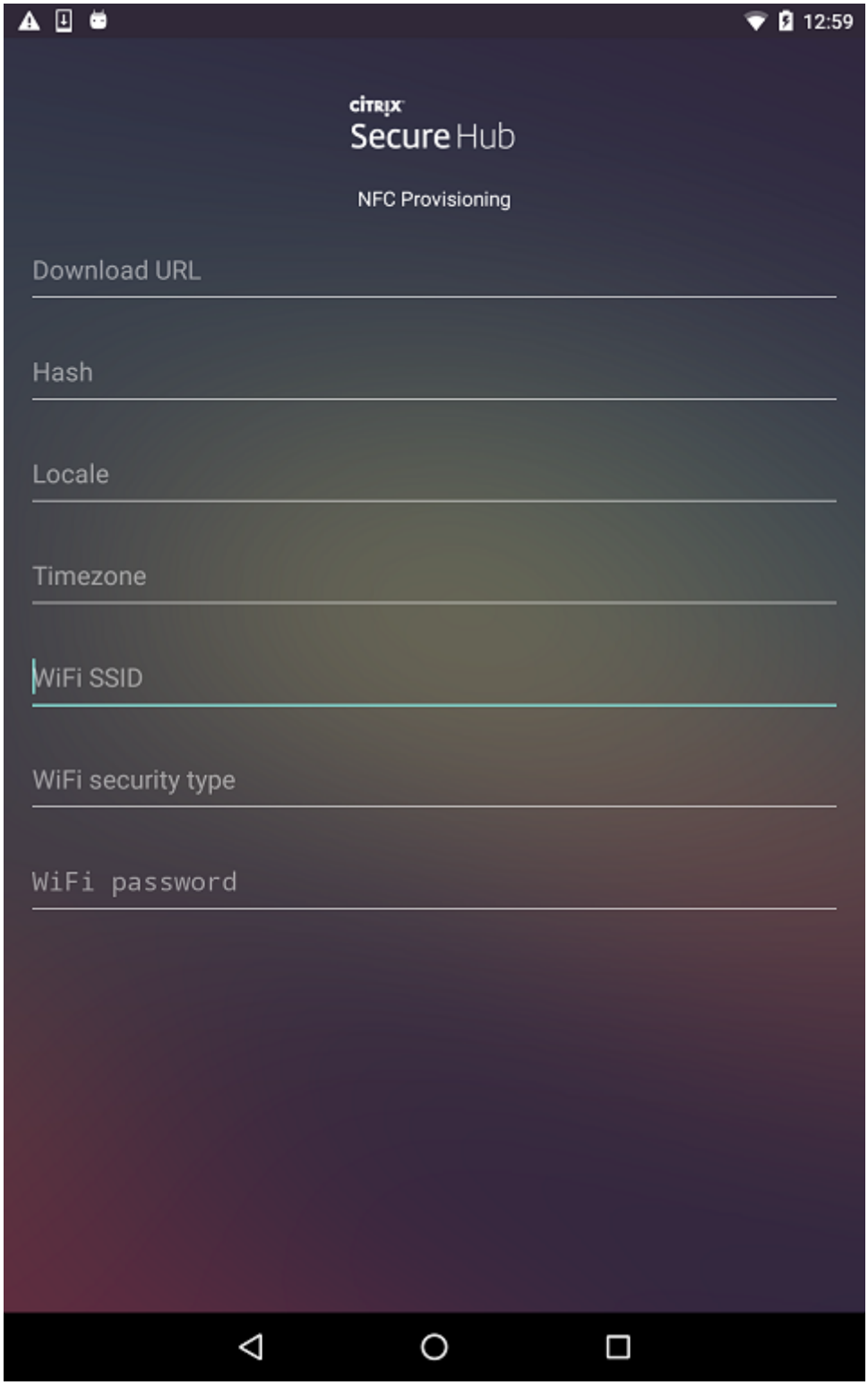
- O nome do pacote do aplicativo do provedor EMM que atua como o proprietário do dispositivo (neste caso, o Secure Hub).
- A localização de Intranet/Internet do qual o dispositivo pode baixar o aplicativo do provedor EMM.
- O hash SHA1 do aplicativo do provedor EMM para verificar se o download é bem-sucedido.
- Os detalhes da conexão WiFi para que um dispositivo com redefinição de fábrica possa se conectar e baixar o aplicativo do provedor EMM. Nota: No momento, o Android não é compatível com WiFi 802.1x para esta etapa.
- O fuso horário do dispositivo (opcional).
- A localização geográfica do dispositivo (opcional).

Quando os dois dispositivos são aumentados, os dados da Provisioning Tool são enviados para o dispositivo com redefinição de fábrica. Esses dados são usados para baixar o Secure Hub com as configurações do administrador. Se você não inserir os valores de localização e fuso horário, o Android os configura automaticamente no novo dispositivo.

Configuração da XenMobile Provisioning Tool

Antes de realizar um aumento de NFC, você deve configurar a Provisioning Tool. Em seguida, essa configuração é transferida para o dispositivo com redefinição de fábrica durante o aumento de NFC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no procedimento a seguir descrevem como configurar o arquivo de texto e contém descrições para cada campo. O aplicativo não salva as informações depois que as digitar, portanto, convém criar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

um arquivo de texto para manter as informações para uso futuro.

Para configurar a Provisioning Tool usando um arquivo de texto

Dê ao arquivo o nome nfcprovisioning.txt e coloque-o na pasta /sdcard/ no cartão SD do dispositivo. Em seguida, o aplicativo poderá ler o arquivo de texto e preencher os valores.

O arquivo de texto deve conter os seguintes dados:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Essa linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo com redefinição de fábrica se conectar a Wi-Fi em seguida ao aumento de NFC, o dispositivo deve ter acesso a esse local para fazer o download. A URL é uma URL regular, sem necessidade de formatação especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>`

Essa linha é a soma de verificação do aplicativo do provedor EMM. Essa soma de verificação é usada para verificar se o download foi bem-sucedido. As etapas para obter a soma de verificação são discutidas neste artigo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esse é o SSID de Wi-Fi conectado do dispositivo no qual a Provisioning Tool está em execução.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Os valores suportados são WEP e WPA2. Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela ISO 639-1. Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela ISO 3166-1. Por exemplo, digite en_US para o 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 no qual o dispositivo está em execução. Insira um nome Olson da área/localização do formulário. Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir nenhum nome, o fuso horário será preenchido automaticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Isso não é necessário, pois o valor é inserido em código fixo no aplicativo, como o Secure Hub. Ele é mencionado aqui somente por uma questão de conclusão.

Se houver um Wi-Fi protegido por WPA2, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
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=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

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 Wi-Fi desprotegida, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
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=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

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 a soma de verificação do Secure Hub

Para obter a soma de verificação de qualquer aplicativo, adicione o aplicativo como um aplicativo empresarial.

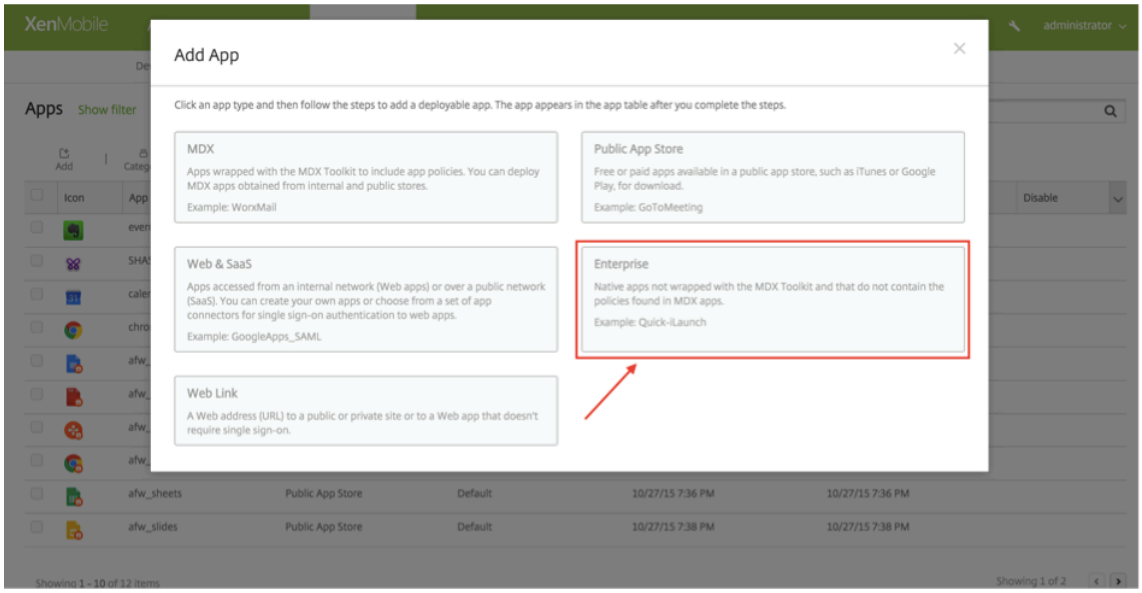
1. No console XenMobile, clique em **Configurar > Aplicativos** e em **Adicionar**.

   A janela **Adicionar aplicativos** é exibida.

2. Clique em **Empresarial**.

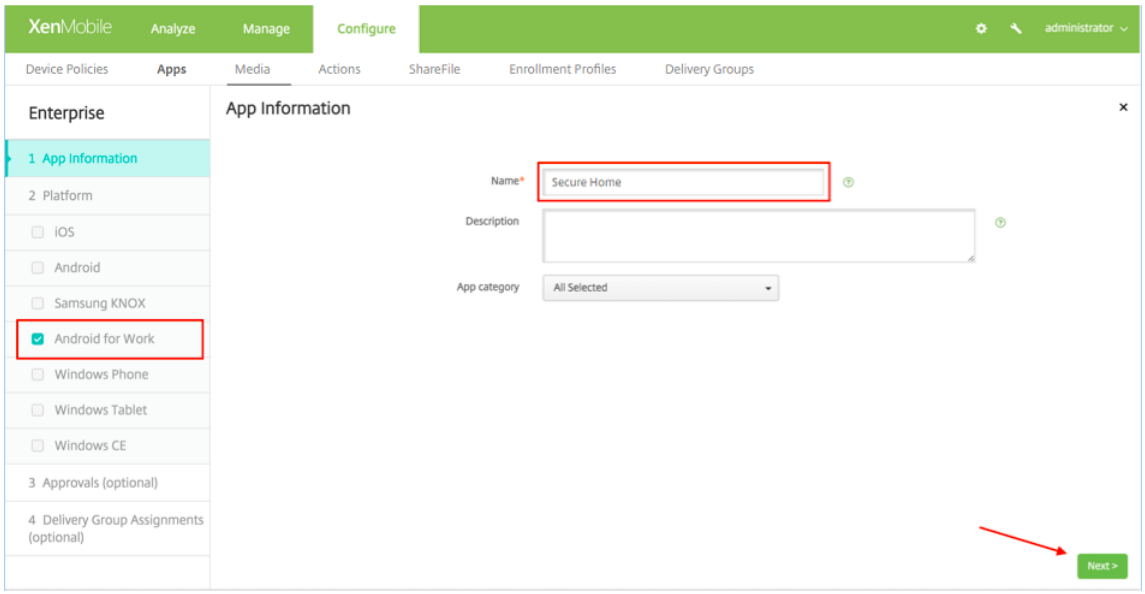
   A página **Informações do Aplicativo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Selecione a configuração a seguir e clique em **Avançar**.

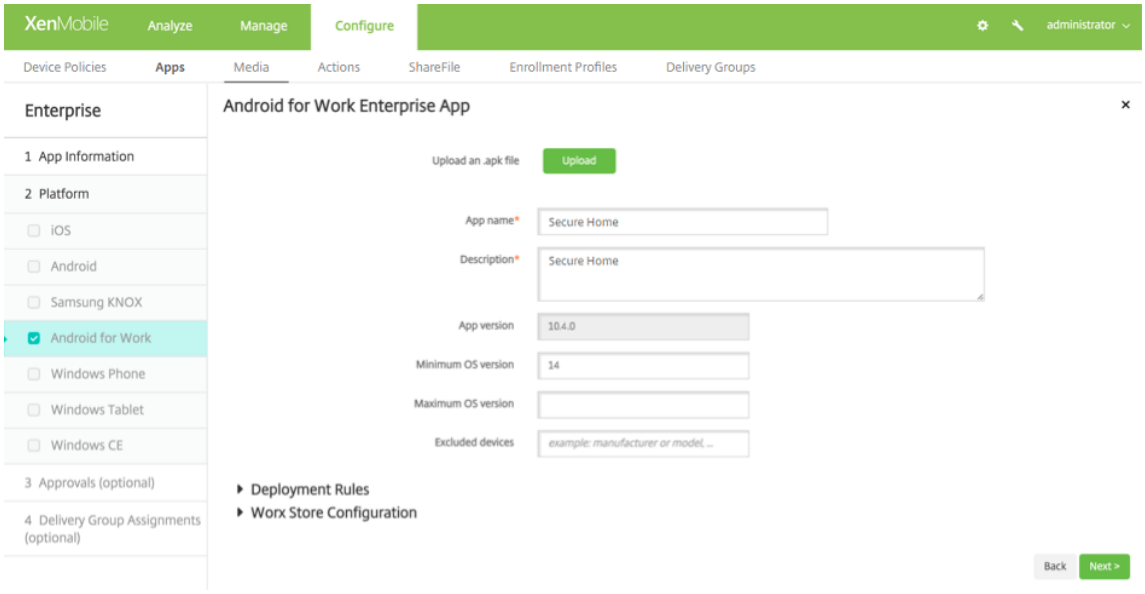
   A tela do **aplicativo Android for Work Enterprise** é exibida.



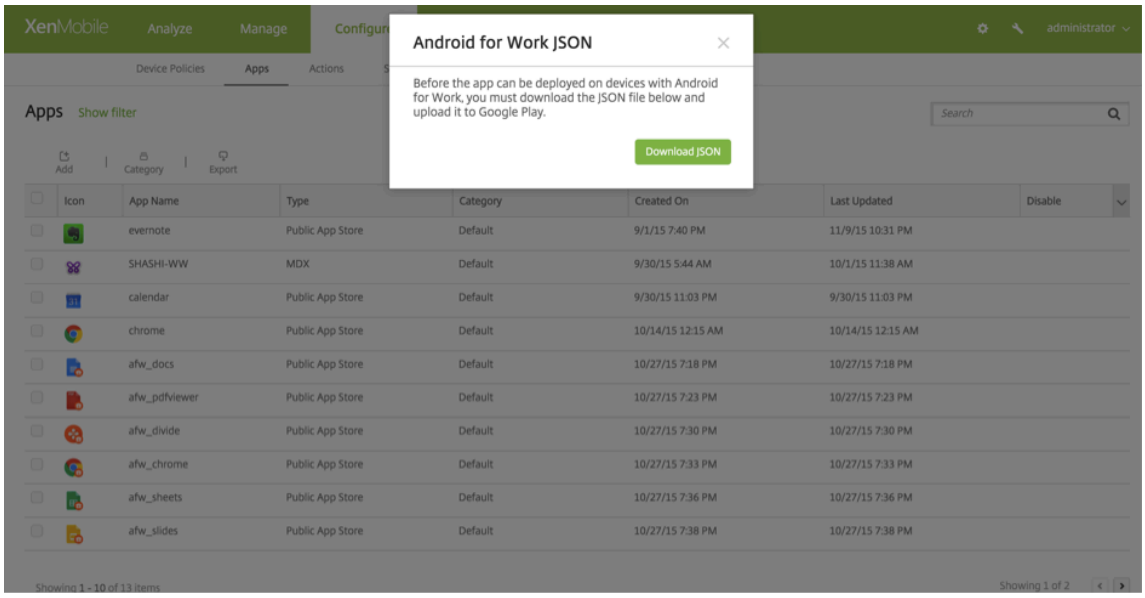
4. Forneça o caminho até o arquivo .apk e clique em **Avançar** para carregá-lo.

   Depois que a instalação for concluída, serão exibidos os detalhes do pacote carregado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Clique em **Avançar** para abrir uma página para baixar o arquivo JSON, que você usará para carregar no Google Play. Para o Secure Hub, não é necessário carregar para Google Play, mas você precisa do arquivo JSON para ler o valor SHA1 dele.



Um arquivo JSON típico tem esta aparência:



6. Copie o **valor file_sha1_base64** e use-o no campo **Hash** na Provisioning Tool.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> O hash deve ser seguro para URLs.

- Converta os símbolos **+** para **-**
- Converta os símbolos **/** para **_**
- Substitua o trailing **\u003d** por **=**

Se você armazenar o hash no arquivo nfcprovisioning.txt no cartão SD do dispositivo, o aplicativo faz a conversão de segurança. No entanto, se você optar por digitar o hash manualmente, será sua responsabilidade garantir a segurança da URL.

Bibliotecas usadas

A Provisioning Tool usa as seguintes bibliotecas no seu código-fonte:

- Biblioteca v7 appcompat, Biblioteca de suporte ao design e biblioteca de paletas v7 do Google sob licença Apache 2.0

  Para obter informações, consulte o Guia de Recursos da Biblioteca de Suporte.

- Butter Knife de Jake Wharton sob a licença Apache 2.0

Provisionar o modo de perfil de trabalho no Android for Work

O modo de perfil de trabalho do Android for Work está disponível para dispositivos nos quais você separa as áreas corporativa e pessoal de um dispositivo. Por exemplo, o modo de perfil de trabalho está disponível para dispositivos BYOD. A experiência de registro do modo de perfil de trabalho é semelhante ao registro do Android no XenMobile. Os usuários fazem o download do Secure Hub a partir do Google Play e registram seus dispositivos.

Por padrão, as configurações de Depuração de USB e Fontes desconhecidas são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

> Dica:
>
> Quando for registrar dispositivos no Android for Work no modo de perfil de trabalho, sempre vá para o Google Play. A partir dali, habilite o Hub Secure para aparecer no perfil pessoal do usuário.

Registrar dispositivos iOS e macOS em massa

April 15, 2019

Você pode registrar um grande número de dispositivos iOS e macOS no XenMobile de duas maneiras.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Você pode usar o Apple Device Enrollment Program (DEP) para registrar os dispositivos iOS e macOS comprados diretamente da Apple, de um revendedor participante autorizado pela Apple ou de uma operadora. O XenMobile é compatível com o Programa de registro de dispositivo para Business e o Apple School Manager para a Educação. Este artigo descreve como integrar contas do DEP Business. Para obter informações sobre as contas DEP do Apple School Manager, consulte Integração com os recursos do Apple Educação.

  Para o registro no DEP de dispositivos macOS, o XenMobile requer que os dispositivos executem o macOS 10.10 ou versões posteriores.

- Outra opção é usar o Apple Configurator para registrar dispositivos iOS, independentemente de você os ter adquirido diretamente da Apple.

Com Business DEP:

- Você não precisa tocar ou preparar os dispositivos. Em vez disso, você envia os números de série ou os números de pedido de compra dos dispositivos por meio do DEP para configurá-los e registrá-los.
- Depois que o XenMobile registrar os dispositivos, você poderá oferecê-los aos usuários, que poderão começar a usá-los imediatamente. Além disso, quando você configura dispositivos usando o DEP, pode eliminar algumas etapas do Assistente de Instalação que os usuários poderiam, de outra forma, precisar concluir quando iniciassem os dispositivos deles pela primeira vez.
- Para obter mais informações sobre como configurar o DEP, consulte a página de Programa de registro de dispositivos da Apple.

Com o Apple Configurator:

- Conecte os dispositivos iOS a um computador Apple que executa o macOS 10.7.2 ou versões posteriores e o aplicativo Apple Configurator 2. Prepare os dispositivos iOS e configure políticas usando o 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. Em seguida, será possível começar a gerenciá-los.
- Para obter mais informações sobre como usar o Apple Configurator, consulte o Configurator Support da Apple.

Pré-requisitos

- Você pode usar o Apple Device Enrollment Program (DEP) para registrar os dispositivos iOS e macOS comprados diretamente da Apple, de um revendedor participante autorizado pela Apple ou de uma operadora. O XenMobile é compatível com o Programa de registro de dispositivo para Business e o Apple School Manager para a Educação. Este artigo descreve como integrar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

contas do DEP Business. Para obter informações sobre as contas DEP do Apple School Manager, consulte Integração com os recursos do Apple Educação.

Você deve abrir as portas necessárias para a conectividade entre o XenMobile e a Apple. Para obter mais informações, consulte Requisitos de porta.

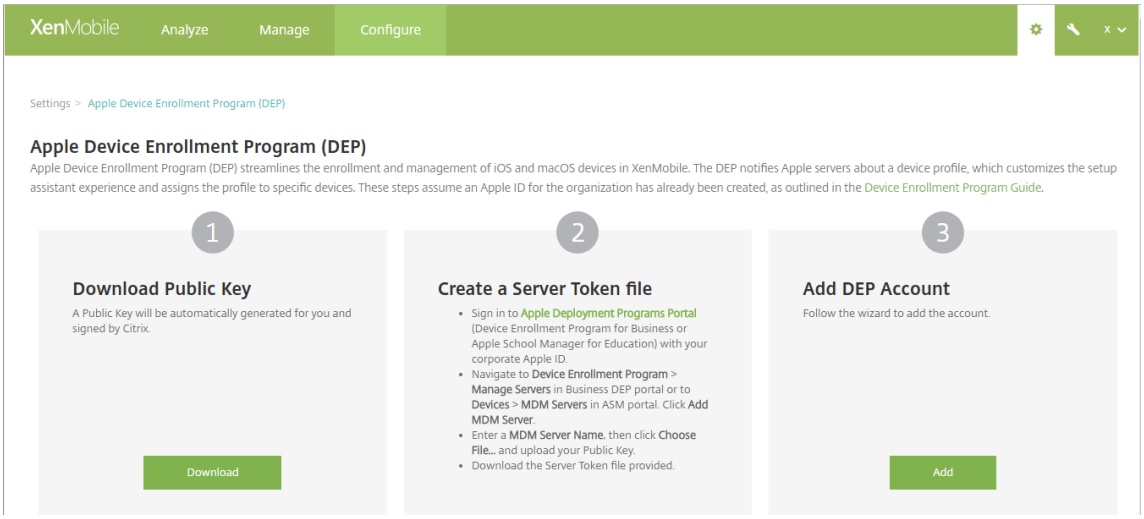
Integrar sua conta do Apple Business DEP ao XenMobile

Se você não tiver uma conta do Apple Business DEP, consulte Implantar dispositivos macOS por meio do Apple DEP.

Para conectar sua conta do Apple Business DEP com sua implantação do XenMobile Server, insira informações no console XenMobile e no Apple DEP Portal, conforme descrito nas etapas a seguir.

Etapa 1: baixe uma chave pública do XenMobile Server

1. Faça login no console XenMobile e acesse **Configurações > Apple Device Enrollment Program (DEP)**.

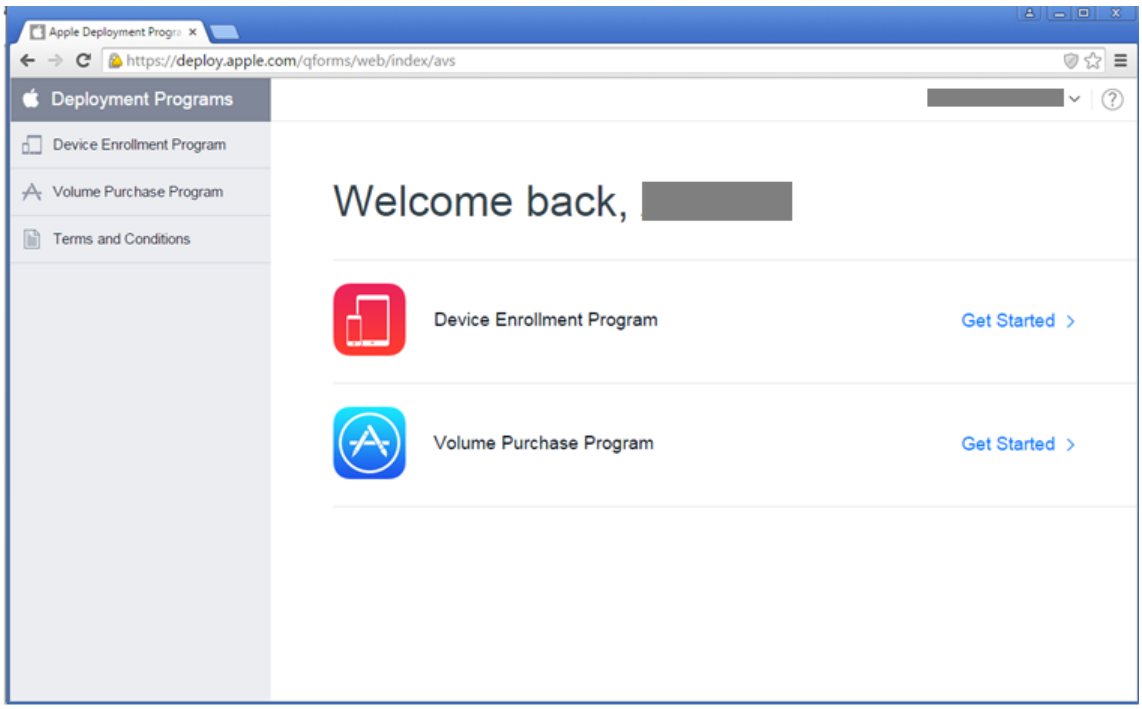


2. Em **Baixar chave pública**, clique em **Baixar**.

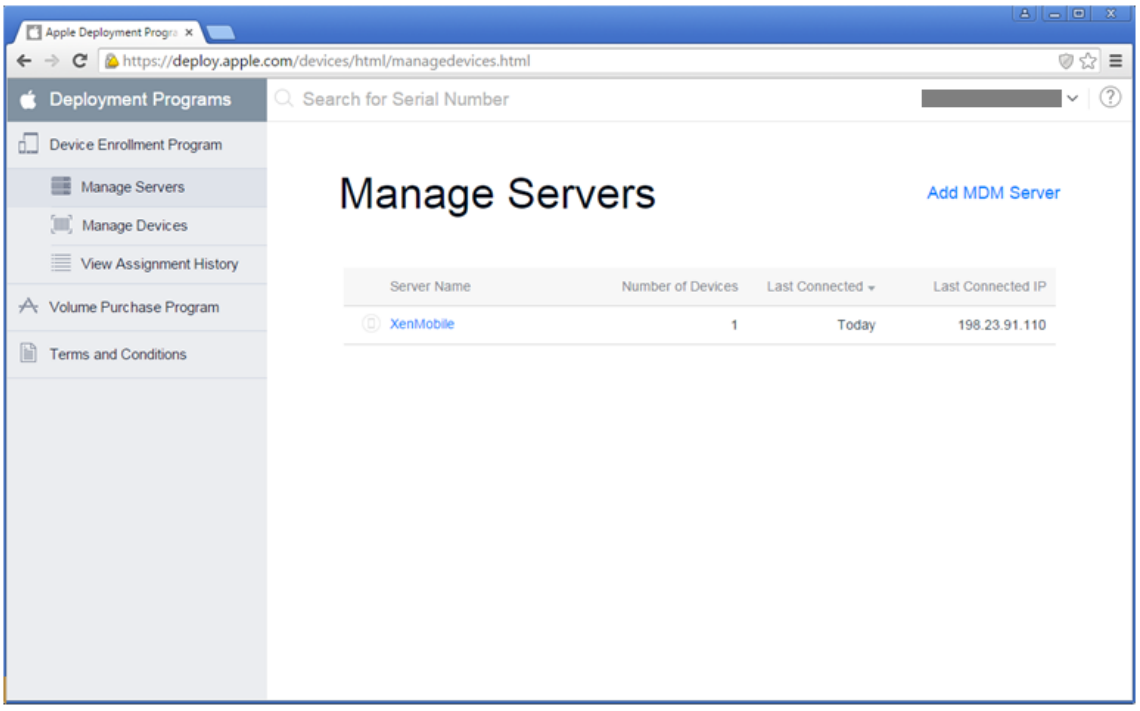
Etapa 2: crie e baixe um arquivo de token de servidor da sua conta da Apple

1. Usando seu ID Apple corporativo, faça login no Portal dos programas de implantação da Apple.
2. No Apple DEP Portal, clique em **Device Enrollment Program**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

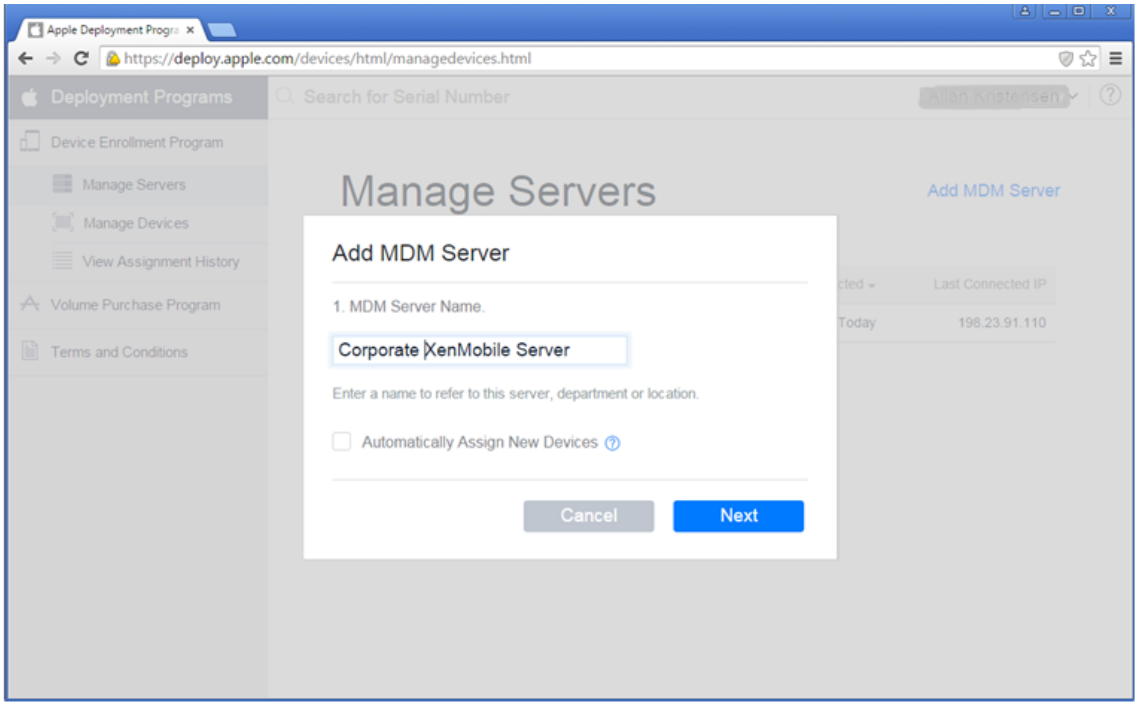


3. Clique em **Manage Servers** e, no lado direito, clique em **Add MDM Server**.

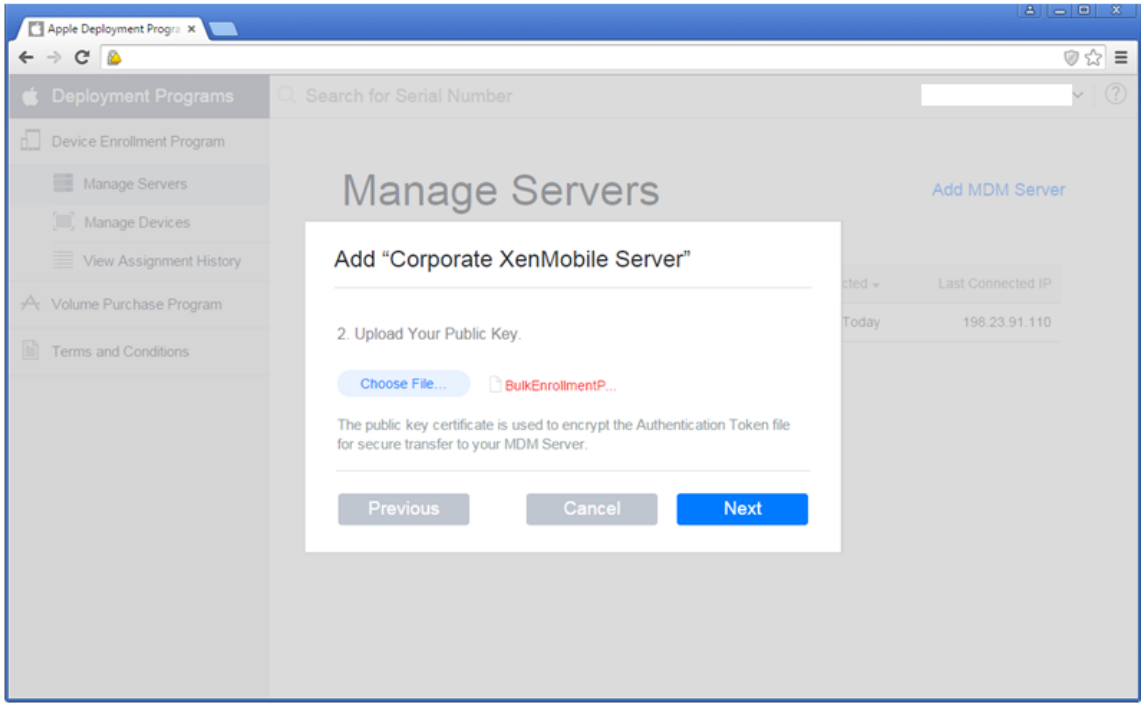


4. Em **Add MDM Server**, digite um nome para o XenMobile Server e clique em **Next**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

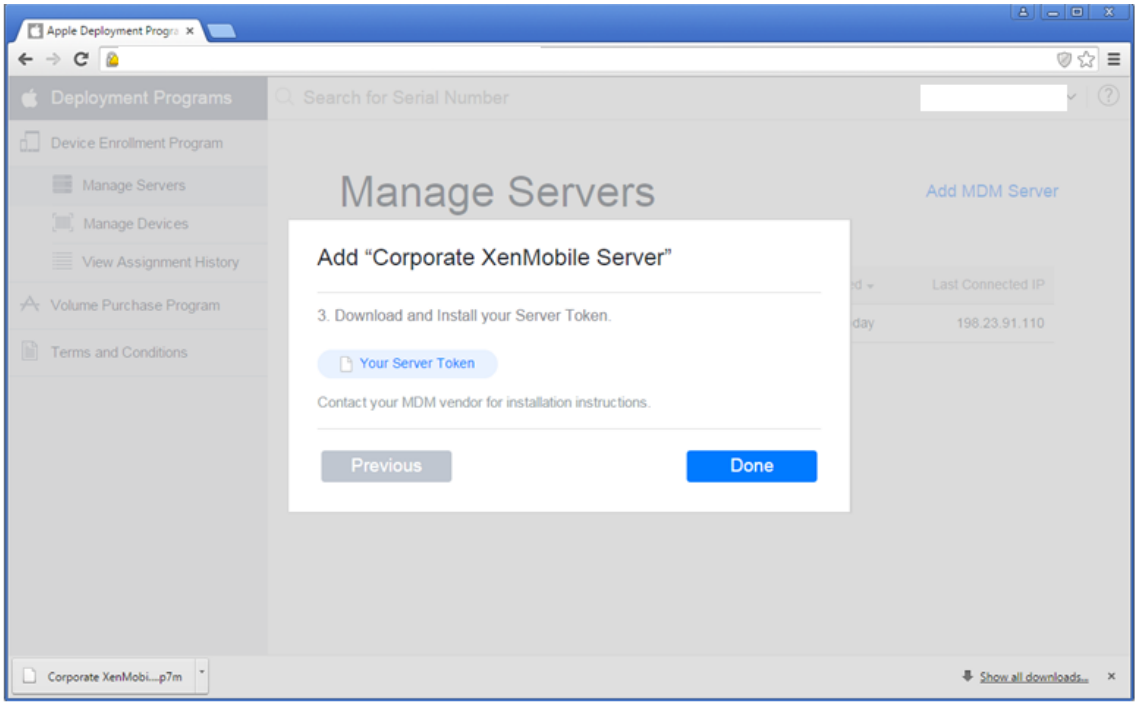


5. No Apple DEP Portal, clique em **Choose file**, selecione a chave pública que você baixou do XenMobile e clique em **Next**.



6. Clique em **Your Server Token** para gerar um token de servidor, que é baixado do navegador, e clique em **Done**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



As informações de token do Apple DEP são exibidas no console do XenMobile depois que você importa o arquivo de token. Você carregará o arquivo de token de servidor ao adicionar a conta do DEP ao XenMobile.

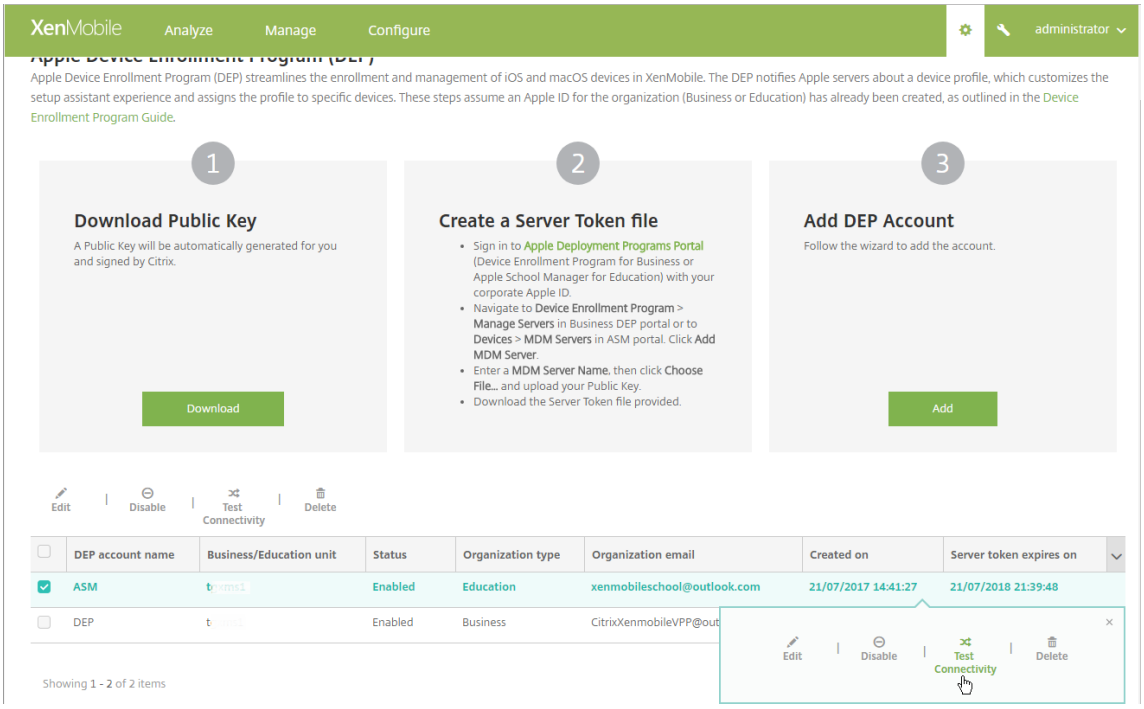
Etapa 3: adicione uma conta do DEP ao XenMobile

Você pode adicionar várias contas do DEP ao XenMobile. Este recurso permite usar diversas configurações de registro e opções de assistente de configuração por país, departamento e assim por diante. Em seguida, você associa contas do DEP a diferentes políticas de dispositivo.

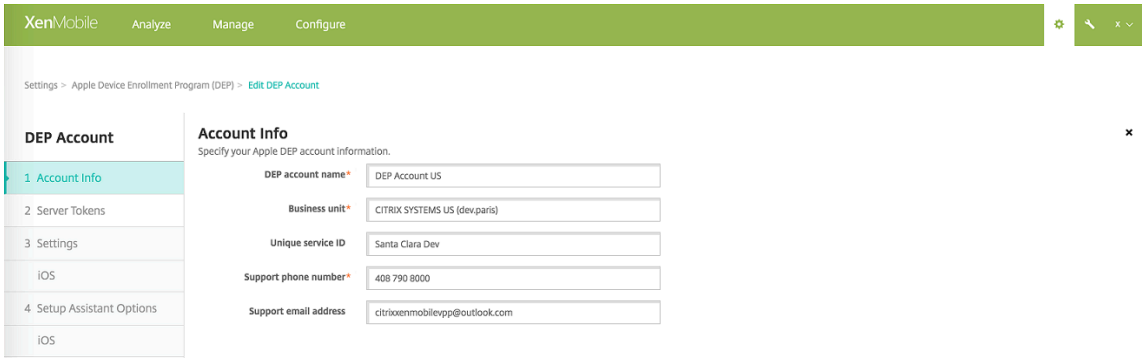
Por exemplo, você pode centralizar a todas as suas contas do DEP de diferentes países no mesmo servidor XenMobile, para importar e supervisionar todos os dispositivos DEP. Personalizando as configurações de registro e as opções do assistente de instalação por departamento, hierarquia organizacional ou outra estrutura, você pode garantir que as políticas ofereçam funcionalidades apropriadas em toda a organização e que os dispositivos dos usuários recebam a assistência de instalação apropriada.

1. No console XenMobile, vá para **Configurações > Apple Device Enrollment Program (DEP)** e, em **Adicionar conta do DEP**, clique em **Adicionar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



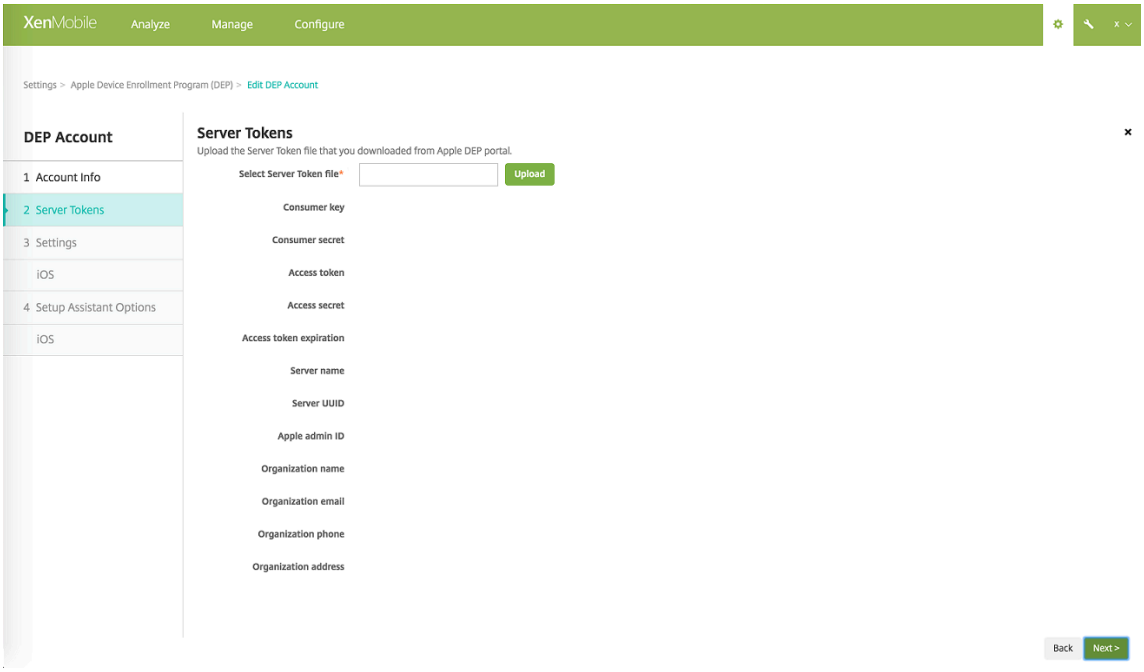
2. Na página **Informações sobre a conta**, especifique estas configurações:



- **Nome de conta do DEP:** um nome exclusivo para essa conta do DEP. Use nomes que reflitam como organizar contas do DEP, como por país ou hierarquia organizacional.
- **Unidade de negócios/educação:** a unidade de negócios ou o departamento ao qual o dispositivo é atribuído. Este campo é obrigatório.
- **ID de serviço exclusiva:** um ID exclusivo opcional para ajudar você 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 pedir ajuda durante a instalação. Este campo é obrigatório.
- **Endereço de email de suporte:** um endereço de email de suporte opcional, disponível para os usuários finais.

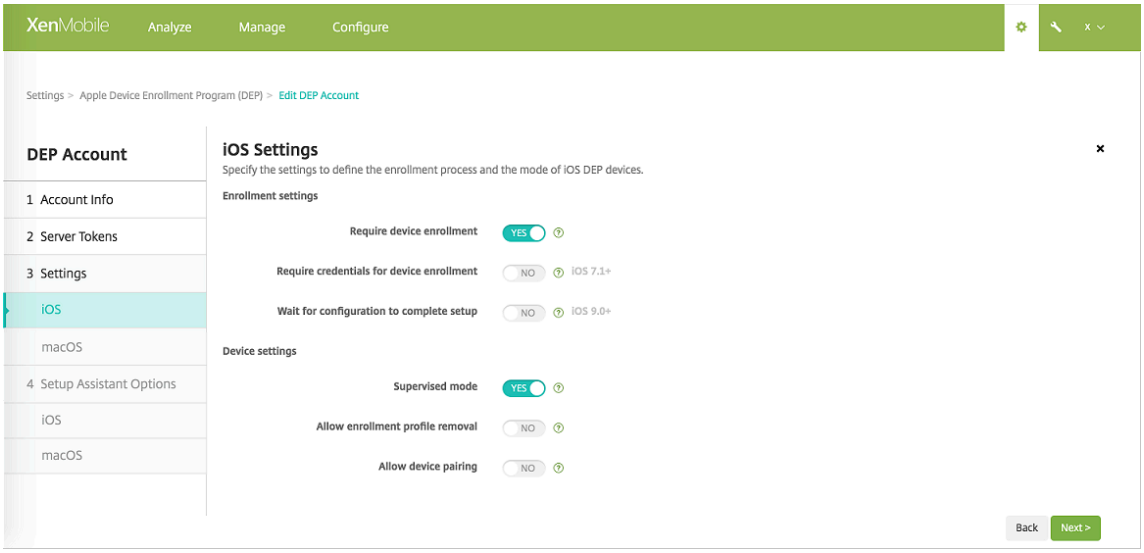
3. Na página **Tokens de servidor**, especifique o arquivo de token de servidor e clique em **Carregar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Suas informações de token de servidor são exibidas.

4. Em **Configurações do iOS**, especifique estas configurações:



Configurações de registro:

- **Exigir registro de dispositivo:** selecione se os usuários devem ser obrigados a registrar seus dispositivos. O padrão é **Sim**.
- **Exigir credenciais para registro de dispositivo:** selecione se os usuários são obrigados a inserir as respectivas credenciais durante a configuração do DEP. Essa configuração está disponível para o iOS 7.1 e versões posteriores. O padrão é **Não**.

  Quando o DEP é ativado pela primeira vez e você não seleciona essa opção, os compo-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

nentes do DEP, como o usuário do DEP, o Secure Hub, o inventário de software e o grupo de implantação do DEP, são criados. Se você selecionar essa opção, o XenMobile não criará os componentes. Como resultado, se mais tarde você desmarcar essa opção, os usuários que não inseriram suas credenciais não podem executar o registro do DEP porque esses componentes do DEP não existem. Para adicionar componentes do DEP, nesse caso, desative e ative a conta do DEP.

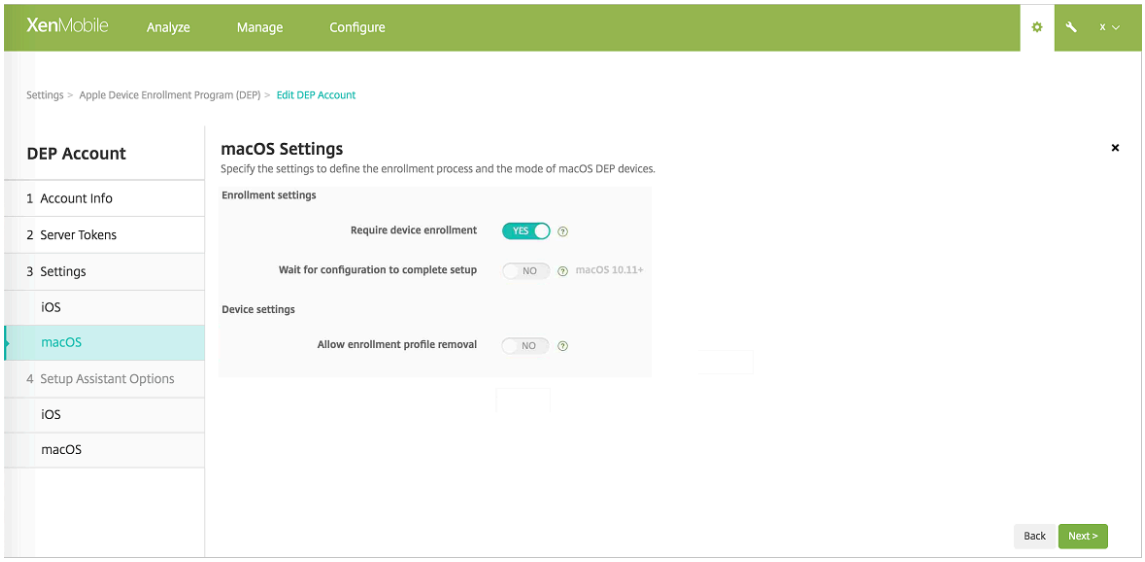
- **Aguardar que a configuração conclua a instalação:** selecione se os dispositivos dos usuários devem ser obrigados a permanecer no modo do Assistente de instalação até que todos os recursos do MDM sejam implantados no dispositivo. Essa configuração está disponível para os dispositivos iOS 9.0 e versões posteriores no modo supervisionado. O padrão é **Não**.
- A documentação da Apple declara que os seguintes comandos poderão não funcionar enquanto o dispositivo estiver no modo Assistente de Instalação:
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Configurações do dispositivo:

- **Modo supervisionado:** deverá ser definido como **Sim** se você estiver usando o Apple Configurator para gerenciar dispositivos registrados para DEP ou quando a opção **Aguardar que a configuração conclua a instalação** estiver ativada. 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:** selecione se os dispositivos devem ter permissão para usar um perfil que você pode remover remotamente. O padrão é **Não**.
- **Permitir emparelhamento de dispositivo:** para dispositivos registrados por meio do DEP, selecione se você pode gerenciá-los usando o iTunes e o Apple Configurator. O padrão é **Não**.

5. Em **Configurações do iOS**, especifique estas configurações:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Configurações de registro:

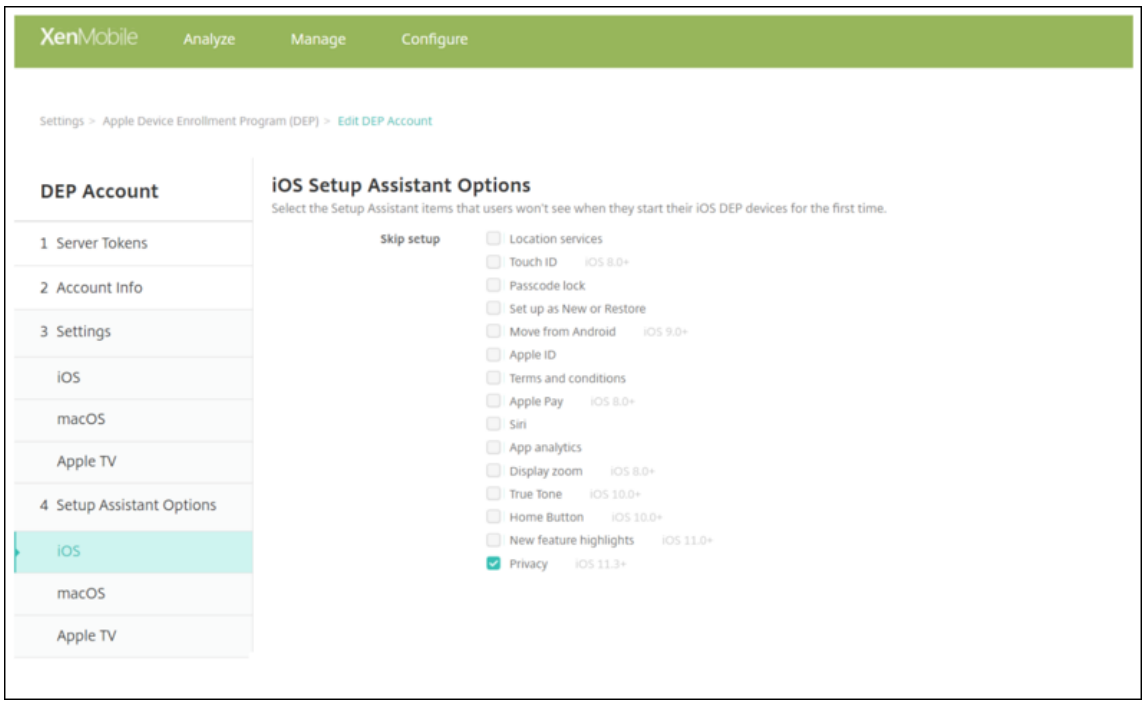
- **Exigir registro de dispositivo:** selecione se os usuários devem ser obrigados a registrar seus dispositivos. O padrão é **Sim**.
- **Aguardar que a configuração conclua a instalação:** se a opção for **Sim**, o dispositivo macOS não continuará o assistente de instalação até que o código secreto de recursos do MDM seja implantado no dispositivo. Essa implantação ocorre antes de a criação da conta local. Essa configuração está disponível para dispositivos macOS 10.11 e versões posteriores. O padrão é **Não**.

Configurações do dispositivo:

- **Permitir remoção do perfil de registro:** selecione se os dispositivos devem ter permissão para usar um perfil que você pode remover remotamente. O padrão é **Não**.

6. Em **Opções do assistente de instalação do iOS**, selecione as etapas do Assistente de instalação do iOS que os usuários irão ignorar quando iniciarem seus dispositivos pela primeira vez. O padrão é desmarcar essa opção para todos os itens.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



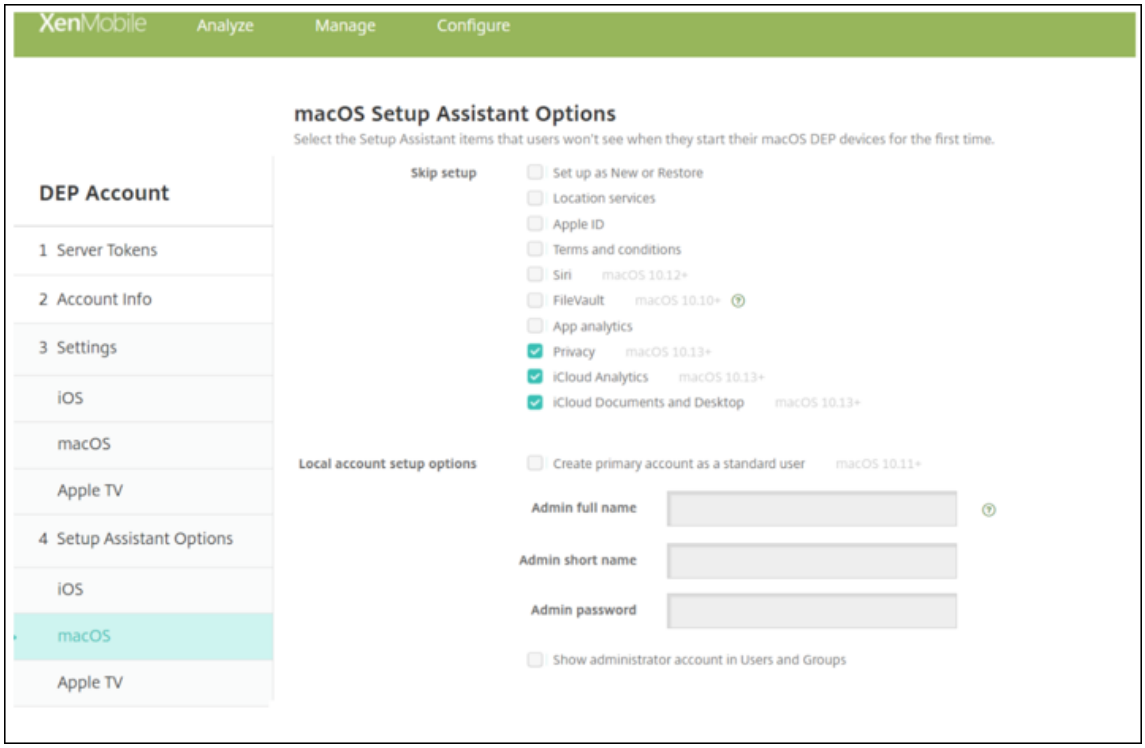
- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **Touch ID:** configurar o Touch ID nos dispositivos iOS 8.0 e versões posteriores.
- **Bloqueio de código secreto:** criar uma senha para o dispositivo.
- **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou iTunes.
- **Mover do Android:** permitir a transferência de dados de um dispositivo Android para um dispositivo iOS 9 ou versões posteriores. Essa opção está disponível somente quando **Configurar como novo ou restaurar** está selecionada (ou seja, a etapa é ignorada).
- **ID Apple:** configurar uma conta do ID Apple para o dispositivo.
- **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo.
- **Apple Pay:** configurar o Apple Pay nos dispositivos iOS 8.0 e versões posteriores.
- **Siri:** usar ou não a Siri no dispositivo.
- **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
- **Zoom de exibição:** configurar a resolução da tela (padrão ou ampliada) nos dispositivos iOS 8.0 ou versões posteriores.
- **True Tone:** configurar o True Tone Display nos dispositivos iOS 10.0 (versão mínima).
- **Botão Home:** configurar a sensibilidade da tela do botão Home em dispositivos iOS 10.0 (versão mínima).
- **Destaques do novo recurso:** configurar as telas informativas de integração, acessar o Dock em qualquer lugar e alternar entre aplicativos recentes em dispositivos iOS 11.0 (versão mínima).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Privacidade:** impedir que os usuários vejam os dados e o painel de privacidade durante a configuração dos dispositivos DEP. Para iOS 11.3 e posterior.
- **Aparência:** impedir que o usuário veja a tela Escolher sua aparência durante a configuração dos dispositivos DEP. Para iOS 12.0 e posterior.
- **SoftwareUpdate:** impedir que o usuário veja a tela de atualização de software obrigatória durante a configuração dos dispositivos DEP. Para iOS 12.0 e posterior.
- **ScreenTime:** impedir que o usuário veja a tela Tempo de Tela durante a configuração dos dispositivos DEP. Para iOS 12.0 e posterior.
- **Configuração do SIM:** impedir que o usuário veja a tela Add Cellular Plan durante a configuração de dispositivos DEP. Para iOS 12.0 e posterior.
- **iMessage & FaceTime:** impedir que o usuário veja a tela do iMessage e do FaceTime durante a configuração dos dispositivos DEP. Para iOS 12.0 e posterior.

A conta do DEP é exibida em **Configurações > Apple Device Enrollment Program (DEP)**.

1. Em **Opções do assistente de instalação do macOS**, selecione as etapas do Assistente de instalação do macOS que os usuários ignoram quando iniciam seus dispositivos pela primeira vez. O padrão é desmarcar essa opção para todos os itens.



- **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou iTunes.
- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **ID Apple:** configurar uma conta do ID Apple para o dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo.
- **Siri:** usar ou não a Siri no dispositivo.
- **FileVault:** usar o FileVault para criptografar o disco de inicialização. O XenMobile aplicará a configuração do FileVault somente se o sistema tiver uma conta de usuário local e essa conta estiver conectada ao iCloud.

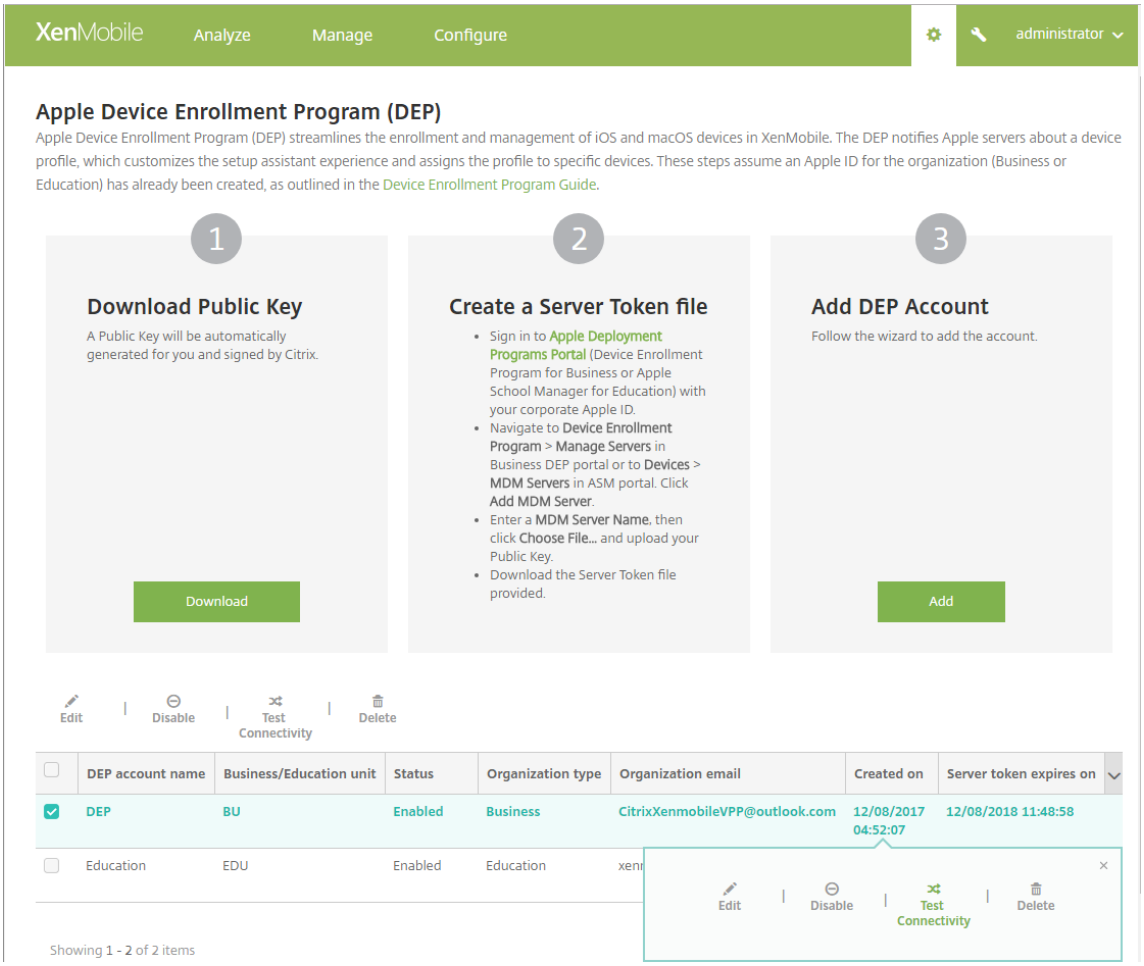
  Você pode usar o recurso de Criptografia de disco do FileVault do macOS para proteger o volume do sistema, criptografando seu conteúdo (https://support.apple.com/en-us/HT204837). Se o Assistente de instalação for executado em um Mac portátil mais atual sem o FileVault ativado, talvez você seja solicitado a ativar esse recurso. O aviso aparecerá em sistemas novos e em sistemas atualizados para o OS X 10.10 ou 10.11, mas somente se esse sistema tiver uma única conta de administrador local e essa conta estiver conectada ao iCloud.
- **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
- **Registro:** exija que os usuários registrem seus dispositivos.

  A configuração de informações de registro estava disponível por meio do OS X 10.9. O processo de registro permitiu enviar informações de registro do sistema para a Apple. Essas informações associaram suas informações de contato ao hardware do Mac. A Apple usou essas informações principalmente para facilitar o suporte do AppleCare. Se você inseriu anteriormente um ID Apple, o Assistente de instalação enviou opcionalmente o registro com base na sua conta do ID Apple. Se você não inseriu um ID Apple, pode inserir manualmente suas informações de contato.

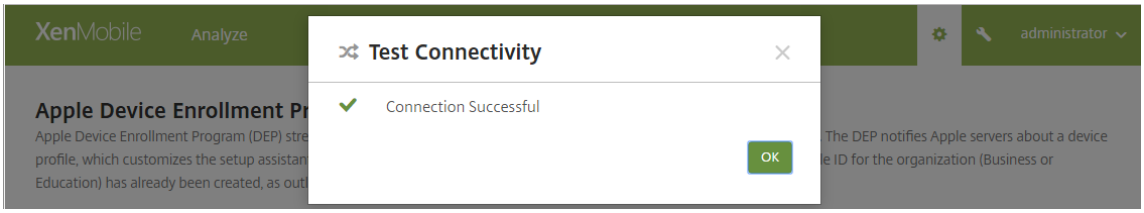
  Em **Opções de configuração de conta local**, especifique as configurações para criar uma conta de administrador, que é necessária para o macOS. O XenMobile cria a conta usando as informações especificadas.
- **Privacidade:** impedir que os usuários vejam os dados e o painel de privacidade durante a configuração dos dispositivos DEP. Para macOS 10.13 e versões posteriores.
- **iCloud Analytics:** impedir que os usuários vejam a tela de análise do iCloud durante a configuração dos dispositivos DEP. Para macOS 10.13 e versões posteriores.
- **Área de trabalho e documentos do iCloud:** impedir que os usuários vejam os documentos do iCloud e a tela da área de trabalho durante a configuração dos dispositivos DEP. Para macOS 10.13 e versões posteriores.
- **Aparência:** impedir que o usuário veja a tela Escolher sua aparência durante a configuração dos dispositivos DEP. Para macOS 10.14 e versões posteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Para testar a conectividade entre o XenMobile e a Apple, selecione a conta e clique em **Testar conectividade**.



É exibida uma mensagem de status.



Configurar regras de implantação de políticas de dispositivo e aplicativos para contas do DEP

Você pode associar contas do DEP a políticas de dispositivo e aplicativos diferentes usando a seção **Regras de implantação** em **Configurar > Políticas de dispositivo** e **Configurar > Aplicativos**. É possível especificar que uma política ou um aplicativo:

- Seja implantado somente para uma determinada conta do Apple DEP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Seja implantado para todas as contas do Apple DEP, exceto uma selecionada.

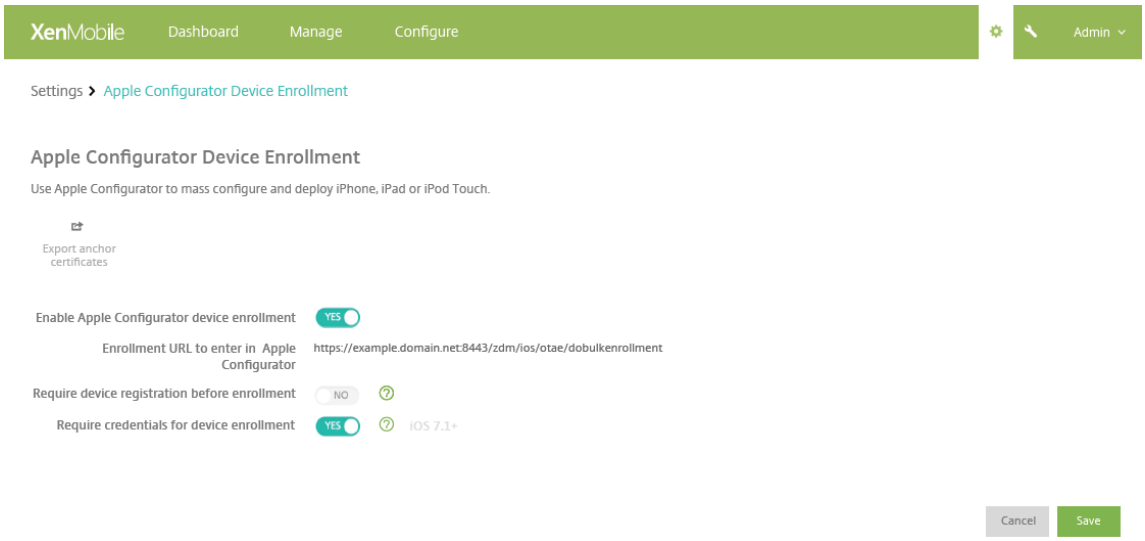
A lista de contas do DEP inclui apenas as contas com o status Ativada ou Desativada. Se a conta do DEP estiver desativada, o dispositivo do DEP não pertencerá a essa conta. Portanto, o XenMobile não implantará o aplicativo ou a política nesse dispositivo.

No exemplo a seguir, uma política de dispositivo é implantada somente para dispositivos com a conta do Apple DEP "DEP Account NR".

```
1 ![Imagem da tela de configurações do Apple DEP](/en-us/xenmobile/server
    /media/apple-dep-deployment-rule-policy-example.png)
```

Definir configurações do Apple Configurator

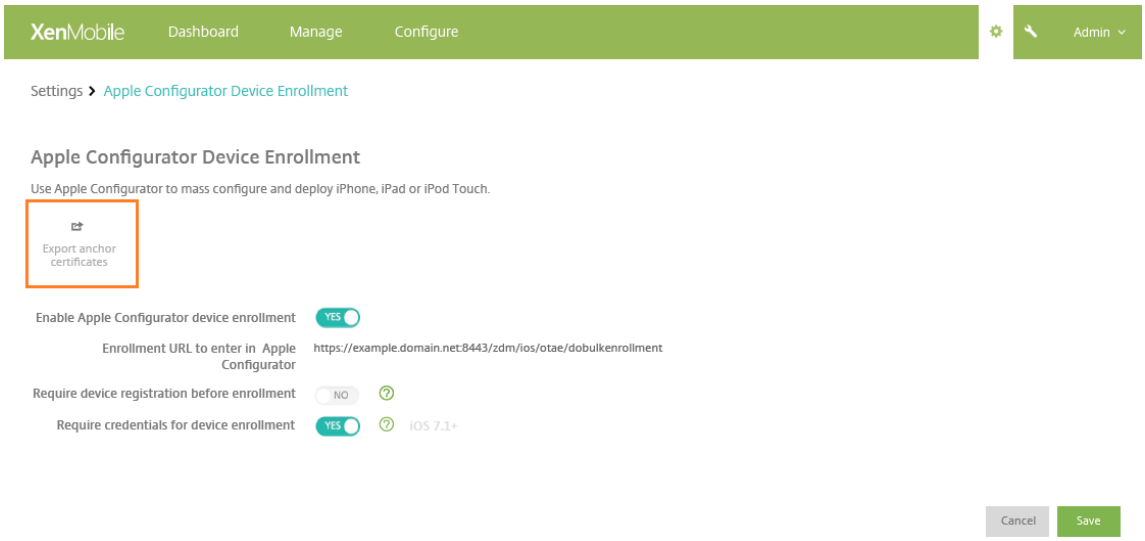
1. No console XenMobile, vá para **Configurações > Registro no Apple Configurator Device Enrollment**.



2. Defina **Ativar registro de dispositivo no Apple Configurator** como **Sim**.
3. O campo **URL de registro para entrar no Apple Configurator** é somente leitura. Essa é a URL para o XenMobile Server que se comunica com a Apple. Nas próximas etapas, você copiará e colará a URL no Apple Configurator. 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 respectivo endereço IP.
4. Para impedir que dispositivos desconhecidos se registrem, defina **Exigir cadastro do dispositivos antes do registro** como **Sim**. Nota: se essa configuração for **Sim**, você deverá adicionar os dispositivos configurados a **Gerenciar > Dispositivos** no XenMobile manualmente ou usando um arquivo CSV antes do registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Para exigir que os usuários de dispositivos iOS 7.1 e versões posteriores insiram suas credenciais ao se registrarem, defina **Exigir credenciais para registro de dispositivo** como **Sim**. O padrão é não exigir credenciais para o registro.
6. Nota: se o XenMobile Server estiver usando um certificado SSL confiável, ignore essa etapa. Clique em **Exportar certificados de âncora** e salve o arquivo certchain.pem nas chaves do macOS (login ou System).



7. Inicie o Apple Configurator e acesse **Prepare > Setup > Configure Settings**.
8. Na configuração **Device Enrollment**, cole a URL do servidor MDM da etapa 4 na caixa **MDM server URL** no Configurator.
9. Na configuração **Device Enrollment**, copie a Autoridade de certificação raiz e a Autoridade de certificação de servidores SSL para os certificados **Anchor** se o XenMobile não estiver usando um certificado SSL confiável.
10. Use um Cabo Dock Connector para USB para conectar os dispositivos ao Mac que executa o Apple Configurator e configurar simultaneamente até 30 dispositivos conectados. Se você não tiver um Dock Connector, use um ou mais hubs de alta velocidade USB 2.0 alimentados para conectar os dispositivos.
11. Clique em **Prepare**. Para obter mais informações sobre como preparar os dispositivos com o Apple Configurator, consulte a página de ajuda do Apple Configurator, Prepare devices.
12. No Apple Configurator, configure as políticas de dispositivo de que necessita.
13. À medida que cada dispositivo for preparado, ligue-o para iniciar o Assistente de Instalação do iOS, que prepara o dispositivo para ser usado pela primeira vez.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para renovar ou atualizar certificados durante o uso do Apple DEP

Quando o certificado Secure Sockets Layer (SSL) do XenMobile é renovado, você carrega um novo certificado no console XenMobile em **Configurações > Certificados**. Na caixa de diálogo **Importar**, em **Usar como**, clique em **Ouvinte SSL** para que o certificado seja usado para SSL. Depois que você reiniciar o servidor, o XenMobile usará o novo certificado SSL. Para obter mais informações sobre certificados no XenMobile, consulte Carregando certificados para o XenMobile.

Não é necessário restabelecer a relação de confiança entre o Apple DEP e o XenMobile quando você renova ou atualiza o certificado SSL. Você pode, no entanto, redefinir as configurações do DEP a qualquer momento seguindo as etapas anteriores neste artigo.

Para obter mais informações sobre o Apple DEP, consulte a Documentação da Apple.

Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator

> Importante:
>
> Colocar um dispositivo no modo supervisionado instalará a versão selecionada do iOS no dispositivo, apagando completamente os dados ou os aplicativos do usuário armazenados anteriormente.

1. Instale o Apple Configurator pelo iTunes.
2. Conecte o dispositivo iOS ao seu computador Apple.
3. Inicie o Apple Configurator. O Configurator mostra que você tem um dispositivo a ser preparado para supervisão.
4. Para preparar o dispositivo para supervisão:
   - Configure **Supervision control** como **On**. A Citrix recomenda que você escolha essa configuração se pretende manter o controle do dispositivo reaplicando uma configuração regularmente.
   - Opcionalmente, forneça um nome para o dispositivo.
   - No iOS, clique em **Latest** para obter a versão mais recente do iOS que você deseja instalar.
5. Quando você estiver pronto para preparar o dispositivo para supervisão, clique em **Prepare**.

Propriedades do cliente

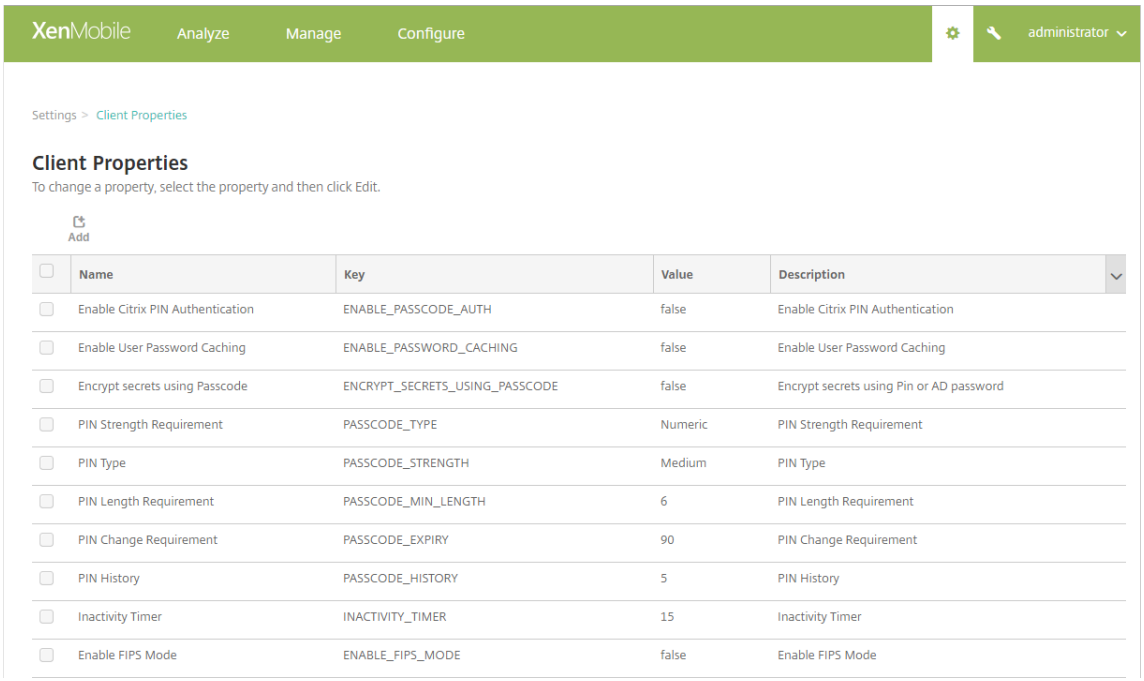
April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

As propriedades do cliente contêm informações que são fornecidas diretamente para o Secure Hub em dispositivos de usuários. Você pode usar essas propriedades para definir configurações avançadas, como PIN da Citrix. Obtenha as propriedades do cliente junto ao suporte da Citrix.

As propriedades do cliente estão sujeitas a alterações a cada versão do Secure Hub e, ocasionalmente, em aplicativos clientes. Para obter detalhes sobre as propriedades do cliente mais comumente configuradas, consulte Referência da propriedade de cliente, posteriormente neste artigo.

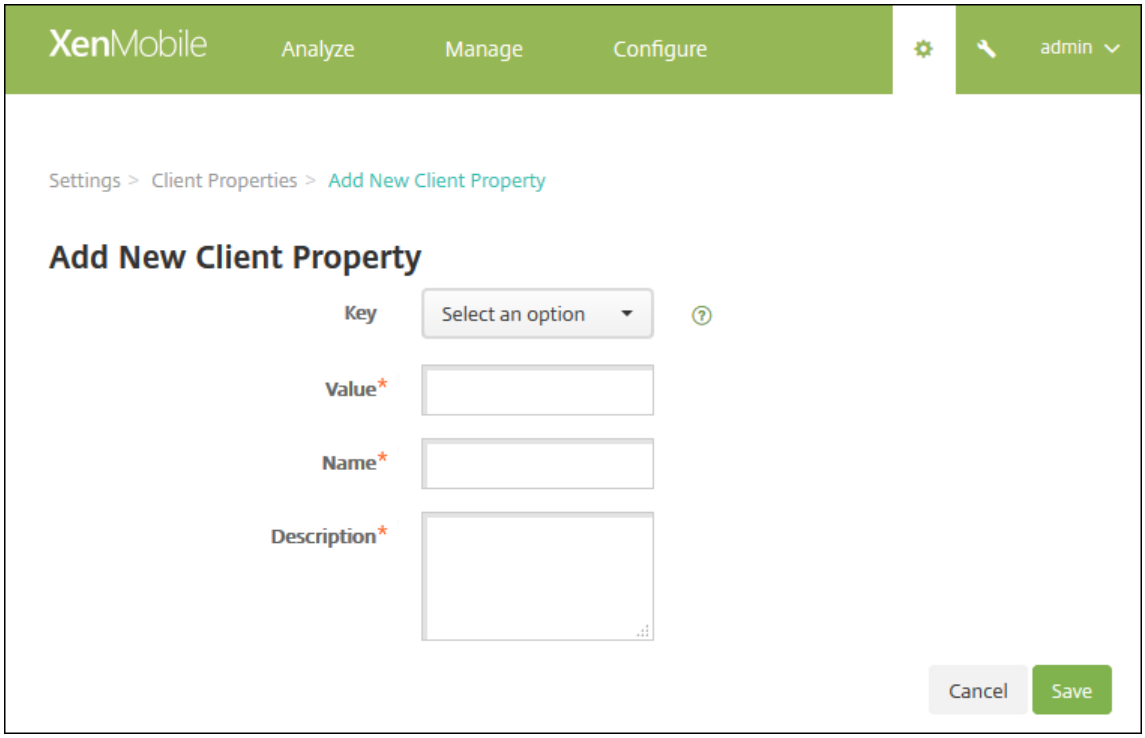
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Cliente**, clique em **Propriedades do cliente**. A página **Propriedades do cliente** é exibida. Você pode adicionar, editar e excluir propriedades do cliente nessa página.



Para adicionar uma propriedade do cliente

1. Clique em **Adicionar**. A página **Adicionar nova propriedade de cliente** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:
   - **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 do cliente

1. Na tabela **Propriedades do cliente**, selecione a propriedade do cliente que você deseja editar.

   Quando você marca a caixa de seleção ao lado de uma propriedade de cliente, o menu de opções é exibido acima da lista de propriedades do cliente. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.
2. Clique em **Edit**. A página **Editar propriedade do cliente** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Altere as seguintes informações conforme apropriado:
   - **Chave:** você não pode alterar esse 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 do 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 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.

Referência da propriedade de cliente

As propriedades de cliente predefinidas do XenMobile e suas configurações padrão estão descritas abaixo.

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Nome de exibição: Período de autodestruição do contêiner de MDX
  - A autodestruição impede o acesso ao Secure Hub e aos aplicativos gerenciados, após um determinado número de dias de inatividade. Depois do limite de tempo, os aplicativos deixam de ser utilizáveis. Apagar os dados inclui limpar os dados de cada aplicativo instalado, incluindo o cache do aplicativo e os dados do usuário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O tempo de inatividade é quando o servidor não recebe uma solicitação de autenticação para validar o usuário em um determinado período de tempo. Por exemplo, se essa política for de 30 dias e o usuário não usar os aplicativos por mais de 30 dias, a política entrará em vigor.

Essa política de segurança global é aplicável às plataformas iOS e Android e é um aprimoramento das políticas existentes de bloqueio e apagamento de aplicativos.

- Para configurar essa política global, vá até **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 técnico de TI
  - Essa propriedade ativa ou desativa a capacidade de enviar os logs para o suporte técnico de TI.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **DISABLE_LOGGING**
  - Nome de exibição: Desativar log
  - Use esta propriedade para impedir que os usuários coletem e enviem logs de seus dispositivos. Esta propriedade desativa o registro em log no Secure Hub e para todos os aplicativos MDX instalados. Os usuários não podem enviar logs para nenhum aplicativo na página de Suporte. Embora a caixa de diálogo de composição de email seja exibida, os logs não são anexados. Uma mensagem indica que o registro em log está desativado. Esta configuração também evita que você atualize as configurações de log no console XenMobile para aplicativos do Secure Hub e MDX.

    Quando esta propriedade está definida como **true**, o Secure Hub define **Bloquear logs de aplicativo** como **true**. Como resultado, os aplicativos MDX param o registro em log quando a nova política é aplicada.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false** (a geração de log não é desativada)
- **ENABLE_CRASH_REPORTING**
  - Nome de exibição: Ativar relatórios de falhas
  - Se for **true**, a Citrix coletará relatórios e diagnósticos de falhas para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se for **false**, não haverá coleta de dados.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **true**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **ENABLE_CREDENTIAL_STORE**
  - Nome de exibição: ativar armazenamento de credenciais
  - Com a ativação do armazenamento de credenciais, os usuários de Android ou iOS informam a senha uma única vez ao acessarem os aplicativos móveis de produtividade. Você pode usar o armazenamento de credenciais independentemente da ativação ou não do PIN da Citrix. Se você não ativar o PIN da Citrix, os usuários devem digitar a senha do Active Directory. O XenMobile dá suporte ao uso de senhas do Active Directory com o armazenamento de credenciais somente para o Secure Hub e os aplicativos de loja pública. Se você usa senhas do Active Directory com o armazenamento de credenciais, o XenMobile não dá suporte à autenticação de PKI.
  - O registro automático no Secure Mail requer que você defina esta propriedade como **true**.
  - Para configurar essa 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: ativar o modo FIPS
  - Essa propriedade ativa ou desativa 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 não a autenticação online Avançar.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **ENABLE_NETWORK_EXTENSION**
  - Nome de exibição: ENABLE_NETWORK_EXTENSION
  - Por padrão, o XenMobile permite que o framework de extensão de rede Apple quando a instalação do Secure Hub. Para desativar a extensão de rede, vá até **Configurações > Propriedades do cliente**, adicione a chave personalizada **ENABLE_NETWORK_EXTENSION** e defina o **Valor** como **false**.
  - Valor padrão: **true**
- **ENABLE_PASSCODE_AUTH**
  - Nome de exibição: Ativar Autenticação do PIN da Citrix
  - Essa propriedade permite que você ative a funcionalidade do PIN da Citrix. Com o PIN ou código secreto da Citrix, os usuários são solicitados a definir um PIN a ser usado em vez da senha do Active Directory. Essa configuração é ativada automaticamente quando a ENABLE_PASSWORD_CACHING está ativada, ou quando o XenMobile está usando a autenticação de certificado.

    Para a autenticação offline, o PIN da Citrix será validado localmente e os usuários terão permissão para acessar o aplicativo ou o conteúdo que eles solicitaram. Para a autenti-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cação online, o PIN ou código secreto da Citrix desbloqueará a senha ou o certificado do Active Directory, que é enviado para realizar a autenticação no 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: Ativar Armazenamento em Cache de Senha do Usuário
  - Esta propriedade permite as senhas do Active Directory sejam armazenadas em cache localmente no dispositivo móvel. Quando você define essa propriedade como **true**, também deve definir a propriedade **ENABLE_PASSCODE_AUTH** como **true**. Com o cache de senha de usuário ativado, o XenMobile avisa aos usuários para configurar um PIN ou código secreto da Citrix.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - Nome de exibição: Ativar Autenticação de Touch ID
  - Em dispositivos que dão suporte à autenticação Touch ID, essa propriedade ativa ou desativa a autenticação Touch ID no dispositivo. Requisitos:

    Os dispositivos de usuário devem ter o PIN ou LDAP da Citrix ativado. Se a autenticação LDAP estiver desativada (por exemplo, porque somente a autenticação baseada em certificados é usada), os usuários deverão definir um PIN da Citrix. Nesse caso, o XenMobile exige o PIN da Citrix mesmo que a propriedade do cliente **ENABLE_PASSCODE_AUTH** seja **false**.

    Defina **ENABLE_PASSCODE_AUTH** como **false** para que, quando os usuários iniciarem um aplicativo, eles devam responder a uma solicitação para usar o Touch ID.

  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **ENABLE_WORXHOME_CEIP**
  - Nome de exibição: Ativar CEIP do Worx Home
  - Essa propriedade ativa o Programa de Melhoria de Experiência do Cliente. Esse recurso envia dados de configuração e de uso anônimos para a Citrix periodicamente. Os dados ajudam a Citrix a melhorar a qualidade, a confiabilidade e o desempenho do XenMobile.
  - Valor: **true** ou **false**
  - Valor padrão: **false**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **ENABLE_WORXHOME_GA**
  - Nome de exibição: Ativar o Google Analytics no Worx Home
  - Essa propriedade ativa ou desativa a capacidade de coletar dados usando o Google Analytics no Secure Hub. Quando você alterar essa configuração, o novo valor será definido somente quando o usuário fizer login novamente no Secure Hub (chamado anteriormente Worx Home).
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **true**
- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Nome de exibição: Criptografar segredos usando o Código Secreto
  - Essa propriedade armazena dados confidenciais no dispositivo em um cofre secreto em vez de em um armazenamento nativo baseada na plataforma, como as chaves do iOS. Esta propriedade permite uma forte criptografia de artefatos-chave e adiciona entropia de usuário. A entropia de usuário é um código PIN aleatório gerado pelo usuário que apenas o usuário conhece.

    A Citrix recomenda que você ative essa propriedade para ajudar a proporcionar maior segurança nos dispositivos de usuário. Como resultado, os usuários recebem mais pedidos de autenticação para o PIN da Citrix.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **false**
- **INACTIVITY_TIMER**
  - Nome de exibição: Timer de Inatividade
  - Essa propriedade define por quanto tempo os usuários podem deixar seus dispositivos inativos e acessar um aplicativo sem que lhes seja solicitado um PIN ou código secreto da Citrix. Para ativar essa configuração em um aplicativo MDX, defina a política Código Secreto do Aplicativo como Ativado. Se a configuração de código secreto de aplicativo estiver definido como Desativado, os usuários serão redirecionados para o Secure Hub para uma autenticação completa. Quando você altera essa configuração, o valor entra em vigor na próxima vez em que houver solicitação para que os usuários se autentiquem.

    No iOS, o Timer de Inatividade também rege 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**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Nome de exibição: Em caso de falha use email para enviar logs do dispositivo para o suporte técnico de TI
  - Essa chave ativa ou desativa a capacidade de usar emails para enviar os logs do dispositivo para a TI.
  - Valores possíveis: **true** ou **false**
  - Valor padrão: **true**

- **PASSCODE_EXPIRY**
  - Nome de exibição: Requisito de troca do PIN
  - Essa propriedade define por quanto tempo o PIN ou código secreto da Citrix é válido, após o qual o usuário é forçado a alterar seu PIN ou código secreto da Citrix. Quando você alterar essa configuração, o novo valor será definido somente quando o PIN ou código secreto da Citrix atual expirar.
  - Valores possíveis: **1** até **99** recomendados. Para eliminar redefinições de PINs, defina o valor como um número muito alto (por exemplo, 100.000.000.000). Se você definiu originalmente o período de expiração entre 1 e 99 dias e depois mudou para o número grande durante esse período, os PINs ainda expirarão no final do período inicial, mas nunca mais expirarão novamente.
  - Valor padrão: **90** (dias)

- **PASSCODE_HISTORY**
  - Nome de exibição: Histórico de PIN
  - Essa propriedade define o número de PINs ou códigos secretos da Citrix usados anteriormente que os usuários não podem reutilizar quando mudam o PIN ou código secreto da Citrix. Quando você alterar essa configuração, o novo valor será definido somente na próxima vez em que os usuários reiniciarem o PIN ou código secreto da Citrix.
  - Valores possíveis: **1** até **99**
  - Valor padrão: **5**

- **PASSCODE_MAX_ATTEMPTS**
  - Nome de exibição: Tentativas de PIN
  - Essa propriedade define quantas tentativas erradas de PIN ou código secreto da Citrix os usuários podem fazer antes que a autenticação completa seja solicitada. Depois que os usuários executam com êxito uma autenticação completa, eles são solicitados a criar um PIN ou código secreto da Citrix.
  - Valores possíveis: qualquer número inteiro positivo
  - Valor padrão: **15**

- **PASSCODE_MIN_LENGTH**
  - Nome de exibição: Requisito de comprimento do PIN
  - Essa propriedade define o comprimento mínimo de PINs da Citrix.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Valores possíveis: **1** até **99**
- Valor padrão: **6**

- **PASSCODE_STRENGTH**
  - Nome de exibição: Requisito de Força do PIN
  - Essa propriedade define a força do PIN ou código secreto da Citrix. Quando você alterar essa configuração, os usuários serão solicitados a criar um PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.
  - Valores possíveis: **Baixa**, **Média** ou **Forte**
  - Valor padrão: **Média**
  - As regras de senha para cada configuração de força baseada na configuração PASSCODE_TYPE são as seguintes:

Regras para códigos secretos numéricos:

Força do código secreto	Regras para o tipo de senha numérica	Permitido	Não permitido
Baixo	Todos os números, qualquer sequência permitida	444444, 123456, 654321	
Média (configuração padrão)	Os números não podem ser todos consecutivos nem os mesmos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Alta	O mesmo que a força de código secreto Média.		
Forte	O mesmo que a força de código secreto Média.		

Regras para códigos secretos alfanuméricos:

Força do código secreto	Regras para tipos de códigos secretos alfanuméricos	Permitido	Não permitido
Baixo	Deve conter pelo menos um número e uma letra	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Força do código secreto	Regras para tipos de códigos secretos alfanuméricos	Permitido	Não permitido
Média (configuração padrão)	Além das regras para a força de código secreto baixa, as letras e todos os números não podem ser os mesmos. As letras 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
Alta	Incluir pelo menos uma letra maiúscula e uma letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Forte	Incluir 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
  - Essa propriedade define se os usuários são capazes de definir um PIN numérico ou um código secreto alfanumérico da Citrix. Quando você seleciona **Numérico**, os usuários podem usar apenas números (PIN da Citrix). Quando você seleciona **Alfanumérico**, os usuários podem usar uma combinação de letras e números para o código secreto.

    Se você alterar essa configuração, os usuários deverão definir um novo PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.
  - Valores possíveis: **Numérico** ou **Alfanumérico**
  - Valor padrão: **Numérico**
- **REFRESHINTERVAL**
  - Nome de exibição: REFRESHINTERVAL
  - Por padrão, o XenMobile ping Auto Discovery servidor (ADS) para os certificados fixados cada 3 dias. Para alterar o intervalo de atualização, vá para **Configurações > Propriedades**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

do cliente, adicione a chave personalizada **REFRESHINTERVAL** e defina o **Valor** como o número de horas.
- Valor padrão: **72** horas (3 dias)

- **SEND_LDAP_ATTRIBUTES**
  - Para implantações de somente MAM de dispositivos Android, iOS ou macOS: você pode configurar o XenMobile para que os usuários que se registrarem no Secure Hub com credenciais de email sejam automaticamente registrados no Secure Mail. Como resultado, os usuários não fornecem informações adicionais ou tomam medidas extras para se registrar no Secure Mail.
  - Para configurar essa política global de cliente, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **SEND_LDAP_ATTRIBUTES** e defina o **Valor** da seguinte maneira.
  - Valor: `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
  - Os valores de atributo estão especificados como macros, semelhante a políticas MDM.
  - Aqui está um exemplo de resposta de serviço de conta de exemplo para esta propriedade:

    ```
    <property value="userPrincipalName=eng1@xmslab.com,sAMAccountName=eng1,displayName=eng1\,test1,email=eng1@xmslab.com\,eng1@xmslab.com"name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - Para esta propriedade, XenMobile trata caracteres de vírgula como terminadores de sequências de caracteres. Portanto, se um valor de atributo incluir uma vírgula, preceda-a com uma barra invertida. A barra invertida impede que o cliente interprete a vírgula inserida como o fim do valor do atributo. Represente caracteres de barra invertida com "\\".

- **HIDE_THREE_FINGER_TAP_MENU**
  - Quando essa propriedade não estiver configurada ou estiver definida como **false**, os usuários podem acessar o menu de recursos ocultos executando um toque de três dedos em seus dispositivos. O menu de recursos ocultos permitia aos usuários redefinir os dados do aplicativo. Definir esta propriedade como **true** desabilita o acesso dos usuários ao menu de recursos ocultos.
  - Para configurar essa política global de cliente, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **HIDE_THREE_FINGER_TAP_MENU** e defina o **Valor**.

- **TUNNEL_EXCLUDE_DOMAINS**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Nome de exibição: Tunnel Exclude Domains
- Por padrão, o MDX exclui do encapsulamento de micro VPN alguns pontos de extremidade de serviço que XenMobile SDKs e aplicativos usam para vários recursos. Por exemplo, os pontos de extremidade incluem serviços que não exigem roteamento por meio de redes corporativas, como o Google Analytics, serviços do Citrix Cloud e serviços do Active Directory. Use essa propriedade de cliente para substituir a lista padrão de domínios excluídos.
- Para configurar essa política global de cliente, 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 deseja excluir do encapsulamento, digite uma lista de sufixos de domínio separados por vírgulas. Para incluir todos os domínios em encapsulamento, 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,fabric.io,firehose.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
  ```

Implantar dispositivos macOS por meio do Apple DEP

April 15, 2019

A Apple possui programas de registro de dispositivos para contas de negócios e educação. Para contas de negócios, você se inscreve no Apple Deployment Program para usar o Apple Device Enrollment Program (DEP) para cadastro e gerenciamento de dispositivos no XenMobile. Esse programa é para dispositivos iOS e macOS. Para obter informações sobre como se cadastrar para obter uma conta de negócios do Apple Deployment Program, consulte este PDF da Apple.

Lembre-se de que o Apple Deployment Program está disponível para organizações e não para pessoas físicas. Você deve fornecer uma quantidade considerável de detalhes e informações corporativos para criar uma conta do Apple Deployment Program. Portanto, o processo de solicitação e recebimento de aprovação para contas pode ser demorado.

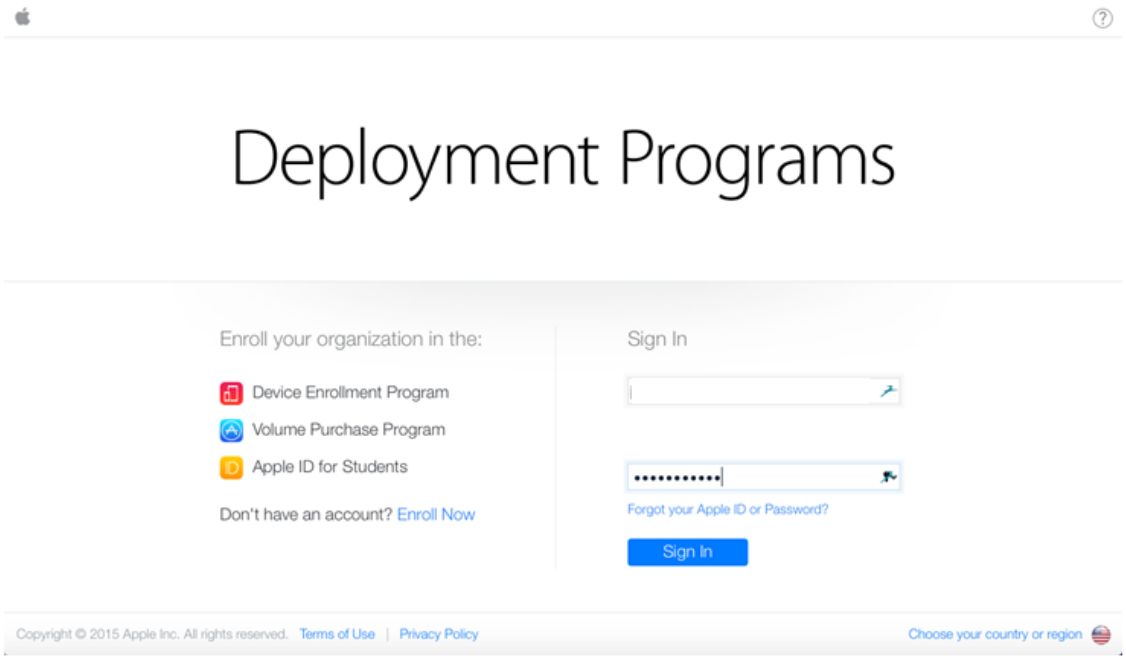
Para contas de educação, você cria uma conta do Apple School Manager. O Apple School Manager unifica o Programa de Registro de Dispositivo (DEP) e o Volume Purchase Program (VPP). O Apple School Manager é um tipo de DEP de Educação. Para criar uma conta do Apple School Manager, acesse https://school.apple.com/.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cadastrar-se no Apple Deployment Program

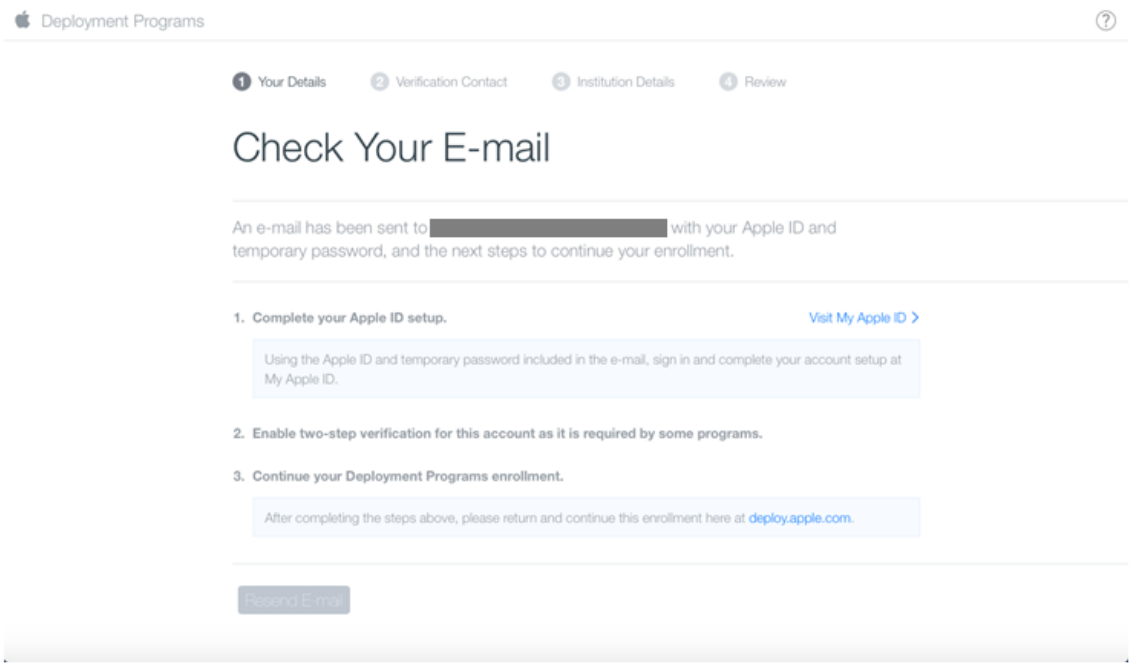
1. Vá para deploy.apple.com para solicitar uma conta do Apple Deployment Program. Quando você solicita uma conta do DEP, a prática recomendada é usar um endereço de email relacionado à organização, como dep@empresa.com.

   > Nota:
   >
   > Para contas de educação, acesse https://school.apple.com/.

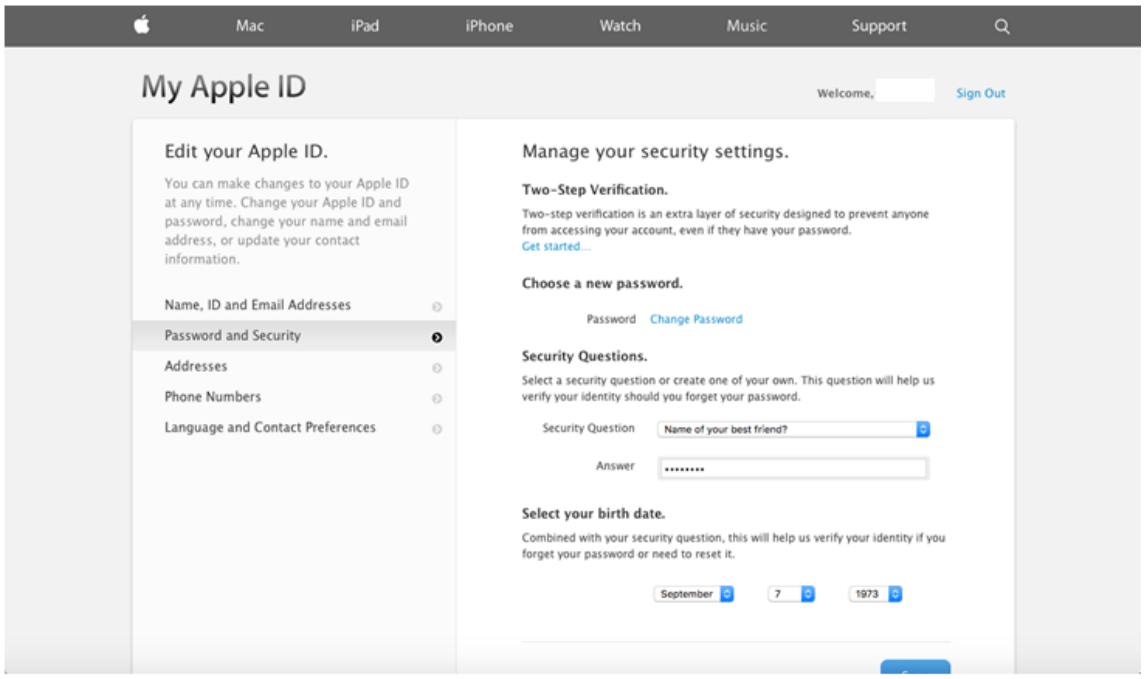


2. Depois que você inserir as informações da sua organização, a Apple enviará uma senha temporária para o novo ID Apple por email.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

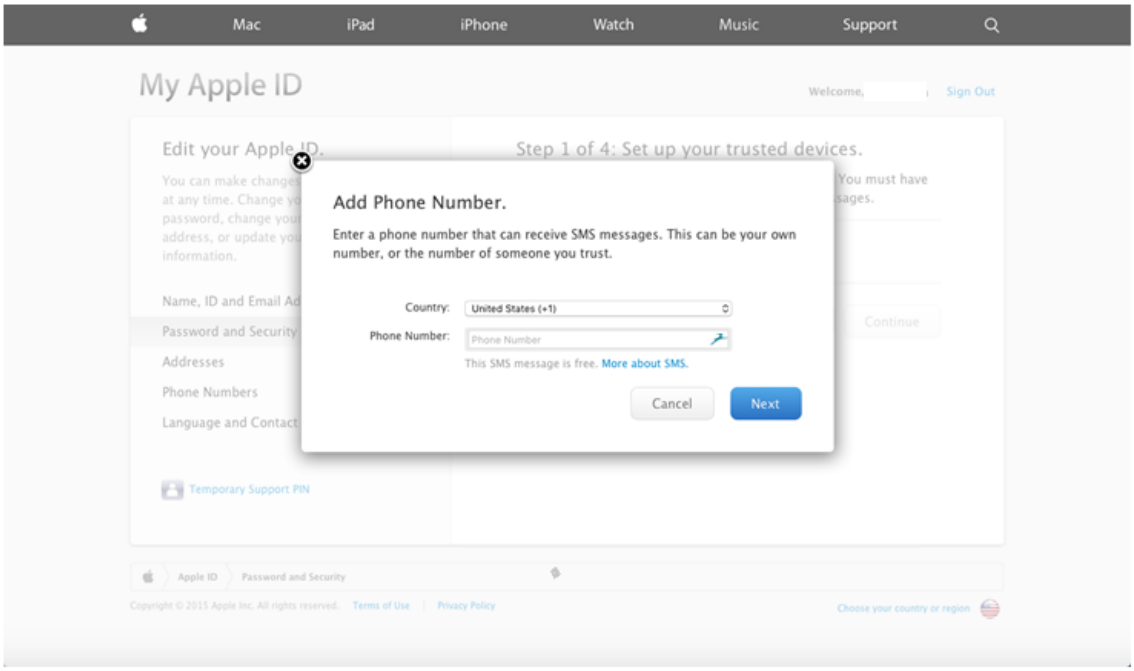


3. Em seguida, faça login com o ID Apple e conclua as configurações de segurança da conta.

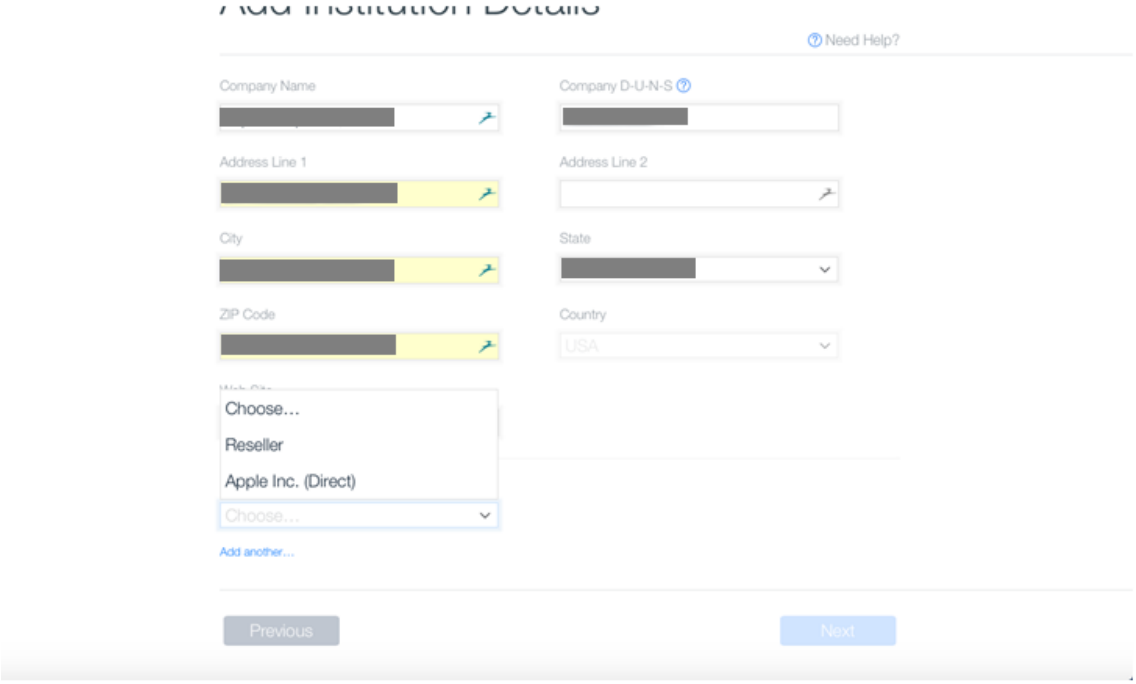


4. Configure e ative a verificação em duas etapas, que é necessária para uso com o DEP Portal. Durante essas etapas, depois de adicionar um número de telefone, você receberá o PIN de quatro dígitos para a verificação em duas etapas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

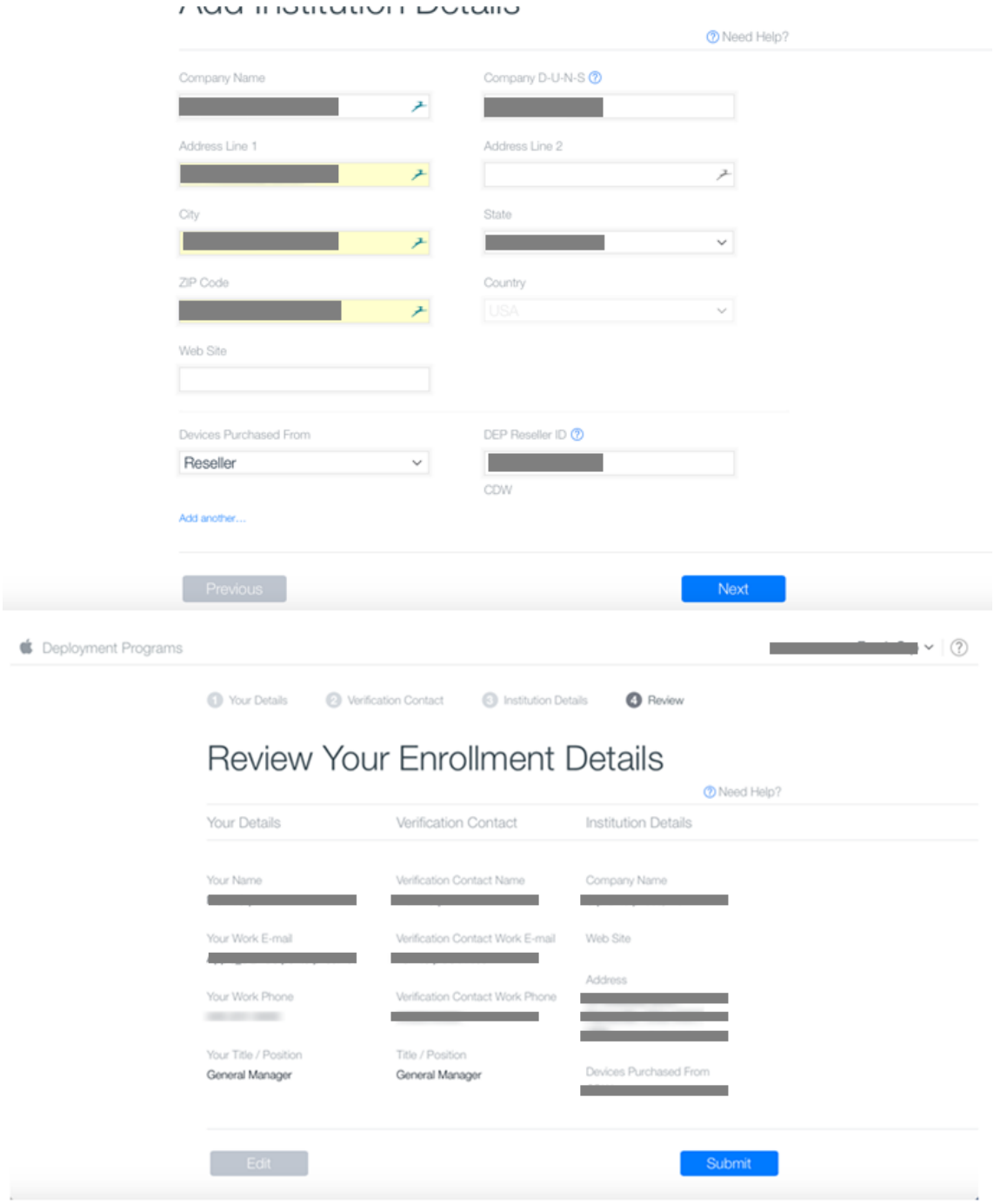


5. Faça login no DEP Portal para concluir a configuração da conta usando a verificação em duas etapas que você configurou.
6. Adicione os dados da empresa e selecione de onde você compra dispositivos. Para obter detalhes sobre as opções de compra, consulte a próxima seção, Solicitar dispositivos ativados para o DEP.



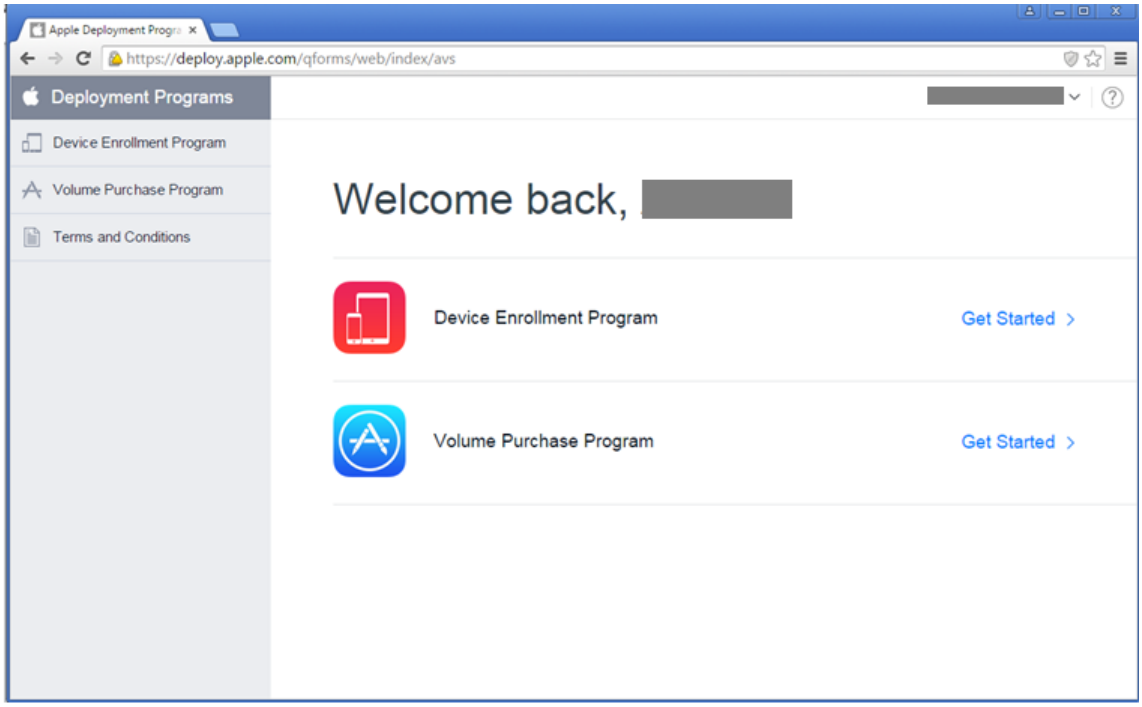
7. Adicione o número de cliente da Apple ou o ID de revendedor do DEP. Em seguida, verifique os detalhes de registro e aguarde que a Apple aprove sua conta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



8. Depois de receber suas credenciais de login da Apple, faça logon no Apple DEP Portal.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para conectar sua conta ao XenMobile, consulte “Integrar a conta do Apple DEP ao XenMobile” em Registrar dispositivos iOS e macOS em massa.

Solicitar dispositivos ativados para o DEP

Você pode encomendar dispositivos ativados para DEP diretamente da Apple ou de revendedores ou operadoras autorizadas ativadas para DEP. Para encomendar da Apple, forneça o ID de cliente Apple no Apple DEP Portal. Seu ID de cliente permite que a Apple associe à sua conta do Apple DEP os dispositivos que você adquiriu.

Para encomendar junto ao seu revendedor ou operadora, entre em contato com o revendedor da Apple ou a operadora para verificar se eles participam do Apple DEP. Peça o ID do Apple DEP do revendedor ao adquirir dispositivos. A Apple exige essas informações quando você adiciona seu revendedor do Apple DEP à conta do Apple DEP. Depois de adicionar o ID do Apple DEP do revendedor, você receberá um ID de cliente do DEP. Forneça o ID de cliente do DEP ao revendedor, que o usará para enviar informações sobre suas compras de dispositivo para a Apple. Para obter mais informações, consulte este Site da Apple.

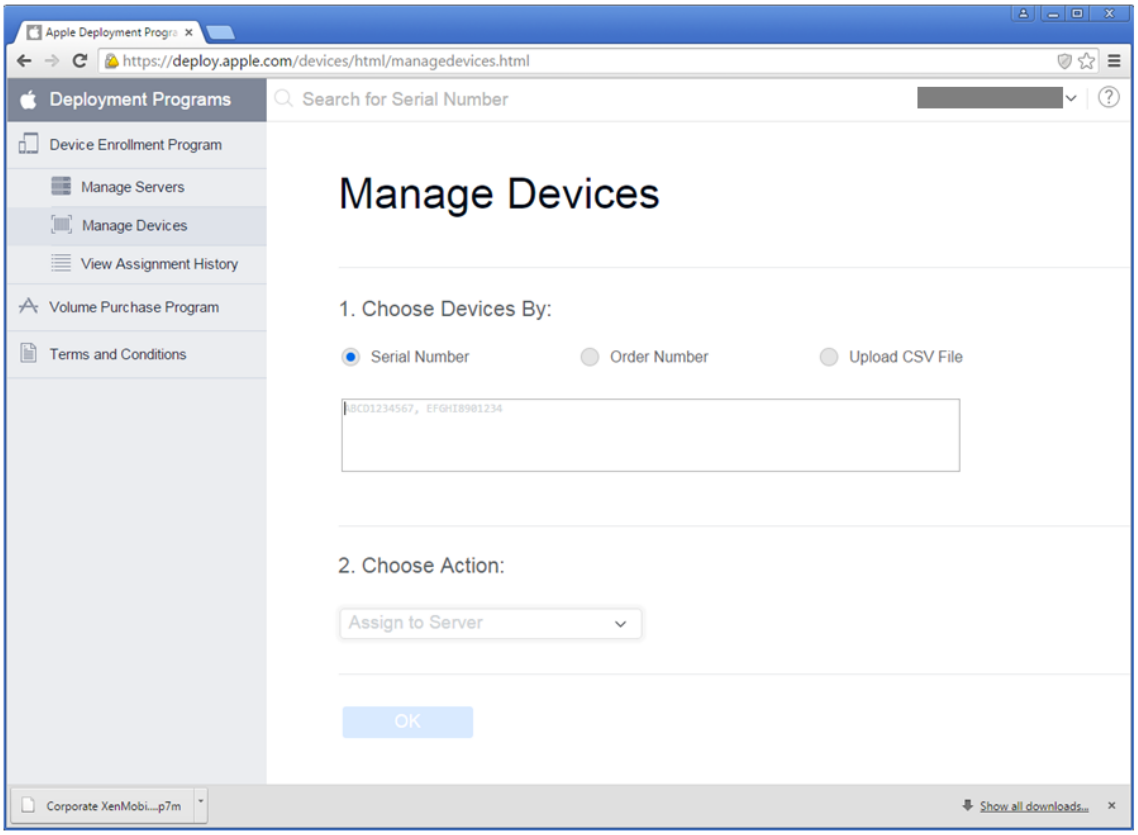
Gerenciar dispositivos ativados para DEP

Siga estas etapas para associar dispositivos ao Servidor XenMobile usando o DEP Portal para atualizar sua conta do Apple DEP

1. Faça login no Apple DEP Portal.

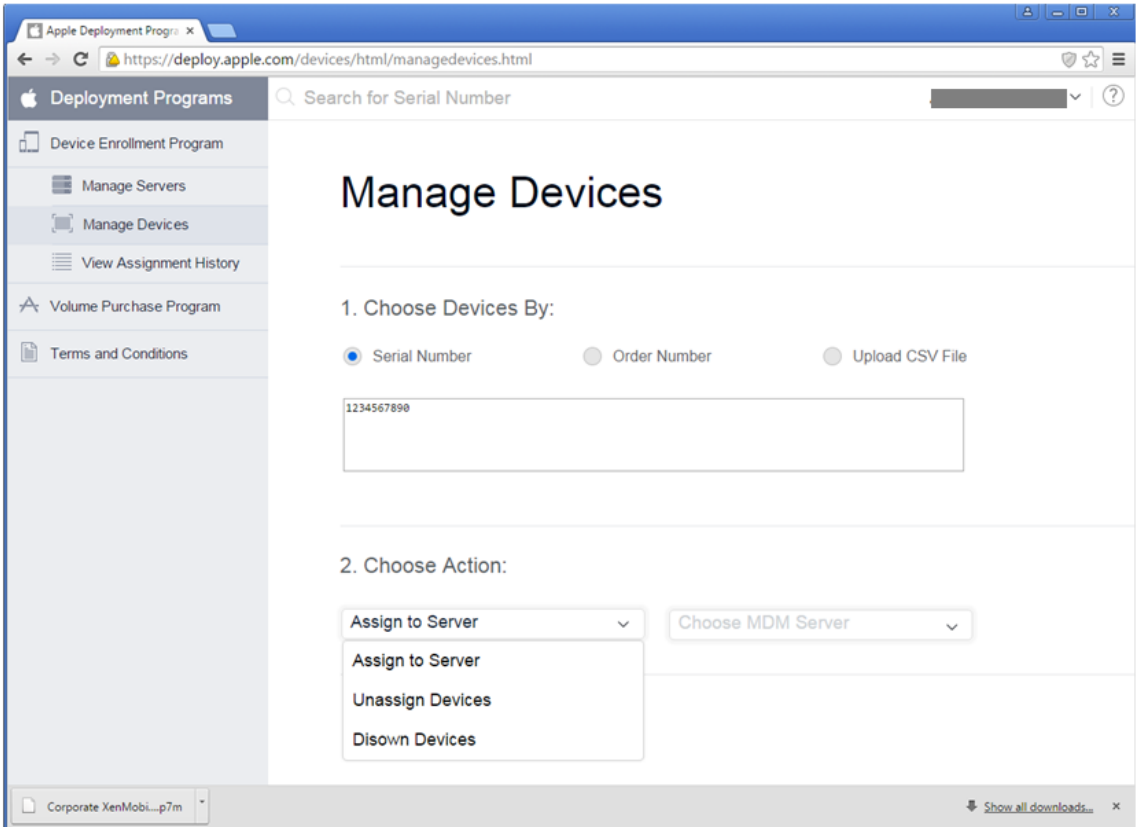
© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Clique em **Device Enrollment Program** e em **Manage Devices**. Em **Choose Devices By**, escolha a opção para a qual você deseja carregar e defina seus dispositivos ativados para o Apple DEP: **Serial Number**, **Order Number** ou **Upload CSV File**.



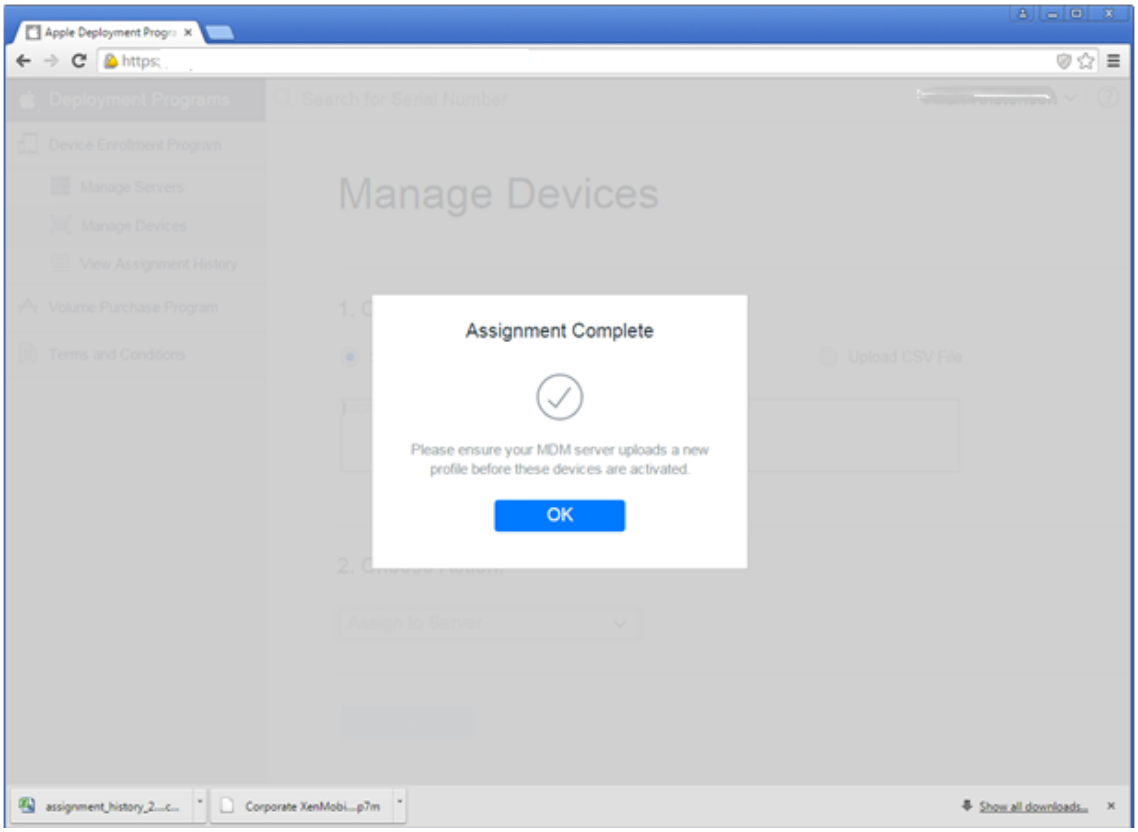
3. Para atribuir seus dispositivos a um XenMobile Server, em **Choose Action**, escolha **Assign to Server**. Em seguida, na lista, escolha o nome do seu XenMobile Server. Clique em **OK**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

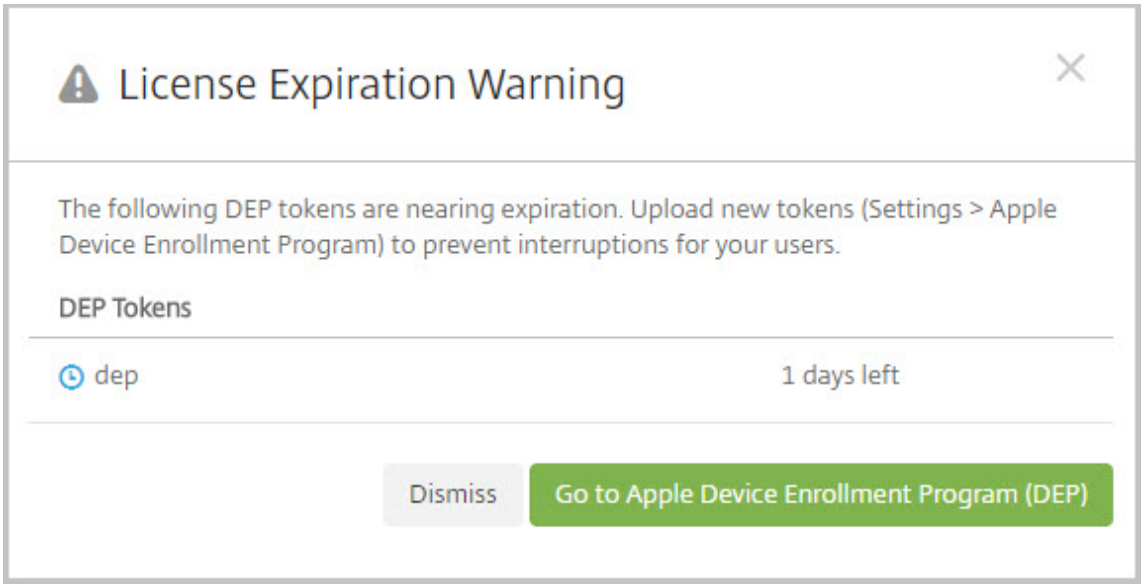


Os dispositivos do Apple DEP estão associados ao XenMobile Server selecionado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



O XenMobile exibe um Aviso de Expiração de Licença quando os tokens Apple DEP estão prestes a expirar ou expiraram.



Experiência do usuário ao registrar um dispositivo ativado para o Apple DEP

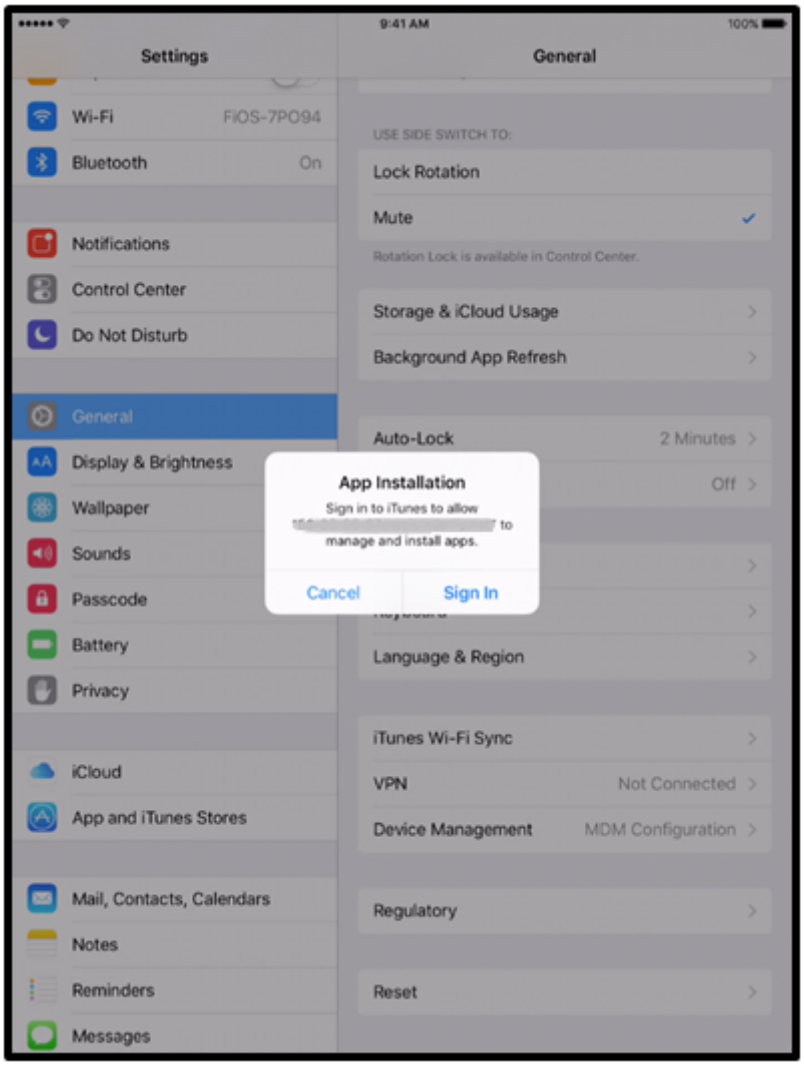
Quando os usuários registram um dispositivo ativado para Apple DEP, a experiência deles é a seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Os usuários iniciam o dispositivo ativado para o Apple DEP.
2. O XenMobile fornece a configuração do Apple DEP que você definiu no console XenMobile ao dispositivo ativado para o Apple DEP.
3. Os usuários definem as configurações iniciais em seus dispositivos.
4. O dispositivo inicia automaticamente o processo de registro de dispositivo do XenMobile.
5. Os usuários continuam a definir as outras configurações iniciais em seus dispositivos.
6. Na tela inicial, os usuários podem ser solicitados a fazer logon no iTunes para baixar o Citrix Secure Hub.

   > Nota:
   >
   > Essa etapa será opcional se o XenMobile estiver configurado para implantar o aplicativo Secure Hub usando a atribuição de aplicativos do Volume Purchase Program (VPP) com base em dispositivo. Nesse caso, você não precisa criar uma conta do iTunes ou usar uma conta existente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



7. Os usuários abrem o Secure Hub e digitam as respectivas credenciais. Se for exigido pela política, os usuários poderão ser solicitados a criar e verificar um PIN da Citrix.

   O XenMobile implanta os aplicativos necessários restantes no dispositivo.

Limite de registro de dispositivos

August 31, 2018

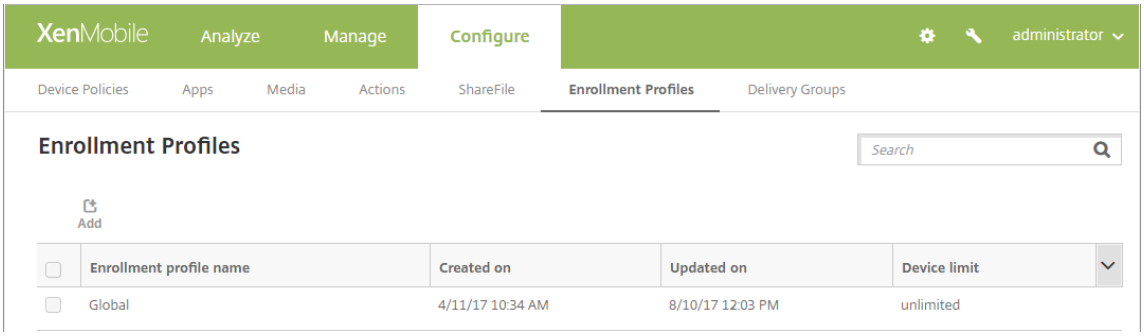
O XenMobile inclui um perfil de registro padrão que permite aos usuários registrar um número ilimitado de dispositivos. O perfil padrão é chamado de Global. Crie perfis de registro somente se você desejar limitar o número de dispositivos que os usuários podem registrar. Você associa perfis de registro com grupos de entrega.

O limite de registro do dispositivo se aplica aos modos de servidor ENT, MDM e MAM. O recurso está

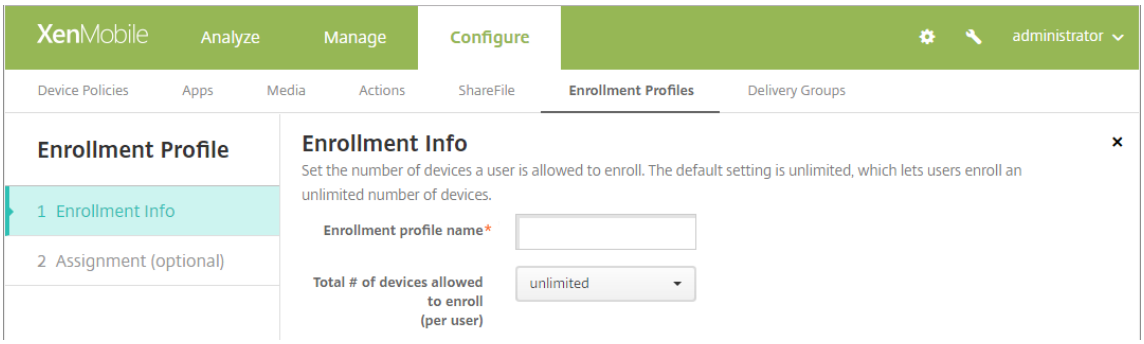
© 1999-2019 Citrix Systems, Inc. All rights reserved.

disponível apenas para dispositivos iOS e Android.

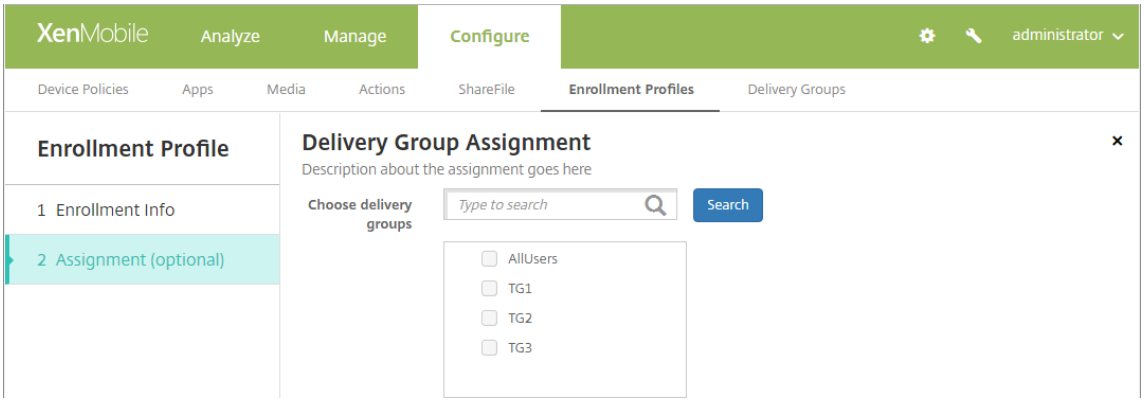
1. Acesse **Configurar > Perfis de registro**. O perfil Global padrão é exibido.



2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de **Informações do registro**, digite um nome para o perfil de registro e selecione o número de dispositivos que membros com este perfil podem registrar.



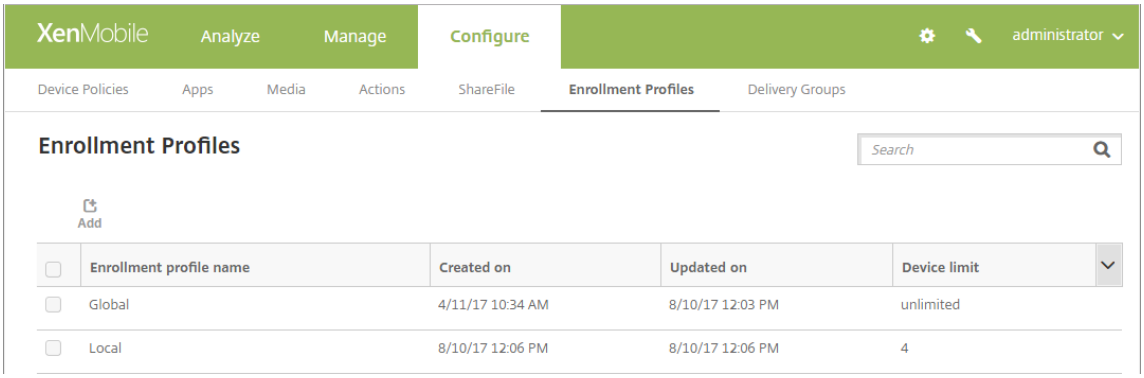
3. Clique em **Avançar**. A tela **Atribuição de grupo de entrega** é exibida.



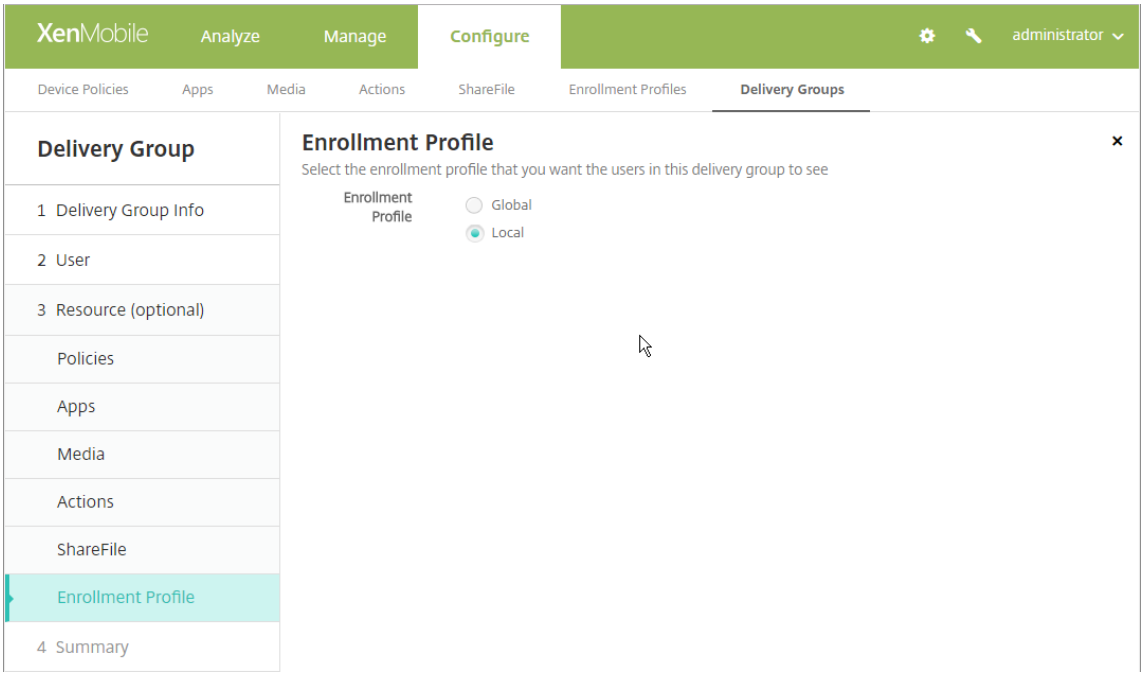
4. Selecione os grupos de entrega para este perfil de registro e, em seguida, clique em **Salvar**.

   A página **Grupos de entrega** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para alterar os perfis de registro associados a um grupo de entrega, vá para **Configurar > Grupos de entrega** e, em seguida, clique em **Perfis de registro**.

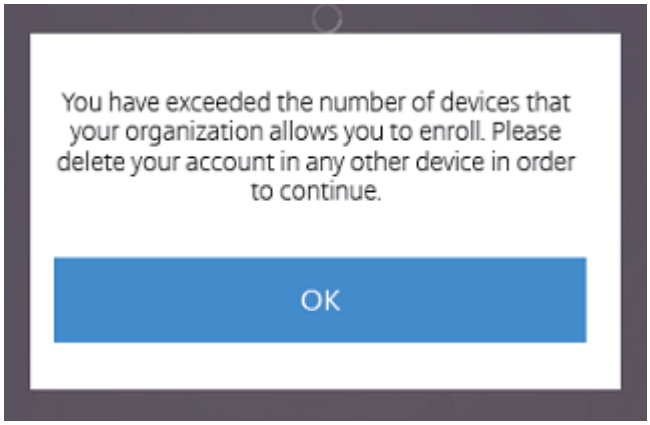


Experiência do usuário com um limite de registro de dispositivos

Quando você define o limite de registro de dispositivos e os usuários tentam registrar um novo dispositivo, estas etapas devem ser seguidas:

1. Faça logon no Secure Hub.
2. Insira um endereço de servidor a ser registrado.
3. Insira as credenciais.
4. Se o limite do dispositivo for atingido, uma mensagem de erro informará o usuário que ele excedeu o limite de registro do dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A tela de registro do Secure Hub é exibida novamente.

Registrar dispositivos

April 15, 2019

Para gerenciar dispositivos de usuários remotamente e com segurança, registre-os 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. Em seguida, no console XenMobile, você pode realizar tarefas de gerenciamento de dispositivo. Você pode aplicar políticas, implantar aplicativos, enviar dados por push para o dispositivo, além de bloquear, apagar e localizar dispositivos perdidos ou roubados.

O registro do Active Directory do Azure é compatível com dispositivos iOS, Android e Windows 10. 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 que você possa registrar usuários de dispositivos iOS, é necessário solicitar um certificado de APNs. Para obter detalhes, consulte Certificados e autenticação.

Para atualizar as opções de configuração para os usuários e dispositivos, use a página **Gerenciar > Convites para registro**. Para obter detalhes, consulte Envie um convite para registro neste artigo.

Dispositivos Android

> Nota:
>
> Para obter informações sobre como registrar os dispositivos do Android for Work, consulte Android for Work.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Acesse a Google Play Store no seu dispositivo Android, baixe o aplicativo Citrix Secure Hub e toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, clique em **Avançar** e, em seguida, clique em **Instalar**.
3. Depois que o Secure Hub for instalado, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome do XenMobile Server, o nome UPN ou o endereço de email. Em seguida, clique em **Avançar**.
5. Na tela **Ativar o administrador do dispositivo**, toque em **Ativar**.
6. Digite sua senha corporativa e toque em **Conectar**.
7. Dependendo da forma como XenMobile está configurado, você pode ser solicitado a criar um PIN da Citrix. Esse PIN pode ser usado para fazer login no Secure Hub e em outros aplicativos habilitados para o XenMobile, como o Secure Mail e o ShareFile. Insira o PIN da Citrix duas vezes. Na tela **Criar PIN da Citrix**, insira um PIN.
8. Insira novamente o PIN. O Secure Hub é aberto. Você pode acessar a XenMobile Store para exibir os aplicativos que pode instalar no seu dispositivo Android.
9. Se você tiver configurado o XenMobile para enviar aplicativos automaticamente por push aos dispositivos após o registro, os usuários serão solicitados a instalar esses aplicativos. Além disso, as políticas que você define no XenMobile são implantadas no dispositivo. Toque em **Instalar** para instalar os aplicativos.

Para cancelar o registro e registrar novamente um dispositivo Android

Os usuários podem cancelar o registro no Secure Hub. Quando os usuários cancelam o registro usando o procedimento aseguir, o dispositivo ainda é exibido no inventário de dispositivos do console XenMobile. No entanto, você não pode executar nenhuma ação 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 de você ter um telefone ou um tablet, faça o seguinte:

   Em um telefone:

   - Deslize a partir do lado esquerdo 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 email no canto superior direito.
   - Toque em **Preferências**, toque em **Contas** e, em seguida, toque em **Excluir conta**.
3. Toque em **Registrar novamente**. Uma mensagem é exibida para confirmar que você deseja registrar novamente o dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Toque em **OK**.

   O registro do dispositivo é cancelado.

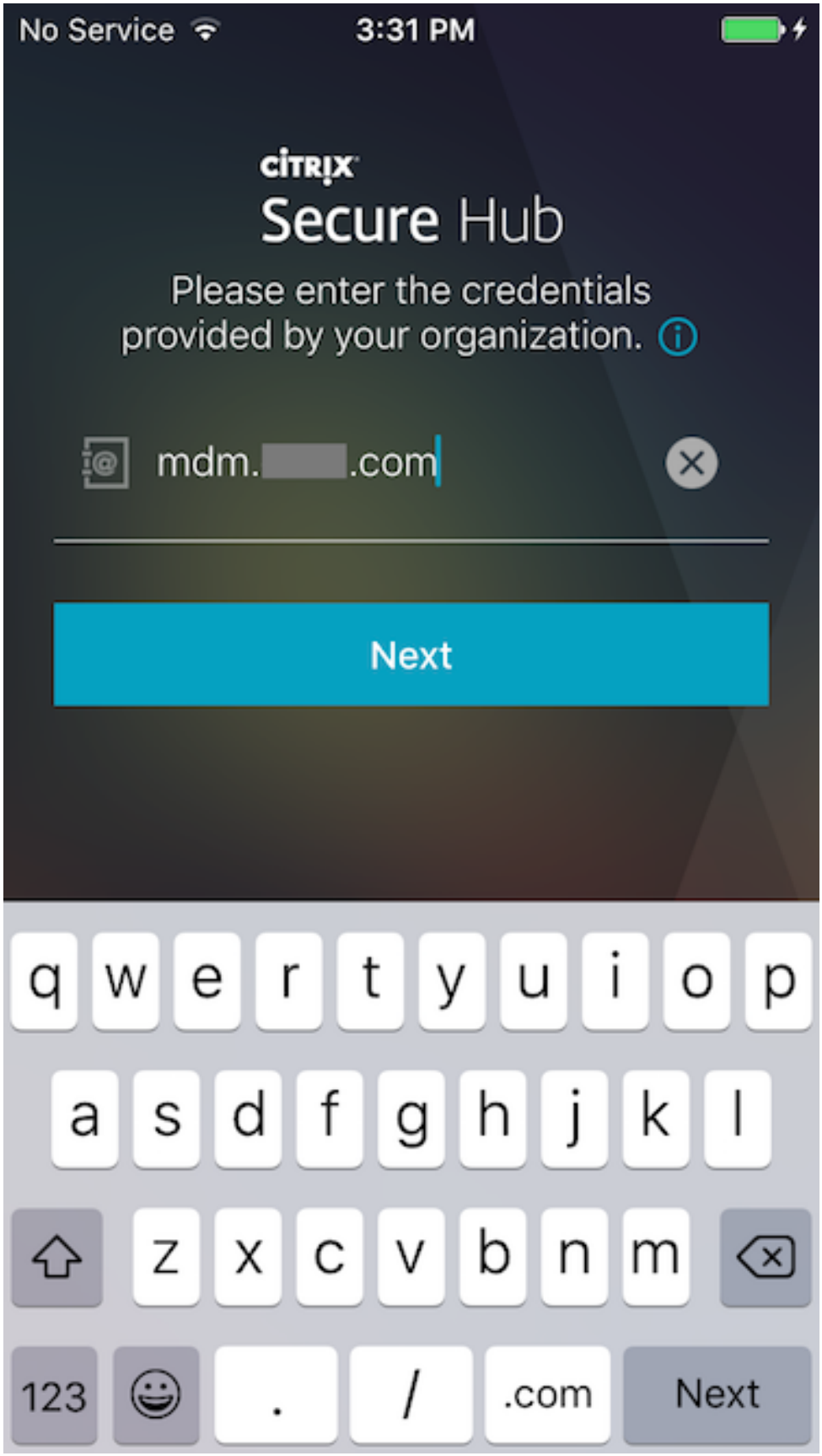
5. Siga-as instruções na tela para registrar novamente o dispositivo.

Dispositivos iOS que usam credenciais fornecidas pelo usuário

1. Baixe o aplicativo Secure Hub da App Store do Apple iTunes no dispositivo e instale-o no dispositivo.
2. Na tela inicial do dispositivo iOS, toque no aplicativo Secure Hub.
3. Quando o aplicativo Secure Hub é aberto, insira o endereço de servidor fornecido pela sua central de ajuda.

   A tela apresentada pode ser diferente destes exemplos, dependendo de como o XenMobile está configurado.

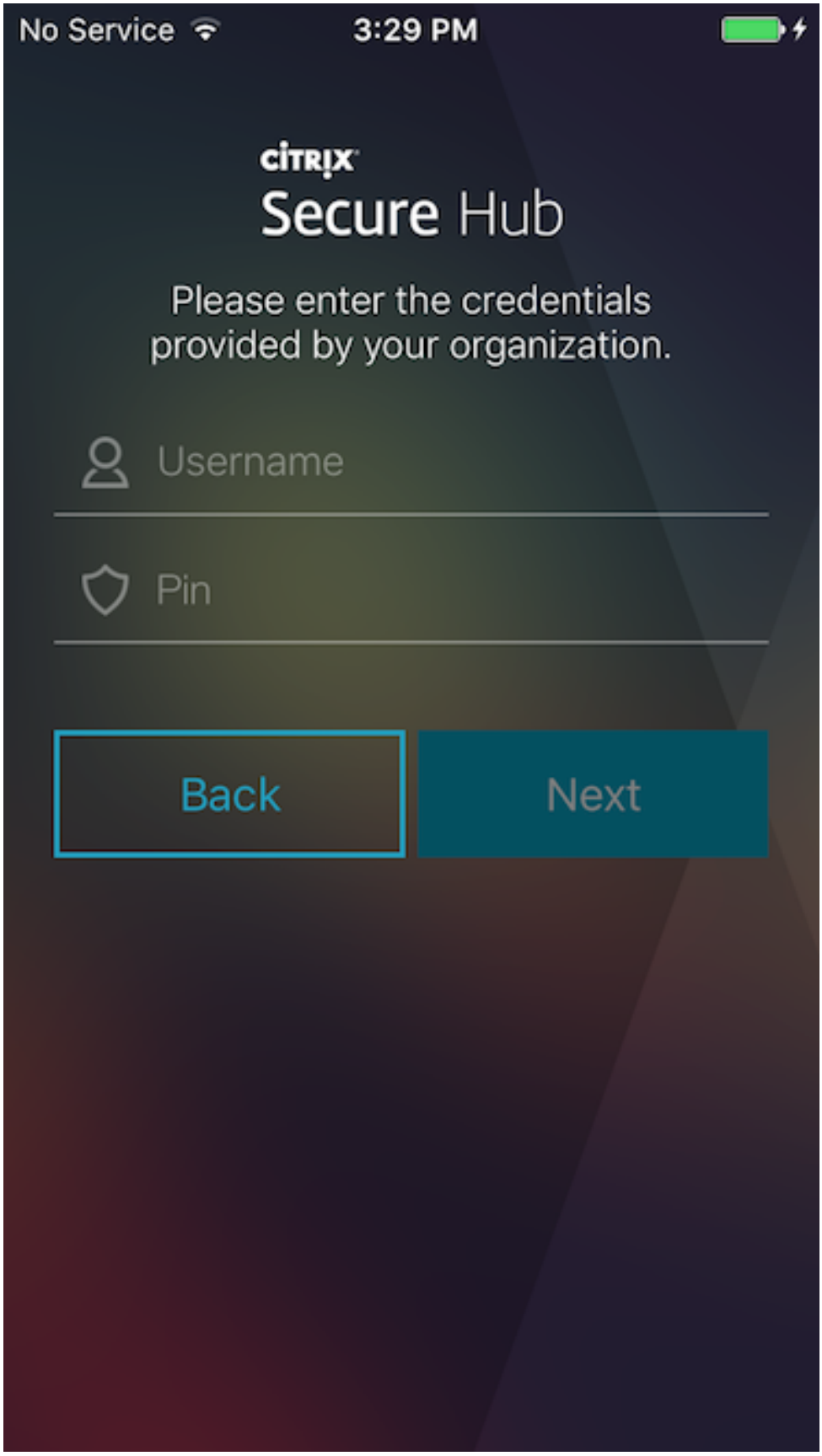
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Quando solicitado, digite o nome de usuário e senha ou PIN. Clique em **Avançar**.

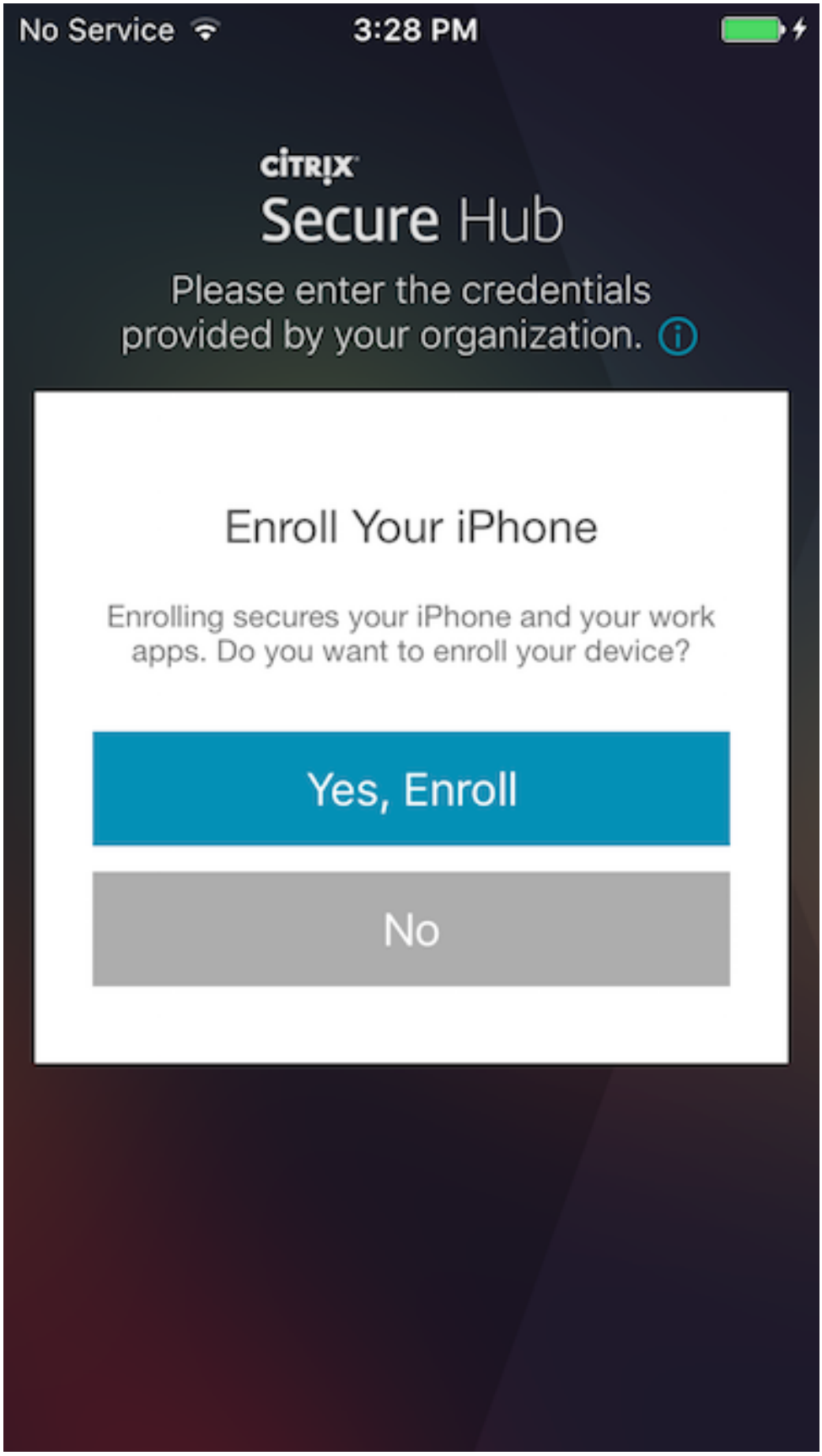
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

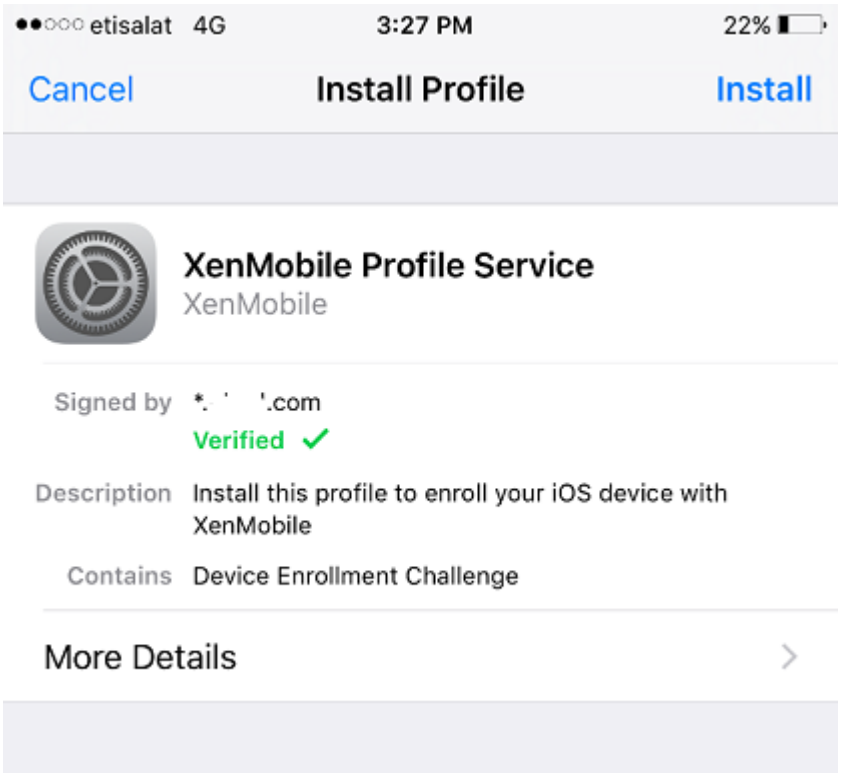
5. Quando solicitado a se registrar, clique em **Sim, registrar** e insira suas credenciais quando solicitado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

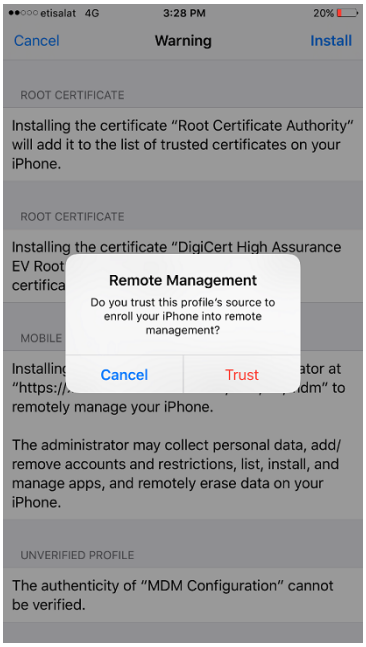


© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Toque em **Instalar** para instalar o Citrix Profile Services.



7. Toque em **Confiar**.



8. Toque em **Abrir** e insira suas credenciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dispositivos iOS que usam credenciais derivadas

O registro requer que os usuários inseriram seu cartão inteligente em um leitor conectado à sua área de trabalho.

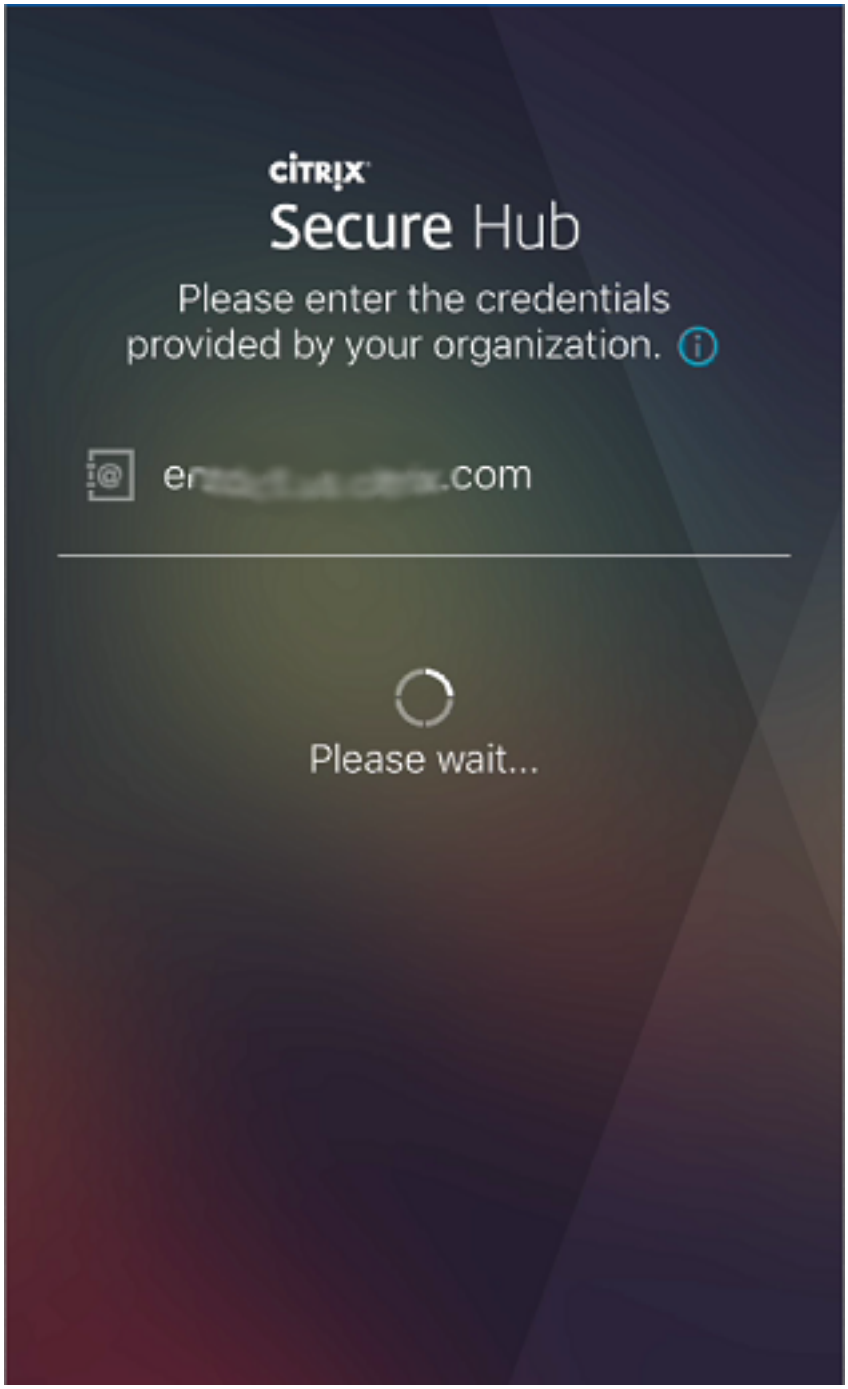
1. O usuário instala Secure Hub e o aplicativo do provedor de credencial derivada.

   O aplicativo do provedor de identidade para Intercede é o MyID for Citrix. Segue o logotipo desse aplicativo.

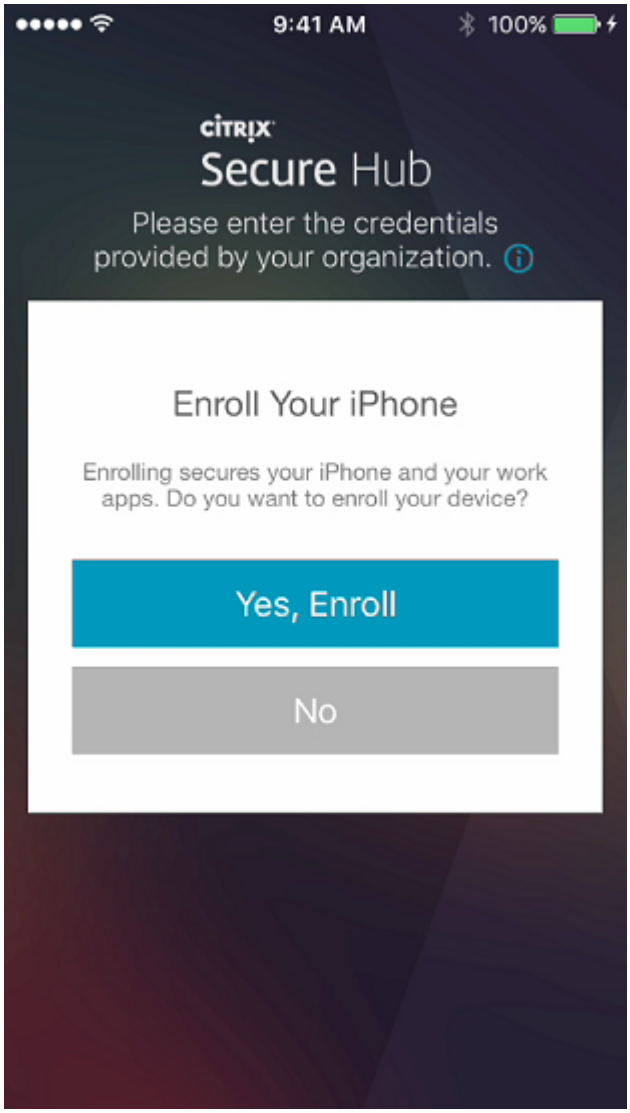
   

2. O usuário inicia o Secure Hub. Quando solicitado, o usuário digita o nome de domínio totalmente qualificado do XenMobile Server e clica em **Avançar**. O registro no Secure Hub é iniciado. Se o XenMobile Server oferecer suporte a credenciais derivadas, o Secure Hub solicita ao usuário que crie um PIN da Citrix.

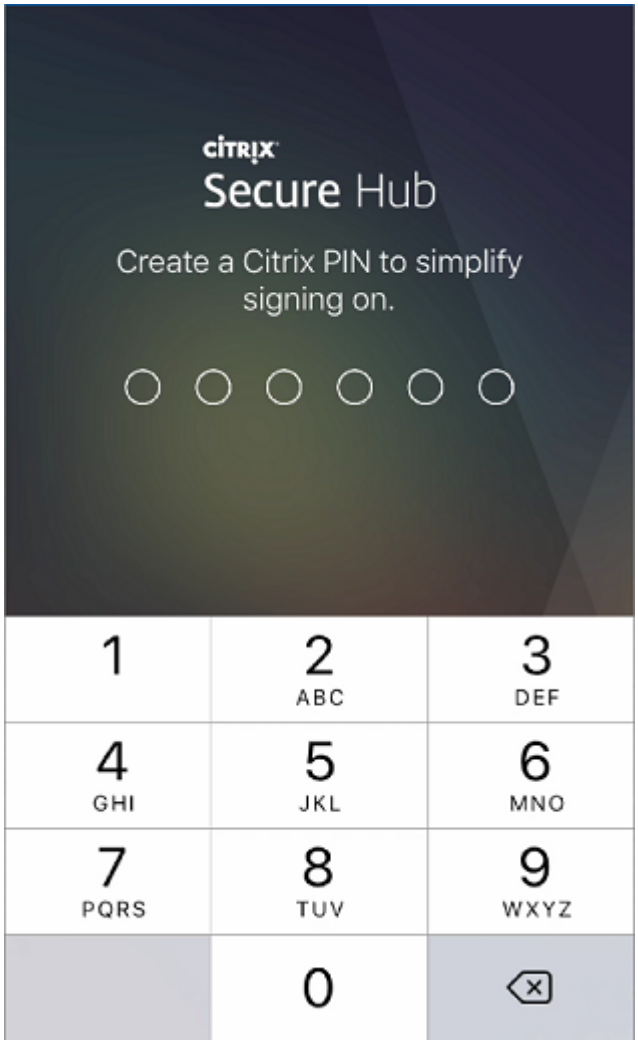
© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



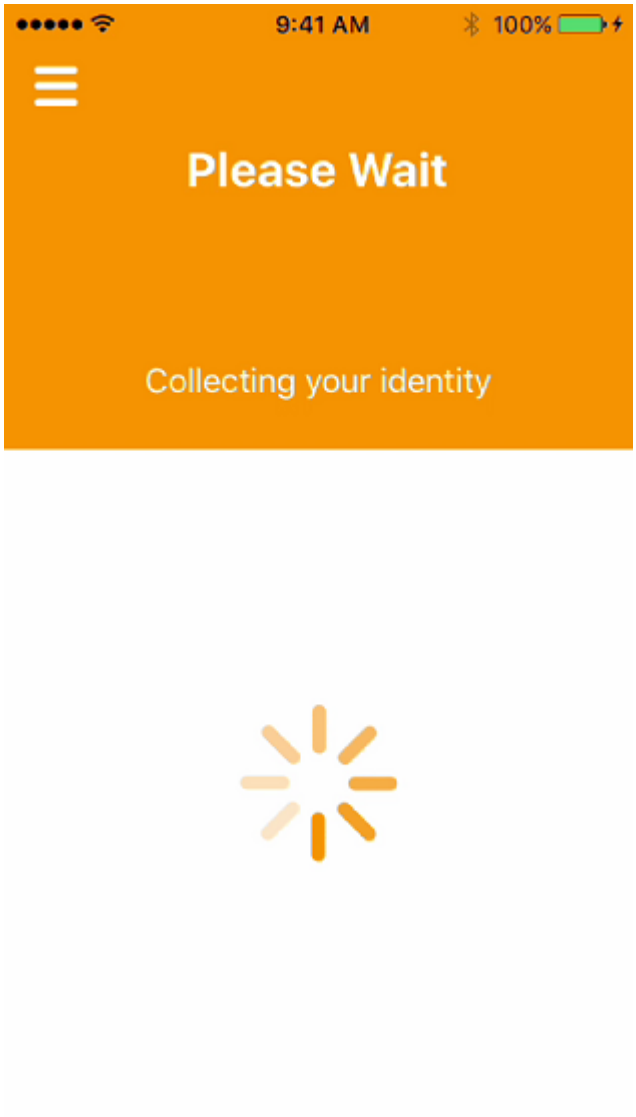
3. O usuário segue as instruções para ativar suas credenciais inteligentes. Será exibida uma tela de abertura, seguida por um aviso para escanear um código QR.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



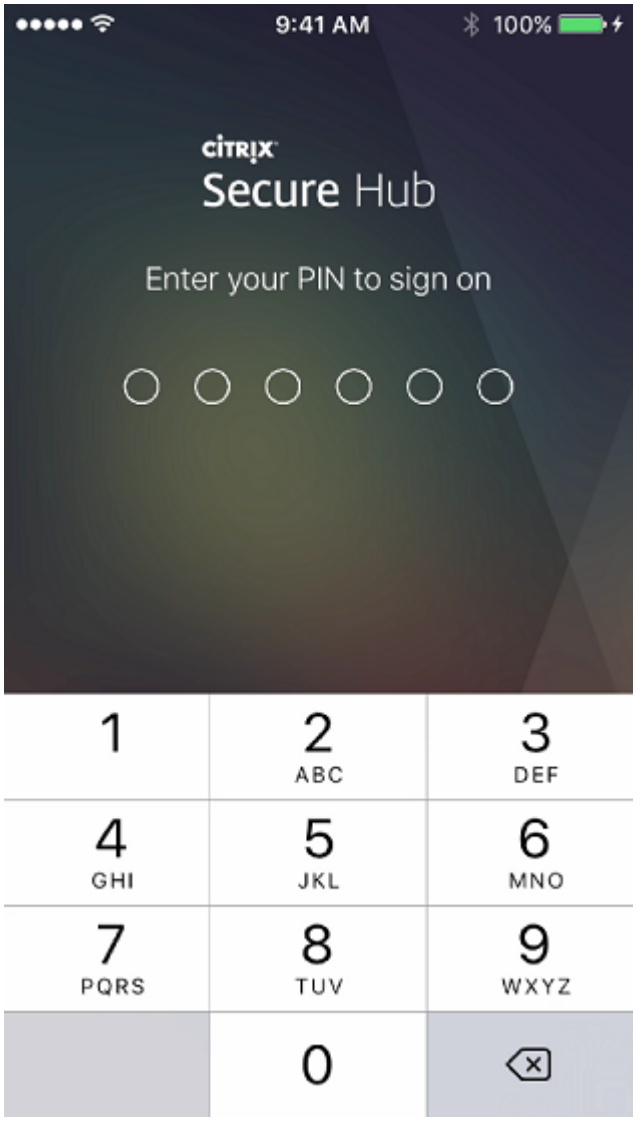
4. O usuário insere seu cartão no leitor de cartão inteligente conectado à área de trabalho. O aplicativo de desktop exibe um código QR e solicita que o usuário faça a leitura do código usando seu dispositivo móvel.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. O usuário insere seu PIN do Secure Hub quando solicitado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Depois de autenticar o PIN, o Secure Hub baixa os certificados. O usuário segue os prompts para concluir o registro.

Para exibir informações do dispositivo no console XenMobile:

- Vá para **Gerenciar > Dispositivos** e selecione um dispositivo para exibir uma caixa de comando. Clique em **Mostrar mais**.
- Vá para **Analisar > Painel.**

Dispositivos macOS

O XenMobile fornece dois métodos para registrar dispositivos que executam o macOS. Os dois modos permite que os usuários de macOS façam o registro diretamente dos seus dispositivos pela rede celular.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Enviar aos usuários um convite para registro:** Esse método de registro permite definir qualquer um dos seguintes modos de registro para dispositivos macOS:
  - Nome de usuário + senha
  - Nome de usuário + PIN
  - Dois Fatores

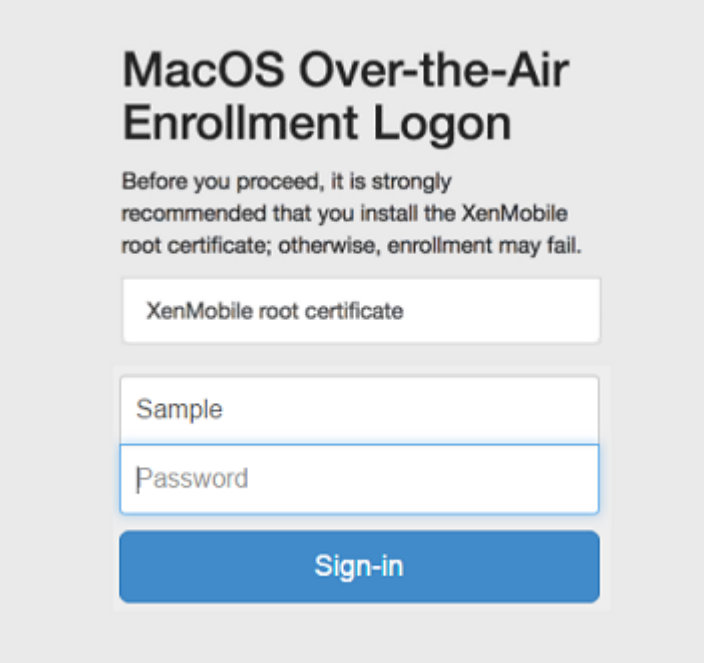
  Quando o usuário segue as instruções no convite de registro, é exibida uma tela de logon com o nome de usuário preenchido.
- **Enviar um link de instalação para os usuários:** esse método de registro para dispositivos macOS envia aos usuários um link de registro que eles podem abrir nos navegadores Safari ou Chrome. Um usuário se registra fornecendo seu nome de usuário e senha.

  Para impedir o uso de um link de registro para dispositivos macOS, defina a propriedade do servidor **Enable macOS OTAE** como **false**. Como resultado, os usuários do macOS apenas podem se registrar usando um convite para registro.

Enviar aos usuários um convite para registro

1. Opcionalmente, configure as políticas de dispositivo macOS no console XenMobile. Para obter mais informações sobre políticas de dispositivo, consulte Políticas de dispositivo.
2. Adicione um convite para registro de usuário do macOS. Para obter mais informações, consulte Envie um convite para registro neste artigo.
3. Depois que os usuários recebem o convite e clicam no link, é exibida a seguinte tela no navegador Safari. O XenMobile preenche o nome do usuário. Se você escolher **Dois fatores** para o modo de registro, outro campo será exibido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Os usuários instalam os certificados conforme necessário. A exibição do prompt para os usuários instalarem certificados depende se você configurou o seguinte para o 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 como gerencia os dispositivos móveis.

Enviar um link de instalação para os usuários

1. Opcionalmente, configure as políticas de dispositivo macOS no console 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 tiver configurado uma porta diferente, use essa porta em vez da 8443.
   - O **instanceName**, geralmente mostrado como zdm, é o nome especificado durante a instalação do servidor.

   Para obter mais informações sobre o envio de links de instalação, consulte Para enviar um link de instalação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 verão o prompt para instalar certificados. Para obter mais informações sobre certificados, consulte Certificados e autenticação.
4. Os usuários fazem login nos Macs.

   As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar Macs com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Dispositivos Windows

> Nota:
>
> Esta seção inclui referências aos dispositivos Windows Phone 8.1, que a Microsoft moveu para Fim de Suporte em 11 de julho de 2017. O XenMobile atualmente oferece suporte aos dispositivos Windows Phone 8.1 para o registro de MDM apenas.

Os dispositivos que executam o Windows 10 são registrados no Azure como um meio federado de autenticação do Active Directory. Você pode ingressar os dispositivos Windows 10 no AD do Microsoft Azure de qualquer uma das seguintes maneiras:

- Registre-se no MDM como parte do Ingresso no AD do Azure imediato na primeira vez que o dispositivo for ligado.
- Registre-se no MDM como parte do Ingresso no AD do Azure da página Configurações do Windows, depois que o dispositivo for configurado.

Você pode registrar dispositivos no XenMobile que executam os seguintes sistemas operacionais Windows:

- Windows 10 Phone e Tablet
- Windows Phone 8.1

Os usuários podem se registrar diretamente por meio de seus dispositivos.

> Nota:
>
> Para telefones e tablets Windows 10 RS2, durante o novo registro, um usuário não é solicitado a especificar a URL do servidor. Para resolver esse problema, reinicie o dispositivo. Ou, na tela de endereço de email, toque no X em **Conectando-se a um serviço** para ir até a página da URL do servidor. Esse é um problema de terceiros.

Você deve configurar a detecção automática e o serviço de detecção do Windows para o registro de usuário para ativar o gerenciamento de dispositivos Windows com suporte.

Antes que os usuários de dispositivos do 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 do Active Directory do Microsoft Azure.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Para que os dispositivos Windows se registrem, o certificado de ouvinte SSL deve ser um certificado público. O registro não ocorrerá se você tiver carregado um certificado SSL autoassinado.

Para registrar dispositivos Windows com a detecção automática

Para ativar o gerenciamento de dispositivos Windows, a Citrix recomenda que você configure o Serviço de Descoberta Automática e o serviço de Descoberta do Windows. Para obter detalhes, consulte XenMobile Autodiscovery Service.

1. No dispositivo, verifique e instale todas as atualizações disponíveis do Windows.
2. Em Windows 10: no menu de botões, toque em **Configurações** e em **Contas > Acessar o trabalho ou a escola > Conectar ao trabalho ou à escola**. Em telefones Windows 8.1: toque em **Configurações do PC > Rede > Local de Trabalho**.
3. Insira o seu endereço de email corporativo e toque em **Continuar** no Windows 10 ou em **Ativar o gerenciamento de dispositivo** no Windows 8.1. Para se registrar como um usuário local, insira um endereço de email inexistente com o nome de domínio correto (por exemplo, `foo@mydomain.com`). Isso permite que você ignore uma limitação conhecida da Microsoft na qual o registro é realizado pelo Gerenciamento de Dispositivo interno no Windows; na caixa de diálogo **Conectando a um serviço**, digite o nome do usuário e a senha associados ao usuário local. O dispositivo detecta automaticamente um XenMobile Server e inicia o processo de registro.
4. Digite sua senha. Use a senha associada a uma conta que faz parte de um grupo de usuários no XenMobile.
5. Em Windows 10: na caixa de diálogo **Termos de uso**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Aceitar**. Em Windows 8.1: na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Ligar**.

Para registrar dispositivos Windows sem a detecção automática

É possível registrar dispositivos Windows sem a detecção automática. A Citrix, no entanto, recomenda que você configure a detecção automática. O registro sem detecção automática resulta em uma chamada para a porta 80 antes da conexão com a URL desejada, portanto, não é considerado uma prática recomendada para implantações de produção. A Citrix recomenda que você use esse processo somente em ambientes de teste e implantações de prova de conceito.

1. No dispositivo, verifique e instale todas as atualizações disponíveis do Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em Windows 10: no menu de botões, toque em **Configurações** e em **Contas > Acessar o trabalho ou a escola > Conectar ao trabalho ou à escola**. Em Windows 8.1: toque em **Configurações do PC > Rede > Local de Trabalho**.
3. Insira o seu endereço de email da empresa.
4. Em Windows 10: se a detecção automática não estiver configurada, uma opção será exibida na qual você pode inserir os detalhes do servidor, conforme descrito na etapa 5. No Windows 8.1: se a opção **Detectar automaticamente o endereço do servidor** estiver definida como **ativada**, **desative** a opção.
5. Em Windows 10, no campo **Inserir endereço do servidor**, digite o endereço: `https://serverfqdn:8443/serverInstance/wpe`.

   Se uma porta diferente de 8443 for usada para as conexões SSL não autenticadas, use esse número de porta em vez de 8443 nesse endereço.

   No 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 as conexões SSL não autenticadas, use esse número de porta em vez de 8443 nesse endereço.
6. Digite sua senha.
7. Em Windows 10: na caixa de diálogo **Termos de uso**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Aceitar**. Em Windows 8.1: na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Ligar**.

Para registrar dispositivos Windows Phone

Para registrar dispositivos Windows Phone no XenMobile, os usuários precisam dos respectivos endereços de email e senha do Active Directory ou da rede interna. Se a detecção automática não estiver configurada, os usuários precisarão também do endereço da Web do XenMobile Server. Em seguida, eles seguem este procedimento nos dispositivos deles para se registrarem.

> Nota:
>
> Se você planeja implantar aplicativos usando a loja da empresa do Windows Phone, antes que os usuários se registrem, verifique se uma política do Hub empresarial foi configurada (com um aplicativo assinado Secure Hub e Windows Phone para cada plataforma à qual você desejar oferecer compatibilidade).

1. Na tela principal do Windows Phone, toque no ícone **Configurações**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Em Windows 10: dependendo da versão, toque em **Contas > Acessar trabalho ou escola > Conectar ao trabalho ou à escola** ou toque em **Contas > Acesso corporativo > Registrar-se no gerenciamento de dispositivo**.
- Em Windows 8.1: toque em **Configurações do PC > Rede> Local de trabalho** e depois toque em **Adicionar conta**.

2. Na tela seguinte, insira um endereço de email e uma senha e, em seguida, toque em **entrar**.

   Se a detecção automática estiver configurada para o seu domínio, as informações solicitadas nas próximas etapas serão preenchidas automaticamente. Prossiga para a Etapa 8.

   Se a detecção automática não estiver configurada para o seu domínio, continue até a próxima etapa. Para se registrar como um usuário local, insira um endereço de email inexistente com o nome de domínio correto (por exemplo, `foo@mydomain.com`). Isso permite que você ignore uma limitação conhecida da Microsoft: na caixa de diálogo **Conectando a um serviço**, digite o nome do usuário e a senha associados ao usuário local.

3. Na tela seguinte, digite o endereço da Web do XenMobile Server, como: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. Por exemplo, `https://mycompany.mdm.com:8443/zdm/wpe`.

   > Nota:
   >
   > O número da porta deve ser adaptado para a sua implementação. Ela deve ser a mesma porta que você usou para uma inscrição do iOS.

4. Insira o nome do usuário e o domínio se a autenticação for validada por meio de um nome do usuário e um domínio e, em seguida, toque em **entrar**.
5. Se uma tela for exibida indicando um problema com o certificado, o erro será o resultado do uso de um certificado autoassinado. Se o servidor for confiável, toque em **continuar**. Caso contrário, toque em **Cancelar**.
6. No Windows Phone 8.1, quando a conta é adicionada, você tem a opção de selecionar **Instalar aplicativo da empresa**. Se o administrador tiver configurado uma loja de aplicativos da empresa, selecione essa opção e toque em **concluído**. Se você desmarcar essa opção, precisará registrar novamente o seu dispositivo para receber a Loja de aplicativos da empresa.
7. No Windows Phone 8.1, na tela **Conta adicionada**, toque em **concluído**.
8. Para forçar uma conexão com o servidor, toque no ícone de atualização. Se o dispositivo não se conectar manualmente ao servidor, o XenMobile tentará se reconectar. O XenMobile se conecta ao dispositivo a cada três minutos por cinco vezes sucessivas, e depois a cada duas horas. Você pode alterar essa taxa de conexão na opção **Windows WNS Heartbeat Interval** localizada em **Propriedades do servidor**. Depois que o registro for concluído, o Secure Hub se registrará em segundo plano. Nenhum indicador é exibido quando a instalação é concluída. Toque em Secure Hub na tela **Todos os Aplicativos**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Envie um convite para registro

No console XenMobile, você pode enviar um convite para registro aos usuários com dispositivos iOS, macOS e Android. Você também pode enviar um link de instalação aos usuários com dispositivos iOS ou Android.

Convites para registro são enviados da seguinte maneira:

- Se o convite para registro for para um local ou um usuário do Active Directory: o usuário receberá o convite via SMS com o nome de número e a operadora de telefone especificada.
- Se o convite para registro é para um grupo: os usuários recebem convites via SMS. Se os usuários do Active Directory tiverem um endereço de email e número do telefone celular no Active Directory, eles receberão o convite. Usuários locais recebem o convite no email e número de telefone especificados nas propriedades do usuário.

Após o registro dos usuários, seus dispositivos aparecem como gerenciados em **Gerenciar > Dispositivos**. O status da URL de convite é mostrado como **Resgatado**.

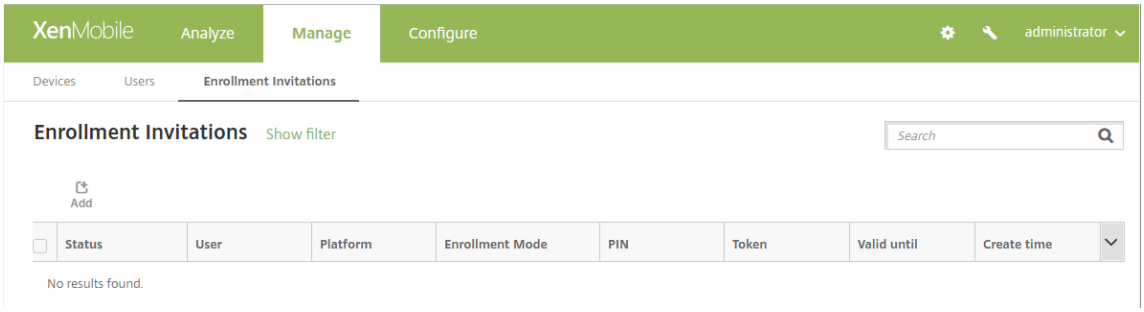
Pré-requisitos

- XenMobile Server configurado no modo Empresarial (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 são associados a grupos locais.
- Se estiver usando o Active Directory:
  - Grupos de entrega são associados a grupos do Active Directory.

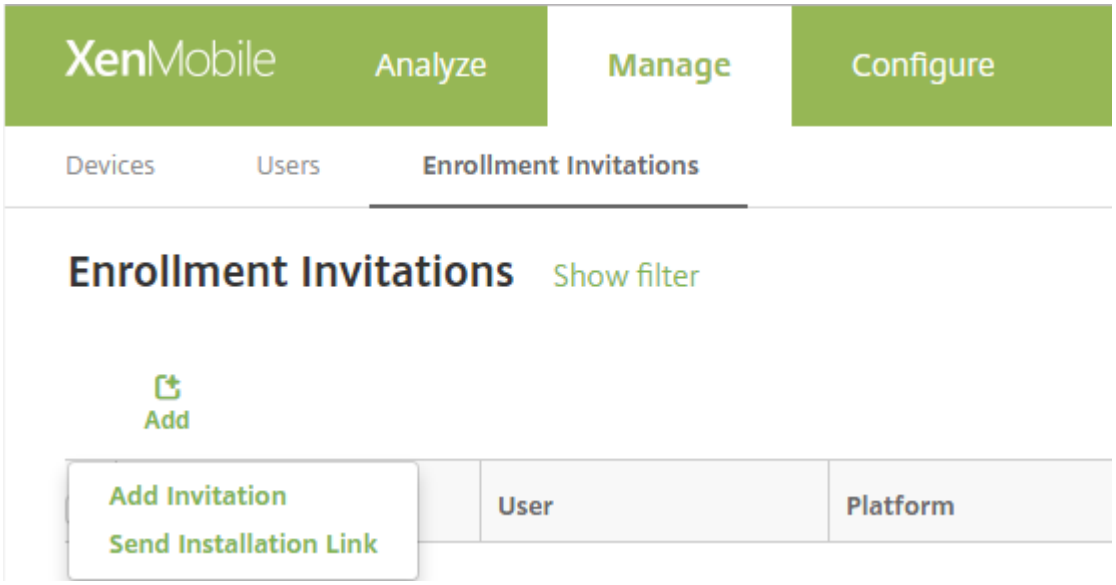
Criar um convite para registro

1. No console XenMobile, clique em **Gerenciar > Convites para registro**. A página **Convites para registro** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



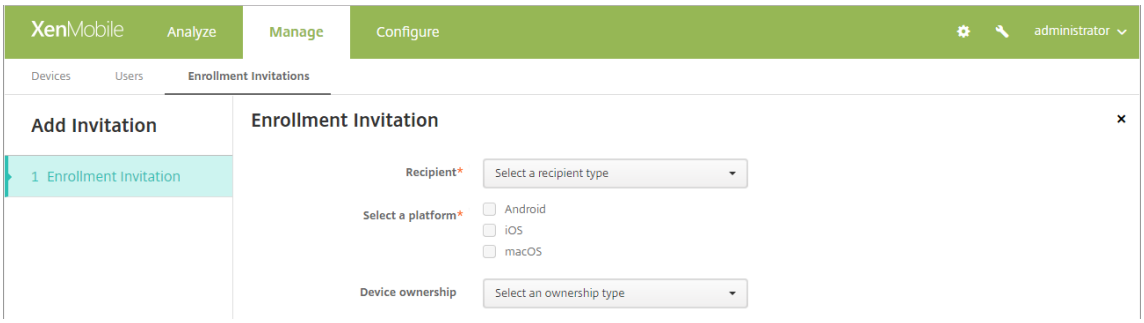
2. Clique em **Adicionar**. É exibido um menu de opções de registro.



   - Para enviar um convite para registro para um usuário ou grupo, clique em **Adicionar convite**.
   - Para enviar um link de instalação de registro para uma lista de destinatários via SMTP ou SMS, clique em **Enviar link de instalação**.

   O processo de enviar convites para registro e links de instalação é descrito após estas etapas.

3. Clique em **Adicionar convite**. A tela **Convite para registro** é exibida.



4. Defina estas configurações:

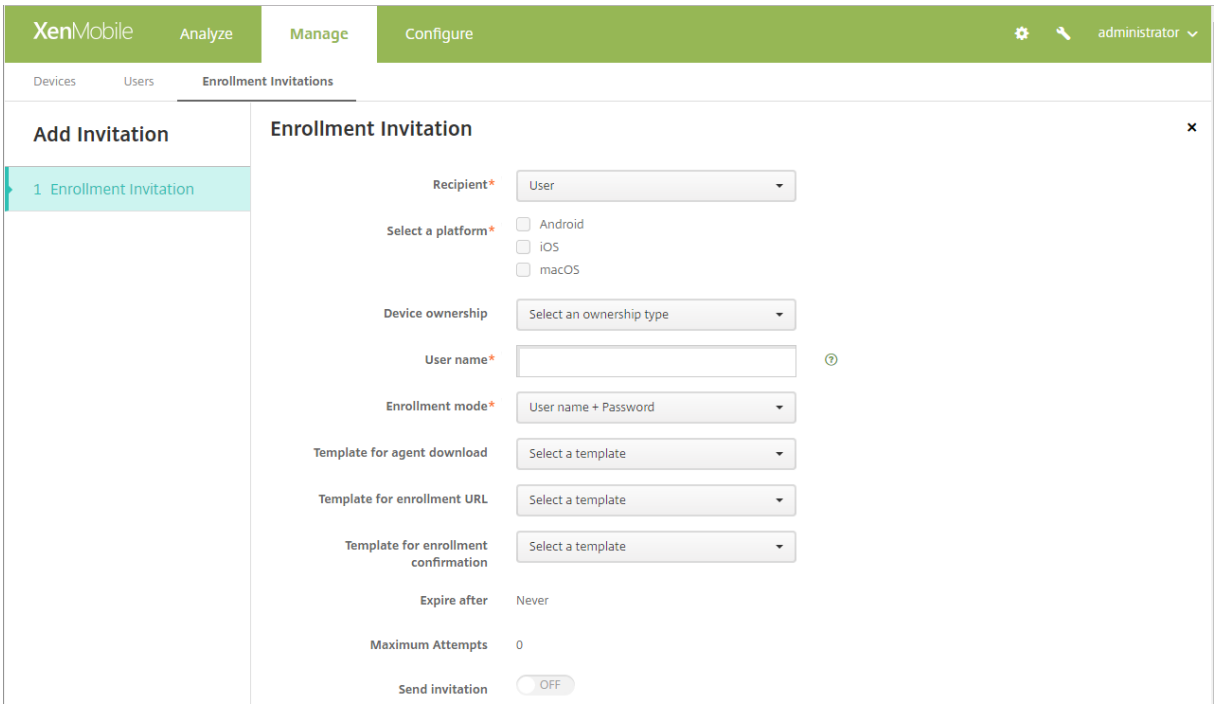
   - **Destinatário:** escolha **Grupo** ou **Usuário**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Selecionar uma plataforma:** se **Destinatário** for **Grupo**, todas as plataformas estarão selecionadas. É possível alterar a seleção da plataforma. Se **Destinatário** for **Usuário**, nenhuma plataforma estará selecionada. Selecione uma plataforma.
- **Propriedade do dispositivo**: selecione **Corporativo** ou **BYOD**.

Configurações para usuários ou grupos são exibidas, conforme descrito nas seções a seguir.

Para enviar um convite para registro a um usuário



1. Defina 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, verifique se a propriedade de email desse usuário esteja definida, para que você possa enviar notificações ao usuário. Se o usuário estiver no Active Directory, verifique se o LDAP está configurado.
   - **Informações do dispositivo:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Escolha **Número de série**, **UDID** ou **IMEI**. Depois de escolher uma opção, é exibido um campo no qual você pode digitar o valor correspondente do dispositivo.
   - **Número de telefone:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Opcionalmente, digite o número de telefone do usuário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Operadora:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Escolha uma operadora a ser associada ao número de telefone do usuário.
- **Modo de registro:** escolha como você deseja que os usuários se registrem. 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

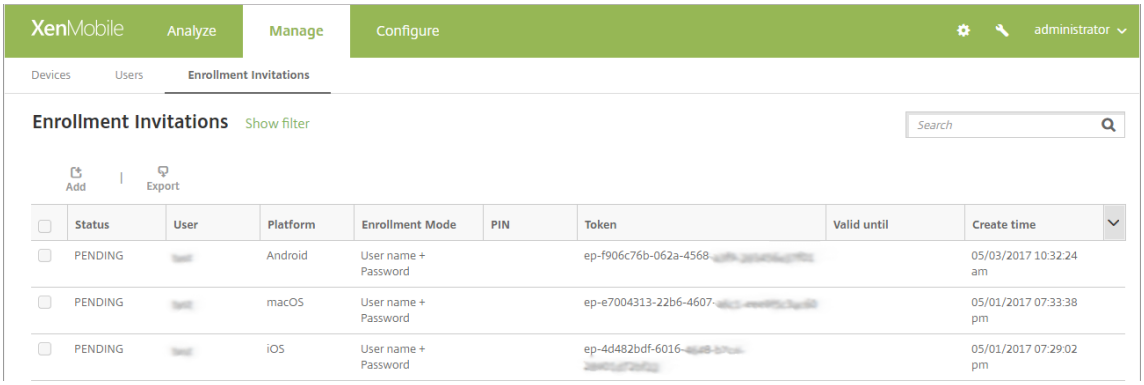
Somente os modos de registro válidos para cada uma das plataformas selecionadas são exibidos. Um PIN para o registro também é chamado de PIN ocasional. Esses PINs são válidos somente quando o usuário se registra.

> Nota:
>
> Quando você seleciona qualquer modo de registro que inclui um PIN, o campo **Modelo de PIN de registro** é exibido, onde você clica em **PIN de registro**.

- **Modelo para download do agente:** escolha o modelo do link de download denominado **Link para download**. Esse modelo é para todas as plataformas com suporte.
- **Modelo para URL de registro:** escolha **Convite para registro**.
- **Modelo para confirmação de registro:** escolha **Confirmação de registro**.
- **Expira após:** esse campo é definido quando você configura o modo de registro e indica quando o registro expira. Para obter mais informações sobre como configurar os modos de registro, consulte Para configurar modos de registro.
- **Máximo de tentativas:** esse campo é definido quando você configura o **Modo de registro** e indica o número máximo de vezes que o processo de registro ocorre. Para obter mais informações sobre como configurar os modos de registro, consulte Para configurar modos de registro.
- **Enviar convite:** selecione **I** para enviar o convite imediatamente. Selecione **O** para adicionar o convite à tabela na página **Convites para registro**, mas não enviá-lo.

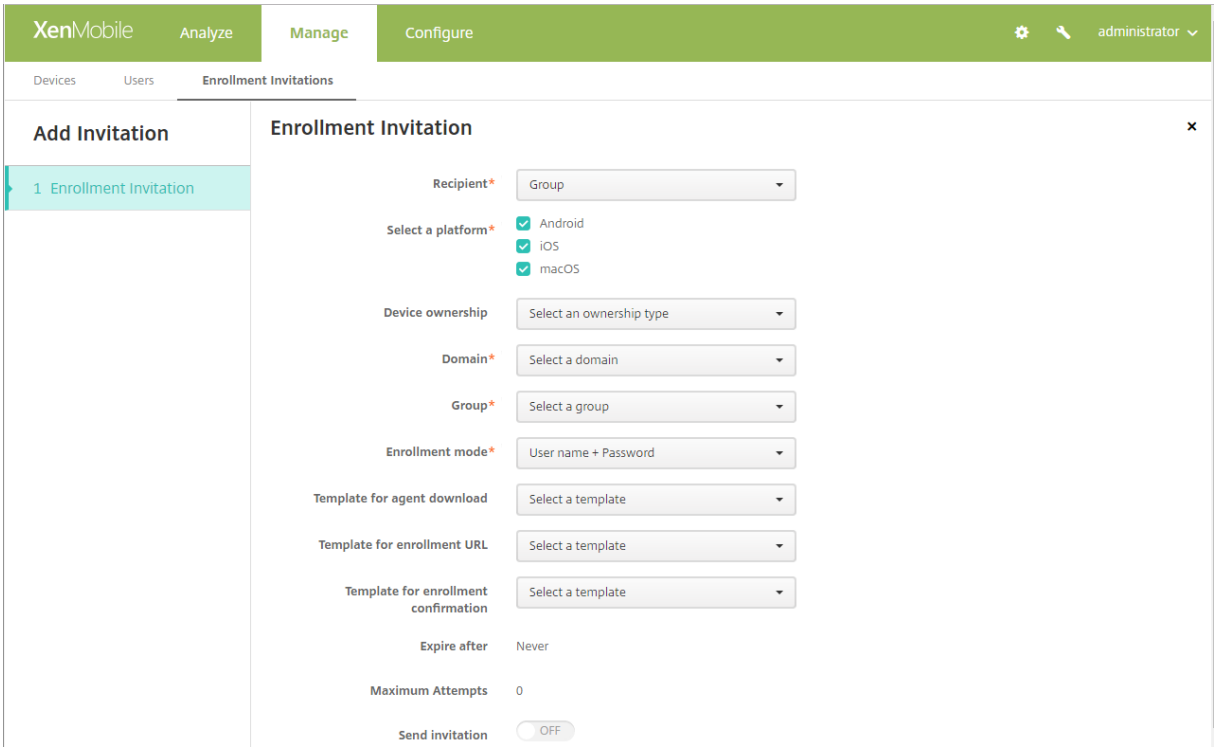
2. Clique em **Salvar e enviar** se tiver ativado a opção **Enviar convite**. Caso contrário, clique em **Salvar**. O convite é exibido na tabela na página **Convites para registro**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para enviar um convite para registro a um grupo

A figura a seguir mostra as definições para configurar um convite de registro para um grupo.



1. Defina estas configurações:
   - **Domínio:** selecione o domínio do grupo para receber o convite.
   - **Grupo:** escolha o grupo que receberá o convite.
   - **Modo de registro:** escolha como você deseja que os usuários do grupo se registrem. 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

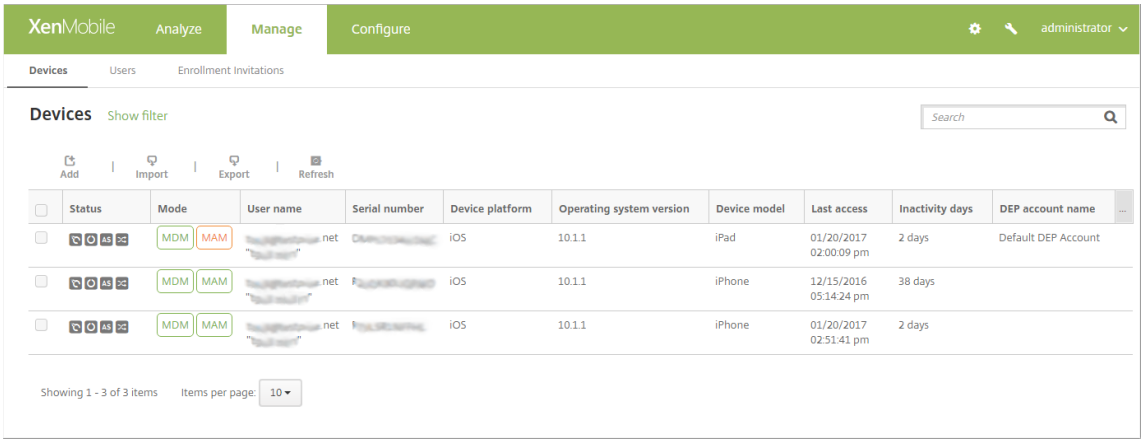
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Dois Fatores
- Nome de usuário + PIN

Somente os modos de registro válidos para cada uma das plataformas selecionadas são exibidos.

> Nota:
>
> Quando você seleciona qualquer modo de registro que inclui um PIN, o campo **Modelo de PIN de registro** é exibido, onde você clica em **PIN de registro**.

- **Modelo para download do agente:** escolha o modelo do link de download denominado **Link para download:**. Esse modelo é para todas as plataformas com suporte.
- **Modelo para URL de registro:** escolha **Convite para registro**.
- **Modelo para confirmação de registro:** escolha **Confirmação de registro**.
- **Expira após:** esse campo é definido quando você configura o modo de registro e indica quando o registro expira. Para obter mais informações sobre como configurar os modos de registro, consulte Para configurar modos de registro.
- **Máximo de tentativas:** esse campo é definido quando você configura o Modo de registro e indica o número máximo de vezes que o processo de registro ocorre. Para obter mais informações sobre como configurar os modos de registro, consulte Para configurar modos de registro.
- **Enviar convite:** selecione **I** para enviar o convite imediatamente. Selecione **O** para adicionar o convite à tabela na página **Convites para registro**, mas não enviá-lo.

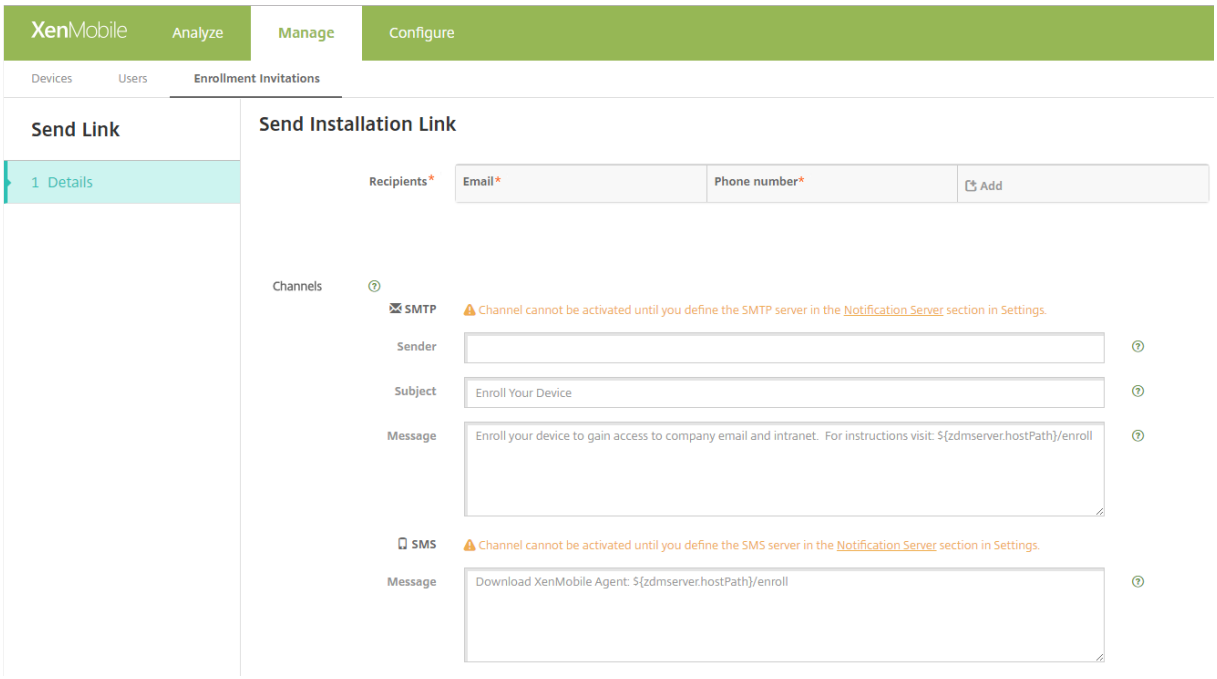
2. Clique em **Salvar e enviar** se tiver ativado a opção **Enviar convite**. Caso contrário, clique em **Salvar**. O convite é exibido na tabela na página **Convite para registro**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para enviar um link de instalação

Para enviar um link de instalação de registro, antes é preciso configurar canais (SMTP ou SMS) no servidor de notificação na página **Configurações**. Para obter detalhes, consulte [Notificações](/pt-br/xenmobile/server/users/notifications.html



1. Defina essas configurações e clique em **Salvar**.
   - **Destinatário:** para cada destinatário que você desejar adicionar, clique em **Adicionar** e 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.

   > Nota:
   >
   > Para excluir um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira à direita. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou em **Cancelar** para mantê-la.

   Para editar um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Atualize a listagem e clique em **Salvar** para salvar a alteração ou em **Cancelar** para deixá-la inalterada.

   - **Canais:** selecione um canal a ser usado para enviar o link de instalação de registro. Você pode enviar notificações por **SMTP** ou **SMS**. Esses canais não podem ser ativados até que você defina as configurações de servidor na página **Configurações** em **Servidor de notificação**. Para obter detalhes, consulte Notificações.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **SMTP:** defina estas configurações opcionais. Se você não digitar nada nesses campos, os valores padrão especificados no modelo de notificação configurado para a plataforma que você selecionou serão usados:
  - **Remetente:** insira um remetente opcional.
  - **Assunto:** digite um assunto opcional para a mensagem. Por exemplo, “Registre o seu dispositivo”.
  - **Mensagem:** digite uma mensagem opcional a ser enviada para o destinatário. Por exemplo, “Registre o seu dispositivo para obter acesso aos aplicativos e ao email organizacionais”.
- **SMS:** defina essa configuração. Se você não digitar nada nesse campo, o valor padrão especificado no modelo de notificação configurado para a plataforma que você selecionou será usado:
  - **Mensagem:** digite uma mensagem opcional a ser enviada para os destinatários. Esse campo é obrigatório para notificações baseadas em SMS.

> Nota: na América do Norte, as mensagens SMS que excedem 160 caracteres são entregues em várias mensagens.

2. Clique em **Send**.

> Nota:
>
> Se seu ambiente usar sAMAccountName, depois que os usuários receberem o convite e clicarem no link, eles deverão editar o nome do usuário para concluir a autenticação. O nome do usuário é exibido no formato sAMAccountName@domainname.com. Os usuários devem remover a parte @domainname.com.

Firebase Cloud Messaging

March 6, 2019

> Nota:
>
> Firebase Cloud Messaging (FCM) era anteriormente conhecido como Google Cloud Messaging (GCM). Alguns rótulos e mensagens do console XenMobile Server usam a terminologia do GCM.

A Citrix recomenda que você use o Firebase Cloud Messaging (FCM) para controlar como e quando dispositivos Android se conectam ao XenMobile Server. O XenMobile Server, quando configurado para FCM, envia notificações de conexão para dispositivos Android habilitados para FCM. Qualquer ação de segurança ou comando de implantação dispara uma notificação por push para solicitar ao usuário que se reconecte ao XenMobile Server.

Depois de concluir as etapas de configuração deste artigo e um dispositivo fazer check-in, o dispositivo se registra no serviço FCM no XenMobile Server. Essa conexão permite a comunicação quase em

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tempo real do seu XenMobile Server com o seu dispositivo usando o FCM. O registro do FCM funciona para registros de novos dispositivos e dispositivos registrados anteriormente.

Quando o XenMobile Server precisa iniciar uma conexão com o dispositivo, ele se conecta ao serviço FCM. Em seguida, 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 por Push.

Pré-requisitos

- Secure Hub cliente mais recente
- Credenciais de conta de desenvolvedor do Google
- Serviços do Google Play instalados em dispositivos Android habilitados para FCM

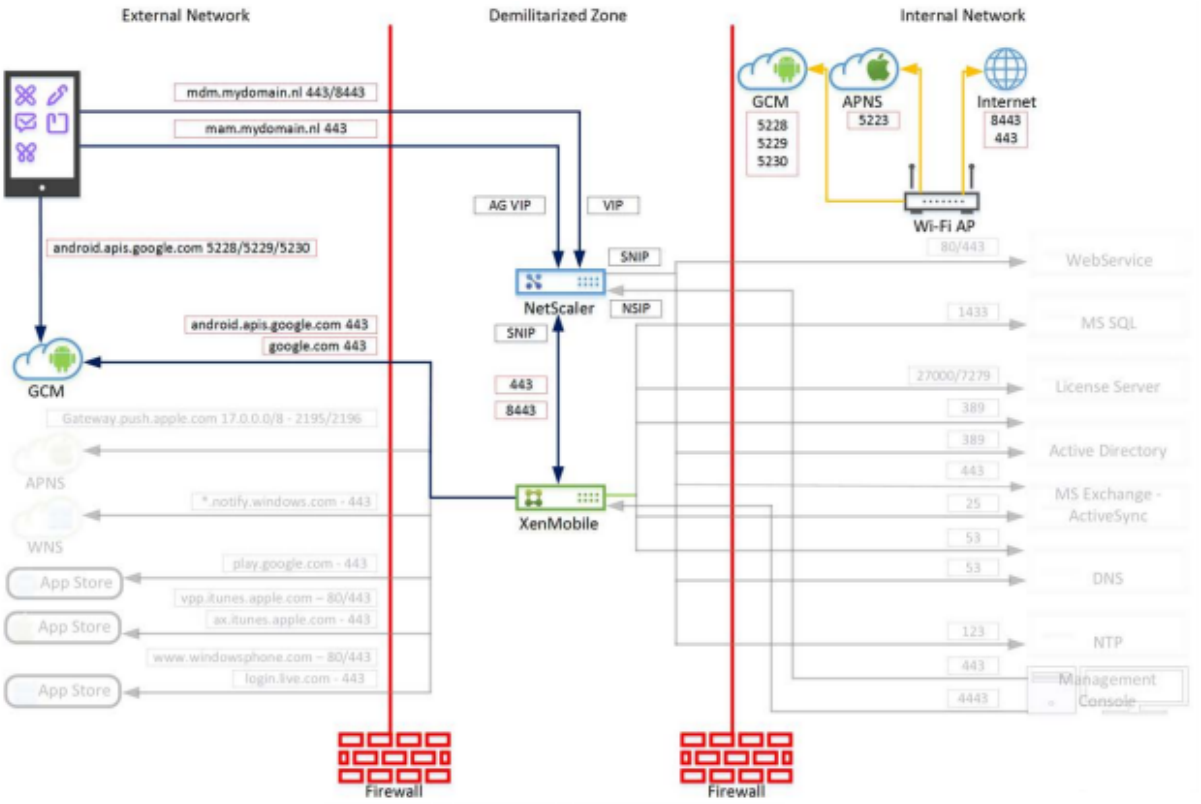
Portas de firewall

- Abra a porta 443 no XenMobile para `Android.apis.google.com` e `Google.com`.
- Abra as portas 5228, 5229 e 5230 para mensagens recebidas.
- Para permitir conexões de saída, o FCM recomenda a inclusão das portas de 5228 a 5230 na lista branca sem restrições de IP. No entanto, se você precisar de restrições de IP, o FCM recomenda colocar na lista branca todos os endereços IP nos blocos IPv4 e IPv6 Esses blocos estão listados no Google ASN de 15169. Atualize essa lista mensalmente.

Arquitetura

Esse diagrama mostra o fluxo de comunicação do FCM nas redes externa e interna.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



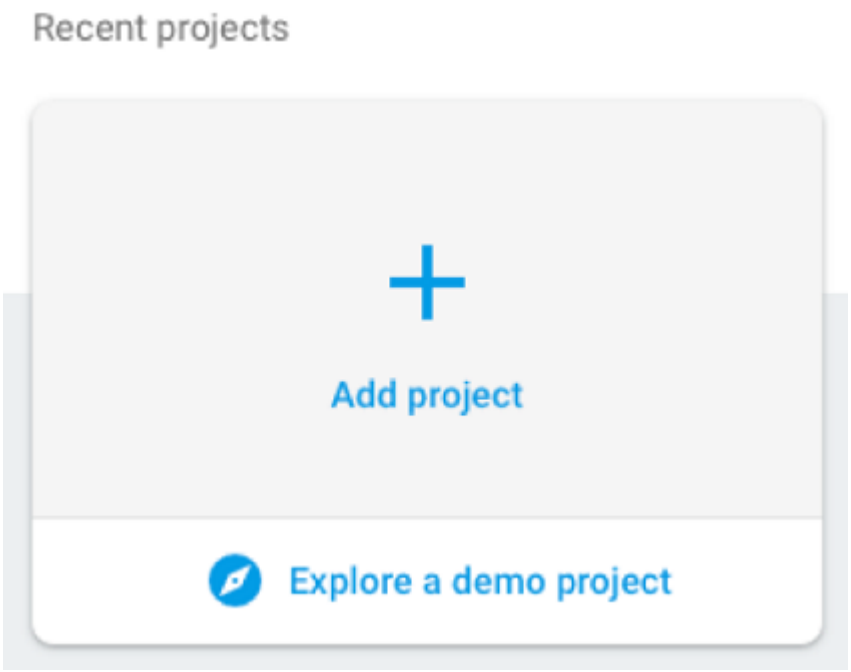
Para configurar sua conta do Google para GCM

1. Faça login na seguinte URL usando suas credenciais de conta de desenvolvedor do Google:

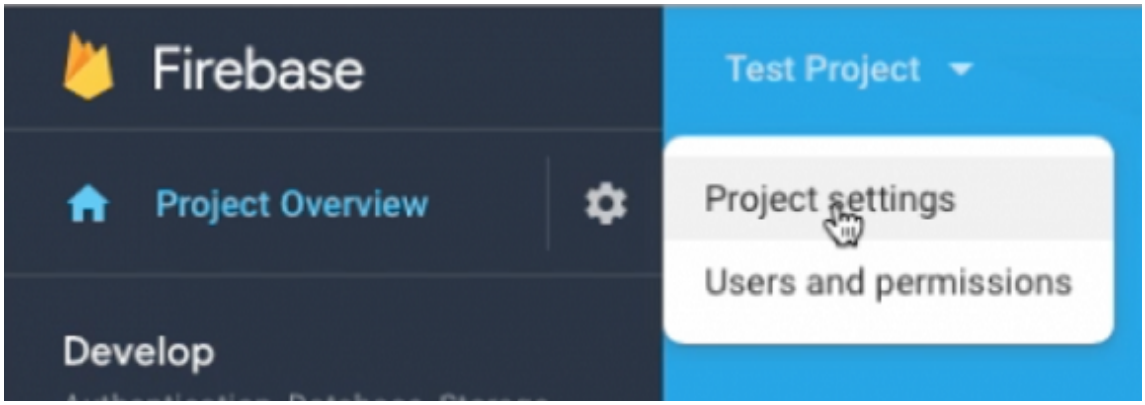
   https://console.firebase.google.com/

2. Clique em **Add project**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

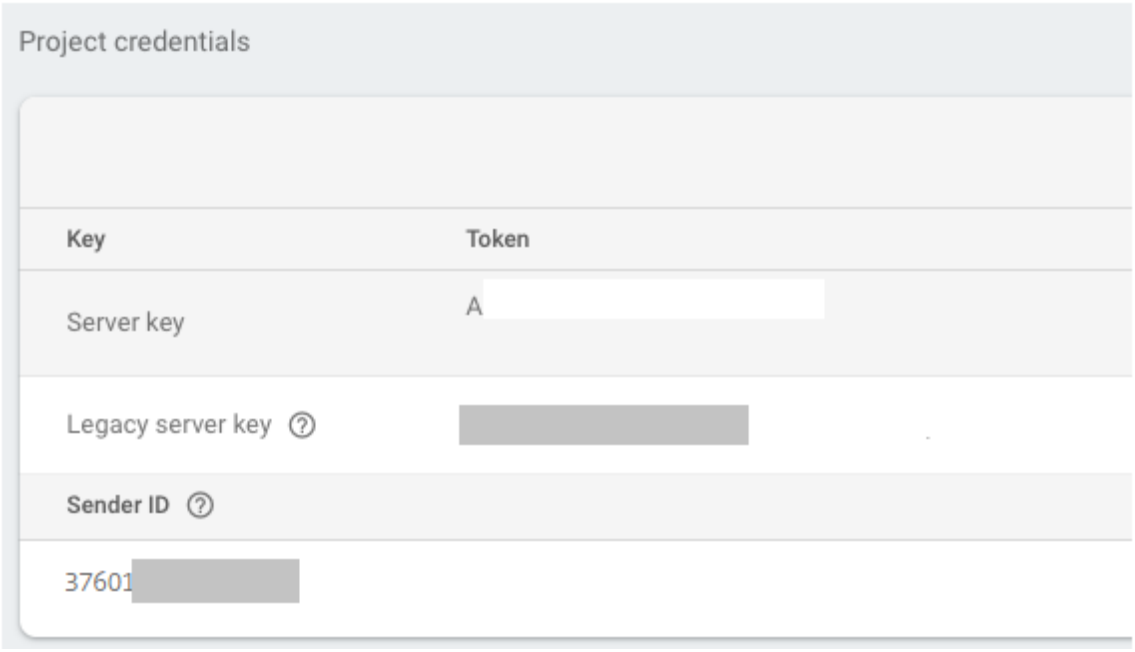


3. Depois de criar o projeto, clique em **Project settings**.



4. Clique na guia **Cloud Messaging**. Copie os valores de **Server key** e **Sender ID**. No próximo procedimento, você cola esses valores no console XenMobile Server. A partir de outubro de 2016, você deve criar chaves de servidor no console do Firebase.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

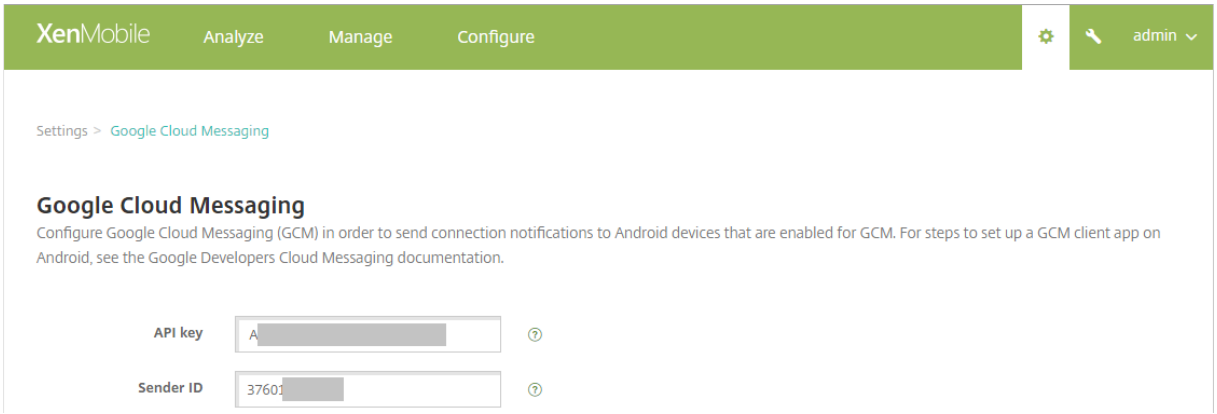


Para obter as etapas para configurar um aplicativo cliente FCM no Android, consulte este artigo do Google Developers Cloud Messaging: https://firebase.google.com/docs/cloud-messaging/android/client.

Para configurar o XenMobile para FCM

No console XenMobile, acesse **Configurações > Google Cloud Messaging**.

- Edite a **chave de API do GCM** e digite a **chave do servidor** do Firebase Cloud Messaging que você copiou na última etapa da configuração do Firebase Cloud Messaging.
- Edite o **ID do remetente do GCM** e digite o valor de **ID do remetente** copiado no procedimento anterior.

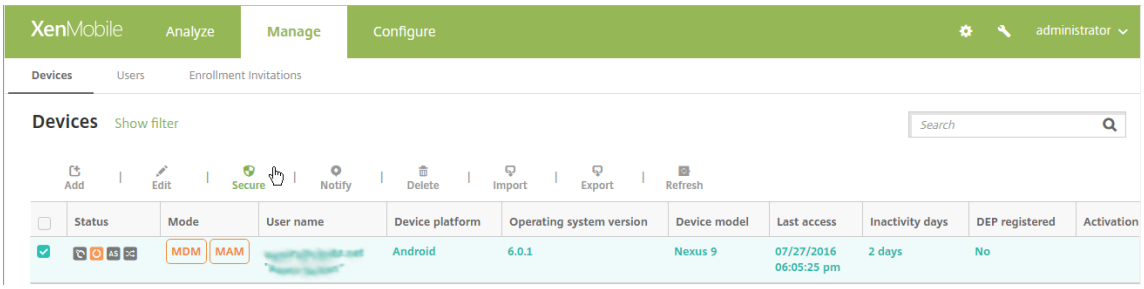


Depois de concluir a configuração, você pode remover a política de dispositivo Agendamento ou alterar essa política para se conectar com menos frequência.

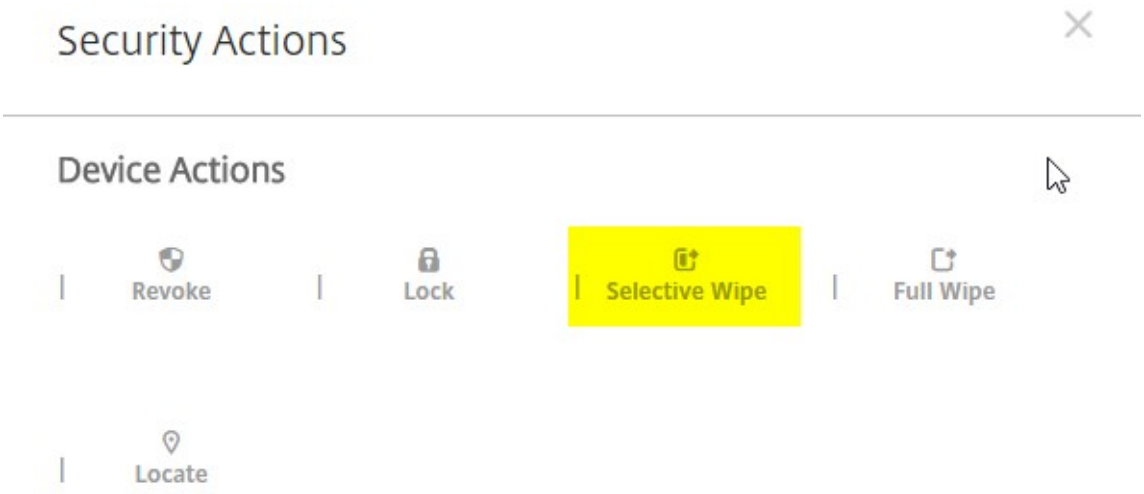
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para testar sua configuração

1. Registre um dispositivo Android.
2. Deixe o dispositivo ocioso por algum tempo, para que ele seja desconectado do XenMobile Server.
3. Faça login no console XenMobile, clique em **Gerenciar**, selecione o dispositivo Android e clique em **Segurança**.



4. Em **Ações do dispositivo**, clique em **Apagamento seletivo**.



Em uma configuração bem-sucedida, o apagamento seletivo ocorre no dispositivo.

Credenciais do Google Play

March 6, 2019

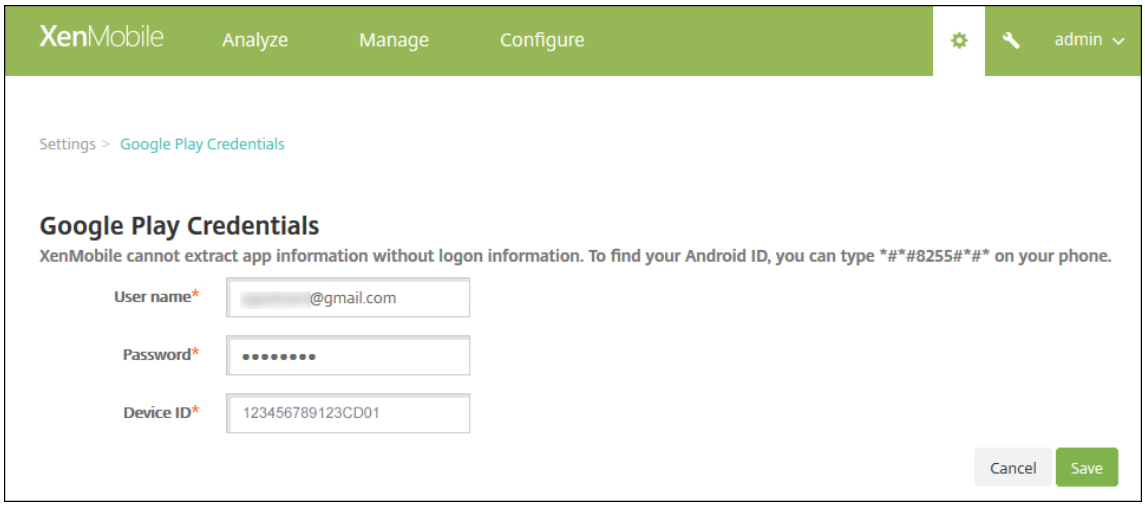
O XenMobile usa credenciais do Google Play para extrair informações do aplicativo do dispositivo.

Para localizar o seu ID do Android, digite ##8255## no seu telefone. Se o código não revelar a ID de dispositivo no seu tipo de dispositivo, talvez seja possível usar um aplicativo de terceiro para obter a ID do dispositivo. A ID a ser obtida é a ID do Google Services Framework com o rótulo GSF ID.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Durante a pesquisa de aplicativos no Google Play Store no console XenMobile, a pesquisa retorna aplicativos com base no sistema operacional Android no dispositivo registrado. Por exemplo, uma borda do Samsung S6 está executando uma versão de sistema operacional 6.0.1. Quando você pesquisa de aplicativos, somente os aplicativos que são exibidos no resultado da pesquisa são aplicativos que são compatíveis com Android versão 6.0.1.
>
> Para ativar o XenMobile para extrair informações do aplicativo, talvez você precise configurar a sua conta do Gmail para permitir conexões não seguras. Para obter instruções, consulte o site de suporte do Google.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Plataformas**, clique em **Credenciais do Google Play**. A página Credenciais do Google Play é exibida.



3. Defina essas configurações e clique em **Salvar**.
   - **Nome de usuário:** digite o nome associado à conta do Google Play.
   - **Senha:** digite a senha de usuário.
   - **ID do dispositivo:** digite o seu ID do Android.

   Veja a nota anterior no artigopara conhecer os procedimentossobre como obter o ID do Android.

Integração com os recursos do Apple Educação

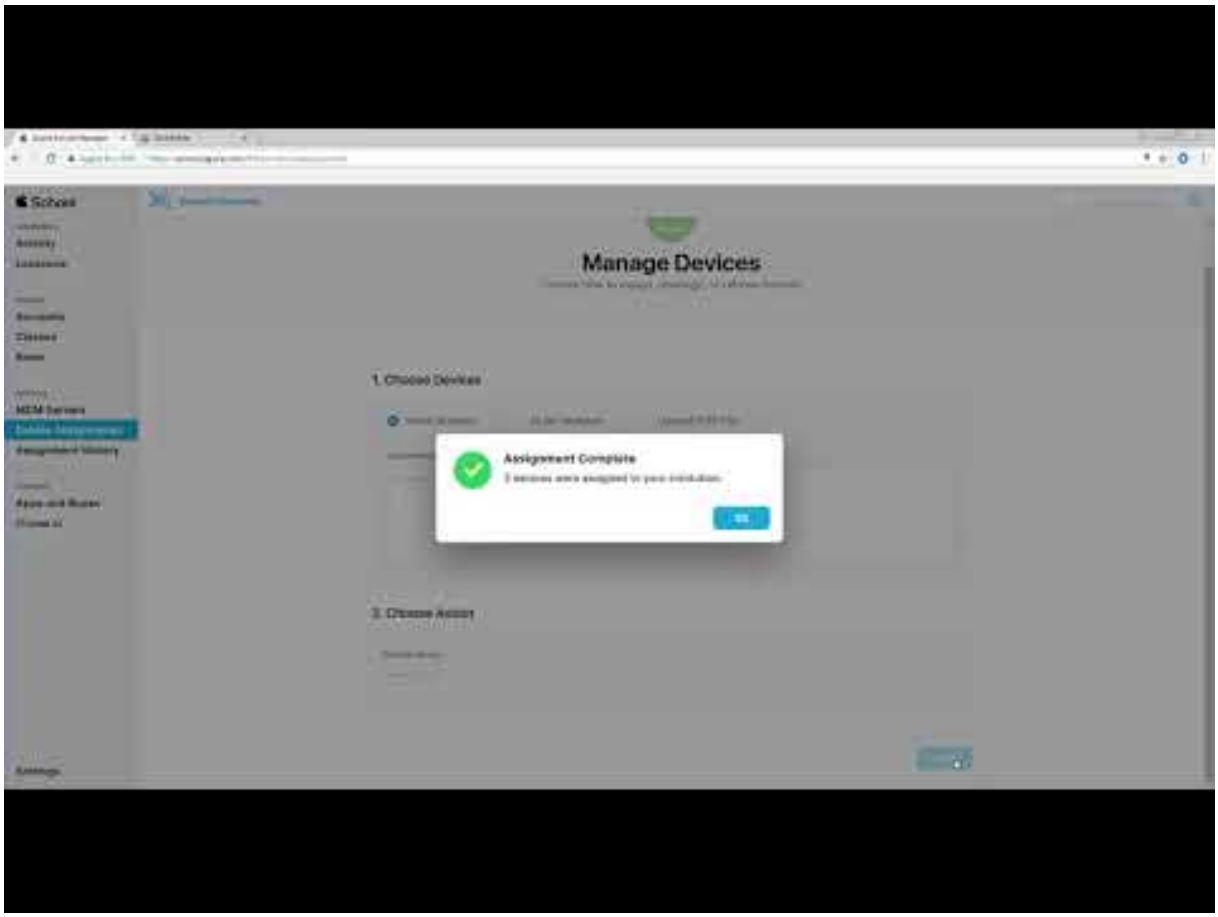
April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Você pode usar o XenMobile Server como sua solução de gerenciamento de dispositivos móveis (MDM) em um ambiente que usa o Apple Educação. O XenMobile suporta os aprimoramentos do Apple Educação introduzidos no iOS 9.3, incluindo o Apple School Manager e o aplicativo Classroom para iPad. A política de dispositivo de Configuração do XenMobile Education configura os dispositivos de instrutor e estudante para uso com o Apple Educação.

Você fornece iPads pré-configurados e supervisionados para instrutores e alunos. Essa configuração inclui a inscrição do DEP do Apple School Manager no XenMobile, uma conta do ID Apple gerenciado configurada com uma nova senha e os aplicativos VPP e iBooks necessários.

O seguinte vídeo fornece um tour rápido das alterações feitas ao Apple School Manager e ao XenMobile Server.



Aqui estão os destaques do suporte do XenMobile para os recursos do Apple Educação.

Apple School Manager

O Apple School Manager é um serviço que permite configurar, implantar e gerenciar dispositivos iOS e laptops macOS utilizados em instituições educacionais. O Apple School Manager inclui um portal baseado na web que permite aos administradores de TI:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Atribua os dispositivos DEP a diferentes servidores MDM.
- Comprar licenças de VPP para aplicativos e iBooks
- Crie **IDs Apple gerenciados** em massa. Esses IDs Apple personalizados fornecem acesso aos serviços da Apple, como armazenar documentos no iCloud Drive e registrar-se em cursos iTunes.

O Apple School Manager é um tipo de DEP de Educação. O XenMobile é compatível com a inscrição ao Business DEP e Apple School Manager.

Você pode adicionar várias contas do DEP do Apple School Manager ao XenMobile Server. Por exemplo, este recurso permite usar diversas configurações de registro e opções de Assistente de Configuração por departamento ou unidade Educação. Em seguida, você associa contas do DEP a diferentes políticas de dispositivo.

Depois de adicionar uma conta do DEP do Apple School Manager ao console XenMobile, o XenMobile recupera as informações da aula e da lista. Durante a configuração do dispositivo, o XenMobile Server:

- Registra os dispositivos.
- Instala os recursos que você configurou para a implantação, como as políticas de dispositivo (Configuração de Educação, layout da tela inicial e assim por diante). Também instala aplicativos e iBooks comprados via VPP.

Você fornece dispositivos pré-configurados e supervisionados para instrutores e alunos. Se um dispositivo for perdido ou roubado, você pode usar o recurso de modo Perdido do MDM para bloquear e localizar dispositivos.

Aplicativo Sala de Aula para iPad

O aplicativo Sala de Aula para iPad permite que os instrutores se conectem e gerenciem os dispositivos dos alunos. Você pode visualizar as telas do dispositivo, abrir aplicativos em iPads, compartilhar e abrir links da web e apresentar uma tela de estudante na Apple TV.

O Sala de Aula é gratuito na App Store. Você carrega os arquivos para o console XenMobile. Em seguida, você usa a política do dispositivo Configuração de Educação para configurar o aplicativo Sala de Aula, que você implementa nos dispositivos dos instrutores.

Para obter mais informações sobre os recursos do Apple Educação, consulte o site Apple Education e o Education Deployment Guide da Apple.

Pré-requisitos

- NetScaler Gateway

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- XenMobile Server configurado no modo Empresarial (XME, também chamado MDM+MAM) ou no modo MDM. Se você já tem um XenMobile Server configurado no modo XME ou MDM, você pode usá-lo com o Apple School Manager.
- Apple iPad 3ª geração (versão mínima) ou iPad Mini, com iOS 9.3 (versão mínima)

Notas:

- Atualmente, o XenMobile suporta o modelo one-to-one da Apple Education. Você pode atribuir um iPad a apenas um usuário do Apple School Manager.
- O XenMobile Server não valida as contas de usuários do Apple School Manager com relação ao LDAP ou ao Active Directory. No entanto, você pode conectar o XenMobile Server ao LDAP ou ao Active Directory para gerenciamento de usuários e dispositivos não relacionados aos instrutores ou alunos do Apple School Manager. Por exemplo, você pode usar o Active Directory para fornecer o Secure Mail e Secure Web para outros membros do Apple School Manager, como administradores de TI e gerentes.
- Como os instrutores e estudantes do Apple School Manager são usuários locais, não é necessário implantar o Citrix Secure Hub em seus dispositivos.
- A inscrição da MAM que inclui a autenticação do NetScaler Gateway não é compatível com usuários locais (apenas usuários do Active Directory). Portanto, o XenMobile implanta apenas aplicativos VPP e iBooks necessários para os dispositivos dos instrutores e dos estudantes.

Configurar o Apple School Manager e o XenMobile Server

Depois de comprar iPads da Apple ou de Revendedores ou operadoras autorizadas da Apple: siga o fluxo de trabalho nesta seção para configurar sua conta do Apple School Manager e seus dispositivos. Este fluxo de trabalho inclui etapas que você executa no portal Apple School Manager e no console XenMobile.

Etapa 1: Crie sua conta do Apple School Manager e siga o Assistente de Configuração

Se você planeja atualizar os programas de implantação da Apple, consulte o artigo de suporte da Apple Prepare to upgrade to Apple School Manager. Para criar sua conta do Apple School Manager, acesse https://school.apple.com/ e siga as instruções para se registrar. Na primeira vez que você efetua login no Apple School Manager, o Assistente de Configuração é aberto.

- Para obter informações sobre os pré-requisitos do Apple School Manager, o Assistente de Configuração e as tarefas de gerenciamento, consulte a Ajuda do Apple School Manager.
- Ao configurar um Apple School Manager, use um nome de domínio diferente do nome de domínio do Active Directory. Por exemplo, prefixe o nome de domínio do Apple School Manager com algo como **idapple**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Quando você conecta o Apple School Manager aos dados na sua lista, o Apple School Manager cria IDs Apple gerenciados para instrutores e alunos. Os seus dados de listagem incluem instrutores, alunos e aulas. Para obter informações sobre como adicionar dados de lista para o Apple School Manager, consulte os artigos em "Encontrar equipes, alunos e aulas" na ajuda do Ajuda do Apple School Manager.
- Você pode personalizar o formato do ID Apple gerenciado para sua instituição, como descrito em "IDs Apple gerenciados" na Ajuda do Apple School Manager.

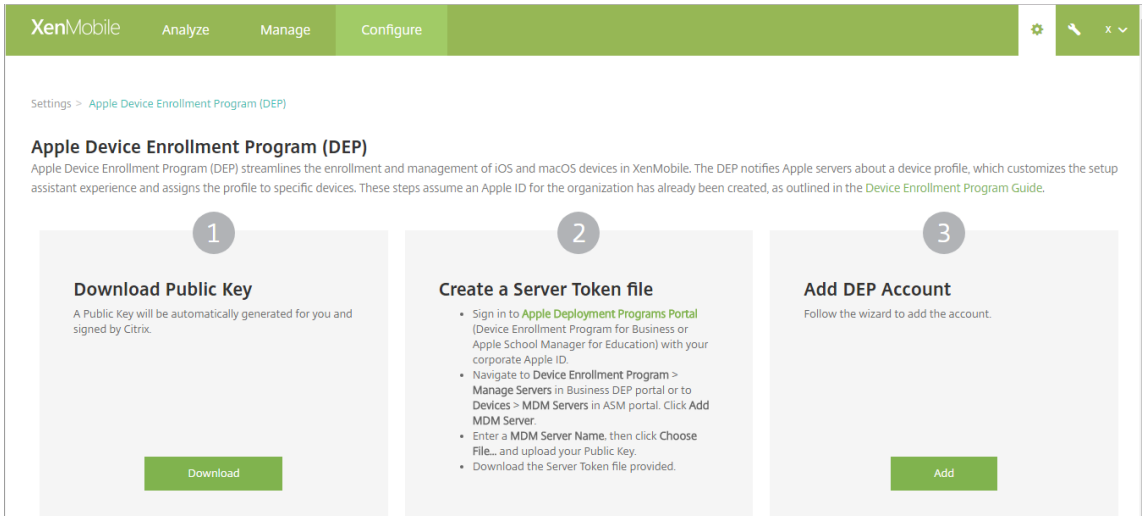
  > Importante:
  >
  > Não altere IDs Apple gerenciados depois de importar informações do Apple School Manager para o XenMobile Server.

- Se você comprou dispositivos através de revendedores ou operadoras, faça a ligação desses dispositivos ao Apple School Manager. Para obter informações, consulte os artigos em "Gerenciar dispositivos" na Ajuda do Apple School Manager.

Etapa 2: Configure o XenMobile Server como o servidor MDM para o Apple School Manager e configure as atribuições do dispositivo

O portal Apple School Manager inclui uma guia de **Servidores MDM**. Você precisa do arquivo de chave pública do XenMobile Server para concluir a configuração.

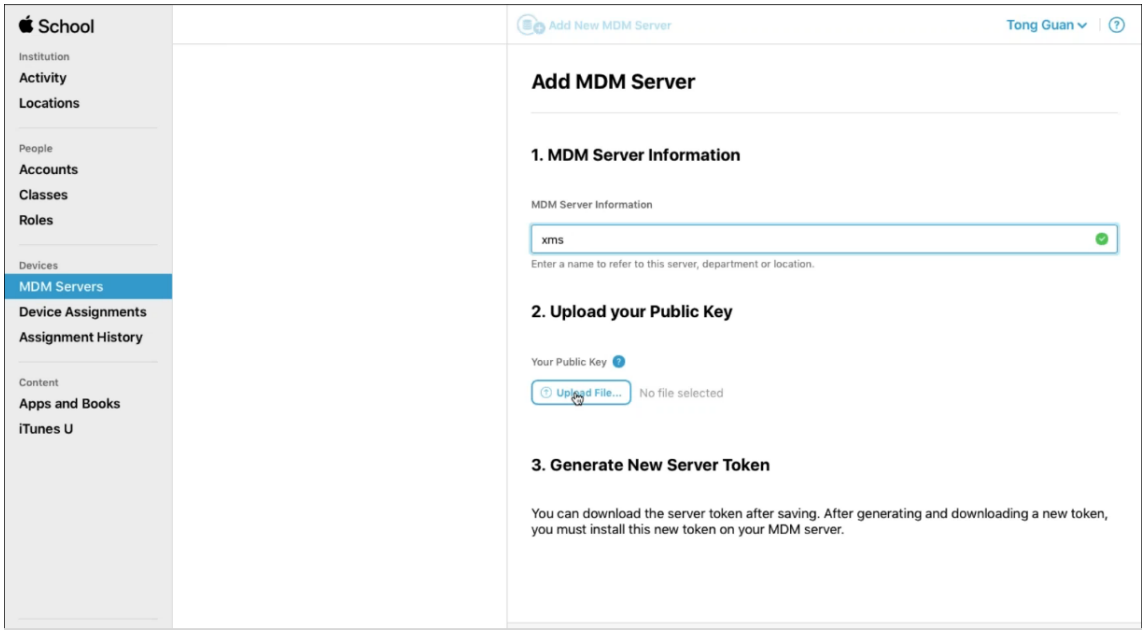
1. Baixe a chave pública do seu XenMobile Server para o seu computador local: faça logon no console XenMobile e vá para **Configurações > Programa de registro de dispositivo Apple (DEP)**.



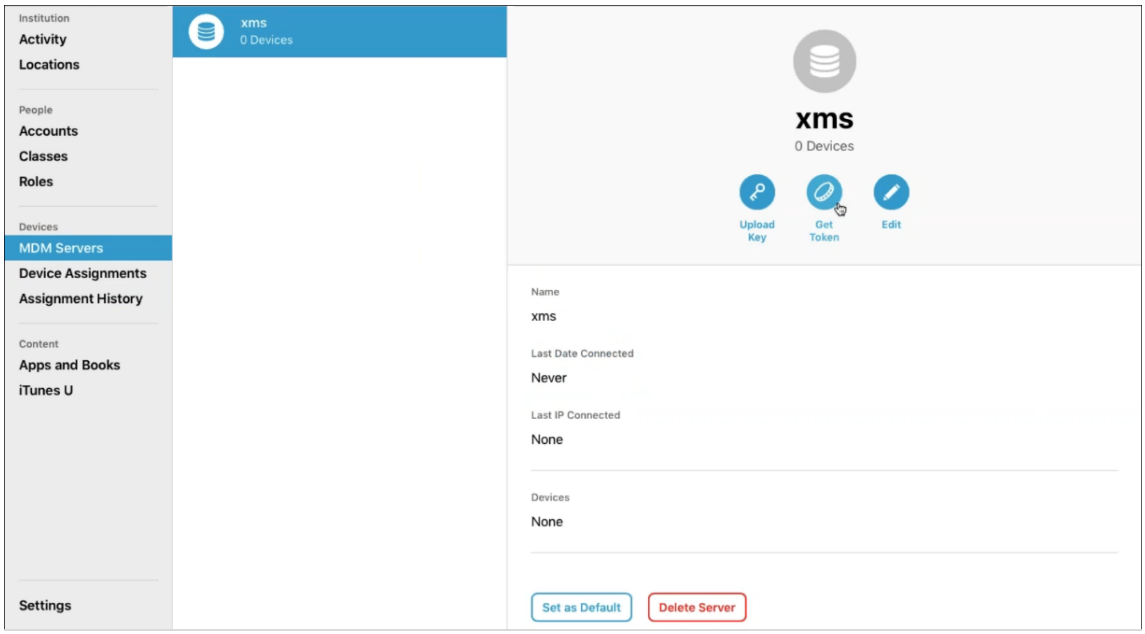
2. Em **Baixar chave pública**, clique em **Baixar** e salve o arquivo PEM.
3. No portal do Apple School Manager, clique em **MDM Servers** e digite um nome para o XenMobile Server. O nome do servidor que você digita é para sua referência e não é a URL ou o nome do servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Em **Upload your Public Key**, clique em **Upload File**.



5. Carregue a chave do servidor que você baixou do XenMobile Server e clique em **Save**.
6. Gerar um token de servidor: clique em **Get Token** e, em seguida, baixe o arquivo de token do servidor para o seu computador.



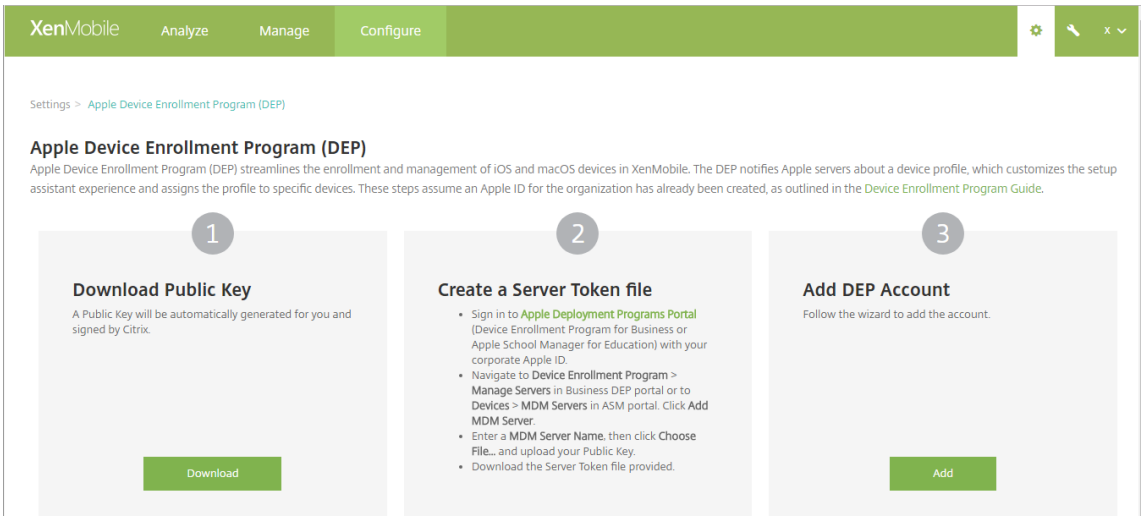
7. Clique em **Device Assignments**, escolha como deseja atribuir dispositivos e, em seguida, forneça as informações solicitadas. Para obter informações, consulte a seção “Assign devices” na Ajuda do Apple School Manager.
8. Em **Choose Action**, no menu **Perform Action**, clique em **Assign to Server**. No menu **MDM**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

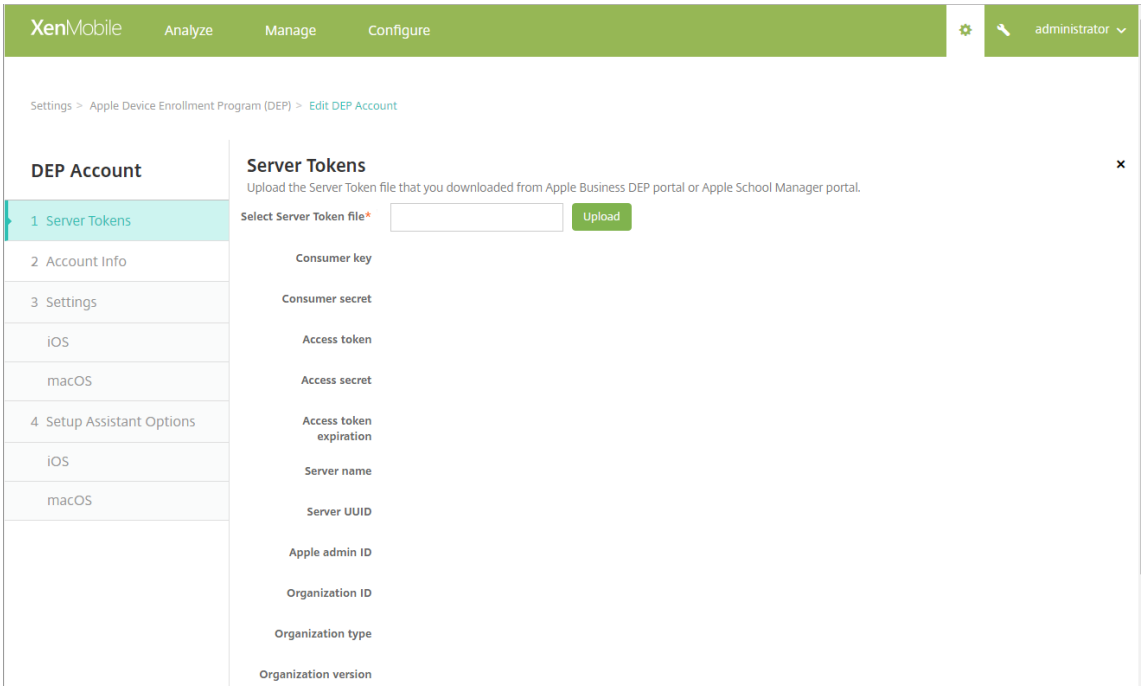
Server, clique em XenMobile Server para gerenciar os dispositivos e, em seguida, clique em **Done**.

Etapa 3: Adicione a conta do Apple School Manager ao XenMobile Server

1. No console XenMobile, vá para **Configurações > Apple Device Enrollment Program (DEP)** e, em **Adicionar conta do DEP**, clique em **Adicionar**.



2. Na página **Tokens de servidor**, clique em **Carregar** e escolha o arquivo de token do servidor (.p7m) que você baixou do portal do Apple School Manager. As informações do token são exibidas.

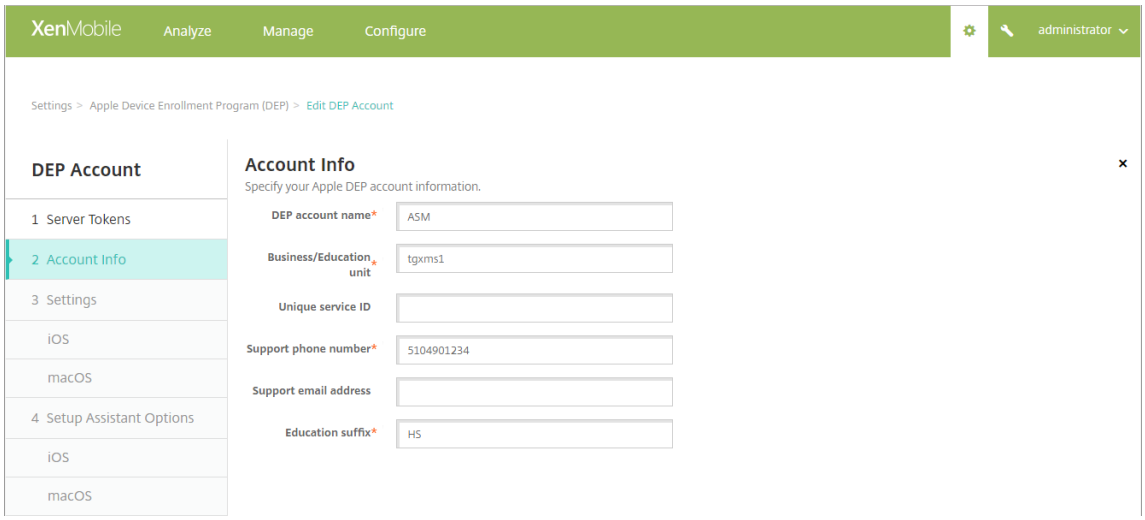


© 1999-2019 Citrix Systems, Inc. All rights reserved.

Notas:

- **ID da organização** é o seu ID de cliente do DEP.
- As contas do Apple School Manager possuem um **Tipo de organização** de **Educação** e uma **Versão da organização** de **v2**.

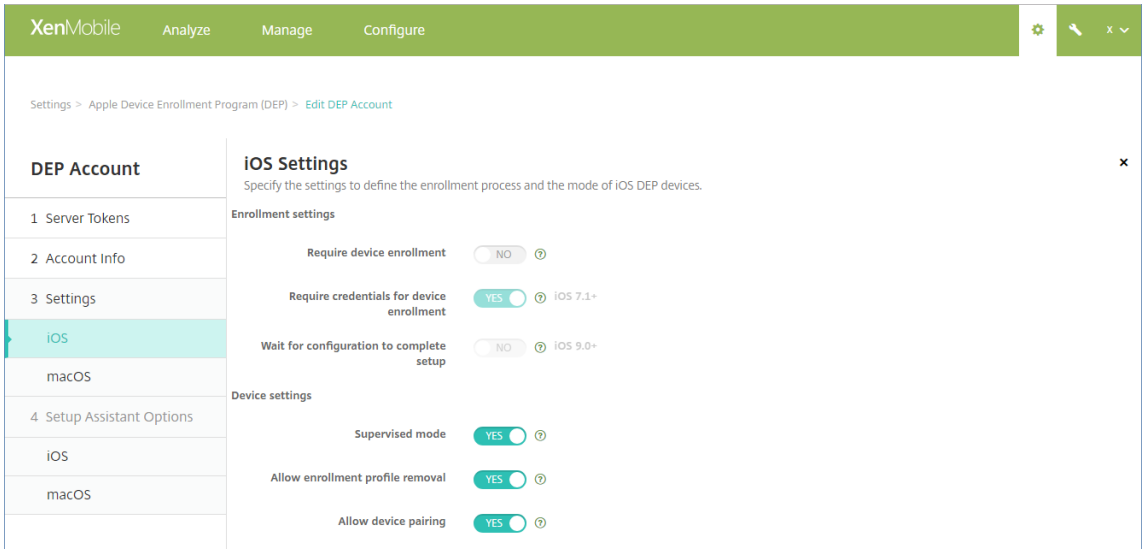
3. Na página **Informações sobre a conta**, especifique as seguintes configurações.



- **Nome de conta do DEP:** um nome exclusivo para essa conta do DEP. Use nomes que reflitam como organizar contas do DEP, como por país ou hierarquia organizacional.
- **Unidade de negócios/educação:** a unidade ou departamento de Educação para a atribuição de dispositivos. Este campo é obrigatório.
- **ID de serviço exclusiva:** um ID exclusivo opcional para ajudar você 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 pedir ajuda durante a instalação. Este campo é obrigatório.
- **Endereço de email de suporte:** um endereço de email de suporte opcional, disponível para os usuários finais.
- **Sufixo de educação:** sinaliza as classes de uma determinada conta DEP do Apple School Manager. (O sufixo VPP sinaliza aplicativos e iBooks de uma determinada conta VPP.) A recomendação é usar o mesmo sufixo para ambas as contas: Apple School Manager DEP e Apple School Manager VPP.

4. Clique em **Avançar**. Em **Configurações do iOS**, especifique as seguintes configurações.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Configurações de registro**
  - **Exigir registro de dispositivo:** solicite que os usuários registrem seus dispositivos. Altere essa configuração para **Não**.
  - **Exigir credenciais para registro de dispositivo:** selecione se os usuários são obrigados a inserir as respectivas credenciais durante a configuração do DEP. Para a integração do Apple School Manager com o XenMobile Server, esta configuração é **Sim** por padrão.
  - **Aguardar que a configuração conclua a instalação:** selecione se os dispositivos do usuário devem ser obrigados a permanecer no modo do Assistente de instalação até que todos os recursos do MDM sejam implantados no dispositivo. Para a integração do Apple School Manager com o XenMobile Server, esta configuração é **Não** por padrão. De acordo com a documentação da Apple, os seguintes comandos poderão não funcionar enquanto o dispositivo estiver no modo Assistente de Instalação:
    * InviteToProgram
    * InstallApplication
    * InstallMedia
    * ApplyRedemptionCode
- **Configurações do dispositivo**
  - **Modo supervisionado:** coloque os dispositivos iOS no modo supervisionado. Não altere o padrão, **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:** na integração do Apple School Manager, permita que o usuário remova o perfil de registro do dispositivo. Altere essa configuração

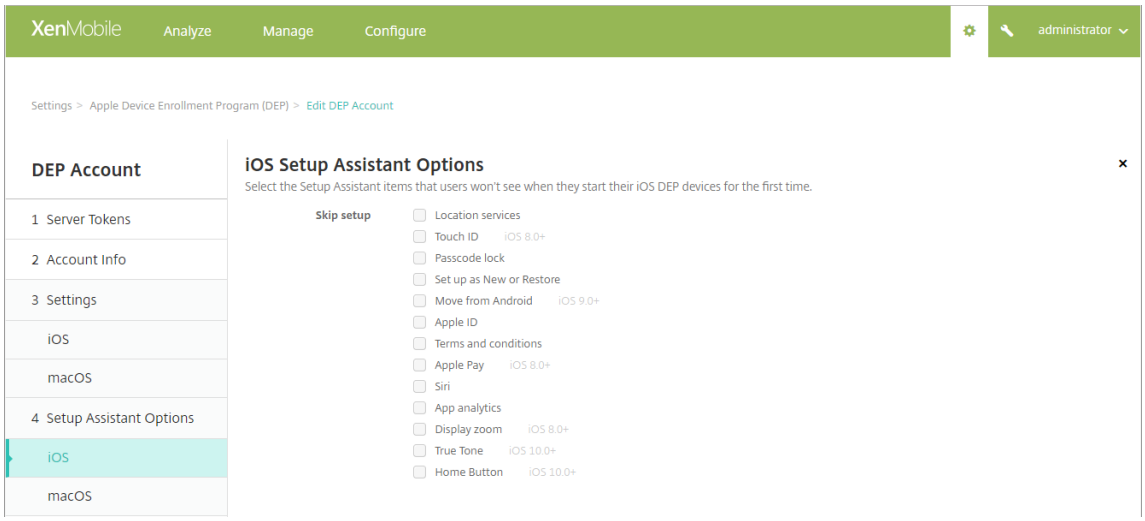
© 1999-2019 Citrix Systems, Inc. All rights reserved.

para **Sim**.

- **Permitir o emparelhamento de dispositivos:** na integração do Apple School Manager, permita o emparelhamento de dispositivos para que você possa gerenciá-los através do iTunes e do Apple Configurator. Altere essa configuração para **Sim**.

5. Em **Opções do assistente de instalação do iOS**, selecione as etapas do Assistente de instalação do iOS que serão ignoradas quando os usuários iniciarem seus dispositivos pela primeira vez. Por padrão, o Assistente de instalação inclui todas as etapas. Considere que remover etapas do Assistente de Configuração simplifica a experiência do usuário.

> Importante:
>
> A Citrix recomenda que você inclua as etapas de **ID Apple** e **Termos e Condições**. Essas etapas permitem que os instrutores e os alunos forneçam suas novas senhas do ID Apple Gerenciado e aceitem os termos e condições exigidos.

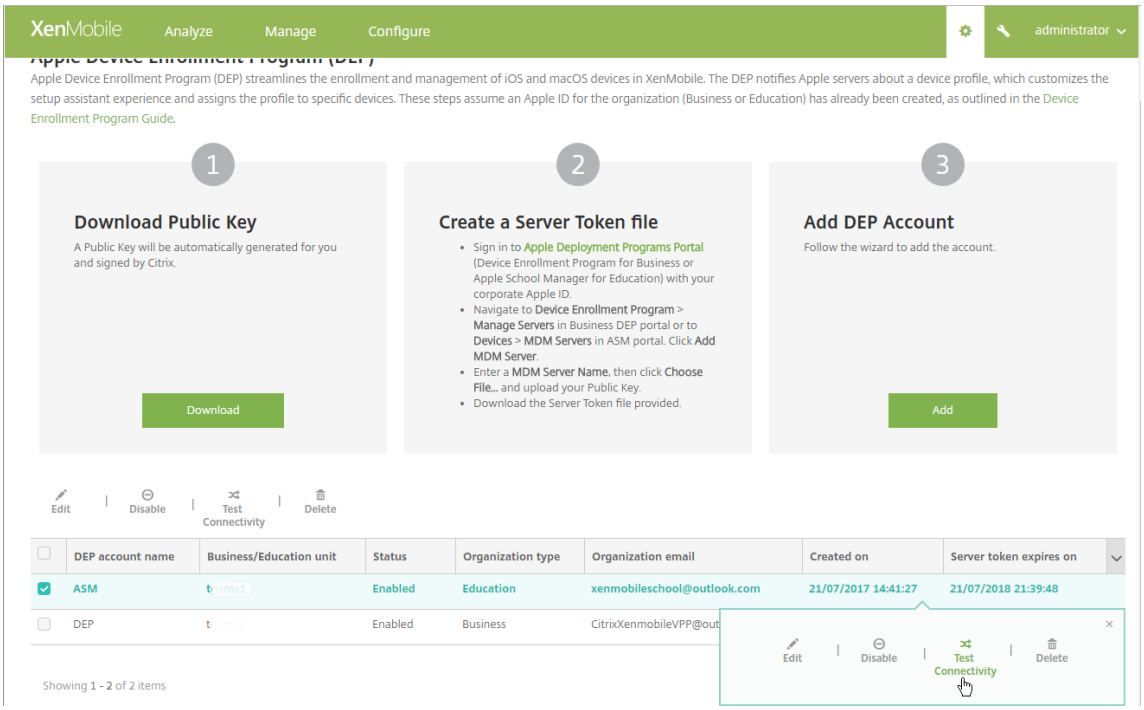


- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **Touch ID:** configurar o Touch ID nos dispositivos iOS 8.0 e versões posteriores.
- **Bloqueio de código secreto:** criar uma senha para o dispositivo.
- **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou iTunes.
- **Mover do Android:** permitir a transferência de dados de um dispositivo Android para um dispositivo iOS 9 ou versões posteriores. Essa opção está disponível somente quando **Configurar como novo ou restaurar** está selecionada (ou seja, a etapa é ignorada).
- **ID Apple:** configurar uma conta do ID Apple para o dispositivo. A Citrix recomenda que você marque a caixa de seleção para incluir esta etapa.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

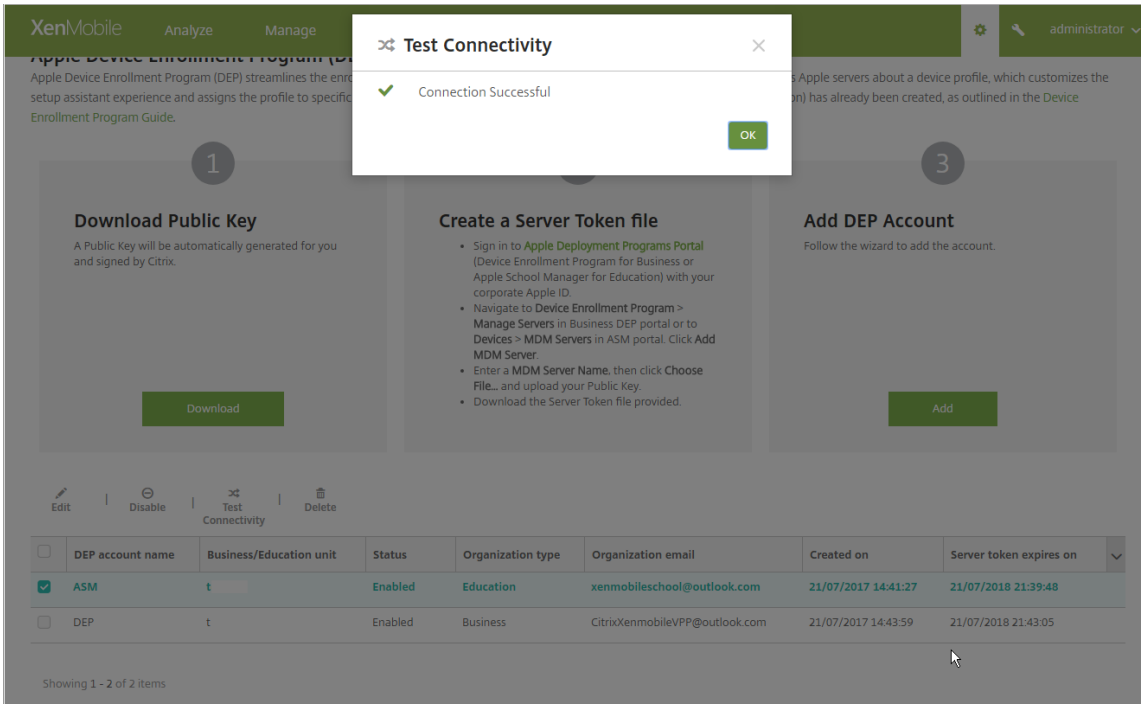
- **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo. A Citrix recomenda que você marque a caixa de seleção para incluir esta etapa.
- **Apple Pay:** configurar o Apple Pay nos dispositivos iOS 8.0 e versões posteriores.
- **Siri:** usar ou não a Siri no dispositivo.
- **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
- **Zoom de exibição:** configurar a resolução da tela (padrão ou ampliada) nos dispositivos iOS 8.0 ou versões posteriores.
- **True Tone:** configurar o True Tone Display nos dispositivos iOS 10.0 (versão mínima).
- **Botão Home:** configurea sensibilidade da tela do botão Home em dispositivos iOS 10.0 (versão mínima).

6. A conta do DEP é exibida em **Configurações > Apple Device Enrollment Program (DEP)**. Para testar a conectividade entre o XenMobile Server e a conta do Apple School Manager, selecione a conta e clique em **Testar conectividade**.

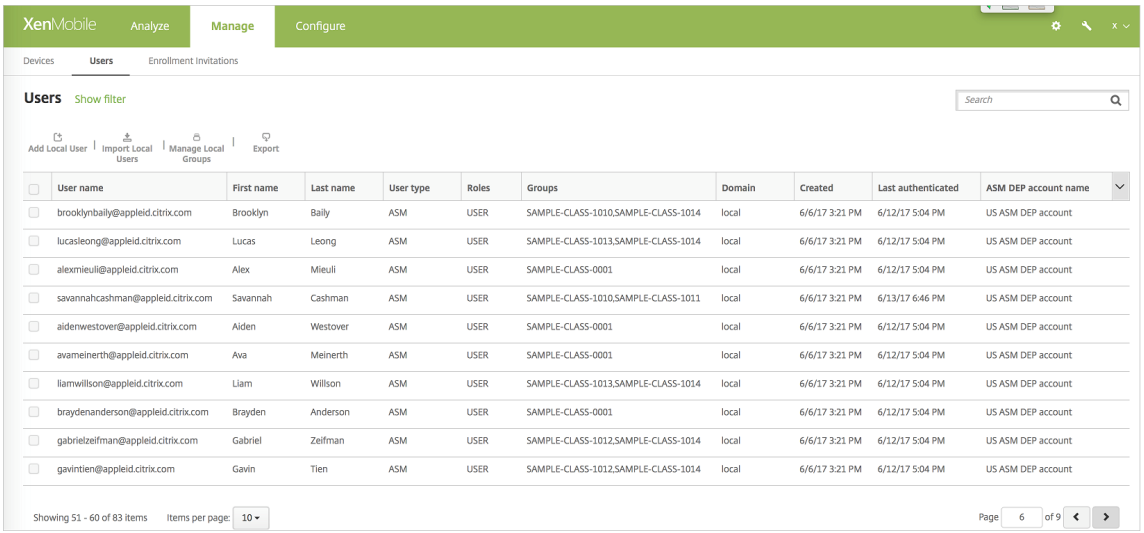


É exibida uma mensagem de status.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Após alguns minutos, as contas de usuários do Apple School Manager aparecem na página **Gerenciar > Usuários**. O XenMobile Server cria contas de usuário locais com base no ID Apple gerenciado importado para cada usuário. No exemplo a seguir, o prefixo de nome de domínio de IDs Apple personalizados para contas de usuário é **appleid**.



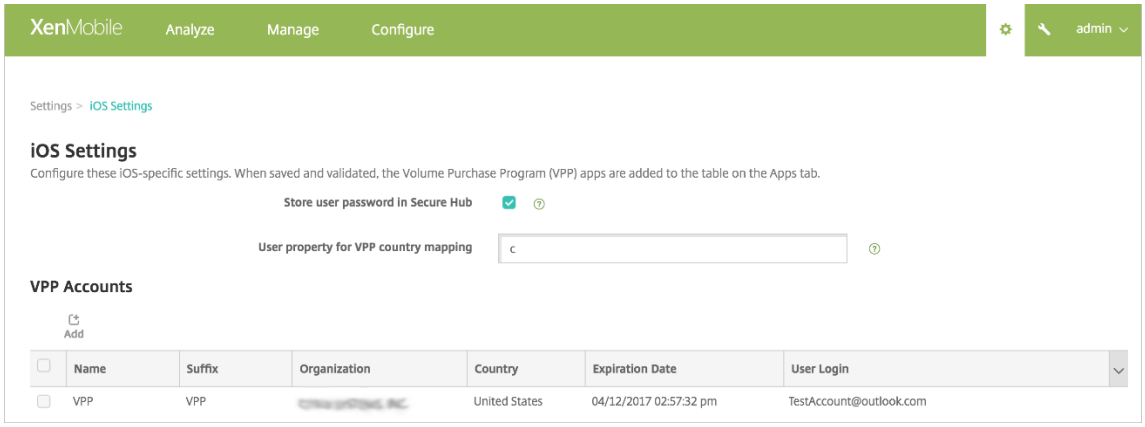
Para encontrar todos os usuários de uma determinada conta DEP do Apple School Manager, digite o nome da conta no filtro de pesquisa do usuário.

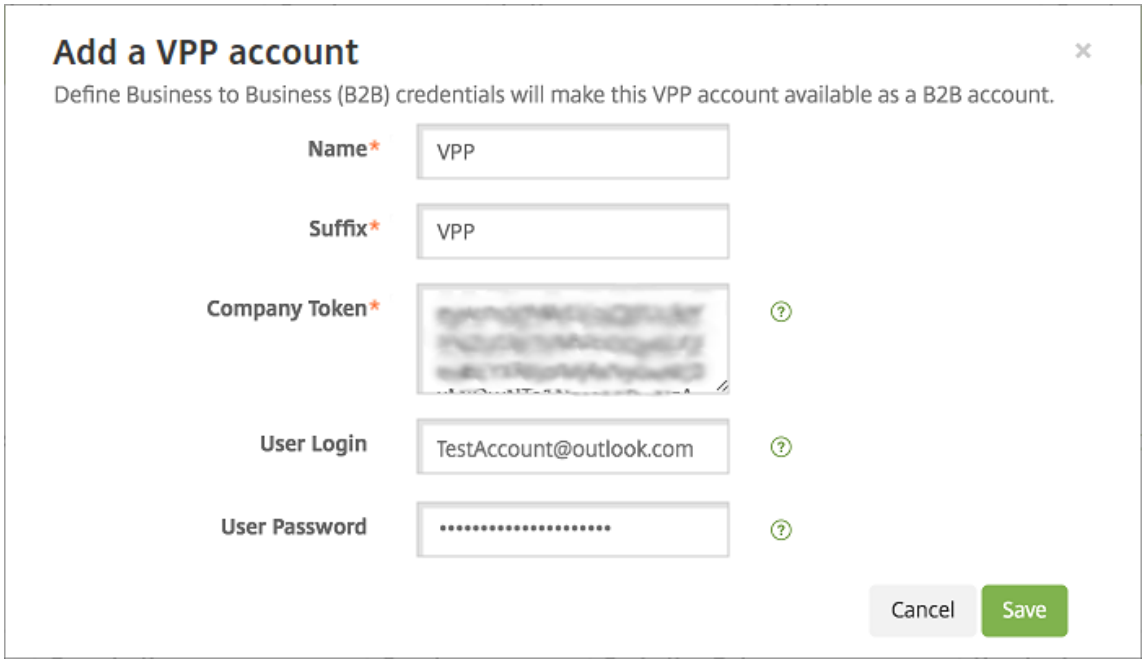
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Etapa 4: Configure uma conta VPP de Educação para o Apple School Manager

Nesta seção, aponte o XenMobile para a conta VPP que você usa para comprar licenças de VPP para aplicativos e iBooks.

1. Para configurar uma conta VPP de Educação para o Apple School Manager, siga as instruções no Programa de compra por volume do iOS. A tela Adicionar uma conta VPP requer que você forneça um Company Token. Baixe o token diretamente da sua conta VPP de Educação https://volume.itunes.apple.com/us/store e cole-o na tela **Adicionar uma conta VPP**.





2. Aguarde alguns minutos para as licenças VPP serem importadas para o XenMobile Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Etapa 5: Adicione senhas para usuários do Apple School Manager

Depois de adicionar uma conta DEP do Apple School Manager, o XenMobile Server importa classes e usuários do Apple School Manager. O XenMobile trata classes como grupos locais e usa o termo "grupo" no console. Se uma classe tiver um nome de grupo no Apple School Manager, 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 Apple School Manager não são exclusivos.

O XenMobile usa os IDs Apple gerenciados para criar usuários locais com o tipo de usuário **ASM**. Os usuários são locais porque o Apple School Manager 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 Apple School Manager não envia senhas de usuário temporárias para o XenMobile Server. Você pode importá-las de um arquivo CSV ou adicioná-las manualmente. Para importar senhas temporárias de usuários:

1. Obtenha o arquivo CSV gerado pelo Apple School Manager ao criar as senhas temporárias do ID Apple gerenciado.
2. Edite o arquivo CSV, substituindo as senhas temporárias por novas senhas que os usuários fornecem para se inscrever no XenMobile Server. Não há restrições no tipo de senha para este propósito.

   O formato de uma entrada no arquivo CSV é o seguinte: `elizabethabeles@appleid.citrix.com,Elizabeth,Anne,Abeles,Citrix123!`

   Onde:

   Usuário: `elizabethabeles@appleid.citrix.com`

   Nome: `Elizabeth`

   Segundo nome: `Anne`

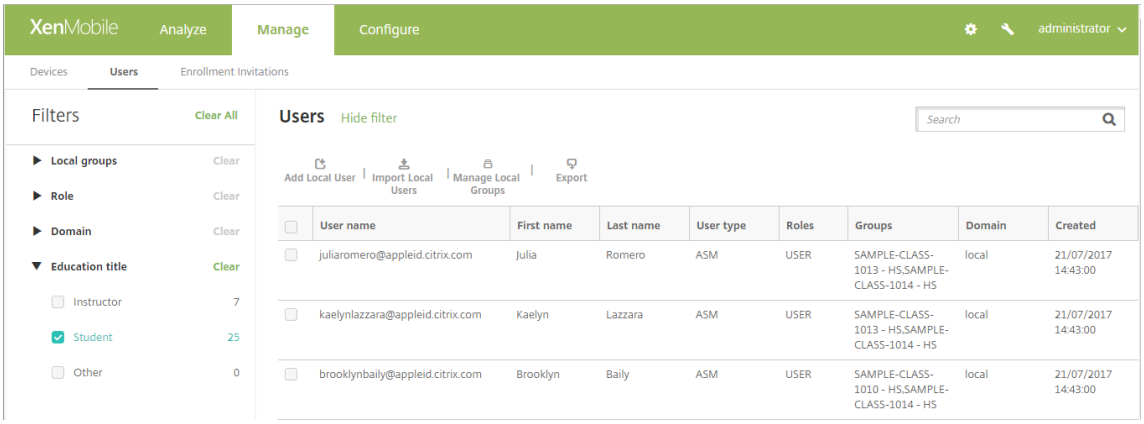
   Sobrenome: `Abeles`

   Senha: `Citrix123!`
3. No console XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.

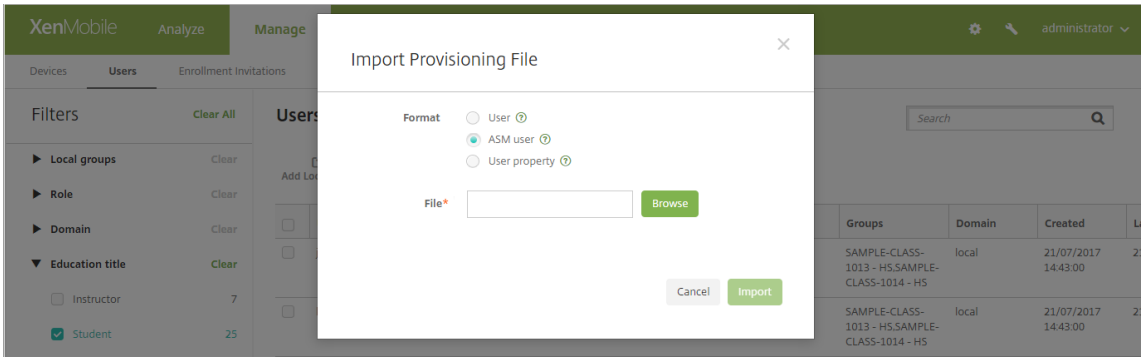
   O seguinte exemplo da tela **Gerenciar > Usuários** mostra uma lista de usuários importados do Apple School Manager. Na lista **Usuários**:

   - **Nome do usuário** mostra o ID Apple gerenciado.
   - O tipo de usuário é **ASM**, para indicar que a conta originou do Apple School Manager.
   - **Grupos** mostram as classes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

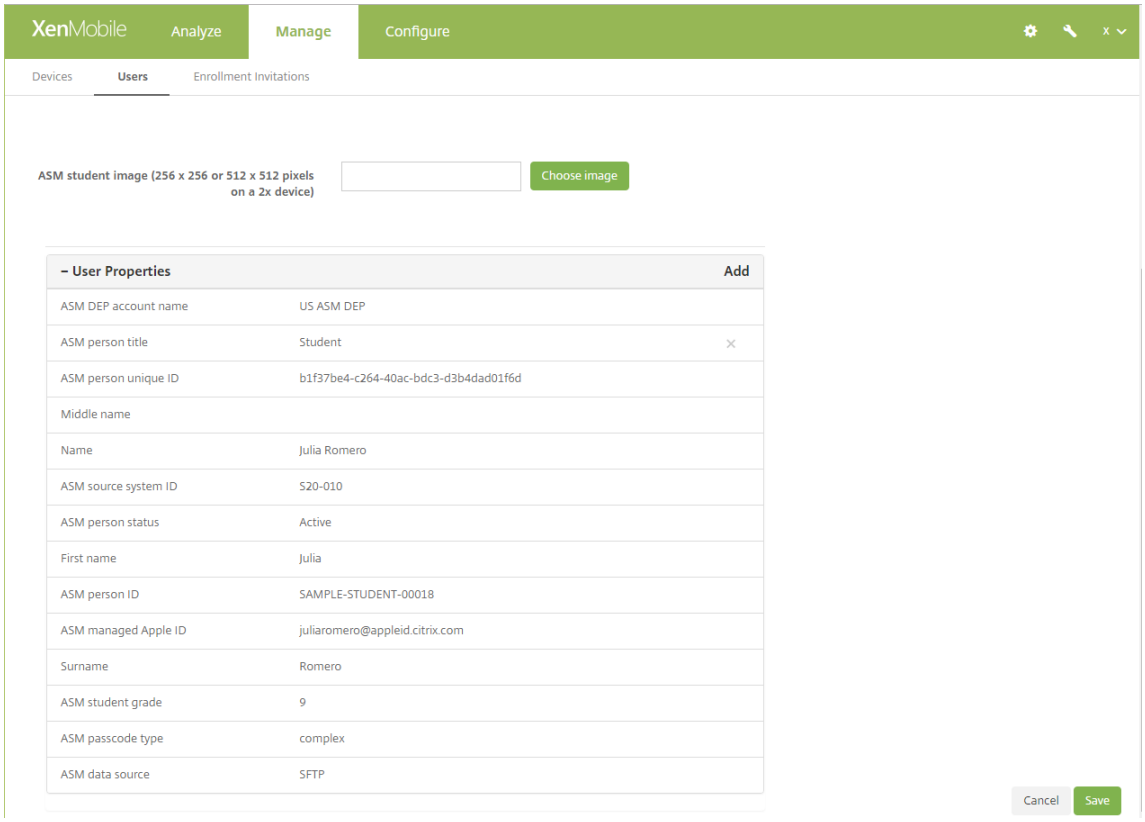


4. Clique em **Importar usuários locais**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.
5. Para Formato, escolha **Usuário ASM**, navegue até o arquivo CSV que você preparou na etapa 2 e clique em **Importar**.



6. Para exibir as propriedades de um usuário local, selecione o usuário e, em seguida, clique em **Editar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Além das propriedades do nome, estas propriedades do Apple School Manager aparecem:

- **Conta DEP ASM:** o nome que você deu à conta no XenMobile Server.
- **Título de pessoa no ASM:** o instrutor, aluno ou outro.
- **ID exclusivo da pessoa no ASM:** um identificador exclusivo para o usuário.
- **ID do sistema de origem ASM:** um identificador configurado pela sua organização para o usuário.
- **Status da pessoa no ASM:** especifica se o ID Apple gerenciado está **Ativo** ou **Inativo**. Esse status se torna ativo depois que o usuário fornece sua nova senha da conta do ID Apple gerenciado.
- **ID Apple gerenciado no ASM:** o ID Apple gerenciado pode incluir o nome da sua instituição e **appleid**. Por exemplo, o ID pode ser semelhante a johnapple-seed@appleid.myschool.edu. O XenMobile Server requer um ID Apple Gerenciado para autenticação.
- **Nível do aluno no ASM:** informações do nível do aluno (não utilizadas pelos instrutores).
- **Tipo de código secreto do ASM:** política de senha da pessoa: **complexa** (uma senha não estudantil de oito ou mais números e letras), **quatro** (dígitos) ou **seis** (dígitos).
- **Origem de dados ASM:** a origem dos dados da classe, como **CSV** ou **SFTP**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

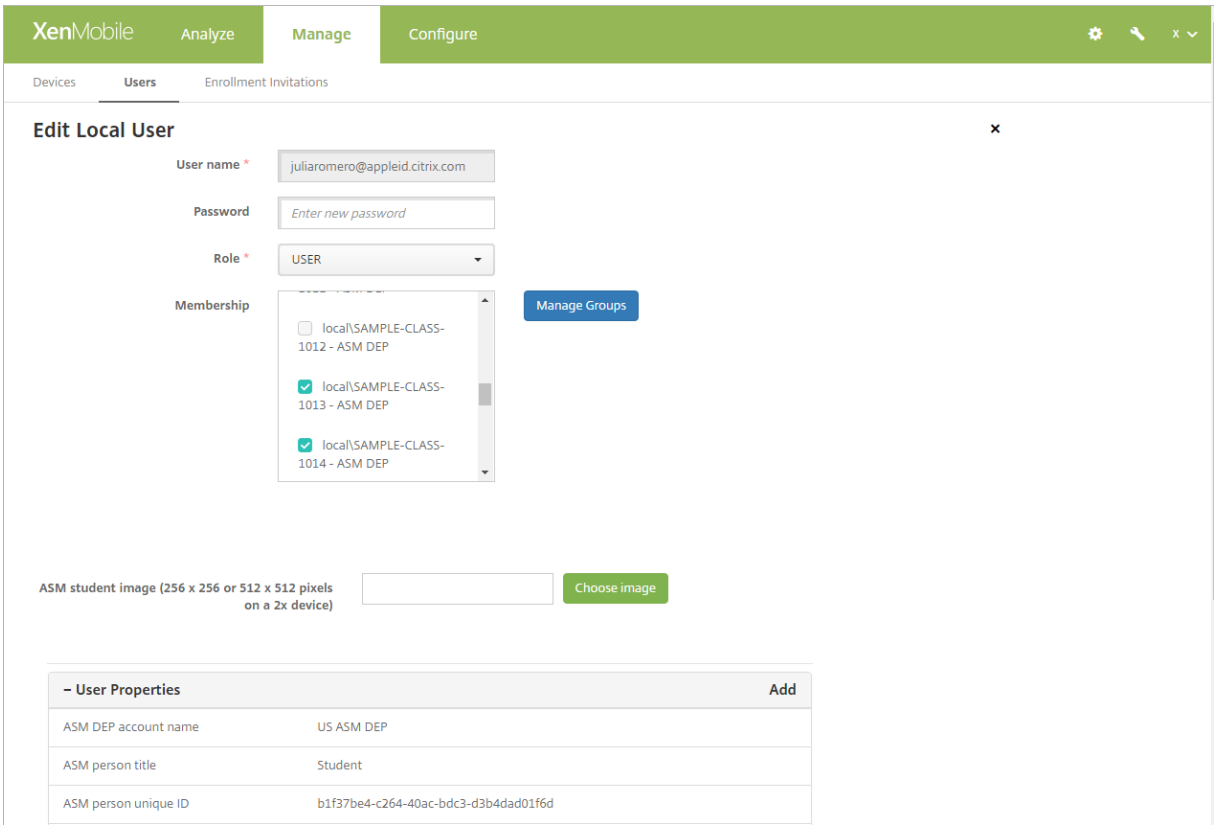
Etapa 6: Opcionalmente, adicione fotos de alunos

Você pode adicionar uma foto de cada aluno. Se os instrutores usam o aplicativo Apple Classroom, as fotos aparecem 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: Planeje e adicione recursos e grupos de entrega ao XenMobile Server

Um grupo de entrega especifica os recursos para implantar em 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 poder personalizar aplicativos, mídias e políticas enviadas para vários instrutores ou alunos. Você pode criar um ou mais grupos de entrega por aula. Você também pode criar um ou mais grupos de entrega para gerentes (outras equipes na sua instituição educacional).

Os recursos que você implementa nos dispositivos do usuário incluem políticas do dispositivo, aplicativos VPP e iBooks.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Políticas de dispositivo:

  Se os instrutores usam o aplicativo de Sala de Aula, é necessária a política do dispositivo Configuração de Educação. Lembre-se de revisar outras políticas de dispositivo para determinar como você deseja configurar e restringir iPadsd e alunos e instrutores.

- Aplicativos VPP:

  O XenMobile requer que você implante aplicativos VPP como aplicativos necessários para que os usuários de educação. O XenMobile Server atualmente não dá suporte à implantação desses aplicativos VPP como opcionais.

  Se você usa o aplicativo Apple Classroom, implemente-o apenas nos dispositivos de instrutores.

  Implemente quaisquer outros aplicativos que você queira fornecer aos instrutores ou alunos. Esta solução não usa o aplicativo Citrix Secure Hub, portanto, não há necessidade de implementá-lo para instrutores ou alunos.

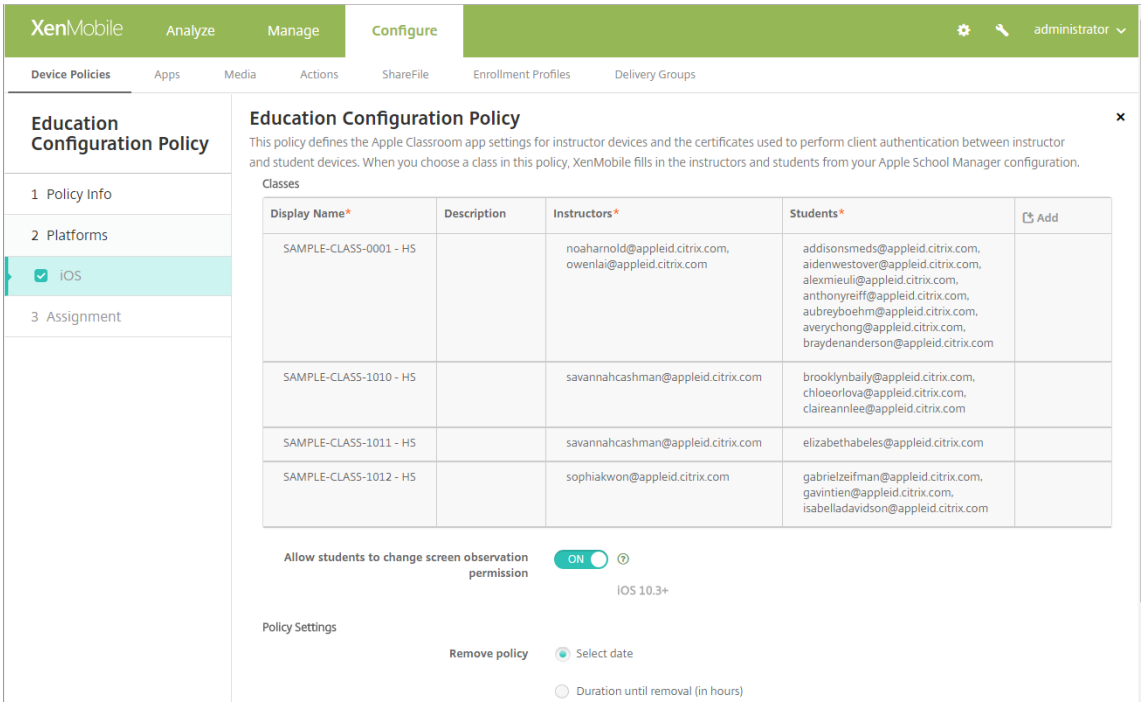
- iBooks VPP:

  Depois que o XenMobile Server se conecta à sua conta VPP do Apple School Manager, seus iBooks adquiridos aparecem no console XenMobile, em **Configurar > Mídia**. Os iBooks listados nessa página estão disponíveis para adicionar a grupos de entrega. Atualmente, o XenMobile Server suporta a adição de iBooks apenas como mídia obrigatória.

Depois de planejar os recursos e os grupos de entrega para instrutores e alunos, você pode criar esses itens no console XenMobile.

1. Crie as políticas de dispositivo que você deseja implantar nos dispositivos do instrutor ou aluno. Para obter informações sobre a política do dispositivo de Configuração de Educação, consulte a Política de dispositivo Configuração de Educação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



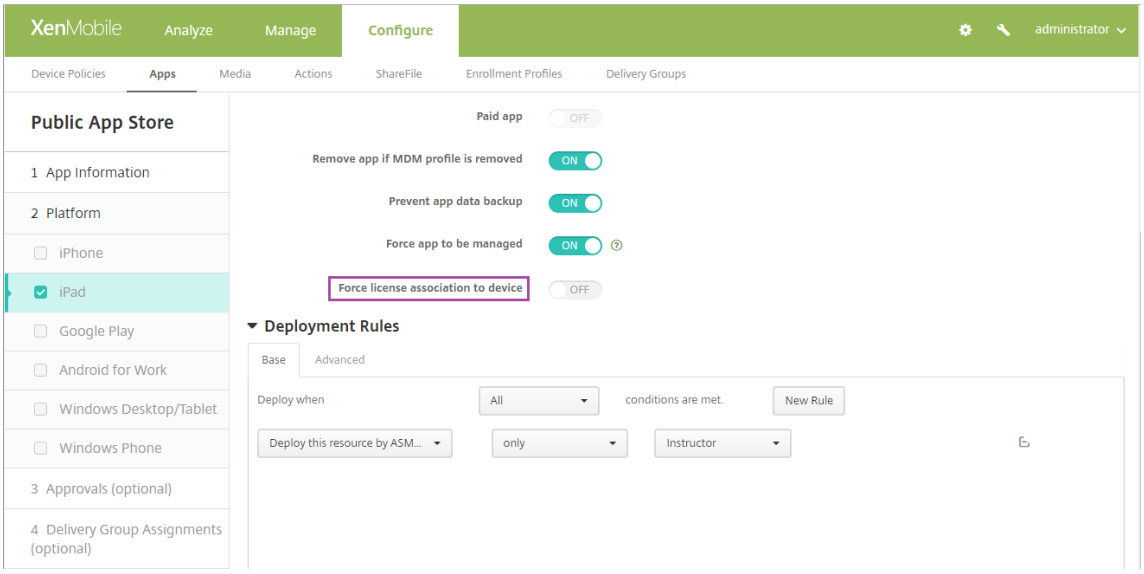
Consulte Políticas de dispositivo e os artigos individuais para obter informações sobre as políticas de dispositivo.

2. Configure aplicativos (**Configurar > Aplicativos**) e iBooks (**Configurar > Mídia**):

   - Por padrão, o XenMobile atribui aplicativos e iBooks no nível do usuário. Durante a implantação pela primeira vez, instrutores e alunos recebem uma mensagem para se registrar no VPP. Após aceitar o convite, os usuários recebem seus aplicativos VPP e iBooks na próxima implantação (dentro seis horas). A Citrix recomenda que você force a implantação de aplicativos e iBooks para novos usuários VPP. Para fazer isso, selecione o grupo de entrega e clique em **Implantar**.

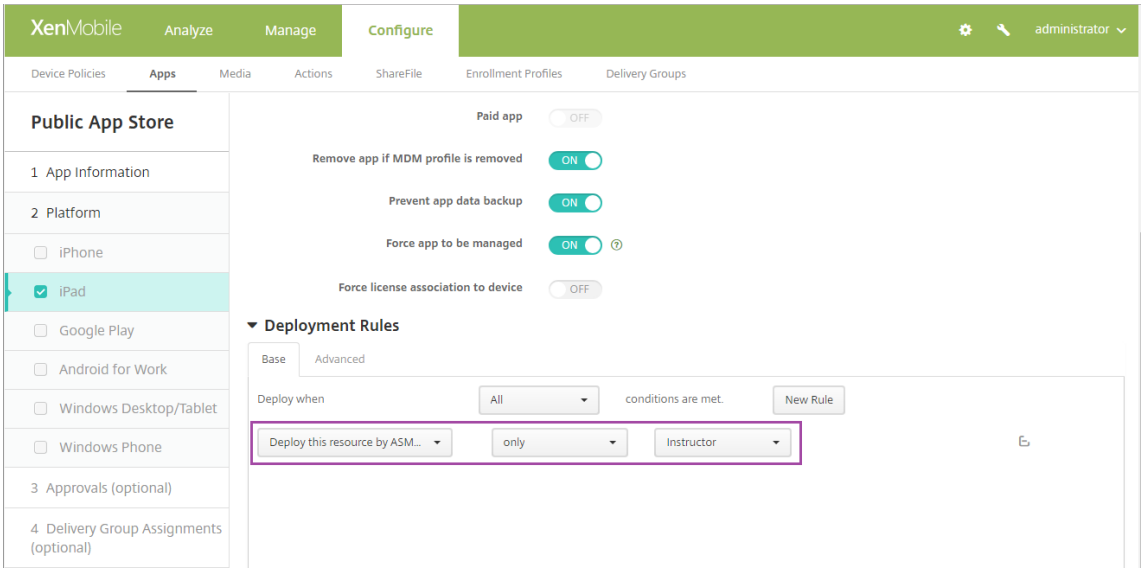
     Você pode optar por atribuir aplicativos (mas não iBooks) no nível do dispositivo. Para fazer isso, mude a configuração **Forçar a associação da licença ao dispositivo** para **Ativado**. Quando você atribui aplicativos no nível de dispositivo, os usuários não recebem um convite para participar do programa VPP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Para implantar um aplicativo somente para instrutores, selecione um grupo de entrega que inclua apenas instrutores ou use a seguinte regra de implantação:

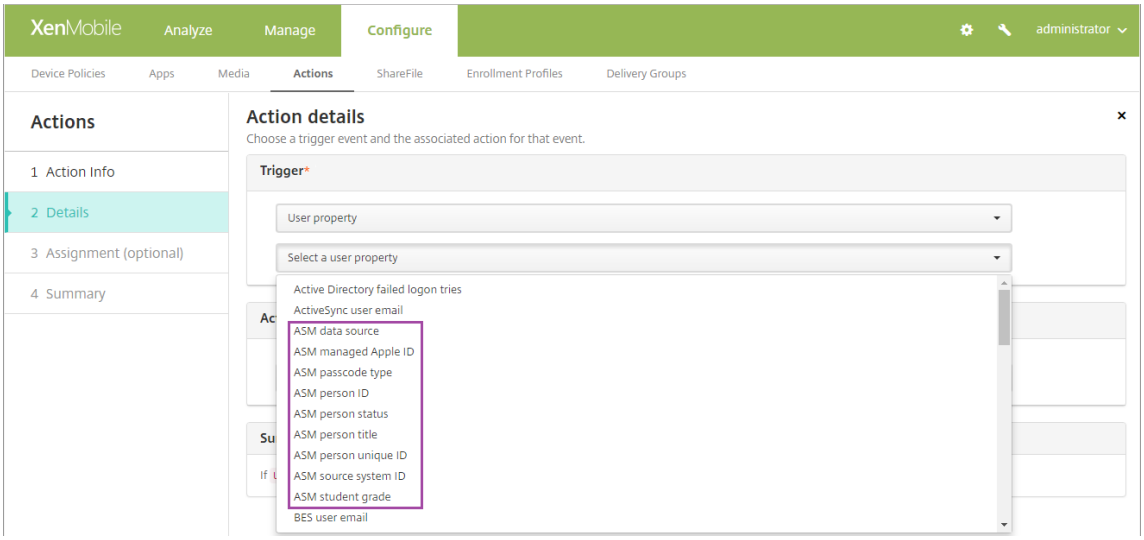
```
1  Deploy this resource by ASM DEP device type
2  only
3  Instructor
```



- Para obter ajuda com a adição de aplicativos VPP, consulte Acrescentar um aplicativo de loja de aplicativos pública.

3. Opcional. Crie ações com base nas propriedades do usuário do Apple School Manager. Por exemplo, você pode criar uma ação para enviar uma notificação para os dispositivos do aluno quando um novo aplicativo for instalado. Alternativamente, você pode criar uma ação que uma propriedade do usuário dispara, como mostrado no exemplo a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



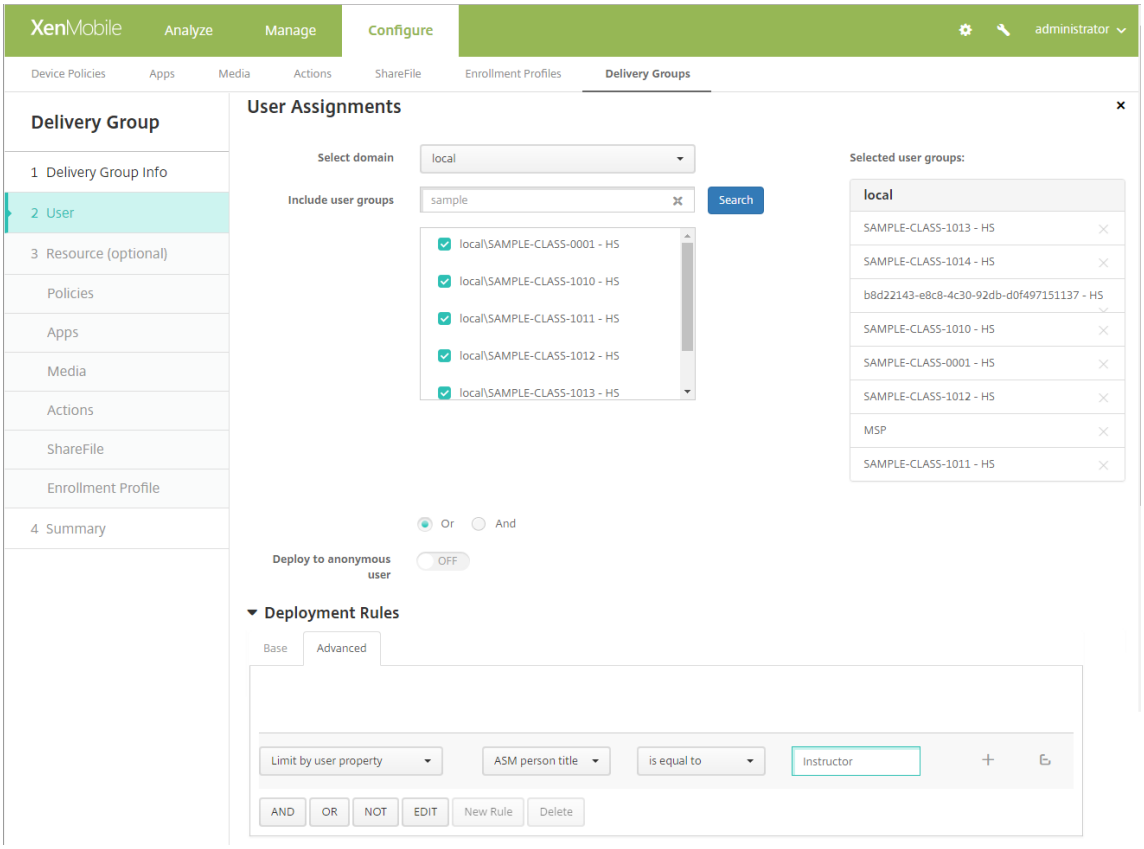
Para criar uma ação, vá para **Configurar > Ações**. Para obter informações sobre as ações, consulte Ações automatizadas.

4. Em **Configurar > Grupos de entrega**, crie os grupos de entrega para instrutores e alunos. Escolha as classes que foram importadas do Apple School Manager. Além disso, crie uma regra de implantação para instrutores e alunos.

   Por exemplo, as seguintes atribuições do usuário são para instrutores. A regra de implantação é:

```
Limit by user property
ASM person title
is equal to
Instructor
```

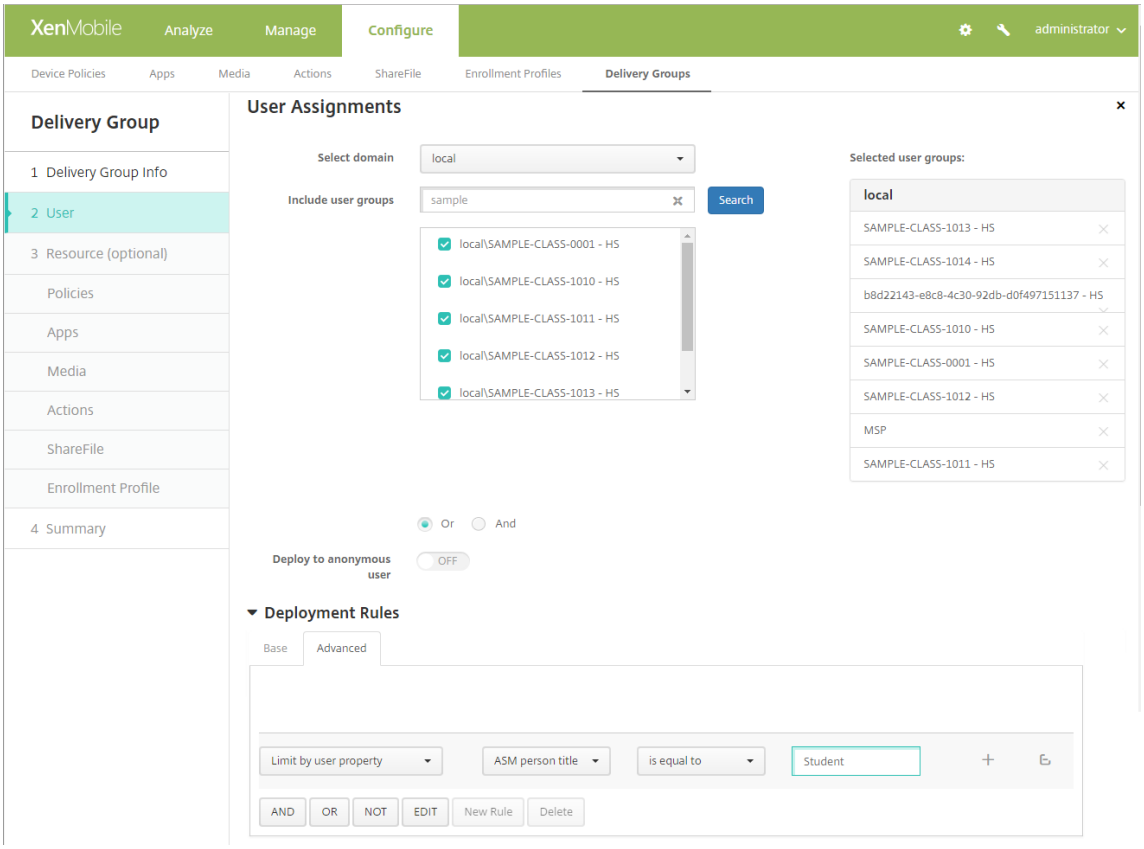
© 1999-2019 Citrix Systems, Inc. All rights reserved.



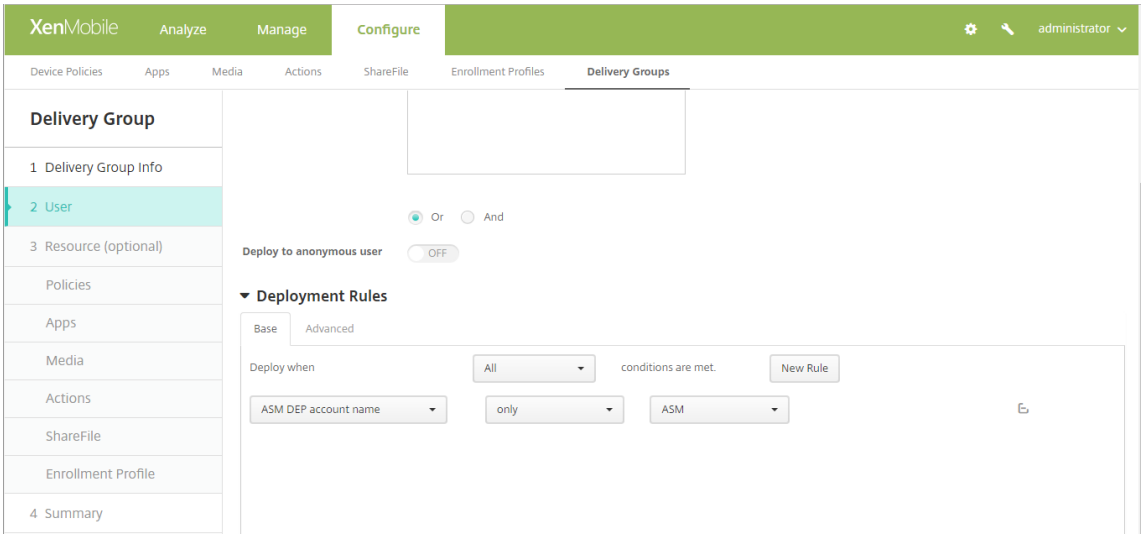
As seguintes atribuições do usuário são para alunos. A regra de implantação é:

```
Limit by user property
ASM person title
is equal to
Student
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

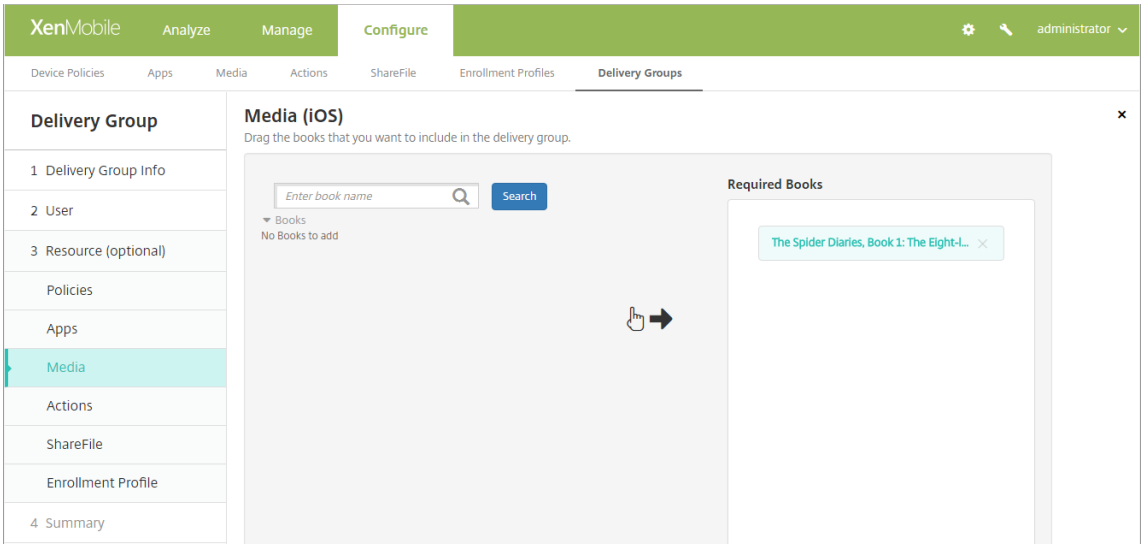


Você também pode filtrar um grupo de entrega usando uma regra de implantação com base no nome da conta DEP do Apple School Manager.

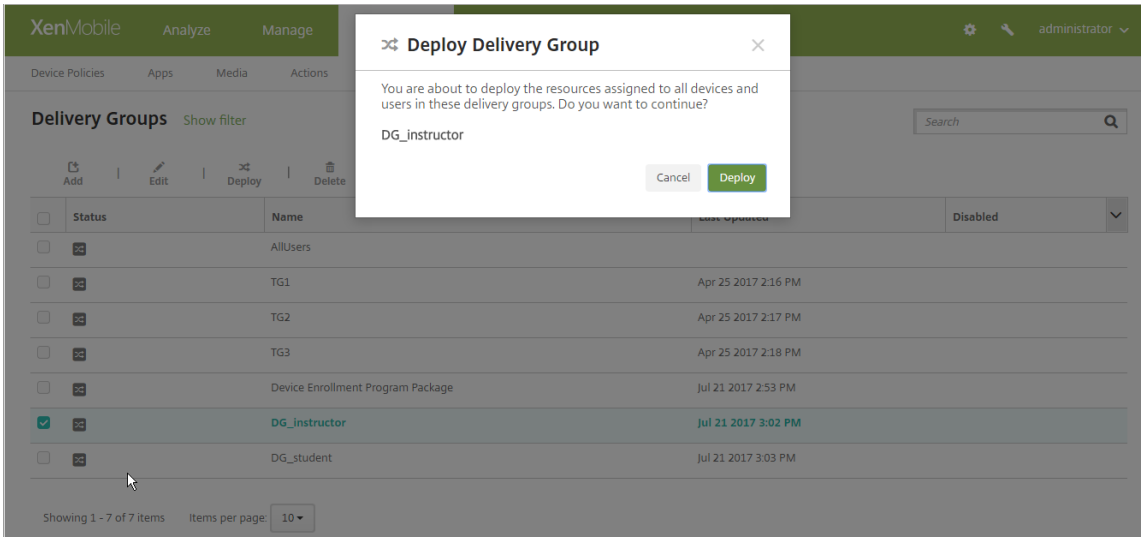


5. Atribua os recursos a grupos de entrega. O exemplo a seguir mostra um iBook contido em um grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



O exemplo a seguir mostra a caixa de diálogo de confirmação que é exibida 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: Teste o registro do dispositivo do instrutor e aluno

Você pode registrar dispositivos por meio de um dos seguintes métodos:

- O administrador da escola pode registrar dispositivos de instrutores e alunos usando a senha de usuário que você pode configurar no console XenMobile. Como resultado, você pode fornecer aos usuários dispositivos que já estejam configurados com aplicativos e mídia.
- Quando os usuários recebem os dispositivos, eles se registram usando a senha de usuário que

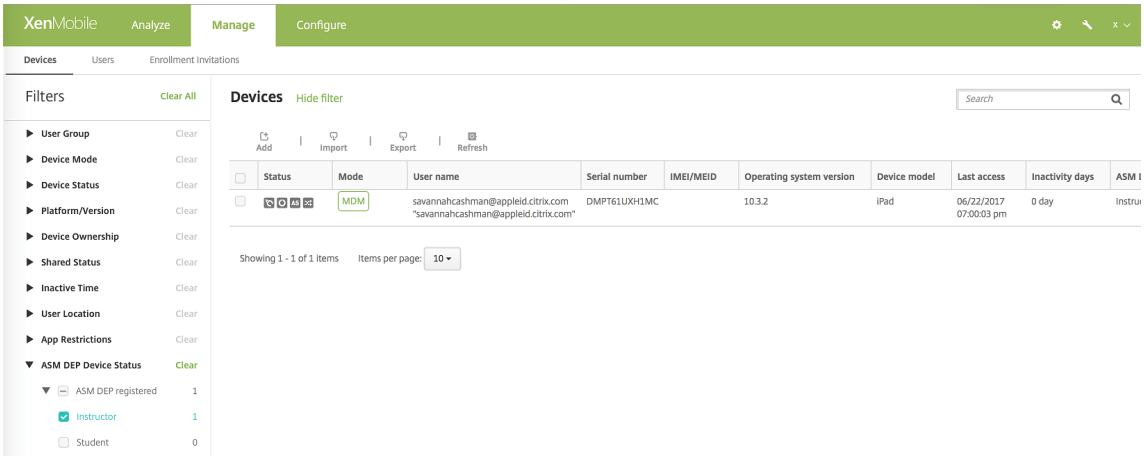
© 1999-2019 Citrix Systems, Inc. All rights reserved.

você fornece a eles. Depois que o registro for concluído, o XenMobile Server envia as políticas de dispositivo, aplicativos e mídia para os dispositivos.

Para testar o registro, use os dispositivos DEP que estão vinculados ao Apple School Manager.

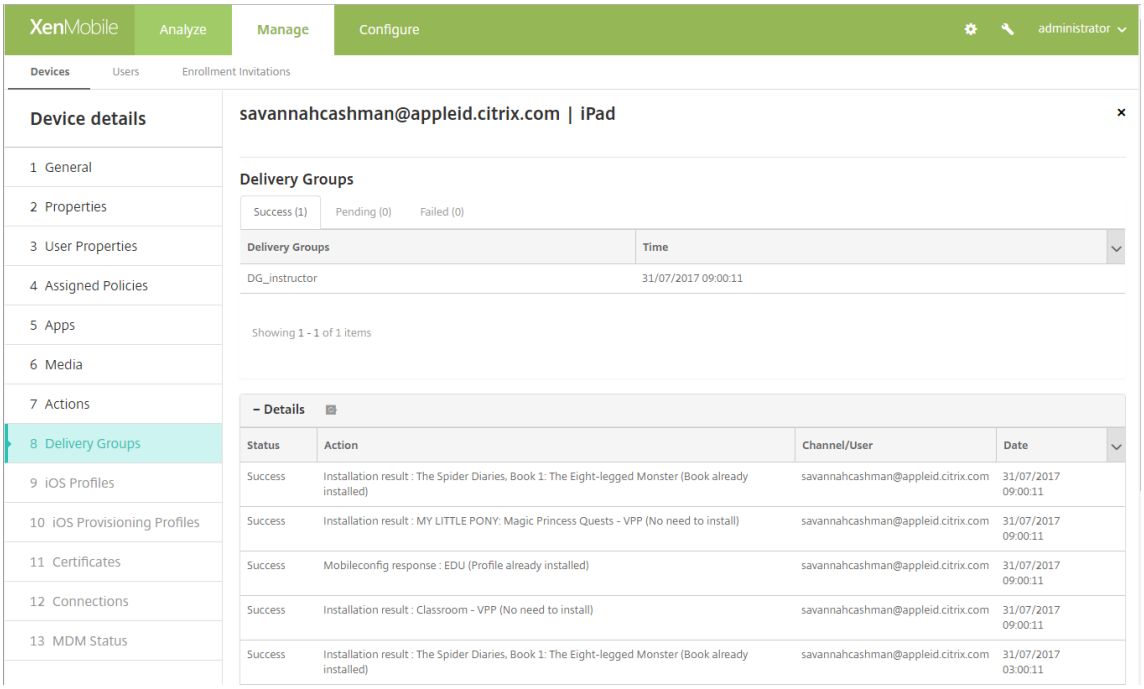
1. Se os dispositivos não estiverem vinculados ao Apple School Manager, apague o conteúdo e as configurações do dispositivo executando uma reinicialização.
2. Registre um dispositivo DEP do Apple School Manager com um instrutor. Depois, registre um dispositivo DEP do Apple School Manager com um aluno.
3. Na página **Gerenciar > Dispositivos**, verifique se ambos os dispositivos DEP do Apple School Manager estão registrados apenas no MDM.

   Você pode filtrar a página **Dispositivos** pelo status do dispositivo DEP do Apple School Manager: **DEP do ASM registrado**, **Instrutor** e **Aluno**.



4. Para verificar se os recursos do MDM foram implantados corretamente para cada dispositivo: selecione o dispositivo, clique em **Editar** e verifique as várias páginas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Etapa 9: Distribua os dispositivos

A Apple recomenda que você promova um evento para que possa distribuir dispositivos para instrutores e alunos.

Se você não distribuir dispositivos pré-inscritos, forneça o seguinte a esses usuários:

- Senhas do XenMobile Server para o registro do DEP
- Senhas temporárias do Apple School Manager para IDs Apple gerenciados.

A primeira experiência de uso do usuário é a seguinte.

1. A primeira vez que um usuário inicia o seu dispositivo após uma reinicialização, o XenMobile solicita, na tela de registro do DEP, que o usuário registre o dispositivo.
2. O usuário fornece o ID Apple gerenciado e a senha do XenMobile Server usados para se autenticar no XenMobile Server.
3. Na etapa de configuração do ID Apple, o dispositivo solicita ao usuário que forneça seu ID Apple gerenciado e a senha temporária do Apple School Manager. Esses itens autenticam o usuário nos serviços Apple.
4. O dispositivo solicita ao usuário que crie uma senha para o ID Apple gerenciado usado para proteger seus dados no iCloud.
5. No final do Assistente de Configuração, o XenMobile Server inicia a instalação das políticas, aplicativos e mídia no dispositivo. Para aplicativos e iBooks atribuídos no nível de usuário, o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

assistente solicita a instrutores e alunos o registro no VPP. Após aceitar o convite, os usuários recebem seus aplicativos VPP e iBooks na próxima implantação (dentro seis horas).

Gerenciar instrutor, aluno e dados da classe

Ao gerenciar o instrutor, aluno e dados da classe, observe o seguinte:

- Não altere IDs Apple gerenciados depois de importar informações do Apple School Manager para o XenMobile Server. O XenMobile também usa os identificadores de usuários do Apple School Manager para identificar os usuários.
- Se você adicionar ou alterar dados de classe no Apple School Manager depois de criar uma ou mais políticas de dispositivo de Configuração de Educação: edite as políticas e, em seguida, reimplante-as.
- Se o instrutor de uma classe mudar depois de você implantar a política do dispositivo de Configuração de Educação: revise a política para garantir que ela seja atualizada no console XenMobile e depois reimplante a política.
- Se você atualizar as propriedades do usuário no portal do Apple School Manager, o XenMobile também atualizará essas propriedades no console. No entanto, o XenMobile não recebe a propriedade do título da pessoa no ASM (Instrutor (Professor), Estudante ou Outros) da mesma forma que recebe outras propriedades. Assim, se você alterar o título de pessoa do ASM no Apple School Manager, conclua as seguintes etapas para refletir essa alteração no XenMobile.

Para gerenciar os dados:

1. No portal do Apple School Manager, atualize a nota do aluno e limpe a nota do instrutor.
2. Se você tiver alterado uma conta de aluno para uma conta de instrutor, remova o usuário da lista de alunos na classe. Em seguida, adicione o usuário à lista de instrutores na mesma ou em outra classe.

   Se você tiver alterado uma conta de instrutor para uma conta de aluno, remova o usuário da classe. Em seguida, adicione o usuário à lista de alunos na mesma ou em outra classe. Suas atualizações aparecem no console XenMobile durante a próxima sincronização (a cada cinco minutos por padrão) ou obtenção/busca (a cada 24 horas, por padrão).
3. Edite a política do dispositivo Configuração de Educação para aplicar a alteração e reimplante-a.

   - Se você excluir um usuário do portal Apple School Manager, o XenMobile Server também exclui esse usuário do console XenMobile após uma busca.

     Você pode reduzir o intervalo entre duas linhas de base alterando este valor da propriedade de servidor: **bulk.enrollment.fetchRosterInfoDelay** (o padrão é **1440** minutos).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Depois de implantar recursos: se um aluno ingressar em uma classe, crie um grupo de entrega com apenas esse aluno e implemente os recursos para o aluno.
- Se um aluno ou instrutor perder sua senha temporária, entre em contato com o administrador do Apple School Manager. O administrador pode fornecer a senha temporária ou gerar uma nova.

Gerenciar um dispositivo perdido ou roubado que esteja registrado no DEP do Apple School Manager

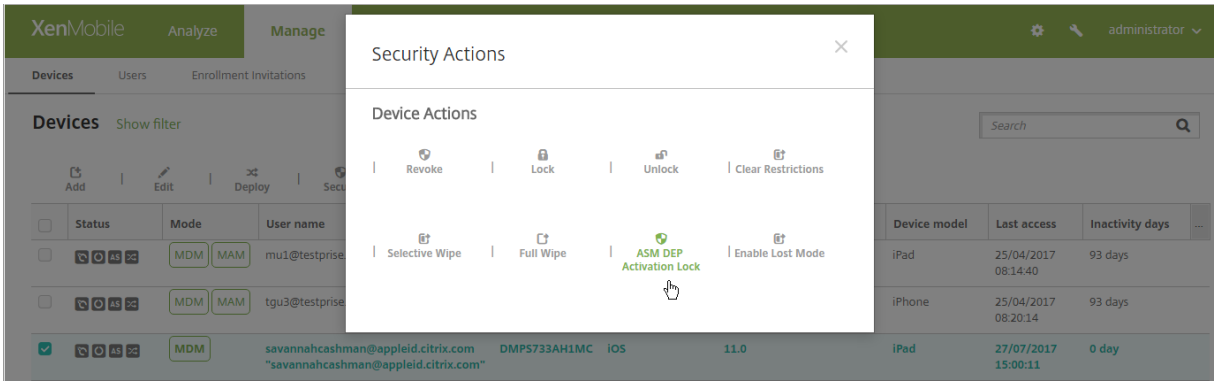
O serviço Apple Buscar do iPhone/iPad inclui um recurso de bloqueio de ativação. O Bloqueio de Ativação impede usuários não autorizados de usar ou revender um dispositivo perdido ou roubado que esteja registrado no DEP.

O XenMobile inclui uma ação de segurança de **Bloqueio de ativação DEP ASM** que permite que você envie um código de bloqueio para um dispositivo registrados em DEP do Apple School Manager.

Quando você usa a ação de segurança de **Bloqueio de ativação DEP ASM**, o XenMobile pode localizar dispositivos sem a necessidade de os usuários ativarem o serviço Buscar do iPhone/iPad. Quando um dispositivo do Apple School Manager é reconfigurado ou totalmente apagado, o usuário fornece o ID Apple gerenciado e a senha para desbloquear o dispositivo.

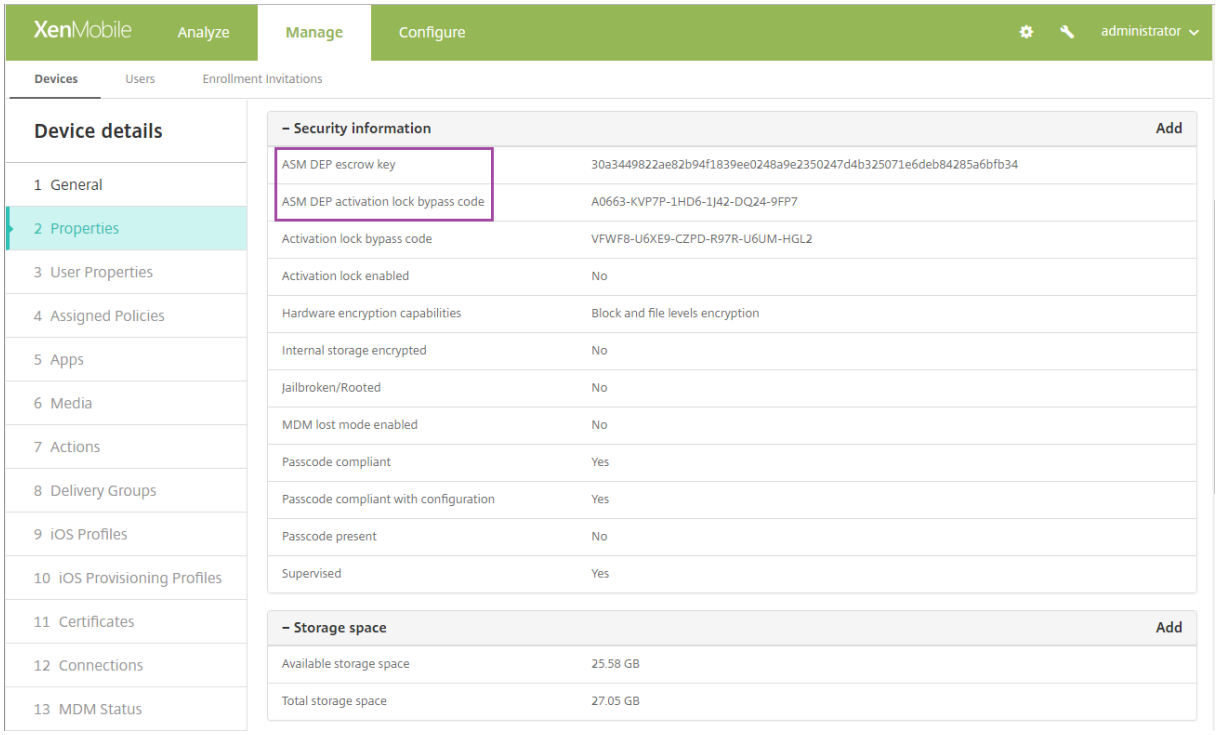
Para liberar o bloqueio a partir do console, clique na ação de segurança **Ignorar bloqueio de ativação**. Para obter informações sobre como ignorar um bloqueio de ativação, consulte Ignorar bloqueio de ativação do iOS no artigo de ações de segurança. O usuário também pode deixar o logon em branco e digitar o **código de desvio do bloqueio de ativação DEP ASM** como a senha. Essa informação está disponível em **Detalhes do dispositivo**, na guia **Propriedades**.

Para configurar o bloqueio de ativação, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e, em seguida, clique em **Bloqueio de ativação do DEP ASM**.

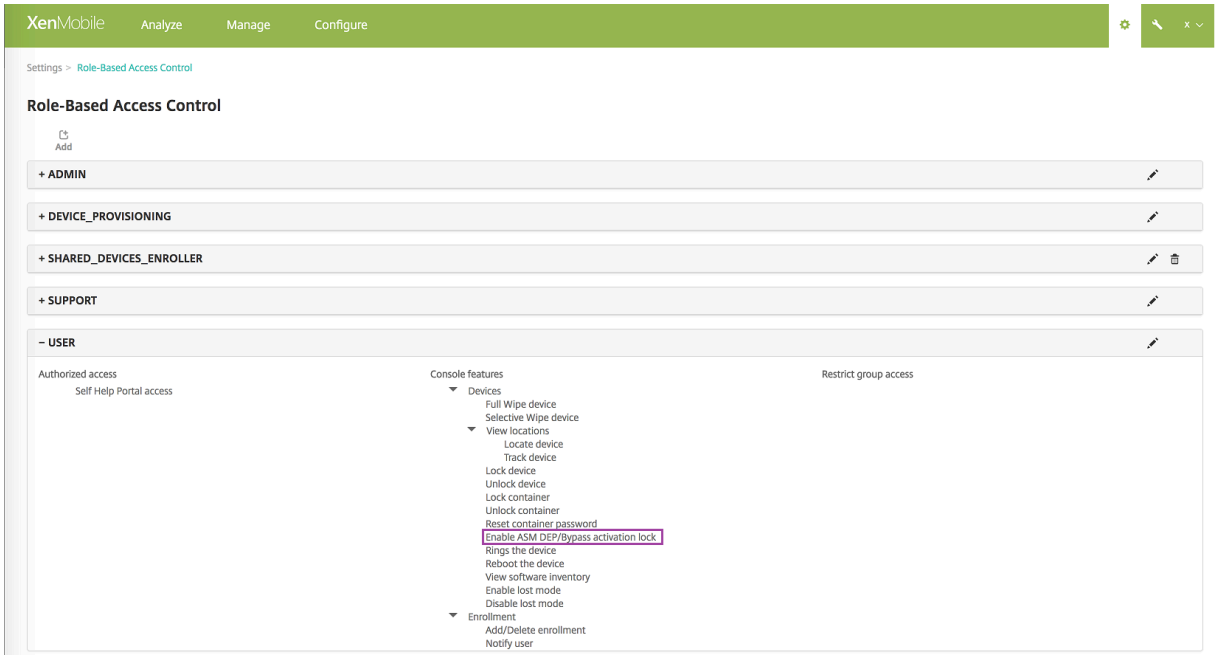


As propriedades **Chave de caução DEP ASM** e **código de desvio do bloqueio de ativação DEP ASM** aparecem nos **Detalhes do dispositivo**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A permissão RBAC para um bloqueio de ativação DEP ASM é **Dispositivos >Ativar desvio do bloqueio de ativação/DEP ASM**.



Controle de Acesso da Rede

March 6, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Se você tiver um dispositivo de Controle de Acesso da Rede (NAC) configurado na sua rede, como um Cisco ISE, poderá ativar filtros no XenMobile para definir dispositivos como compatíveis ou não compatíveis com NAC com base em regras ou propriedades. Se um dispositivo gerenciado no XenMobile não atender aos critérios especificados e, como resultado, estiver marcado como Não compatível, o dispositivo NAC bloqueará o dispositivo em sua rede. Nos dispositivos iOS, você pode implantar a política de VPN e habilitar um filtro NAC para bloquear uma conexão VPN para dispositivos que tenham aplicativos não compatíveis instalados. Para mais detalhes, consulte a seção "Configuração do iOS NAC" abaixo.

No console XenMobile, você pode selecionar um ou mais critérios na lista para definir um dispositivo como não compatível.

O XenMobile é compatível com os seguintes filtros de conformidade com NAC:

Dispositivos Anônimos: verifica se um dispositivo está no modo anônimo. Essa verificação estará disponível se o XenMobile não conseguir autenticar novamente o usuário quando um dispositivo tentar se reconectar.

Erro de atestado de Samsung KNOX: verifica se um dispositivo falhou em uma consulta do servidor de atestado do Samsung KNOX.

Aplicativos proibidos: verifica se um dispositivo tem aplicativos proibidos, conforme definido em uma política de Acesso aos Aplicativos. Para obter mais informações sobre a política de acesso aos aplicativos, consulte Políticas de dispositivo de acesso aos 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 não tem os aplicativos obrigatórios, conforme definido em uma política de Acesso aos aplicativos.

Aplicativos não sugeridos: verifica se um dispositivo tem aplicativos não sugeridos, conforme definido em uma Política de acesso aos aplicativos.

Senha não compatível: verifica se a senha de usuário está em conformidade. Nos dispositivos Android e iOS, o XenMobile pode determinar se a senha no dispositivo no momento está em conformidade com a política de código secreto enviada para o dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de código secreto para o dispositivo. Antes que o usuário defina a senha, o código secreto pode não estar em conformidade.

Dispositivos sem conformidade: verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Sem Conformidade. Essa propriedade normalmente é alterada pelas ações automatizadas ou por um terceiro que utiliza as APIs do XenMobile.

Status revogado: verifica se o certificado do dispositivo foi revogado. Um dispositivo revogado não pode se registrar novamente até que tenha autorização novamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dispositivos Android com root e iOS com jailbreak: verifica se um dispositivo Android ou iOS tem jailbreak.

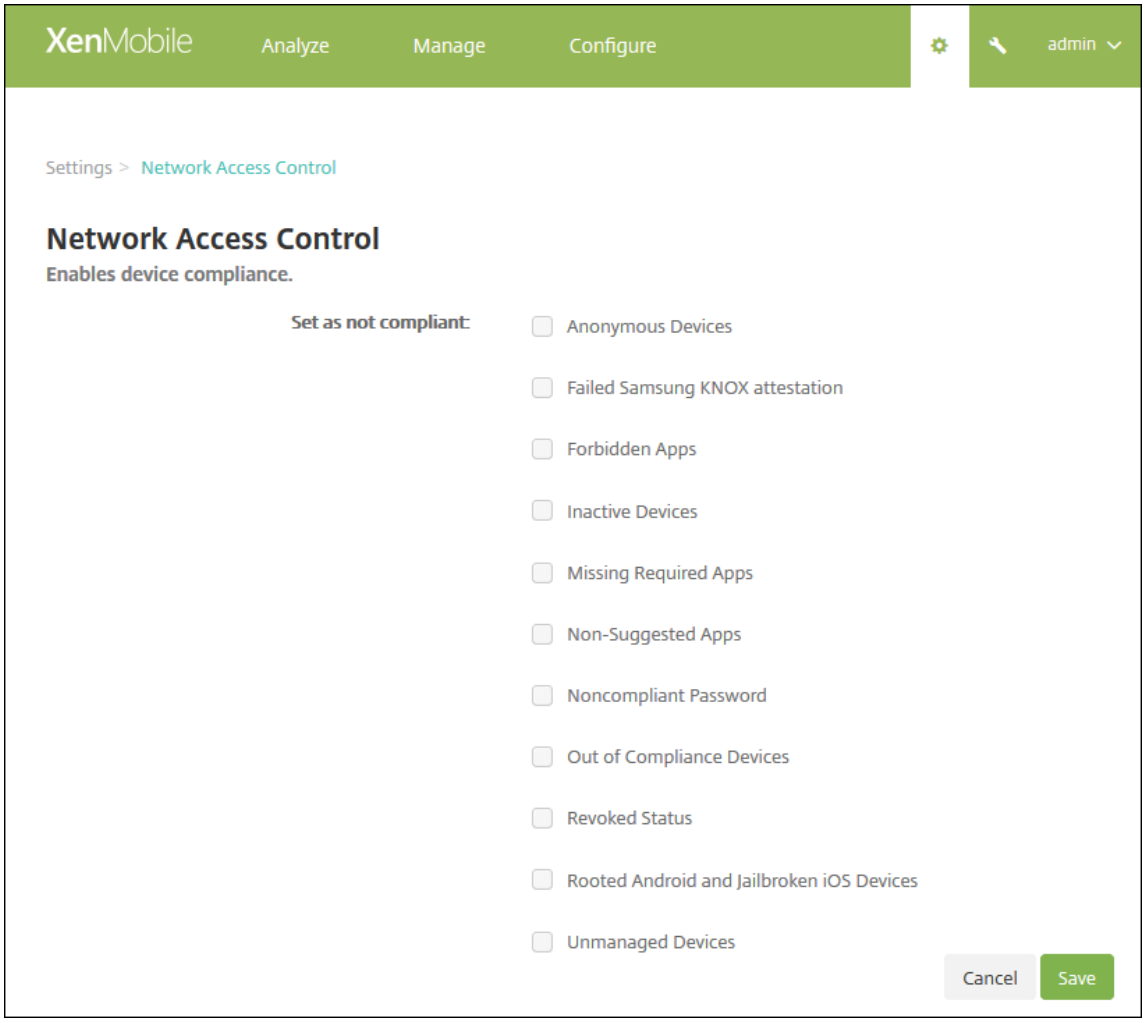
Dispositivos não gerenciados: verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo que está em execução no modo MAM ou um dispositivo não registrado não é gerenciado.

> Nota:
>
> O filtro Conformidade/Não conformidade implícita define o valor padrão somente nos dispositivos gerenciados pelo XenMobile. Por exemplo, qualquer dispositivo com um aplicativo na lista negra instalado ou que não seja registrado é marcado como Não compatível e será bloqueado da sua rede pelo dispositivo de NAC.

Configurar o controle de acesso da rede

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Controle de acesso da rede**. A página **Controle de acesso da rede** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Marque as caixas de seleção dos filtros **Definir como não compatível** que você desejar ativar.
4. Clique em **Salvar**.

Samsung KNOX

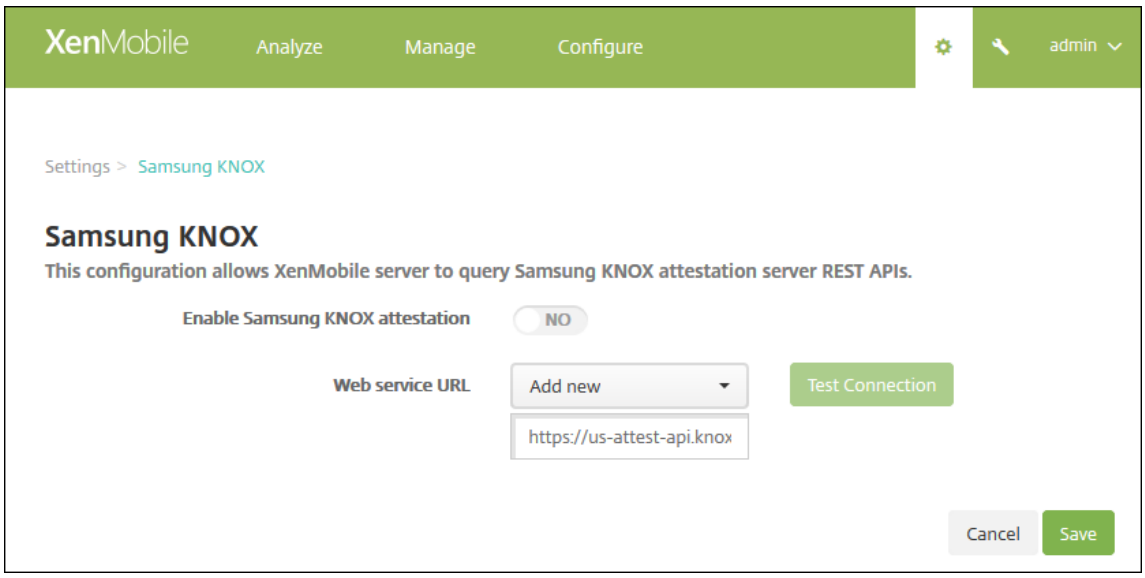
April 15, 2019

Você pode configurar o XenMobile para consultar as APIs REST do servidor de atestado do Samsung KNOX.

O Samsung KNOX aproveita os recursos de segurança de hardware que oferecem vários níveis de proteção para o sistema operacional e os aplicativos. Um nível dessa segurança reside na plataforma por meio do atestado. Um servidor de atestado fornece a verificação do software de 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. No console da Web 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 **Ativar atestado do Samsung KNOX**, selecione se o atestado do Samsung KNOX deve ser ativado. O padrão é **NÃO**.
4. Quando você define **Ativar atestado do Samsung KNOX** como **SIM**, a opção **URL de serviço da Web** é ativada. Em seguida, na lista, siga um dos seguintes procedimentos:
   - Clique no servidor de atestado apropriado.
   - Clique em **Adicionar novo** e, em seguida, digite a URL do serviço da Web.
5. Clique em **Testar conexão** para verificar a conexão. É exibida uma mensagem de êxito ou falha.
6. Clique em **Salvar**.

> Nota:
>
> Você pode usar o Samsung KNOX Mobile Enrollment para registrar vários dispositivos Samsung KNOX no XenMobile (ou qualquer gerenciador de dispositivos móveis) sem configurar manualmente cada dispositivo. Para obter informações, consulte Inscrição em massa no Samsung KNOX.

Ações de segurança

March 6, 2019

Você pode executar ações de segurança em um dispositivo e aplicativo na página **Gerenciar > Dispositivos**. Ações do dispositivo incluem revoke, bloqueio, desbloqueio e apagar. Ações de segurança de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aplicativo incluem o bloqueio de aplicativo e apagamento de aplicativos.

- **Ignorar bloqueio de ativação:** remove o bloqueio de ativação dos dispositivos iOS supervisionados antes da ativação do dispositivo. Esse comando não requer o ID Apple pessoal ou a senha de um usuário.
- **Bloqueio de aplicativo:** nega acesso a todos os aplicativos em um dispositivo. No Android, depois de um bloqueio de aplicativo, os usuários não podem fazer login no XenMobile. No iOS, os usuários podem fazer login, mas não podem acessar aplicativos.
- **Apagamento de aplicativos:** no Android, o apagamento de aplicativo exclui a conta do usuário do XenMobile. No iOS, exclui uma conta de usuário no Secure Hub.
- **Bloqueio de ativação DEP ASM:** cria um código de desvio de bloqueio de ativação para dispositivos iOS registrados no DEP Apple School Manager.
- **Limpar restrições:** em dispositivos iOS supervisionados, este comando permite que o XenMobile Server limpe as restrições de configurações de senha e restrições configuradas pelo usuário.
- **Ativar/desativar o 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 esse comando tira o dispositivo do Modo Perdido.
- **Apagamento completo:** apaga imediatamente todos os dados e aplicativos de um dispositivo, inclusive de qualquer cartão de memória.
  - Para dispositivos Android, esta solicitação também pode incluir a opção de apagar os cartões de memória.
  - Para dispositivos iOS e macOS, o apagamento ocorre imediatamente, mesmo que o dispositivo esteja bloqueado. Para dispositivos iOS 11 (versão mínima): quando você confirmar o apagamento completo, poderá optar por preservar o plano de dados celulares no dispositivo.
  - Para os dispositivos do Windows Phone, um apagamento completo remove todas as informações do XenMobile e todos os dados do usuário, incluindo conteúdo pessoal, como aplicativos, e-mails, contatos e mídia.
  - Para dispositivos Windows Mobile que estão executando o Windows Mobile 6 ou versões anteriores, após o apagamento, pode ser necessário enviar o dispositivo de volta para o fabricante para recarregar o sistema operacional, o software ou ambos.
  - Se o usuário do dispositivo desligar o dispositivo antes do conteúdo do cartão de memória ser excluído, o usuário ainda poderá ter acesso aos dados do dispositivo.
  - Você pode cancelar a solicitação de apagamento até que a solicitação seja enviada para o dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Localizar:** localiza um dispositivo e relata a localização do dispositivo, incluindo um mapa, na página **Gerenciar > Dispositivos**, em **Detalhes do dispositivo > Geral**.
- **Bloqueio:** bloqueia remotamente um dispositivo, o que é útil se um dispositivo for perdido, mas você não tiver certeza se ele foi roubado. O XenMobile gera um código PIN e o configura no dispositivo. Para acessar o dispositivo, o usuário digita o código PIN. Use **Cancelar bloqueio** para remover o bloqueio do console XenMobile
- **Bloquear e redefinir senha:** bloqueia remotamente um dispositivo e redefine a senha.
- **Notificar (toque):** emite um som em dispositivos Android.
- **Reinicializar:** reinicia os dispositivos Windows 10. Em Windows Tablet e PCs, a mensagem "Sistema reinicializará em breve" aparece e a reinicialização ocorre em cinco minutos. No Windows Phone, a reinicialização ocorre após alguns poucos minutos, sem mensagem de aviso para os usuários.
- **Solicitar/Parar espelhamento de AirPlay:** inicia e interrompe o espelhamento do AirPlay em dispositivos iOS supervisionados.
- **Reiniciar/Desligar:** reinicia imediatamente ou encerra os dispositivos iOS supervisionados.
- **Revogar:** proíbe um dispositivo de se conectar ao XenMobile Server.
- **Revogar/Autorizar (iOS, macOS):** executa as mesmas ações que um apagamento seletivo. Depois de revogação, você pode reautorizar um dispositivo para registrá-lo novamente.
- **Tocar:** se o dispositivo estiver no Modo Perdido, Tocar emite um som em um dispositivo iOS supervisionado. O som toca até que você retire o dispositivo do Modo Perdido ou o usuário desative o som.
- **Apagamento seletivo:** apaga todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local. Depois de um apagamento seletivo, um usuário pode registrar novamente o dispositivo.
  - Apagar seletivamente um dispositivo Android não desconecta o dispositivo do Device Manager nem da rede corporativa. Para impedir que o dispositivo acesse o Device Manager, você também precisa revogar os certificados do dispositivo.
  - Se a API KNOX Samsung estiver habilitada, apagar seletivamente o dispositivo também remove o contêiner Samsung KNOX.
  - Para dispositivos iOS e macOS, esse comando remove qualquer perfil instalado por meio do MDM.
  - Um apagamento seletivo em um dispositivo Windows também remove o conteúdo da pasta de perfil para qualquer usuário atualmente conectado. Um apagamento seletivo não remove os clipes web que você fornece para os usuários por meio de uma configuração. Para remover clipes web, os usuários manualmente cancelam o registro de seus dispositivos. Você não poderá registrar novamente um dispositivo seletivamente apagado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Limpar seletivamente um dispositivo Windows Phone remove o token da empresa que permite que o XenMobile para instale os aplicativos no dispositivo. Além disso, o apagamento remove todos os certificados do XenMobile e as configurações implantadas no dispositivo. Você não poderá registrar novamente um dispositivo Windows Phone seletivamente apagado.
  - O apagamento seletivo em dispositivos Android também revoga o dispositivo, e o dispositivo pode ser registrado de novo somente após autorizá-lo novamente ou excluí-lo do console.

- **Desbloquear:** libera o código secreto enviado para o dispositivo quando ele foi bloqueado. Este comando não desbloqueia o dispositivo.

Em **Gerenciar > Dispositivos**, a **página de 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 de **apagamento completo do dispositivo** inclui o código PIN do usuário. O usuário deve digitar o código depois que o dispositivo for apagado. Se o usuário esquecer o código, você pode procurá-lo aqui.

Ações de segurança para dispositivos Android

Ação de segurança	Android (exceto para dispositivos Android for Work)	Android for Work (BYOD)	Android for Work (propriedade da empresa)
Bloqueio de aplicativo	Sim	Não	Não
Apagamento de aplicativos	Sim	Não	Não
Apagamento completo	Sim	Não	Sim

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ação de segurança	Android (exceto para dispositivos Android for Work)	Android for Work (BYOD)	Android for Work (propriedade da empresa)
Localizar	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.
Bloquear	Sim	Sim	Sim
Bloquear e redefinir senha	Sim	Não	Sim
Notificar (Tocar)	Sim	Sim	Sim
Revogar	Sim	Sim	Sim
Apagamento seletivo	Sim	Sim	Não

Ações de segurança para dispositivos iOS e macOS

Ação de segurança	**iOS**	**macOS**
Ignorar bloqueio de ativação	Sim	Não
Bloqueio de aplicativo	Sim	Não
Apagamento de aplicativos	Sim	Não

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ação de segurança	iOS	macOS
Bloqueio de ativação DEP ASM	Sim	Não
Limpar restrições	Sim	Não
Ativar/Desativar o Modo Perdido	Sim	Não
Ativar/Desativar rastreamento	Sim	Não
Apagamento completo	Sim	Sim
Localizar	Sim	Não
Bloquear	Sim	Sim
Anel	Sim	Sim
Solicitar/Parar espelhamento de AirPlay	Sim	Não
Reiniciar/Desligar	Sim	Não
Revogar/Autorizar	Sim	Sim
Apagamento seletivo	Sim	Sim
Desbloquear	Sim	Não

Ações de segurança para dispositivos Windows

Ação de segurança	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Localizar	Sim	Sim	Não
Bloquear	Sim	Sim	Sim
Bloquear e redefinir senha	Sim	Não	Sim
Reinicializar	Sim	Sim	Não
Revogar	Sim	Sim	Sim
Anel	Sim	Não	Sim
Apagamento seletivo	Sim	Sim	Sim
Apagar	Sim	Não	Sim

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O restante deste artigo fornece as etapas para executar várias ações de segurança. Você também pode automatizar algumas ações. Para obter mais informações, consulte Ações automatizadas.

Bloquear dispositivos iOS

Você pode bloquear um dispositivo iOS perdido com uma exibição de acompanhamento de uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo. Esse recurso tem suporte em dispositivos que executam o iOS 7 e versões posteriores.

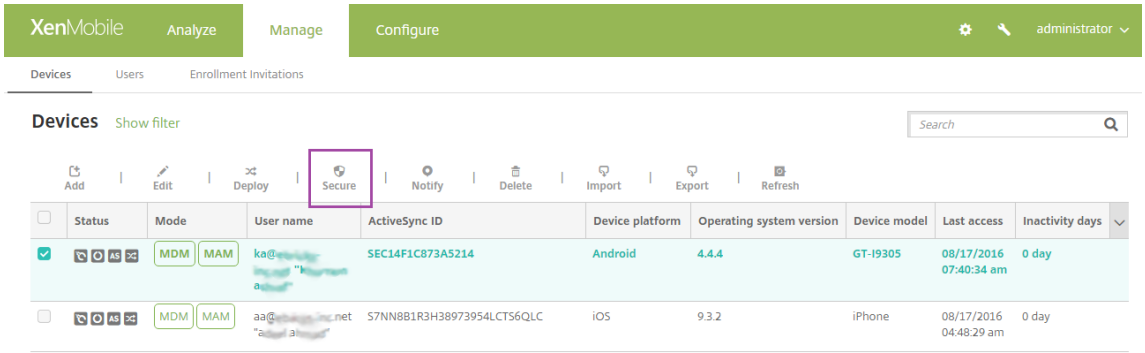
Para exibir uma mensagem e o número de telefone em um dispositivo bloqueado, defina a política de Código secreto como **true** no console XenMobile. Como alternativa, os usuários podem ativar o código secreto no dispositivo manualmente.

1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

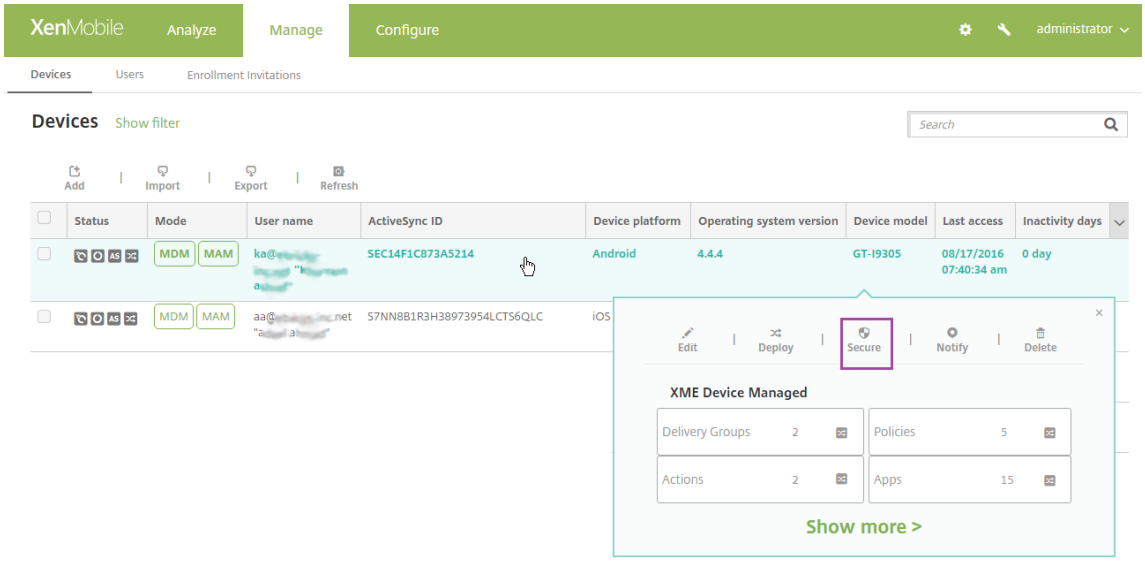


2. Selecione o dispositivo iOS que você deseja bloquear.

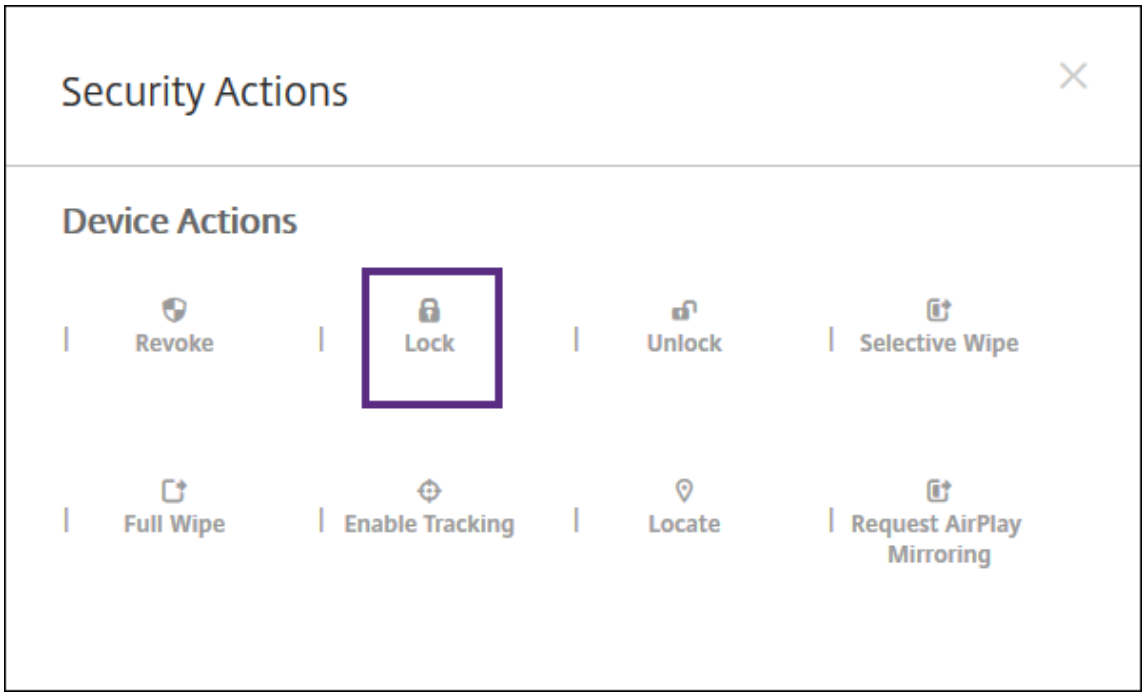
   Quando você marca a caixa de seleção ao lado de um dispositivo, o menu de opções é exibido acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

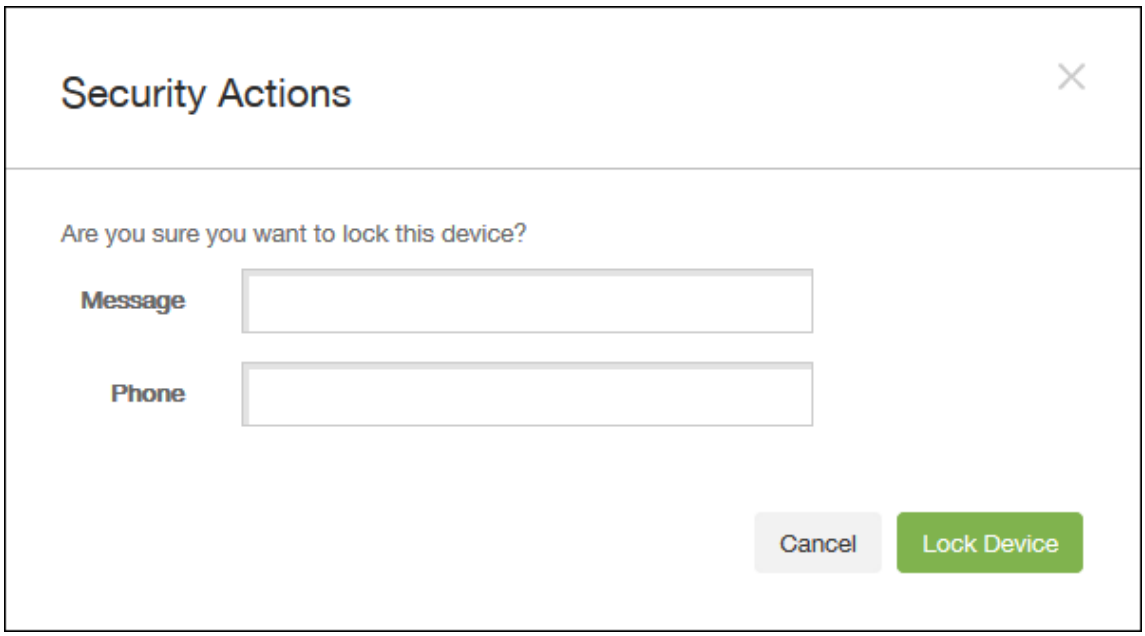


3. No menu de opções, clique em **Segurança**. A caixa de diálogo **Ações de Segurança** é exibida.



4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de segurança** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Opcionalmente, digite uma mensagem e um número de telefone que aparecerão na tela de bloqueio do dispositivo.

   Para iPads com iOS 7 e versões posteriores: o iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado na caixa **Mensagem**.

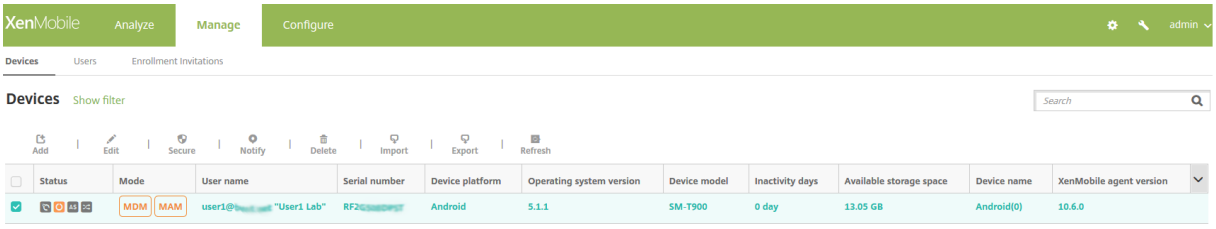
   Para iPhones que executam o iOS 7 e versões posteriores: se você deixar o campo **Mensagem** vazio e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

6. Clique em **Bloquear Dispositivo**.

Remover um dispositivo do console XenMobile

> Importante:
>
> Quando você remove um dispositivo do console XenMobile, aplicativos gerenciados e dados permanecem no dispositivo. Para remover os aplicativos gerenciados e os dados do dispositivo, consulte “Excluir um dispositivo” neste artigo.

Para remover um dispositivo do console XenMobile, vá até **Gerenciar > Dispositivos**, selecione o dispositivo gerenciado e, em seguida, clique em **Excluir**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Apagar dispositivo seletivamente

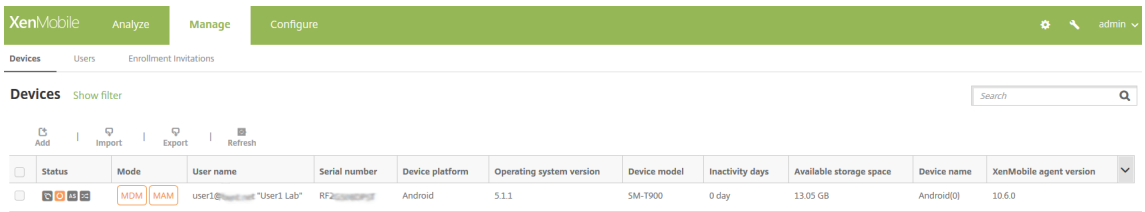
1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Em **Ações de segurança**, clique em **Apagamento seletivo**.
3. Somente para dispositivos Android, desconecte o dispositivo da rede corporativa: depois que o dispositivo for apagado, em **Ações de segurança**, clique em **Revogar**.

   Para retirar uma solicitação de apagamento seletivo antes do apagamento ocorrer, em **Ações de segurança**, clique em **Cancelar apagamento seletivo**.

Excluir um dispositivo

Este procedimento remove aplicativos gerenciados e dados do dispositivo e exclui o dispositivo da lista Dispositivos no console XenMobile.

1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Clique em **Apagamento seletivo**. Quando solicitado, clique em **Executar apagamento seletivo**.
3. Para verificar se o comando de apagamento foi bem-sucedido, atualize **Gerenciar > Dispositivos**. Na coluna **Modo**, a cor âmbar para MDM e MAM indica que o comando de apagamento foi bem-sucedido.



4. Em **Gerenciar > Dispositivos**, selecione o dispositivo e, em seguida, clique em **Excluir**. Quando solicitado, clique em **Excluir** novamente.

Bloquear, desbloquear, apagar ou cancelar apagamento de aplicativos

1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Em **Ações de segurança**, clique na ação do aplicativo.

   Você também pode usar a caixa **Ações de segurança** para verificar o status de um dispositivo para um usuário cuja conta está desabilitada ou foi excluída do Active Directory. A presença das ações Desbloqueio de aplicativo ou Cancelar apagamento de aplicativos indica que os aplicativos estão atualmente bloqueados ou apagados.

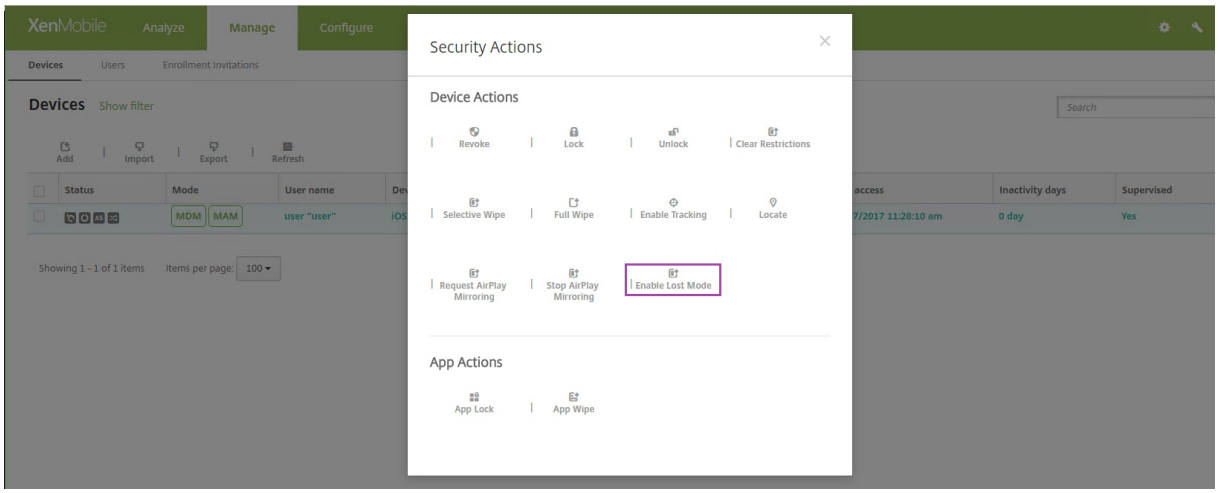
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Colocar dispositivos iOS no Modo Perdido

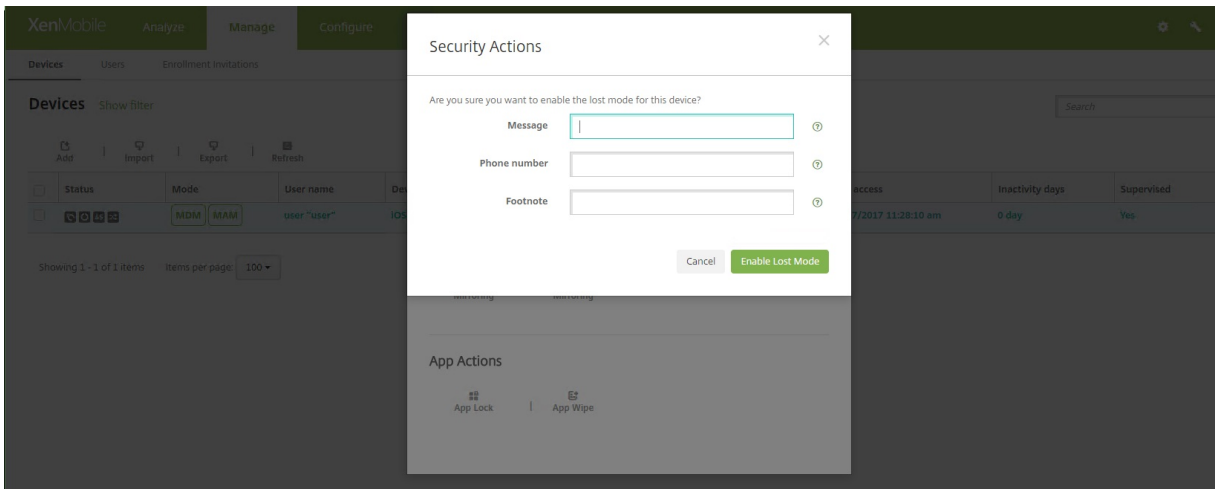
A propriedade de dispositivo Modo Perdido do XenMobile coloca um dispositivo iOS no Modo Perdido. Ao contrário do Modo perdido gerenciado da Apple, o Modo perdido do XenMobile não requer que um usuário realize nenhuma das seguintes ações para ativar a localização de seu dispositivo: definir a configuração do iPad Buscar iPhone ou ativar os Serviços de localização para o Citrix Secure Hub.

No Modo perdido do XenMobile, somente o XenMobile Server 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 fornecido por você.

Para ativar ou desativar o Modo perdido: vá para **Gerenciar > Dispositivos**, escolha um dispositivo iOS supervisionado e clique em **Segurança**. Em seguida, clique em **Ativar modo perdido** ou **Desativar modo perdido**.



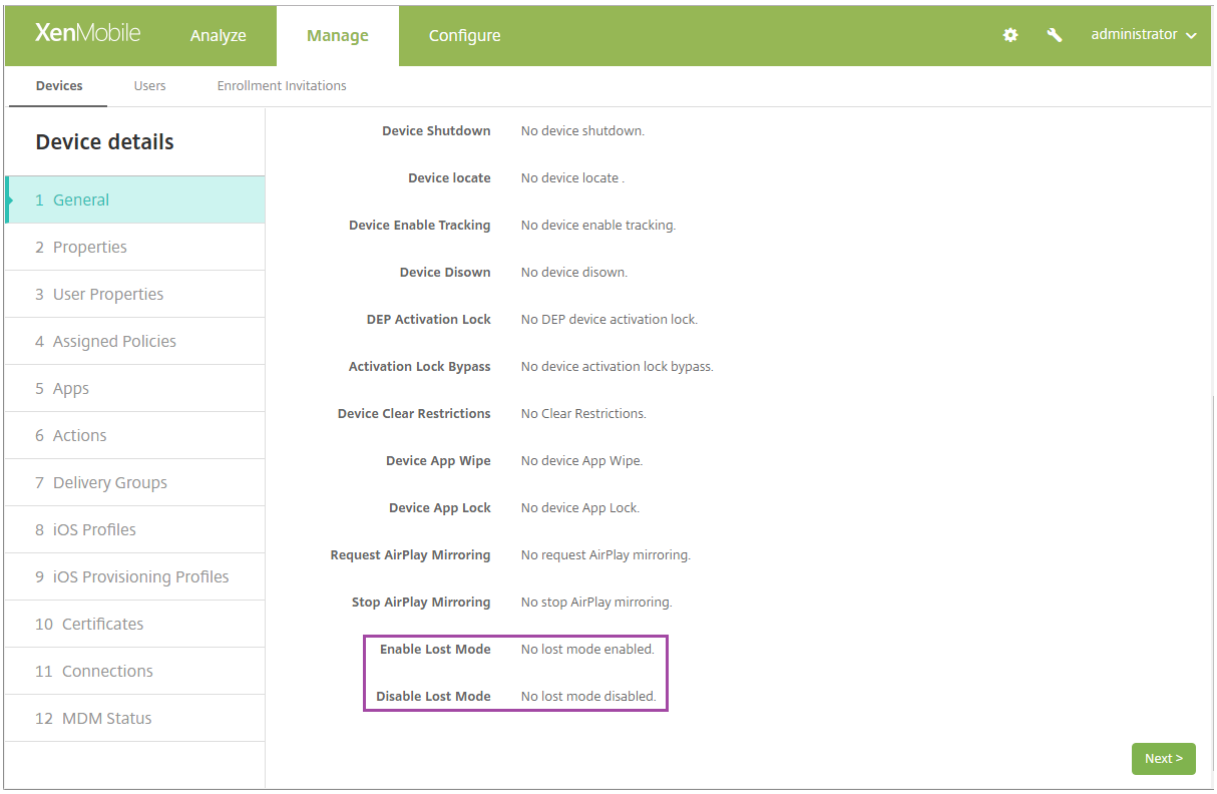
Se você clicar em **Ativar Modo Perdido**, digite informações para aparecer no dispositivo quando estiver no modo perdido.



Use qualquer um dos seguintes métodos para verificar o status do Modo perdido:

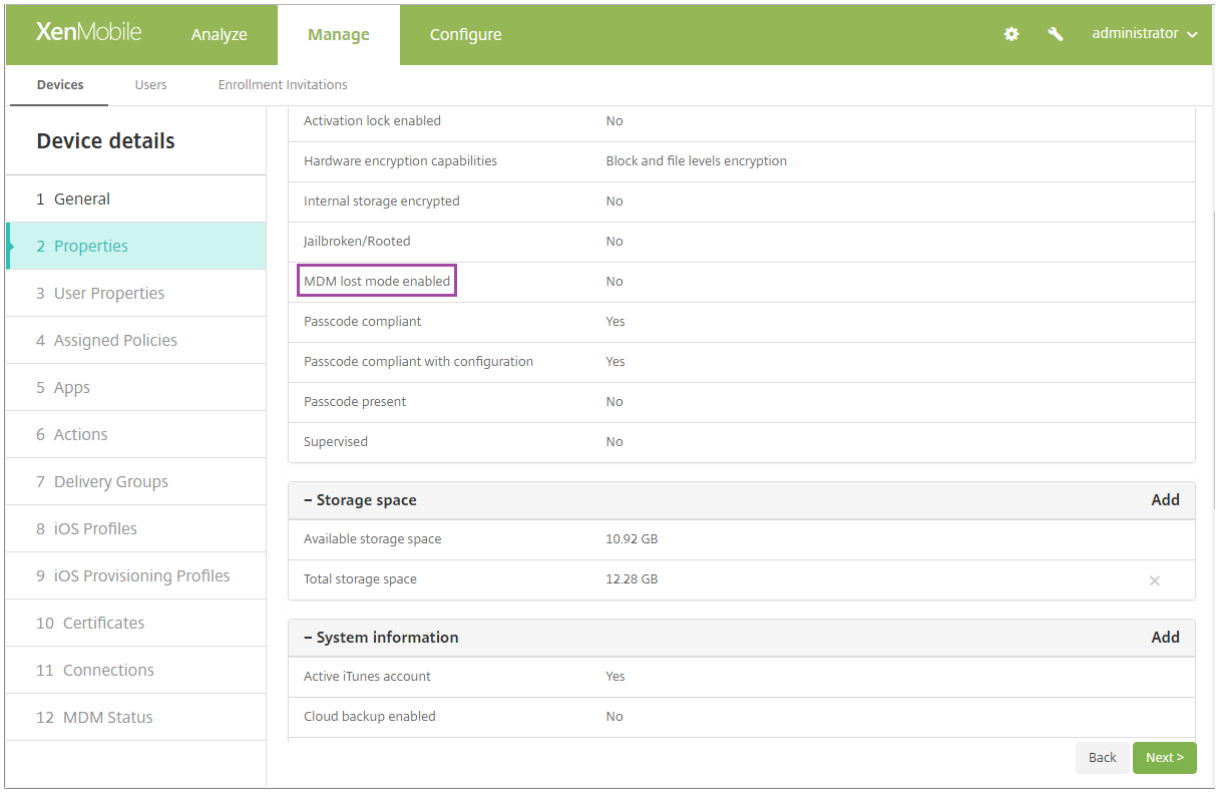
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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**, confirme que o valor da configuração de **Modo perdido de MDM ativado** esteja correta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se você ativar o Modo perdido do XenMobile em um dispositivo iOS, o console XenMobile também mudará, da seguinte maneira:

- Em **Configurar > Ações**, a lista **Ações** não inclui estas ações automatizadas: **Revogar o dispositivo**, **Apagar seletivamente o dispositivo** e **Apagar completamente o dispositivo**.
- Em **Gerenciar > Dispositivos**, a lista **Ações de segurança** não inclui mais as ações de dispositivo **Revogar** e **Apagamento seletivo**. Você ainda pode usar uma ação de segurança para executar uma ação de **Apagamento completo**, conforme necessário.

Para iPads com iOS 7 e versões posteriores: o iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado na caixa **Mensagem** na tela **Ações de segurança**.

Para iPhones com iOS 7 e versões posteriores: 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 bloqueio de ativação do iOS

Bloqueio de ativação é um recurso do Buscar iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário antes que qualquer pessoa possa desligar o Buscar iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos de propriedade da organização, ignorar um bloqueio de ativação é necessário, por exemplo, para redefinir ou realocar dispositivos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para ativar o Bloqueio de Ativação, você configura e implanta a política do dispositivo de Opções XenMobile MDM. Você pode gerenciar um dispositivo a partir do console XenMobile sem as credenciais Apple do usuário. Para desviar do requisito de credenciais Apple de um bloqueio de ativação, execute a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Por exemplo, se o usuário retorna um telefone perdido ou para configurar o dispositivo antes ou após um apagamento completo: quando o telefone pede as credenciais de conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação no console XenMobile.

Requisitos do dispositivo para o desvio de bloqueio de ativação

- iOS 7.1 (versão mínima)
- Supervisionados por meio do Apple Configurator ou Apple DEP
- Configurado com uma conta do iCloud
- Buscar iPhone/iPad ativado
- Registrado no XenMobile
- A política de dispositivo de Opções do MDM, com o bloqueio de ativação habilitado, é implantada nos dispositivos

Para ignorar um bloqueio de ativação antes de emitir um apagamento completo de um dispositivo:

1. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
2. Apagar o dispositivo. A tela de bloqueio de ativação não aparece durante a configuração do dispositivo.

Para ignorar um bloqueio de ativação depois de emitir um apagamento completo de um dispositivo:

1. Redefinir ou apagar o dispositivo. A tela de bloqueio de ativação aparece durante a configuração do dispositivo.
2. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
3. Toque no botão Voltar no dispositivo. É exibida a tela de início.

Tenha em mente o seguinte:

- Aconselhe seus usuários a não desligar o Buscar iPhone/iPad. Não execute um apagamento completo a partir do dispositivo. Em ambos os casos, o usuário é solicitado a digitar a senha da conta do iCloud. Após a validação da conta, o usuário não verá uma tela Ativar iPhone/iPad depois de apagar todo o conteúdo e configurações.
- Para um dispositivo com um código de desvio do bloqueio de ativação gerado e com o bloqueio de ativação ativado: se você não pode ignorar a página Ativar iPhone/iPad após um apagamento completo, não é necessário excluir o dispositivo do XenMobile. Você ou o usuário pode entrar em contato com o suporte da Apple para desbloquear o dispositivo diretamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Durante um inventário de hardware, o XenMobile 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. Em seguida, para remover o código de desvio do dispositivo, envie a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile. Nesse ponto, o XenMobile Server e a Apple têm o código de desvio necessário para desbloquear o dispositivo.
- A ação de segurança Ignorar Bloqueio de Ativação utiliza a disponibilidade de um serviço Apple. Se a ação não funcionar, você pode desbloquear um dispositivo da seguinte maneira. No dispositivo, insira manualmente as credenciais da conta do iCloud. Ou deixe o campo do nome de usuário vazio e digite o código de desvio no campo da senha. Para ver o código de desvio, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Propriedades**. O **código de desvio do bloqueio de ativação** está em **Informações de segurança**.

Dispositivos compartilhados

April 15, 2019

O XenMobile permite configurar dispositivos que podem ser compartilhados por vários usuários. O recurso de dispositivos compartilhados permite que, por exemplo, médicos em hospitais usem qualquer dispositivo próximo para acessar aplicativos e dados, em vez de precisar transportar um dispositivo específico. Você também pode deslocar os trabalhadores em áreas como aplicação da lei, varejo e fabricação para compartilhar dispositivos para reduzir os custos com equipamentos.

Pontos principais sobre dispositivos compartilhados

Você pode usar qualquer um dos dispositivos iOS e Android compatíveis como dispositivos compartilhados. Para obter uma lista de dispositivos compatíveis, consulte Sistemas operacionais compatíveis de dispositivos.

Modo MDM

- Disponível em tablets e telefones iOS e Android. O registro básico no programa de registro de dispositivo (DEP) não é compatível com um dispositivo compartilhado do XenMobile Enterprise. Você deve usar um DEP autorizado para registrar um dispositivo compartilhado dessa maneira.
- Não há suporte para a autenticação de certificado de cliente, o PIN da Citrix, Touch ID, entropia de usuário e autenticação de dois fatores.

Modo MDM+MAM

- Disponível somente para tablets iOS e Android.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Autenticação de nome de usuário e senha do Active Directory apenas tem suporte.
- Não há suporte para a autenticação de certificado de cliente, o PIN da Worx, Touch ID, entropia de usuário e autenticação de dois fatores.
- O modo somente MAM não é compatível. Os dispositivos devem se registrar no MDM.
- Somente o Secure Mail, o Secure Web e o aplicativo móvel do ShareFile têm suporte. Os aplicativos HDX não são compatíveis.
- Os usuários do Active Directory são os únicos usuários compatíveis; os usuários e os grupos locais não são compatíveis
- O registro repetido é necessário para dispositivos compartilhados somente MDM existentes para atualização para o modo MDM+MAM.
- Os usuários não podem compartilhar aplicativos nativos nos dispositivos.
- Depois de baixados durante o primeiro registro, os aplicativos móveis de produtividade não são baixados novamente toda vez que um usuário faz login no dispositivo. O novo usuário pode escolher o dispositivo, fazer login e começar.
- No Android, para isolar os dados de cada usuário por motivos de segurança, a política **Não permitir dispositivos com root** no console XenMobile deve estar **ativada**.

Pré-requisitos para registrar dispositivos compartilhados

Antes de poder registrar dispositivos compartilhados, você deve fazer o seguinte:

- Crie uma função de usuário de registro de dispositivo compartilhado. Veja Configuração de funções com RBAC.
- Crie um usuário do dispositivo compartilhado. Veja Para adicionar, editar ou excluir contas de usuários.
- Crie um grupo de entrega que contenha as políticas, os aplicativos e as ações base que você deseja que sejam aplicados ao usuário de registro de dispositivo compartilhado. Veja Implantar recursos.

Pré-requisitos do modo MDM+MAM

1. Crie um grupo do Active Directory com o nome de **Assistente de registro de dispositivos compartilhados**.
2. Adicione a esse grupo os usuários do Active Directory que registrarão dispositivos compartilhados. Se você desejar uma nova conta para esse fim, crie um novo usuário do Active Directory (por exemplo, **sdenroll**) e adicione-o ao grupo do Active Directory.

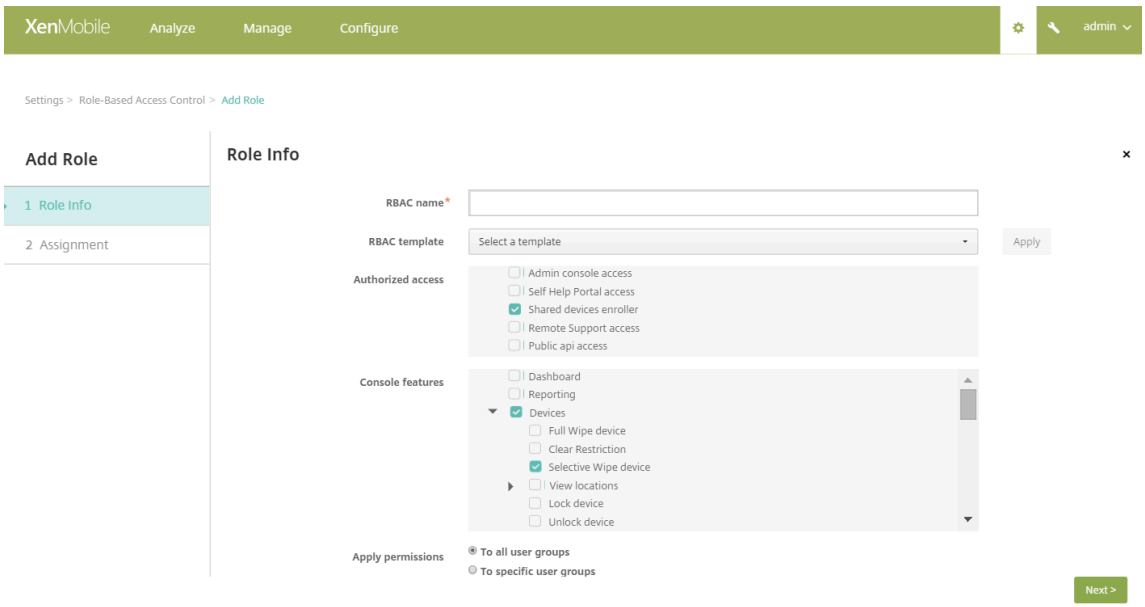
Configuração de um dispositivo compartilhado

Siga estas etapas para configurar um dispositivo compartilhado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

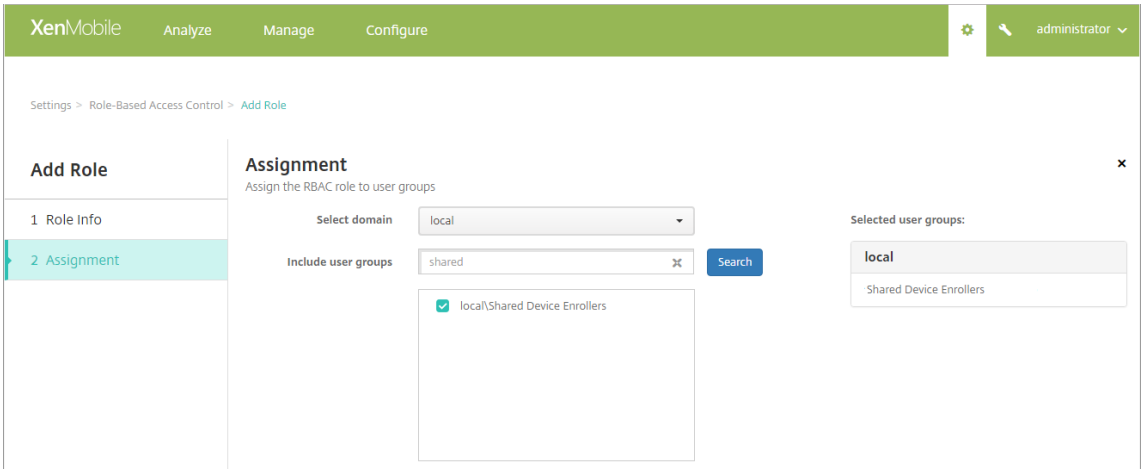
1. No console XenMobile, clique na engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **Controle de acesso baseado em função** e clique em **Adicionar**. A tela **Adicionar função** é exibida.
3. Crie uma função de usuário de registro de dispositivo compartilhado chamada **Usuário de registro de dispositivo compartilhado** com permissões de **Assistente de registro de dispositivos compartilhados** em **Acesso autorizado**. Não se esqueça de expandir **Dispositivos** nos **Recursos do console** e selecionar **Apagamento seletivo do dispositivo**. Essa configuração garante que os aplicativos e as políticas provisionadas por meio da conta do assistente de registro de dispositivos compartilhados sejam excluídos por meio do Secure Hub quando o registro do dispositivo é cancelado.

   Em **Aplicar Permissões**, mantenha a configuração padrão, **Para todos os grupos de usuários**, ou atribua permissões a grupos de usuários específicos do Active Directory com **Para grupos de usuários específicos**.

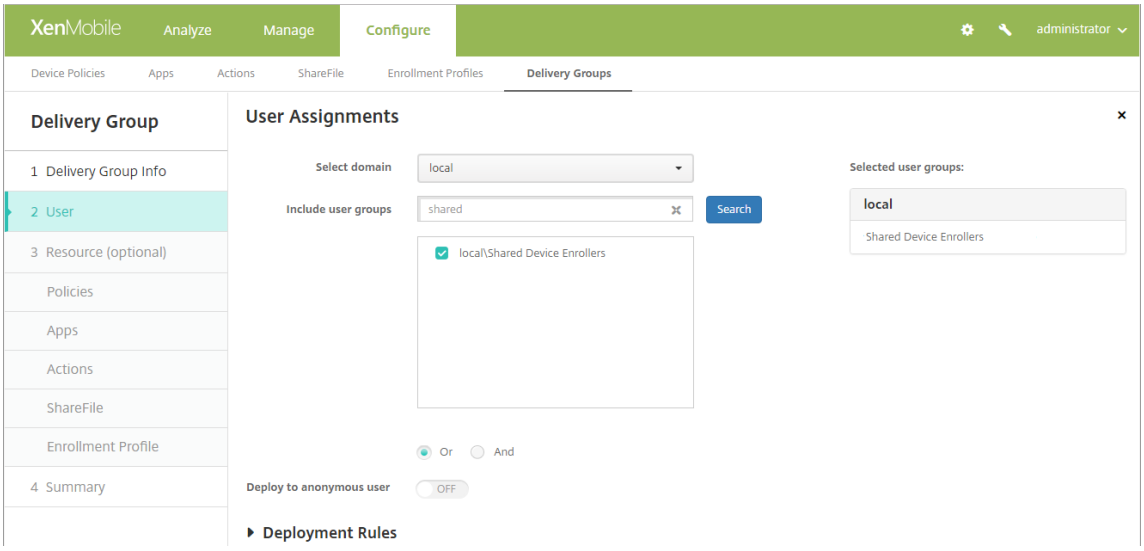


   Clique em **Avançar** para ir para a tela **Atribuição**. Atribua a função de registro de dispositivo compartilhado que você acabou de criar ao grupo do Active Directory que você criou para os usuários de registro de dispositivos compartilhados na Etapa 1, em Pré-requisitos. Na imagem abaixo, **citrix.lab** é o domínio do Active Directory e o **Shared Device Enrollers** é o grupo do Active Directory.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Crie um grupo de entrega que contenha as políticas, os aplicativos e as ações base que você deseja aplicar ao dispositivo quando um usuário não está conectado e, em seguida, associe esse grupo de entrega ao grupo do Active Directory do usuário de registro de dispositivo compartilhado.



5. Instale o Secure Hub no dispositivo compartilhado e registre-o no XenMobile usando a conta de usuário de registro de dispositivo compartilhado. Agora você pode exibir e gerenciar o dispositivo por meio do console XenMobile. Para obter mais informações, consulte Registrar dispositivos.

6. Para aplicar diferentes políticas ou fornecer mais aplicativos aos usuários autenticados, você deve criar um grupo de entrega associado a esses usuários e implantado somente em dispositivos compartilhados. Quando você criar os grupos, configure regras de implantação para garantir que os pacotes sejam implantados em dispositivos compartilhados. Para obter mais informações, consulte Implantar recursos.

7. Para interromper o compartilhamento do dispositivo, realize um apagamento seletivo para re-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

mover a conta de usuário de registro de dispositivo compartilhado do dispositivo, juntamente com todas as políticas e os aplicativos implantados nele.

Experiência do usuário de dispositivos compartilhados

Modo MDM

Os usuários veem somente os recursos disponíveis para eles e têm a mesma experiência em todos os dispositivos compartilhados. As políticas de registro e os aplicativos do dispositivo compartilhado sempre permanecem no dispositivo. Quando um usuário que não está registrado em dispositivos compartilhados faz login no Secure Hub, as políticas e os aplicativos dessa pessoa são implantados no dispositivo. Quando o usuário faz logout, as políticas e os aplicativos que são diferentes daqueles do registro de dispositivo compartilhado são removidos, enquanto que os recursos do registro de dispositivo compartilhado permanecem intactos.

Modo MDM+MAM

O Secure Mail e o Secure Web são implantados no dispositivo quando registrados pelo usuário de registro de dispositivo compartilhado. Os dados do usuário são mantidos de forma protegida no dispositivo. Os dados não são expostos para outros usuários quando eles fazem login no Secure Mail e no Secure Web.

Somente um usuário por vez pode fazer login no Secure Hub. O usuário anterior deve fazer logout antes que o próximo usuário possa fazer login. Por motivos de segurança, o Secure Hub não armazena as credenciais do usuário em dispositivos compartilhados, portanto, os usuários devem digitar as credenciais deles sempre que fizerem login. Para garantir que um novo usuário não possa acessar os recursos direcionados para o usuário anterior, o Secure Hub não permite que novos usuários façam login enquanto as políticas, os aplicativos e os dados associados ao usuário anterior estão sendo removidos.

O registro de dispositivo compartilhado não altera o processo de atualização de aplicativos. Você pode enviar por push atualizações para os usuários de dispositivo compartilhado como sempre, e os usuários de dispositivo compartilhado podem atualizar aplicativos diretamente nos dispositivos deles.

Políticas recomendadas do Secure Mail

- Para o melhor desempenho do Secure Mail, defina **Max sync period** com base no número de usuários que compartilharão o dispositivo. Não é recomendável permitir a sincronização ilimitada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Número de usuários compartilhando o dispositivo	Período máximo recomendado de sincronização
21 a 25	1 semana ou menos
6 a 20	2 semanas ou menos
5 ou menos	1 mês ou menos

- Bloqueie **Enable contact export** para evitar a exposição dos contatos de um usuário a outros usuários que compartilham o dispositivo.
- No iOS, somente as configurações a seguir podem ser definidas por usuário. Todas as outras configurações serão comuns entre os usuários que compartilham o dispositivo:
  - Notificações
  - Assinatura
  - Ausência Temporária
  - Período de Sincronização de Email
  - S/MIME
  - Verificar ortografia

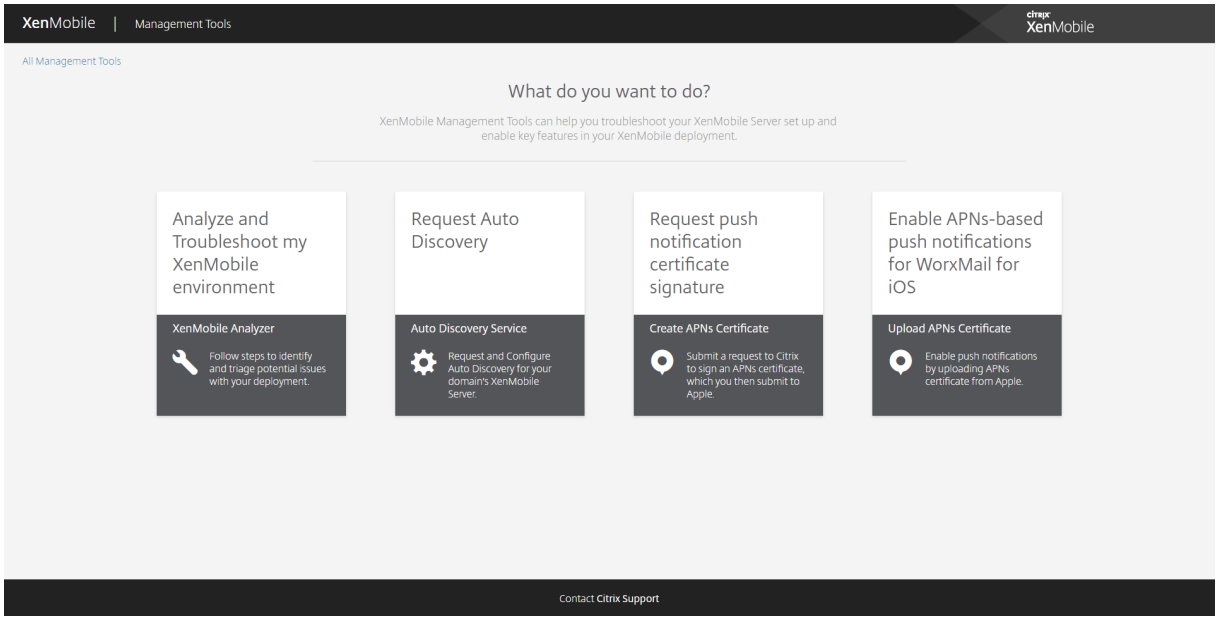
XenMobile Autodiscovery Service

April 15, 2019

A detecção automática é uma parte importante de várias implantações XenMobile. A detecção automática simplifica o processo de registro dos usuários. Eles podem usar os nomes do usuário da respectiva rede e as senhas do Active Directory para registrar os dispositivos deles, em vez de precisar também inserir detalhes sobre o servidor XenMobile. Os usuários inserem o nome do usuário no formato de nome UPN; por exemplo, usuario@minhaempresa.com. O XenMobile AutoDiscovery Service permite a você a criar ou editar um registro de detecção automática ajuda do suporte da Citrix.

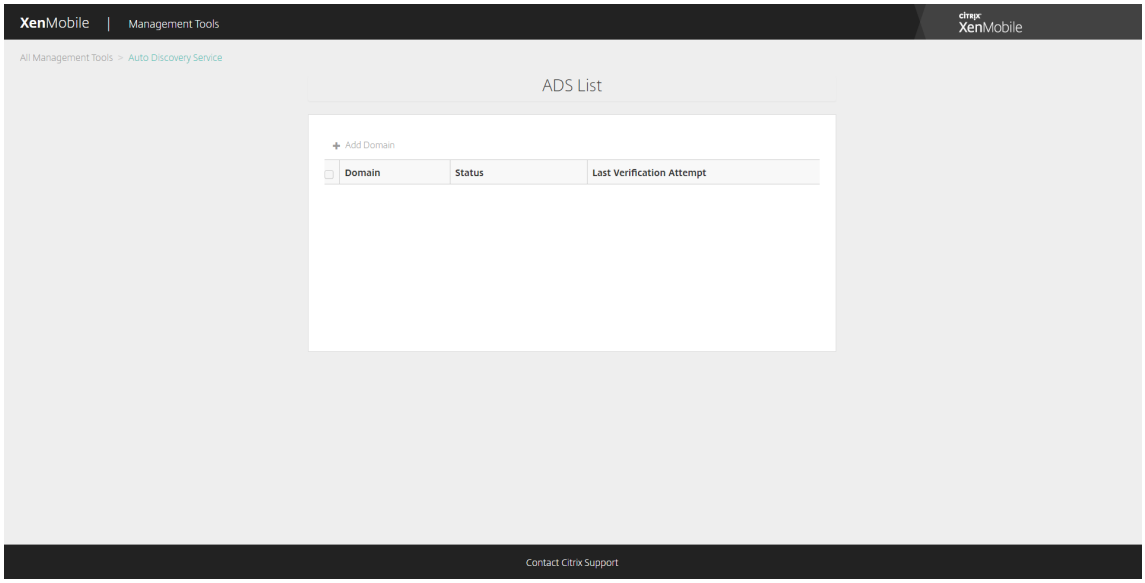
Para acessar o XenMobile AutoDiscovery Service, navegue até https://xenmobiletools.citrix.com e clique em **Request Auto Discovery**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



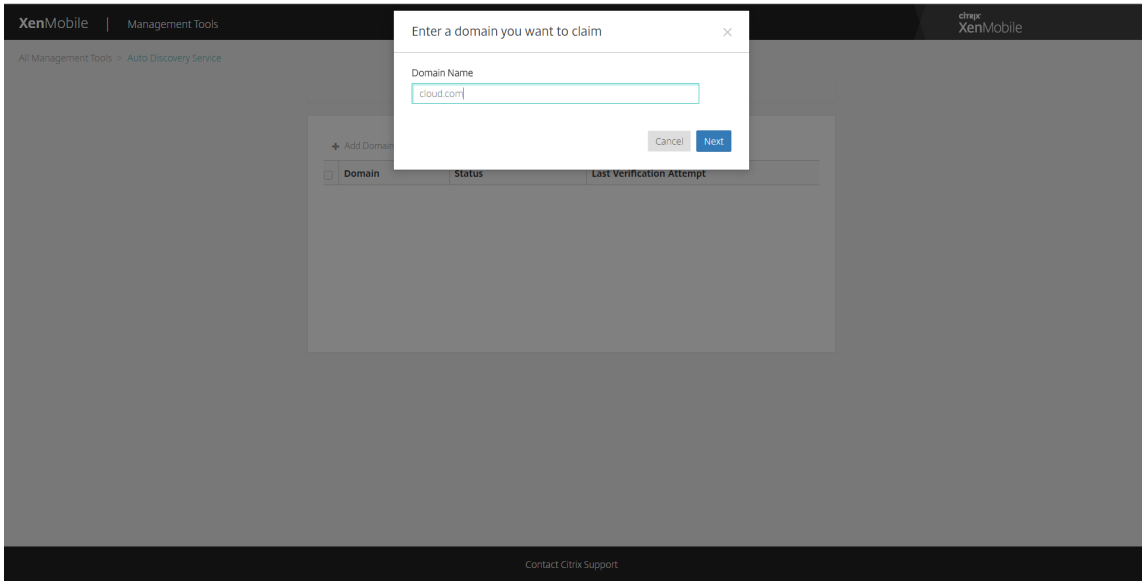
Solicitação de AutoDiscovery

1. Na página AutoDiscovery Service, você deverá primeiramente solicitar um domínio. Clique em **Add Domain**.



2. Na caixa de diálogo exibida, insira o nome do domínio do seu ambiente XenMobile e, em seguida, clique em **Next**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. A próxima etapa fornece instruções para verificar se você possui o domínio.

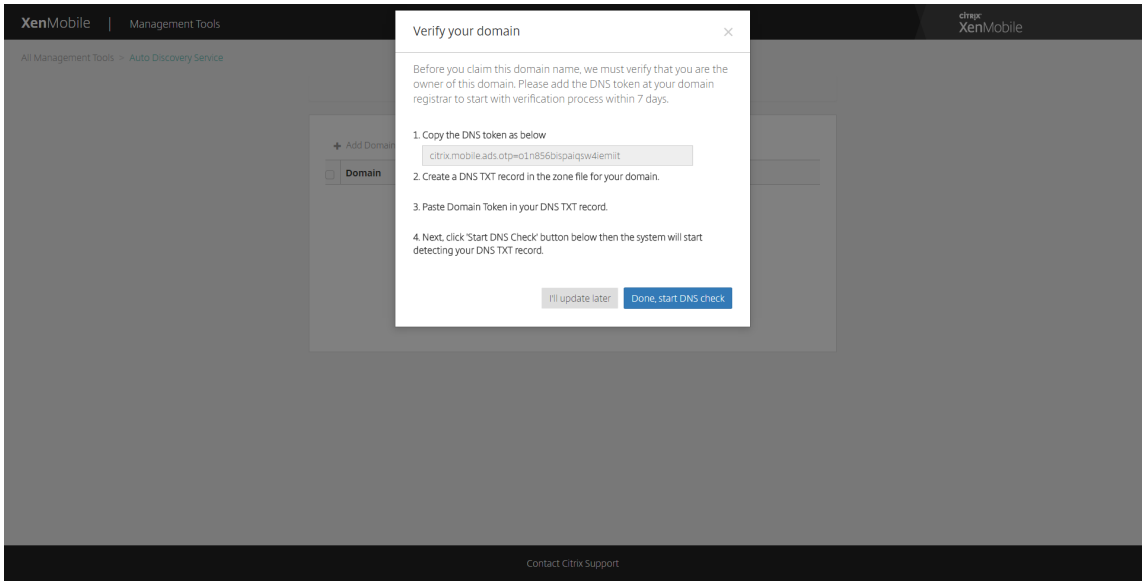
   - Copie o token de DNS fornecido no Portal do XenMobile Tools.
   - Crie um registro TXT de DNS no arquivo de zona para o seu domínio no portal do provedor de hospedagem do seu domínio.

     Para criar um registro TXT DNS você precisa para fazer logon no portal do provedor de hospedagem de domínio para o domínio que você adicionou na etapa 2 acima. No portal de hospedagem de domínio você pode editar os seus registros de servidor de nomes de domínio e adicionar um registro TXT personalizado. Abaixo está um exemplo de adição de uma entrada TXT de DNS em um portal de hospedagem para o domínio de exemplo domain.com.
   - Cole o Token de Domínio no seu registro TXT de DNS e salve seu registro de servidor de nome de domínio.
   - De volta ao Portal do XenMobile Tools, clique em **Done** para começar a verificação.

   O sistema detecta o registro TXT de DNS. Como alternativa, você pode clicar em **I'll update later** e o registro será salvo. A verificação de DNS não será iniciada até que você selecione o registro Waiting e clique em **DNS Check**.

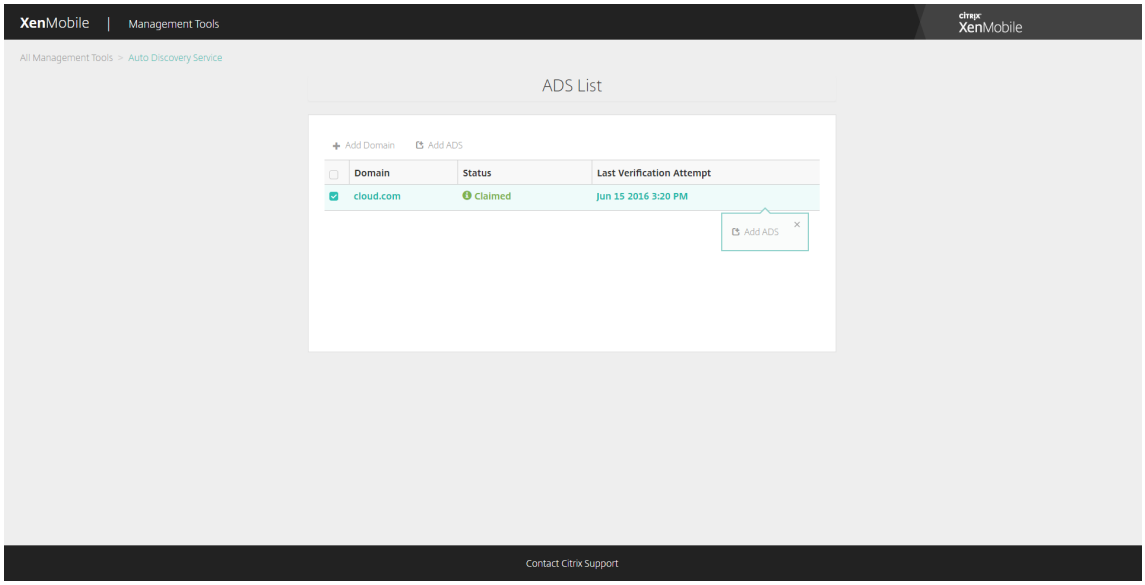
   O ideal é que esta verificação leve cerca de uma hora, mas pode levar até dois dias para retornar uma resposta. Além disso, talvez você precise sair do portal e retornar para ver a alteração de status.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



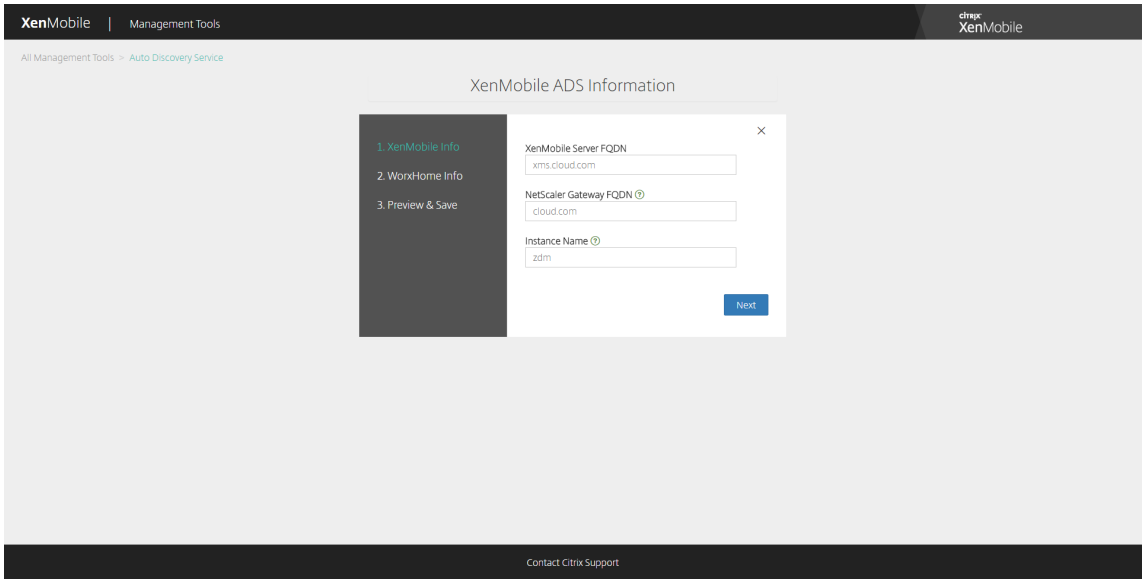
4. Depois que você solicitar o seu domínio, poderá inserir informações do AutoDiscovery Service. Clique com o botão direito do mouse no registro de domínio para o qual deseja solicitar a descoberta automática e clique em **Add ADS**.

   Se o seu domínio já possui um registro de AutoDiscovery, registre uma ocorrência com o Suporte Técnico da Citrix para modificar detalhes conforme necessário.



5. Insira o **XenMobile Server FQDN**, o **NetScaler Gateway FQDN** e o **Instance Name** e, em seguida, clique em **Next**. Se você não tiver certeza, adicione uma instância padrão do “zdm”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Na captura de tela anterior, observe que o Worx Home agora é chamado de Secure Hub.

6. Insira as informações a seguir para o Secute Hub e, em seguida, clique em **Next**.

   - **User ID Type:** selecione o tipo de ID com o qual o usuário faz login como **E-mail address** ou **UPN**.

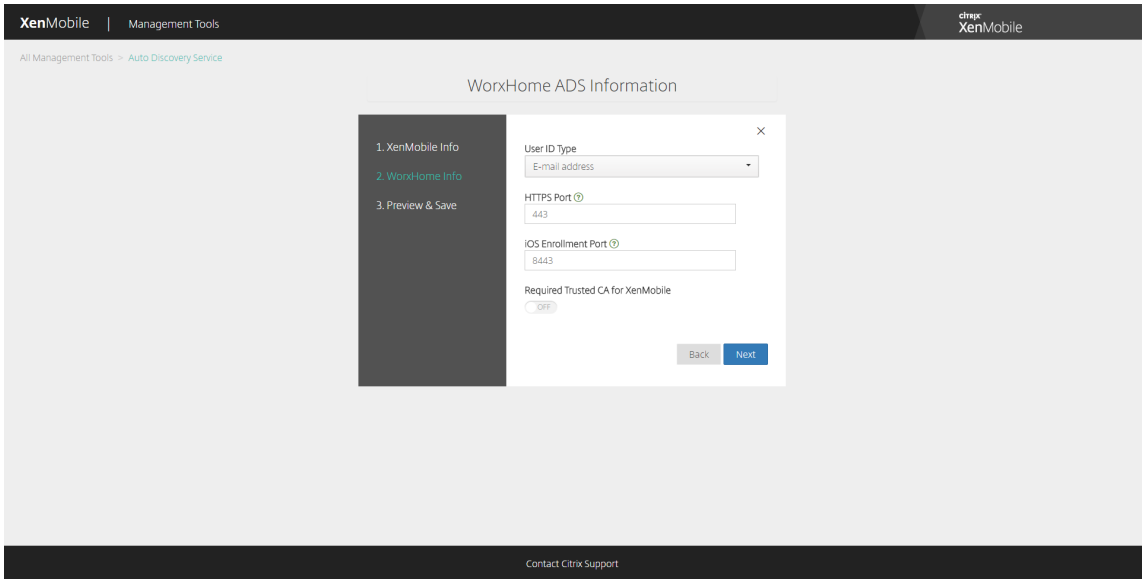
     UPN é usado quando o UPN do usuário (Nome Principal do Usuário) é o mesmo que o endereço de email. Ambos os métodos usam o domínio fornecido para localizar o endereço do servidor. Com o **E-mail address**, o usuário será solicitado a digitar seu nome de usuário e senha, e com o **UPN**, ele será solicitado a digitar sua senha.

   - **HTTPS Port:** digite a porta usada para acessar o Secure Hub sobre HTTPS. Em geral, é a porta 443.

   - **iOS Enrollment Port:** digite a porta usada para acessar o Secure Hub para registro de iOS. Em geral, é a porta 8443.

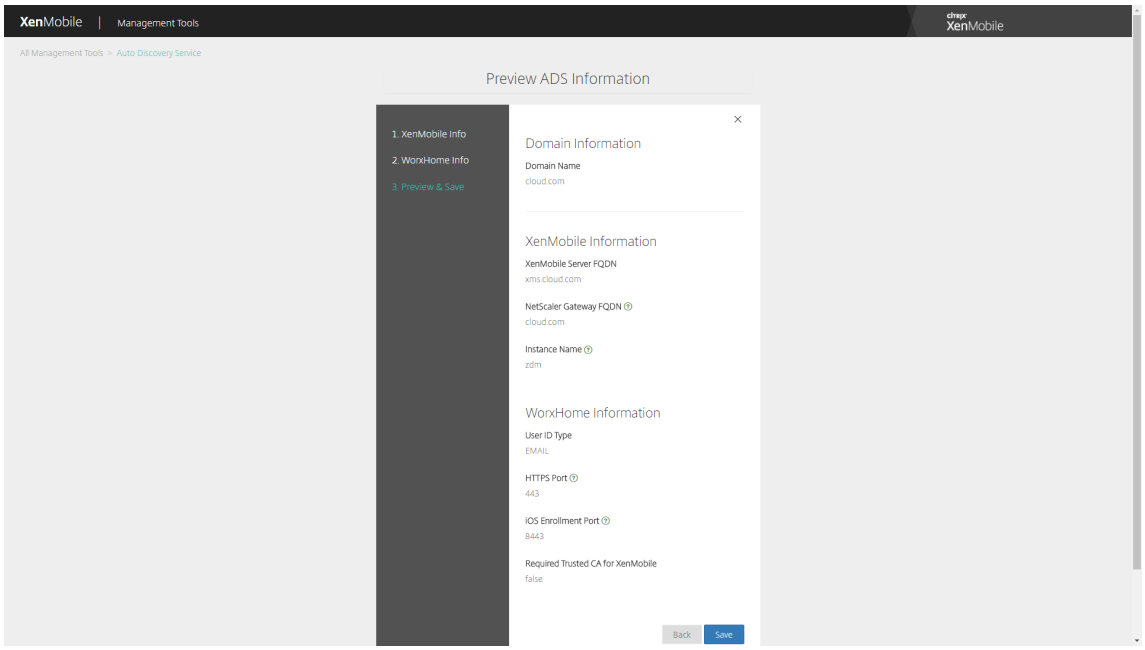
   - **Required Trusted CA for XenMobile:** indica se é ou não obrigatório um certificado confiável para acessar o XenMobile. Esta opção pode ser **OFF** ou **ON**. No momento, não existe a capacidade de carregar um certificado para este recurso. Se quiser usar certificados confiáveis para XenMobile, você precisa chamar o Suporte Citrix. Para saber mais sobre a fixação de certificado, consulte a seção sobre Certificate Pinning no tópico Secure Hub na documentação dos aplicativos móveis de produtividade. Para ler sobre as portas necessárias para que o certificate pinning funcione, consulte o artigo de suporte XenMobile Port Requirements for ADS Connectivity.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> Nota:
>
> Na captura de tela anterior, observe que o Worx Home agora é chamado de Secure Hub.

7. Um resumo da página exibe todas as informações que você inseriu nas etapas anteriores. Verifique se os dados estão corretos e clique em **Save**.



> Nota:
>
> Na captura de tela anterior, observe que o Worx Home agora é chamado de Secure Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de dispositivo

April 15, 2019

Você pode configurar como o XenMobile interage em seus dispositivos por meio de políticas. Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. Como resultado, você poderá encontrar diferenças entre plataformas e até mesmo entre dispositivos com Android de diferentes fabricantes.

Para obter uma descrição resumida de cada política de dispositivo, consulte Resumos de políticas de dispositivo neste artigo.

> Nota:
>
> Se o seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):
>
> Quando você configurar políticas de dispositivo do XenMobile para o Windows 10, lembre-se da regra a seguir. Se uma política em um ou mais dispositivos Windows 10 registrados for conflitante, a política alinhada ao GPO terá precedência.

Para ver quais políticas às quais o Android for Work dá suporte, consulte Android for Work.

Pré-requisitos

- Crie os grupos de entrega que você planeja usar.
- Instale todos os certificados AC necessários.

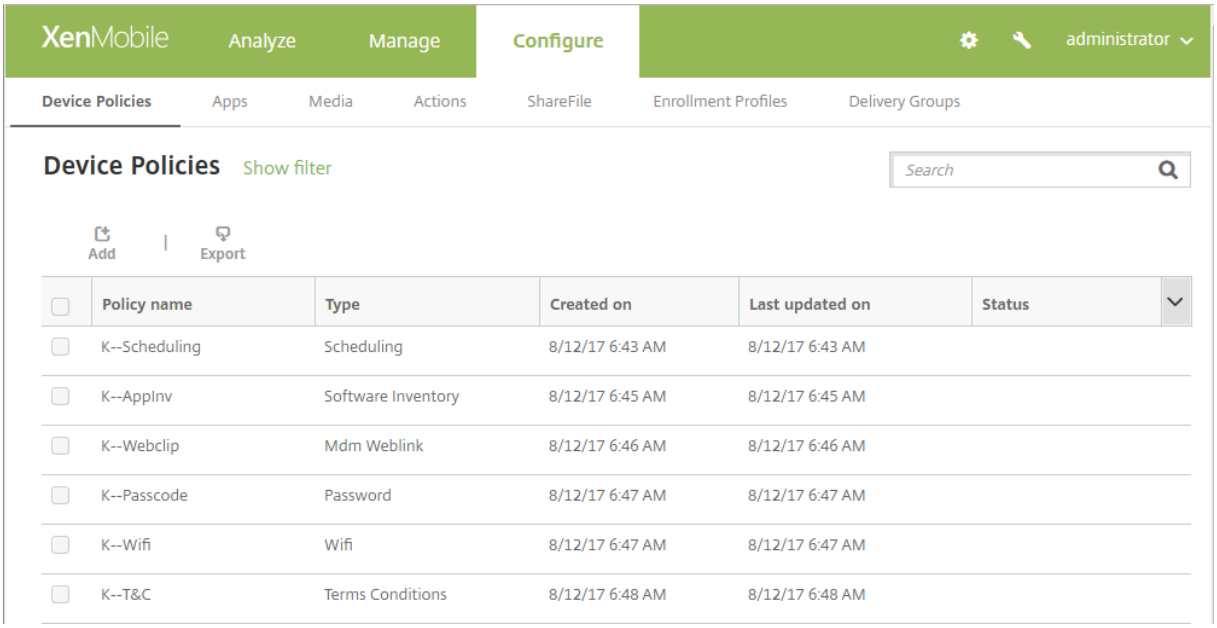
Adicionar uma política de dispositivo

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 cronograma de implantação (opcional).

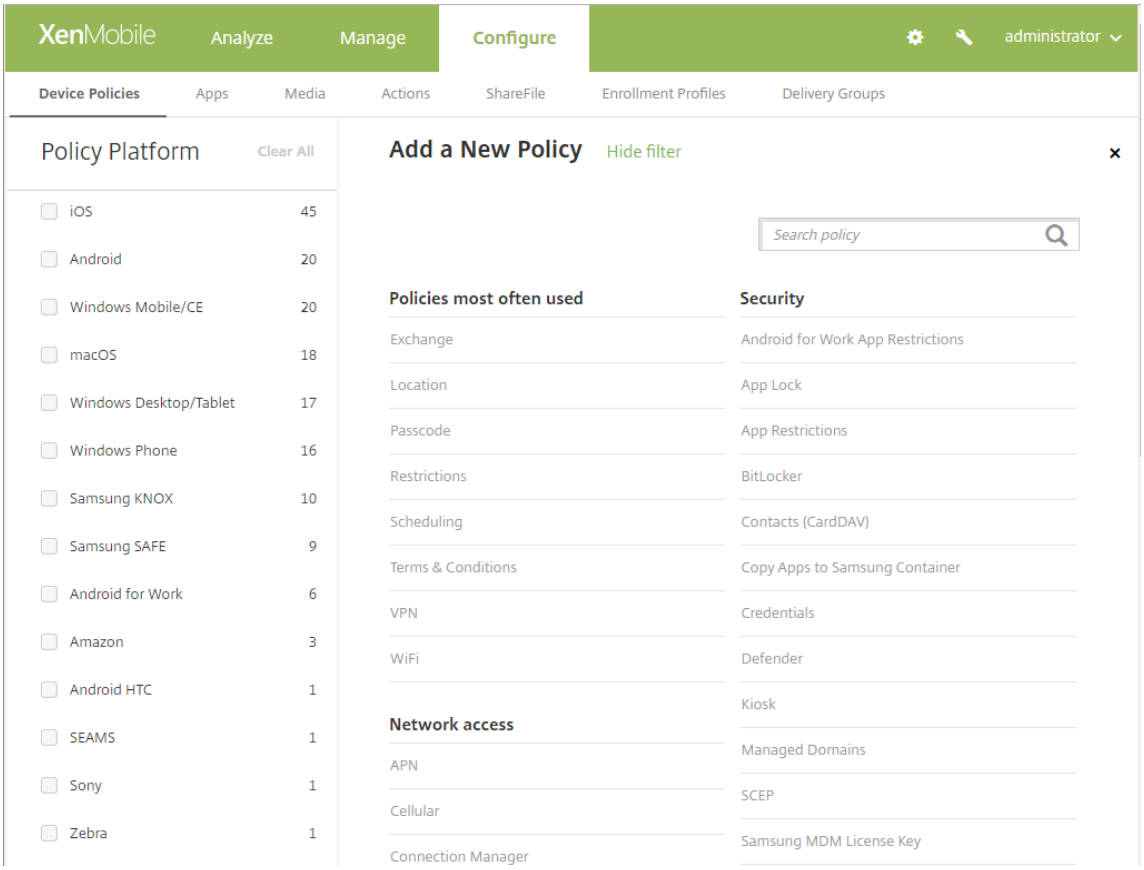
Para criar e gerenciar políticas de dispositivos, acesse **Configurar > Políticas de dispositivo**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para adicionar uma política:

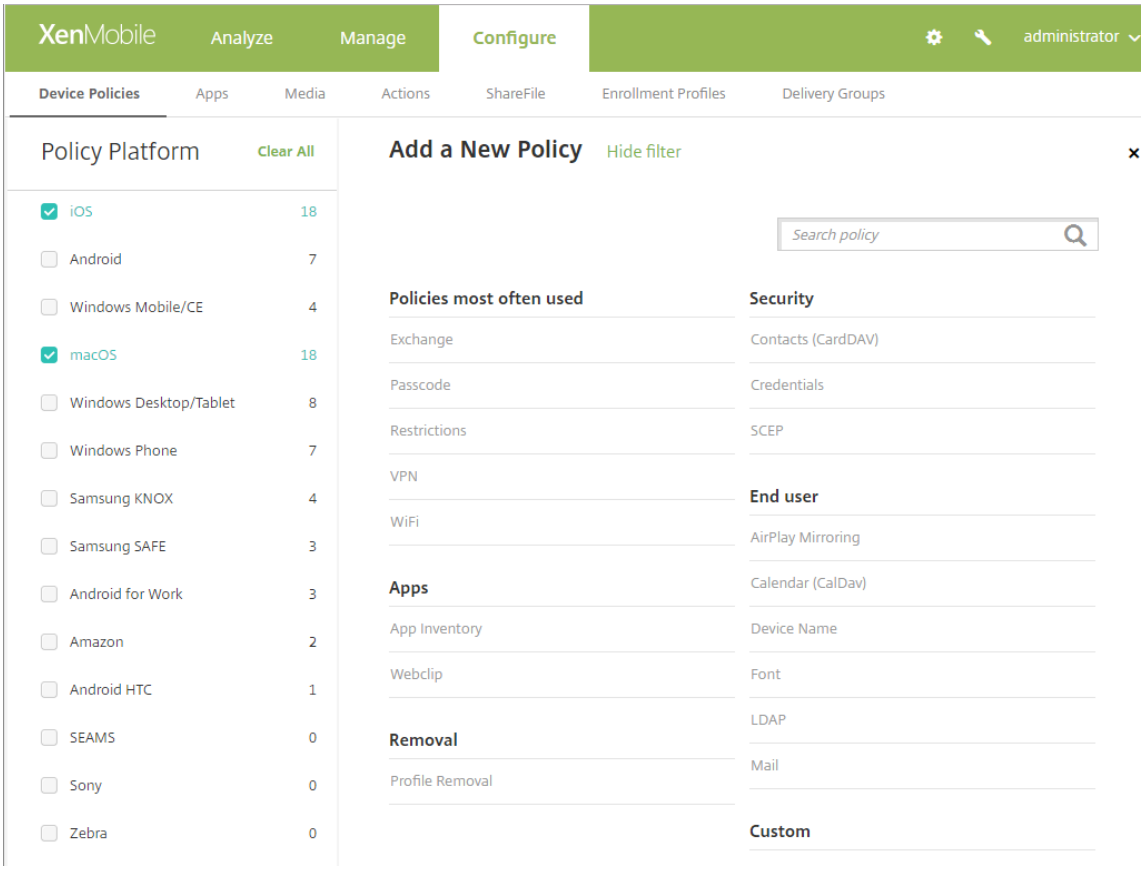
1. Na página **Políticas de dispositivo**, clique em **Adicionar**. A página **Adicionar uma Nova Política** é exibida.



2. Clique em uma ou mais plataformas para exibir uma lista das políticas de dispositivo para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 são exibidas. Se a sua política estiver na lista, clique nela. Somente a política selecionada permanece nos resultados. Clique nela para abrir a página **Informações sobre a política** referente a essa política.

3. Selecione as plataformas que você deseja incluir na política. As páginas de configuração das plataformas selecionadas são exibidas na Etapa 5.
4. Preencha a página **Informações sobre a política** e clique em **Avançar**. A página **Informações sobre a política** reúne as informações, como o nome da política, para ajudá-lo a identificar e rastrear as políticas. Essa página é semelhante para todas as políticas.
5. Preencha as páginas de plataforma. As páginas de plataforma são exibidas para cada plataforma selecionada na Etapa 3. Essas páginas são diferentes para cada política. Uma política pode ser diferente entre as 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 de lixeira no lado direito. Na caixa de diálogo de confirmação, clique em **Excluir**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 cronograma

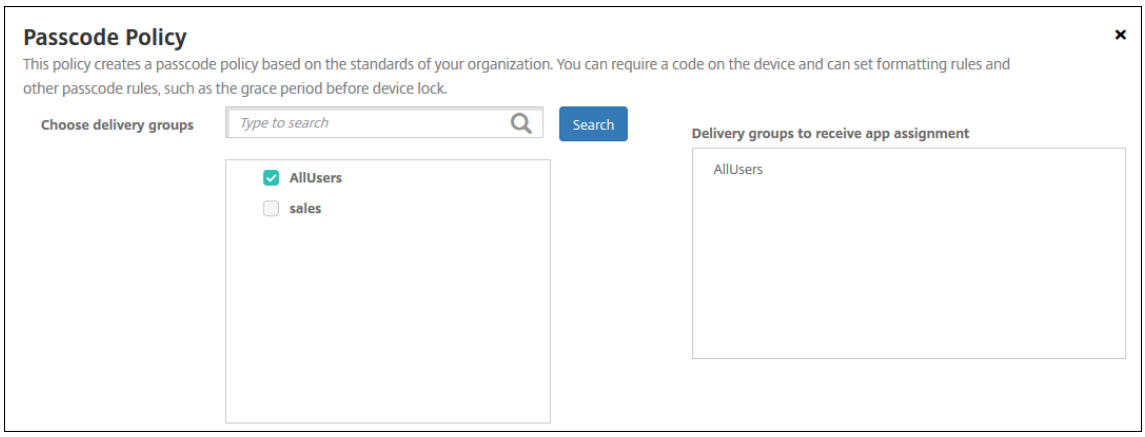
Para obter mais informações sobre como configurar as regras de implantação, incluindo ilustrações, consulte Implantar recursos.

1. Na página da plataforma, expanda **Regras de implantação** e defina estas configurações: A guia **Base** é exibida 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 **Tudo**.
   - 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 você desejar adicionar mais condições. Você pode adicionar quantas condições desejar.
2. Clique na guia **Avançado** para combinar as regras com as opções boolianas. As condições que você escolheu na guia **Base** são exibidas.
3. Você pode usar a lógica booliana mais avançada para combinar, editar ou adicionar regras.
   - Clique em **AND**, **OR** ou **NOT**.
   - Nas listas, selecione 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, clique para selecionar uma condição e, em seguida, clique em **EDITAR** para alterar a condição ou em **Excluir** para removê-la.
   - Clique em **Nova regra** para adicionar outra condição.
4. Clique em **Avançar** para ir até a próxima página de plataforma ou, quando todas as páginas da plataforma estiverem preenchidas, até 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 será exibido na caixa **Grupos de entrega que receberão a atribuição de aplicativos**.

   Grupos de entrega que receberão a atribuição de aplicativos não aparece até que você selecione um grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

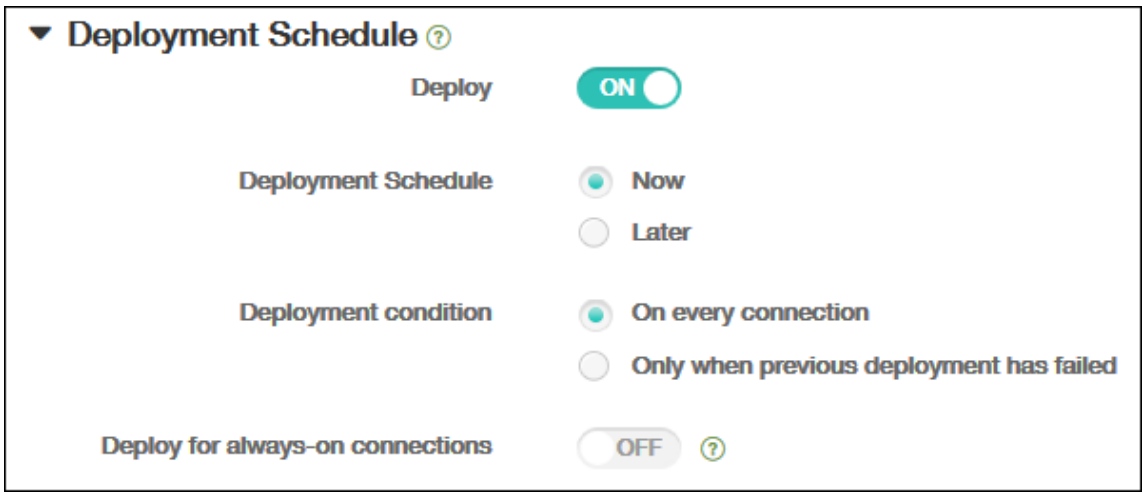


6. Na página **Atribuições**, expanda o **Cronograma de implantação** e depois defina as seguintes configurações:

   - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
   - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
   - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
   - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
   - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

     > Nota:
     >
     > Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
     >
     > O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

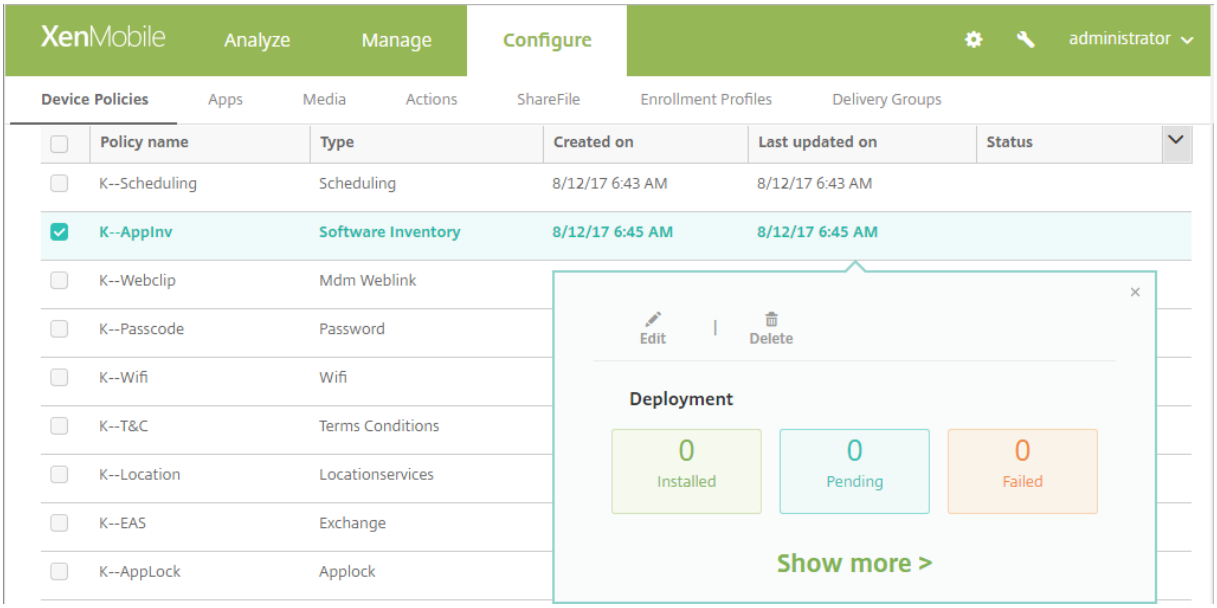


7. Clique em **Salvar**.

   A política é exibida na tabela **Políticas de dispositivo**.

Editar ou excluir uma política de dispositivo

Para editar ou excluir uma política, selecione a caixa de seleção ao lado de uma política para mostrar o menu de opções acima da lista de políticas. Ou clique em uma política na lista para exibir o menu de opções no lado direito da lista.



Para exibir os detalhes da política, clique em **Mostrar mais**.

Para editar as configurações de uma política de dispositivo, clique em **Editar**.

Se você clicar em **Excluir**, é exiba uma caixa de diálogo de confirmação. Clique em **Excluir** novamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 dispositivo de desinstalação do XenMobile. Para obter informações, consulte Política de dispositivo de desinstalação 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 resto das políticas e o perfil permanecem no dispositivo. Para obter informações, consulte Política de dispositivo de remoção de perfil.

- Windows 10

  Você não pode remover diretamente uma política de dispositivo de um dispositivo Desktop ou Tablet com Windows 10. No entanto, você pode usar um dos seguintes métodos:

  - Cancelar o registro do dispositivo e, em seguida, enviar por push um novo conjunto de políticas para o dispositivo. Depois, os usuários se registram novamente para continuar.
  - Enviar uma ação de segurança por push para limpar 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 por push. Depois, os usuários se registram novamente para continuar.

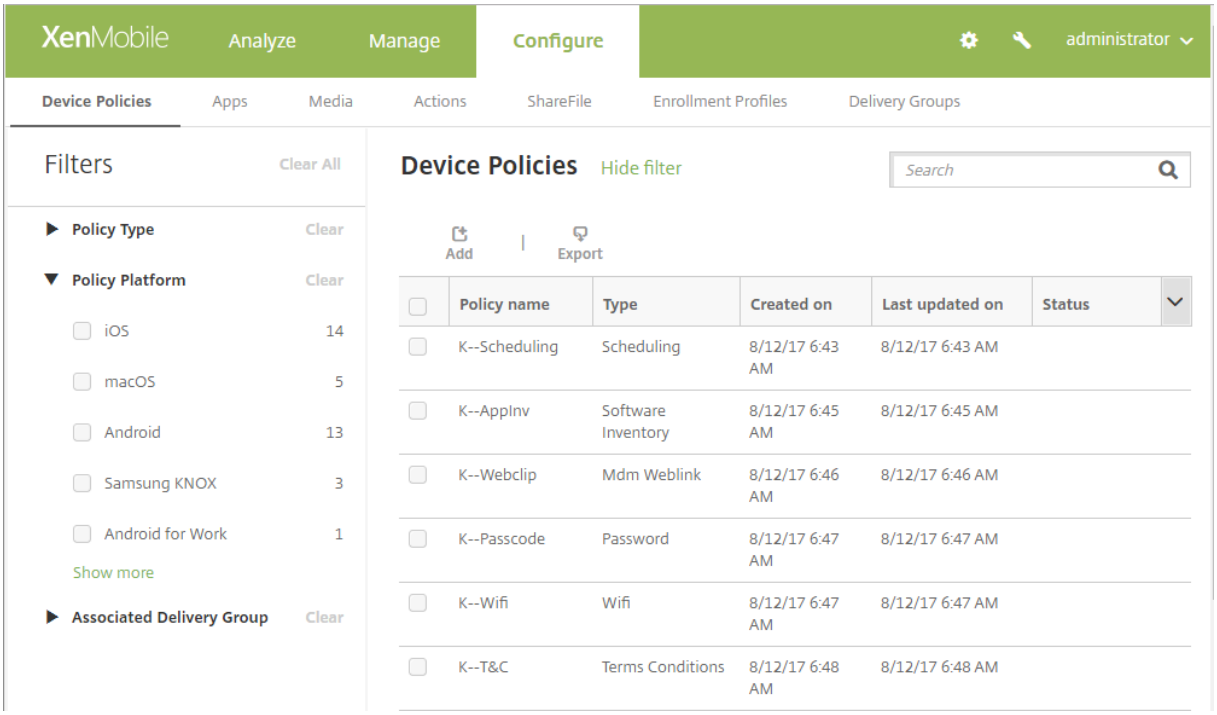
- SO Chrome

  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 por push.

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 dispositivos**, clique em **Mostrar Filtro**. Na lista, selecione as caixas de seleção relativas aos itens que deseja ver.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Clique em **SALVAR ESTA EXIBIÇÃO** para salvar um filtro. O nome do filtro, em seguida, é exibida 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 de AirPlay	Adiciona dispositivos AirPlay específicos (como o Apple TV ou outro computador Mac) aos dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista branca de dispositivos supervisionados. Essa opção limita os usuários a apenas os dispositivos AirPlay na lista branca.
AirPrint	Adiciona impressoras AirPrint à lista de impressoras AirPrint nos dispositivos iOS. Essa política facilita o suporte aos ambientes nos quais as impressoras e os dispositivos estão em sub-redes diferentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Permissões do aplicativo Android for Work	Configura como as solicitações para aplicativos do Android for Work nos perfis de trabalho lidam com o que o Google chama de permissões “perigosas”.
Restrições de aplicativo Android for Work	Atualiza as restrições associadas aos aplicativos Android.
APN	Determina as configurações usadas para conectar os seus dispositivos ao General Packet Radio Service (GPRS) de uma operadora de telefonia específica. Essa configuração já está definida na maioria dos novos telefones. Use essa política se sua organização não usar um APN de consumidor para conexão com a Internet de um dispositivo móvel.
Acesso aos aplicativos	Define uma lista dos aplicativos necessários, opcionais ou evitados no dispositivo. Você pode criar uma ação automatizada para reagir à conformidade do dispositivo com essa lista de aplicativos.
Atributos de aplicativo	Especifica atributos, como o ID d eum pacote de aplicativo gerenciado ou um identificador de VPN por aplicativo, para dispositivos iOS.
Configuração do aplicativo	Define remotamente várias configurações e comportamentos de aplicativos que dão suporte à configuração gerenciada. Para fazer isso, você deve implantar um arquivo de configuração XML (chamado de lista de propriedades, ou plist) nos dispositivos iOS. Ou você pode implantar pares de chave/valor no Windows 10 phone, área de trabalho ou dispositivos de tablet.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Inventário de aplicativos	Coleta um inventário dos aplicativos em dispositivos gerenciados. O XenMobile compara então o inventário com todas políticas de acesso aos aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que estão em uma lista negra ou branca de acesso de aplicativos e tomar as respectivas providências.
Bloqueio de aplicativo	Define uma lista de aplicativos que os usuários podem ou não executar em determinados dispositivos Android ou iOS.
Uso de rede de aplicativos	Define regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares, nos dispositivos iOS. As regras se aplicam somente aos aplicativos gerenciados. Os aplicativos gerenciados são aqueles que você implanta nos dispositivos de usuários por meio do XenMobile.
Restrições de aplicativo	Cria listas negras de aplicativos que você deseja impedir que os usuários instalem em dispositivos Samsung KNOX. Você também pode criar listas brancas de aplicativos que você deseja permitir que os usuários instalem.
Desinstalação de aplicativo	Remova aplicativos dos dispositivos do usuário.
Restrições de desinstalação de aplicativo	Especifica os aplicativos que os usuários podem ou não desinstalar.
Notificações de aplicativos	Controla como os usuários do iOS recebem notificações de aplicativos especificados.
BitLocker	Ajusta as configurações disponíveis na interface do BitLocker em dispositivos Windows 10.
Navegador	Define se os dispositivos dos usuários podem usar o navegador ou quais funções de navegador os dispositivos podem usar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
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 compatível com CalDAV.
Celular	Define as configurações de rede celular.
Gerenciador de conexões	Especifica as configurações de conexão dos aplicativos que se conectam automaticamente à Internet e a redes privadas. Essa política está disponível somente em Windows Pocket PCs.
Contatos (CardDAV)	Adiciona uma conta de contato do iOS (CardDAV) a dispositivos iOS ou macOS. A conta CardDAV permite que os usuários sincronizem dados de contato com qualquer servidor compatível com CardDAV.
Controlar atualizações do sistema operacional	Implanta as mais recentes atualizações de sistema operacional em dispositivos supervisionados com suporte.
Copiar aplicativos para o contêiner da Samsung	Copia os aplicativos que já estão instalados em um dispositivo para um contêiner SEAMS ou para um contêiner KNOX em dispositivos Samsung com suporte. Os aplicativos copiados para o contêiner do SEAMS estão disponíveis na tela inicial do dispositivo. Os aplicativos copiados para o contêiner KNOX ficam disponíveis somente quando os usuários fazem login no contêiner KNOX.
Credenciais	Permite que autenticação integrada com sua configuração de 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 do dispositivo, configuração do dispositivo e gerenciamento de falhas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Defender	Define configurações do Windows Defender no Windows 10 para desktop e tablet.
Excluir arquivos e pastas	Exclui arquivos e pastas específicos dos dispositivos Windows Mobile/CE.
Excluir chaves e valores do registro	Exclui chaves e valores específicos do registro dos dispositivos Windows Mobile/CE.
Atestado de integridade de dispositivo	Requer que os dispositivos Windows 10 informem o estado da sua integridade. Para que eles 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 envia para o XenMobile. Quando o XenMobile recebe o Certificado de Atestado de Integridade, com base no conteúdo daquele certificado, ele pode implantar ações automáticas que você configurou.
Nome do dispositivo	Define os nomes em dispositivos iOS e macOS para que você possa identificá-los. Você pode usar macros, texto ou uma combinação de ambos para definir um nome de dispositivo.
Configuração de educação	Configura os dispositivos de instrutor e estudante para uso com o Apple Educação. Se os instrutores usam o aplicativo de Sala de Aula, é necessária a política do dispositivo Configuração de Educação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Hub empresarial	Distribui aplicativos a Windows Phones por meio da loja Enterprise Hub Company. O XenMobile é compatível somente com uma política do Hub Empresarial para um modo do Secure Hub para Windows Phone. Por exemplo, não crie várias políticas do Hub Empresarial com versões diferentes do Secure Home para XenMobile Enterprise Edition. Você pode implantar a política inicial do Hub Empresarial somente durante registro do dispositivo.
Exchange	Ativa os emails do ActiveSync para o cliente de email nativo no dispositivo.
Arquivos	Adiciona os arquivos de script ao XenMobile que executam determinadas funções para usuários. Ou você pode adicionar arquivos de documento que deseja que os usuários do dispositivo Android tenham acesso em seus dispositivos. Quando você adiciona o arquivo, pode também especificar o diretório no qual deseja que o arquivo seja armazenado no dispositivo.
FileVault	Esta política permite que você ative a criptografia do dispositivo FileVault em dispositivos macOS registrados. Você também pode controlar o número de vezes que um usuário pode ignorar a configuração do FileVault durante o logon. Disponível para macOS 10.7 ou versões posteriores.
Firewall	Define as configurações de firewall Você fornece os endereços IP, as portas e os nomes de host que desejar permitir ou bloquear nos dispositivos. Você também pode definir o proxy e as configurações de redirecionamento do proxy.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Fonte	Adiciona mais fontes para dispositivos iOS e macOS. As fontes devem ser TrueType (.TTF) ou OpenType (.OFT). O XenMobile não dá 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 iOS 9.3 e versões posteriores.
Importar perfil de iOS e macOS	Importa arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém as políticas de segurança do dispositivo e as restrições que você prepara por meio do Apple Configurator.
Quiosque	Restringe o uso do aplicativo em dispositivos Samsung SAFE. Você pode limitar os aplicativos disponíveis a um ou mais aplicativos específicos. Essa política é útil para dispositivos corporativos que foram criados para executar somente um tipo ou classe específico de aplicativos. Esta política também permite que você escolha imagens personalizadas para a tela inicial do dispositivo e papéis de parede de bloqueio de tela no modo de quiosque.
Configuração do Launcher	Especifica as configurações para o Citrix Launcher nos dispositivos Android, como os aplicativos permitidos e uma imagem de logotipo personalizado para o ícone do Launcher.
LDAP	Oferece informações sobre um servidor LDAP a ser usado nos dispositivos iOS, incluindo qualquer informação de conta necessária como o nome de host do servidor LDAP. A política também fornece um conjunto de políticas de pesquisa de LDAP a serem usadas ao consultar o servidor LDAP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Localização	Permite geolocalizar dispositivos em um mapa, desde que o aparelho esteja com o GPS ativado no Secure Hub. Depois de implantar essa política no dispositivo, você pode enviar um comando de localização a partir do XenMobile Server. O dispositivo responde com as suas coordenadas de localização. O XenMobile também oferece suporte a políticas de geocerca e de rastreamento.
Email	Configura uma conta de email em dispositivos iOS ou macOS.
Domínios gerenciados	Define os domínios gerenciados que se aplicam a emails e ao navegador Safari. Os domínios gerenciados ajudam você a proteger dados corporativos ao controlar quais aplicativos podem abrir documentos baixados de domínios usando o Safari. Para dispositivos supervisionados iOS 8 e versões posteriores, você pode especificar as URLs ou os subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador.
Opções de MDM	Gerencia o bloqueio de ativação Buscar iPhone e iPad em dispositivos supervisionados iOS 7.0 e versões posteriores.
Informações sobre a organização	Especifica as informações da organização para mensagens de alerta que o XenMobile implanta em dispositivos iOS.
Código secreto	Impõe um código PIN ou senha em um dispositivo gerenciado. Você pode definir a complexidade e os tempos limite do código secreto no dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Ponto de acesso pessoal	Permite que os usuários se conectem à internet quando não estão dentro do alcance de uma rede WiFi. Os usuários se conectam por meio da conexão de dados celulares no seu dispositivo iOS, usando a funcionalidade de ponto de acesso pessoal.
Remoção de perfil	Remove o perfil de aplicativo dos dispositivos iOS ou macOS.
Perfil de provisionamento	Especifica um perfil de provisionamento de distribuição empresarial para enviar para os dispositivos. Quando você desenvolve assina com código um aplicativo empresarial iOS, você geralmente inclui um perfil de provisionamento. A Apple requer que o perfil para o aplicativo seja executado em um dispositivo iOS. Se um perfil de configuração estiver ausente ou tiver expirado, o aplicativo falhará quando um usuário tocar para abri-lo.
Remoção de perfil de provisionamento	Remove perfis de provisionamento do iOS.
Proxy	Especifica as configurações de proxy HTTP globais para dispositivos que executam o Windows Mobile/CE e o iOS. Você pode implantar somente uma política de proxy HTTP global por dispositivo.
Registro	Define as chaves e os valores do registro que permitem administrar dispositivos Windows Mobile/CE. O Registro do Windows Mobile/CE armazena dados sobre as definições de aplicativos, drivers, preferências do usuário e configurações.
Suporte remoto	Fornece a você o acesso remoto aos dispositivos Samsung KNOX.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Restrições	Fornece 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 forçar o acesso a serviços de terceiros, como lojas de aplicativos.
Roaming	Configura se deve ser permitida voz e o roaming de dados em dispositivos iOS e Windows Mobile/CE. Se o roaming de voz está desativado, o roaming de dados é automaticamente desativado.
Chave de licença MDM Samsung	Especifica a chave interna do Enterprise License Management (ELM) Samsung que você precisa implantar em um dispositivo antes de implantar as políticas e restrições do SAFE. O XenMobile também suporta o serviço Enterprise Firmware Over-The-Air (E-FOTA) da Samsung. O XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung KNOX e as estende.
Programação	Obrigatória nos dispositivos Android e Windows Mobile para se conectar de volta ao XenMobile Server para gerenciamento do MDM, envio por push de aplicativos e implantação de políticas. Se você não enviar essa política a dispositivos e não ativar o Google FCM, um dispositivo não poderá se conectar de volta ao servidor.
SCEP	Configura dispositivos iOS e macOS para recuperar um certificado de um servidor SCEP externo. Você também pode fornecer um certificado para o dispositivo usando SCEP de uma PKI que esteja conectada ao XenMobile. Para fazer isso, crie uma entidade de PKI e um provedor de PKI em modo distribuído.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Conta SSO	Cria contas de logon único (SSO) para que os usuários façam logon somente uma vez para acessar o XenMobile e seus recursos internos da empresa. Os usuários não precisam armazenar nenhuma credencial no dispositivo. O XenMobile usa as credenciais do usuário empresarial da conta SSO entre aplicativos, incluindo os aplicativos da App Store. Essa política é compatível com a autenticação Kerberos. Disponível para o iOS.
Criptografia de armazenamento	Criptografa armazenamento interno e externo. Em alguns dispositivos, essa política impede que os usuários usem um cartão de armazenamento nos respectivos dispositivos.
Calendários inscritos	Adiciona um calendário inscrito à lista de calendários nos dispositivos iOS. Inscreva-se em um calendário antes de adicioná-lo à lista de calendários inscritos nos dispositivos dos usuários.
Termos e condições	Requer que os usuários aceitem as políticas específicas da empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos no XenMobile, eles devem aceitar os termos e condições para registrar os dispositivos. Não aceitar os termos e condições cancela o processo de registro.
Túnel	Usada somente para suporte remoto. O suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
VPN	Fornece acesso a sistemas de backend que usam a tecnologia de Gateway VPN de legado. Esta política fornece detalhes de conexão gateway VPN que você pode implantar nos dispositivos. XenMobile é compatível com vários provedores de VPN, incluindo Cisco AnyConnect, Juniper e Citrix VPN. Se o seu gateway VPN der suporte a esta opção, você poderá vincular essa política a uma CA e ativar VPN sob demanda.
Papel de parede	Adiciona um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio ou na tela inicial de um dispositivo iOS, ou em ambas. Para usar papéis de parede diferentes em iPads e iPhones, crie políticas diferentes de papéis de parede e implantá-las nos usuários apropriados.
Filtro de conteúdo Web	Filtra conteúdo web nos dispositivos iOS. O XenMobile usa a função de filtro automático da Apple e os sites que você adiciona a listas brancas e negras. Disponível somente para dispositivos supervisionados iOS.
Clip web	Insere atalhos ou clipes Web em sites para que apareçam junto com aplicativos nos dispositivos de usuários. Você pode especificar seus próprios ícones para representar os clipes Web para dispositivos iOS, macOS e Android. O tablet Windows requer somente um rótulo e uma URL.
WiFi	Permite que os administradores implantem detalhes do roteador de WiFi em dispositivos gerenciados. Os detalhes do roteador incluem SSID, dados de autenticação e dados de configuração.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Certificado Windows CE	Cria e fornece certificados Windows Mobile/CE de uma PKI externa para os dispositivos de usuários.
Proteção de informações do Windows	Especifica os aplicativos que exigem a Proteção de informações do Windows no nível de imposição definido na política. A política é para dispositivos supervisionados Windows 10 versão 1607 e versões posteriores.
XenMobile Store	Especifica se um clip Web da XenMobile Store aparece na tela inicial dos dispositivos do usuário.
Opções do XenMobile	Configura o comportamento do Secure Hub quando ele se conecta ao XenMobile a partir de dispositivos Android e Windows Mobile/CE.
Desinstalação do XenMobile	Desinstala o XenMobile dos dispositivos Android e Windows Mobile/CE. Quando implantada, essa política remove o XenMobile de todos os dispositivos no grupo de implantação.

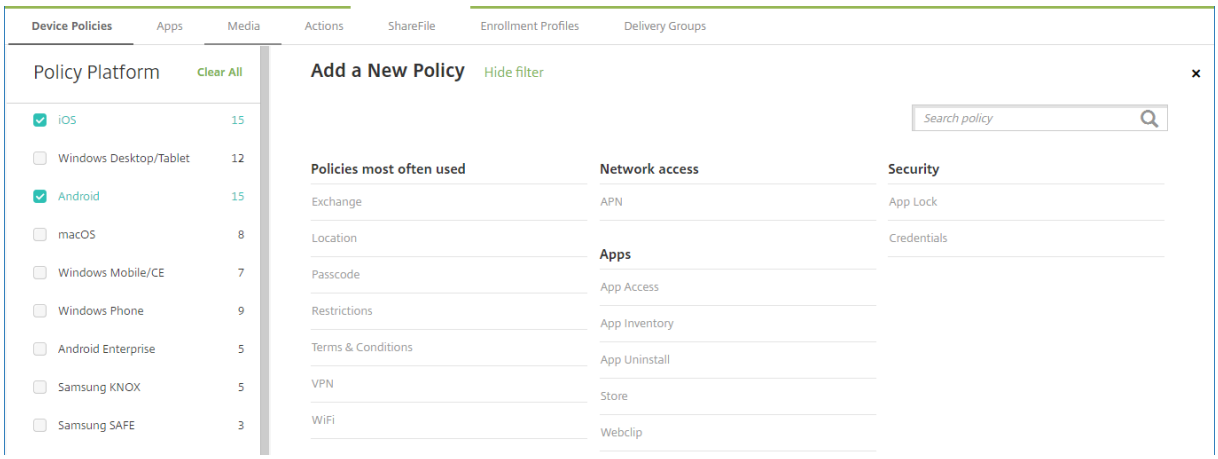
Políticas de dispositivo por plataforma

March 6, 2019

Para exibir as políticas disponíveis por plataforma:

1. No console XenMobile, vá para **Configurar > Políticas de dispositivo**.
2. Clique em **Adicionar**.
3. Cada plataforma de dispositivo é exibida 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 a plataforma. Para ver uma lista das políticas que estão disponíveis para várias plataformas, selecione cada uma dessas plataformas. Uma política aparece na lista somente se ela se aplicar a cada plataforma selecionada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A versão mais recente do XenMobile é compatível com políticas de dispositivo para as seguintes plataformas:

- Amazon
- Android
- Android HTC
- Android Sony
- Android TouchDown
- Android Enterprise
- Android Zebra
- SO Chrome
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows 10 Desktop/Tablet
- Telefone Windows 10
- Windows Mobile/CE

Para obter detalhes sobre os dispositivos com suporte na versão mais recente do XenMobile, consulte Plataformas de dispositivo com suporte.

> Nota:
>
> Se o seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):
>
> Quando você configurar políticas de dispositivo do XenMobile para o Windows 10, lembre-se da regra a seguir. Se uma política em um ou mais dispositivos Windows 10 registrados for conflitante, a política alinhada ao GPO terá precedência.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de espelhamento de AirPlay

April 15, 2019

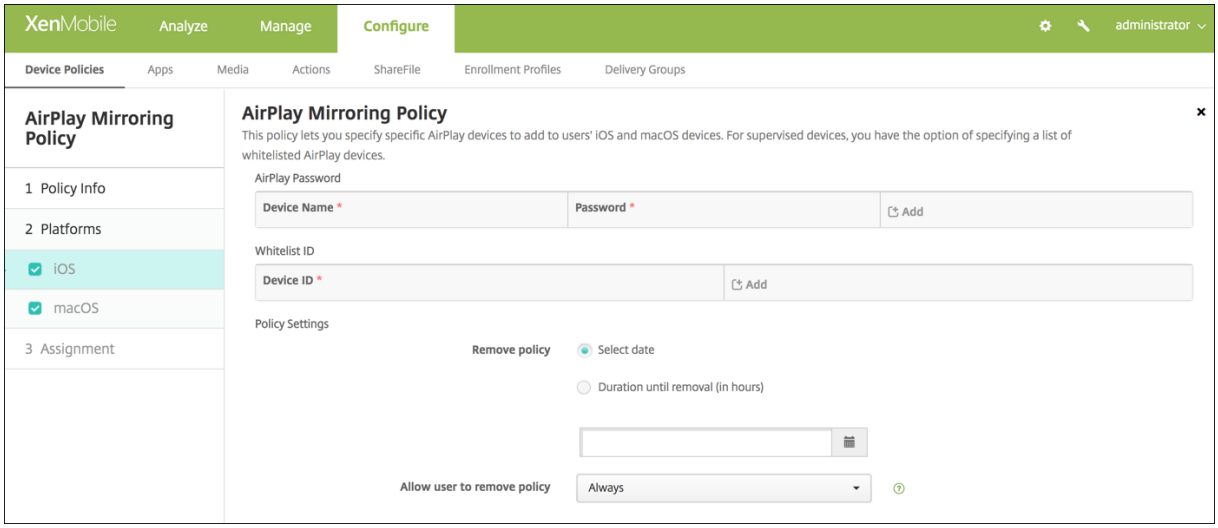
O recurso AirPlay da Apple permite que os usuários transmitam sem fios o conteúdo de um dispositivo iOS para uma tela de TV usando o Apple TV ou espelhem exatamente o que está na tela de um dispositivo em uma tela de TV ou outro computador Mac.

Você pode adicionar uma política de dispositivo do XenMobile para adicionar dispositivos específicos AirPlay (como o Apple TV ou outro computador Mac) aos dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista branca de dispositivos supervisionados, o que limita os usuários a somente os dispositivos AirPlay na lista branca. 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, verifique se você tem os IDs de dispositivo e todas as senhas de todos os dispositivos que deseja adicionar.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



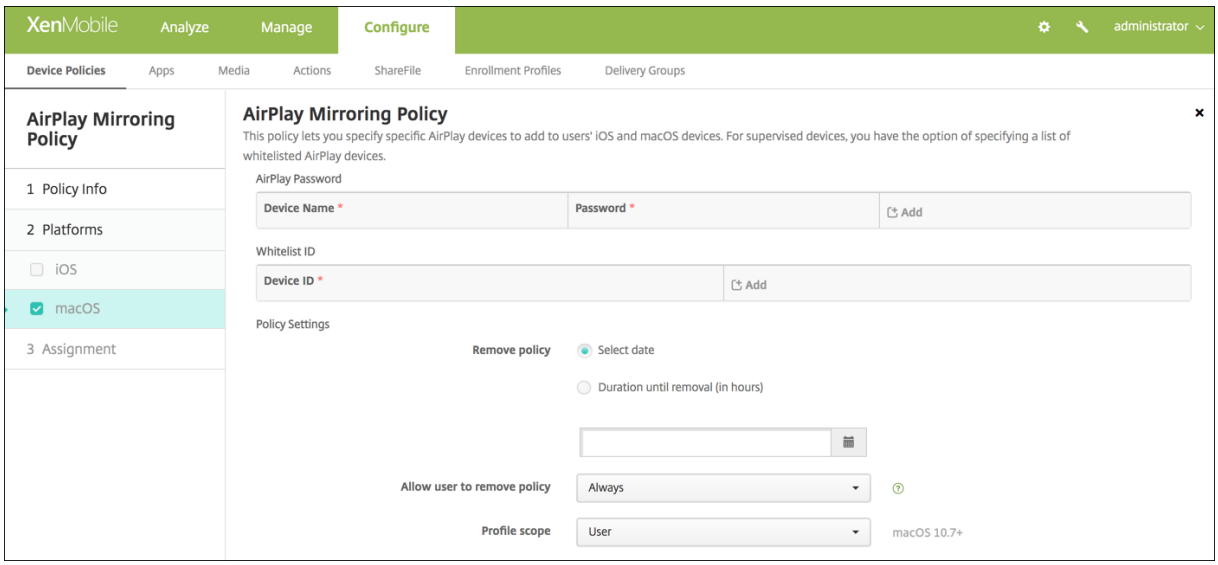
- **Senha do AirPlay:** para cada dispositivo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **ID do dispositivo:** insira o endereço de hardware (endereço Mac) no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Senha:** insira uma senha opcional para o dispositivo.
  - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.

- **ID da lista branca:** essa lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nessa lista são os únicos dispositivos AirPlay disponíveis para os dispositivos dos usuários. Para cada dispositivo AirPlay que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:
  - **ID do dispositivo:** digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
  - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.

Configurações do macOS



- **Senha do AirPlay:** para cada dispositivo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **ID do dispositivo:** insira o endereço de hardware (endereço Mac) no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
  - **Senha:** insira uma senha opcional para o dispositivo.
  - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.
- **ID da lista branca:** essa lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nessa lista são os únicos dispositivos AirPlay disponíveis para os dispositivos dos usuários. Para cada dispositivo AirPlay que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **ID do dispositivo:** digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
  - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.

Política de dispositivo do AirPrint

April 15, 2019

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar impressoras AirPrint à lista de impressoras AirPrint nos dispositivos iOS. Essa política facilita o suporte aos ambientes nos quais as impressoras e os dispositivos estão em sub-redes diferentes.

Essa política se aplica ao iOS 7.0 e versões posteriores.

> Nota:
>
> Verifique se você tem o endereço IP e o caminho do recurso de cada impressora.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Destino do AirPrint:** para cada destino do AirPrint que você desejar 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. Esse valor corresponde ao parâmetro do registro _ipps.tcp Bonjour. Por exemplo, printers/-Canon_MG5300_series ou printers/Xerox_Phaser_7600.
  - Clique em **Salvar** para adicionar a impressora ou em **Cancelar** para cancelar a adição da impressora.

Política de restrições de aplicativo do Android for Work

April 15, 2019

Você pode modificar as restrições associadas aos aplicativos do Android for Work.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos

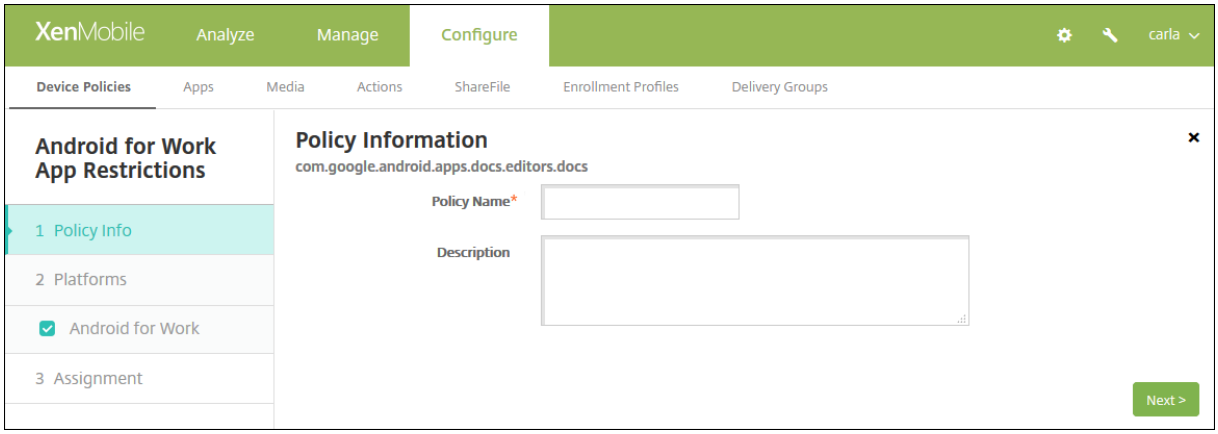
- Conclua as tarefas de instalação do Android for Work no Google. Para obter mais informações, consulte Gerenciamento de dispositivos com Android for Work.
- Crie uma conta do Android for Work. Para obter mais informações, consulte Criar uma conta do Android for Work.
- Adicione os aplicativos do Android for Work ao XenMobile. Para obter mais informações, consulte Adição de aplicativos ao XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android for Work

Depois que você optar por adicionar uma política de restrição de aplicativos do Android for Work, será exibida uma solicitação para selecionar um aplicativo. Se não houver nenhum aplicativo do Android for Work adicionado ao XenMobile, você não poderá continuar.

Depois de selecionar um aplicativo, defina as configurações de política. As configurações são específicas para cada aplicativo.



Permissões do Android for Work

April 15, 2019

Você pode configurar como as solicitações para aplicativos do Android for Work nos perfis de trabalho lidam com 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 o Android 7.0 e posterior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O Google define permissões perigosas como permissões que dão ao aplicativo acesso a dados ou recursos que envolvem as informações particulares 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.

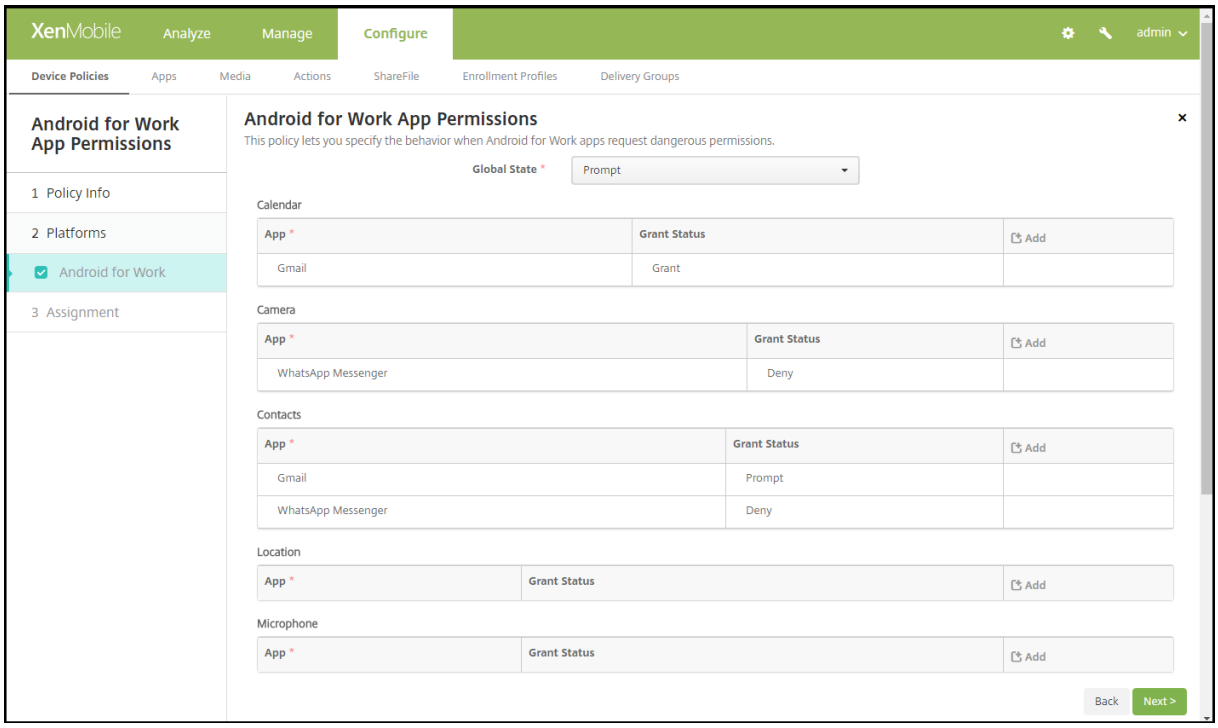
Você pode configurar um estado global que controla o comportamento de todas as solicitações de permissões perigosas para os aplicativos do Android for Work em perfis de trabalho. Você também pode controlar o comportamento de solicitações de permissões perigosas para grupos de permissão individual, conforme definido pelo Google, para cada aplicativo. Essas configurações individuais substituem o estado global.

Para obter informações sobre como o Google define grupos de permissões, consulte "Grupos de permissões" neste Guia de desenvolvedores do Android.

Por padrão, os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android for Work



- **Estado global:** controla o comportamento de todas as solicitações de permissões perigosas. Na lista, clique em **Solicitar**, **Conceder** ou **Negar**.
  - **Solicitar:** os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Conceder:** todas as solicitações de permissões perigosas são concedidas. O usuário não é solicitado.
  - **Negar:** todas as solicitações de permissões perigosas são negadas. O usuário não é solicitado.

  O padrão é **Solicitar**.

- Defina um comportamento individual para cada grupo de permissões, para cada aplicativo. Para configurar o comportamento de um grupo de permissões: clique em **Adicionar** e, em **Aplicativo**, escolha um aplicativo na lista. Em Estado de concessão, escolha **Solicitar**, **Conceder** ou **Negar**. Esse estado de concessão substitui o estado global.

  - **Solicitar:** os usuários são solicitados a conceder ou negar solicitações de permissões perigosas desse grupo de permissões para este aplicativo.
  - **Conceder:** as solicitações de permissões perigosas desse grupo de permissões para este aplicativo são concedidas. O usuário não é solicitado.
  - **Negar:** solicitações de permissões 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 ao grupo de permissões, clique em **Adicionar** novamente e repita essas etapas.
- Quando você terminar de definir os estados de concessão para todos os grupos de permissões desejados, clique em **Avançar**.

Política de dispositivo do APN

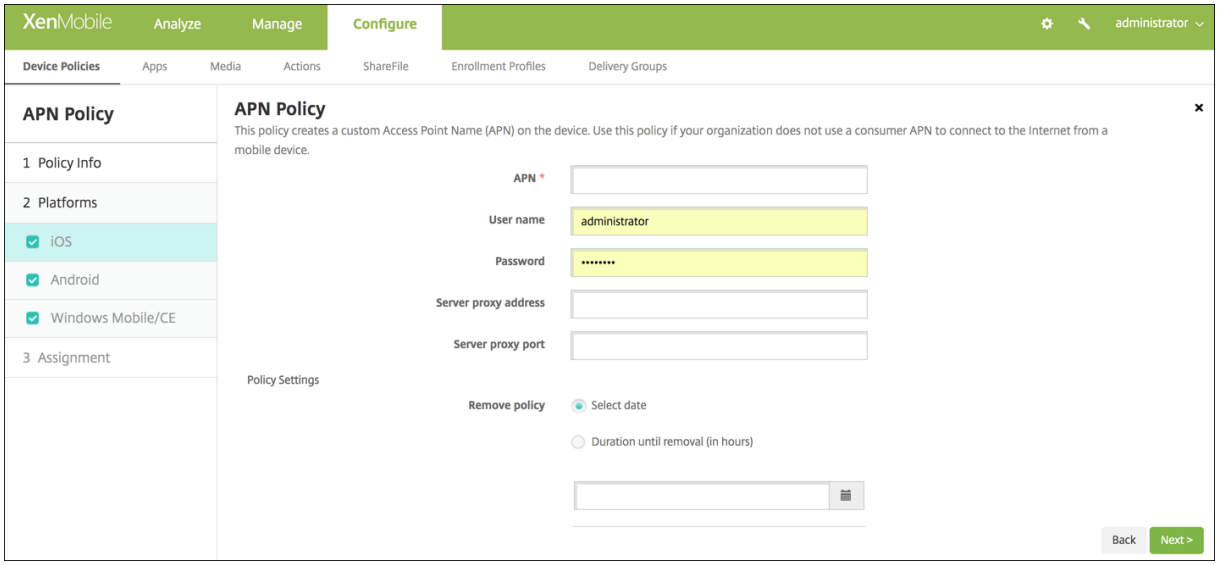
April 15, 2019

Você pode adicionar uma política de dispositivo de Nome de Ponto de Acesso (APN) personalizado a dispositivos iOS, Android e Windows Mobile/CE. Use essa política se sua organização não usar um APN de consumidor para conexão com a Internet de um dispositivo móvel. Uma política de APN determina as configurações usadas para conectar os seus dispositivos a um GPRS da operadora de telefonia específica. Essa configuração já está definida na maioria dos telefones mais recentes.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

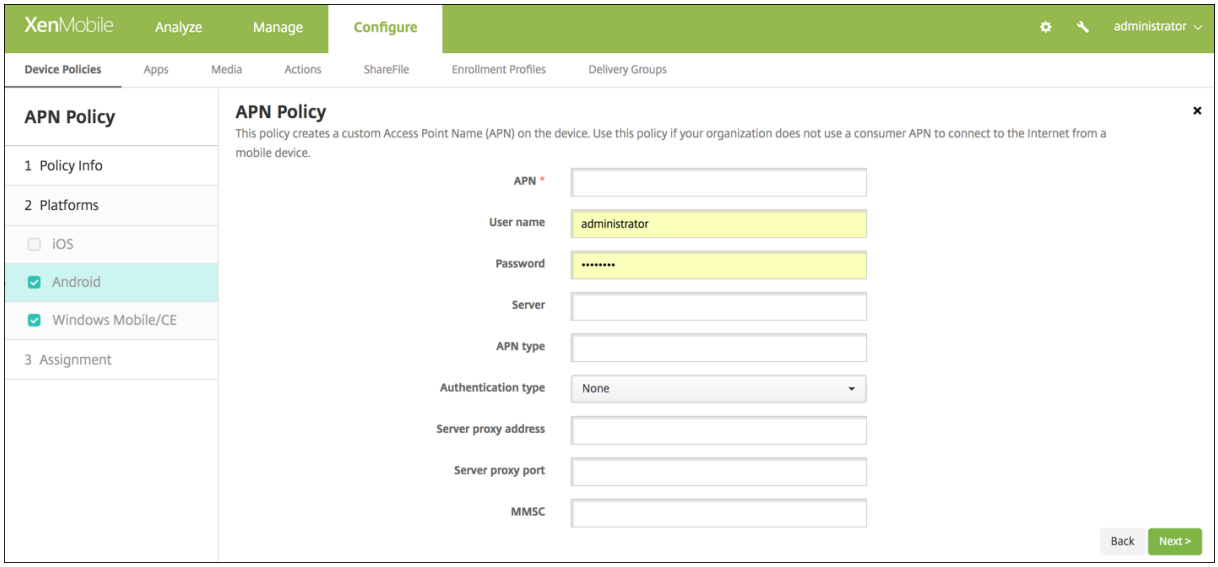
Configurações de iOS



- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito pelo iOS, ou a política falhará.
- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.
- **Endereço do servidor proxy:** o endereço IP ou a URL do proxy do APN.
- **Porta do servidor proxy:** o número da porta do proxy do APN. Ele será necessário se você tiver inserido um endereço de servidor proxy.
- Em **Configurações de política**, ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android

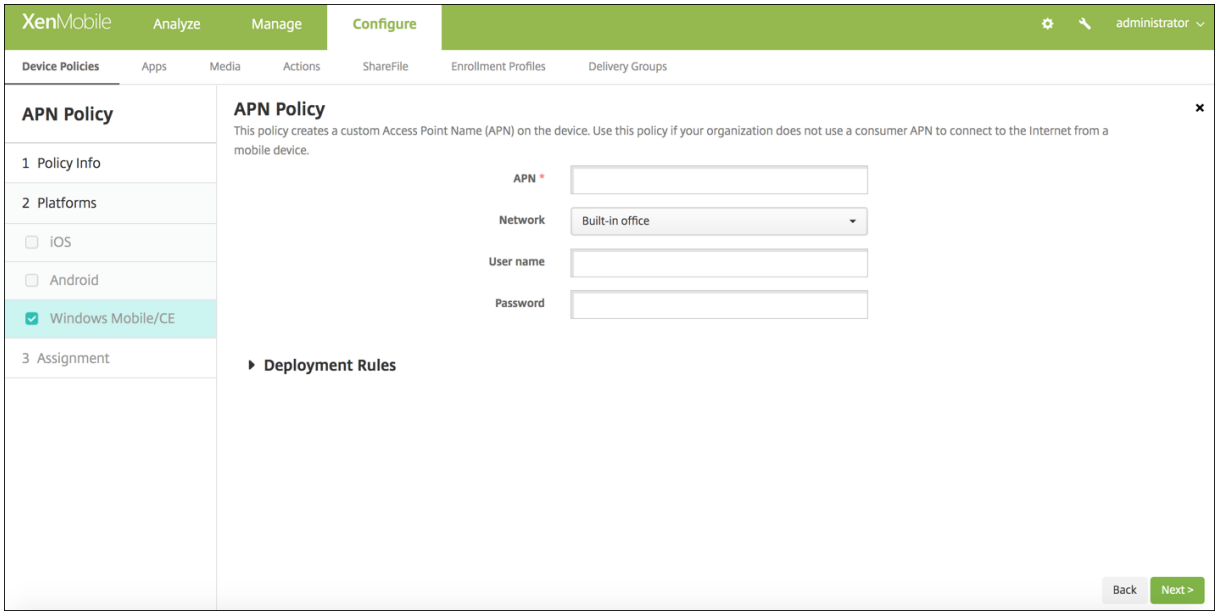


- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito do Android, ou a política falhará.
- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.
- **Servidor:** essa configuração, que é anterior aos smartphones, geralmente está vazia. Ela faz referência a um servidor de gateway Wireless Application Protocol (WAP) para telefones que não puderam acessar ou renderizar sites da web comuns.
- **Tipo de APN:** essa configuração deve coincidir com o uso pretendido da operadora para o ponto de acesso. Trata-se de uma cadeia de caracteres separada por vírgulas de especificadores do serviço do APN e deve coincidir com as definições publicadas da operadora sem fio. Alguns exemplos:
  - *. Todo o tráfego passa por esse ponto de acesso.
  - mms. Todo o tráfego multimídia passa por esse ponto de acesso.
  - padrão. Todo o tráfego, incluindo multimídia, passa por esse ponto de acesso.
  - supl. A localização de plano de usuário segura é associada ao GPS assistido.
  - dun. A rede de Conexão discada está desatualizada e raramente deve ser usada.
  - hipri. Redes de alta prioridade.
  - fota. O firmware por rede celular é usado para receber as atualizações de firmware.
- **Tipo de autenticação:** na lista, clique no tipo de autenticação a ser usado. O padrão é Nenhum.
- **Endereço do servidor proxy:** o endereço IP ou a URL do proxy HTTP de APN da operadora.
- **Porta do servidor proxy:** o número da porta do proxy do APN. Ele será necessário se você tiver

© 1999-2019 Citrix Systems, Inc. All rights reserved.

inserido um endereço de servidor proxy.
- **MMSC:** o endereço do Servidor de Gateway MMS fornecido pela operadora.
- **Endereço do proxy MMS (Multimedia Messaging Server):** esse é o servidor do serviço de mensagens multimídia do tráfego MMS. O MMS sucedeu o SMS para enviar mensagens maiores com conteúdo multimídia, como imagens ou vídeos. Esses servidores exigem protocolos específicos (como MM1, … MM11).
- **Porta MMS:** a porta usada para o proxy MMS.

Configurações do Windows Mobile/CE



- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito do Android, ou a política falhará.
- **Rede:** na lista, clique no tipo de rede a ser usada. O padrão é **Escritório interno**.
- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.

Política de dispositivo de acesso aos aplicativos

April 15, 2019

A política de dispositivo de acesso aos aplicativos no XenMobile permite definir uma lista de aplicativos cuja instalação é necessária no dispositivo, que podem ser instalados no dispositivo ou que não

© 1999-2019 Citrix Systems, Inc. All rights reserved.

devem ser instalados no dispositivo. Você pode criar uma ação automatizada para reagir à conformidade do dispositivo com essa lista de aplicativos. Você pode criar políticas de acesso aos aplicativos para dispositivos iOS, Android e Windows Mobile/CE.

Você pode configurar somente um tipo de política de acesso por vez. Você pode adicionar uma política de qualquer lista de aplicativos necessários, aplicativos sugeridos ou aplicativos proibidos, mas não uma mistura na mesma política de acesso aos aplicativos. Se você criar uma política para cada tipo de lista, recomendamos que você nomeie cada política cuidadosamente, para que saiba qual política no XenMobile se aplica à qual lista de aplicativos.

Para adicionar ou configurar essa política, acesse **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 de aplicativo:** insira um identificador de aplicativo opcional.
  - Clique em **Salvar** ou em **Cancelar**.
  - Repita essas etapas para cada aplicativo que você desejar adicionar.

Política de dispositivo de atributos de aplicativo

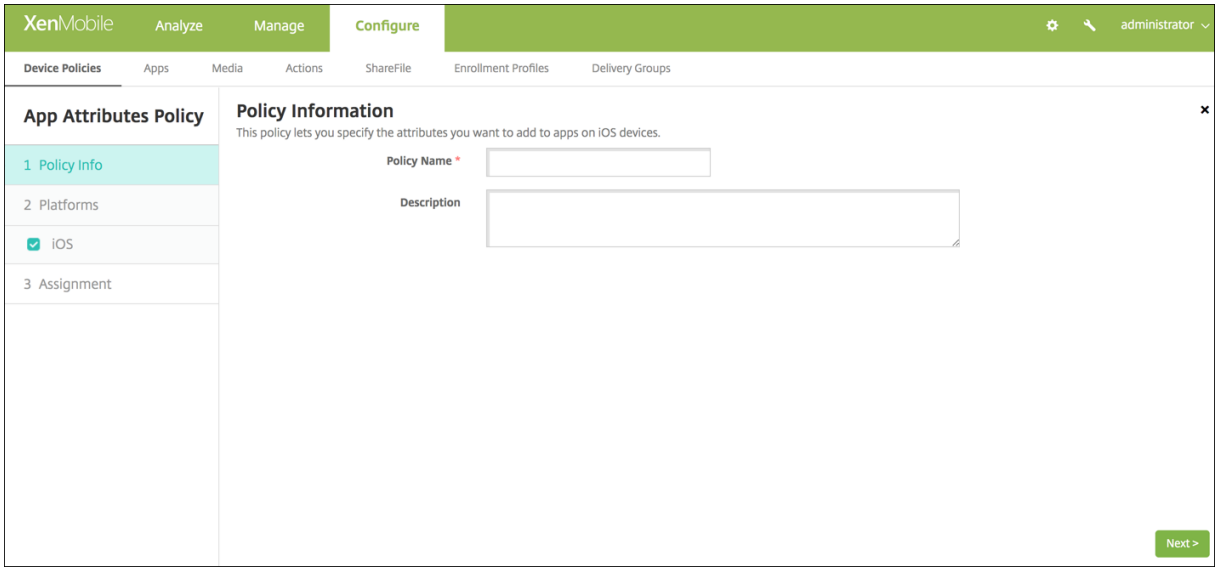
April 15, 2019

A política de dispositivos de atributos de aplicativo permite especificar atributos, como um ID do pacote do aplicativo gerenciado ou um identificador de VPN por aplicativo, para dispositivos iOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



- **ID de pacote de aplicativos gerenciados:** na lista, clique em um ID de pacote de aplicativo ou em **Adicionar novo**.
  - Se você clicar em **Adicionar novo**, digite o código do pacote de aplicativos no campo exibido.
- **Identificador VPN por aplicativo:** na lista, clique no identificador VPN por aplicativo.

Política de dispositivo de configuração de aplicativo

April 15, 2019

Você pode configurar remotamente aplicativos que suportam configuração gerenciada implantando:

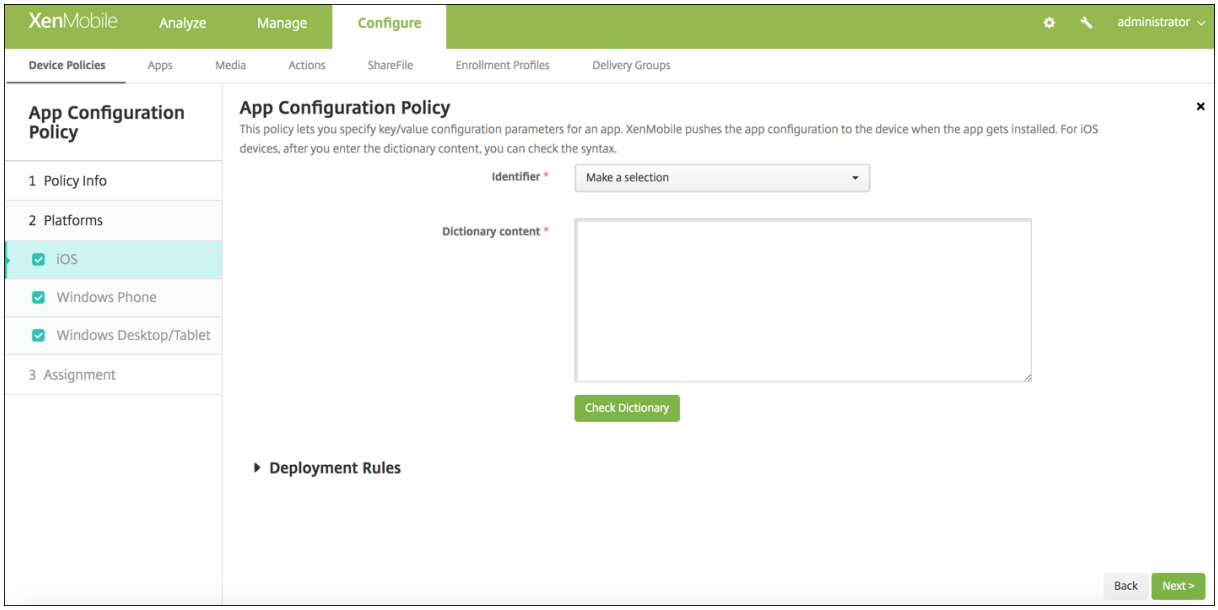
- Um arquivo de configuração XML (chamado de lista de propriedades, ou plist) nos dispositivos iOS
- Ou pares de chave/valor para dispositivos de telefone, tablet ou desktop do Windows 10.

A configuração especifica várias definições e comportamentos no aplicativo. O XenMobile envia a configuração para os dispositivos quando o usuário instala o aplicativo. As definições e os comportamentos reais que você pode configurar dependem do aplicativo e estão além do escopo deste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

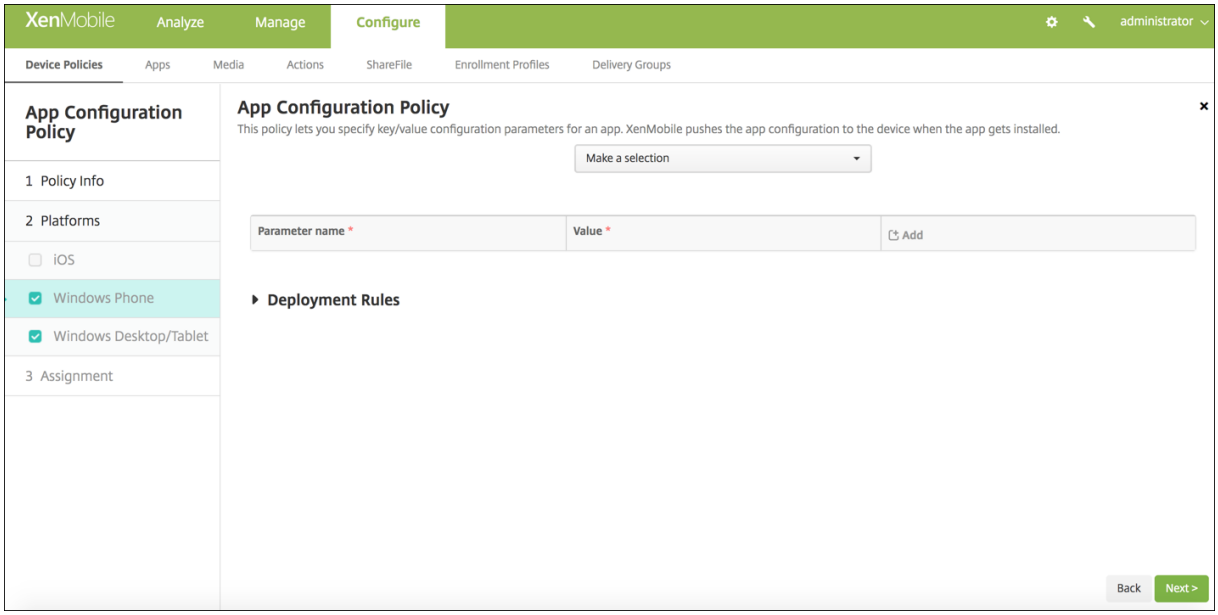
Configurações de iOS

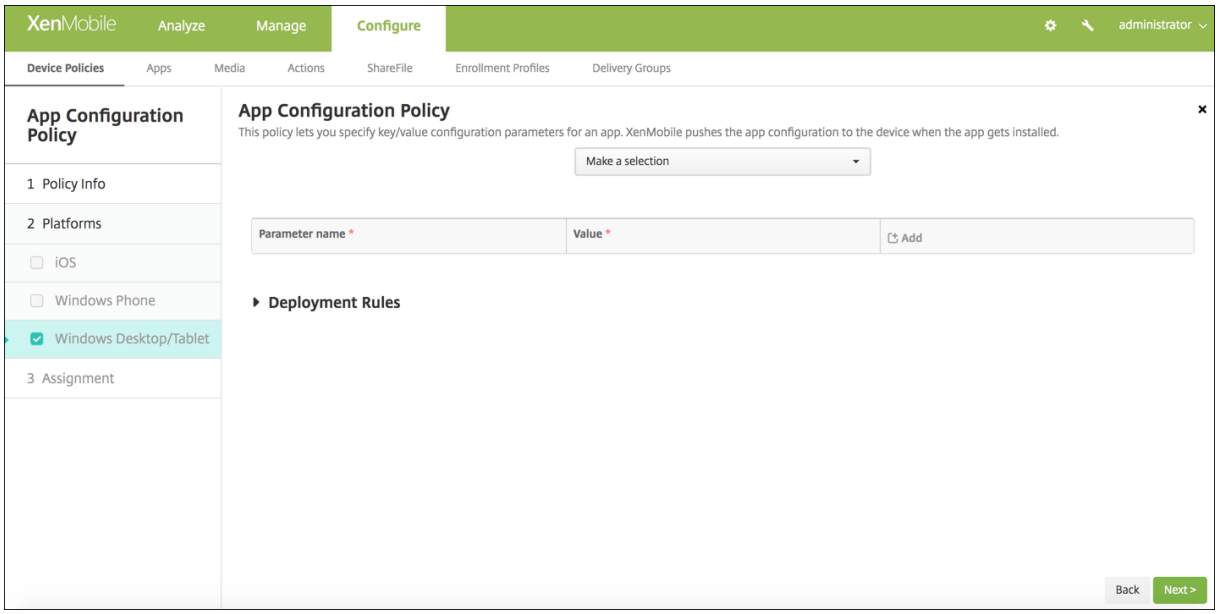


- **Identificador:** na lista, clique no aplicativo que você desejar configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
  - Se você clicar em **Adicionar novo**, digite o identificador do aplicativo no campo exibido.
- **Conteúdo do dicionário:** digite ou copie e cole as informações de configuração da lista de propriedades XML (plist).
- Clique em **Verificar dicionário**. O XenMobile verifica o XML. Se não houver nenhum erro, você verá **XML válido** abaixo da caixa de conteúdo. Se algum erro de sintaxe for exibido abaixo da caixa de conteúdo, você deverá corrigi-lo antes de continuar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Phone ou Desktop/Tablet





- Na lista **Fazer uma seleção**, clique no aplicativo que você desejar configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
  - Se você clicar em **Adicionar novo**, digite o nome da família do pacote no campo exibido.
- Para cada parâmetro de configuração que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do parâmetro:** Digite o nome de chave para uma configuração de aplicativo para o dispositivo Windows. Para obter informações sobre as configurações de aplicativo Windows, consulte a documentação da Microsoft.
  - **Valor:** Digite o valor do parâmetro especificado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

– Clique em **Adicionar** para adicionar o parâmetro ou em **Cancelar** para cancelar a adição do parâmetro.

Política de dispositivo de inventário de aplicativos

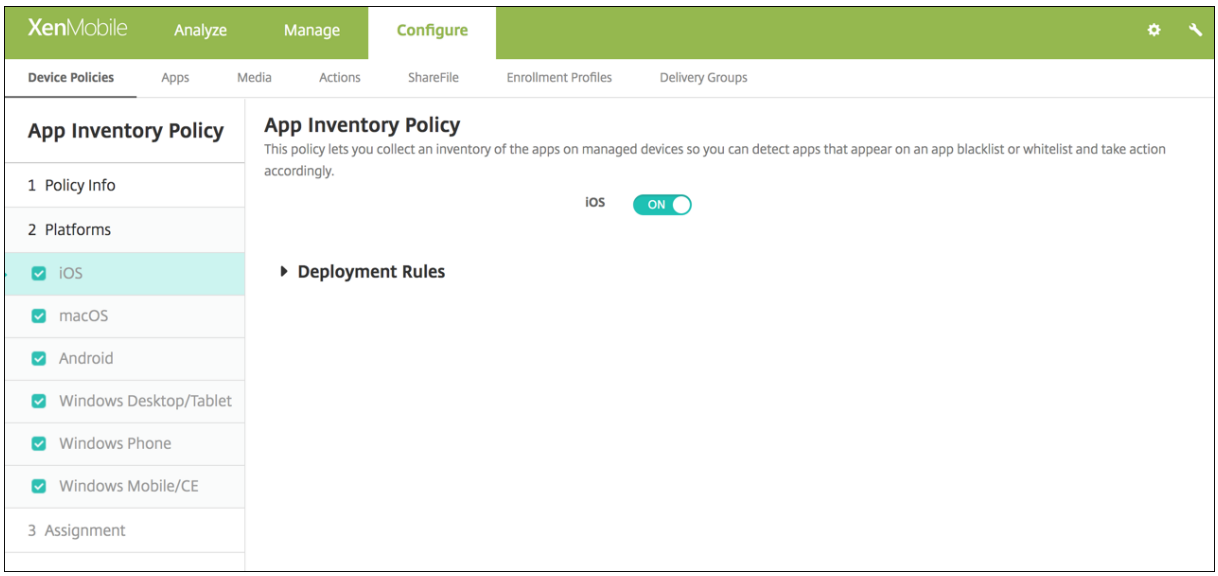
April 15, 2019

A política de inventário de aplicativos permite que você colete um inventário dos aplicativos em dispositivos gerenciados. O XenMobile pode então comparar o inventário com todas políticas de acesso aos aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que são exibidos em uma lista negra de aplicativos (proibidos em uma política de acesso aos aplicativos) ou lista branca (obrigatórios em uma política de acesso aos aplicativos) e tomar uma ação apropriada.

Você pode criar as políticas de acesso a aplicativos para iOS, macOS X e Android (inclusive para dispositivos para Android for Work), dispositivos Windows Desktop/Tablet, Windows Phone ou Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma



- Para cada plataforma que você selecionar, mantenha a configuração padrão ou altere a configuração para **O**. O padrão é **I**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de bloqueio de aplicativo

April 15, 2019

A Política de dispositivo de bloqueio de aplicativo define uma lista de aplicativos que podem ser executados em um dispositivo ou uma lista de aplicativos cuja execução é bloqueada em um dispositivo. Você pode configurar essa política para os dispositivos Android e iOS, mas a maneira exata pela qual a política funciona é diferente em cada plataforma. Por exemplo, você não pode bloquear vários aplicativos em um dispositivo iOS.

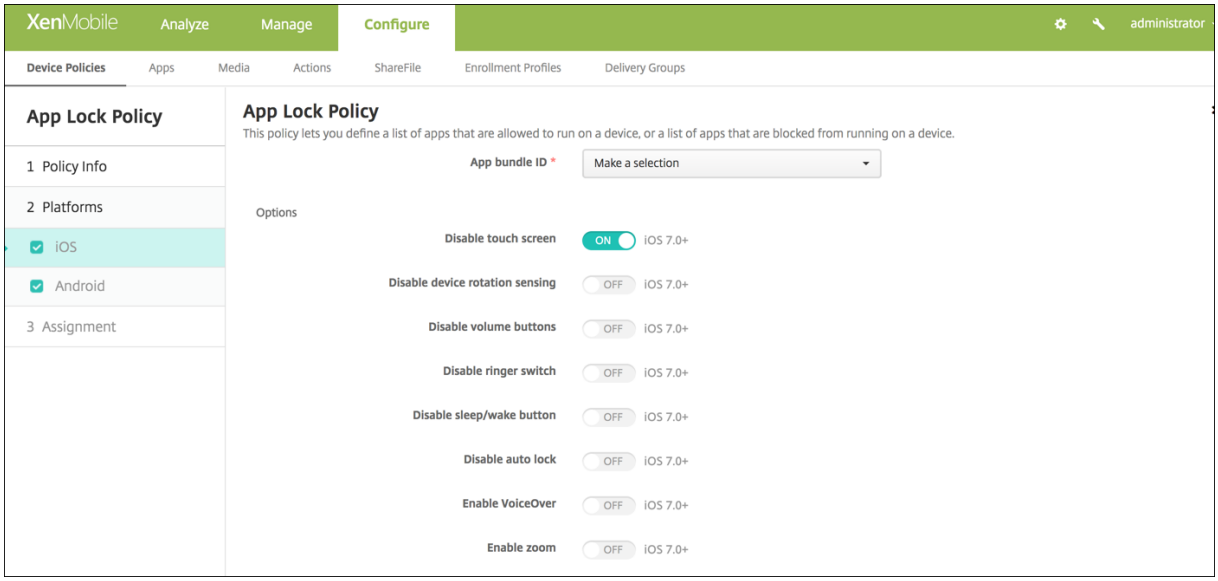
Da mesma forma, em dispositivos iOS, você pode selecionar apenas um aplicativo iOS por política. Isso significa que os usuários só são capazes de usar o dispositivo para executar um único aplicativo. Eles não podem realizar outras atividades no dispositivo. exceto as opções permitidas especificamente quando a política de bloqueio de aplicativo é aplicada.

Além disso, os dispositivos iOS devem ser supervisionados para enviar por push 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 de versões posteriores porque o Google não utilizada mais a API.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



- **ID do pacote de aplicativos:** na lista, clique no aplicativo ao qual esta política se aplica ou

© 1999-2019 Citrix Systems, Inc. All rights reserved.

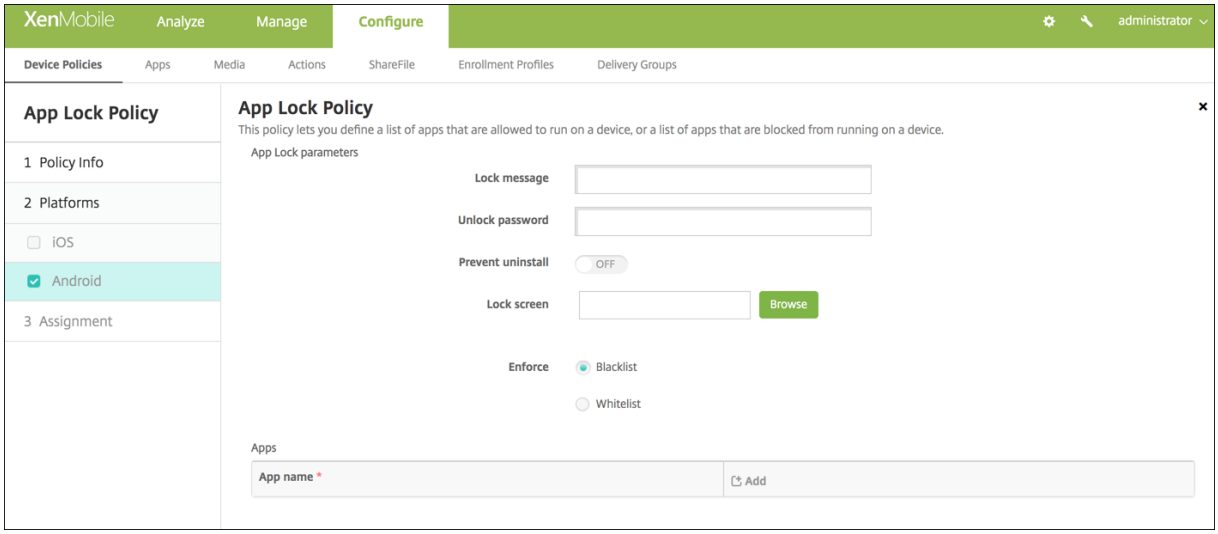
clique em **Adicionar novo** para adicionar um novo aplicativo à lista. Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo exibido.

- **Opções:** cada uma das opções a seguir se aplica somente ao iOS 7.0 ou versões posteriores. Em cada opção, o padrão é **O**, exceto para a opção Desativar tela de toque, que é **I** por padrão.
  - Desativar tela de toque
  - Desativar sensor de rotação do dispositivo
  - Desativar botões de volume
  - Desativar botão de toque
    Quando Desativar botão de toque está **I**, o comportamento do toque depende da posição do botão quando foi desativado pela primeira vez.
  - Desativar botão soneca/despertador
  - Desativar bloqueio automático
  - Desativar VoiceOver
  - Ativar zoom
  - Ativar inversão de cores
  - Ativar o AssistiveTouch
  - Ativar fala de seleção
  - Ativar áudio mono
- **Opções ativadas pelo usuário:** cada uma das opções a seguir se aplica somente ao iOS 7.0 ou versões posteriores. Para cada opção, o padrão é **O**.
  - Permitir ajuste do VoiceOver
  - Permitir ajuste do zoom
  - Permitir ajuste da inversão de cores
  - Permitir ajuste do AssistiveTouch

Configurações do Android

> Nota:
>
> Você não pode bloquear o aplicativo de configurações do Android usando a política de dispositivo de bloqueio de aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Parâmetros de bloqueio de aplicativo**
  - **Mensagem de bloqueio:** digite a 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 **Off**.
  - **Tela de bloqueio:** selecione a imagem que aparece na tela de bloqueio do dispositivo clicando em Procurar e navegando para a localização 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 podem ser executados em dispositivos.
- **Aplicativos:** clique em **Adicionar** e faça o seguinte:
  - **Nome do aplicativo:** na lista, clique no nome do aplicativo para adicioná-lo à lista branca ou negra, ou clique em **Adicionar novo** para adicionar um novo aplicativo à lista de aplicativos disponíveis.
  - Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo exibido.
  - Clique em **Salvar** ou em **Cancelar**.
  - Repita essas etapas para cada aplicativo que você deseja adicionar à lista branca ou negra.

Política de dispositivo de uso de rede de aplicativos

April 15, 2019

Você pode definir regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares, nos dispositivos iOS. As regras se aplicam somente aos aplicativos gerenciados. Aplicativos gerenciados são aqueles que você implanta nos dispositivos dos usuários usando o XenMobile. Eles não incluem aplicativos que os usuários baixaram diretamente para os

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dispositivos deles sem que fossem implantados usando o XenMobile ou aqueles já instalados nos dispositivos quando eles foram registrados no XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Permitir dados celulares de roaming:** selecione se os aplicativos especificados podem usar uma conexão de dados celulares enquanto estiverem em roaming. O padrão é **Off**.
- **Permitir dados celulares:** selecione se os aplicativos especificados podem usar uma conexão de dados celulares. O padrão é **Off**.
- **Correspondências de identificador de aplicativo:** para cada aplicativo que você desejar adicionar à lista, clique em **Adicionar** e 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.

Política de dispositivo de notificações de aplicativo

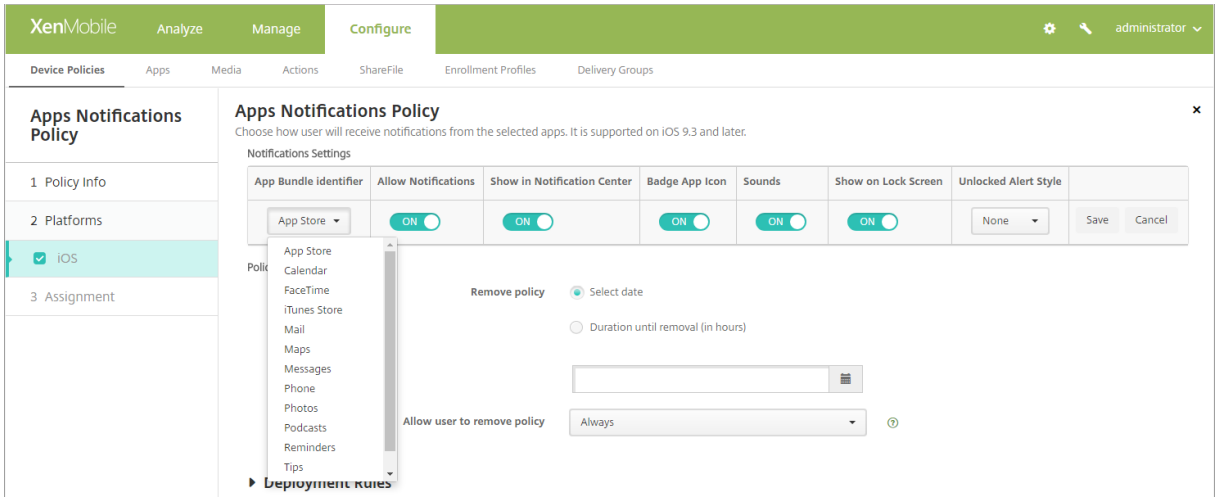
April 15, 2019

A política de notificações de aplicativos permite controlar como os usuários de iOS recebem notificações de aplicativos especificados. Essa política é compatível em dispositivos com o iOS 9.3 ou versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



- **Identificador do pacote de aplicativos:** especifique os aplicativos aos quais você deseja aplicar essa política.
- **Permitir notificações:** selecione **I** para permitir notificações.
- **Mostrar no Centro de notificação:** selecione **I** para mostrar notificações no Centro de Notificação dos dispositivos dos usuários.
- **Ícone de Aviso nos Aplicativos:** selecione **I** para mostrar um ícone de aviso do aplicativo com as notificações.
- **Sons:** selecione **I** para incluir sons com as notificações.
- **Mostrar na tela de bloqueio:** selecione **I** para mostrar notificações na tela de bloqueio dos dispositivos do usuário.
- **Estilo de alerta desbloqueado:** na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.

Política de dispositivo de restrições de aplicativo

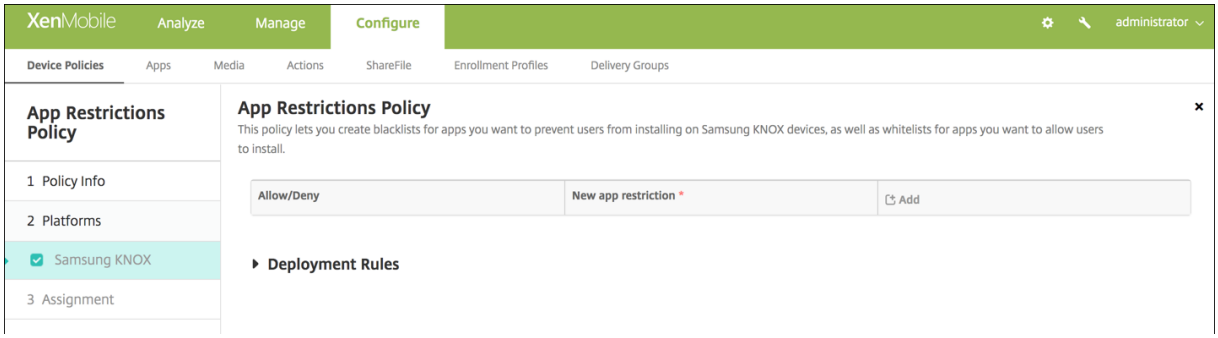
April 15, 2019

Você pode criar listas negras para os aplicativos que deseja impedir que os usuários instalem nos dispositivos Samsung KNOX, bem como listas brancas para os aplicativos que deseja permitir que os usuários instalem.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Samsung KNOX



Para cada aplicativo que você desejar adicionar à lista Permitir ou Negar, clique em **Adicionar** e faça o seguinte:

- **Permitir ou negar:** selecione se os usuários têm permissão para instalar o aplicativo.
- **Nova restrição de aplicativo:** digite o ID de pacote do aplicativo; por exemplo, com.kmdm.af.crackle.
- Clique em **Salvar** para salvar o aplicativo na lista Permitir ou Negar ou clique em **Cancelar** para não salvar.

Política de dispositivo de encapsulamento de aplicativo

April 15, 2019

> Importante:
>
> A política de encapsulamento de aplicativo é usado somente para suporte remoto. Para obter informações sobre o Suporte Remoto, consulte Opções de suporte e suporte remoto.

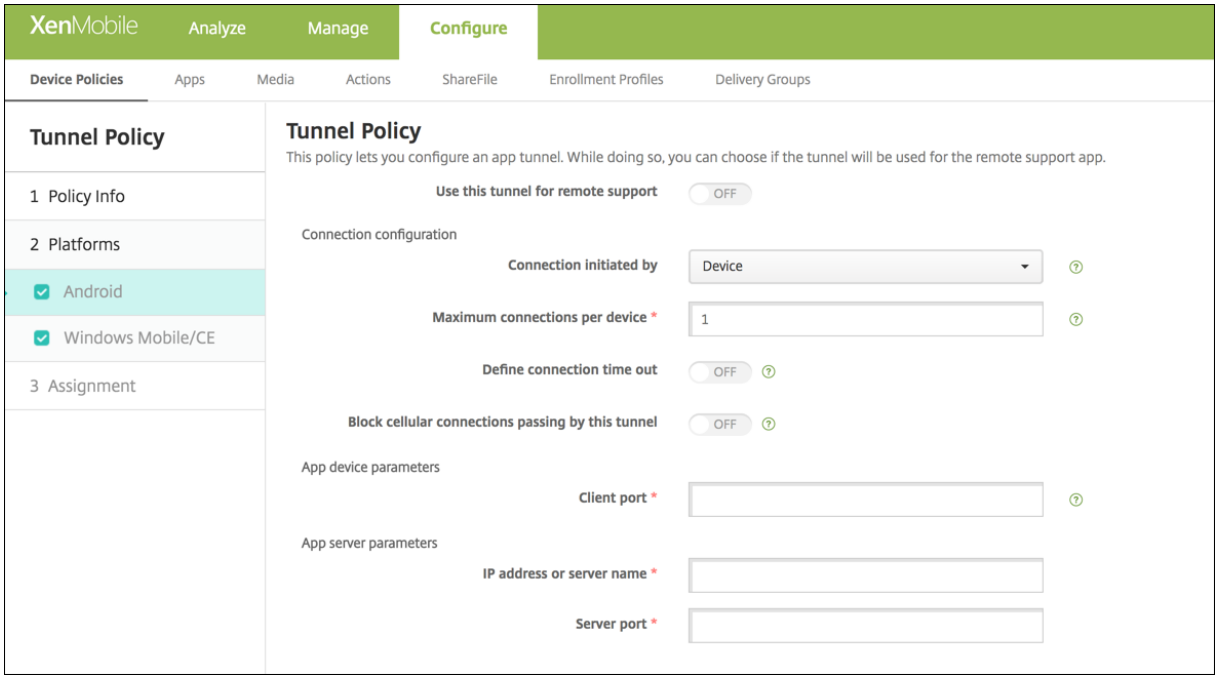
Os túneis de aplicativos foram projetados para aumentar a continuidade do serviço e a confiabilidade de transferência de dados de seus aplicativos móveis. Os túneis de aplicativo definem os parâmetros de proxy entre o componente de cliente de qualquer aplicativo do dispositivo móvel e o componente de servidor de aplicativos. Você também pode usar os túneis de aplicativo para criar túneis de suporte remoto para um dispositivo a fim de oferecer suporte ao gerenciamento. Você pode configurar a política de encapsulamento de aplicativo para dispositivos Android e Windows Mobile/CE.

Qualquer tráfego de aplicativo enviado por meio de um túnel definido nesta política passa pelo XenMobile antes de ser redirecionado para o servidor que executa o aplicativo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android



- **Usar este túnel para suporte remoto:** selecione se o túnel será usado para suporte remoto.

  As etapas de configuração são diferentes, dependendo se você selecionou o suporte remoto.

- Se você não selecionar o suporte remoto, faça o seguinte:
  - **Conexão iniciada por:** clique em **Dispositivo** ou **Servidor** para especificar a origem que inicia a conexão.
  - **Máximo de conexões por dispositivo:** digite um número para especificar quantas conexões TCP simultâneas o aplicativo pode estabelecer. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
  - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
    * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
  - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming.

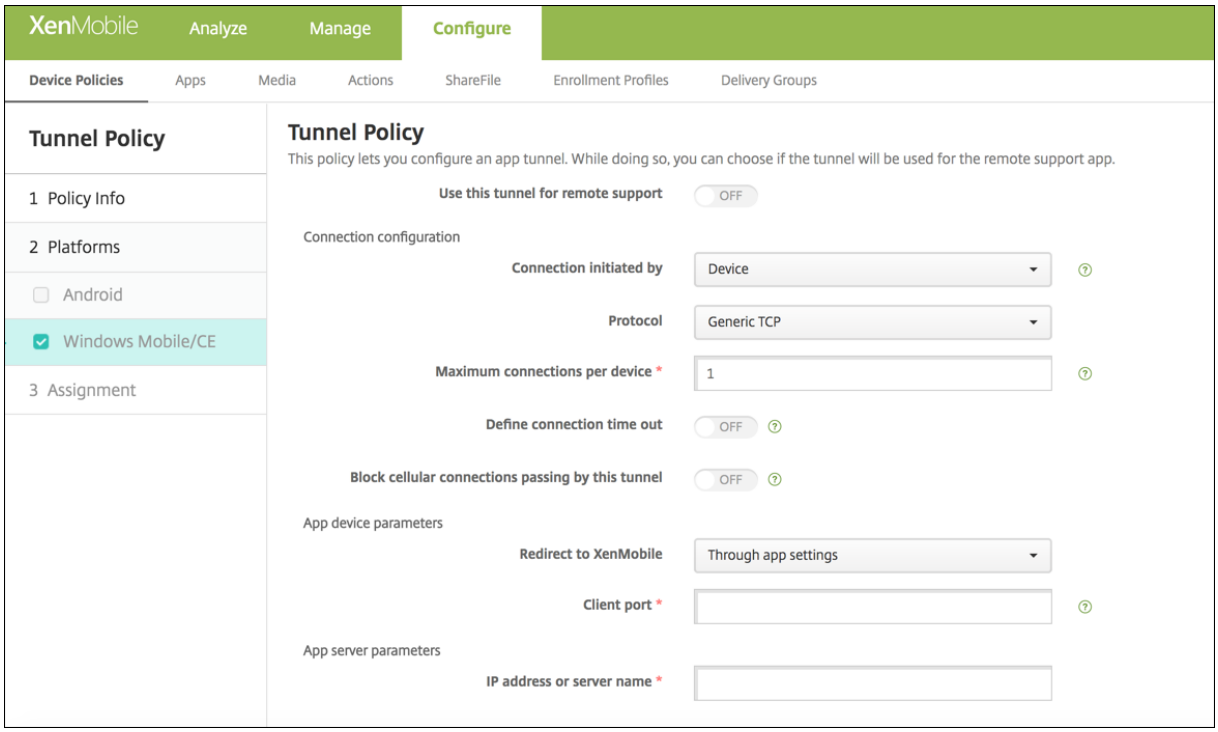
    > Nota:
    >
    > Conexões Wi-Fi e USB não serão bloqueadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Porta do cliente:** digite o número da porta. Na maioria dos casos, esse valor é o mesmo para a porta do servidor.
  - **Endereço IP ou nome do servidor:** digite o endereço IP ou nome do servidor do aplicativo. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
  - **Porta do servidor:** digite o número de porta do servidor.

- Se você selecionar o suporte remoto, faça o seguinte:
  - **Usar este túnel para suporte remoto:** defina como **Ativado**.
  - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
    * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
  - **Usar conexão SSL:** selecione se deseja usar uma conexão SSL segura para este túnel.
  - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming. Esta configuração não bloqueia conexões WiFi e USB.

Configurações do Windows Mobile/CE



- **Usar este túnel para suporte remoto:** selecione se o túnel será usado para suporte remoto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

As etapas de configuração são diferentes, dependendo se você selecionou o suporte remoto.

- Se você não selecionar o suporte remoto, faça o seguinte:
  - **Conexão iniciada por:** clique em **Dispositivo** ou **Servidor** para especificar a origem que inicia a conexão.
  - **Protocolo:** na lista, clique no protocolo a ser usado. O padrão é o **TCP genérico**.
  - **Máximo de conexões por dispositivo:** digite um número para especificar quantas conexões TCP simultâneas o aplicativo pode estabelecer. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
  - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
    - **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
  - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming.

    > Nota:
    > Conexões Wi-Fi e USB não serão bloqueadas.

  - **Redirecionar para o XenMobile:** na lista, clique na opção de conexão do dispositivo ao XenMobile. O padrão é **Através de configurações de aplicativo**.
    - Se você selecionar **Usando um alias local**, digite o alias no **Alias local**. O padrão é **localhost**.
    - Se você selecionar **Um intervalo de endereços IP**, digite o endereço IP inicial em **Intervalo de endereços IP de** e digite o endereço IP final em **Intervalo de endereços IP para**.
  - **Porta do cliente:** digite o número da porta. Na maioria dos casos, esse valor é o mesmo para a porta do servidor.
  - **Endereço IP ou nome do servidor:** digite o endereço IP ou nome do servidor do aplicativo. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
  - **Porta do servidor:** digite o número de porta do servidor.
- Se você selecionar o suporte remoto, faça o seguinte:
  - **Usar este túnel para suporte remoto:** defina como **Ativado**.
  - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
    - **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
  - **Usar conexão SSL:** selecione se deseja usar uma conexão SSL segura para este túnel.
  - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming. As conexões Wi-Fi e USB não são bloqueadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de desinstalação de aplicativo

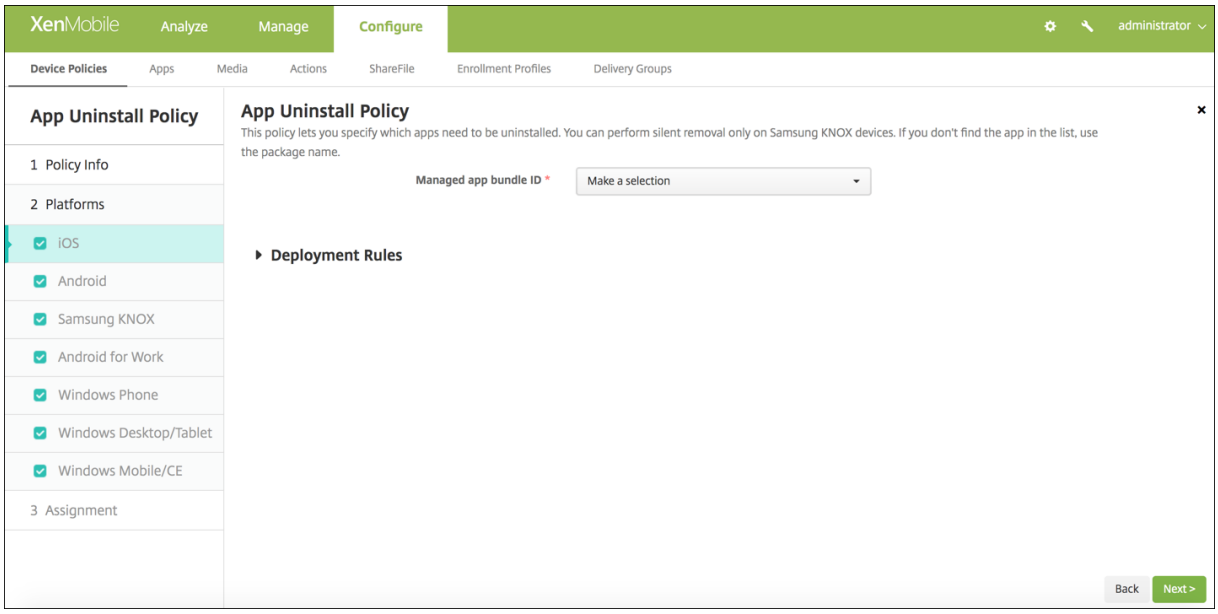
April 15, 2019

Você pode criar uma política de desinstalação de aplicativo para as plataformas iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet e Windows Mobile/CE. Uma política de desinstalação de aplicativo permite que você remova aplicativos dos dispositivos do usuário por uma série de razões. Talvez você não deseje mais oferecer compatibilidade com determinados aplicativos, sua empresa pode desejar substituir os aplicativos existentes por aplicativos semelhantes de diferentes fornecedores e assim por diante.

Os aplicativos são removidos quando essa política é implantada nos dispositivos dos usuários. Com exceção dos dispositivos Samsung KNOX, os usuários recebem um prompt para desinstalar o aplicativo. Os usuários de dispositivos Samsung KNOX não recebem um aviso para desinstalar o aplicativo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



- **ID de pacote de aplicativos gerenciados:** na lista, clique em um aplicativo existente ou em **Adicionar novo**. Se não houver nenhum aplicativo configurado para essa plataforma, a lista estará vazia e você deverá adicionar um novo aplicativo.
  - Quando você clica em **Adicionar**, aparece um campo em que você pode digitar um nome de aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Todas as outras configurações da plataforma

- **Aplicativos a desinstalar:** para cada aplicativo que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do aplicativo:** na lista, clique em um aplicativo existente ou em **Adicionar novo** para adicionar um novo nome de aplicativo. Se não houver nenhum aplicativo configurado para essa plataforma, a lista estará vazia e você deverá adicionar novos aplicativos.
  - Clique em **Adicionar** para adicionar o aplicativo ou em **Cancelar** para cancelar a adição do aplicativo.

Desinstalar um aplicativo corporativo automaticamente depois que o aplicativo da loja de aplicativos pública correspondente for instalado

Você pode configurar o XenMobile para remover a versão corporativa dos aplicativos Citrix após a instalação da versão da loja de aplicativos pública. Esse recurso evita que os dispositivos dos usuários tenham dois ícones de aplicativo idênticos após a instalação da versão da loja de aplicativos pública.

Uma condição de implantação para a Política de dispositivo de desinstalação de aplicativo dispara o XenMobile para remover aplicativos mais antigos de dispositivos de usuários durante a instalação da nova versão. Esse recurso está disponível somente 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 de aplicativos gerenciados** para o aplicativo Empresarial.
- Adicionar uma regra: Clique em **Nova regra** e, em seguida, como mostrado no exemplo, escolha **Nome do aplicativo instalado** e **é igual a**. Digite a ID do pacote de aplicativo para o aplicativo de loja de aplicativos pública.

No exemplo, quando o aplicativo da loja de aplicativos pública (com.citrix.mail.ios) é instalado em um dispositivo nos grupos de entrega especificados, o XenMobile remove a versão Empresarial (com.citrix.mail).

Política de dispositivo de restrições de desinstalação de aplicativo

April 15, 2019

Você pode especificar os aplicativos que os usuários podem ou não podem desinstalar em um dispositivo Samsung SAFE ou Amazon.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações Samsung SAFE ou Amazon

- **Configurações de restrição de desinstalação de aplicativo:** para cada regra de aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do aplicativo:** na lista, clique em um aplicativo ou em **Adicionar novo** para adicionar um novo aplicativo.
  - **Regra:** selecione se os usuários podem desinstalar o aplicativo. O padrão é permitir a desinstalação.
  - Clique em **Salvar** ou em **Cancelar**.

Política de dispositivo BitLocker

April 15, 2019

O Windows 10 inclui um recurso de criptografia de disco chamado BitLocker, que fornece proteções de arquivos e sistemas adicionais contra o acesso não autorizado de um dispositivo Windows perdido ou roubado. Para obter mais proteção, você pode usar o BitLocker com chips TPM (Trusted Platform Module), versão 1.2 ou posterior. Um chip TPM manipula operações criptográficas e gera, armazena e limita o uso de chaves criptográficas.

Começando com o Windows 10, compilação 1703, as políticas do MDM podem controlar o BitLocker. Você pode usar a política de dispositivo de BitLocker no XenMobile para definir as configurações disponíveis no Assistente de BitLocker nos dispositivos Windows 10. Por exemplo, em um dispositivo com o BitLocker habilitado, o BitLocker pode solicitar aos usuários como eles querem desbloquear sua unidade na inicialização, como fazer backup de sua chave de recuperação e como desbloquear uma unidade fixa. A configuração da política do dispositivo BitLocker também configura o seguinte deve ocorrer ou não:

- Ativar o BitLocker em dispositivos sem chip TPM
- Mostrar opções de recuperação na interface BitLocker.
- Negar acesso de gravação a uma unidade fixa ou removível quando o BitLocker não está habilitado.

> Nota:
>
> Depois de a criptografia BitLocker ter sido iniciada em um dispositivo, você não pode alterar posteriormente as configurações de BitLocker no dispositivo por meio da implantação de uma atualização da política BitLocker no dispositivo.

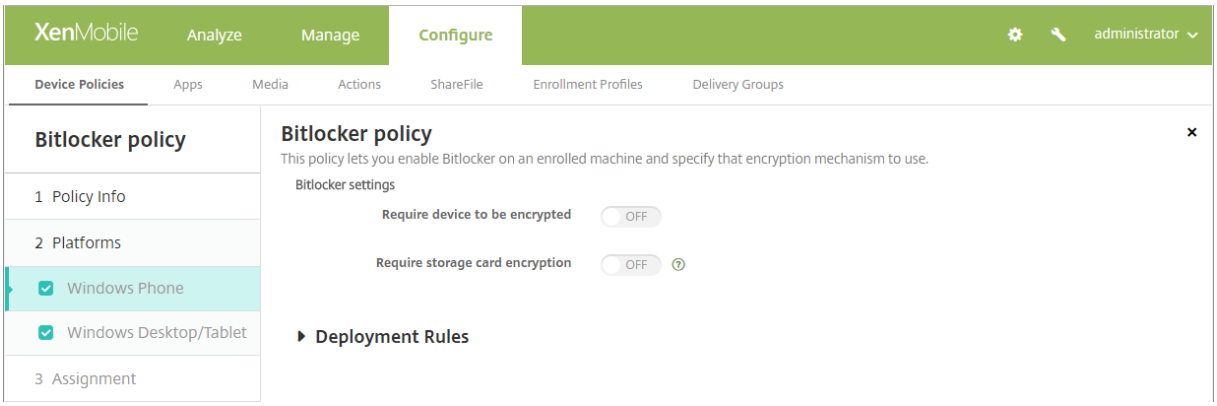
Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos

- A política de dispositivo BitLocker requer o Windows 10 Enterprise Edition.
- Antes de implantar a política do dispositivo BitLocker, prepare seu ambiente para o uso do BitLocker. Para obter informações detalhadas da Microsoft, incluindo requisitos e configuração do sistema BitLocker, consulte BitLocker e os artigos abaixo daquele nó.

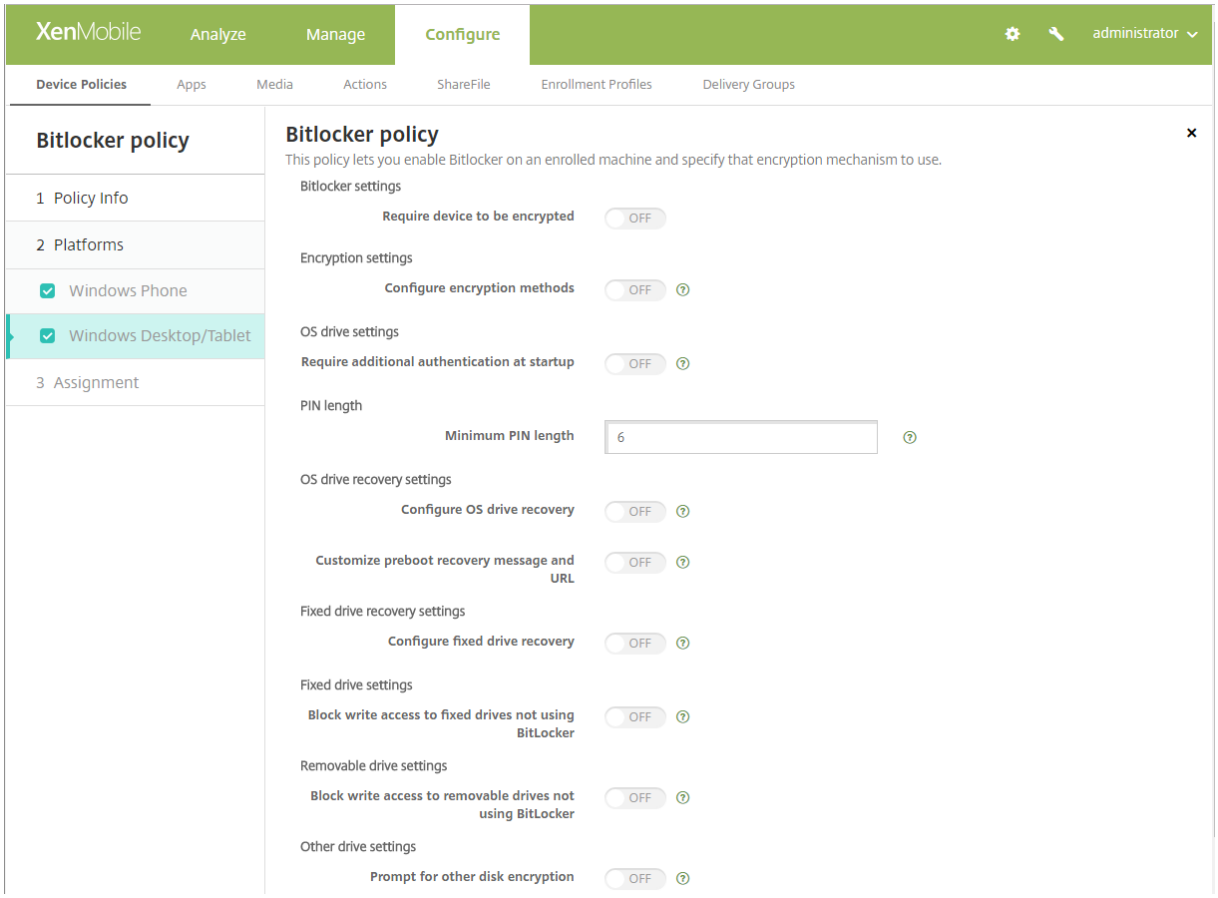
Configurações do Windows Phone



- **Exigir que o dispositivo seja criptografado:** determina se os usuários devem para ativar a criptografia de BitLocker em um cartão de sistema do Windows Phone. Se o valor for **Ativado**, os dispositivos mostram uma mensagem após a conclusão do registro, indicando que a empresa requer criptografia do dispositivo. Se o usuário optar por não gerenciar a criptografia do dispositivo, o usuário não terá acesso para gravar na placa de sistema. Se o valor for **Desativado**, o usuário não é solicitado e a política de BitLocker determina se o dispositivo está criptografado. O padrão é **Desativado**.
- **Exigir criptografia de cartão de armazenamento:** determina se os usuários devem ativar a criptografia de BitLocker em um cartão de armazenamento do Windows Phone. Se o valor for **Ativado**, a criptografia de cartão de armazenamento é necessária para obter a permissão de gravação no cartão. O padrão é **Desativado**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Desktop e Tablet



- **Exigir que o dispositivo seja criptografado:** determina se os usuários devem para ativar a criptografia de BitLocker em um cartão de sistema do Windows Desktop ou Tablet. Se o valor for **Ativado**, os dispositivos mostram uma mensagem após a conclusão do registro, indicando que a empresa requer criptografia do dispositivo. Se o valor for **Desativado**, o usuário não é solicitado e o BitLocker usa as configurações de política. O padrão é **Desativado**.
- **Configurar métodos de criptografia:** determina os métodos de criptografia a serem usados para tipos de unidade específicos. Se o valor for **Desativado**, o Assistente para BitLocker solicita ao usuário para identificar 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 as unidades removíveis é AES-CBC de 128 bits. Se o valor for **Ativado**, o BitLocker usa o método de criptografia especificado na política. Se o valor for **Ativado**, essas configurações adicionais são exibidas: **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 necessária durante a inicialização do dispositivo. Especifica se deseja permitir BitLocker em dispositivos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

que não têm um chip TPM também. Se o valor for **Desativado**, os dispositivos sem TPM não podem usar criptografia BitLocker. Para obter informações sobre TPM, consulte o artigo da Microsoft, Visão geral da tecnologia Trusted Platform Module. Se o valor for **Ativado**, as seguintes configurações adicionais são exibidas. O padrão é **Desativado**.

- **Bloquear o 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 TPM:** em um dispositivo com TPM, há quatro modos de desbloquear: 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 um usuário forneça dados de desbloqueio adicionais. O dispositivo do usuário desbloqueie automaticamente durante a reinicialização, usando a chave de criptografia do chip TPM. O padrão é **Permitir TPM**.
- **PIN de inicialização TPM:** esta configuração é o modo de desbloqueio TPM + PIN. Um PIN pode ter até 20 dígitos. Use a configuração de **Comprimento mínimo do PIN** para especificar o tamanho mínimo do PIN. Um usuário configura um PIN durante a instalação do BitLocker e fornece o PIN durante a inicialização do dispositivo.
- **Chave de inicialização 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 TPM e PIN**: esta configuração é o modo de desbloqueio TPM + PIN + Chave.

  Se o desbloqueio for bem-sucedido, o sistema operacional inicia o carregamento. Se o desbloqueio falhar, o dispositivo entra no modo de recuperação.

- **Comprimento mínimo do PIN:** o tamanho mínimo do PIN de inicialização do TPM. O padrão é **6**.
- **Configurar recuperação da unidade do sistema operacional:** se a etapa de desbloqueio falhar, o BitLocker solicita ao usuário a chave de recuperação configurada. Essa configuração define as opções de recuperação da unidade do sistema operacional, disponíveis para os usuários que não tenham 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 deseja ou não permitir um agente de recuperação de dados baseado em certificado. Adicione um agente de recuperação de dados das Políticas de chave pública, que está localizado no

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Microsoft Configurações da Política de Grupo do BitLocker. O padrão é **Desativado**.

- **Criar senha de recuperação de 48 dígitos para recuperação da unidade do sistema operacional:** especifica se você deseja permitir ou exigir que os usuários usem uma senha de recuperação. O BitLocker gera a senha e a armazena em um arquivo ou conta do Microsoft Cloud. O padrão é **Permitir senha de 48 dígitos**.
- **Criar chave de recuperação de 256 bits:** especifica se você deseja 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 uma chave de recuperação de 256 bits**.
- **Ocultar opções de recuperação da unidade do sistema operacional:** especifica se você deseja mostrar ou ocultar as opções de recuperação na interface do BitLocker. Se o valor for **Ativado**, nenhuma opção de recuperação aparece na interface BitLocker. Nesse caso, registre os dispositivos no Active Directory, salve as opções de recuperação no Active Directory e defina **Salvar informações de recuperação no AD DS** para **Ativado**. O padrão é **Desativado**.
- **Salvar informações de recuperação no AD DS:** especifica se deseja 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 deseja armazenar a senha de recuperação do BitLocker ou a senha de recuperação e o pacote de chaves nos Serviços do Domínio Active Directory. Armazenar o pacote de chaves dá suporte à recuperação de dados de uma unidade que está fisicamente corrompida. O padrão é **Senha de recuperação de backup**.
- **Ativar BitLocker depois de armazenar as informações de recuperação no AD DS:** especifica se deseja impedir que os usuários ativem o BitLocker, a menos que o dispositivo esteja conectado ao domínio e o backup das informações de recuperação de BitLocker no Active Directory seja bem-sucedido. Se estiver **Ativado**, um dispositivo deve ser ingressado no domínio antes de iniciar o BitLocker. O padrão é **Desativado**.

- **Personalizar mensagem de recuperação de pré-inicialização e URL:** especifica se o BitLocker mostra uma mensagem personalizada e a URL na tela de recuperação. Se o valor for **Ativado**, as seguintes configurações adicionais são exibidas: **Usar mensagem de recuperação e URL padrão**, **Usar mensagem de recuperação vazia e URL**, **Usar mensagem personalizada de recuperação** e **Usar URL de recuperação personalizada**. Se o valor for **Desativado**, são exibidas a mensagem de recuperação de padrão e a URL. O padrão é **Desativado**.
- **Configurar recuperação da unidade fixa:** configura as opções de recuperação aos usuários para uma unidade fixa de criptografia BitLocker. O BitLocker não exibe uma mensagem aos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

usuários sobre a criptografia de unidade fixa. Para desbloquear uma unidade durante a inicialização, um usuário fornece uma senha ou um cartão inteligente. As configurações de desbloqueio de inicialização, que não estão nesta política, aparecem na interface BitLocker quando um usuário habilita a criptografia BitLocker em uma unidade fixa. Para obter informações sobre as configurações relacionadas, consulte **Configurar recuperação da unidade do sistema operacional**, anteriormente nessa 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 o 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 o BitLocker. Defina essa configuração dependendo se a sua organização permite ou não o acesso de gravação em unidades removíveis de outra organização. O padrão é **Desativado**.
- **Solicitar outra criptografia de disco:** permite que você desabilite a mensagem de aviso para outra criptografia de disco em dispositivos. O padrão é **Desativado**.

Política de dispositivo de navegador

April 15, 2019

Você pode criar políticas de dispositivo de navegador para dispositivos Samsung SAFE ou Samsung KNOX para definir se os dispositivos do usuário podem usar o navegador ou para limitar as funções do navegador que os dispositivos podem usar.

Nos dispositivos Samsung, você pode desativar completamente o navegador ou pode ativar ou desativar pop-ups, JavaScript, cookies, preenchimento automático e decidir se deseja impor avisos de fraude.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Samsung SAFE e do Samsung KNOX

- **Desativar navegador:** selecione se o navegador Samsung deve ser desativado completamente nos dispositivos dos usuários. O padrão é **O**, o que permite que os usuários usem o navegador. Quando você desativa o navegador, as opções a seguir desaparecem.
- **Desativar pop-up:** selecione se mensagens pop-up são permitidas no navegador.
- **Desativar Javascript:** selecione se JavaScript pode ser executado no navegador.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Desativar cookies:** selecione se você deseja permitir cookies.
- **Desativar preenchimento automático:** selecione se os usuários têm permissão para ativar a função de preenchimento automático do navegador.
- **Forçar aviso de fraude:** selecione se um aviso deverá ser exibido quando os usuários visitarem um site fraudulento ou comprometido.

Política de dispositivo de calendário (CalDav)

April 15, 2019

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 compatível com CalDAV.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de 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 à qual o servidor CalDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CalDAV deve ser usada. O padrão é **I**.

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 à qual o servidor CalDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CalDAV deve ser usada. O padrão é **I**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo celular

April 15, 2019

Essa política permite que você defina as configurações da rede celular em um dispositivo iOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Anexar APN**
  - **Nome:** um nome para essa configuração.
  - **Tipo de autenticação:** na lista, clique em Protocolo CHAP (**CHAP**) ou em Protocolo PAP (**PAP**). O padrão é **PAP**.
  - **Username** e **Password:** o nome do usuário e a senha que deseja usar para autenticação.
- **APN**
  - **Nome:** um nome para a configuração Nome do ponto de acesso (APN).
  - **Tipo de autenticação:** na lista, clique em **CHAP** ou **PAP**. O padrão é **PAP**.
  - **Username** e **Password:** o nome do usuário e a senha que deseja usar para autenticação.
  - **Servidor proxy:** o endereço de rede do servidor proxy.
  - **Porta do servidor proxy:** a porta do servidor proxy.

Política de dispositivo do gerenciador de conexões

April 15, 2019

No XenMobile, você pode especificar as configurações de conexão dos aplicativos que se conectam automaticamente à Internet e a redes privadas. Essa política está disponível somente em Windows Pocket PCs.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Mobile/CE

> Nota:
>
> **Escritório interno** significa que todas as conexões estão na intranet da sua empresa. **Internet integrada** significa que todas as conexões são para a Internet.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Aplicativos que se conectam a uma rede privada usam automaticamente:** na lista, clique em **Escritório interno** ou **Internet integrada**. O padrão é **Escritório interno**.
- **Aplicativos que se conectam à Internet automaticamente usam:** na lista, clique em **Escritório interno** ou **Internet integrada**. O padrão é **Escritório interno**.

Política de dispositivo de agendamento de conexão

April 15, 2019

Crie políticas de agendamento de conexão para controlar como e quando os dispositivos do usuário se conectam ao XenMobile. Observe que você pode configurar essa política também para dispositivos ativados para Android for Work.

Você pode especificar que os usuários conectem os dispositivos deles manualmente, que os dispositivos se mantenham conectados permanentemente ou que os dispositivos se conectem em um período de tempo definido.

Para adicionar ou configurar essa política, acesse **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 esse agendamento.
  - **Sempre:** manter a conexão ativa de forma permanente. O XenMobile no dispositivo do usuário tenta se reconectar ao servidor XenMobile após uma perda de conexão de rede e monitorará a conexão mediante a transmissão de pacotes de controle em intervalos regulares. A Citrix recomenda esta opção para segurança otimizada. Quando você escolher **Sempre**, use também para a **Política de Túnel** do dispositivo, 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 por push, como apagar ou bloquear o dispositivo sob demanda. Você também deve selecionar a opção **Cronograma de implantação Implantar para conexões permanentes** em cada política implantada no dispositivo.
  - **Nunca:** conectar manualmente. Os usuários têm de iniciar a conexão no XenMobile, nos seus dispositivos. A Citrix não recomenda essa opção para implantações de produção, pois ela impede que você implante políticas de segurança nos dispositivos e, portanto, os usuários nunca receberão novos aplicativos ou políticas.
  - **A cada:** conectar no intervalo designado. Quando essa opção está em vigor e você envia uma política de segurança, como um bloqueio ou um apagamento, o XenMobile processa

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a ação no dispositivo na próxima vez em que ele se conectar. Quando você seleciona essa opção, o campo **Conectar a cada N minutos** é exibido, em que você deve digitar o número de minutos após o qual o dispositivo deve reconectar. O padrão é **20**.

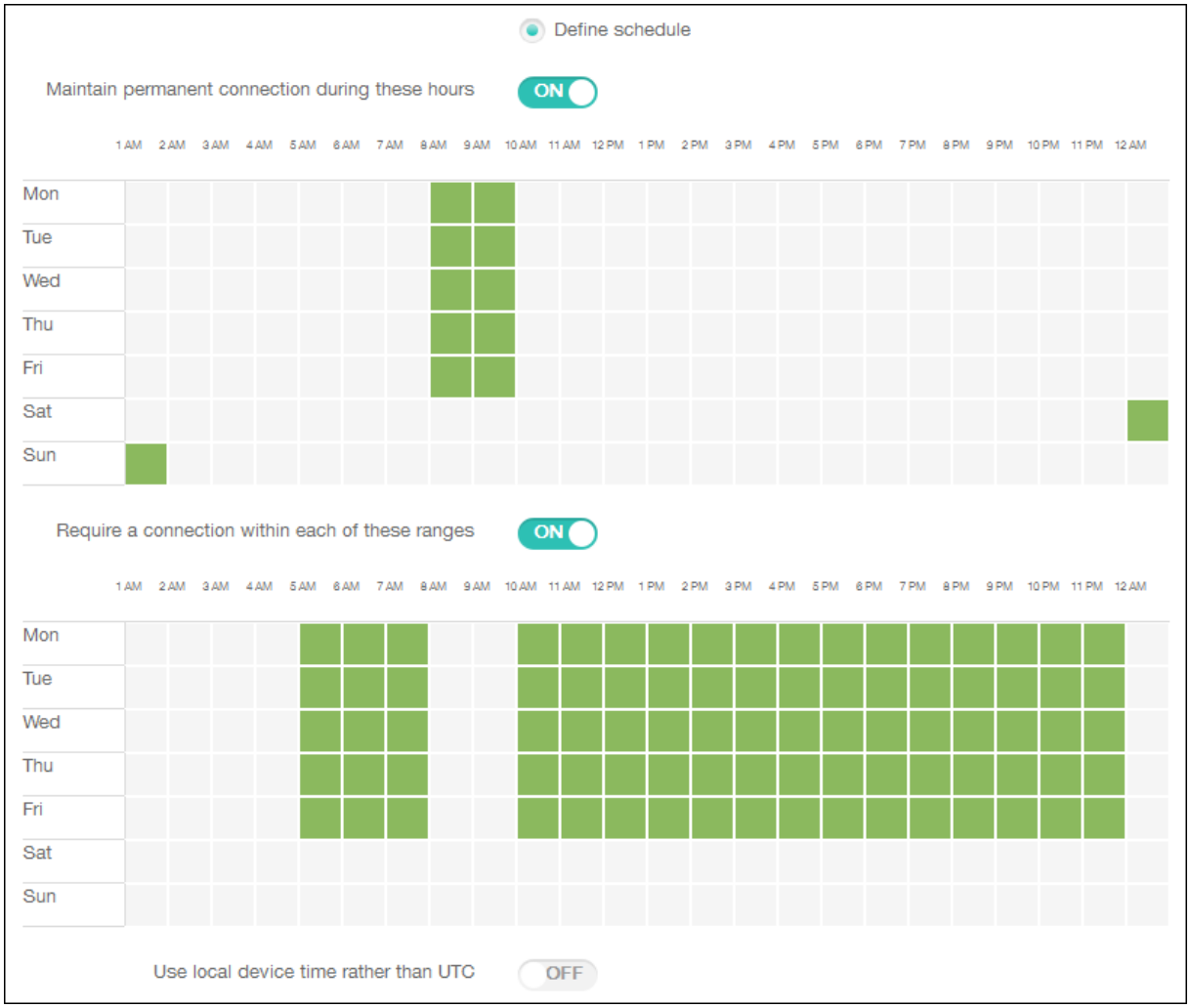
- **Definir programação:** quando ativada, o XenMobile no dispositivo do usuário tenta se reconectar ao XenMobile Server após uma perda de conexão de rede e monitora a conexão mediante a transmissão de pacotes de controle em intervalos regulares no período de tempo que você definir. Consulte Definição de um período de tempo de conexão, mais adiante, para saber como definir um período de tempo de conexão.
  * **Manter a 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 destes intervalos:** os dispositivos dos usuários devem ser conectados pelo menos uma vez em qualquer um dos períodos de tempo definidos.
  * **Usar hora do dispositivo local em vez de UTC:** sincronizar os períodos de tempo definidos para o horário local do dispositivo em vez do Tempo Universal Coordenado (UTC).

Definição de um período de tempo de conexão

Quando você ativa as opções a seguir, é exibida uma linha do tempo na qual você pode definir os períodos de tempo que desejar. Você pode ativar uma ou ambas as opções para exigir uma conexão permanente durante horários específicos ou para exigir uma conexão em determinados períodos de tempo. Cada quadrado na linha do tempo é 30 minutos, portanto, se você desejar uma conexão entre 8:00 e 9:00 da manhã todo dia da semana, clique nos dois quadrados na linha do tempo entre 8 e 9 da manhã todo dia da semana.

Por exemplo, as duas linhas do tempo na figura a seguir exigem uma conexão permanente entre 8:00 e 9:00 da manhã todo dia da semana, uma conexão permanente entre 12:00 da manhã de sábado e 1:00 da manhã de domingo e pelo menos uma conexão todo dia da semana entre 5:00 e 8:00 da manhã ou entre 10:00 da manhã e 11:00 da noite.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Política de dispositivo de contatos (CardDAV)

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para adicionar uma conta de contatos do iOS (CardDAV) aos dispositivos iOS ou macOS dos usuários para permitir que eles sincronizem dados de contato com qualquer servidor compatível com CardDAV.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Porta:** digite a porta à qual o servidor CardDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CardDAV deve ser usada. O padrão é **I**.

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 à qual o servidor CardDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CardDAV deve ser usada. O padrão é **I**.

Política de dispositivo Controlar atualizações do sistema operacional

April 15, 2019

A política de dispositivo Controlar atualizações do sistema operacional permite que você implemente:

- As atualizações mais recentes do sistema operacional a dispositivos iOS com supervisão.

  Para dispositivos que executam o iOS 10.3 e versões posteriores, a política Controlar atualizações do sistema operacional funciona em dispositivos supervisionados. Para dispositivos que executam uma versão anterior ao iOS 10.3, a política Controlar atualizações do sistema operacional funciona em dispositivos supervisionados e registrados no DEP.

- As atualizações mais recentes de sistema operacional e aplicativo para dispositivos macOS registrados em DEP com macOS 10.11.5 e versões posteriores.

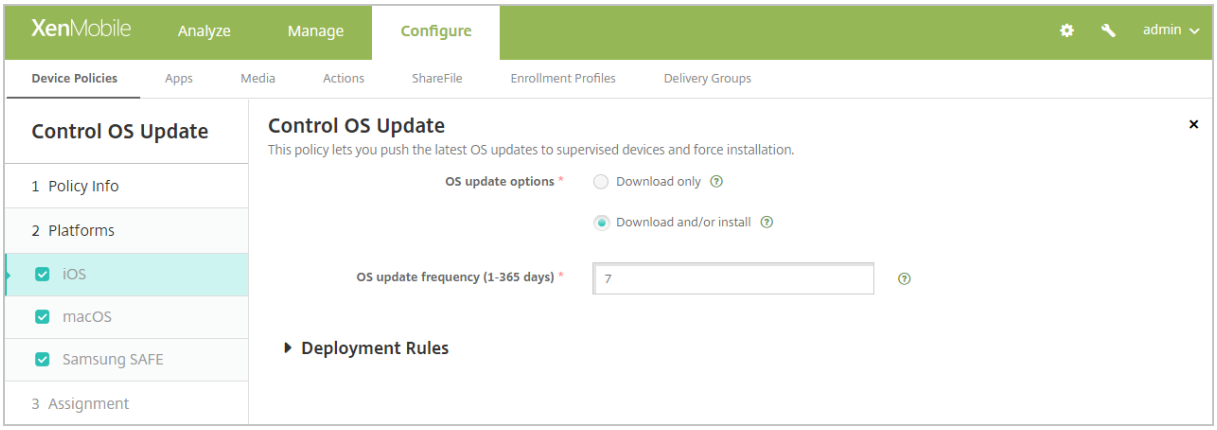
- As atualizações do sistema operacional mais recentes a dispositivos Samsung SAFE com supervisão.

  Nos dispositivos Samsung SAFE, o XenMobile envia a política Controlar atualizações do sistema operacional para o Secure Hub, que então aplica a política ao dispositivo. A página **Gerenciar > Dispositivos** é exibida quando o XenMobile Server envia a política e quando o dispositivo recebe a política.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

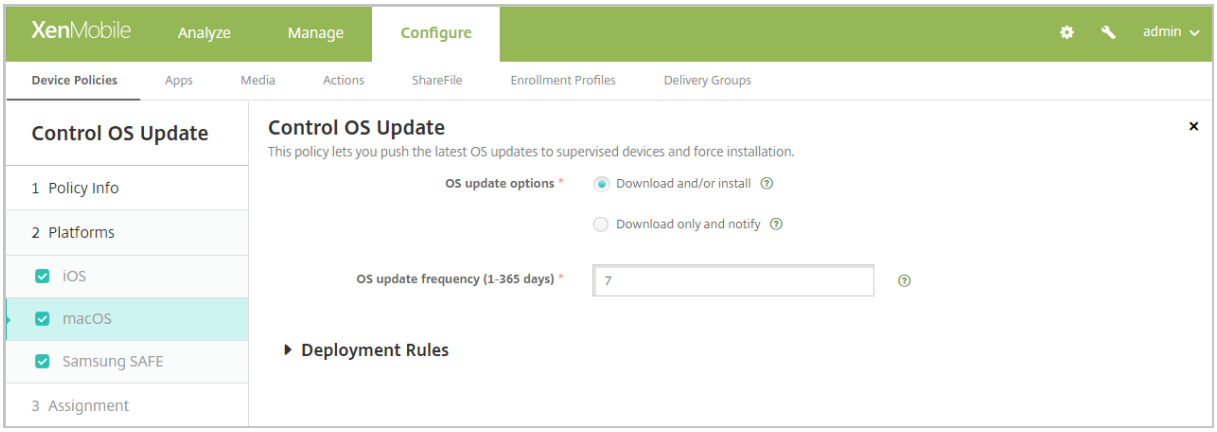
Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



- **Opções de atualização do sistema operacional:** ambas as opções baixam as mais recentes atualizações de sistema operacional para dispositivos supervisionados de acordo com a **frequência de atualização do SO**. O dispositivo solicita que os usuários instalem atualizações. O aviso é visível depois que o usuário desbloqueia o dispositivo.
- **Frequência de atualização do SO:** determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

Configurações do macOS



- **Opções de atualização do sistema operacional:** ambas as opções baixam as mais recentes atualizações de sistema operacional para macOS de acordo com a **frequência de atualização do OS**. Você pode optar por instalar as atualizações ou notificar o usuário por meio da loja de aplicativos que as atualizações estão disponíveis.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

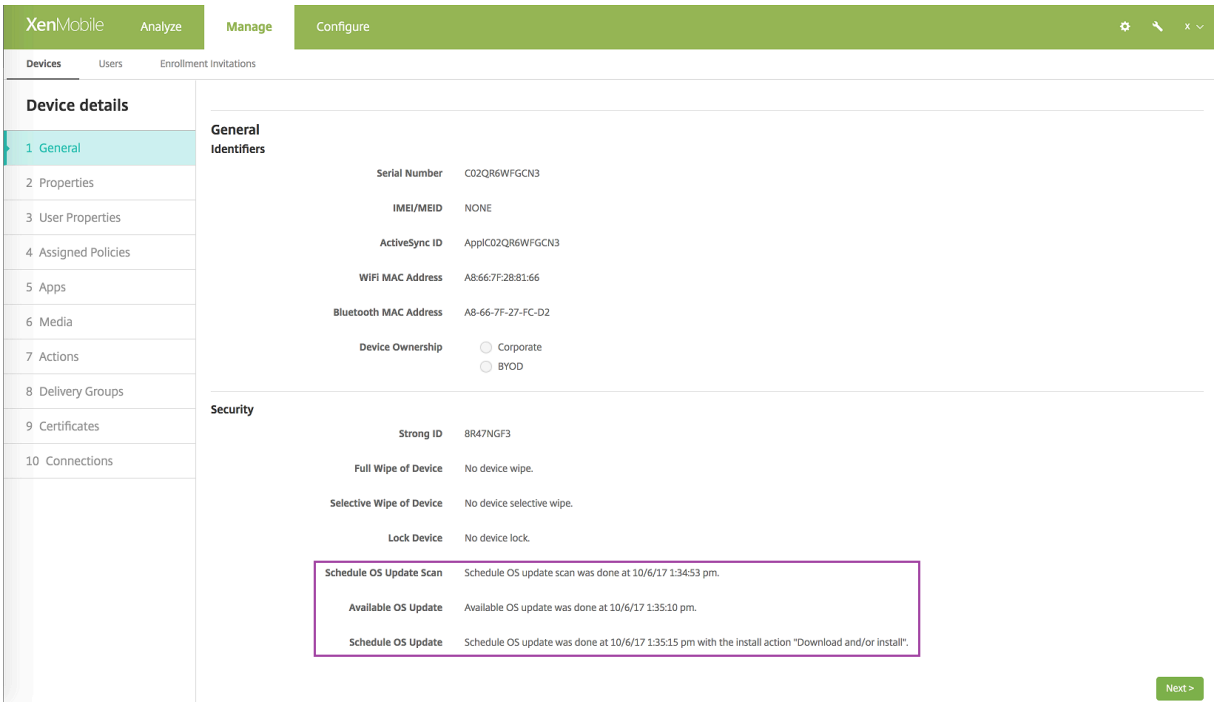
- **Frequência de atualização do SO:** determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

Obter status para ações de atualização do iOS e do macOS

No iOS e macOS, o XenMobile não implementa a política de controle de atualizações do sistema operacional nos dispositivos. Em vez disso, o XenMobile usa a política para enviar esses comandos do MDM para dispositivos:

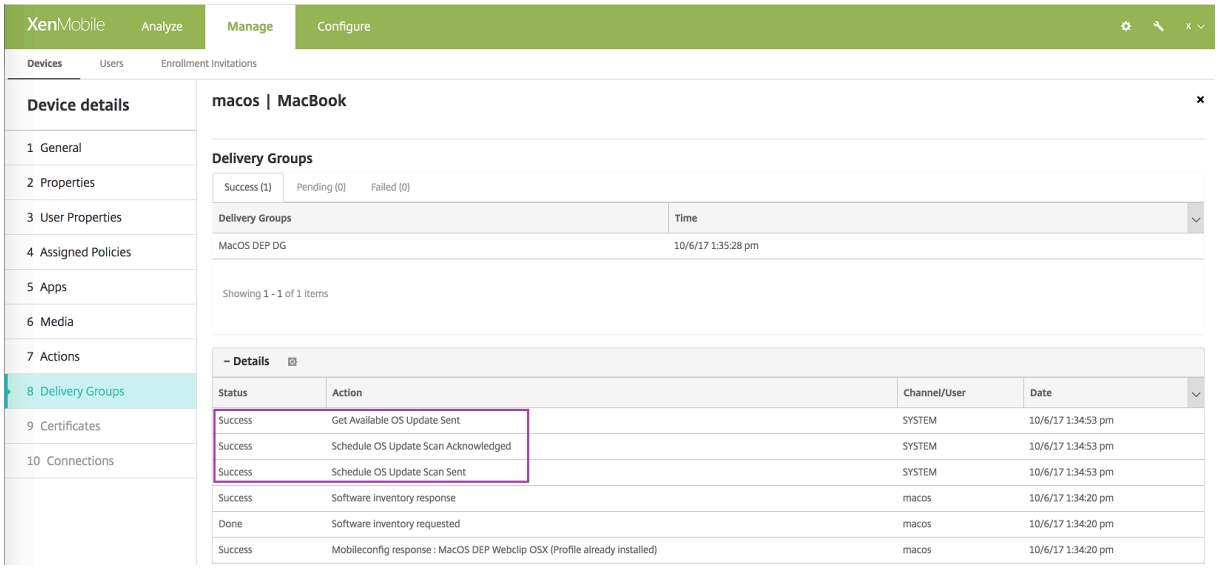
- Cronograma de verificação de atualização do SO: solicita que o dispositivo execute uma verificação em segundo plano de atualizações do sistema operacional. (opcional para iOS)
- Atualização de SO disponível: consulta o dispositivo para obter uma lista de atualizações do sistema operacional disponíveis.
- Planejar atualização de SO: solicita que o dispositivo execute atualizações do macOS, atualizações de aplicativos ou ambas. Assim, o sistema operacional do dispositivo determina quando deve baixar ou instalar as atualizações do sistema operacional e do aplicativo.

A página **Gerenciar > Dispositivos > Detalhes do dispositivo (Geral)** mostra o status das verificações de atualizações agendadas e disponíveis do sistema operacional e atualizações agendadas do macOS e do aplicativo.

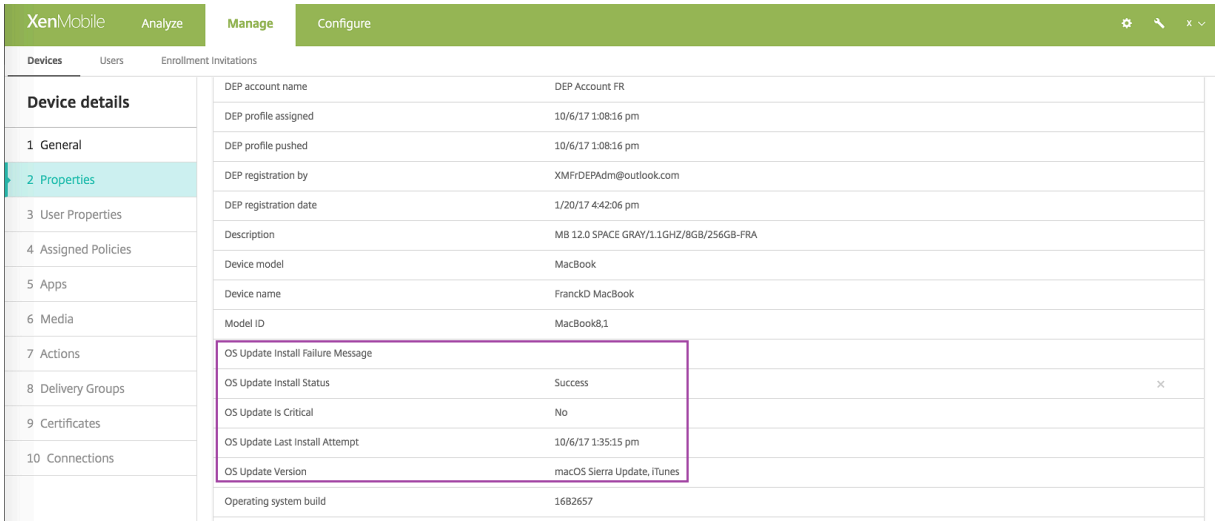


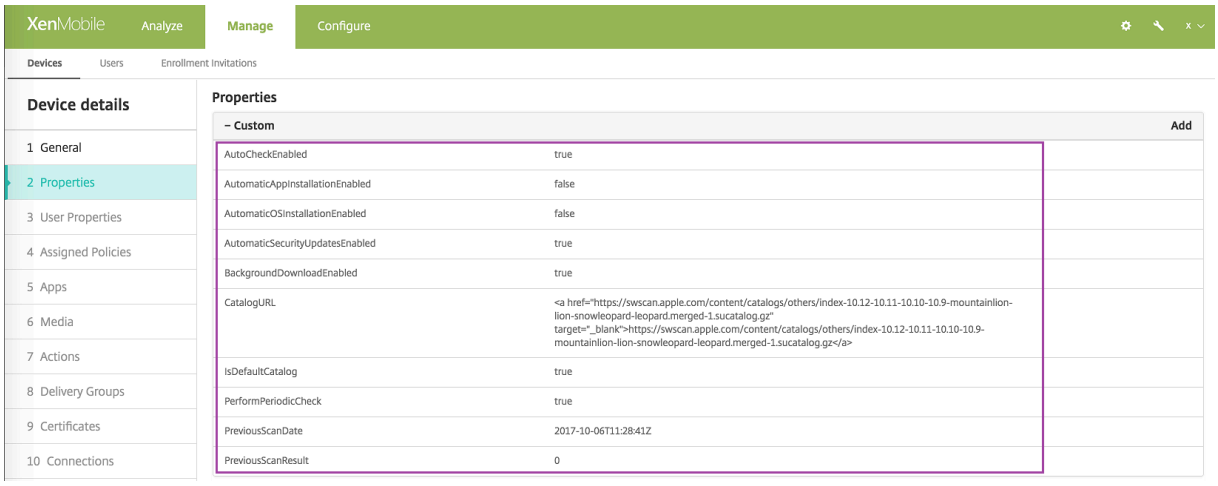
Para obter mais detalhes sobre o status das ações de atualização, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Grupos de entrega)**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para obter detalhes como atualizações disponíveis do sistema operacional e a última tentativa de instalação, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Propriedades)**.



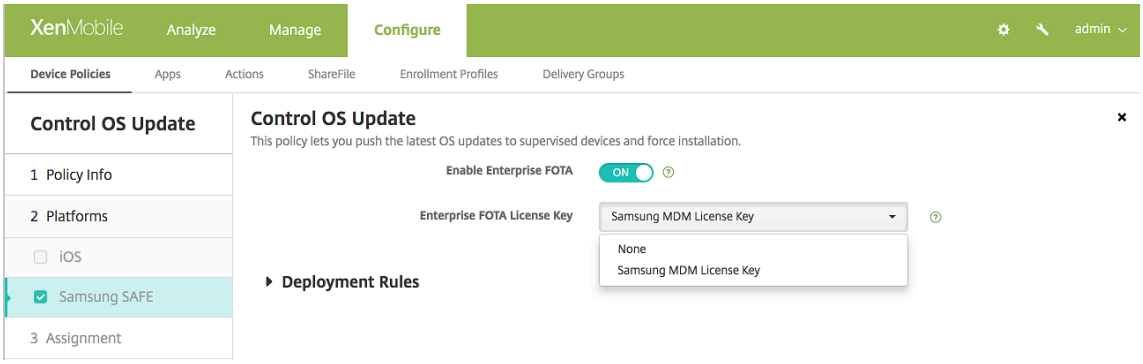


© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Samsung SAFE

O Samsung Enterprise FOTA, também conhecido como E-FOTA, permite determinar quando os dispositivos são atualizados e a versão do firmware a ser usada. Para usar o E-FOTA:

1. Crie uma política de dispositivo chave de licença de MDM Samsung com as chaves e as informações de licença que você recebeu da Samsung. Para obter mais informações, consulte Política de dispositivo de chave de licença MDM Samsung.
2. Crie uma política de dispositivo de controle de atualizações do sistema operacional para habilitar o Enterprise FOTA.



   - **Ativar Enterprise FOTA:** defina como **Ativado**.
   - **Chave de licença Enterprise FOTA:** selecione o nome da política de dispositivo de chave de licença Samsung MDM.

Política de dispositivo Copiar aplicativos para o contêiner da Samsung

April 15, 2019

Para aplicativos que já estão instalados em um dispositivo, você pode especificar a cópia de aplicativos para um contêiner do SEAMS ou para um contêiner do KNOX em dispositivos Samsung com suporte. Para obter informações sobre dispositivos com suporte, consulte o artigo da Samsung Devices built on Knox.

Os aplicativos copiados para o contêiner do SEAMS estão disponíveis nas telas iniciais dos usuários. Os aplicativos copiados para o contêiner KNOX ficam disponíveis somente quando os usuários fazem login no contêiner KNOX.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos

- Registre o dispositivo no XenMobile.
- Implante as chaves MDM da Samsung (ELM e KLM). Para saber como fazer isso, consulte Política de dispositivo de chave de licença MDM Samsung.
- Instale aplicativos no dispositivo.
- Inicialize o KNOX no dispositivo para copiar os aplicativos para o contêiner do KNOX.

Configurações da plataforma

- **Novo aplicativo:** para cada aplicativo que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:
  - Digite um ID de pacote; por exemplo, com.mobiwolf.lacingart para o aplicativo LacingArt.
  - Clique em **Salvar** ou em **Cancelar**.

Política de dispositivo de credenciais

April 15, 2019

Você pode criar políticas de dispositivo de credenciais no XenMobile para ativar a autenticação integrada com sua configuração de PKI no XenMobile, como uma entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor. Para obter mais informações sobre as credenciais, consulte Certificados e autenticação.

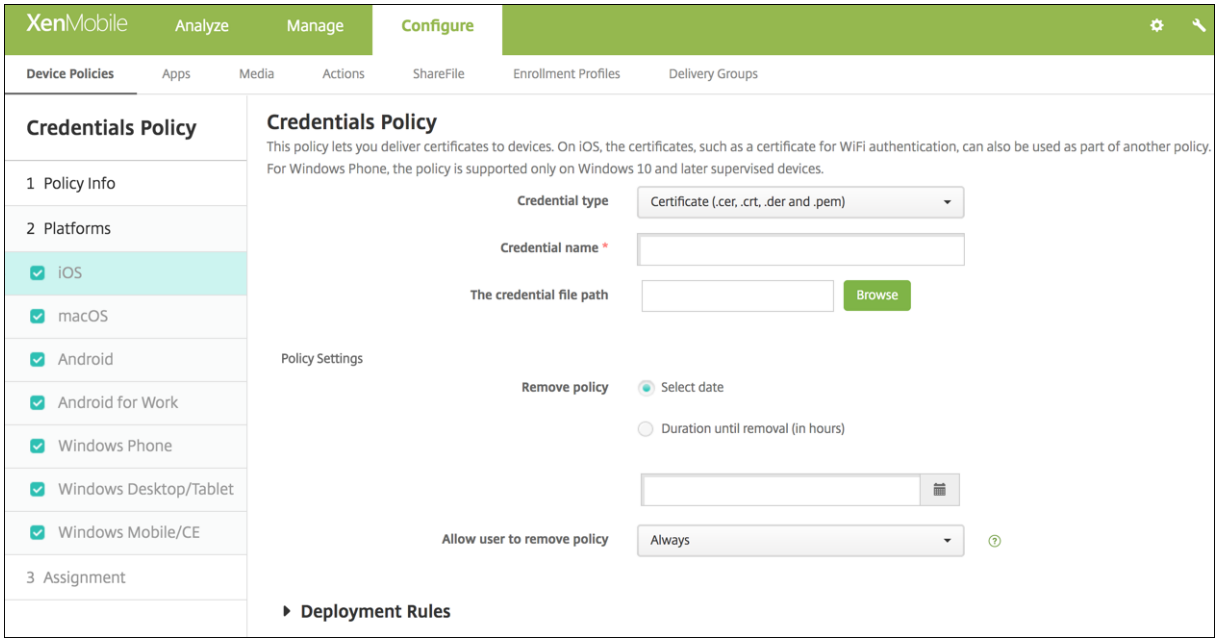
Você pode criar as políticas de credenciais para dispositivos com iOS, macOS, Android, Android for Work, desktop/tablet Windows, Windows Mobile/CE e Windows Phone. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

> Nota:
>
> Antes de criar esta política, você precisa ter as informações de credencial que planeja usar para cada plataforma, além de quaisquer certificados e senhas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS

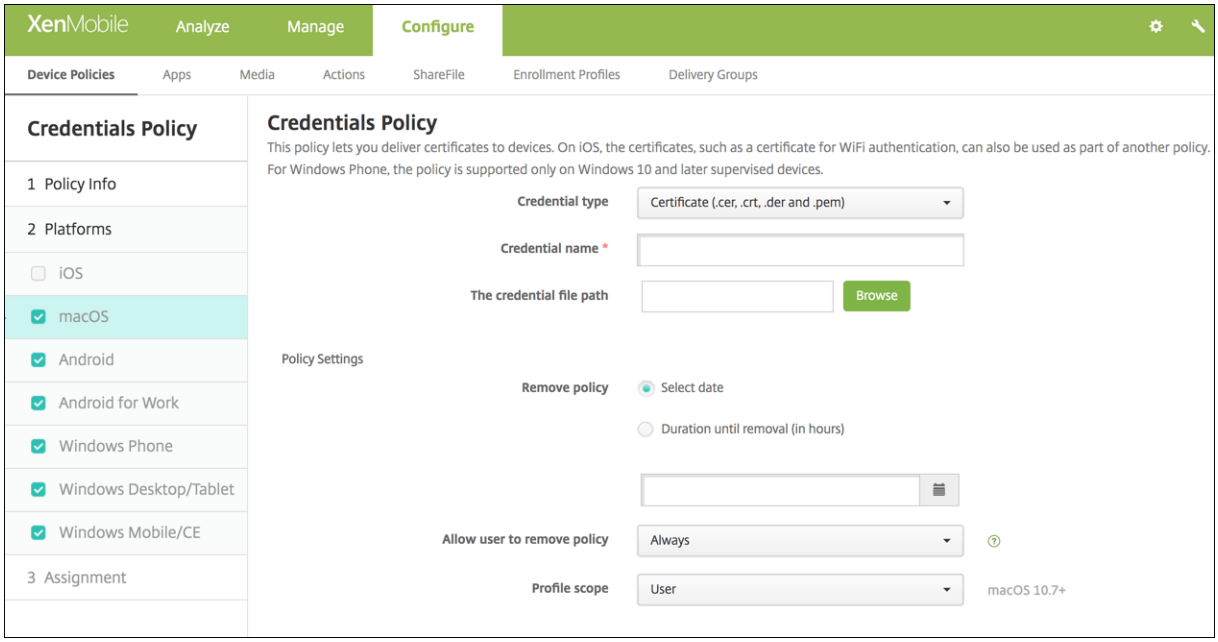


Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e 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 a localização 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 a localização do arquivo.
    - **Senha:** Insira a senha do keystore para a credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** na lista, clique no certificado a ser usado.
  - **Provedor de credenciais**
    - **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do macOS

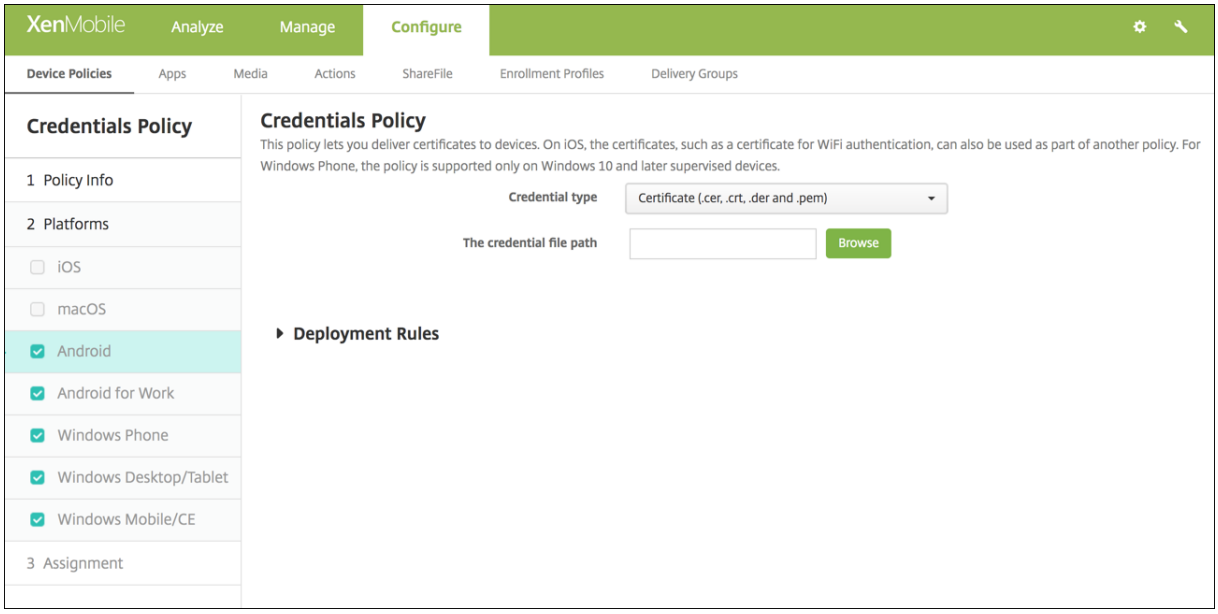


Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e 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 a localização 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 para a localização do arquivo.
    - **Senha:** Insira a senha do keystore para a credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** na lista, clique no certificado a ser usado.
  - **Provedor de credenciais**
    - **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android e do Android for Work

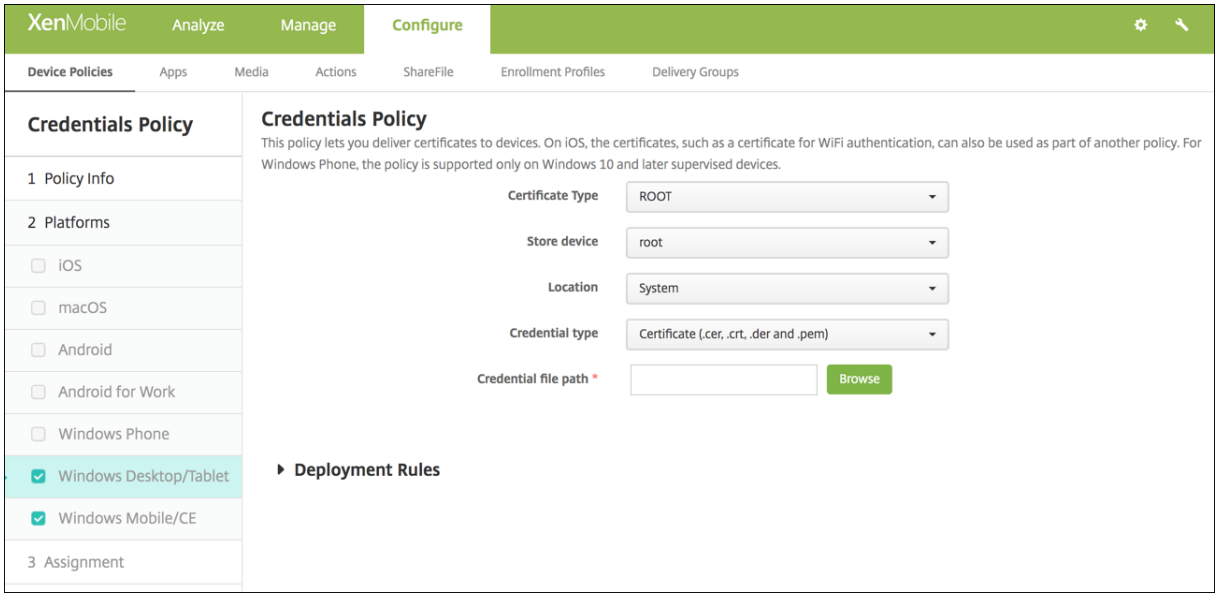


Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e insira as seguintes informações para a credencial selecionada:
  - **Certificado**
    - **Nome da credencial:** digite um nome exclusivo para a credencial.
    - **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em Procurar e navegando para a localização do arquivo.
  - **Keystore**
    - **Nome da credencial:** digite um nome exclusivo para a credencial.
    - **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
    - **Senha:** digite a senha do keystore para a credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** na lista, clique no certificado a ser usado.
  - **Provedor de credenciais**
    - **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

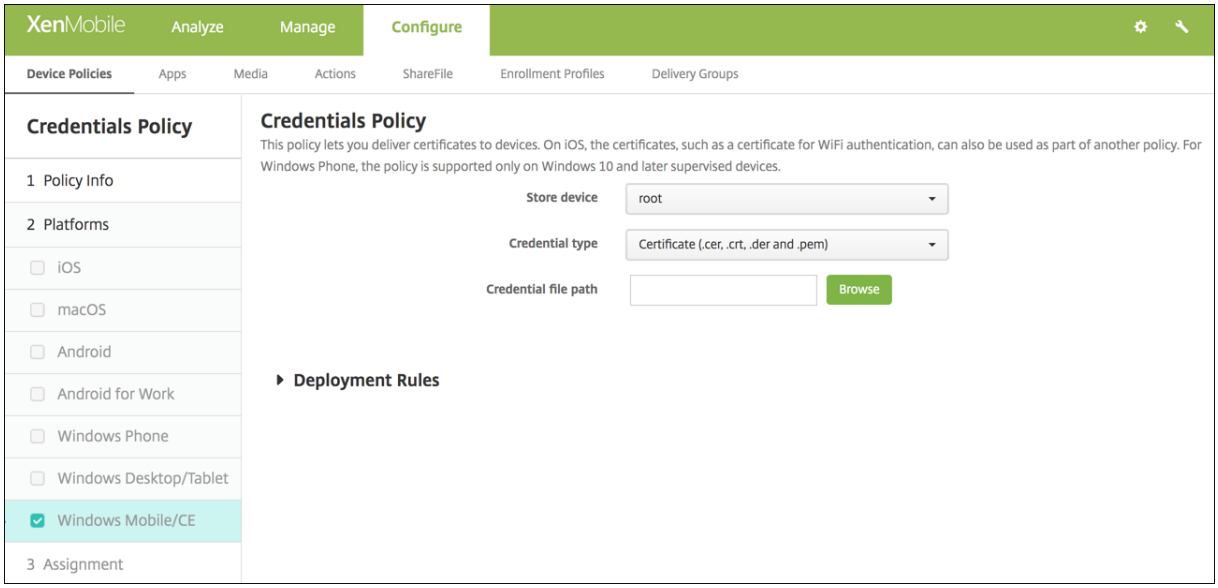
Configurações do Windows Desktop/Tablet



- **Tipo de Certificado:** na lista, clique em **RAIZ** ou **CLIENTE**.
- Se você clicar em **RAIZ**, defina estas configurações:
  - **Dispositivo de armazenamento:** na lista, clique em **raiz**, **Meu** ou **CA** referente à localização do repositório de certificados para a credencial. **Meu** armazena o certificado em repositórios de certificados dos usuários.
  - **Localização:** em Tablets Windows 10, **Sistema** é a única localização.
  - **Tipo de credencial:** em Tablets Windows 10, **Certificado** é o único tipo de credencial.
  - **Caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
- Se você clicar em **CLIENTE**, defina estas configurações:
- **Localização:** em Tablets Windows 10, **Sistema** é a única localização.
- **Tipo de credencial:** em Tablets Windows 10, **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 credencial clicando em **Procurar** e navegando para a localização do arquivo.
- **Senha:** digite a senha associada à credencial. Este campo é obrigatório.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

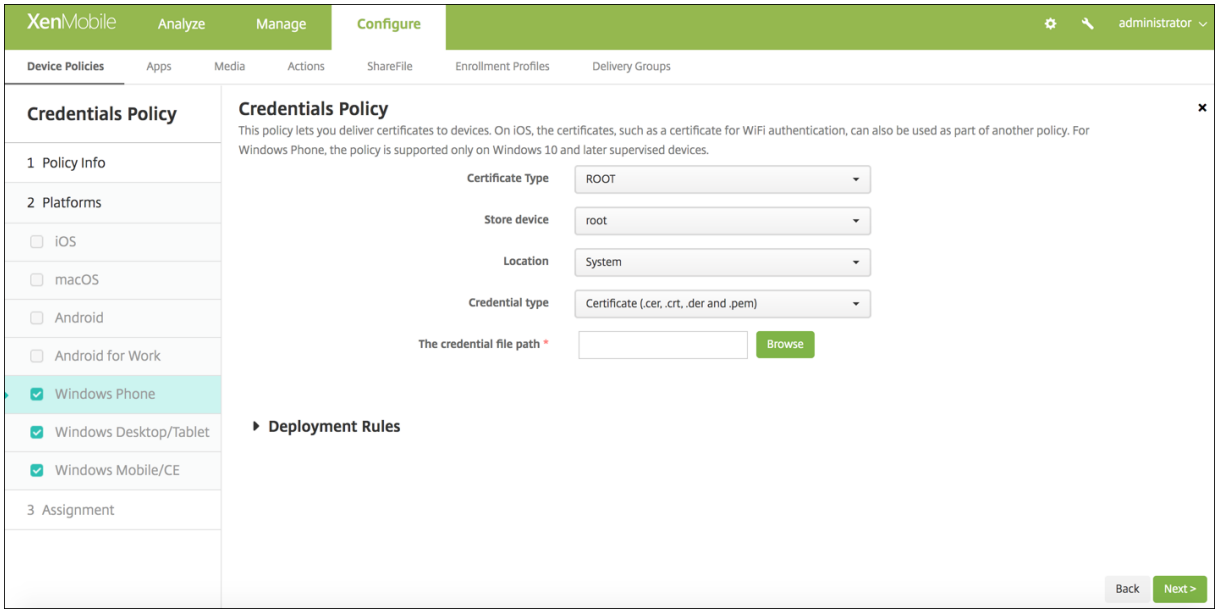
Configurações do Windows Mobile/CE



- **Dispositivo de armazenamento:** na lista, clique na localização do repositório de certificados para a credencial. O padrão é **raiz**. As opções são:
  - **Autoridades confiáveis de execução privilegiada:** os aplicativos assinados com um certificado pertencente a esse repositório serão executados com nível de confiança privilegiada.
  - **Autoridades confiáveis de execução não privilegiada:** os aplicativos assinados com um certificado pertencente a esse repositório serão executados com nível de confiança normal.
  - **SPC (Certificado de Editor de Software):** o Software Publishing Certificate (SPC) é usado para assinar arquivos .cab.
  - **raiz:** um repositório de certificados que contém certificados raiz ou autoassinados.
  - **CA:** um repositório de certificados que contém informações de criptografia, incluindo autoridades de certificação intermediárias.
  - **MEU:** um repositório de certificados que contém certificados pessoais do usuário final.
- **Tipo de credencial:** certificado é o único tipo de credencial para telefones Windows Mobile/CE.
- **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Phone



- **Tipo de Certificado:** na lista, clique em **RAIZ** ou **CLIENTE**.
- Se você clicar em **RAIZ**, defina estas configurações:
  - **Dispositivo de armazenamento:** na lista, clique em **raiz**, **Meu** ou **CA** referente à localização do repositório de certificados para a credencial. **Meu** armazena o certificado em repositórios de certificados dos usuários.
  - **Localização:** sistema é a única localização no caso de telefones Windows.
  - **Tipo de credencial:** certificado é o único tipo de credencial dos telefones Windows.
  - **Caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
- Se você clicar em **CLIENTE**, defina estas configurações:
  - **Localização:** em telefones Windows, **Sistema** é a única localização.
  - **Tipo de credencial:** em telefones Windows, **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 credencial clicando em **Procurar** e navegando para a localização do arquivo.
  - **Senha:** digite a senha associada à credencial. Este campo é obrigatório.

Política de dispositivo de XML personalizado

April 15, 2019

Você pode criar políticas de XML personalizado no XenMobile para personalizar os seguintes recursos em dispositivos Windows e Android Zebra com suporte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Provisionamento, o que inclui configurar o dispositivo e ativar ou desativar recursos
- Configuração do dispositivo, o que inclui permitir que os usuários alterem configurações e parâmetros do dispositivo
- Atualizações de software, incluindo o fornecimento de novos softwares ou correções de bugs a serem carregados no dispositivo, entre eles softwares do sistema e aplicativos
- Gerenciamento de falhas, o que inclui receber relatórios de erro e status do dispositivo

Para dispositivos Windows, crie sua configuração de XML personalizado usando a API Open Mobile Alliance Device Management (OMA DM) no Windows. A criação do 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 OMA Device Management no site da Microsoft Developer Network.

Para dispositivos Android Zebra, crie sua configuração de XML personalizado usando o MX Management System (MXMS). A criação do XML personalizado com a API MXMS está além do escopo deste artigo. Para obter mais informações sobre como usar o MXMS, consulte About MX no site do Zebra.

> Nota:
>
> Para telefones Windows 10 RS2, depois que uma política de XML personalizado ou de Restrições que desativa o Internet Explorer é implantada no telefone, o navegador permanece ativado. Para resolver esse problema, reinicie o telefone. Esse é um problema de terceiros.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma

- **Conteúdo XML:** digite ou recorte e cole o código XML personalizado que você desejar adicionar à política.

  Depois que você clica em **Avançar**, o XenMobile verifica a sintaxe do conteúdo XML. Todos os erros de sintaxe são exibidos abaixo da caixa de conteúdo. Corrija todos os erros antes de continuar.

  Se não houver nenhum erro de sintaxe, a página de atribuição **Política de XML personalizado** será exibida.

Política de dispositivo do Defender

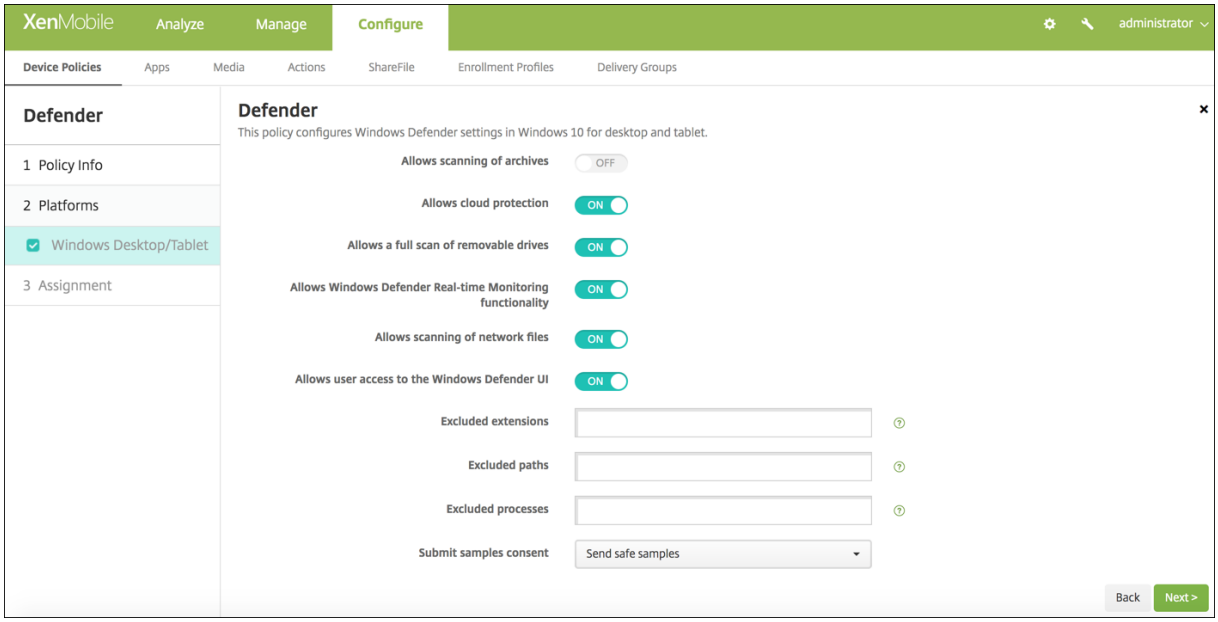
April 15, 2019

O Windows Defender é uma proteção contra malware incluída com o Windows 10. Você pode usar a política de dispositivo do XenMobile, Defender, para configurar a política do Microsoft Defender para o Windows 10 para desktop e tablet.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Desktop e Tablet



- **Permite exame de arquivos:** permite ou proíbe que o Defender examine arquivos armazenados. O padrão é **Desativado**.
- **Permite proteção da nuvem:** permite ou proíbe que o Defender envie informações à Microsoft sobre atividades de malware. O padrão é **Ativado**.
- **Permite exame completo de unidades removíveis:** permite ou proíbe que o Defender examine unidades removíveis, como pen drives. O padrão é **Ativado**.
- **Permite funcionalidade de monitoramento em tempo real do Windows Defender:** o padrão é **Ativado**.
- **Permite exame de arquivos de rede:** permite ou proíbe que o Defender examine arquivos de rede. O padrão é **Ativado**.
- **Permite o acesso do usuário à interface de usuário do Windows Defender:** especifica se os usuários podem acessar a interface de usuário do Windows Defender. Essa configuração entrará em vigor da próxima vez em que o dispositivo do usuário for iniciado. Se essa configuração for **Desativado**, os usuários não receberão notificações do Windows Defender. O padrão é **Ativado**.
- **Extensões excluídas:** as extensões a serem excluídas de exames em tempo real ou agendados. Para separar extensões, use o caractere |. Por exemplo, “lib|obj”.
- **Caminhos excluídos:** os caminhos a serem excluídos de exames em tempo real ou agendados. Para separar caminhos, use o caractere |. Por exemplo, “C:\Exemplo|C:\Exemplo1”.
- **Processos excluídos:** os processos a serem excluídos de exames em tempo real ou agendados. Para separar processos, use o caractere |. Por exemplo, “C:\Exemplo.exe|C:\Exemplo1.exe”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Enviar consentimento de amostras:** controla se é ou não necessário enviar à Microsoft arquivos que possam exigir análise adicional para determinar se eles são mal-intencionados. Opções: **Sempre avisar**, **Enviar amostras seguras**, **Nunca enviar**, **Enviar todas as amostras**. O padrão é **Enviar amostras seguras**.

Política de dispositivo de excluir arquivos e pastas

April 15, 2019

Você pode criar uma política no XenMobile para excluir arquivos e pastas específicos dos dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Mobile/CE

- **Arquivos e pastas a serem excluídos:** para cada arquivo ou pasta que você desejar excluir, clique em Adicionar e faça o seguinte:
  - **Caminho:** digite o caminho para o arquivo ou a pasta.
  - **Tipo:** na lista, clique em Arquivo ou Pasta. O padrão é Arquivo.
  - Clique em **Salvar** para salvar o arquivo ou a pasta, ou clique em **Cancelar** para não salvar.

Política de dispositivo Excluir chaves e valores do Registro

April 15, 2019

Você pode criar uma política no XenMobile para excluir chaves e valores específicos do Registro dos dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Mobile/CE

- **Chaves e valores de Registro a serem excluídos:** para cada chave e valor do Registro que você desejar excluir, clique em **Adicionar** e faça o seguinte:
  - **Chave:** digite o caminho da chave do Registro. Esse é um campo obrigatório. O caminho da chave do Registro deve começar com HKEY_CLASSES_ROOT\, HKEY_CURRENT_USER\, HKEY_LOCAL_MACHINE\ ou HKEY_USERS\.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Valor:** digite o nome do valor a ser excluído ou deixe esse campo em branco para excluir a chave do Registro inteira.
- Clique em **Salvar** para salvar a chave e o valor ou clique em **Cancelar** para não salvar.

Política de dispositivo de Atestado de Integridade de Dispositivo

April 15, 2019

No XenMobile, você pode exigir que os dispositivos Windows 10 relatem o estado da 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 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 de Bit Locker
- Depuração de inicialização ativada
- Versão da lista de revisões do Gerenciador de inicialização
- Integridade do código ativada
- Versão da lista de revisões de integridade do código
- Política DEP
- Driver ELAM carregado
- Emitido em
- Depuração de kernel ativada
- PCR
- Redefinir contagem
- Reiniciar contagem
- Modo de segurança ativado
- Hash SBCP
- Inicialização segura ativada
- Sinalização de teste ativada
- VSM ativado
- WinPE ativado

Para obter mais informações, consulte a página HealthAttestation CSP da Microsoft.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar DHA usando o Microsoft Cloud

Adicione uma política de atestado de integridade do dispositivo e defina essa configuração para cada plataforma escolhida:

- **Ativar atestado de integridade de dispositivo:** selecione se pretende exigir o Atestado de Integridade de Dispositivo. O padrão é **Off**.

Para configurar o DHA usando um servidor DHA do Windows no local

Para habilitar o DHA no local, você primeiro 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 de dispositivo no local.
2. Adicione uma política de atestado de integridade do dispositivo e defina estas configurações:
   - **Ativar atestado de integridade do dispositivo: ON**.
   - **Configurar o serviço de atestado de integridade no local: ON**.
   - **FQDN do Serviço DHA no local:** digite o nome de domínio totalmente qualificado do servidor DHA que você configurou.
   - **Versão da API DHA no local:** selecione a versão do serviço DHA instalado no servidor DHA.

Política de dispositivo de nome do dispositivo

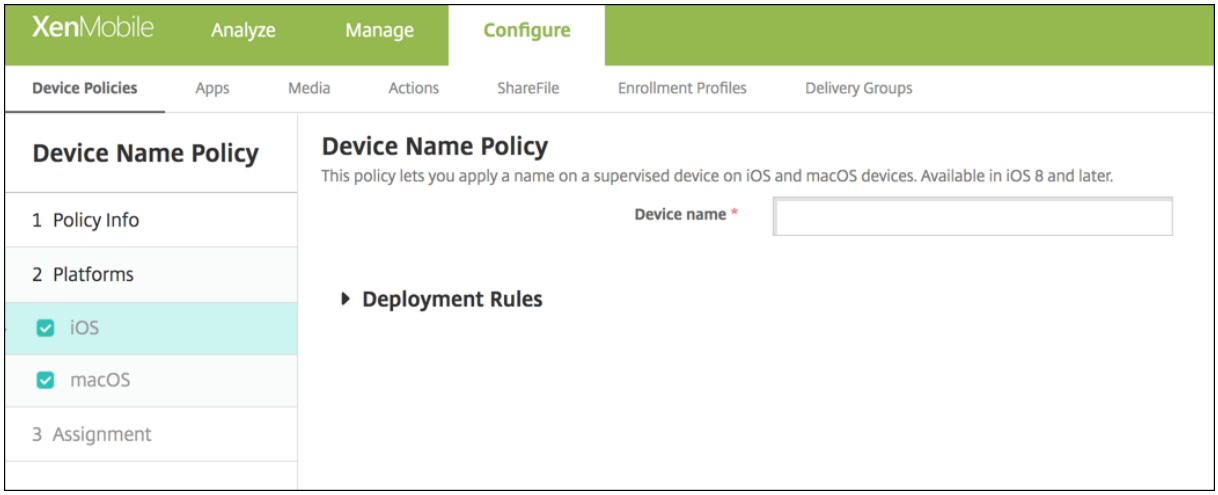
April 15, 2019

Você pode definir os nomes nos dispositivos iOS e macOS supervisionados para que você possa identificá-los facilmente. 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 usaria ${device.serialnumber}. Para definir o nome do dispositivo como uma combinação do nome do usuário e do seu domínio, você usaria ${user.username}@exemplo.com. Para obter informações sobre macros, consulte Macros no XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do iOS e do 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 de dispositivo 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 Configuração de Educação

April 15, 2019

A Política de dispositivo Configuração de Educação define:

- As configurações de aplicativo Sala de Aula da Apple para dispositivos de instrutores.
- Os certificados usados para realizar a autenticação de cliente entre os dispositivos do instrutor e do aluno.

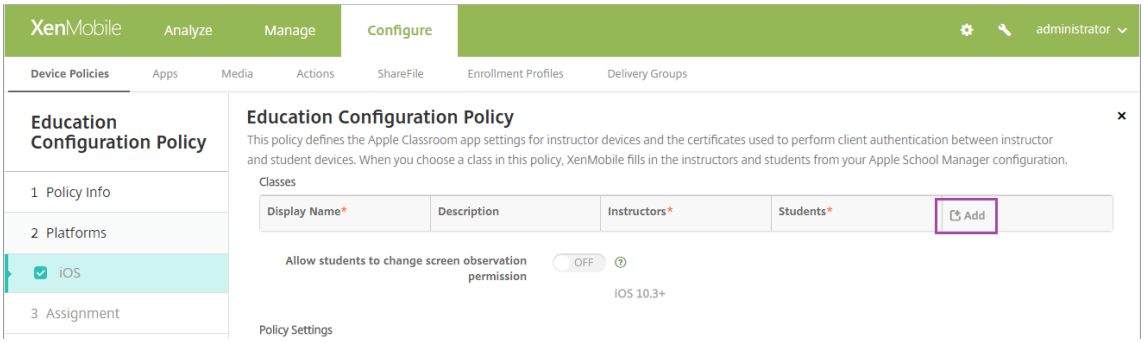
Quando você escolhe uma aula nessa política, o console XenMobile preenche a configuração de instrutores e alunos com a configuração do Apple School Manager. Crie uma política se as configurações do aplicativo Apple Sala de Aula nesta política forem iguais para todas as classes.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

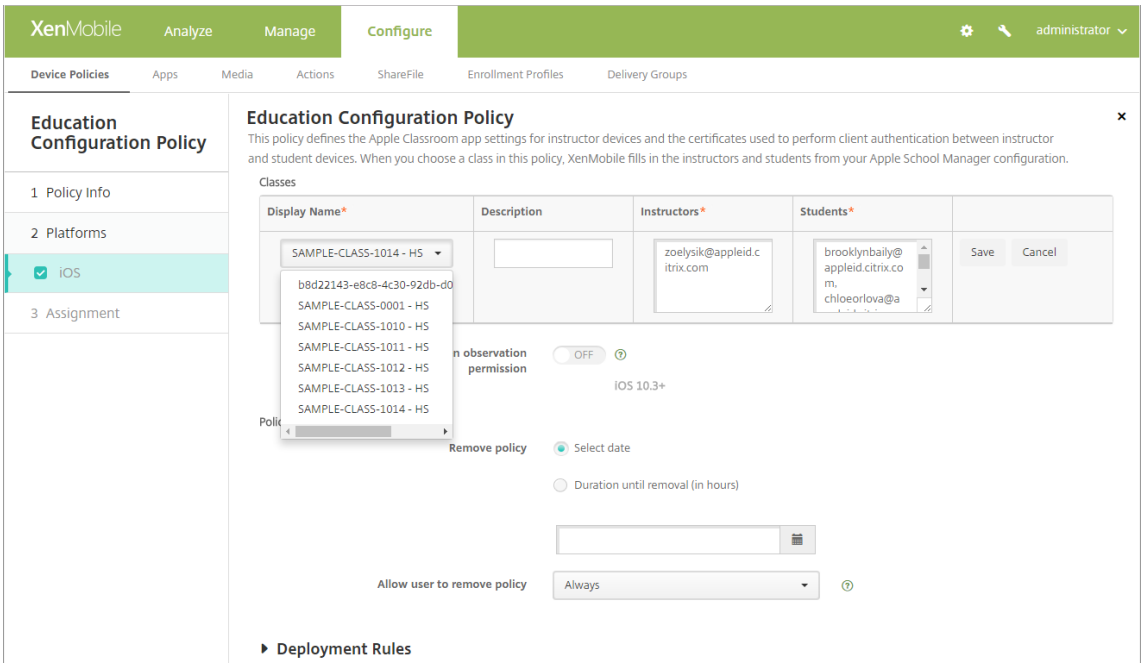
Para configurar a política

1. Depois de adicionar a Política de Configuração de Educação, clique em **Adicionar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

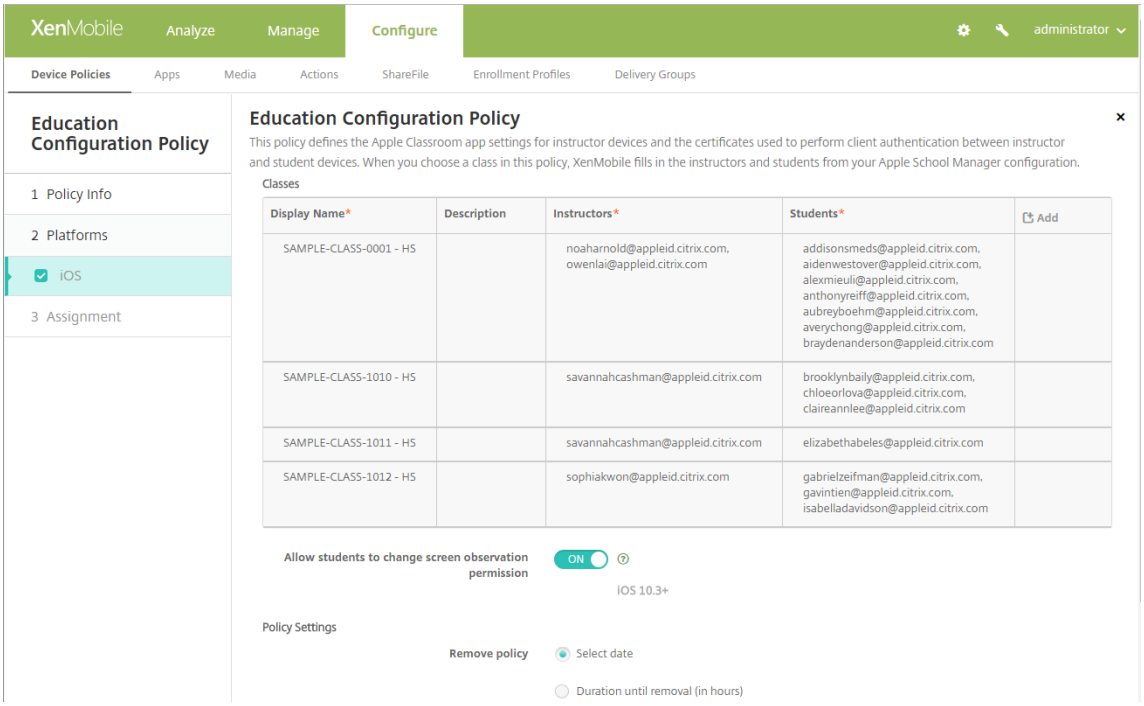


2. Clique na lista **Nome de Exibição**. É exibida uma lista de classes obtidas da sua conta do Apple School Manager conectada.



Quando você escolhe uma classe de **nome de exibição**, o XenMobile preenche as informações de instrutores e alunos. Continue adicionando classes.

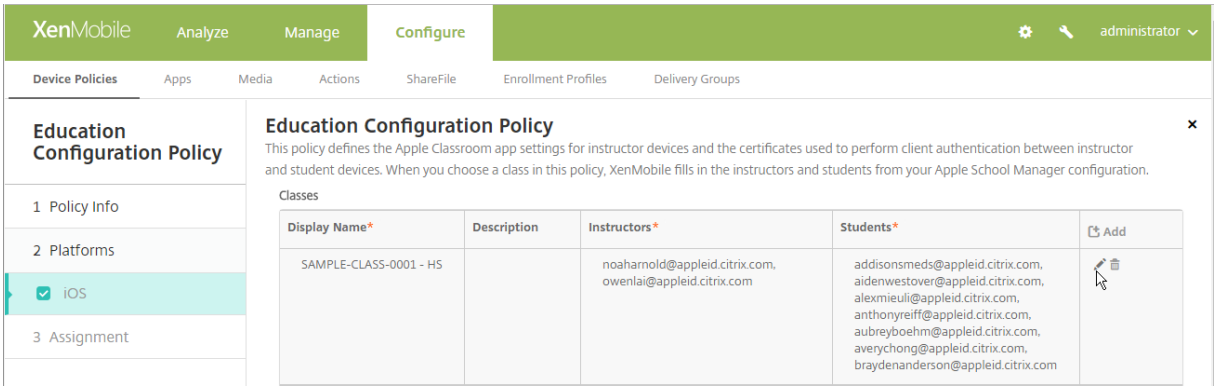
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para editar informações de classes na política

Você pode adicionar uma descrição para uma classe (o “nome de exibição” no aplicativo Sala de Aula). Você também pode adicionar ou remover instrutores e alunos. O XenMobile Server não salva essas alterações na sua conta Apple School Manager. Para obter mais informações, consulte “Gerenciar informações do instrutor, aluno e classe” em Integração com os recursos do Apple Educação.

Passe o mouse sobre a coluna **Adicionar** da classe que deseja editar e, em seguida, clique no ícone de lápis.



Para excluir uma classe da política, passe o mouse sobre a coluna **Adicionar** da classe que deseja excluir e clique no ícone de lixeira.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do Hub Empresarial

April 15, 2019

Uma política de dispositivo do hub empresarial para Windows Phone permite distribuir aplicativos por meio da loja do hub empresarial.

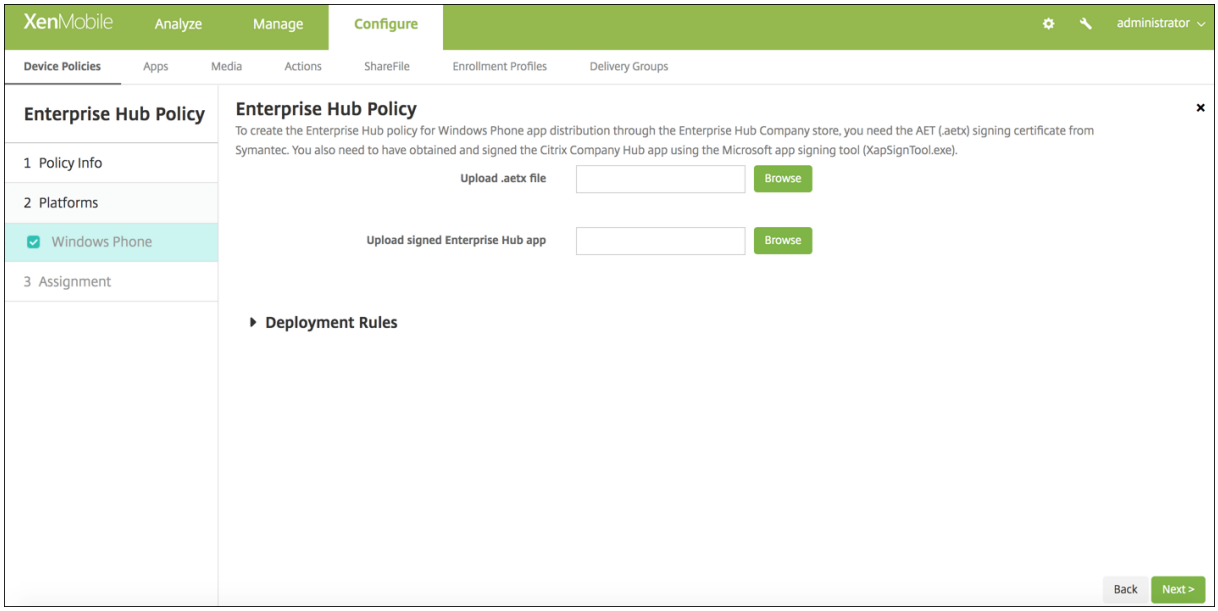
Antes de criar a política, o seguinte é necessário:

- Um certificado de assinatura AET (.aetx) da Symantec
- O aplicativo Citrix Company Hub assinado usando a ferramenta de assinatura de aplicativos da Microsoft (XapSignTool.exe)

> Nota:
>
> O XenMobile é compatível somente com uma política do Hub Empresarial para um modo do Secure Hub para Windows Phone. Por exemplo, para carregar o Secure Hub para Windows Phone para XenMobile Enterprise Edition, você não deve criar várias políticas do Hub Empresarial com versões diferentes do Worx Home para XenMobile Enterprise Edition. Você pode implantar somente a política inicial do Hub Empresarial durante registro do dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Phone



- **Upload de arquivo .aetx:** selecione o arquivo .aetx clicando em **Procurar** e navegando até a localização do arquivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Carregar o aplicativo de hub empresarial:** selecione o aplicativo Hub Enterprise clicando em **Procurar** e navegando até a localização do aplicativo.

Política de dispositivo do Exchange

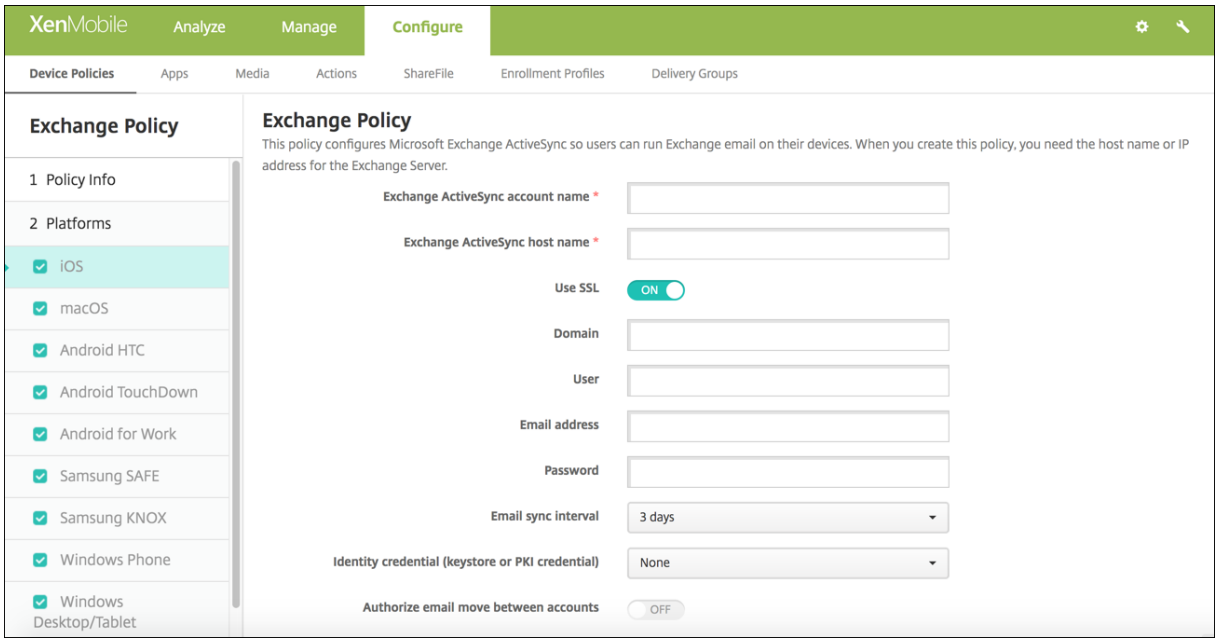
April 15, 2019

Você pode usar a política de dispositivo do Exchange ActiveSync para configurar um cliente de email em dispositivos dos usuários e permitir que eles acessem emails corporativos hospedados no Exchange. Você pode criar políticas para iOS, macOS, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX, Windows Phone e Windows Tablet. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes nas seções a seguir.

Para criar essa política, você precisa do nome do host ou endereço IP do Exchange Server. Para obter informações sobre as configurações do ActiveSync, consulte o artigo da Microsoft ActiveSync CSP.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



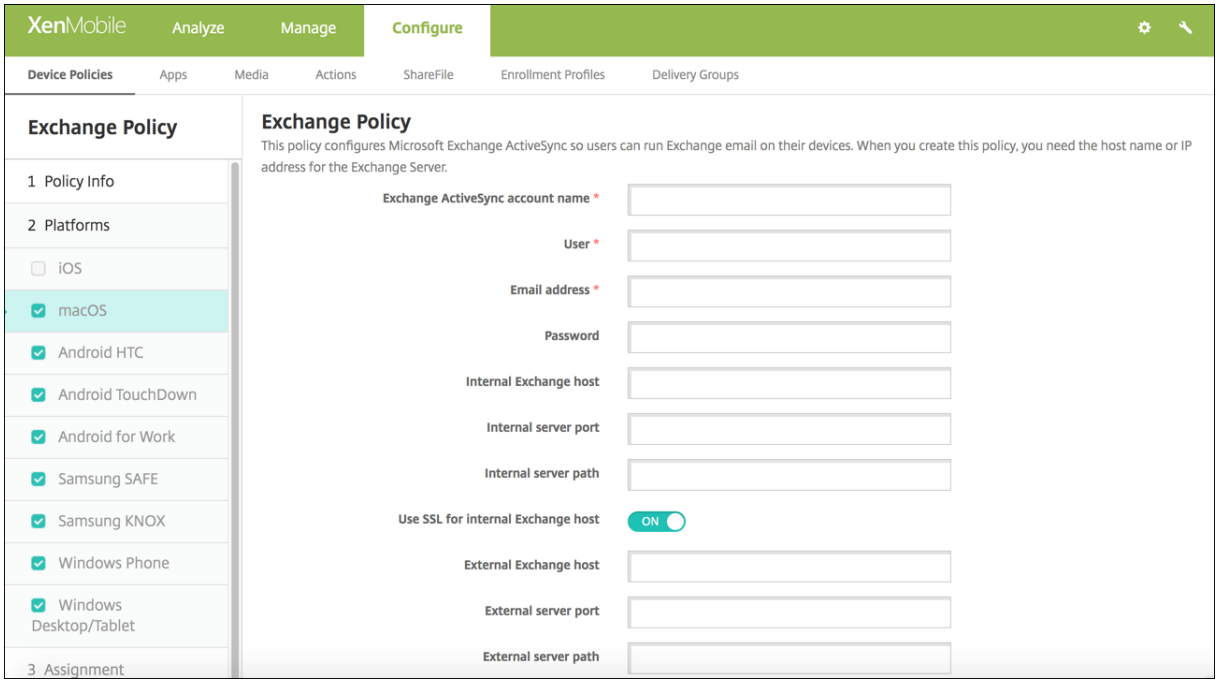
- **Nome de conta do Exchange ActiveSync:** digite a descrição da conta de email exibida nos dispositivos do usuário.
- **Nome do host do Exchange ActiveSync:** digite o endereço do servidor de email.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Usar SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **I**.
- **Domínio:** insira o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **Usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Intervalo de sincronização de emails:** na lista, escolha com que frequência o email é sincronizado com o Exchange Server. O padrão é **3 dias**.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente. O padrão é **Nenhum**.
- **Autorizar a mudança de emails entre contas:** selecione se os usuários têm permissão para mover emails dessa conta para outra conta, além de encaminhar e responder de uma conta diferente. O padrão é **Off**.
- **Enviar email somente do aplicativo de email:** selecione se os usuários têm restrições no aplicativo de correio do iOS para enviar emails. O padrão é **Off**.
- **Desativar a sincronização de emails recentes:** selecione se os usuários devem ser impedidos de sincronizar endereços recentes. O padrão é **Off**. Essa opção se aplica somente ao iOS 6.0 e versões posteriores.
- **Ativar S/MIME:** selecione se essa conta é compatível com a autenticação e a criptografia S/MIME. O padrão é **Off**. Quando definido como **On**, os dois campos abaixo são exibidos.
  - **Credencial de identidade de assinatura**. O padrão é **Nenhum**.
  - **Credencial de identidade de criptografia**. O padrão é **Nenhum**.
- **Ativar comutador de S/MIME por mensagem:** selecione se os usuários têm permissão para criptografar emails enviados a cada mensagem. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do macOS

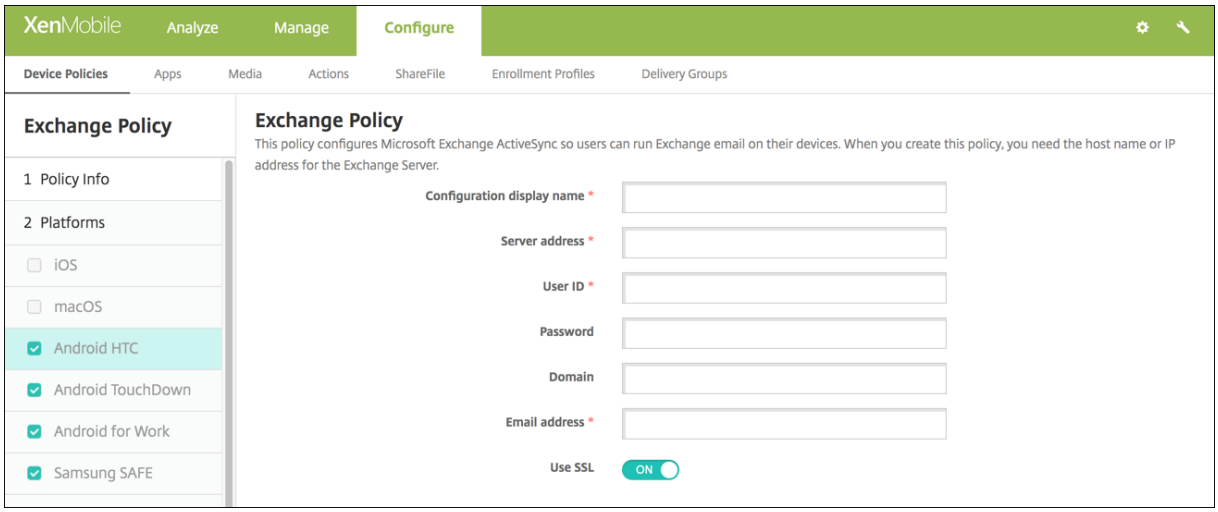


- **Nome de conta do Exchange ActiveSync:** digite a descrição da conta de email exibida nos dispositivos do usuário.
- **Usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Host interno do Exchange:** se desejar que os nomes de host interno e externo do Exchange sejam diferentes, digite um nome de host interno do Exchange opcional.
- **Porta de servidor interno:** se você desejar que as portas de servidor interno e externo do Exchange sejam diferentes, digite um número de porta de servidor interno do Exchange opcional.
- **Caminho de servidor interno:** se você desejar que os caminhos de servidor interno e externo do Exchange sejam diferentes, digite um caminho de servidor interno do Exchange opcional.
- **Usar SSL para host interno do Exchange:** selecione se as conexões entre os dispositivos dos usuários e o host interno do Exchange devem ser protegidas. O padrão é **I**.
- **Host externo do Exchange:** se você desejar 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 desejar que as portas de servidor interno e externo do Exchange sejam diferentes, digite um número de porta opcional do servidor externo do Exchange.
- **Caminho de servidor externo:** se você desejar que os caminhos de servidor interno e externo do Exchange sejam diferentes, digite um caminho de servidor externo do Exchange opcional.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Usar SSL para host externo do Exchange:** selecione se as conexões entre os dispositivos dos usuários e o host interno do Exchange devem ser protegidas. O padrão é **On**.
- **Permitir Mail Drop:** selecione se os usuários têm permissão para compartilhar arquivos sem fio entre dois Macs, sem a necessidade de conexão com uma rede existente. O padrão é **Off**.

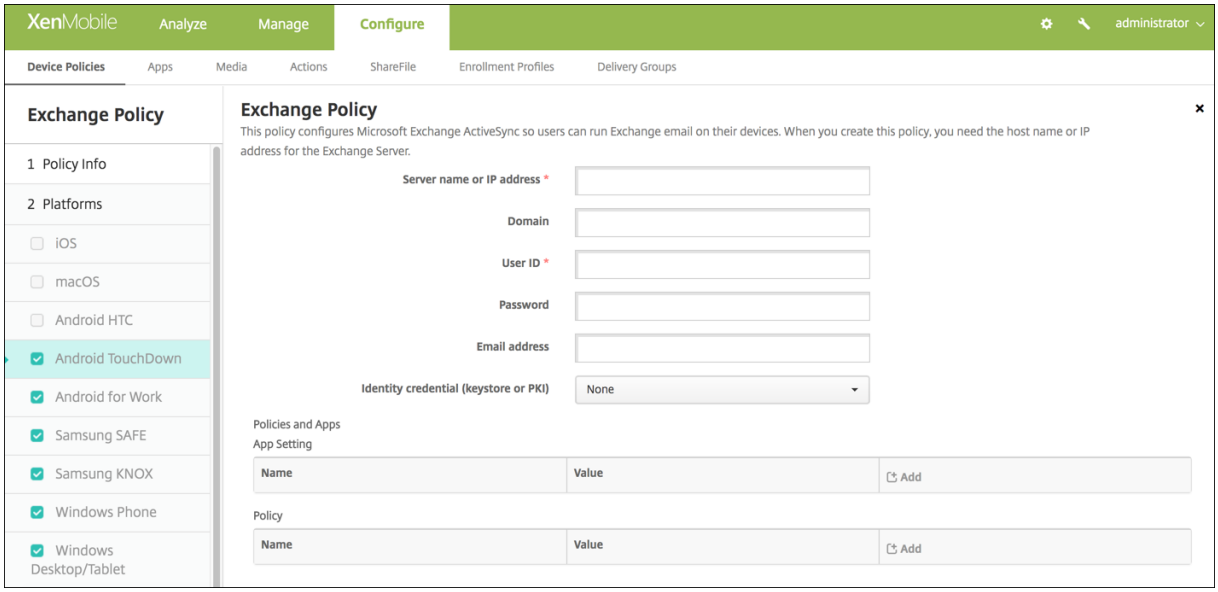
Configurações do Android HTC



- **Nome para exibição da configuração:** digite o nome dessa política que aparece nos dispositivos do usuário.
- **Endereço de servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Domínio:** insira o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Usar SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **I**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

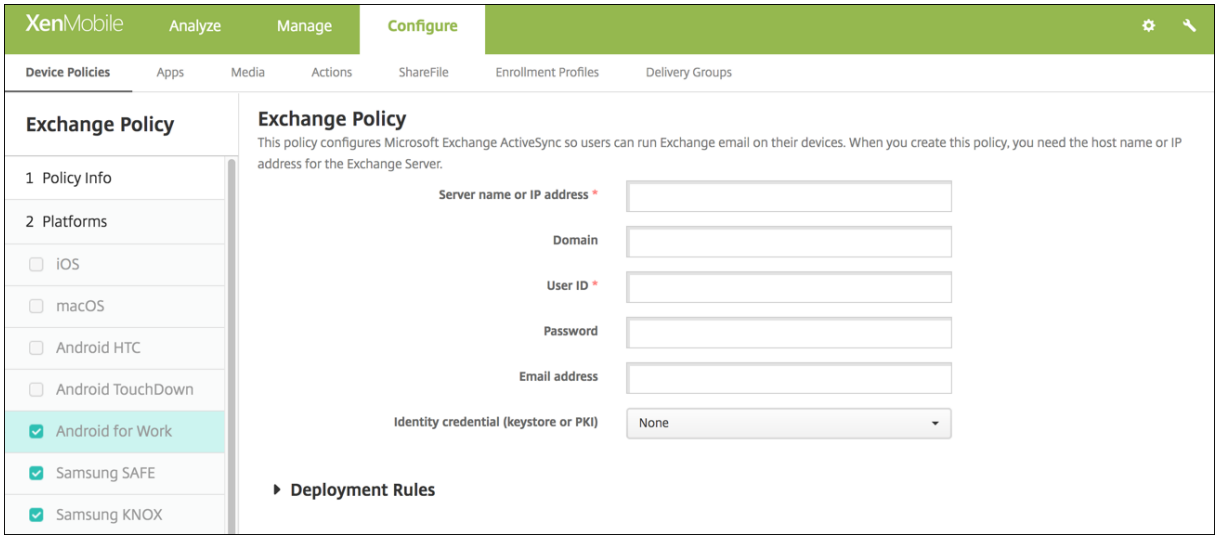
Configurações do Android TouchDown



- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** digite o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente. O padrão é **Nenhum**.
- **Configuração do aplicativo:** opcionalmente, adicione configurações de aplicativo TouchDown para essa política.
- **Política:** opcionalmente, adicione políticas do TouchDown para essa política.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

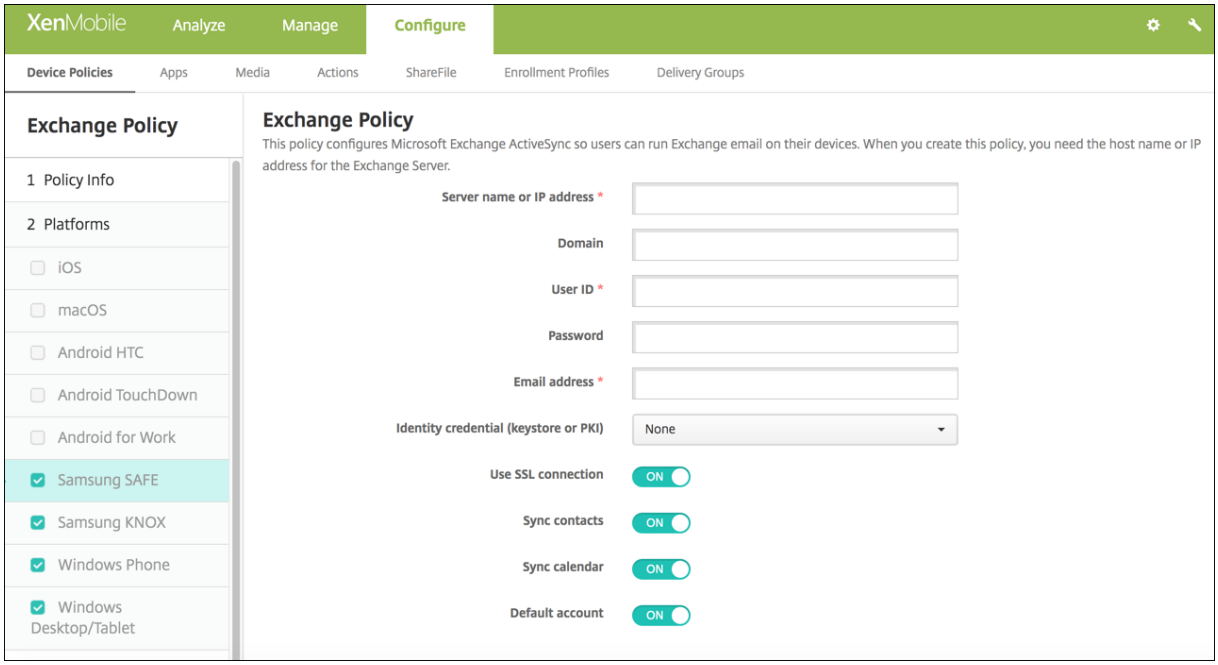
Android for Work



- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** digite o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente. O padrão é **Nenhum**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

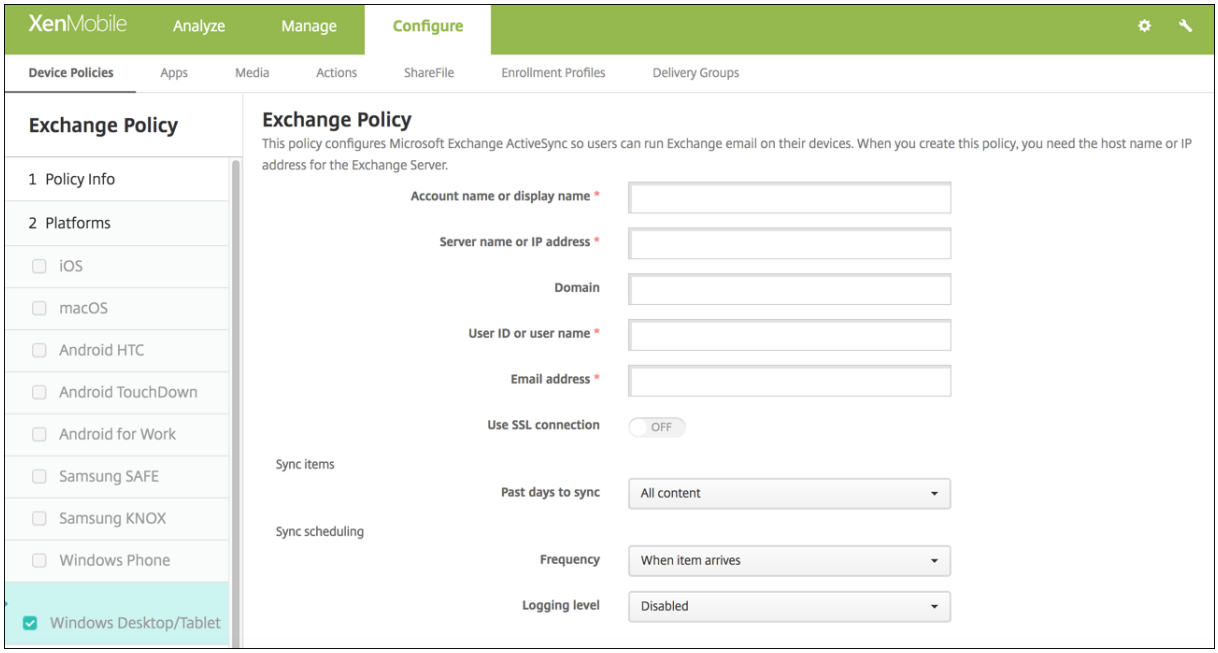
Configurações do Samsung SAFE e do Samsung KNOX



- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** digite o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente.
- **Usar conexão SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **On**.
- **Sincronizar os contatos:** selecione se a sincronização dos contatos dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **On**.
- **Sincronizar o calendário:** selecione se a sincronização do calendário dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **On**.
- **Conta padrão:** selecione se as contas do Exchange dos usuários devem ser o padrão para envio de email dos respectivos dispositivos. O padrão é **On**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Phone e do Windows Desktop/Tablet



> Nota:
>
> Essa política não permite que você defina a senha do usuário. Os usuários devem definir esse parâmetro nos dispositivos deles depois que você enviar a política por push.

- **Nome da conta ou nome de exibição:** digite o nome de conta do Exchange ActiveSync.
- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** insira o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema $user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID de usuário ou nome de usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema $user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Usar conexão SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **Off**.
- **Últimos dias para sincronizar:** na lista, clique em quantos dias no passado todo o conteúdo do dispositivo deve ser sincronizado com o Exchange Server. O padrão é **Todo o conteúdo**.
- **Frequência:** na lista, clique na agenda a ser usada durante a sincronização dos dados que são enviados para o dispositivo do Exchange Server. O padrão é **Quando chega**.
- **Nível de log:** na lista, clique em **Desativado**, **Básico** ou **Avançado** para especificar o nível de detalhes do registro em log da atividade do Exchange. O **padrão é Desativado**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de arquivo

April 15, 2019

Você pode adicionar arquivos de script ao XenMobile para realizar determinadas funções para os usuários, ou pode adicionar arquivos de documento que você deseja que os usuários de dispositivos Android consigam acessar nos dispositivos deles. Quando você adiciona o arquivo, pode também especificar o diretório no qual deseja que o arquivo seja armazenado no dispositivo. Por exemplo, se você desejar que os usuários Android recebam um arquivo de documento ou .pdf da empresa, poderá implantar o arquivo no dispositivo e avisar aos usuários onde o arquivo está localizado.

Você pode adicionar os seguintes tipos de arquivo com essa política:

- Arquivos baseados em texto (.xml, .html, .py e assim por diante)
- Outros arquivos, como documentos, fotos, planilhas ou apresentações
- Para Windows Mobile e Windows CE somente: Arquivos de script criados com MortScript

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android

- **Arquivo a ser importado:** selecione o arquivo a ser importado clicando em Procurar e navegando até a localização do arquivo.
- **Tipo de arquivo:** selecione **Arquivo** ou **Script**. Quando você seleciona **Script**, **Executar imediatamente** é exibido. Selecione se o script deve ser executado quando o arquivo é carregado. O padrão é **Off**.
- **Substituir expressões de macro:** selecione se você deseja substituir nomes de token de macro em um script com uma propriedade de dispositivo ou usuário. O padrão é **Off**.
- **Pasta de destino:** na lista, selecione a localização na qual o arquivo enviado deve ser armazenado ou clique em **Adicionar nova** para escolher uma localização de arquivo não listada. Além disso, você pode usar a macro %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 for alterado antes de ser implantado em um dispositivo.
- **Copiar arquivo somente se for diferente:** na lista, selecione se o arquivo deverá ser copiado se for diferente do arquivo existente. O padrão é copiar o arquivo somente se ele for diferente.

Configurações do Windows Mobile/CE

- **Arquivo a ser importado:** selecione o arquivo a ser importado clicando em Procurar e navegando até a localização do arquivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Tipo de arquivo:** selecione **Arquivo** ou **Script**. Quando você seleciona **Script**, **Executar imediatamente** é exibido. Selecione se o script deve ser executado quando o arquivo é carregado. O padrão é **Off**.
- **Substituir expressões de macro:** selecione se você deseja substituir nomes de token de macro em um script com uma propriedade de dispositivo ou usuário. O padrão é **Off**.
- **Pasta de destino:** na lista, selecione a localização na qual o arquivo enviado deve ser armazenado ou clique em **Adicionar nova** para escolher uma localização de arquivo não listada. Além disso, você pode usar qualquer uma das macros abaixo como o início de um identificador de caminho:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Nome do arquivo de destino:** opcionalmente, digite um nome diferente para o arquivo se ele for alterado antes de ser implantado em um dispositivo.
- **Copiar arquivo somente se for diferente:** na lista, selecione se o arquivo deverá ser copiado se for diferente do arquivo existente. O padrão é copiar o arquivo somente se ele for diferente.
- **Arquivo somente leitura:** selecione se o arquivo deve ser somente leitura. O padrão é **Off**.
- **Arquivo oculto:** selecione se o arquivo não deve ser mostrado na lista de arquivos. O padrão é **Off**.

Política de dispositivo FileVault

August 31, 2018

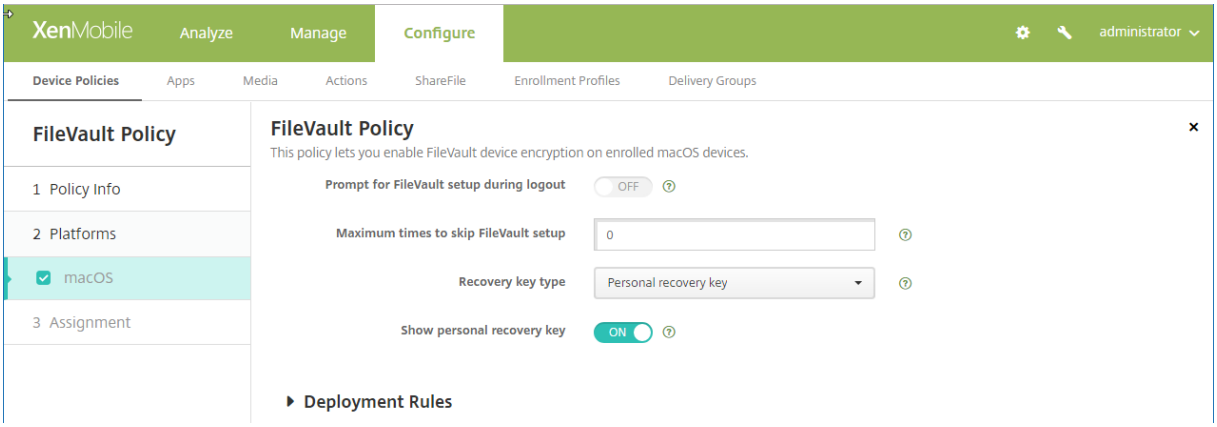
O recurso de Criptografia de disco do FileVault do macOS protege o volume do sistema, criptografando seu conteúdo. Com o FileVault ativado em um dispositivo macOS, um usuário efetua login com a senha da conta sempre que o dispositivo é iniciado. Se o usuário perde a sua senha, uma chave de recuperação permite desbloquear o disco e redefinir sua senha.

A política do dispositivo XenMobile, FileVault, habilita as telas de configuração do usuário do FileVault e define as configurações, como as 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, acesse **Configurar > Políticas de dispositivo**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do macOS



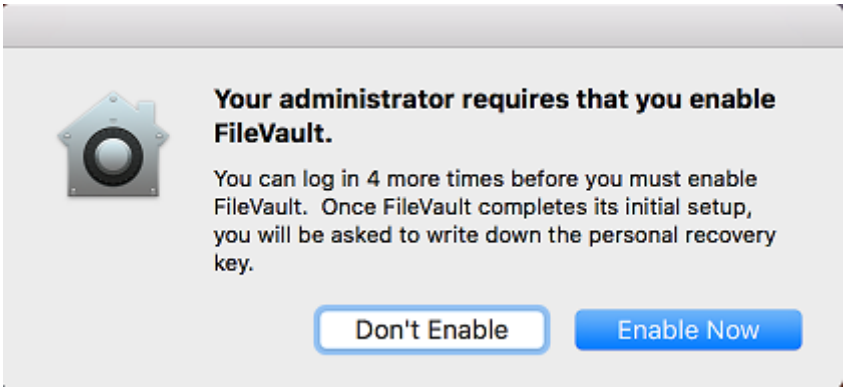
- **Solicitar a configuração do FileVault durante o logout:** se estiver **I**, solicita que o usuário ative o FileVault durante os próximos N logouts, conforme especificado pela opção **Número máximo de vezes para ignorar a configuração do FileVault**. Se o valor for **O**, o aviso de senha do FileVault não aparecerá.

Depois de implantar a política FileVault com essa configuração ativada, a seguinte tela aparece quando um usuário faz o logoff do dispositivo. A tela dá ao usuário a opção de ativar o FileVault antes de logoff.

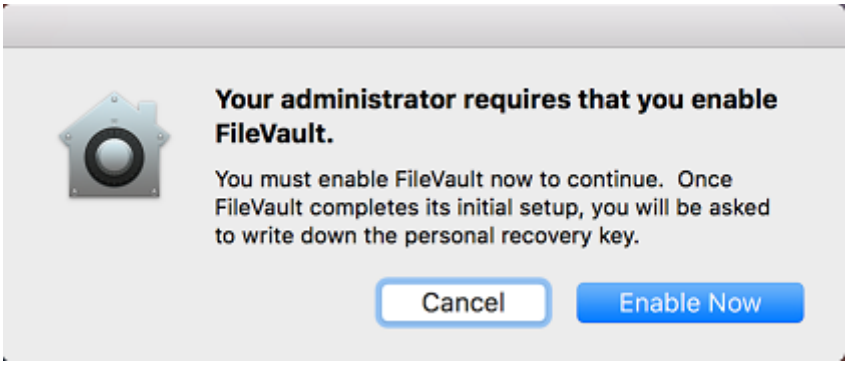


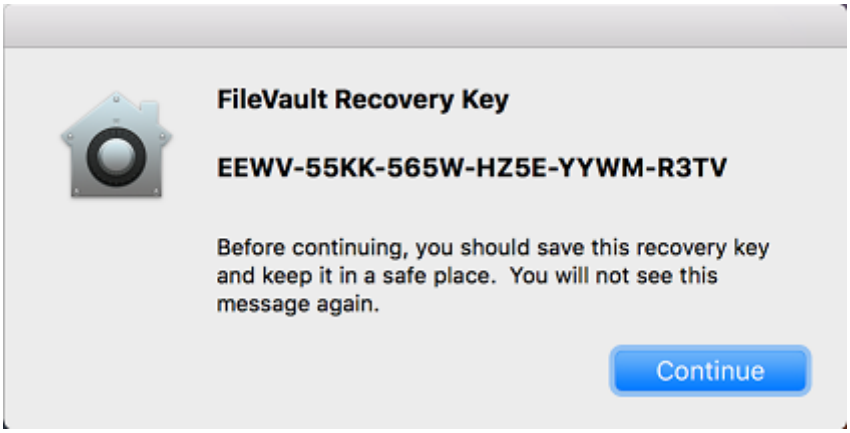
Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** não for 0: depois que você implantar a política do FileVault com essa configuração desativada e, quando o usuário fizer logon, a tela a seguir será exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** for 0 ou o usuário tiver ignorado a configuração do número máximo de vezes, a tela a seguir será exibida.





Política de dispositivo de fonte

April 15, 2019

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar mais fontes aos dispositivos iOS e macOS. As fontes devem ser TrueType (.ttf) ou OpenType (.oft). Coleções de fontes (.ttc ou .otc) não são compatíveis.

Para o iOS, essa política se aplica somente ao iOS 7.0 e versões posteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Nome visível para o usuário:** digite o nome que os usuários veem nas respectivas listas de fonte.
- **Arquivo de fonte:** selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e navegando até a localização do arquivo.

Configurações do macOS

- **Nome visível para o usuário:** digite o nome que os usuários veem nas respectivas listas de fonte.
- **Arquivo de fonte:** selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e navegando até a localização do arquivo.

Política de dispositivo de layout de tela inicial

April 15, 2019

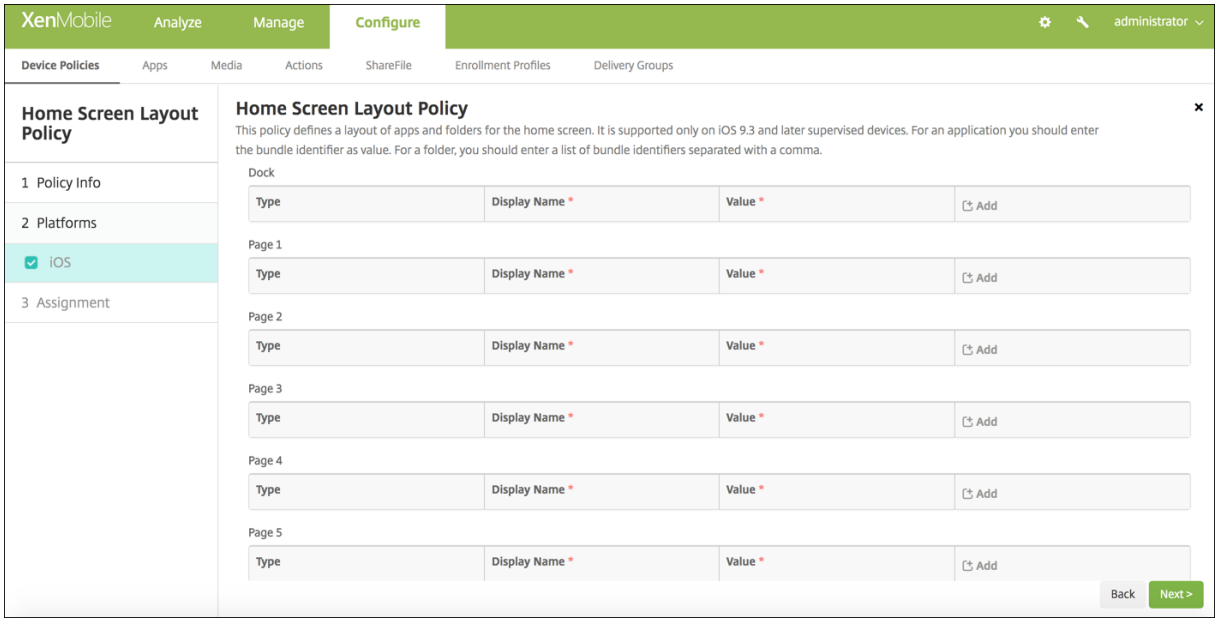
Você pode especificar o layout de aplicativos e pastas para a tela inicial do iOS. A política de dispositivo de layout da tela inicial é para dispositivos supervisionados iOS 9.3 e versões posteriores.

> Importante:
>
> Implantar várias políticas de layout da tela inicial em um dispositivo resulta em um erro do iOS no dispositivo. Essa limitação é aplicável independentemente de você definir a tela inicial usando essa política do XenMobile ou usando o Apple Configurator.

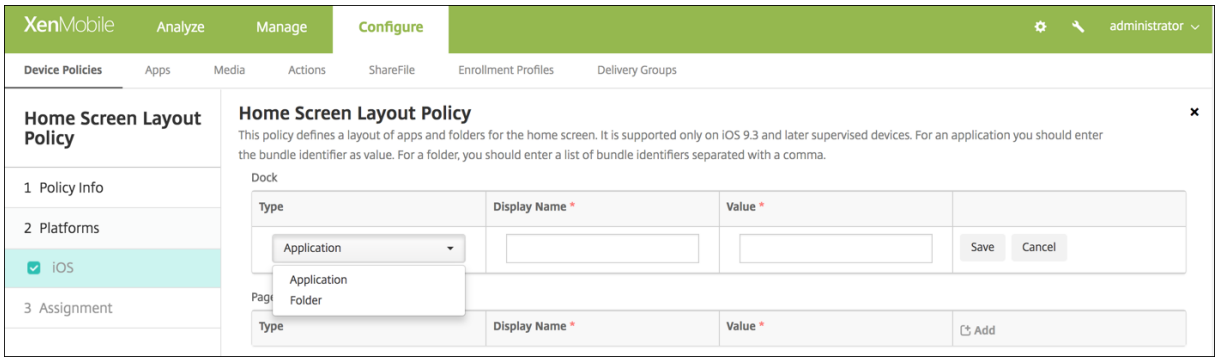
Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



- Para cada uma das áreas da tela que você deseja configurar (como **Dock** ou **Página 1**), clique em **Adicionar**.
- **Tipo:** escolha **Aplicativo** ou **Pasta**.



- **Nome para exibição:** o nome que aparece na tela inicial do aplicativo ou pasta.
- **Valor:** para aplicativos, o identificador do pacote. Para pastas, uma lista de identificadores de pacote separados por vírgulas.

Política de dispositivo de importação do perfil de iOS e macOS

April 15, 2019

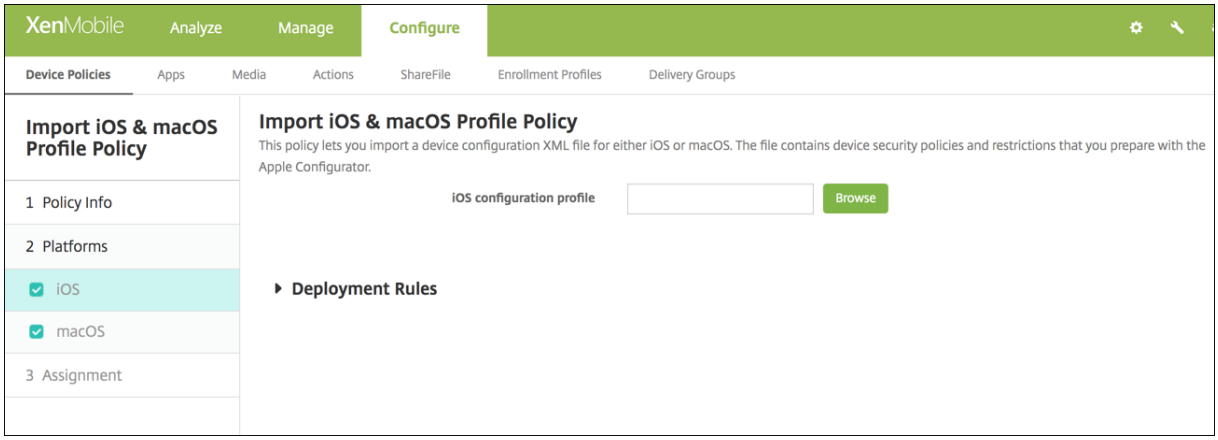
Você pode importar arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém as políticas de segurança do dispositivo e as restrições que você prepara com o Apple Configurator.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Você pode colocar um dispositivo iOS no modo supervisionado no Apple Configurator, como descrito posteriormente neste artigo. Para obter mais informações sobre como usar o Apple Configurator para criar um arquivo de configuração, consulte a página Configurator Support da Apple.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS e do MacOS



- **Perfil de configuração do iOS** ou **Perfil de configuração do macOS:** para selecionar o arquivo de configuração para importar, clique em em **Procurar** e navegue até a localização do arquivo.

Colocar um dispositivo iOS no modo Supervisionado com o Apple Configurator

Para usar o Apple Configurator, você precisa de um computador Apple que execute o macOS 10.7.2 ou versões posteriores.

> Importante:
>
> Colocar um dispositivo no modo supervisionado instala a versão selecionada do iOS no dispositivo, apagando completamente os dados ou os aplicativos do usuário armazenados anteriormente.

1. Instale o Apple Configurator pelo iTunes.
2. Conecte o dispositivo iOS ao seu computador Apple.
3. Inicie o Apple Configurator. O Configurator mostra que você tem um dispositivo a ser preparado para supervisão.
4. Para preparar o dispositivo para supervisão:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a) Mude o controle de **Supervision** para **On**. A Citrix recomenda que você escolha essa configuração se pretender manter o controle contínuo do dispositivo reaplicando uma configuração regularmente.

b) Opcionalmente, forneça um nome para o dispositivo.

c) No iOS, clique em **Latest** para obter a versão mais recente do iOS que você deseja instalar.

5. Quando você estiver pronto para preparar o dispositivo para supervisão, clique em **Prepare**.

Política de dispositivo do quiosque para Samsung SAFE

April 15, 2019

Crie uma política de Quiosque no XenMobile para permitir especificar que somente um ou mais aplicativos específicos podem ser usados em dispositivos Samsung SAFE. Essa política é útil para dispositivos corporativos que foram projetados para executar somente um tipo ou classe específico de aplicativos. A política também permite que você escolha imagens personalizadas para a tela inicial do dispositivo e papéis de parede da tela de bloqueio para quando o dispositivo estiver no Modo de quiosque.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Para colocar um dispositivo Samsung SAFE no modo de quiosque

1. Ative a chave de API do Samsung SAFE no dispositivo móvel, conforme descrito em Políticas de dispositivo de chave de licença MDM Samsung. Esta etapa permite que você habilitar as políticas em dispositivos Samsung SAFE.
2. Habilite a Política de agendamento de conexão para dispositivos Android, conforme descrito em Políticas de dispositivo de agendamento de conexão. Esta etapa permite que dispositivos Android se conectem ao XenMobile.
3. Adicione uma política de dispositivo do Quiosque, conforme descrito na próxima seção.
4. Atribua essas três políticas de dispositivo aos grupos de entrega apropriados. Considere se você deseja incluir outras políticas, como de inventário de aplicativos, nesses grupos de entrega.

   Para remover os dispositivos móveis do modo de Quiosque, crie uma política de dispositivo que tenha o **Modo de quiosque** definido como **Desativar**. Atualize os grupos de entrega para remover a política de quiosque que ativou o modo de quiosque e para adicionar a política de quiosque que desativa o modo de quiosque.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar uma política de dispositivo

Todos os aplicativos que você especificar para o Modo de quiosque já deverão estar instalados nos dispositivos do usuário.

Algumas opções se aplicam somente à API do Samsung Mobile Device Management (MDM) 4.0 e posterior.

Configurações do Samsung SAFE

- **Modo de quiosque:** clique em **Ativar** ou **Desativar**. O padrão é **Ativar**. Quando você clica em **Desativar**, todas as opções a seguir desaparecem.
- **Pacote de inicializador:** a Citrix recomenda deixar esse campo em branco, a menos que você tenha desenvolvido um inicializador interno para permitir que os usuários abram os aplicativos de Quiosque. Se você usar um inicializador interno, digite o nome completo do pacote de aplicativos do inicializador.
- **Número de telefone de emergência:** digite um número de telefone opcional. Qualquer um pode usar esse método para contatar sua empresa para localizar um dispositivo perdido. Aplica-se somente ao MDM 4.0 e versões posteriores.
- **Permitir barra de navegação:** selecione se deseja permitir que os usuários visualizem e usem a barra de navegação no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir modo de várias janelas:** selecione se deseja permitir que os usuários usem várias janelas enquanto estão no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir barra de status:** selecione se deseja permitir que os usuários visualizem a barra de status no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir barra de sistema:** selecione se deseja permitir que os usuários visualizem a barra de sistema no Modo de quiosque. O padrão é **On**.
- **Permitir gerenciador de tarefas:** selecione se deseja permitir que os usuários visualizem e usem o gerenciador de tarefas no Modo de quiosque. O padrão é **On**.
- **Alterar código secreto SAFE comum:** essa configuração ajuda a proteger contra alterações inadvertidas no campo Código secreto SAFE comum. Quando essa configuração é **Off**, não é possível alterar o campo Código secreto SAFE comum. O padrão é **Off**.
- **Código secreto SAFE comum:** se você definir uma política de código secreto geral para todos os dispositivos Samsung SAFE, digite este código secreto opcional neste campo.
- **Papéis de parede**
  - **Definir um papel de parede para a página inicial:** selecione se deseja usar uma imagem personalizada para a tela inicial no Modo de quiosque. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Imagem da página inicial:** ao ativar a opção **Definir um papel de parede para a página inicial**, selecione o arquivo de imagem clicando em **Procurar** e navegando até a localização do arquivo.
    - **Definir um papel de parede de bloqueio:** selecione se deseja usar uma imagem personalizada para a tela de bloqueio no Modo de quiosque. O padrão é **Off**. Aplica-se somente ao MDM 4.0 e versões posteriores.
        * **Imagem de bloqueio:** ao ativar a opção **Definir um papel de parede de bloqueio**, selecione o arquivo de imagem clicando em **Procurar** e navegando até a localização do arquivo.
- **Aplicativos:** para cada propriedade de usuário que você desejar adicionar ao Modo de quiosque, clique em **Adicionar** e faça o seguinte:
    - **Novo aplicativo a ser adicionado:** digite o nome completo do aplicativo a ser adicionado. Por exemplo, com.android.calendar permite aos usuários usar o aplicativo de calendário do Android.
    - Clique em **Salvar** para adicionar o aplicativo ou em **Cancelar** para cancelar a adição do aplicativo.

Política de dispositivos de configuração de Launcher para Android

April 15, 2019

O Citrix Launcher permite que você personalize a experiência do usuário para dispositivos Android implantados pelo XenMobile. O Citrix Launcher e a política do dispositivo de configuração do Launcher não são compatíveis com o Android Enterprise.

Você pode adicionar uma política de Configuração para controlar estes recursos do Citrix Launcher:

- Gerenciar dispositivos Android para que os usuários possam acessar somente os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizado para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizado para o Citrix Launcher.
- Especifique uma senha que os usuários devem digitar para sair do Launcher.

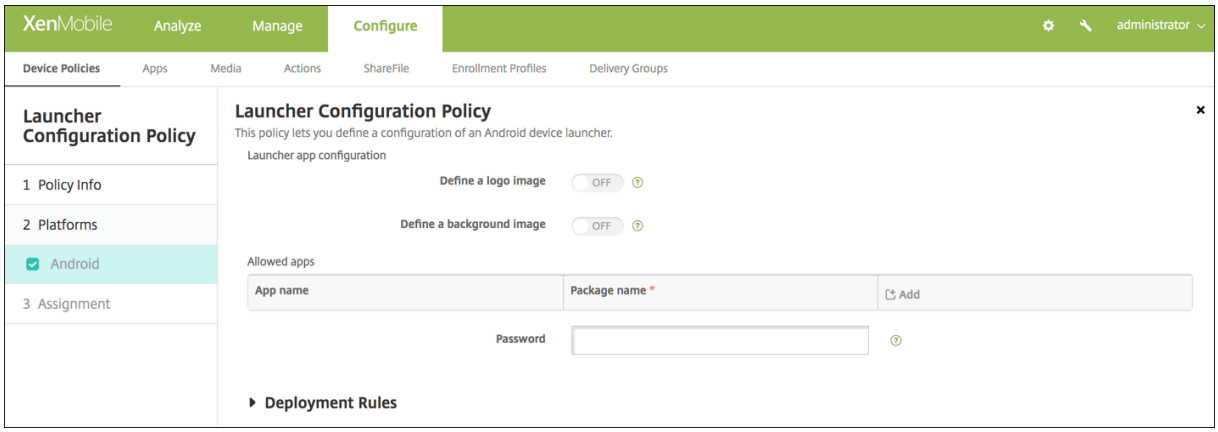
Apesar do Citrix Launcher permitir aplicar essas restrições no nível de dispositivo, o iniciador concede aos usuários a flexibilidade operacional de que necessitam por meio do acesso incorporado às configurações de dispositivos como configurações de WiFi, Bluetooth e de código secreto de dispositivo. O Citrix Launcher não foi criado com a intenção de ser uma camada extra de segurança além da que a plataforma de dispositivo já fornece.

Depois de ter implantado o Citrix Launcher, o XenMobile o instala, substituindo o iniciador padrão do Android.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Android



- **Definir uma imagem de logotipo:** selecione se deve ser usada uma imagem de logotipo personalizada para o ícone do Citrix Launcher. O padrão é **Off**.
- **Imagem de logotipo:** ao ativar a opção **Definir uma imagem de logotipo**, selecione o arquivo de imagem clicando em **Procurar** e navegar para a localização do arquivo. Tipos de arquivo suportados são PNG, JPG, GIF, JPEG e GIF.
- **Definir uma imagem de fundo:** selecione se deve ser usada uma imagem personalizada para o fundo do Citrix Launcher. O padrão é **Off**.
- **Imagem de fundo:** ao ativar a opção **Definir uma imagem de fundo**, selecione o arquivo de imagem clicando em **Procurar** e navegando para a localização do arquivo. Tipos de arquivo suportados são PNG, JPG, GIF, 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 ser adicionado:** digite 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 em **Cancelar** para cancelar a adição do aplicativo.
- **Senha:** a senha que um usuário deve digitar para sair do Citrix Launcher.

Política de dispositivo do LDAP

April 15, 2019

Crie uma política de LDAP para os dispositivos iOS no XenMobile para fornecer informações sobre um servidor LDAP a ser usado, incluindo qualquer informação de conta necessária. A política também

© 1999-2019 Citrix Systems, Inc. All rights reserved.

fornece um conjunto de políticas de pesquisa de LDAP a serem usadas ao consultar o servidor LDAP.

Você precisa do nome do host LDAP antes de configurar essa política.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de 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 esse campo somente com perfis criptografados.
- **Nome do host LDAP:** insira o nome de host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** selecione se uma conexão SSL com o servidor LDAP deve ser usada. O padrão é **On**.
- **Configurações de Pesquisa:** adicione configurações de pesquisa a serem usadas ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa desejar, mas deve adicionar pelo menos uma configuração para tornar a conta útil. Clique em **Adicionar** e faça o seguinte:
  - **Descrição:** digite uma descrição da configuração da pesquisa. Este campo é obrigatório.
  - **Escopo:** escolha **Base**, **Um nível** ou **Subárvore** para definir o quão profunda a pesquisa na árvore LDAP deve ser. O padrão é **Base**.
    - **Base** pesquisa o nó para o qual a base de pesquisa aponta.
    - **Um nível** pesquisa o nó Base e um nível abaixo dele.
    - **Subárvore** pesquisa o nó Base, além de todos os seus filhos, independentemente da profundidade.
  - **Base de pesquisa:** digite o caminho para o nó no qual a pesquisa deve ser iniciada. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.
  - Clique em **Salvar** para adicionar a configuração de pesquisa ou em **Cancelar** para cancelar a inclusão dessa configuração.
  - Repita essas etapas para cada configuração de pesquisa que você deseja adicionar.

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 esse campo somente com perfis criptografados.
- **Nome do host LDAP:** insira o nome de host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** selecione se uma conexão SSL com o servidor LDAP deve ser usada. O padrão é **On**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Configurações de Pesquisa:** adicione configurações de pesquisa a serem usadas ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa desejar, mas deve adicionar pelo menos uma configuração para tornar a conta útil. Clique em **Adicionar** e faça o seguinte:
  - **Descrição:** digite uma descrição da configuração da pesquisa. Este campo é obrigatório.
  - **Escopo:** escolha **Base**, **Um nível** ou **Subárvore** para definir o quão profunda a pesquisa na árvore LDAP deve ser. O padrão é **Base**.
    * **Base** pesquisa o nó para o qual a base de pesquisa aponta.
    * **Um nível** pesquisa o nó Base e um nível abaixo dele.
    * **Subárvore** pesquisa o nó Base, além de todos os seus filhos, independentemente da profundidade.
  - **Base de pesquisa:** digite o caminho para o nó no qual a pesquisa deve ser iniciada. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.
  - Clique em **Salvar** para adicionar a configuração de pesquisa ou em **Cancelar** para cancelar a inclusão dessa configuração.
  - Repita essas etapas para cada configuração de pesquisa que você desejar adicionar.

Política de dispositivo de localização

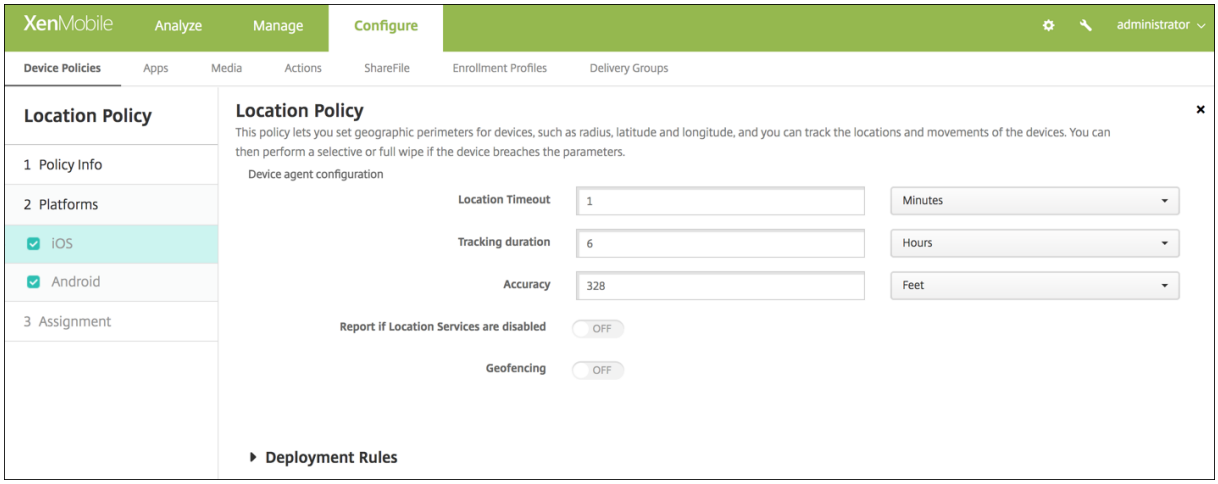
April 15, 2019

Crie políticas de dispositivo de localização no XenMobile para impor fronteiras geográficas. Quando os usuários violam o limite definido, também chamado de *geocerca*, o XenMobile pode realizar certas ações. Por exemplo, você pode configurar a política para emitir uma mensagem de aviso para os usuários quando eles ultrapassam o perímetro definido. Você também pode configurar a política para limpar os dados corporativos dos usuários quando eles ultrapassarem um perímetro, seja imediatamente ou após determinado tempo. Para obter informações sobre as ações de segurança, como a ativação de rastreamento e localização de um dispositivo, consulte Ações de segurança.

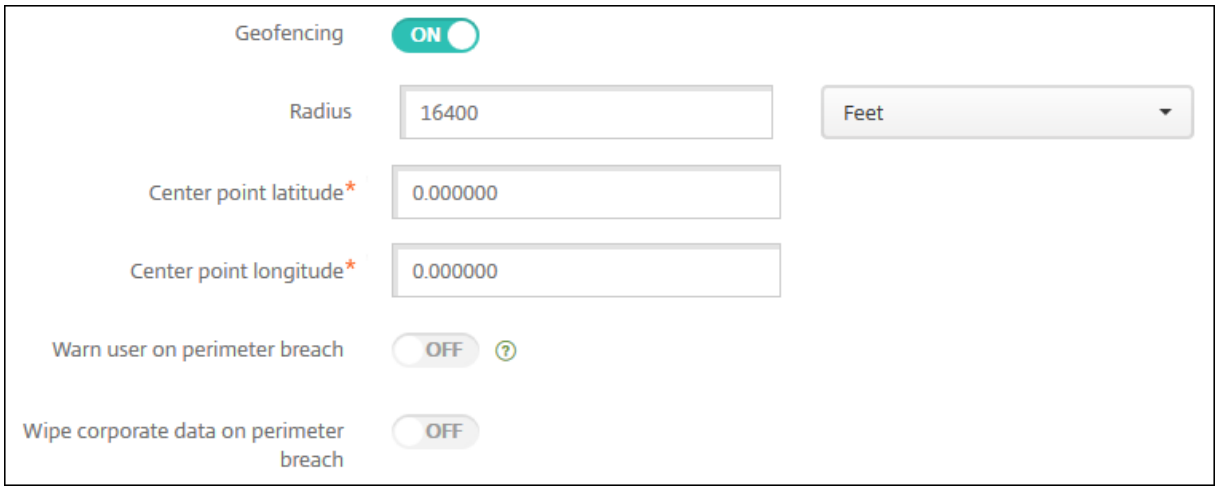
Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



- **Tempo limite de localização:** digite um numeral e, na lista, clique em **Segundos** ou **Minutos** para definir a frequência com a qual o XenMobile tenta corrigir a localização do dispositivo. Os valores válidos são de 60 a 900 segundos ou de 1 a 15 minutos. O padrão é 1 minuto.
- **Duração de rastreamento:** digite um numeral e, na lista, clique em **Horas** ou **Minutos** para definir por quanto tempo o XenMobile rastreia o dispositivo. Os valores válidos são de 1 a 6 horas ou de 10 a 360 minutos. O padrão é 6 horas.
- **Precisão:** digite um numeral e, na lista, clique em **Metros**, **Pés** ou **Jardas** para definir a proximidade a um dispositivo que o XenMobile usa para rastreá-lo. Os valores válidos são de 10 a 5000 jardas ou metros ou de 30 a 15000 pés. O padrão é 328 pés.
- **Informar se os serviços de localização estiverem desativados:** selecione se o dispositivo envia um relatório para o XenMobile quando o GPS está desativado. O padrão é **Off**.
- **Cerca geográfica**



Quando você ativar a Geocerca, defina estas configurações:

- **Raio:** digite um numeral e, na lista, clique nas unidades a serem usadas para medir o raio. O

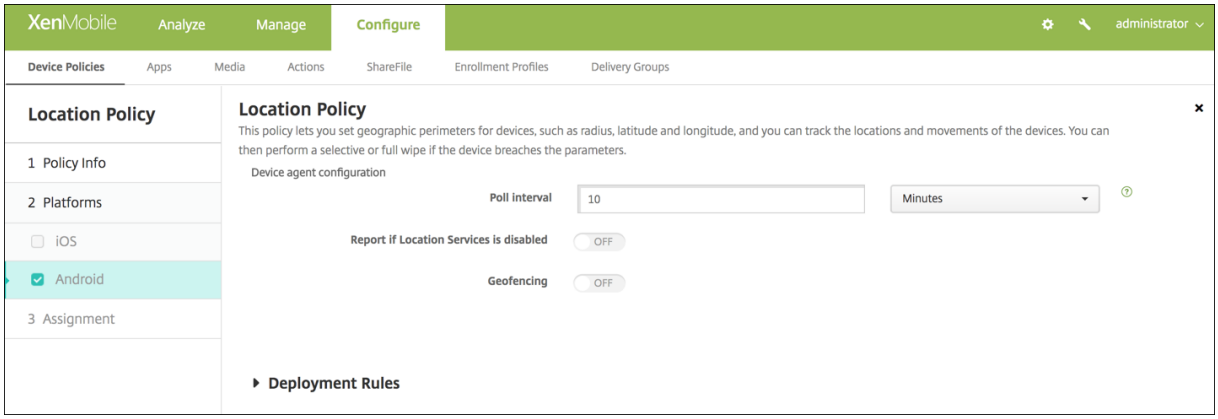
© 1999-2019 Citrix Systems, Inc. All rights reserved.

padrão é 16.400 pés. Valores válidos para o raio são:

- 164 a 164000 pés
- 50 a 50000 metros
- 54 a 54680 jardas
- 1 a 31 milhas

- **Latitude do ponto central:** digite uma latitude, como 37.787454, para definir a latitude do ponto central da geocerca.
- **Longitude do ponto central:** digite uma longitude, como 122.402952, para definir a longitude do ponto central da geocerca.
- **Avisar ao usuário sobre a violação do perímetro:** selecione se uma mensagem de aviso deverá ser emitida quando os usuários violarem o perímetro definido. O padrão é **Off**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **Apagar dados corporativos em caso de violação de perímetro:** selecione se os dispositivos dos usuários deverão ser apagados quando eles violarem o perímetro. O padrão é **Off**. Quando você ativa essa opção, o **campo Atraso no apagamento local** é exibido.
  - Digite um numeral e, na lista, clique em **Segundos** ou **Minutos** para definir o período de tempo a aguardar antes de limpar os dados corporativos dos dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile apague seletivamente os dispositivos deles. O padrão é 0 segundos.

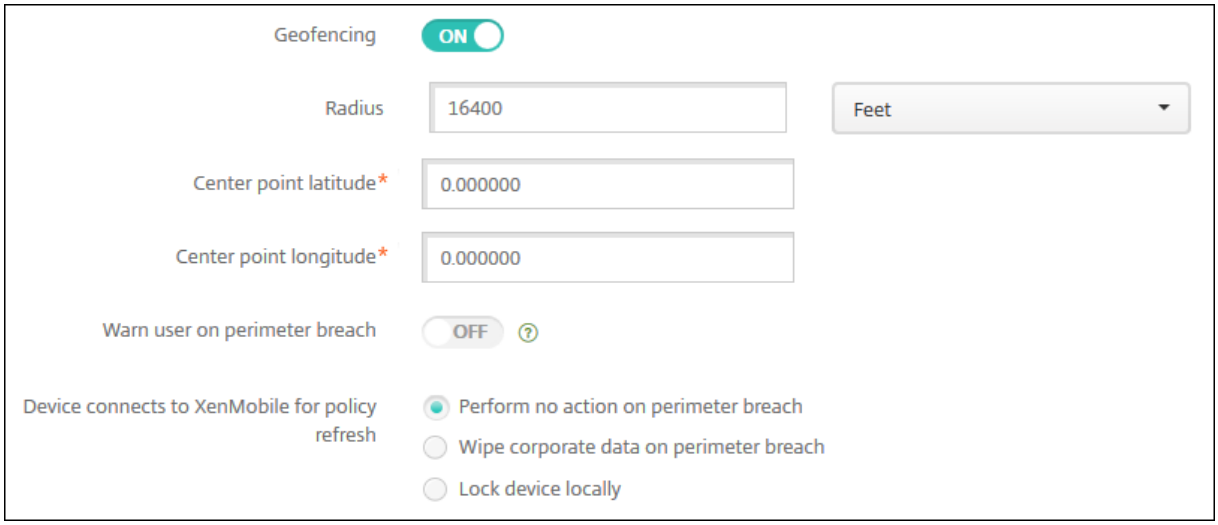
Configurações do Android



- **Intervalo de sondagem:** digite um numeral e, na lista, clique em **Minutos**, **Horas** ou**Dias** para definir a frequência com a qual o XenMobile tenta fixar a localização do dispositivo. Os valores válidos são de 1 a 1440 minutos, de 1 a 24 horas ou qualquer número de dias. O padrão é 10 minutos. Definir esse valor como menos de 10 minutos pode afetar negativamente a duração da bateria do dispositivo.
- **Informar se os serviços de localização estiverem desativados:** selecione se o dispositivo envia um relatório para o XenMobile quando o GPS está desativado. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Cerca geográfica**



Quando você ativar a Geocerca, defina estas configurações:

- **Raio:** digite um numeral e, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Valores válidos para o raio são:
  - 164 a 164000 pés
  - 1 a 50 quilômetros
  - 50 a 50000 metros
  - 54 a 54680 jardas
  - 1 a 31 milhas
- **Latitude do ponto central:** digite uma latitude, como 37.787454, para definir a latitude do ponto central da geocerca.
- **Longitude do ponto central:** digite uma longitude, como 122.402952, para definir a longitude do ponto central da geocerca.
- **Avisar ao usuário sobre a violação do perímetro:** selecione se uma mensagem de aviso deverá ser emitida quando os usuários violarem o perímetro definido. O padrão é **Off**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **O dispositivo se conecta ao XenMobile para atualização de política:** selecione uma das seguintes opções para quando os usuários violarem o perímetro:
  - **Não realizar nenhuma ação em caso de violação do perímetro:** não fazer nada. Esse é o padrão.
  - **Apagar dados corporativos em caso de violação de perímetro:** apagar os dados corporativos depois de um período de tempo especificado. Quando você ativa essa opção, o campo **Atraso no apagamento local** é exibido.
    * Digite um numeral e, na lista, clique em Segundos ou Minutos para definir o período de tempo a aguardar antes de limpar os dados corporativos dos dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido

© 1999-2019 Citrix Systems, Inc. All rights reserved.

antes que o XenMobile apague seletivamente os dispositivos deles. O padrão é 0 segundos.

- **Atraso no bloqueio:** bloquear os dispositivos dos usuários após um período de tempo especificado. Quando você ativa essa opção, o **campo Atraso no bloqueio** é exibido.
  * Digite um numeral e, na lista, clique em Segundos ou Minutos para definir o período de tempo a aguardar antes de bloquear os dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile bloqueie os dispositivos deles. O padrão é 0 segundos.

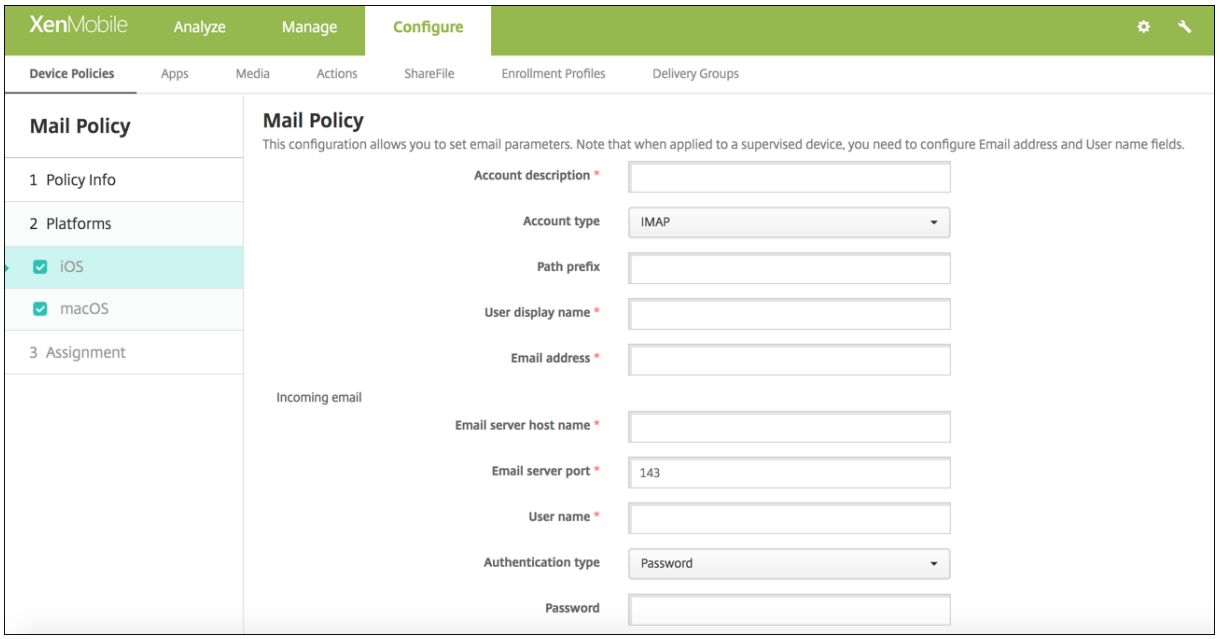
Política de dispositivo de email

April 15, 2019

Você pode adicionar uma política de dispositivo de email ao XenMobile para configurar uma conta de email em dispositivos iOS ou macOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS e do MacOS



- **Descrição da conta:** digite uma descrição da conta que é exibida nos aplicativos Email e Configurações. Este campo é obrigatório.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Tipo de conta:** escolha **IMAP** ou **POP** para selecionar o protocolo a ser usado para contas de usuário. O padrão é **IMAP**. Quando você seleciona **POP**, a opção de prefixo de **Caminho** a seguir desaparece.
- **Prefixo de caminho:** digite **INBOX** ou o prefixo de caminho da sua conta de email IMAP. Este campo é obrigatório.
- **Nome para exibição do usuário:** digite o nome do usuário completo a ser usado para mensagens e outras finalidades. Este campo é obrigatório.
- **Endereço de email:** digite o endereço de email completo da conta. Este campo é obrigatório.
- **Configurações de email de entrada**
  - **Nome de host do servidor de email:** digite o nome do host ou endereço IP do servidor de email de entrada. Este campo é obrigatório.
  - **Porta do servidor de email:** digite o número da porta de servidor de email de entrada. O padrão é **143**. Este campo é obrigatório.
  - **Nome de usuário:** digite o nome de usuário da conta de email. Esse nome é geralmente o mesmo que o endereço de email até o caractere @. Este campo é obrigatório.
  - **Tipo de autenticação:** escolha o tipo de autenticação que deve ser usado. O padrão é **Senha**. Quando **Nenhum** está selecionado, o campo **Senha** a seguir desaparece.
  - **Senha:** digite uma senha opcional para o servidor de email de entrada.
  - **Usar SSL:** selecione se o servidor de email de entrada usa a autenticação Secure Socket Layer. O padrão é **Off**.
- **Configurações de email de saída**
  - **Nome de host do servidor de email:** digite o nome do host ou endereço IP do servidor de email de saída. Este campo é obrigatório.
  - **Porta do servidor de email:** digite o número da porta de servidor de email de saída. Se não houver porta, você não digitará um número da porta, pois a porta padrão para o protocolo especificado será usada.
  - **Nome de usuário:** digite o nome de usuário da conta de email. Esse nome é geralmente o mesmo que o endereço de email até o caractere @. Este campo é obrigatório.
  - **Tipo de autenticação:** escolha o tipo de autenticação para usar. O padrão é **Senha**.
  - **Senha:** digite uma senha opcional para o servidor de email de saída.
  - **Senha de saída idêntica à de entrada:** selecione se as senhas de entrada e de saída são iguais. O padrão é **Off**, o que significa que as senhas são diferentes.
  - **Usar SSL:** selecione se o servidor de email de saída usa a autenticação Secure Socket Layer. O padrão é **Off**.
- **Política**

  Para configurações do iOS, essas opções se aplicam somente ao iOS 5.0 e versões posteriores. Não há restrições para o macOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Autorizar a mudança de emails entre contas:** selecione se os usuários têm permissão para mover emails dessa conta para outra conta, além de encaminhar e responder de uma conta diferente. O padrão é **Off**.
- **Enviar email somente do aplicativo de email:** selecione se os usuários têm restrições no aplicativo de email do iOS para enviar emails.
- **Desativar a sincronização de emails recentes:** selecione se os usuários devem ser impedidos de sincronizar endereços recentes. O padrão é **Off**. Essa opção se aplica somente ao iOS 6.0 e versões posteriores.
- **Permitir Mail Drop:** selecione se deseja permitir o uso do Apple Mail Drop para dispositivos que executam o iOS 9.2 e versões posteriores. O padrão é **Off**.
- **Ativar S/MIME:** selecione se essa conta é compatível com a autenticação e a criptografia S/MIME. O padrão é **Off**. Quando definido como I, os dois campos abaixo são exibidos.
  * **Credencial de identidade de assinatura:** escolha a credencial de assinatura a ser usada.
  * **Credencial de identidade de criptografia:** escolha a credencial de criptografia a ser usada.

Política de dispositivo de domínios gerenciados

April 15, 2019

Você pode definir os domínios gerenciados que se aplicam a emails e ao navegador Safari. Os domínios gerenciados ajudam você a proteger dados corporativos ao controlar quais aplicativos podem abrir documentos baixados de domínios usando o Safari.

Para dispositivos iOS 8 e versões posteriores no modo supervisionado, especifique as URLs ou os subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador. Para iOS 9.3 e versões posteriores em dispositivos supervisionados, você pode especificar as URLs das quais os usuários podem salvar senhas no Safari.

Para ver 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 email para um destinatário cujo domínio não está na lista de domínios de email gerenciados, a mensagem é sinalizada no dispositivo do usuário para avisá-lo que ele está enviando uma mensagem para alguém fora de seu domínio corporativo.

Para itens como documentos, anexos ou downloads: quando um usuário abre um item usando o Safari de um domínio Web que está na lista de domínios Web gerenciados, o aplicativo corporativo adequado abre o item. Se o item não for originário de um domínio Web na lista de domínios Web gerenciados, o usuário não conseguirá abrir o item com um aplicativo corporativo. Ele deverá usar um aplicativo pessoal e não gerenciado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para dispositivos supervisionados, mesmo se você não especificar domínios de preenchimento automático de senha do Safari: se o dispositivo estiver configurado como multiusuários efêmeros, os usuários não poderão salvar as senhas. No entanto, se o dispositivo não estiver configurado como multiusuários efêmeros, os usuários poderão salvar todas as senhas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

Para especificar domínios:

Formato	Descrição
`example.com`	Trate qualquer caminho sob `example.com` como gerenciado, mas não `site.example.com/`.
`foo.example.com`	Trate qualquer caminho sob `foo.example.com` como gerenciado, mas não `example.com/` ou `bar.example.com/`.
`\*.example.com`	Trate qualquer caminho sob `foo.example.com` ou `bar.example.com` como gerenciado, mas não `example.com/`.
`example.com/sub`	Tratar `example.com/sub` e qualquer caminho sob ele como gerenciado, mas não `example.com/`.
`foo.example.com/sub`	Trate qualquer caminho sob `foo.example.com/sub` como gerenciado, mas não `example.com`, `example.com/sub`, `foo.example.com/` ou `bar.example.com/sub`.
`\*.example.com/sub`	Trate qualquer caminho sob `foo.example.com/sub` ou `bar.example.com/sub` como gerenciado, mas não `example.com` ou `foo.example.com/`.

Regras:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Barras à esquerda e à direita de “www.” em URLs são ignoradas quando os domínios são comparados.
- Se uma entrada contiver um número de porta, somente os endereços que especificam esse número de porta são considerados gerenciados. Caso contrário, somente 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`, enquanto 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 Web gerenciado do Safari são cumulativas. Os padrões definidos por todas as cargas de domínio Web gerenciado do Safari são usados para realizar a correspondência com uma solicitação de URL.

Configurações:

- **Domínios gerenciados**
  - **Domínios de email não marcados:** para cada domínio de email que você desejar incluir na lista, clique em **Adicionar** e faça o seguinte:
    * **Domínio de email gerenciado:** digite o domínio de email.
    * Clique em **Salvar** para salvar o domínio de email ou em **Cancelar** para não salvar.
  - **Domínios Web Safari gerenciados:** para cada domínio Web que você desejar incluir na lista, clique em **Adicionar** e faça o seguinte:
    * **Domínio Web gerenciado:** digite o domínio Web.
    * Clique em **Salvar** para salvar o domínio Web ou em **Cancelar** para não salvar.
  - **Domínios de preenchimento automático de senha do Safari:** para cada domínio de preenchimento automático que você desejar 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.

Políticas de dispositivo das opções de MDM

April 15, 2019

Você pode criar uma política de dispositivo no XenMobile para gerenciar o Bloqueio de ativação buscar iPhone/iPad nos dispositivos de telefone supervisionados iOS 7.0 e versões posteriores. Para ver 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

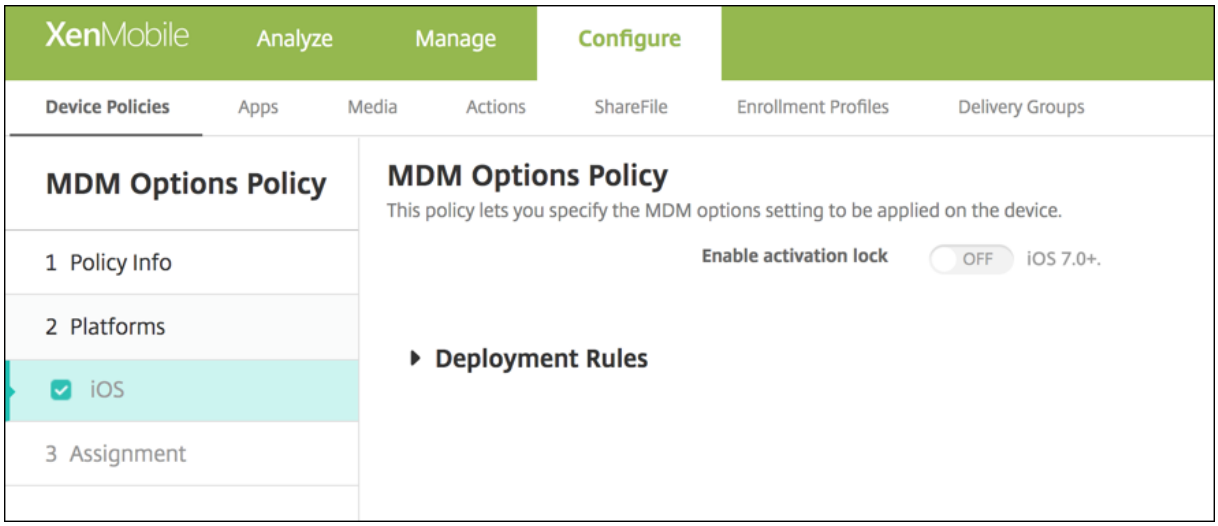
Bloqueio de ativação é um recurso do Buscar iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário antes que qualquer pessoa possa desligar o Buscar iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos de propriedade da organização, ignorar um bloqueio de ativação é necessário, por exemplo, para redefinir ou realocar dispositivos.

Para ativar o Bloqueio de Ativação, você configura e implanta a política do dispositivo de Opções XenMobile MDM. Você pode gerenciar um dispositivo a partir do console XenMobile sem as credenciais Apple do usuário. Para desviar do requisito de credenciais Apple de um bloqueio de ativação, execute a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Por exemplo, se o usuário retorna um telefone perdido ou para configurar o dispositivo antes ou após um apagamento completo: quando o telefone pede as credenciais de conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação no console XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



- **Ativar bloqueio de ativação:** selecione se o bloqueio de ativação deve ser ativado nos dispositivos nos quais você implantar essa política. O padrão é **Off**.

Depois de ativar o Bloqueio de Ativação, implantando a política do dispositivo de opções do MDM: a Ação de Segurança **Ignorar bloqueio de ativação** aparece quando você seleciona esses dispositivos na página **Gerenciar > Dispositivos** e clica em **Segurança**. O desvio do bloqueio de ativação permite que você remova 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 desvio do bloqueio de ativação a um dispositivo antes ou depois de um apagamento completo. Para obter mais informações, consulte Ignorar bloqueio de ativação do iOS no artigo de ações de segurança.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de informação da organização

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para especificar as informações da sua organização para mensagens de alerta que são enviadas por push do XenMobile para dispositivos iOS. A política está disponível para dispositivos iOS 7 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de 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.
- **Email:** digite o endereço de email de suporte.
- **Magic:** digite uma palavra ou uma frase que descreva os serviços gerenciados pela organização.

Política de dispositivo de código secreto

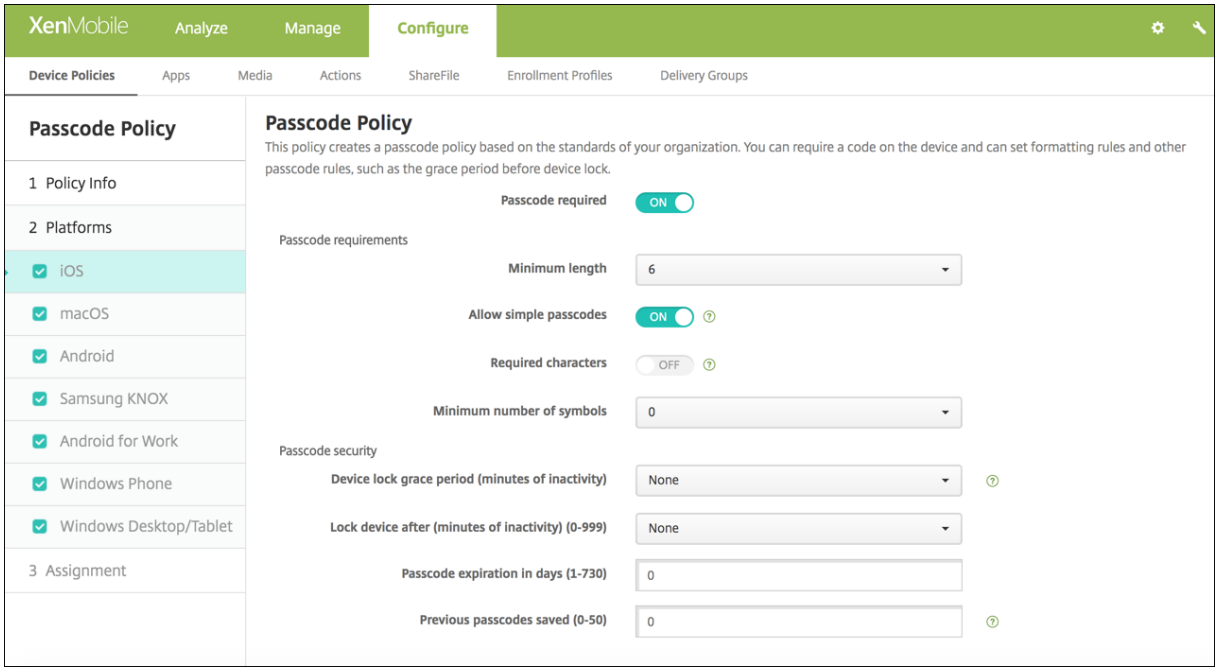
April 15, 2019

Crie uma política de código secreto no XenMobile com base nos padrões da sua organização. Você pode exigir códigos secretos nos dispositivos dos usuários e definir várias regras de formatação e de código secreto. Você pode criar políticas para iOS, macOS, Android, Samsung KNOX, Android for Work, Windows Phone e Windows Desktop/Tablet. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS

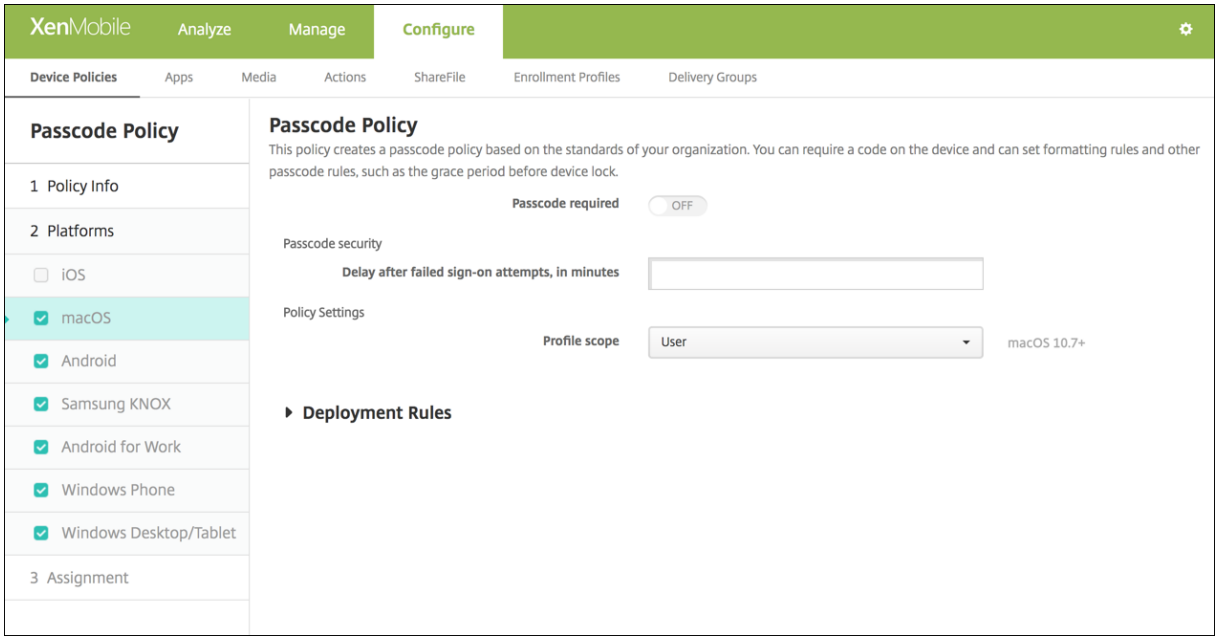


- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do iOS. A página se expande para permitir que você defina as configurações dos requisitos de código secreto, segurança do código secreto e configurações de política.
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
  - **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **On**.
  - **Caracteres obrigatórios:** selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **Off**.
  - **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **0**.
- **Segurança do código secreto**
  - **Período de tolerância de bloqueio do dispositivo (minutos de inatividade):** na lista, clique no período de tempo antes que os usuários tenham que digitar um código secreto para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
  - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é Nenhum.
  - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 730. O padrão é **0**, o que significa que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a senha nunca expira.
  - **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo foi totalmente apagado com êxito. O padrão é **Não definido**.
- **Configurações de política**
  - Ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

Configurações do macOS



- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do iOS. A página se expande para permitir que você defina as configurações dos requisitos de código secreto, segurança do código secreto e configurações de política.
- Se você não ativar **Senha necessária**, ao lado de **Atraso após tentativas de login com falha,**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

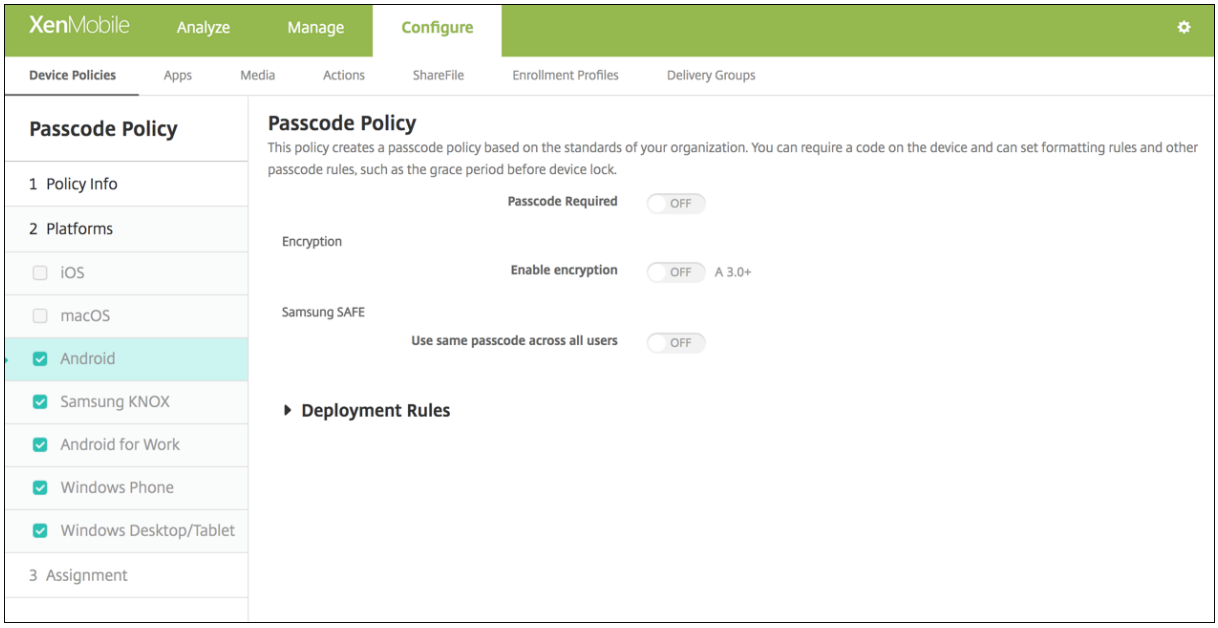
em minutos, digite o número de minutos de atraso antes de permitir que os usuários reinsiram o código secreto.

- Se você ativar **Senha necessária**, defina as seguintes configurações:
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
  - **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **On**.
  - **Caracteres obrigatórios:** selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **Off**.
  - **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **0**.
- **Segurança do código secreto**
  - **Período de tolerância de bloqueio do dispositivo (minutos de inatividade):** na lista, clique no período de tempo antes que os usuários tenham que digitar um código secreto para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
  - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
  - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 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 conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é bloqueado. O padrão é **Não definido**.
  - **Atraso após tentativas de login com falha, em minutos:** digite o número de minutos de atraso antes de permitir que um usuário reinsira um código secreto.
- **Configurações de política**
  - Ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Android



> Nota:
>
> A configuração padrão para o Android é **Off**.

- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do Android. A página se expande para permitir que você defina as configurações de requisitos de código secreto, segurança do código secreto, criptografia e Samsung SAFE.
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é 6.
  - **Reconhecimento biométrico:** selecione se o reconhecimento biométrico deve ser ativado. Se você habilitar essa opção, o campo Caracteres obrigatórios ficará oculto. O padrão é **Off**.
  - **Caracteres obrigatórios:** na lista, clique em Sem restrição, Letras e números, Apenas números ou Apenas letras para configurar como os códigos secretos são compostos. O padrão é Sem restrição.
  - **Regras avançadas:** selecione se regras avançadas de código secreto devem ser aplicadas. Essa opção está disponível para o Android 3.0 e versões posteriores. O padrão é **Off**.
  - Quando você habilitar **Regras avançadas**, em cada uma das seguintes listas, clique no número mínimo de cada tipo de caractere que uma senha deve conter:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

    * **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 do código secreto**
  - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
  - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 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 conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é apagado. O padrão é **Não definido**.

- **Criptografia**
  - **Ativar criptografia:** selecione se a criptografia deve ser ativada. Essa opção está disponível para o Android 3.0 e versões posteriores. A opção está disponível independentemente da configuração da **Senha necessária**.

    Para criptografar seus dispositivos, os usuários devem começar com uma bateria carregada e manter o dispositivo conectado durante o período de uma hora ou mais que é decorrido para a criptografia. Se o processo de criptografia for interrompido, eles poderão perder alguns ou todos os dados nos dispositivos deles. Depois que um dispositivo é criptografado, o processo não pode ser revertido exceto por uma redefinição de fábrica, que apaga todos os dados no dispositivo.

- **Samsung SAFE**

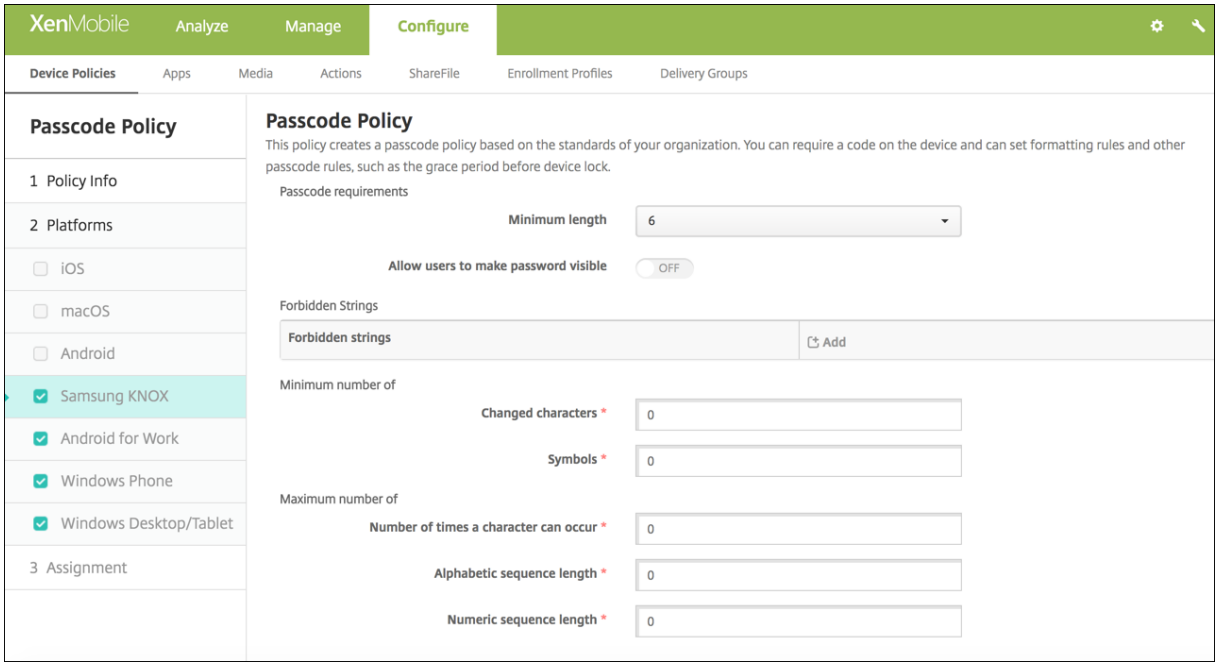
> Nota:
>
> Como solução alternativa para desativar o reconhecimento facial ou de íris em dispositivos Samsung SAFE: crie uma política de dispositivo Restrições para o Samsung SAFE. Na política Restrições, ative **Desativar Aplicativos** e adicione `com.samsung.android.bio.face.service` ou `com.samsung.android.server.iris` à tabela. Em seguida, implante a política de restrições.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Usar o mesmo código secreto para todos os usuários:** selecione se o mesmo código secreto deve ser usado para todos os usuários. O padrão é **Off**. Esta configuração aplica-se somente aos dispositivos Samsung SAFE e está disponível independentemente da configuração de **Senha necessária**.
- Quando você ativar a opção **Usar o mesmo código secreto para todos os usuários**, digite o código secreto a ser usado por todos os usuários no campo **Código secreto**.
- Quando você ativar a **Senha requerida**, configure as seguintes configurações do SAFE da Samsung:
  * **Caracteres alterados:** digite o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
  * **Número de vezes em que um caractere pode ocorrer:** digite o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**.
  * **Tamanho da sequência alfabética:** digite o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**.
  * **Tamanho da sequência numérica:** digite o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**.
  * **Permitir que os usuários tornem a senha visível:** selecione se os usuários podem tornar visíveis os códigos secretos deles. O padrão é **On**.
  * **Configure a autenticação biométrica**. Selecione a autenticação biométrica deve ser ativada. O padrão é **Off**. Se você configurá-la como **On**, você pode definir essas opções:
    · **Permitir impressão digital**. Selecione para permitir que os usuários se autentiquem usando a impressão digital.
    · **Permitir íris**. Selecione para permitir que os usuários se autentiquem usando a íris.
  * **Cadeias de caracteres proibidas:** crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como “senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você desejar negar, clique em **Adicionar** e faça o seguinte:
    · **Cadeias de caracteres proibidas:** digite as cadeias de caracteres que os usuários não podem usar.
    · Clique em **Salvar** para adicionar a cadeia de caracteres ou em **Cancelar** para cancelar a adição da cadeia de caracteres.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Samsung KNOX



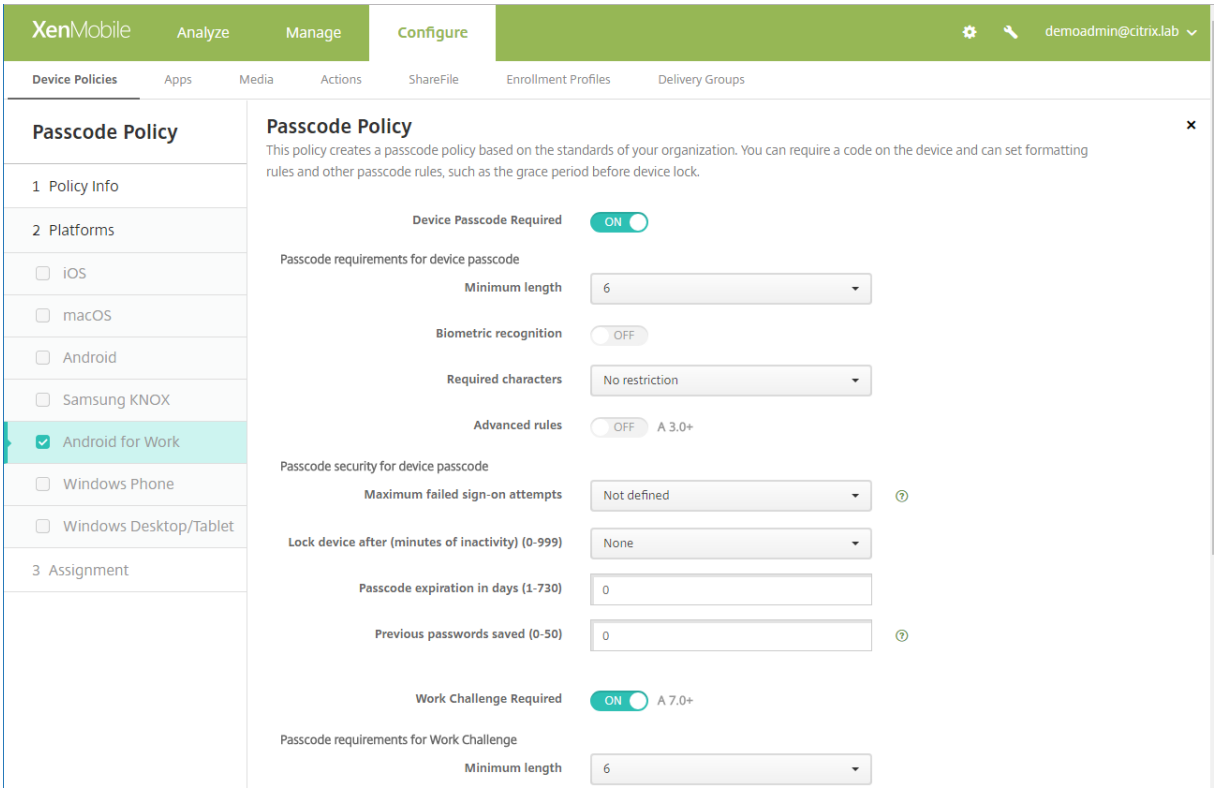
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
  - **Permitir que os usuários tornem a senha visível:** selecione se os usuários podem tornar a senha visível.
  - **Cadeias de caracteres proibidas:** crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como “senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você desejar negar, clique em Adicionar e faça o seguinte:
    * **Cadeias de caracteres proibidas:** digite as cadeias de caracteres que os usuários não podem usar.
    * Clique em **Salvar** para adicionar a cadeia de caracteres ou em **Cancelar** para cancelar a adição da cadeia de caracteres.
- **Número mínimo de**
  - **Caracteres alterados:** digite o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
  - **Símbolos:** digite o número mínimo de símbolos necessários em um código secreto. O padrão é **0**.
- **Número máximo de**
  - **Número de vezes em que um caractere pode ocorrer:** digite o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**.
  - **Tamanho da sequência alfabética:** digite o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Tamanho da sequência numérica:** digite o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**.
- **Segurança do código secreto**
  - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no número de segundos durante os quais um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
  - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 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 conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Se o número de tentativas de login for excedido, o dispositivo é bloqueado:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é bloqueado. O padrão é **Não definido**.
  - **Se o número de tentativas de login for excedido, o dispositivo é apagado**: na lista, clique no número de vezes que um usuário pode não conseguir fazer login com êxito, após as quais o contêiner do KNOX (juntamente com os dados do KNOX) é apagado do dispositivo. Os usuários precisam reinicializar o contêiner KNOX após a limpeza. O padrão é **Não definido**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android for Work



- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do Android for Work. A página se expande para permitir que você defina as configurações dos requisitos de código secreto e segurança do código secreto. O padrão é **Off**.
- **Work Challenge obrigatório:** ative esta configuração para exigir que os usuários concluam um desafio de segurança para acessar aplicativos em execução em um perfil de trabalho do Android for Work. A página se expande para permitir que você defina as configurações dos requisitos de código secreto e segurança do código secreto. Essa opção não está disponível para dispositivos Android anteriores ao Android 7.0. O padrão é **Off**.
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
  - **Reconhecimento biométrico:** selecione se o reconhecimento biométrico deve ser ativado. Se você habilitar essa opção, o campo **Caracteres obrigatórios** ficará oculto. O padrão é **Off**. Observe que esse recurso não é compatível no momento.
  - **Caracteres obrigatórios:** na lista, clique em **Sem restrição**, **Letras e números**, **Apenas números** ou **Apenas letras** para configurar como os códigos secretos são compostos.
    * Para o código secreto do dispositivo: o padrão é **Sem restrição**.
    * Para o Work Challenge: use **Sem restrições** somente para dispositivos que executam o Android 7.0. A configuração **Sem restrições** não é respeitada pelo Android 7.1 e ver-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

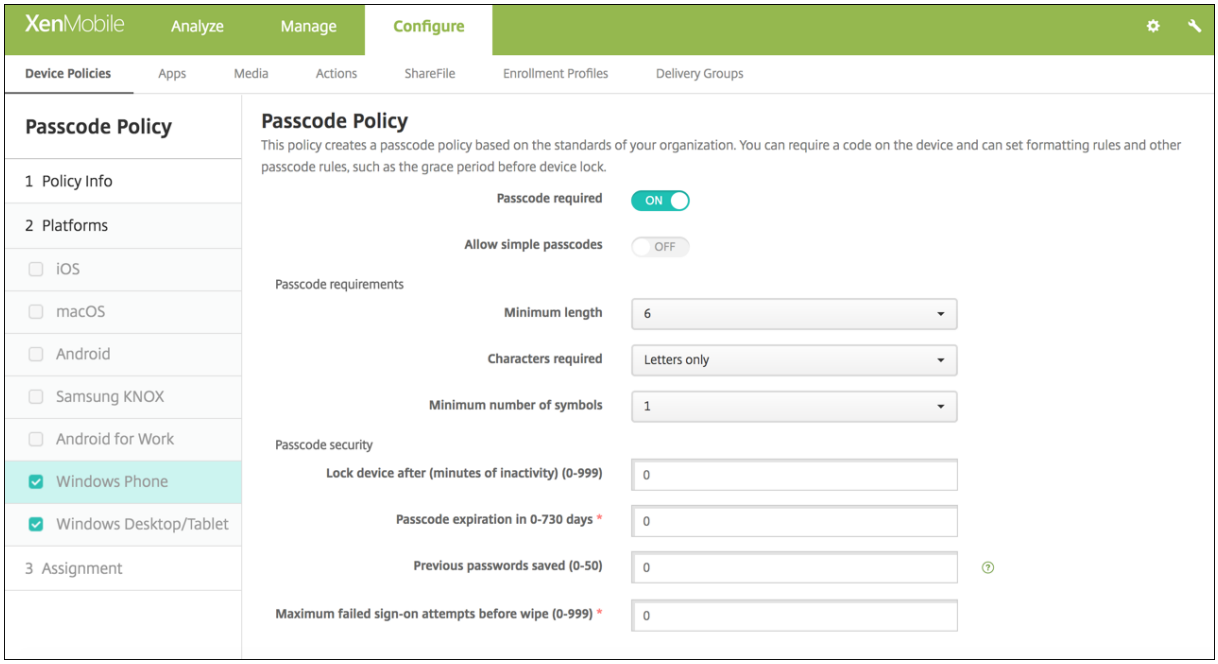
sões posteriores. O padrão é **Letras e números**.

- **Regras avançadas:** selecione se regras avançadas de código secreto devem ser aplicadas. Essa opção não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **Off**.
- Quando você habilitar **Regras avançadas**, em cada uma das seguintes listas, clique no número mínimo de cada tipo de caractere que uma senha deve conter:
  - **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 do código secreto**
  - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no número de minutos durante os quais um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
  - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 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 conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login com êxito, após as quais o contêiner do KNOX (juntamente com os dados do KNOX) é apagado do dispositivo. Os usuários precisam reinicializar o contêiner KNOX após a limpeza. O padrão é **Não definido**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Phone

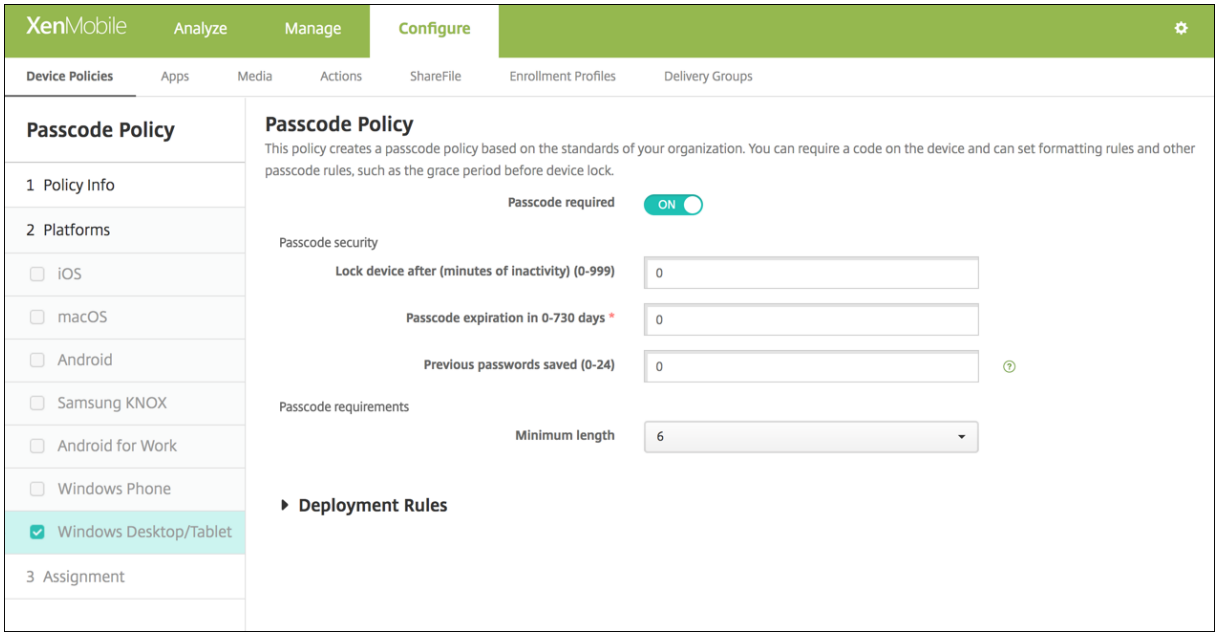


- **Código secreto obrigatório:** selecione essa opção para não exigir um código secreto para dispositivos Windows Phone. A configuração padrão é **I**, o que exige um código secreto. A página é recolhida e as opções a seguir desaparecem quando você desativa essa configuração.
- **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é O.
- **Requisitos de código secreto**
  - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
  - **Caracteres obrigatórios:** na lista, clique em **Numérico ou alfanumérico**, **Apenas letras** ou **Apenas números** para configurar como os códigos secretos são compostos. O padrão é **Apenas letras**.
  - **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **1**.
- **Segurança do código secreto**
  - **Bloquear dispositivos após (minutos de inatividade):** clique no número de minutos durante os quais um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **0**.
  - **Expiração de código secreto em 0-730 dias:** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 0 a 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 conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de login antes de apagamento (0-999):** digite o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

número de vezes que um usuário pode não conseguir fazer login depois que os dados corporativos são apagados do dispositivo. O padrão é **0**.

Configurações do Windows Desktop/Tablet



- **Não permitir login de conveniência:** selecione se os usuários têm permissão para acessar os dispositivos deles com senhas de imagem ou logins biométricos. O padrão é **Off**.
- **Tamanho mínimo do código secreto:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
- **Máximo de tentativas do código secreto antes de apagar:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que os dados corporativos são apagados do dispositivo. O padrão é **4**.
- **Expiração de código secreto em dias (0-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 0 a 730. O padrão é **0**, o que significa que a senha nunca expira.
- **Histórico do código secreto (1-24):** digite o número de códigos secretos usados a serem salvos. Os usuários não conseguem usar nenhum código secreto encontrado nessa lista. Os valores válidos são 1 a 24. Você deve inserir um número entre 1 e 24 nesse campo. O padrão é **0**.
- **Máximo de inatividade antes do bloqueio do dispositivo em minutos (1-999):** digite o período de tempo, em minutos, durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. Os valores válidos são 1 a 999. Você deve inserir um número entre 1 e 999 nesse campo. O padrão é **0**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do ponto de acesso pessoal

April 15, 2019

Você pode permitir que os usuários se conectem à Internet quando não estão ao alcance de uma rede WiFi usando a conexão de dados celulares, por meio da funcionalidade de ponto de acesso pessoal de seus dispositivos iOS. Disponível no iOS 7.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Desativar ponto de acesso pessoal:** selecione se pretende desativar a funcionalidade de ponto de acesso pessoal em dispositivos do usuário. O padrão é **O**, que desliga o ponto de acesso pessoal em dispositivos de usuários. Esta política não desativa a funcionalidade. Os usuários ainda podem usar o ponto de acesso pessoal em seus dispositivos, mas quando a política é implantada, o ponto de acesso pessoal é desativado para que não permaneça ativado por padrão.

Política de dispositivo de remoção de perfil

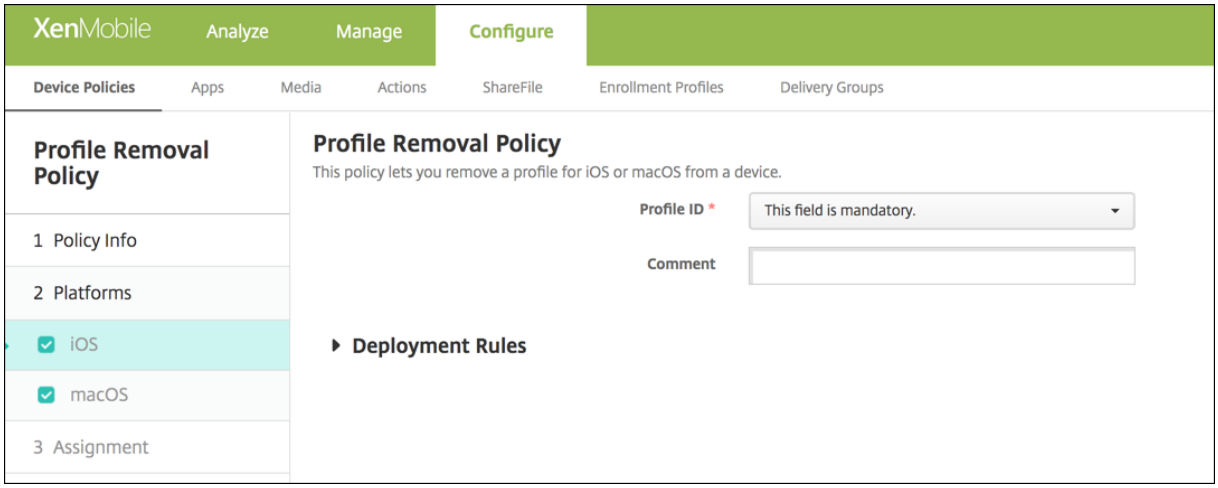
April 15, 2019

Você pode criar uma política de dispositivo de remoção de perfil de aplicativo no XenMobile. A política, quando implantada, remove o perfil de aplicativo dos dispositivos iOS ou macOS dos usuários.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

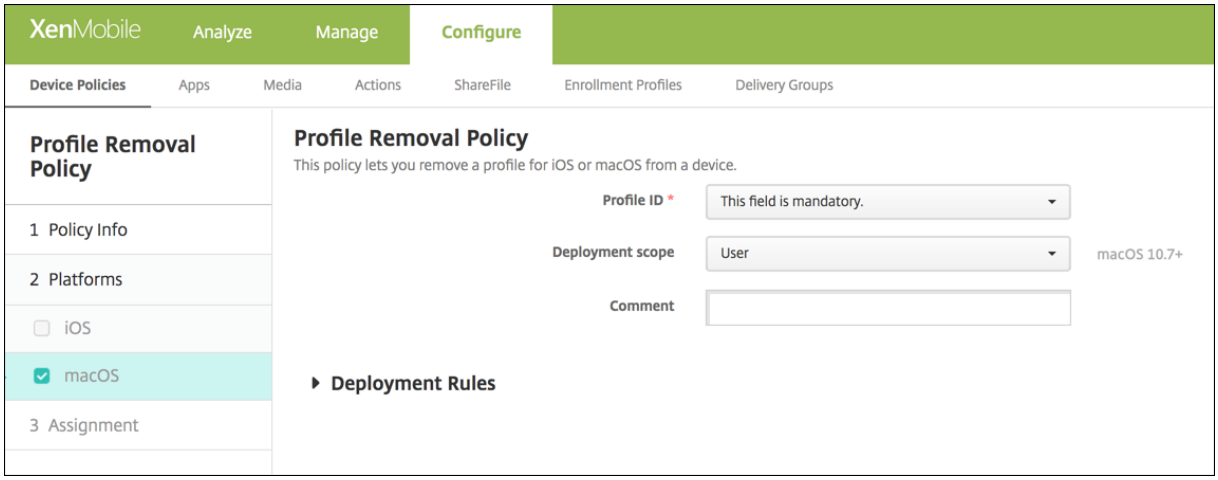
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



- **ID do perfil:** na lista, clique no ID do perfil do aplicativo. Este campo é obrigatório.
- **Comentário:** digite um comentário opcional.

Configurações do macOS



- **ID do perfil:** na lista, clique no ID do perfil do aplicativo. Este campo é obrigatório.
- **Alcance da implantação:** na lista, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.
- **Comentário:** digite um comentário opcional.

Política de dispositivo do perfil de provisionamento

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

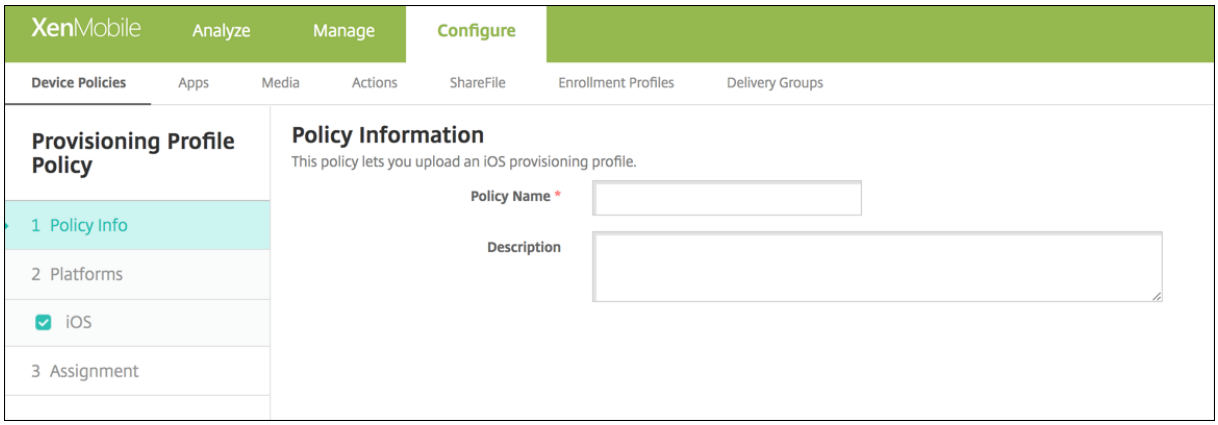
Quando você desenvolve e assina o código de um aplicativo empresarial iOS, geralmente inclui um perfil de provisionamento de distribuição empresarial, exigido pela Apple para que o aplicativo seja executado em um dispositivo iOS. Se um perfil de configuração estiver ausente ou tiver expirado, o aplicativo falhará quando um usuário tocar para abri-lo.

O principal problema dos perfis de provisionamento é que eles expiram um ano depois de terem sido gerados no Apple Developer Portal e você deve manter o controle das datas de expiração de todos os seus perfis de provisionamento em todos os dispositivos iOS registrados por seus usuários. Rastrear as datas de expiração envolve não apenas o acompanhamento das datas de expiração propriamente ditas, mas também de qual versão do aplicativo está sendo usada por usuários específicos. Duas soluções são enviar por email os perfis de configuração para os usuários ou colocá-los em um portal da Web para download e instalação. Essas soluções funcionam, mas são propensas a erro porque elas exigem que os usuários sigam as instruções em um email ou acessem o portal da Web e baixem o perfil correto para instalá-lo.

Para tornar esse processo transparente para os usuários, no XenMobile, você pode instalar e remover perfis de provisionamento com as políticas de dispositivo. Os perfis ausentes ou expirados são removidos conforme necessário e os perfis atualizados são instalados nos dispositivos de usuários, para que seja preciso apenas tocar em um aplicativo para abri-lo.

Antes de criar uma política de perfil de provisionamento, você deve criar um arquivo de perfil de provisionamento. Para obter mais informações, consulte Creating Provisioning Profiles no site Apple Developer.

Configurações de iOS



- **Perfil de provisionamento do iOS:** selecione o arquivo de perfil de provisionamento a ser importado clicando em **Procurar** e navegando até a localização do arquivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo da remoção de perfil de provisionamento

April 15, 2019

Você pode remover os perfis de provisionamento do iOS com as políticas de dispositivo. Para obter mais informações sobre perfis de provisionamento, consulte Política de dispositivo do perfil de provisionamento.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Perfil de provisionamento do iOS**: na lista, clique no perfil de provisionamento que deseja remover.
- **Comentário:** opcionalmente, adicione um comentário.

Política de dispositivo de proxy

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para especificar as configurações de proxy HTTP global dos dispositivos que executam o Windows Mobile/CE e o iOS 6.0 ou versões posteriores. Você pode implantar somente uma política de proxy HTTP global por dispositivo.

> Nota:
>
> Antes de implantar essa política, defina todos os dispositivos iOS para os quais você deseja atribuir um proxy HTTP global no modo Supervisionado. Para obter detalhes, consulte Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Configuração de proxy:** clique em **Manual** ou **Automática** para selecionar como o proxy será configurado nos dispositivos dos usuários.
  - Se você clicar em **Manual**, defina estas configurações:
    * **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **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 autenticação no servidor proxy.
        * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
    - Se você clicar em **Automático**, defina estas configurações:
        * **URL PAC do Proxy:** digite a URL do arquivo PAC que define a configuração de proxy.
        * **Permitir conexão direta se o PAC estiver inacessível:** selecione se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.
- **Permitir ignorar o proxy para acessar redes cativas:** selecione se o proxy pode ser ignorado para o acesso a redes cativas. O padrão é **Off**.
- **Configurações de política**
    - Ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
    - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
    - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
    - Se você clicar em **Senha** obrigatória, ao lado de **Senha de remoção**, digite a senha necessária.

Configurações do Windows Mobile/CE

- **Rede:** na lista, clique no tipo de rede a ser usada. O padrão é **Escritório interno**. As opções possíveis são:
    - Escritório definido pelo usuário
    - Internet definida pelo usuário
    - Escritório interno
    - Internet interna
- **Rede:** na lista, clique no protocolo de conexão de rede a ser usado. O padrão é **HTTP**. As opções possíveis são:
    - HTTP
    - WAP
    - SOCKS 4
    - SOCKS 5
- **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Porta do servidor proxy:** digite o número da porta do servidor proxy. Este campo é obrigatório. O padrão é **80**.
- **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
- **Senha:** digite uma senha opcional para autenticação no servidor proxy.
- **Nome de domínio:** digite um nome de domínio opcional.
- **Ativar:** selecione se o proxy deve ser ativado. O padrão é **On**.

Política de dispositivo do Registro

April 15, 2019

O Registro do Windows Mobile/CE armazena dados sobre as definições de aplicativos, drivers, preferências do usuário e configurações. No XenMobile, você pode definir as chaves e os valores do registro que permitem administrar dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows Mobile/CE

Para cada chave do registro ou par chave/valor do registro que você desejar adicionar, clique em **Adicionar** e faça o seguinte:

- **Caminho da chave do Registro:** digite o caminho completo da chave do registro. Por exemplo, digite **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows** para especificar a rota para a chave do Windows a partir da chave raiz HKEY_LOCAL_MACHINE.
- **Nome do valor do registro:** digite o nome do valor da chave do registro. Por exemplo, digite **ProgramFilesDir** para adicionar esse nome de valor ao caminho de chave do registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion. Se você deixar esse campo em branco, isso significará que você está adicionando uma chave do registro e não um par chave/valor do registro.
- **Tipo:** na lista, clique no tipo de dados do valor. O padrão é **DWORD**. As opções possíveis são:
  - **DWORD:** um inteiro não assinado de 32 bits.
  - **Cadeia de caracteres:** qualquer cadeia de caracteres.
  - **Cadeia de caracteres estendida:** um valor de cadeia de caracteres que pode conter variáveis de ambiente como %TEMP% ou %USERPROFILE%.
  - **Binário:** quaisquer dados binários arbitrários.
- **Valor:** digite o valor associado ao nome do valor do Registro. Por exemplo, para especificar o valor de ProgramFilesDir, digite **C:\Program Files**.
- Clique em **Salvar** para salvar as informações de chave do registro ou em **Cancelar** para não salvá-las.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Suporte remoto à política de dispositivo

April 15, 2019

> Nota:
>
> Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível com somente dispositivos Samsung KNOX.
>
> O suporte remoto não é suportado para implantações do XenMobile Server em cluster no local.
>
> Para obter mais informações, consulte Opções de suporte e suporte remoto.

Crie uma política de suporte remoto no XenMobile para conceder a você acesso remoto aos dispositivos Windows e Android compatíveis. Você pode configurar dois tipos de suporte:

- **Básico**, que permite exibir informações de diagnóstico sobre o dispositivo, como informações do sistema, processos em execução, gerenciador de tarefas (uso da memória e da CPU), conteúdo da pasta do software instalado e assim por diante.
- **Premium**, que permite controlar remotamente a tela do dispositivo, incluindo:
  - controlar cores (na janela principal ou em uma janela flutuante separada)
  - estabelecer uma sessão de Voice-over-IP (VoIP) entre o suporte técnico e o usuário
  - definir configurações
  - criar uma sessão de chat entre o suporte técnico e o usuário

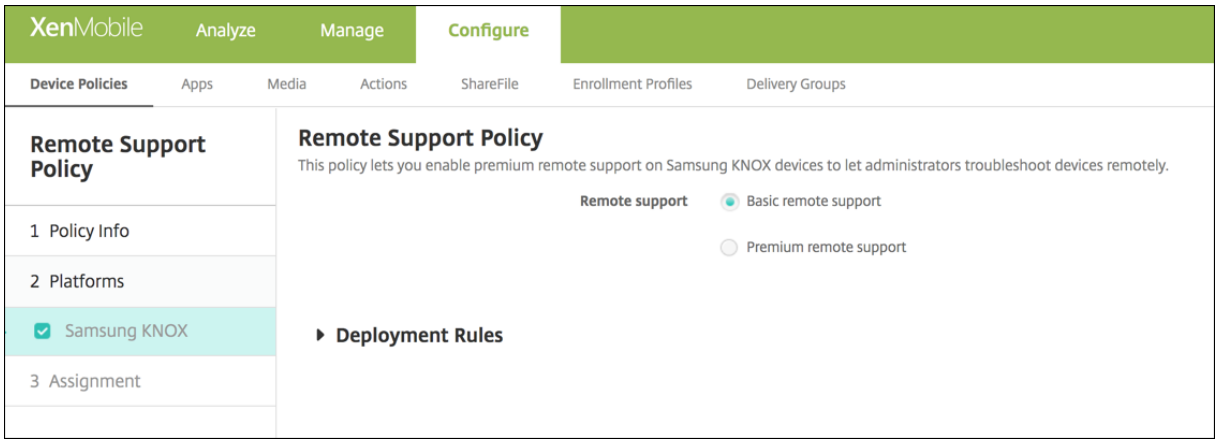
Para implementar essa política, você deve fazer o seguinte:

- Instale o aplicativo XenMobile Remote Support no seu ambiente.
- Configure um túnel de aplicativo de suporte remoto. Para obter detalhes, consulte Política de dispositivo de encapsulamento de aplicativo.
- Configure uma política de dispositivo de suporte remoto do Samsung KNOX, conforme descrito neste tópico.
- Implante a política de suporte remoto do túnel de aplicativo e a política de suporte remoto do Samsung KNOX para os dispositivos do usuário.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android e Windows CE



- **Suporte remoto:** selecione **Suporte remoto básico** ou **Suporte remoto premium**. O padrão é o **Suporte remoto básico**.

Política de dispositivo de restrições

April 15, 2019

Essa política de dispositivo de restrições permite ou restringe certos recursos ou funcionalidades nos dispositivos dos usuários, como a câmera. Você também pode definir restrições de segurança, bem como restrições sobre conteúdo de mídia e restrições sobre os tipos de aplicativos que os usuários podem e não podem instalar. A maior parte das configurações de restrição têm **I**, ou *permite* como padrão. As exceções principais estão no recurso Segurança do iOS - Forçar e em todos os recursos do Tablet Windows, que têm **O** ou *restringe* como padrão.

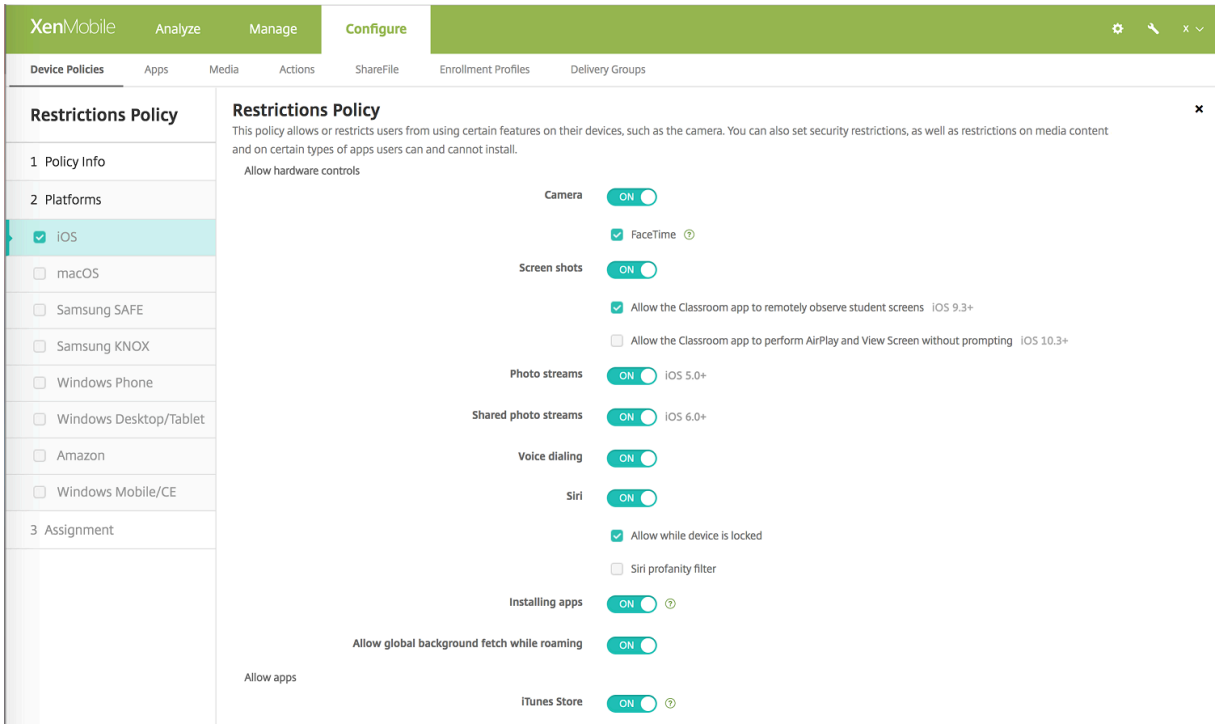
Para telefones Windows 10 RS2, depois que uma política de XML personalizado ou de Restrições que desativa o Internet Explorer é implantada no telefone, o navegador permanece ativado. Para resolver esse problema, reinicie o telefone. Esse é um problema de terceiros.

> Dica:
>
> Qualquer opção para a qual você selecionar **I** significa que o usuário pode executar a operação ou usar o recurso. Por exemplo:
>
> **Câmera**. Se **I**, o usuário poderá usar a câmera no seu dispositivo. Se **O**, o usuário não poderá usar a câmera no seu dispositivo.
>
> **Capturas de tela**. Se **I**, o usuário pode fazer capturas de tela no seu dispositivo. Se **O**, o usuário não pode fazer capturas de tela no seu dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS



Algumas das opções de restrições do iOS se aplicam somente a versões específicas do iOS (e, onde aplicável, essas versões estão descritas na página do console XenMobile). Por exemplo, a capacidade de permitir ou bloquear o AirDrop é compatível somente em dispositivos que executam o iOS 7 e versões posteriores. A capacidade de permitir ou bloquear fluxos de fotos do Photo Stream é compatível somente em dispositivos que executam o iOS 5 e versões posteriores. Além disso, algumas opções se aplicarão somente se o dispositivo for colocado no modo supervisionado. Para ver 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.

- **Permitir controles de hardware**
  - **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
    - **FaceTime:** Permitir que os usuários usem o FaceTime nos respectivos dispositivos. Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
  - **Capturas de tela:** Permitir que os usuários façam capturas de tela nos dispositivos deles.
    - **Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos:** se essa restrição não estiver selecionada, o professor não poderá usar o aplicativo Sala de Aula para observar remotamente as telas dos alunos. A configuração padrão está selecionada, um professor pode usar o aplicativo Sala de Aula para observar as telas dos alunos. A configuração de **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar** determina se os alunos receberão uma solicitação para conceder a permissão ao professor. Para dispositivos supervisionados

© 1999-2019 Citrix Systems, Inc. All rights reserved.

executando o iOS 9.3 (versão mínima).
    * **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 10.3 (versão mínima).
  - **Fluxos de foto:** permitir que os usuários usem o MyPhotoStream para compartilhar fotos usando o iCloud com todos os dispositivos iOS deles (disponível no iOS 5.0 e versões posteriores).
  - **Fluxos de fotos compartilhados:** permitir que os usuários usem o Compartilhamento de fotos do iCloud para compartilhar fotos com colegas de trabalho, amigos e família (disponível no iOS 6.0 e versões posteriores).
  - **Discagem por voz:** ativa a discagem por voz nos dispositivos do usuário.
  - **Siri:** permite que os usuários usem a Siri.
    * **Permitir enquanto o dispositivo estiver travado:** permitir que os usuários usem a Siri enquanto os dispositivos deles estão bloqueados.
    * **Filtro de linguagem indecorosa da Siri:** Ativar o filtro de linguagem indecorosa da Siri. O padrão é restringir esse recurso, o que significa que nenhum filtro de linguagem indecorosa é usado.

      Para obter mais informações sobre Siri e segurança, consulte Siri e políticas de ditado.
  - **Instalação de aplicativos:** Permitir que os usuários instalem aplicativos. Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
  - **Permitir busca em segundo plano durante roaming:** permite que os dispositivos sincronizem automaticamente as contas de correio com o iCloud enquanto estiverem em roaming. Quando **O**, desativa as atividades de busca global em segundo plano quando um telefone iOS está em roaming. O padrão é **Ativado**.

- **Permitir aplicativos**
  - **iTunes Store:** Permitir que os usuários acessem a iTunes Store. Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
  - **Compras no aplicativo:** Permitir que os usuários façam compras no aplicativo.
    * **Exigir senha do iTunes para compras:** Exigir uma senha para compras no aplicativo. O padrão é restringir esse recurso, o que significa que nenhuma senha é necessária para compras no aplicativo (iOS 5.0 e versões posteriores).
  - **Safari:** permitir que os usuários acessem o Safari. Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
    * **Preenchimento automático:** Permitir que os usuários configurem o preenchimento automático de nomes de usuário e senhas no Safari.
    * **Forçar aviso de fraude:** se essa configuração estiver ativada e os usuários visitarem um site de phishing suspeito, o Safari os alertará. O padrão é restringir esse recurso, o que significa que nenhum aviso é emitido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

    * **Ativar JavaScript:** permitir a execução de JavaScript no Safari.
    * **Bloquear pop-ups:** bloquear pop-ups durante a exibição de sites. O padrão é restringir esse recurso, o que significa que pop-ups não são bloqueados.
- **Aceitar cookies:** definir a extensão da aceitação de cookies. Na lista, escolha uma opção para permitir ou restringir cookies. A opção padrão é **Sempre**, o que permite que todos os sites salvem cookies no Safari. Outras opções são **Somente site atual**, **Nunca** e **Somente dos sites visitados**.
- **Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos:** se essa restrição não estiver selecionada, o professor não poderá usar o aplicativo Sala de Aula para observar as telas dos alunos remotamente. A configuração padrão está selecionada, um professor pode usar o aplicativo Sala de Aula para observar as telas dos alunos. A configuração de **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar** determina se os alunos receberão uma solicitação para conceder a permissão ao professor. Para dispositivos supervisionados executando o iOS 9.3 (versão mínima).
- **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 10.3 (versão mínima).
- **Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Aula bloqueará automaticamente os dispositivos do usuário a um aplicativo e bloqueará o dispositivo sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Associar automaticamente às classes do aplicativo Sala de Aula sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Sula associará automaticamente os usuários às classes, sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir AirPrint:** se essa restrição estiver definida como **Desativado**, os usuários não poderão imprimir com o AirPrint. A configuração padrão é **Ativado**. Quando essa restrição está **Ativada**, estas restrições extras são exibidas. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
    * **Permitir o armazenamento de credenciais do AirPrint em Chaves:** se essa restrição não estiver selecionada, o nome de usuário e a senha do AirPrint não serão armazenados em Chaves. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
    * **Permitir a descoberta de impressoras AirPrint usando iBeacons:** se essa restrição não estiver selecionada, a descoberta do iBeacon de impressoras AirPrint será desativada. Desabilitar a descoberta evita que sinalizadores falsos do AirPrint Bluetooth

© 1999-2019 Citrix Systems, Inc. All rights reserved.

causem phishing no tráfego da rede. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

    * **Permitir AirPrint apenas para destinos com certificados confiáveis:** se essa restrição for selecionada, os usuários poderão usar o AirPrint para imprimir apenas em destinos com certificados confiáveis. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

  - **Adicionar configurações de VPN:** se essa restrição estiver definida como **Desativado**, os usuários não poderão criar configurações de VPN. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
  - **Modificar as configurações do plano de celular:** se essa restrição estiver definida como **Desativado**, os usuários não poderão modificar as configurações do plano de celular. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
  - **Remover aplicativos do sistema:** se essa restrição estiver definida como **Desativado**, os usuários não poderão remover aplicativos de sistema de seus dispositivos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
  - **Configurando novos dispositivos próximos:** se essa restrição estiver definida como **Desativado**, os usuários não poderão configurar novos dispositivos próximos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

- **Rede - Permitir ações do iCloud**

  - **Documentos e dados do iCloud:** permitir que os usuários sincronizem documentos e dados com o iCloud (iOS 5.0 e versões posteriores). Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
  - **Backup do iCloud:** permitir que os usuários façam backup dos dispositivos deles no iCloud (iOS 5.0 e versões posteriores).
  - **Chaves do iCloud:** permitir que os usuários armazenem senhas, informações da rede WiFi e informações de cartão de crédito, entre outras, em Chaves do iCloud (iOS 7.0 e versões posteriores).
  - **Biblioteca de fotos na nuvem:** permitir que os usuários acessem a respectiva biblioteca de fotos do iCloud (iOS 9.0 e versões posteriores).

- **Segurança - Força**

  O padrão é restringir os recursos a seguir, o que significa que nenhum dos recursos de segurança é ativado.

  - **Backups criptografados:** forçar a criptografia dos backups no iCloud.
  - **Rastreamento de anúncios limitado:** bloquear o acompanhamento de anúncios direcionados (iOS 7.0 e versões posteriores).
  - **Código secreto no primeiro emparelhamento do AirPlay:** exigir que os dispositivos com-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

patíveis com o AirPlay sejam verificados com um código de uso único na tela antes que possam usar o AirPlay (iOS 7.0 e versões posteriores).
- **Apple Watch emparelhado para usar detecção de pulso:** exigir um Apple Watch emparelhado para usar a **Detecção de pulso** (iOS 8.2 e versões posteriores).
- **Compartilhamento de documentos gerenciados com o AirDrop:** o acesso ao AirDrop é uma opção supervisionada. Definir essa opção como **I** permite que os dispositivos supervisionados usem o AirDrop para compartilhar dados e mídia com dispositivos iOS próximos (iOS 9.0 e versões posteriores).

- **Segurança - Permitir**
  - **Aceitar certificados SSL não confiáveis:** permitir que os usuários aceitem certificados SSL não confiáveis de sites (iOS 5.0 e versões posteriores).
  - **Atualização automática de definições de segurança do certificado:** permitir que certificados confiáveis sejam atualizados automaticamente (iOS 7.0 e versões posteriores).
  - **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 não gerenciados (corporativos).
  - **Envio de informações 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 o dispositivo:** permitir que os usuários usem as impressões digitais deles para desbloquear os respectivos dispositivos (iOS 7.0 e versões posteriores).
  - **Notificações do Passbook quando o dispositivo está bloqueado:** permitir que notificações do Passbook apareçam na tela de bloqueio (iOS 6.0 e versões posteriores).
  - **Handoff:** permitir que os usuários transfiram as atividades de um dispositivo iOS para outro dispositivo iOS próximo (iOS 8.0 e versões posteriores).
  - **Sincronização do iCloud para aplicativos gerenciados:** permitir que os usuários sincronizem aplicativos gerenciados com o iCloud (iOS 8.0 e versões posteriores).
  - **Backup para livros da empresa:** permitir o backup de livros da empresa para o iCloud (iOS 8.0 e versões posteriores).
  - **Sincronização de notas e destaques para livros da empresa:** permitir que as notas e os destaques que os usuários adicionaram aos livros da empresa sejam sincronizados com o iCloud (iOS 8.0 e versões posteriores).
  - **Confiança de aplicativo empresarial:** permitir que aplicativos empresariais sejam confiáveis (iOS 9.0 e versões posteriores).
  - **Resultados de Internet no Spotlight:** permitir que o Spotlight mostre os resultados da pesquisa da Internet, bem como do dispositivo (iOS 8.0 e versões posteriores).
  - **Aplicativos não gerenciados leem contatos gerenciados:** Opcional. Disponível somente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver desativado (iOS 12 e posterior). Se esta política estiver ativada, os aplicativos não gerenciados poderão ler dados dos contatos das contas gerenciadas. O padrão é **Desativado**.

- **Aplicativos gerenciados gravam contatos não gerenciados:** Opcional. Se habilitado, permite que aplicativos gerenciados gravem contatos nos contatos de contas não gerenciadas (iOS 12 e posterior). Se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver habilitado, essa restrição não terá efeito. O padrão é **Desativado**.

- **Apenas configurações supervisionadas - Permitir**

  Estas configurações se aplicam somente a dispositivos supervisionados. Para ver 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.

  - **Apagar todo o conteúdo e configurações:** permitir que os usuários apaguem todo o conteúdo e as configurações dos dispositivos deles (iOS 8.0 e versões posteriores).
  - **Configuração de restrições:** permitir que os usuários configurem os controles dos pais nos dispositivos deles (iOS 8.0 e versões posteriores).
  - **Podcasts:** permitir que os usuários baixem e sincronizem podcasts (iOS 8.0 e versões posteriores).
  - **Instalação de perfis de configuração:** permitir que os usuários instalem um perfil de configuração diferente daquele implantado por você (iOS 6.0 e versões posteriores).
  - **Modificação de impressão digital:** permitir que os usuários alterem ou apaguem a impressão digital Touch ID deles (iOS 8.3 e versões posteriores).
  - **Instalação de aplicativos do dispositivo:** (iOS 9.0 e versões posteriores).
  - **Atalhos de teclado:** permitir que os usuários criem atalhos de teclado personalizados para palavras ou frases que usam com frequência (iOS 9.0 e versões posteriores).
  - **Apple Watch pareado:** permitir que os usuários emparelhem um Apple Watch com um dispositivo supervisionado (iOS 9.0 e versões posteriores).
  - **Modificação de código secreto:** permitir que os usuários alterem a senha em um dispositivo supervisionado (iOS 9.0 e versões posteriores).
  - **Modificação do nome do dispositivo:** permitir que os usuários alterem o nome do seu dispositivo.
  - **Modificação do papel de parede:** permitir que o usuário altere o papel de parede nos dispositivos deles (iOS 9.0 e versões posteriores).
  - **Download automático de aplicativos** (iOS 9.0 e versões posteriores).
  - **AirDrop:** permitir que os usuários compartilhem fotos, vídeos, sites, locais, entre outros, com dispositivos iOS próximos (iOS 7.0 e versões posteriores).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **iMessage:** permitir que os usuários enviem mensagens de texto sobre WiFi usando o iMessage (iOS 6.0 e versões posteriores).
- **Conteúdo gerado pelo usuário de Siri:** permitir que a Siri consulte conteúdo gerado pelo usuário na Web. Os consumidores, e não os jornalistas tradicionais; produzem conteúdo gerado pelo usuário. Por exemplo, o conteúdo encontrado no Twitter ou no Facebook é gerado pelo usuário (iOS 7.0 e versões posteriores).
- **iBooks:** permitir que os usuários usem o aplicativo iBooks (iOS 6.0 e versões posteriores).
- **Remoção de aplicativos:** permitir que usuários removam aplicativos dos dispositivos deles (iOS 7.0 e versões posteriores).
- **Game Center:** permitir que os usuários joguem jogos online usando o Game Center nos dispositivos deles (iOS 6.0 e versões posteriores).
  * **Adicionar amigos:** Permitir que os usuários enviem uma notificação a um amigo para jogar um jogo.
  * **Jogos multiplayer:** permitir que os usuários iniciem jogos multiplayer nos dispositivos deles.
- **Modificando configurações de conta:** permitir que os usuários modifiquem as configurações de conta do respectivo dispositivo (iOS 7.0 e versões posteriores).
- **Modificando configurações de dados celulares do aplicativo:** permitir que os usuários modifiquem a forma como os aplicativos usam dados celulares (iOS 7.0 e versões posteriores).
- **Modificando configurações de Encontrar Meus Amigos:** permitir que os usuários alterem as respectivas configurações de Encontrar Meus Amigos (disponível no iOS 7.0 e versões posteriores).
- **Emparelhamento com hosts não Configurator:** permitir que o administrador controle a quais dispositivos o dispositivo de um usuário pode ser emparelhado. Desativar essa configuração impede o emparelhamento, exceto com o host de supervisão que executa o Apple Configurator. Se nenhum certificado de host de supervisão estiver configurado, todo o emparelhamento será desativado (iOS 7.0 e versões posteriores).
- **Teclados intuitivos:** permitir que os dispositivos dos usuários usem teclados intuitivos para sugerir palavras conforme eles digitam (iOS 8.1.3 e versões posteriores). Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso a palavras sugeridas.
- **Teclado com correção automática:** permitir que os dispositivos dos usuários usem o teclado com correção automática (iOS 8.1.3 e versões posteriores). Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso à correção automática.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Teclado com corretor ortográfico:** permitir que os dispositivos dos usuários usem o corretor ortográfico enquanto digitam (iOS 8.1.3 e versões posteriores). Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso ao corretor ortográfico.
- **Pesquisa de definições:** permitir que os dispositivos dos usuários usem a pesquisa de definições durante a digitação (iOS 8.1.3 e versões posteriores). Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários consigam pesquisar definições conforme digitam.
- **ID de pacote único de aplicativos:** criar uma lista de aplicativos que têm permissão para manter o controle sobre o dispositivo e impedir a interação com os outros aplicativos ou funções.
  Para adicionar um aplicativo, clique em **Adicionar**, digite um **nome de aplicativo** e clique em **Salvar**. Repita esse processo para cada aplicativo que você desejar adicionar.
- **News:** permitir que os usuários usem o aplicativo News (iOS 9.0 e versões posteriores).
- **Serviço Apple Music:** permitir que os usuários usem o serviço Apple Music (iOS 9.3 e versões posteriores). Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássica.
- **iTunes Radio:** permitit que os usuários usem o iTunes Radio (iOS 9.3 e versões posteriores).
- **Modificação de notificações:** permitir que os usuários modifiquem configurações de notificação (iOS 9.3 e versões posteriores).
- **Uso de aplicativos restritos:** permitir que os usuários usem todos os aplicativos ou usem ou não aplicativos com base nos IDs de pacote que você fornecer (iOS 9.3 e versões posteriores). Aplica-se somente a dispositivos supervisionados.

  Depois de configurar a política de dispositivo de restrições para bloquear alguns aplicativos e, em seguida, implantar a política: se mais tarde você desejar permitir alguns ou todos os aplicativos, a alteração e implantação da política de dispositivo de restrições não alteram as restrições. Nesse caso, o iOS não aplica as alterações ao perfil de iOS. Para continuar, use a política de remoção de perfil para remover o perfil de iOS e, em seguida, implantar a política de dispositivo de restrições atualizada.

  Se você alterar essa configuração para **Permitir apenas alguns aplicativos:** antes de implantar essa política, informe os usuários de dispositivos registrados usando o Apple DEP para fazer login em suas contas Apple no Assistente de Instalação. Caso contrário, os usuários podem ter que desativar a autenticação de duas fatores em seus dispositivos para entrar em suas contas da Apple e acessar os aplicativos permitidos.

- **Modificação de submissão de diagnóstico:** permitir que os usuários modifiquem o envio de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

diagnóstico de aplicativo e configurações de análise no painel Diagnóstico e uso em Configurações (iOS 9.3.2 e versões posteriores).

- **Modificação de Bluetooth:** permitir que os usuários modifiquem configurações de Bluetooth (iOS 10.0 e versões posteriores).
- **Permitir ditado:** supervisionado somente. Se essa restrição é definida como **Desativado**, a entrada de ditado não é permitida. A configuração padrão é **Ativado**. Para iOS 10.3 e posterior.
- **Entrar somente em redes WiFi instaladas por uma política de WiFi:** opcional Apenas supervisionado. Se esta restrição estiver definida como **Ativado**, o dispositivo pode se juntar a redes Wi-Fi somente quando elas tiverem sido configuradas através de um perfil de configuração. O padrão é **Desativado**. Para iOS 10.3 e posterior.
- **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 10.3 (versão mínima).
- **Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Aula bloqueará automaticamente os dispositivos do usuário a um aplicativo e bloqueará o dispositivo sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Associar automaticamente às classes do aplicativo Sala de Aula sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Sula associará automaticamente os usuários às classes, sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir AirPrint:** se essa restrição estiver definida como **Desativado**, os usuários não poderão imprimir com o AirPrint. A configuração padrão é **Ativado**. Quando essa restrição está **Ativada**, estas restrições extras são exibidas. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
  - **Permitir o armazenamento de credenciais do AirPrint em Chaves:** se essa restrição não estiver selecionada, o nome de usuário e a senha do AirPrint não serão armazenados em Chaves. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
  - **Permitir a descoberta de impressoras AirPrint usando iBeacons:** se essa restrição não estiver selecionada, a descoberta do iBeacon de impressoras AirPrint será desativada. Isso evita que sinalizadores falsos do AirPrint Bluetooth causem phishing no tráfego da rede. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

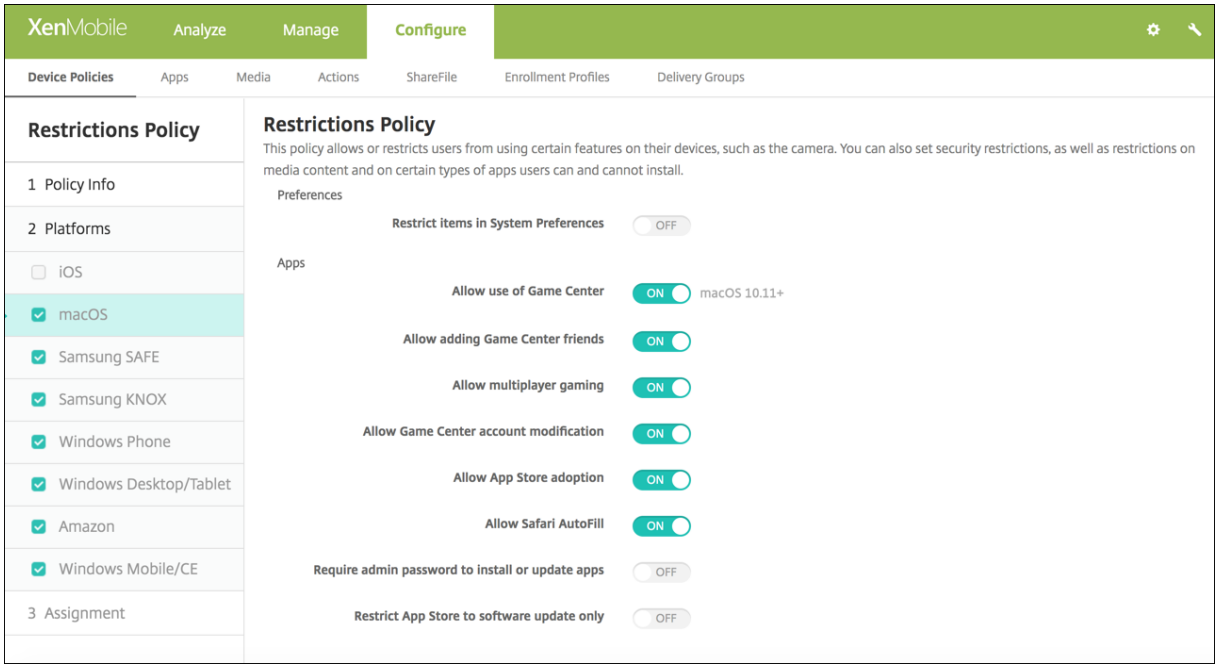
  - **Permitir AirPrint apenas para destinos com certificados confiáveis:** se essa restrição for selecionada, os usuários poderão usar o AirPrint para imprimir apenas em destinos com certificados confiáveis. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

- **Adicionar configurações de VPN:** se essa restrição estiver definida como **Desativado**, os usuários não poderão criar configurações de VPN. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Modificar as configurações do plano de celular:** se essa restrição estiver definida como **Desativado**, os usuários não poderão modificar as configurações do plano de celular. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Remover aplicativos do sistema:** se essa restrição estiver definida como **Desativado**, os usuários não poderão remover aplicativos de sistema de seus dispositivos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Configurando novos dispositivos próximos:** se essa restrição estiver definida como Desativado, os usuários não poderão configurar novos dispositivos próximos. A configuração padrão é Ativado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Segurança - Mostrar na tela de bloqueio**
  - **Centro de controle:** permitir acesso ao Centro de controle na tela de bloqueio, o que permite que os usuários modifiquem facilmente as configurações de Modo avião, Wi-Fi, Bluetooth, Modo não perturbe e Bloquear rotação (iOS 7.0 e versões posteriores).
  - **Notificação:** permitir notificações na tela de bloqueio (iOS 7.0 e versões posteriores).
  - **Exibição de hoje:** permitir a Exibição de Hoje, que agrega informações como a previsão do tempo e os itens de calendário do dia atual, na tela de bloqueio.
- **Conteúdo de mídia - Permitir**
  - **Música, podcasts e material do iTunes U explícitos:** permitir material explícito nos dispositivos dos usuários.
  - **Conteúdo sexual explícito em iBooks:** permitir que material explícito seja baixado do iBooks (iOS 6.0 e versões posteriores).
  - **Região de classificações:** definir a região da qual as classificações de controles dos pais são obtidas. Na lista, clique em um país para definir a região das classificações. O padrão é **Estados Unidos**.
  - **Filmes:** definir se filmes são permitidos nos dispositivos dos usuários. Se filmes forem permitidos, como opção, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Programas de TV:** definir se Programas de TV são permitidos nos dispositivos dos usuários. Se programas de TV forem permitidos, como opção, defina o nível de classificação dos 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:** definir se aplicativos são permitidos nos dispositivos dos usuários. Se aplicativos forem permitidos, como opção, 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 do macOS



- **Preferências**
  - **Restringir itens nas preferências do sistema:** permitir ou restringir o acesso do usuário às Preferências do Sistema. O padrão é **O**, que permite aos usuários acesso completo às Preferências do sistema. Se essa opção estiver ativada, defina as seguintes configurações.
    * **Painel de preferências do sistema:** selecionar se as configurações selecionadas são ativadas ou desativadas. O padrão é ativar todas as configurações, que são **I** por padrão.
      · Usuários e Grupos
      · Geral
      · Acessibilidade
      · App Store
      · Atualização de Software
      · Bluetooth

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- CDs e DVDs
- Data e Hora
- Área de Trabalho e Protetor de Tela
- Monitores
- Dock
- Economia de Energia
- Extensões
- FibreChannel
- iCloud
- Tinta
- Contas da Internet
- Teclado
- Idioma e Texto
- Mission Control
- Mouse
- Rede
- Notificações
- Controles dos Pais
- 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:** permitir que os usuários joguem jogos online usando o Game Center. O padrão é **On**.
  - **Permitir a adição de amigos do Game Center:** permitir que os usuários enviem uma notificação a um amigo para jogar um jogo. O padrão é **On**.
  - **Permitir jogos multiplayer:** permitir que os usuários iniciem jogos multiplayer. O padrão é **On**.
  - **Permitir modificação de conta do Game Center:** permitir que os usuários modifiquem as próprias configurações de conta do Game Center. O padrão é **On**.
  - **Permitir adoção da App Store:** permitir ou restringir a adoção de aplicativos que existiam

© 1999-2019 Citrix Systems, Inc. All rights reserved.

previamente no OS X pela App Store. O padrão é **On**.

- **Permitir preenchimento automático do Safari:** permitir que o Safari preencha automaticamente campos em sites com senhas, endereços e outras informações básicas que ele armazena. O padrão é **On**.
- **Exigir uma senha para instalar ou atualizar aplicativos:** exigir uma senha de administrador para instalar ou atualizar aplicativos. O padrão é **Off**, o que significa que nenhuma senha de administrador é necessária.
- **Restringir a App Store somente à atualização de software:** restringir a App Store somente a atualizações, o que desativa todas as guias na App Store, exceto as atualizações. O padrão é **Off**, que permite total acesso à App Store.
- **Restringir os aplicativos que podem ser abertos:** restringir ou permitir os aplicativos que os usuários podem usar. O padrão é O, o que permite que todos os aplicativos sejam usados. Se essa opção estiver ativada, defina as seguintes configurações:
  * **Aplicativos permitidos:** clique em **Adicionar**, digite o nome e o ID do pacote de um aplicativo com permissão para iniciar e clique em **Salvar**. Repita essa etapa para cada aplicativo com permissão para iniciar.
  * **Pastas não permitidas:** clique em **Adicionar**, digite o caminho de arquivo para uma pasta à qual você deseja restringir o acesso do usuário (por exemplo, /Applications/Utilities) e clique em **Salvar**. Repita essa etapa para todas as pastas que você não deseja que os usuários possam acessar.
  * **Pastas permitidas:** clique em **Adicionar**, digite o caminho de arquivo para uma pasta à qual você deseja conceder o acesso do usuário e clique em **Salvar**. Repita essa etapa para todas as pastas que você deseja que os usuários possam acessar.

- **Widgets**
  - **Permitir que apenas os seguintes widgets do painel sejam executados:** permitir ou restringir quais widgets do Painel, como Relógio ou Calculadora, os usuários têm permissão para executar. O padrão é **Off**, o que permite que os usuários executem todos os widgets. Se essa opção estiver ativada, defina a seguinte configuração:
    * **Widgets permitidos:** clique em **Adicionar**, digite o nome e o ID de um widget que tem permissão de execução e clique em **Salvar**. Repita essa etapa para cada widget que você deseja executar no Painel.
- **Mídia**
  - **Permitir AirDrop:** permitir que os usuários compartilhem fotos, vídeos, sites, locais e mais com dispositivos iOS próximos.
- **Compartilhamento**
  - **Ativar automaticamente novos serviços de compartilhamento:** selecione se os serviços de compartilhamento devem ser ativados automaticamente.
  - **Mail:** selecione se uma caixa de correio compartilhada é permitida.
  - **Facebook:** selecione se uma conta compartilhada do Facebook é permitida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Serviços de Vídeo - Flickr, Vimeo, Tudou e Youku:** selecione se os serviços de vídeo compartilhados são permitidos.
- **Adicionar ao Aperture:** selecione se a capacidade de adição compartilhada ao Aperture é permitida.
- **Sina Weibo:** selecione se uma conta compartilhada de microblogging do Sina Weibo é permitida.
- **Twitter:** selecione se uma conta compartilhada no Twitter é permitida.
- **Mensagens:** selecione se o acesso compartilhado a mensagens é permitido.
- **Adicionar ao iPhoto:** selecione se a capacidade de adição compartilhada ao iPhoto é permitida.
- **Adicionar à lista de leitura:** selecione se a capacidade de adição compartilhada à Lista de Leitura é permitida.
- **AirDrop:** selecione se uma conta compartilhada no AirDrop é permitida.

• **Funcionalidade**

- **Bloquear imagem da área de trabalho:** selecione se os usuários podem alterar a imagem da área de trabalho. O padrão é **Off**, o que significa que os usuários podem alterar a imagem da área de trabalho.
- **Permitir o uso da câmera:** selecione se os usuários podem usar a câmera nos Macs deles. O padrão é **Off**, o que significa que os usuários não podem usar a câmera.
- **Permitir Apple Music:** permitir que os usuários usem o serviço Apple Music (macOS 10.12 e versões posteriores). Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássica. Aplica-se somente a dispositivos supervisionados. O padrão é **Ativado**.
- **Permitir sugestões de Spotlight:** selecione se os usuários podem usar as Sugestões de Spotlight para pesquisar o respectivo Mac e para fornecer Sugestões de Spotlight da Internet, do iTunes e da App Store. O padrão é **Off**, o que impede que os usuários utilizem as Sugestões do Spotlight.
- **Permitir pesquisa:** selecione se os usuários podem pesquisar as definições de palavras usando o menu de contexto ou o menu de pesquisa do Spotlight. O padrão é O, o que impede que os usuários usem a Pesquisa nos respectivos Macs.
- **Permitir o uso de senha do iCloud para contas locais:** selecione se os usuários podem usar o respectivo ID Apple e senha do iCloud para fazer logon nos Macs deles. Ativar isso significa que o usuário usará apenas um ID e senha para *todas* as telas de login em seus Macs. O padrão é **On**, o que permite que os usuários usem o ID Apple e a senha do iCloud para acessar os Macs deles.
- **Permitir documentos e dados de iCloud:** selecione se os usuários têm permissão para acessar documentos e dados armazenados no iCloud nos Macs deles. O padrão é **Off**, o que impede que os usuários usem documentos e dados do iCloud nos Macs deles.
  * **Permitir área de trabalho e documentos iCloud:** (macOS 10.12.4 e posterior) Sele-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cionada por padrão.

- **Permitir sincronização de chaves do iCloud:** permitir a sincronização de chaves do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Mail do iCloud:** permitir que os usuários usem o iCloud Mail (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Contatos do iCloud:** permitir que os usuários usem os Contatos do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Calendários do iCloud:** permitir que os usuários usem os Calendários do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Lembretes do iCloud:** permitir que os usuários usem os Lembretes do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Favoritos do iCloud:** permitir que os usuários sincronizem com os Favoritos do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Notas do iCloud:** permitir que os usuários usem as Notas do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Fotos do iCloud:** se você alterar essa configuração para **Off**, as fotos não baixadas totalmente da biblioteca de fotos do iCloud serão removidas do armazenamento do dispositivo local (macOS 10.12 e posterior). O padrão é **On**.
- **Permitir desbloqueio automático:** para obter informações sobre essa opção e o Apple Watch, consulte https://www.imore.com/auto-unlock (macOS 10.12 e posterior). O padrão é **I**.
- **Permitir Touch ID para desbloquear Mac:** (macOS 10.12.4 e posterior). O padrão é **On**.

Configurações do Android

- **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles. Se o valor for **Off**, a câmera está desabilitada. O padrão é **Ativado**.

Configurações do Android for Work

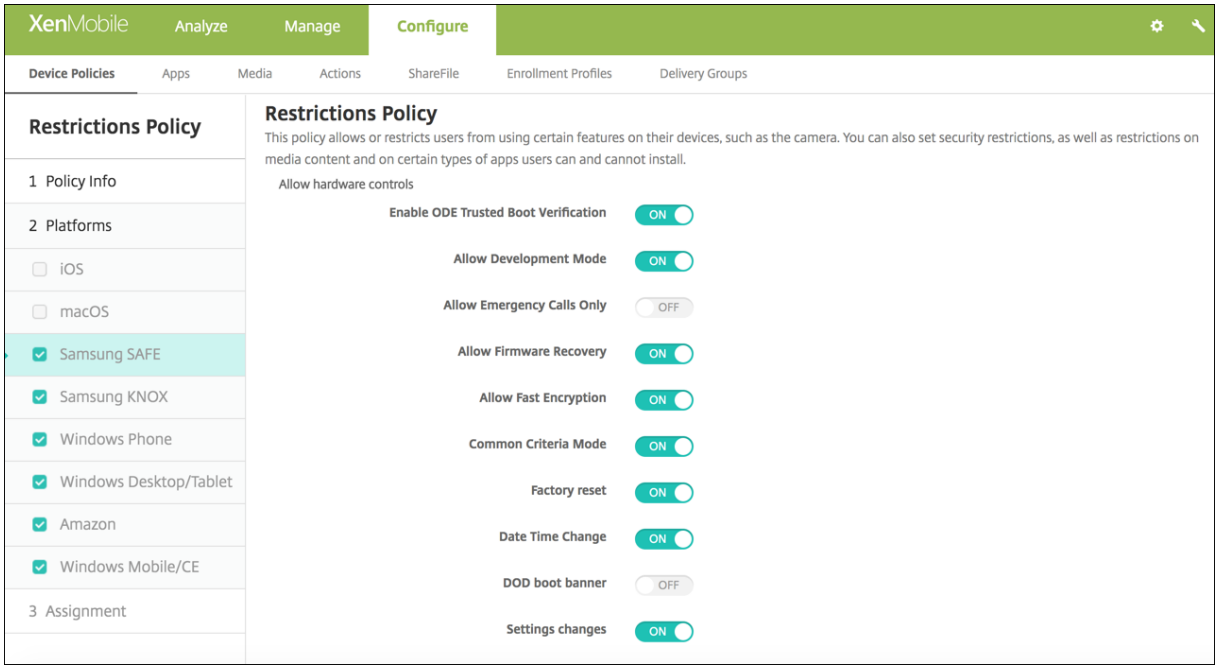
Por padrão, as configurações de Depuração de USB e Fontes desconhecidas são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

- **Depuração:** permite a depuração por USB (Android 5.0 e versões posteriores). O padrão é **Desativado**.
- **Transferência de arquivos:** permite a transferência de arquivos por USB (Android 5.0 e versões posteriores). O padrão é **Desativado**.
- **Tethering:** permite que os usuários configurem hotspots portáteis e vinculem dados (Android 5.0 e versões posteriores). O padrão é **Desativado.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Permitir aplicativos não Google Play:** permite a instalação de aplicativos de lojas diferentes da Google Play (Android 5.0 e posterior). O padrão é **Desativado**.
- **Permitir copiar e colar:** permite ou impede o uso da área de transferência para copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. Essa configuração está disponível em dispositivos que executam o Android 5.0 e posterior. O padrão é **Desativado**.
- **Ativar verificação de aplicativo:** permite que o sistema operacional verifique os aplicativos para detectar comportamentos mal-intencionados (Android 5.0 e posterior). O padrão é **Ativado**.
- **Permitir o controle do usuário das configurações do aplicativo:** permite que os usuários desinstalem aplicativos, desativem aplicativos, limpem o cache e os dados, forcem a interrupção de qualquer aplicativo e cancelem os padrões (Android 5.0 e posterior). O padrão é **Desativado**.
- **Permitir contatos do perfil de trabalho nos contatos do dispositivo:** mostra contatos do perfil gerenciado do Android for Work no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O padrão é **Desativado**.

Configurações do Samsung SAFE



Algumas opções estão disponíveis somente em APIs específicas de gerenciamento de dispositivo móvel da Samsung. Essas opções são marcadas com as informações relevantes da versão.

- **Permitir controles de hardware**
  - **Ativar verificação de inicialização confiável ODE:** usar a verificação de inicialização con-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

fiável ODE para estabelecer uma cadeia de confiança do carregador de inicialização com a imagem do sistema.
- **Permitir modo de desenvolvimento:** permitir que os usuários ativem as configurações do desenvolvedor nos dispositivos deles.
- **Permitir apenas chamadas de emergência:** permitir que os usuários ativem o modo Somente chamadas de emergência nos dispositivos deles.
- **Permitir recuperação de firmware:** permitir que os usuários recuperem o firmware nos dispositivos deles.
- **Permitir criptografia rápida:** permitir a criptografia somente do espaço de memória usado. Isso contrasta com a criptografia completa de disco, que criptografa todos os dados, incluindo configurações, dados de aplicativo, arquivos baixados e aplicativos, mídia e outros arquivos.
- **Modo Common Criteria:** colocar o dispositivo no Common Criteria Mode. A configuração Critérios Comuns impõe processos de segurança rigorosos.
- **Redefinição de fábrica:** permitir que os usuários realizem uma redefinição de fábrica nos dispositivos deles
- **Alteração de data e hora:** permitir que os usuários alterem a data e hora nos dispositivos deles.
- **Faixa de inicialização DOD:** exibir uma mensagem ou uma faixa de mensagem de notificação de uso do sistema aprovado para DoD quando os dispositivos dos usuários são reiniciados.
- **Alterações de configurações:** permitir que os usuários alterem as configurações nos dispositivos deles.
- **Backup:** permitir que os usuários façam backup de aplicativos e dados do sistema nos dispositivos deles.
- **Atualização por rede celular:** permitir que os dispositivos dos usuários recebam atualizações de software sem fio (MDM 3.0 e versões posteriores).
- **Dados de segundo plano:** permitir que os aplicativos sincronizem dados em segundo plano.
- **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
- **Área de transferência:** permitir que os usuários copiem dados para a área de transferência nos dispositivos deles.
    * **Compartilhamento de área de transferência:** permitir que os usuários compartilhem conteúdo da área de transferência entre os respectivos dispositivos e um computador (MDM 4.0 e versões posteriores).
- **Tecla Home:** permitir que os usuários usem a tecla Home nos dispositivos deles.
- **Microfone:** permitir que os usuários usem o microfone nos dispositivos deles.
- **Localização fictícia:** permitir que os usuários usem localizações de GPS fictícias.
- **NFC:** permitir que os usuários usem NFC (comunicação a curta distância) nos dispositivos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

deles (MDM 3.0 e versões posteriores).
  - **Desligar:** permitir que os usuários desliguem os dispositivos deles (MDM 3.0 e versões posteriores).
  - **Capturas de tela:** permitir que os usuários façam capturas de tela nos dispositivos deles.
  - **Cartão SD:** permitir que os usuários usem um cartão SD, se disponível, com os dispositivos deles.
  - **Discador de voz:** permitir que os usuários usem o comunicador de voz nos dispositivos deles (MDM 4.0 e versões posteriores).
  - **SBeam:** permitir que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e versões posteriores).
  - **SVoice:** permitir que os usuários usem o assistente pessoal inteligente e navegador de conhecimento nos dispositivos deles (MDM 4.0 e versões posteriores).
  - **Permitir vários usuários:** permite que vários usuários usem um dispositivo (MDM 4.0 e posterior). O padrão é **Desativado**.
- **Permitir aplicativos**
  - **Navegador:** permitir que os usuários usem o navegador da Web.
  - **Youtube:** permitir que os usuários acessem o YouTube.
  - **Google Play/Marketplace:** permitir que os usuários acessem o Google Play e o Google Apps Marketplace.
  - **Permitir aplicativos não Google Play:** permitir que os usuários baixem aplicativos de outros sites além do Google Play e do Google Apps Marketplace. Se **ativado**, um usuário pode usar as configurações de segurança em seu dispositivo para confiar em aplicativos de fontes desconhecidas.
  - **Parar aplicativo do sistema:** permitir que os usuários desativem os aplicativos de sistema pré-instalados (MDM 4.0 e versões posteriores).
  - **Desativar aplicativos:** se **Ativado**, impede que uma lista especificada de aplicativos sejam executados em dispositivos Samsung SAFE.
- **Rede**
  - **MMS de entrada:** permitir que os usuários recebam mensagens MMS.
  - **SMS de entrada:** permitir que os usuários recebam mensagens SMS.
  - **MMS de saída:** permitir que os usuários enviem mensagens MMS.
  - **SMS de saída:** permitir que os usuários enviem mensagens SMS.
  - **Perfis de rede virtual privada para adicionar usuários:**
  - **Bluetooth:** permitir que os usuários usem Bluetooth.
    * **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando a conexão Bluetooth.
  - **Wi-Fi:** permitir que usuários se conectem a redes Wi-Fi.
    * **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando a conexão Wi-Fi.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

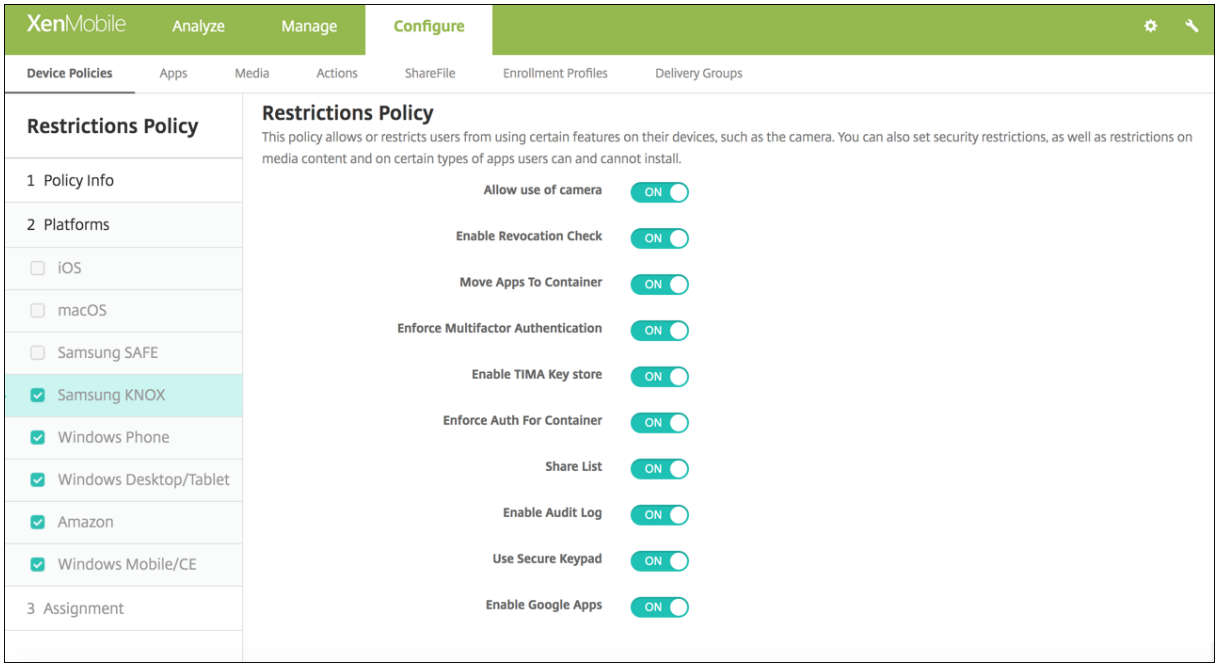
        * **Direto:** permitir que os usuários se conectem diretamente a outro dispositivo usando uma conexão Wi-Fi (MDM 4.0 e versões posteriores).
        * **Alteração de estado:** permitir que os aplicativos alterem o estado da conectividade Wi-Fi.
        * **Alterações de política de usuário:** permitir que os usuários alterem as políticas de Wi-Fi. Se essa opção não estiver selecionada, os usuários poderão alterar somente o nome do usuário e a senha do WiFi. Se essa opção estiver selecionada, os usuários poderão alterar as políticas de WiFi.
    - **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo.
    - **Dados celulares:** permitir que os usuários usem a conexão celular deles para dados.
    - **Permitir roaming:** permitir que os usuários usem dados celulares enquanto estiverem em roaming. O padrão é O, que desativa o roaming nos dispositivos dos usuários.
    - **Apenas conexões seguras:** permitir que os usuários usem somente conexões seguras (MDM 4.0 e versões posteriores).
    - **Android Beam:** permitir que os usuários enviem páginas da Web, imagens, vídeos ou outros conteúdos dos dispositivos deles para outro dispositivo usando NFC (MDM 4.0 e versões posteriores).
    - **Gravação de áudio:** permitir que os usuários gravem áudio usando os dispositivos deles (MDM 4.0 e versões posteriores).
    - **Gravação de vídeo:** permitir que os usuários gravem vídeo usando os dispositivos deles (MDM 4.0 e versões posteriores).
    - **Serviços de localização:** permitir que os usuários liguem o GPS nos dispositivos deles.
    - **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 esse recurso (MDM 4.0 e versões posteriores).
    - **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 esse recurso (MDM 4.0 e versões posteriores).
    - **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 esse recurso (MDM 4.0 e versões posteriores).
- **Permitir ações de USB** permitir a conexão USB entre os dispositivos dos usuários e um computador.
    - **Depuração:** permitir a depuração sobre USB.
    - **Armazenamento em host:** permitir que os dispositivos dos usuários ajam como o host USB quando um dispositivo USB é conectado aos dispositivos deles. Em seguida, os dispositivos dos usuários fornecem energia ao dispositivo USB.
    - **Armazenamento em massa:** permitir a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador sobre uma conexão USB.
    - **Reprodutor de mídia Kies:** permitir que os usuários usem a ferramenta Samsung Kies

© 1999-2019 Citrix Systems, Inc. All rights reserved.

para sincronizar arquivos entre os dispositivos deles e um computador.

- **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando uma conexão USB.

Configurações do Samsung KNOX



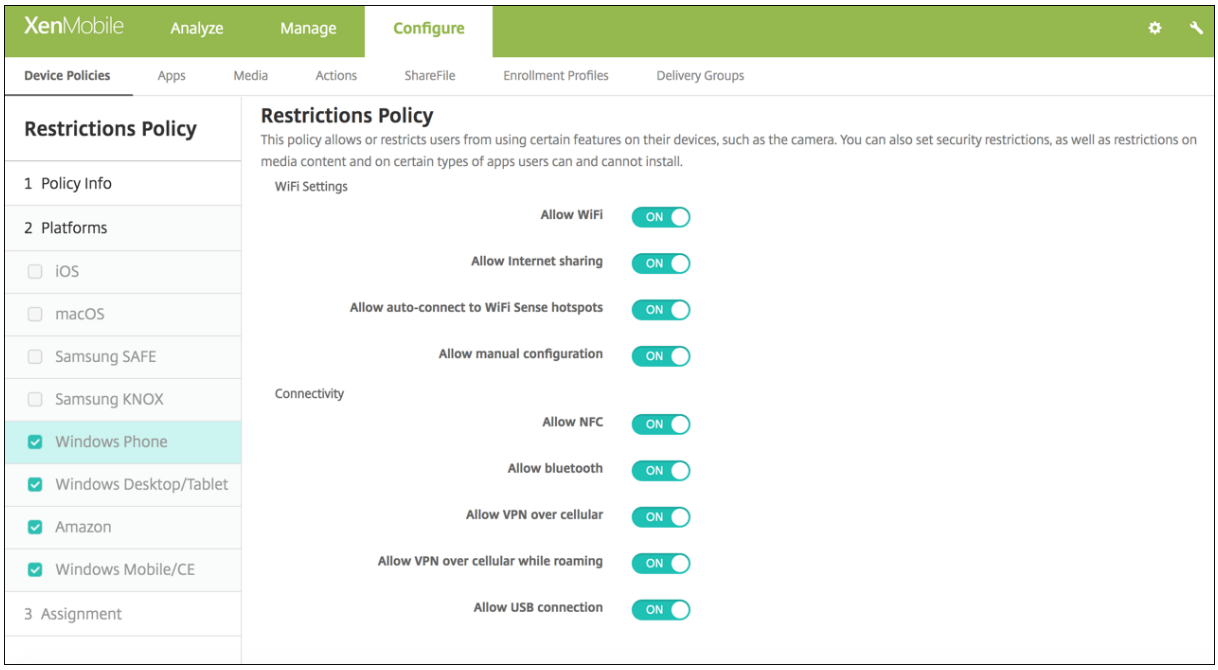
Essas opções estão disponíveis somente no Samsung KNOX Premium (KNOX 2.0).

- **Permitir o uso da câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
- **Permitir verificação de revogação:** ativar a verificação de certificados revogados.
- **Mover aplicativos para o contêiner:** permitir que os usuários movam aplicativos entre o contêiner KNOX e área pessoal nos dispositivos deles.
- **Impor a Autenticação Multifator:** os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir os dispositivos deles.
- **Ativar keystore TIMA:** o KeyStore TIMA fornece o armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Os pares de chaves e os certificados RSA são roteados para o provedor padrão de armazenamento de chaves para armazenamento.
- **Impor autenticação ao contêiner:** usar uma autenticação separada e diferente daquela usada para desbloquear o dispositivo abrir o contêiner KNOX.
- **Lista de Compartilhamento:** permitir que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via.
- **Ativar Log de Auditoria:** permitir a criação de logs de auditoria de eventos para análise forense de um dispositivo.
- **Usar Teclado Seguro:** forçar os usuários a usar um teclado seguro no contêiner KNOX.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Ativar Google Apps:** permitir que os usuários baixem aplicativos do Google Mobile Services para o contêiner KNOX.
- **Autenticação do navegador com cartão inteligente:** ativar a autenticação de navegador nos dispositivos equipados com um leitor de cartão inteligente.

Configurações do Windows Phone e do Windows Desktop/Tablet



- **Configurações de Wi-Fi**
  - **Permitir Wi-Fi:** permitir que um dispositivo se conecte a uma rede Wi-Fi. Windows Phone somente.
  - **Permitir compartilhamento de Internet:** permitir que um dispositivo compartilhe a respectiva conexão com a Internet com outros dispositivos, transformando-o em um ponto de acesso Wi-Fi.
  - **Permitir a conexão automática com pontos de acesso WiFi Sense:** permitir que um dispositivo se conecte automaticamente a pontos de acesso WiFi Sense. Os serviços de localização devem estar ativados para que essa opção funcione. Para obter mais informações sobre o WiFi Sense, consulte as Perguntas frequentes sobre o WiFi Sense do Windows Phone.
  - **Permitir configuração manual:** permitir que os usuários configurem manualmente as conexões Wi-Fi. Windows Phone somente.
- **Conectividade**
  - **Permitir NFC:** permitir que o dispositivo se comunique com uma marca NFC (Comunicação a Curta Distância) ou outro dispositivo de transmissão com tecnologia NFC. Windows Phone somente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Permitir bluetooth:** permitir que o dispositivo se conecte por Bluetooth. Windows Phone somente.
  - **Permitir VPN via celular:** permitir que o dispositivo se conecte sobre VPN a uma rede celular.
  - **Permitir VPN via celular em roaming:** permitir que o dispositivo se conecte sobre VPN quando ele fizer roaming entre redes celulares.
  - **Permitir conexão USB:** permitir que uma área de trabalho acesse o armazenamento de um dispositivo usando uma conexão USB. Windows Phone somente.
  - **Permitir roaming de dados celulares:** permitir que os usuários usem dados celulares enquanto estiverem em roaming.
- **Contas**
  - **Permitir conexão de conta da Microsoft:** permitir que o dispositivo use uma conta da Microsoft para autenticação e serviços de conexão não relacionados a email.
  - **Permitir email não Microsoft:** permitir que o usuário adicione contas de email que não são da Microsoft.
- **Pesquisar:** somente Windows Phone.
  - **Permitir que a pesquisa use localização:** permitir que as pesquisas usem o serviço de localização do dispositivo.
  - **Filtro de conteúdo adulto:** permitir conteúdo adulto. O padrão é **Desativado**, o que significa que o conteúdo adulto não é filtrado.
  - **Permitir que o Bing Vision armazene imagens:** permitir que o Bing Vision armazene as imagens capturadas ao realizar pesquisas do Bing Vision.
- **Sistema**
  - **Permitir cartão de armazenamento:** permitir que o dispositivo use um cartão de memória.
  - **Telemetria:** na lista, clique em uma opção para permitir ou restringir envio de informações de telemetria pelo dispositivo. O padrão é **Permitido**. Outras opções são **Não permitido** e **Permitido, exceto para a solicitação de dados secundários**.
  - **Permitir serviços de localização:** permitir os serviços de localização.
  - **Permitir visualização de compilações internas:** permitir que os usuários visualizem as compilações internas da Microsoft.
- **Câmera:** Windows Desktop/Tablet somente
  - **Permitir o uso da câmera:** permitir que os usuários usem a câmera do respectivo dispositivo.
- **Bluetooth:** Windows Desktop/Tablet somente
  - **Permitir modo detectável:** permitir que dispositivos Bluetooth encontrem o dispositivo local.
  - **Nome do dispositivo local:** um nome para o dispositivo local.
- **Segurança:** Windows Phone somente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

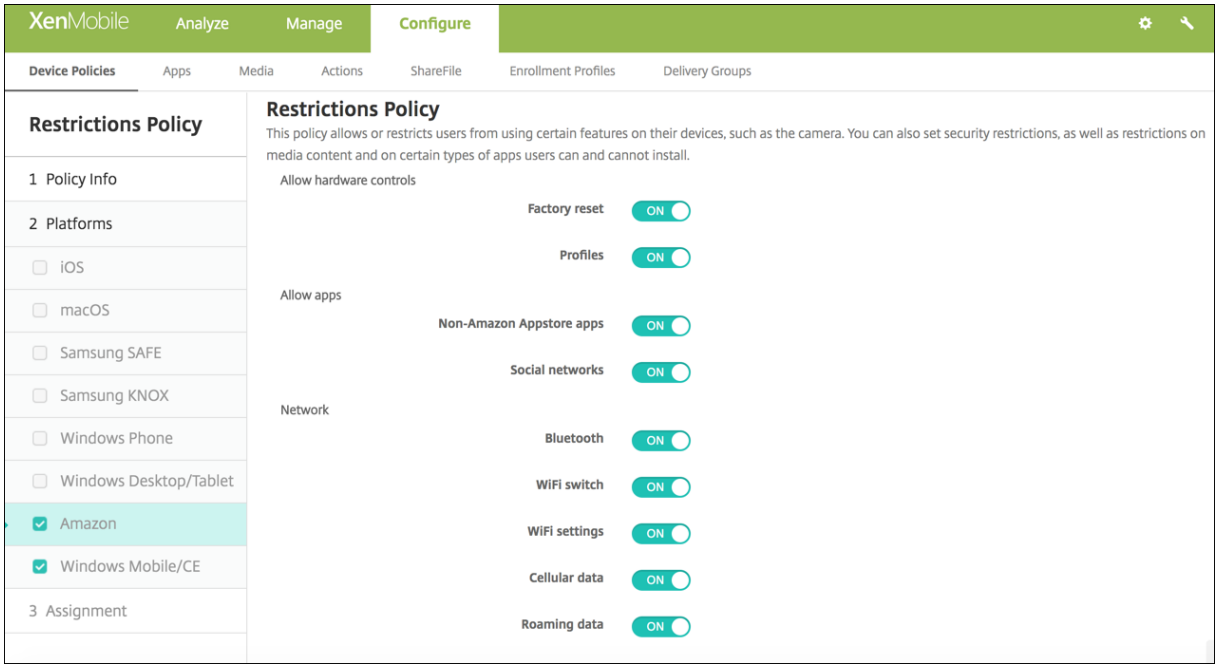
  - **Permitir a instalação manual do certificado raiz:** permitir que os usuários instalem manualmente um certificado raiz.
  - **Exigir criptografia do dispositivo:** exigir a criptografia do dispositivo. Observe que depois que a criptografia é ativada em um dispositivo, ela não pode ser desativada. O padrão é **Off**.
  - **Permitir copiar e colar:** permitir que os usuários copiem e colem dados nos dispositivos deles.
  - **Permitir captura de tela:** permitir que os usuários criem capturas de tela nos dispositivos deles.
  - **Permitir gravação de voz:** permitir que os usuários usem a gravação de voz nos dispositivos deles.
  - **Permitir Salvar como para arquivos do Office:** permitir que os usuários salvem arquivos do Office usando Salvar como.
  - **Permitir notificações do centro de ação:** permitir as notificações do Centro de Ação na tela de bloqueio do dispositivo.
  - **Permitir Cortana:** permitir que os usuários acessem o Cortana, o assistente pessoal inteligente e navegador de conhecimento.
  - **Permitir a sincronização de configurações de dispositivo:** permitir que os usuários sincronizem configurações entre dispositivos Windows Phone 8.1 quando estiverem em roaming.
- **Experiência:** Windows Desktop/Tablet somente
  - **Permitir Cortana:** permitir que os usuários acessem o Cortana, o assistente pessoal inteligente e navegador de conhecimento.
  - **Permitir descoberta do dispositivo:** permitir a descoberta da rede do dispositivo.
  - **Permitir registro manual no MDM:** permitir que os usuários manualmente cancelam o registro de dispositivos no XenMobile MDM.
  - **Permitir a sincronização de configurações de dispositivo:** permitir que os usuários sincronizem configurações entre dispositivos Windows 10 quando estiverem em roaming.
- **Bloqueio acima:** Windows Desktop/Tablet somente
  - **Permitir notificações toast:** permitir notificações na tela de bloqueio. Windows Desktop/Tablet somente
- **Aplicativos**
  - **Permitir o acesso à loja:** permitir que os usuários acessem a Microsoft Store. Windows Phone somente.
  - **Permitir desbloqueio do desenvolvedor:** permitir que os usuários registrem os dispositivos deles com a Microsoft e desenvolvam ou instalem aplicativos que não estão na loja de aplicativos do Windows Phone. Windows Phone somente.
  - **Permitir o acesso do navegador da Web:** permitir o Internet Explorer no dispositivo. Windows Phone somente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Permitir atualização automática da loja de aplicativos:** permitir que os aplicativos da loja de aplicativos sejam atualizados automaticamente. Windows Desktop/Tablet somente.
- **Privacidade:** Windows Desktop/Tablet somente
  - **Permitir personalização de entrada:** permitir que o serviço de personalização de entrada seja executado, para melhorar as entradas preditivas, como a caneta e o teclado de toque, com base no que o usuário digita.
- **Configurações:** Windows Desktop/Tablet somente.
  - **Permitir reprodução automática:** permitir que os usuários alterem as configurações de reprodução automática.
  - **Permitir o sensor de dados:** permitir que os usuários alterem as configurações do Sensor de Dados.
  - **Permitir data e hora:** permitir que os usuários alterem as configurações de data e hora.
  - **Permitir idioma:** permitir que os usuários alterem as configurações de idioma.
  - **Permitir energia e suspensão:** permitir que os usuários alterem as configurações de energia e suspensão.
  - **Permitir região:** permitir que os usuários alterem as configurações de região.
  - **Permitir opções de logon:** permitir que os usuários alterem as configurações de entrada de login.
  - **Permitir local de trabalho:** permitir que os usuários alterem as configurações do local de trabalho.
  - **Permitir a sua conta:** permitir que os usuários alterem as configurações da conta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

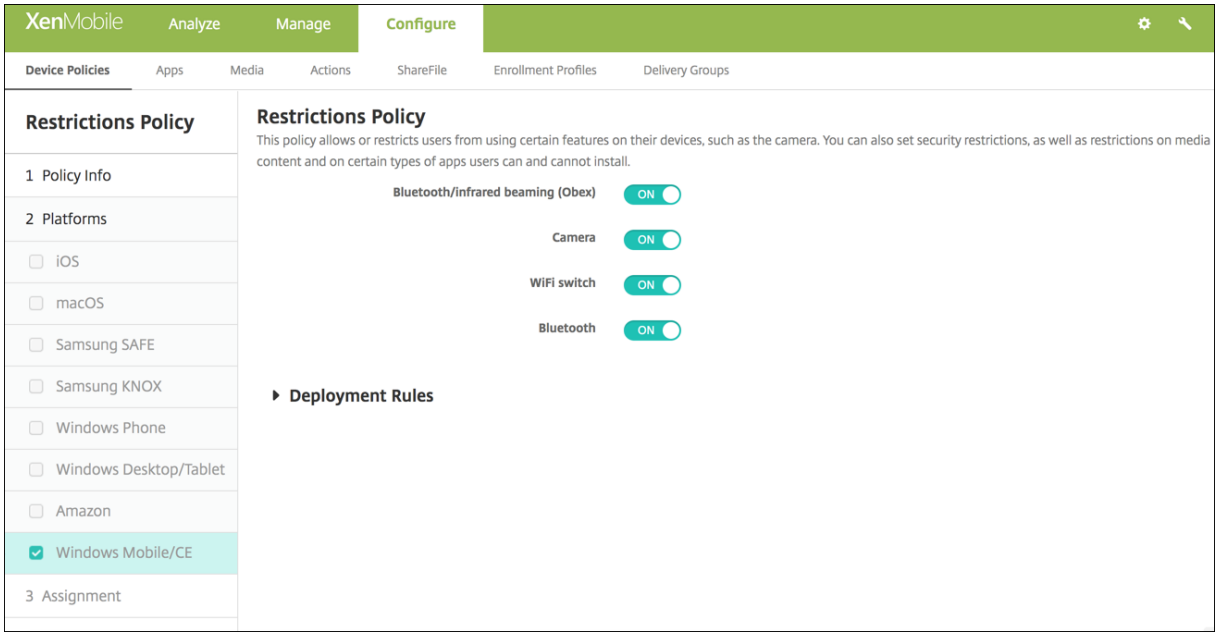
Configurações do Amazon



- **Permitir controles de hardware**
  - **Redefinição de fábrica:** permitir que os usuários realizem uma redefinição de fábrica nos dispositivos deles
  - **Perfis:** permitir que os usuários alterem o perfil de hardware nos dispositivos deles.
- **Permitir aplicativos**
  - **Aplicativos não Amazon Appstore:** permitir que os usuários instalem aplicativos não Amazon Appstore nos dispositivos deles.
  - **Redes sociais:** permitir que os usuários acessem redes sociais nos dispositivos deles.
- **Rede**
  - **Bluetooth:** permitir que os usuários usem Bluetooth.
  - **Comutador de WiFi:** permitir que os aplicativos alterem o estado da conectividade Wi-Fi.
  - **Configurações de WiFi:** permitir que os usuários alterem as configurações de Wi-Fi.
  - **Dados celulares:** permitir que os usuários usem a conexão celular deles para dados.
  - **Dados de roaming:** permitir que os usuários usem dados celulares enquanto estiverem em roaming.
  - **Serviços de localização:** permitir que os usuários usem GPS.
- **Ações USB:**
  - **Depuração:** permitir que os dispositivos dos usuários se conectem por meio de USB a um computador para depuração.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Mobile/CE



- **Bluetooth/feixe infravermelho (Obex):** ativar o OBEX (protocolo OBjectEXchange) sobre Bluetooth ou infravermelho para trocar dados entre dispositivos.
- **Câmera:** permitir a câmera nos dispositivos dos usuários.
- **Comutador de WiFi:** permitir que os usuários alternem entre redes Wi-Fi.
- **Bluetooth:** ativar Bluetooth nos dispositivos dos usuários.

Política de dispositivo em roaming

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para configurar se o roaming de voz e dados é permitido nos dispositivos iOS e Windows Mobile/CE dos usuários. Quando o roaming de voz está desativado, o roaming de dados é automaticamente desativado. Para o iOS, essa política está disponível somente nos dispositivos iOS 5.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Desativar roaming de voz:** selecione se o roaming de voz deve ser desativado. Quando essa opção está ativada, o roaming de dados é automaticamente desativado. O padrão é **O**, o que permite o roaming de voz.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Desativar roaming de dados:** selecione se o roaming de dados deve ser desativado. Essa opção estará disponível somente quando o roaming de voz estiver ativado. O padrão é **O**, o que permite o roaming de dados.

Configurações do Windows Mobile/CE

- **Em roaming**
  - **Usar somente conexão sob demanda:** o dispositivo se conectará ao XenMobile somente se os usuários dispararem manualmente a conexão nos dispositivos deles, ou se um aplicativo móvel solicitar uma conexão forçada (como uma solicitação de correio por push se o Exchange Server tiver sido definido de acordo). Observe que essa opção desativa temporariamente a política padrão de programação de conexão de dispositivo.
  - **Bloquear conexões celulares exceto as gerenciadas pelo XenMobile:** exceto pelo tráfego de dados oficialmente declarado em um túnel de aplicativo do XenMobile ou outras tarefas de gerenciamento de dispositivo do XenMobile, nenhum outro dado é enviado ou recebido pelo dispositivo. Por exemplo, essa opção desativa todas as conexões com a Internet por meio do navegador da Web do dispositivo.
  - **Bloquear todas as conexões celulares gerenciadas pelo XenMobile:** todos os dados de aplicativo em trânsito por meio de um túnel do XenMobile são bloqueados (incluindo o XenMobile Remote Support). O tráfego de dados relacionado ao gerenciamento de dispositivo puro, no entanto, não é bloqueado.
  - **Bloquear todas as conexões celulares com o XenMobile:** nesse caso, até que o dispositivo também seja reconectado por meio de USB, WiFi ou da respectiva rede celular da operadora de telefonia móvel padrão, não haverá nenhum tráfego em trânsito entre o dispositivo e o XenMobile.
- **Em roaming doméstico**
  - **Ignorar roaming doméstico:** nenhum dado é bloqueado enquanto os usuários estão em roaming doméstico.

Política de dispositivo de chave de licença MDM Samsung

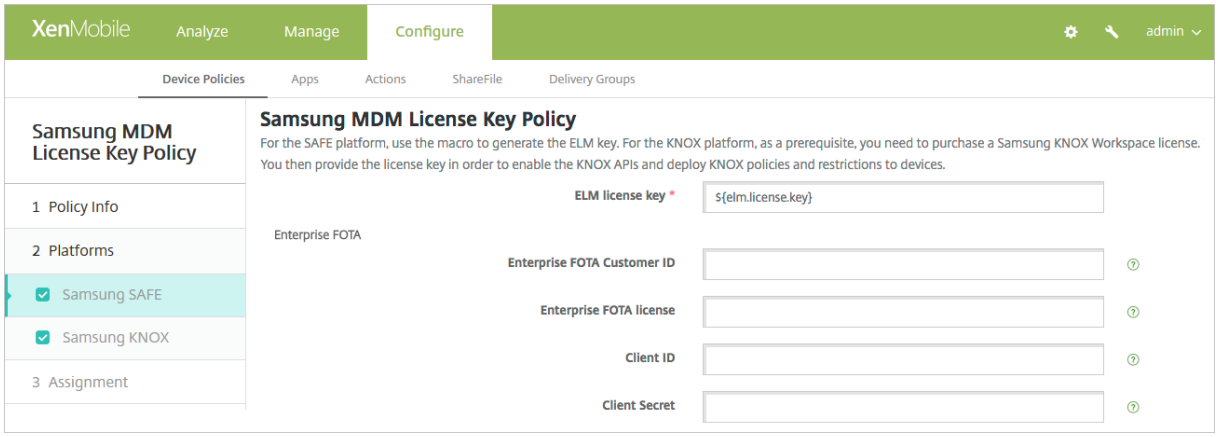
April 15, 2019

Especifica a chave interna do Enterprise License Management (ELM) Samsung que você precisa implantar em um dispositivo antes de implantar as políticas e restrições do SAFE. O XenMobile também suporta o serviço Enterprise Firmware Over-The-Air (E-FOTA) da Samsung. O XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung KNOX e as estende.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Samsung SAFE



- **Chave de licença ELM:** o XenMobile preenche previamente esse campo com a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite esta macro ${elm.license.key}

Definir as configurações do Samsung E-FOTA

Para configurar uma política E-FOTA:

1. Crie uma política de dispositivo chave de licença de MDM Samsung com as chaves e as informações de licença que você recebeu da Samsung. O XenMobile Server valida e registra as informações.

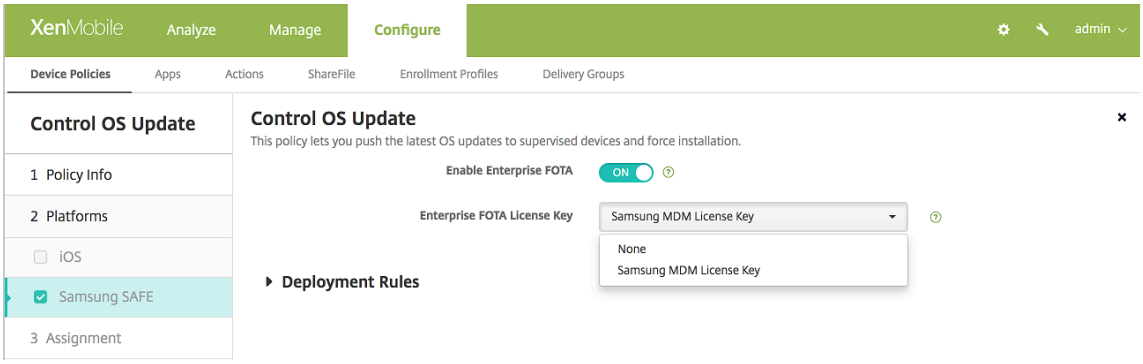
   Digite a **chave de licença ELM:** o XenMobile preenche previamente esse campo com a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite esta macro ${elm.license.key}

   Digite as seguintes informações fornecidas pela Samsung quando você adquiriu um pacote E-FOTA:

   - **ID de cliente do Enterprise FOTA**
   - **Licença do Enterprise FOTA**
   - **ID de cliente**
   - **Código secreto do cliente**

2. Crie uma política de dispositivo de controle de atualização do sistema operacional.

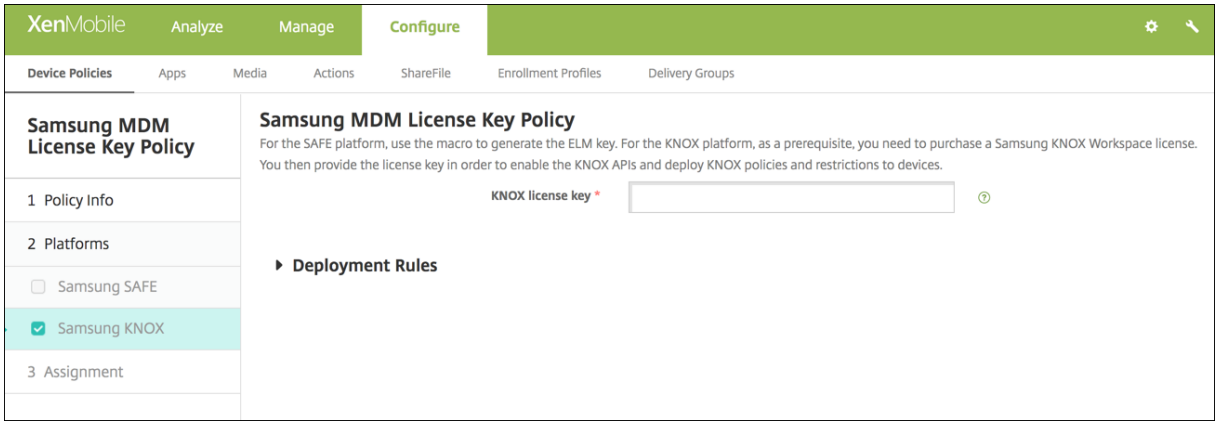
© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Ativar Enterprise FOTA:** defina como **Ativado**.
- **Chave de licença Enterprise FOTA:** selecione o nome da política de chave de licença Samsung MDM que você criou na etapa 1.

3. Implante a política de controle de atualização de sistema operacional no Secure Hub.

Configurações do Samsung KNOX



- **Chave de licença KNOX:** Digite a chave de licença KNOX que você obteve da Samsung.

Política de dispositivo de firewall do Samsung SAFE

April 15, 2019

Essa política permite que você defina as configurações de firewall dos dispositivos Samsung. Você insere os endereços IP, as portas e os nomes de host que desejar permitir ou bloquear. Você também pode definir o proxy e as configurações de redirecionamento do proxy.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Samsung SAFE

- **Permitir/Negar Hosts:** para cada host ao qual você desejar permitir ou negar acesso, clique em **Adicionar** e configure o seguinte:
  - **Nome do host/intervalo de IP:** o nome de host ou o intervalo de endereços IP do site que você desejar afetar.
  - **Porta/intervalo de portas:** a porta ou o intervalo de portas.
  - **Permitir/negar filtro de regra:** clique em **Lista branca** para permitir o acesso ou clique em **Lista negra** para negar o acesso ao site.
- **Configuração de redirecionamento:** para cada proxy que você desejar configurar, clique em **Adicionar** e configure o seguinte:
  - **Nome do host/intervalo de IP:** o nome de host ou o intervalo de endereços IP para o redirecionamento do proxy.
  - **Porta/intervalo de portas:** a porta ou o intervalo de portas para o redirecionamento do proxy.
  - **Proxy IP:** o endereço IP do proxy para o redirecionamento do proxy.
  - **Porta do proxy:** a porta do proxy para o redirecionamento do proxy.
- **Configuração de proxy**
  - **IP do proxy:** o endereço IP do servidor proxy.
  - **Porta:** a porta do servidor proxy.

Política de dispositivo do SCEP

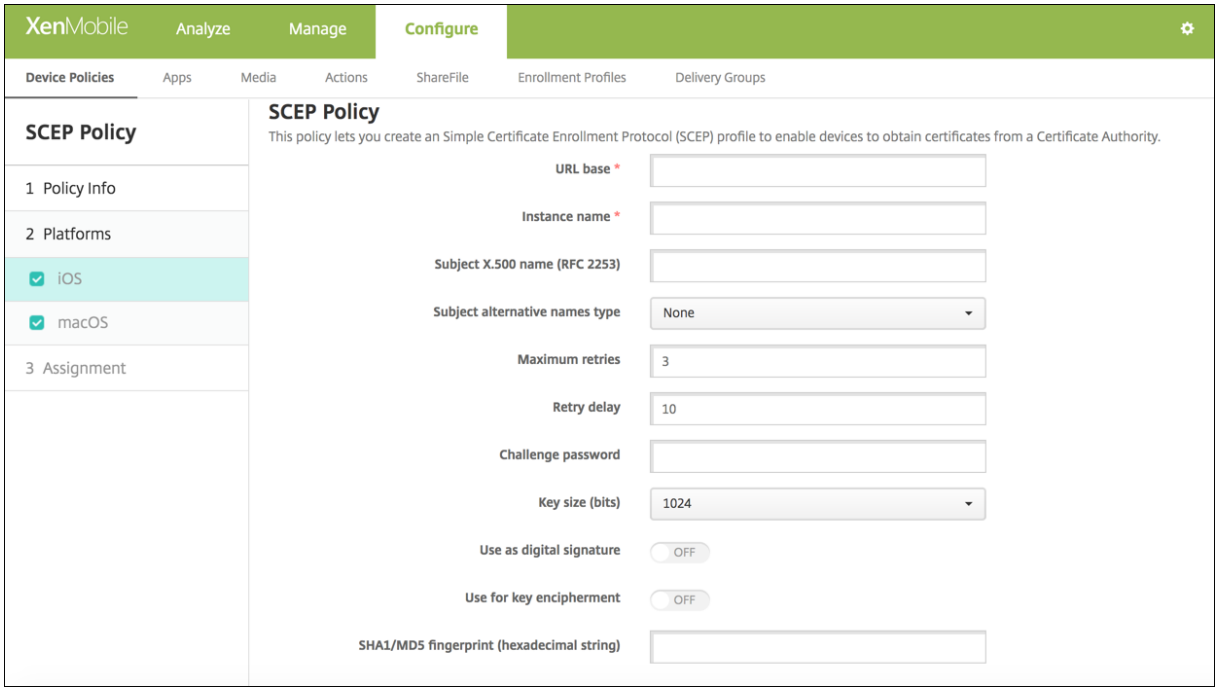
April 15, 2019

Esta política permite que você configure dispositivos iOS e macOS para recuperar um certificado usando o protocolo SCEP de um servidor SCEP externo. Se você desejar entregar um certificado ao dispositivo usando o SCEP de uma PKI que esteja conectada ao XenMobile, deverá criar uma entidade PKI e um provedor PKI no modo distribuído. Para obter detalhes, consulte Entidades PKI.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações de iOS

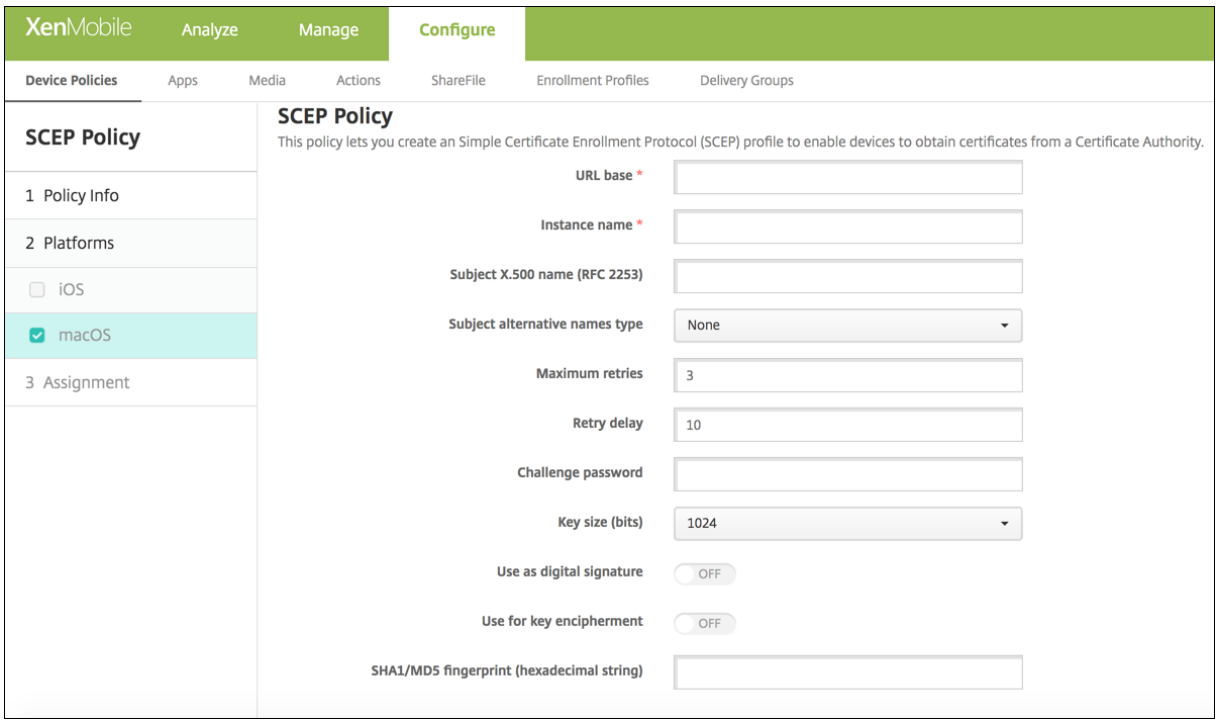


- **URL base:** digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas: sobre HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), portanto, pode ser seguro enviar a solicitação sem criptografia. No entanto, se a reutilização da senha de uso único for permitida, você deverá usar HTTPS para proteger a senha. Essa etapa é obrigatória.
- **Nome da instância:** digite qualquer cadeia de caracteres que o servidor SCEP reconheça. Por exemplo, isso poderia ser um nome de domínio, como exemplo.org. Se uma AC tiver vários certificados de AC, você poderá usar esse campo para distinguir o domínio necessário. Essa etapa é obrigatória.
- **Nome X.500 da entidade (RFC 2253):** digite a representação de um nome X.500, representado como uma matriz de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que seria convertido em: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]. Você pode representar OIDs como números pontilhados com atalhos para o país (C), a localidade (L), o estado (ST), a organização (O), a unidade organizacional (OU) e o nome comum (CN).
- **Tipo de nomes alternativos de assunto:** na lista, clique em um tipo de nome alternativo. A política de SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela autoridade de certificação para a emissão de um certificado. Você pode especificar **Nenhum**, nome **RFC 822**, **nome DNS** ou **URI**.
- **Máximo de repetições:** digite o número de vezes que um dispositivo deve tentar novamente quando o servidor SCEP enviar uma resposta PENDING. O padrão é **3**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Atraso entre cada repetição:** digite o número de segundos de espera entre tentativas subsequentes. A primeira nova tentativa é realizada sem atraso. O padrão é **10**.
- **Senha do desafio:** insira um segredo pré-compartilhado.
- **Tamanho da chave (bits):** na lista, clique no tamanho da chave em bits, **1024** ou **2048**. O padrão é **1024**.
- **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 para verificar se um certificado foi emitido por uma AC, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de utilizar a chave pública para descriptografar o hash.
- **Usar para codificação de chave:** especifique se você deseja que o certificado seja usado para codificação de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se uma parte dos dados foi criptografada usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para codificação de chave. Em caso negativo, a operação falha.
- **Impressão digital SHA1/MD5 (cadeia de caracteres hexadecimal):** se sua AC usar HTTP, use esse campo para fornecer a impressão digital do certificado de AC que o dispositivo usa para confirmar a autenticidade da resposta da AC durante o registro. Você pode inserir uma impressão digital SHA1 ou MD5, ou selecionar um certificado para importar a respectiva assinatura.

Configurações do macOS



© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **URL base:** digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas: sobre HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), portanto, pode ser seguro enviar a solicitação sem criptografia. No entanto, se a reutilização da senha de uso único for permitida, você deverá usar HTTPS para proteger a senha. Essa etapa é obrigatória.
- **Nome da instância:** digite qualquer cadeia de caracteres que o servidor SCEP reconheça. Por exemplo, isso poderia ser um nome de domínio, como exemplo.org. Se uma AC tiver vários certificados de AC, você poderá usar esse campo para distinguir o domínio necessário. Essa etapa é obrigatória.
- **Nome X.500 da entidade (RFC 2253):** digite a representação de um nome X.500, representado como uma matriz de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que seria convertido em: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]. Você pode representar OIDs como números pontilhados com atalhos para o país (C), a localidade (L), o estado (ST), a organização (O), a unidade organizacional (OU) e o nome comum (CN).
- **Tipo de nomes alternativos de assunto:** na lista, clique em um tipo de nome alternativo. A política de SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela autoridade de certificação para a emissão de um certificado. Você pode especificar **Nenhum**, nome **RFC 822**, **nome DNS** ou **URI**.
- **Máximo de repetições:** digite o número de vezes que um dispositivo deve tentar novamente quando o servidor SCEP enviar uma resposta PENDING. O padrão é **3**.
- **Atraso entre cada repetição:** digite o número de segundos de espera entre tentativas subsequentes. A primeira nova tentativa é realizada sem atraso. O padrão é **10**.
- **Senha do desafio:** digite um segredo pré-compartilhado.
- **Tamanho da chave (bits):** na lista, clique no tamanho da chave em bits, **1024** ou **2048**. O padrão é **1024**.
- **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 para verificar se um certificado foi emitido por uma AC, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de utilizar a chave pública para descriptografar o hash.
- **Usar para codificação de chave:** especifique se você deseja que o certificado seja usado para codificação de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se uma parte dos dados foi criptografada usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para codificação de chave. Em caso negativo, a operação falha.
- **Impressão digital SHA1/MD5 (cadeia de caracteres hexadecimal):** se sua AC usar HTTP, use esse campo para fornecer a impressão digital do certificado de AC que o dispositivo usa para confirmar a autenticidade da resposta da AC durante o registro. Você pode inserir uma im-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pressão digital SHA1 ou MD5, ou selecionar um certificado para importar a respectiva assinatura.

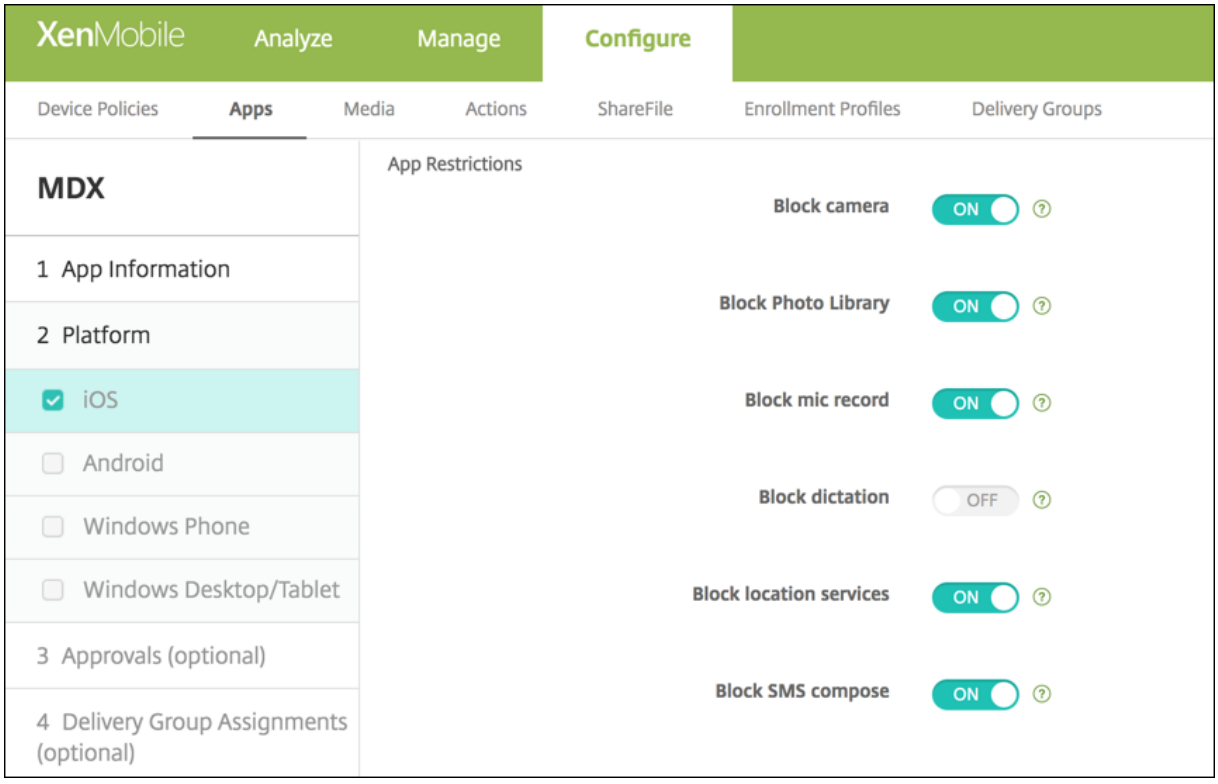
Siri e políticas de ditado

April 15, 2019

Quando os usuários perguntam algo à Siri ou ditam texto em dispositivos iOS gerenciados, a Apple coleta de dados de voz para fins de melhorar a Siri. Os dados de voz a passam por serviços da Apple baseados na nuvem e, portanto, existem fora do contêiner seguro XenMobile. O texto que resultada do ditado, no entanto, permanece no contêiner.

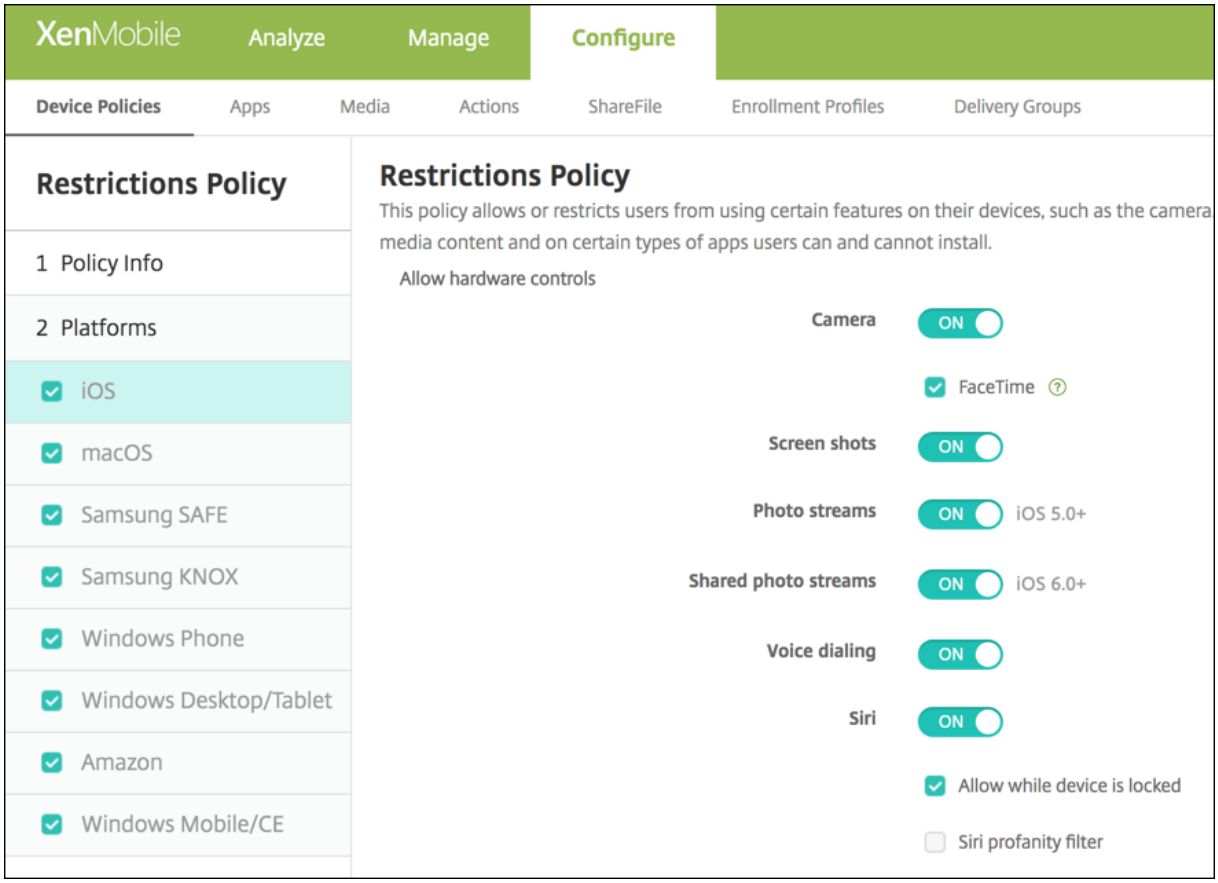
O XenMobile permite que você bloqueie a Siri e os serviços de ditado de acordo com o que determinam suas necessidades de segurança.

Em implantações de MAM, a política **Bloquear ditado** para cada aplicativo é **ativada** por padrão, o que desativa o microfone do dispositivo. Defina como **Desativado** se você quiser permitir o ditado. Você pode encontrar a política no console 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 da Siri em **Configurar > Políticas de dispositivo**. O uso do Siri é permitido por padrão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Alguns poucos pontos para levar em consideração ao decidir se deseja permitir a Siri e ditado:

- De acordo com as informações que a Apple divulgou, a Apple mantém dados da Siri e de clip de voz por até dois anos. É atribuído um número aleatório a esses para representar o usuário e os arquivos de voz arquivos são associados a este número aleatório. Para obter mais informações, consulte este artigo da Wired, Apple reveals how long Siri keeps your data.
- Você pode revisar a política de privacidade da Apple acessando **Configurações > Geral > Teclados** em qualquer dispositivo iOS e tocando no link em **Ativar ditado**.

Políticas de dispositivo de conta SSO

April 15, 2019

Crie contas de logon único (SSO) no XenMobile para permitir que os usuários façam logon somente uma vez para acessar o XenMobile e seus recursos internos da empresa de diversos aplicativos. Os usuários não precisam armazenar nenhuma credencial no dispositivo. As credenciais do usuário empresarial da conta SSO são usadas entre aplicativos, incluindo os aplicativos da App Store. Essa política foi desenvolvida para funcionar com um back-end de autenticação Kerberos.

Essa política se aplica ao iOS 7.0 e versões posteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Nome da conta:** insira o nome de conta SSO Kerberos que é exibida nos dispositivos dos usuários. Este campo é obrigatório.
- **Nome principal Kerberos:** insira o nome principal Kerberos. Este campo é obrigatório.
- **Credencial de identidade (keystore ou credencial PKI):** na lista, clique em uma credencial de identidade opcional que pode ser usada para renovar a credencial do Kerberos sem a interação do usuário.
- **Realm Kerberos:** insira o realm Kerberos dessa política. Geralmente, ele é o seu nome de domínio em letras maiúsculas (por exemplo, EXEMPLO.COM). Este campo é obrigatório.
- **URLs permitidas:** para cada URL para a qual você deseja exigir o SSO, clique em **Adicionar** e faça o seguinte:
  - **URL Permitida:** insira uma URL para a qual você deseja exigir o SSO quando um usuário visitar a URL 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 realizar o SSO fornecendo o token Kerberos que o Kerberos pode ter em cache no dispositivo de um login anterior no Kerberos. A correspondência precisa ser exata na parte do host do URL. Por exemplo, `https://shopping.apple.com` é válido, mas `https://*.apple.com` não é.
    Além disso, se o Kerberos não estiver ativado com base no host correspondente, a URL ainda retornará para uma chamada HTTP padrão. Isso pode significar quase qualquer coisa, inclusive um desafio de senha padrão ou um erro HTTP, se a URL estiver configurada para SSO somente usando o Kerberos.
  - Clique em **Adicionar** para adicionar a URL ou em **Cancelar** para cancelar a adição da URL.
- **Identificadores de aplicativo:** para cada aplicativo que tem permissão para usar esse login, clique em **Adicionar** e faça o seguinte:
  - **Identificador de aplicativo:** insira um identificador de aplicativo para um aplicativo que tem permissão para usar esse login. Se você não adicionar nenhum identificador de aplicativo, esse login corresponderá a **todos** os identificadores de aplicativo.
  - Clique em **Adicionar** para adicionar o identificador de aplicativo ou em **Cancelar** para cancelar a adição do identificador de aplicativo.

Política de dispositivo de criptografia de armazenamento

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Crie políticas de dispositivo de criptografia de armazenamento no XenMobile para criptografar o armazenamento interno e externo, e, dependendo do dispositivo, para impedir que os usuários usem um cartão de armazenamento nos respectivos dispositivos.

Você pode criar políticas para dispositivos Samsung SAFE, Windows Phone e Android Sony. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

Para dispositivos Samsung SAFE, certifique-se de que os seguintes requisitos sejam atendidos antes de configurar esta política:

- Defina a opção Bloqueio de tela nos dispositivos do usuário.
- Conecte dispositivos de usuários e carregue-os pelo menos a 80%.
- Certifique-se de que os dispositivos exijam uma senha contendo números e letras ou símbolos.

Definir as configurações do Samsung SAFE

- **Criptografar armazenamento interno:** selecione se o armazenamento interno deve ser criptografado nos dispositivos dos usuários. O armazenamento interno inclui a memória e o armazenamento interno do dispositivo. O padrão é **On**.
- **Criptografar armazenamento externo:** selecione se o armazenamento externo deve ser criptografado nos dispositivos dos usuários. O padrão é **On**.

Configurações do Windows Phone

- **Exigir criptografia do dispositivo:** selecione se os dispositivos dos usuários devem ser criptografados. O padrão é **Off**.
- **Desativar cartão de armazenamento:** selecione se os usuários devem ser impedidos de usar um cartão de memória nos respectivos dispositivos. O padrão é **Off**.

Definir as configurações do Android Sony

- **Criptografar armazenamento externo:** selecione se o armazenamento externo deve ser criptografado nos dispositivos dos usuários. O dispositivo deve exigir uma senha que contenha números e letras ou símbolos. O padrão é **On**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de loja

April 15, 2019

Você pode criar uma política no XenMobile para especificar se os dispositivos iOS, Android ou Tablet Windows exibem um clipe Web do XenMobile Store na tela inicial dos dispositivos.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações da plataforma

Para cada plataforma que você configurar, selecione se o clipe Web da XenMobile Store aparece nos dispositivos dos usuários. O padrão é **On**.

Política de dispositivo de Calendários inscritos

April 15, 2019

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar um calendário inscrito à lista de calendários nos dispositivos iOS. A lista de calendários públicos nos quais você pode se inscrever está disponível em www.apple.com/downloads/macosx/calendars.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisito

Você deve estar inscrito em um calendário antes de poder adicioná-lo à lista de calendários inscritos nos dispositivos do usuário.

Configurações de iOS

- **Descrição:** insira uma descrição do calendário. Este campo é obrigatório.
- **URL:** insira a URL do calendário. Você pode inserir um URL `webcal://` ou um link `https://` em um arquivo do iCalendar (.ics). Este campo é obrigatório.
- **Nome de usuário:** insira o nome de usuário de login. Este campo é obrigatório.
- **Senha:** insira uma senha de usuário opcional.
- **Usar SSL:** selecione se deseja usar uma conexão Secure Socket Layer no calendário. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Política de dispositivo dos termos e condições

April 15, 2019

Crie as políticas de dispositivo dos termos e condições no XenMobile quando desejar que os usuários aceitam as políticas específicas da empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos no XenMobile, eles visualizam os termos e condições e devem aceitá-los para registrar os dispositivos. Não aceitar os termos e condições cancela o processo de registro.

Você pode criar políticas diferentes para os termos e condições em idiomas diferentes, caso sua empresa tenha usuários internacionais e você deseje 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. Em dispositivos iOS e Android, você deve fornecer arquivos PDF. Em dispositivos Windows, você deve fornecer os arquivos de texto (.txt) e os arquivos de imagem complementares.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do iOS e do Android

- **Arquivo a ser importado:** selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Termos e condições padrão:** selecione se este arquivo é o documento padrão para os usuários que são membros de vários grupos com termos e condições diferentes. O padrão é **Off**.

Configurações do Windows Phone e do Tablet Windows

- **Arquivo a ser importado:** selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Imagem:** selecione o arquivo de imagem a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Termos e condições padrão:** selecione se este arquivo é o documento padrão para os usuários que são membros de vários grupos com termos e condições diferentes. O padrão é **Off**.

Política de dispositivo do VPN

April 15, 2019

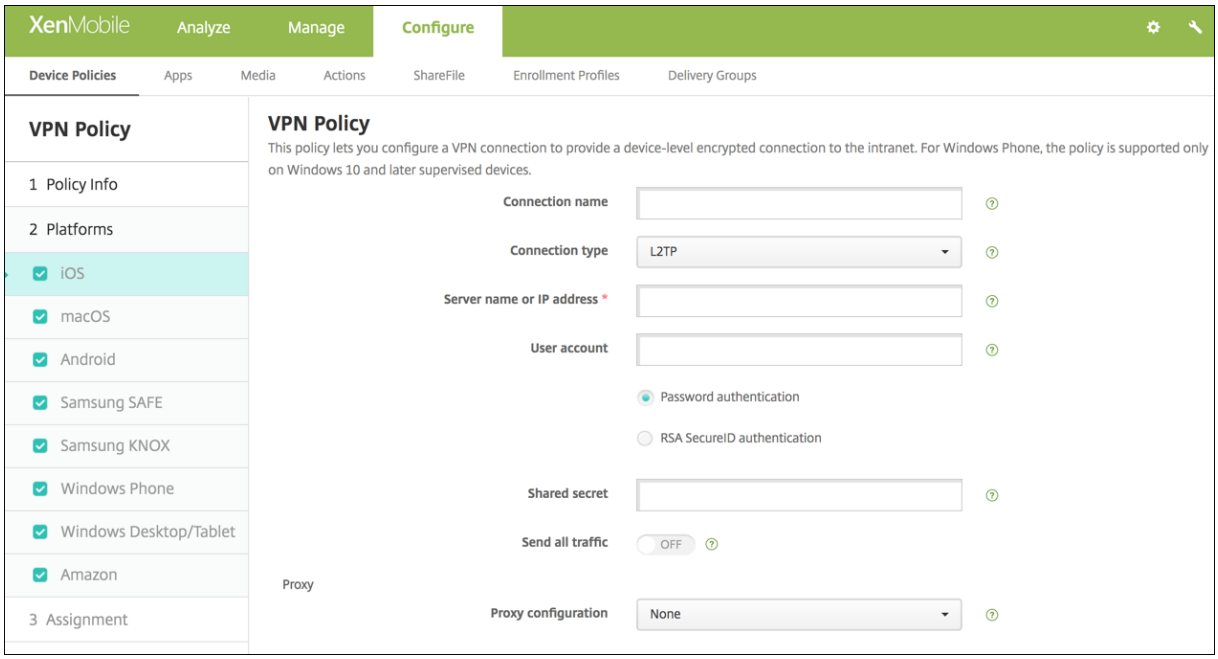
Você pode adicionar uma política de dispositivo no XenMobile para definir as configurações de rede virtual privada (VPN) que permitem que os dispositivos dos usuários se conectem com segurança a

© 1999-2019 Citrix Systems, Inc. All rights reserved.

recursos corporativos. Você pode configurar a política de VPN para as seguintes plataformas. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS



> Importante:
>
> Para se preparar para atualizações de dispositivos para o iOS 12: o tipo de conexão Citrix VPN na política de dispositivos VPN para iOS não suporta o iOS 12. Exclua sua política de dispositivo VPN e crie uma nova 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 10.9, durante o registro do usuário.

- **Nome da conexão:** digite um nome para a conexão.
- **Tipo de conexão:** na lista, clique no protocolo a ser usado para esta conexão. O padrão é **L2TP**.
  - **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
  - **PPTP:** Encapsulamento Ponto a Ponto.
  - **IPSec:** sua conexão VPN corporativa.
  - **Cisco Legacy AnyConnect:** este tipo de conexão requer que o cliente VPN Cisco Legacy AnyConnect esteja instalado no dispositivo do usuário. A Cisco está desativando o cliente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cisco Legacy AnyConnect que foi baseado em uma estrutura VPN agora obsoleta. Para mais informações, consulte o artigo de suporte do XenMobile https://support.citrix.com/article/CTX227708.

Para usar o cliente Cisco AnyConnect atual, use um **Tipo de conexão** de **SSL personalizado**. Para ver as configurações necessárias, consulte “Configurar o protocolo SSL personalizado” nesta seção.

- **Juniper SSL:** cliente VPN Juniper Networks SSL.
- **F5 SSL:** cliente VPN F5 Networks SSL.
- **SonicWALL Mobile Connect:** cliente VPN unificado Dell para iOS.
- **Ariba VIA:** cliente Ariba Networks Virtual Internet Access.
- **IKEv2 (somente iOS):** Internet Key Exchange versão 2 somente para iOS.
- **Citrix VPN:** cliente Citrix VPN para iOS.
- **SSL personalizado:** protocolo SSL personalizado. Esse tipo de conexão é necessário para o cliente Cisco AnyConnect que possui um ID de pacote do **com.cisco.anyconnect**. Especifique um **nome de conexão** do **Cisco AnyConnect**.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione **Autenticação por senha** ou **Autenticação RSA SecureID**.
- **Segredo compartilhado:** digite a chave secreta compartilhada do IPSec.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo PPTP para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione **Autenticação por senha** ou **Autenticação RSA SecureID**.
- **Nível de criptografia:** na lista, clique em um nível de criptografia. O padrão é **Nenhum**.
  - **Nenhum:** não use criptografia.
  - **Automático:** use o nível de criptografia mais forte compatível com o servidor.
  - **Máximo (128 bits):** use sempre criptografia de 128 bits.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o protocolo IPSec para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
- Se você ativar a opção **Segredo compartilhado**, defina as seguintes configurações:
  - **Nome do grupo:** digite um nome de grupo opcional.
  - **Segredo compartilhado:** digite uma chave secreta compartilhada opcional.
  - **Usar autenticação híbrida:** selecione se a autenticação híbrida deve ser usada. Com a autenticação híbrida, o primeiro servidor autentica a si mesmo no cliente e, em seguida, o cliente autentica a si mesmo no servidor. O padrão é **Off**.
  - **Solicitar senha:** selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **Off**.
- Se você ativar a opção **Certificado**, configure as seguintes definições:
  - **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
  - **Solicitar PIN ao conectar:** selecione se os usuários serão obrigados a inserir o respectivo PIN quando se conectarem à rede. O padrão é **Off**.
  - **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível apenas no iOS 9.0 e versões posteriores.
- **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
- **Domínios Safari:** clique em **Adicionar** para adicionar um nome de domínio do Safari.

Configurar o protocolo Cisco Legacy AnyConnect para iOS

Para fazer a transição do cliente Cisco Legacy AnyConnect para o novo cliente Cisco AnyConnect, use o protocolo SSL personalizado.

- **Identificador de pacote de provedor:** para o cliente Legacy AnyConnect, o ID do pacote é com.cisco.anyconnect.gui.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo:** digite um nome de grupo opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo Juniper SSL para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do 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 da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
        * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
        * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo F5 SSL para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar 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.

Configurar o protocolo SonicWALL para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo ou domínio de login:** digite um grupo ou domínio de login opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você definir essa opção como I, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar incluir, clique em **Adicionar** e faça o seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Domínio:** digite o domínio a ser adicionado.
        * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo Ariba VIA para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar 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.

Configurar protocolos IKEv2 para iOS

Essa seção inclui as configurações usadas para os protocolos IKEv2, AlwaysOn IKEv2 e AlwaysOn IKEv2 Dual Configuration.

- **Permitir que o usuário desative a conexão automática:** para os protocolos AlwaysOn. Selecione se os usuários têm permissão para desativar a conexão automática com a rede em seus

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dispositivos. O padrão é **Off**.

- **Nome de host ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Identificador local:** o FQDN ou o endereço IP do cliente IKEv2. Este campo é obrigatório.
- **Identificador remoto:** o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
- **Autenticação de máquina:** escolha **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
  - Se você escolher **Segredo compartilhado**, digite uma chave secreta compartilhada opcional.
  - Se você escolher **Certificado**, escolha uma **Credencial de identidade** a ser usada. O padrão é **Nenhum.**
- **Autenticação estendida ativada:** selecione se o Protocolo de autenticação estendido (EAP) deve ser ativado. Se você escolher **I**, digite a **Conta de usuário** e a **Senha de autenticação**. (iOS 8.0 e versões posteriores)
- **Intervalo de DPD:** escolha quantas vezes um dispositivo par é contactado, para garantir que ele permaneça acessível. O padrão é **Nenhum**. As opções são: (iOS 8.0 e versões posteriores)
  - **Nenhum:** desative a detecção de par inativo.
  - **Baixo:** entre em contato com o par a cada 30 minutos.
  - **Médio:** entre em contato com o par a cada 10 minutos.
  - **Alto:** entre em contato com o par a cada 1 minuto.
- **Desativar mobilidade e multihoming:** escolha se deseja desativar esse recurso. (iOS 9.0+)
- **Usar atributos de sub-rede interna IPv4/IPv6:** escolha se deseja ativar esse recurso. (iOS 9.0+)
- **Desativar redirecionamentos:** escolha se deseja desativar redirecionamentos. (iOS 9.0+)
- **Ativar keepalive NAT enquanto o dispositivo está no modo de suspensão:** para os protocolos AlwaysOn. Pacotes de keepalive mantêm mapeamentos NAT para conexões IKEv2. O chip envia esses pacotes em intervalos regulares quando o dispositivo está ativo. Se esta configuração for I, o chip envia pacotes de keepalive mesmo enquanto o dispositivo estiver no modo de suspensão. O padrão é 20 segundos por WiFi e 110 segundos via rede celular. Você pode alterar o intervalo usando o parâmetro de intervalo de NAT keepalive. (iOS 9.0+)
- **Intervalo de keepalive NAT (segundos):** o padrão é 20 segundos. (iOS 9.0+)
- **Ativar o Perfect Forward Secrecy:** escolha se deseja ativar este recurso. (iOS 9.0+)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Endereços IP do servidor DNS:** opcional. Uma lista de configurações de endereços IP de servidores 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. (iOS 10.0+)
- **Domínios de pesquisa:** opcional. Uma lista de domínios usada para qualificar totalmente nomes de host de rótulo único.
- **Acrescentar domínios correspondentes suplementares à lista do resolvedor:** opcional. Determina se os domínios na lista de domínios correspondentes complementares devem ser acrescentados à lista de domínios de pesquisa do resolvedor. **0** significa acrescentar; **1** significa não acrescentar. O padrão é **0**.
- **Domínios correspondentes suplementares:** opcional. Uma lista de cadeias de domínios usada para determinar as consultas DNS que devem usar as configurações de resolvedor DNS contidas nos endereços de servidor DNS. Essa chave cria uma configuração de DNS dividido em que somente os hosts em determinados domínios resolvem usando o resolvedor DNS do túnel. Os hosts que não estejam em um dos domínios nessa são resolvidos por meio do resolvedor padrão do sistema.

Se esse parâmetro contiver uma cadeia vazia, esta será usada como o domínio padrão. É assim que uma configuração de túnel dividido pode direcionar todas as consultas DNS primeiramente para os servidores DNS da VPN antes dos servidores DNS primários. Se o túnel VPN se tornar a rota padrão da rede, os servidores DNS listados se tornarão o resolvedor padrão. Nesse caso, a lista de domínios correspondentes suplementares é ignorada.

- **Parâmetros IKE SA** e **Parâmetros SA filho**. Defina estas configurações para cada opção de parâmetros de Associação de segurança (SA):
  - **Algoritmo de criptografia:** na lista, clique no algoritmo de criptografia IKE a ser usado. O padrão é **3DES**.
  - **Algoritmo de integridade:** na lista, clique no algoritmo de integridade a ser usado. O padrão é **SHA1-96**.
  - **Grupo Diffie Hellman:** na lista, clique no número do grupo Diffie Hellman. O padrão é **2**.
  - **Tempo de vida em minutos:** digite um inteiro entre 10 e 1.440 que representa o tempo de vida SA (intervalo de rechaveamento). O padrão é **1440** minutos.
- **Exceções de serviço:** para os protocolos AlwaysOn. Exceções de serviço são serviços do sistema isentos da VPN AlwaysOn. Defina estas configurações de exceções de serviço:
  - **Correio de voz:** na lista, clique em como lidar com a exceção de correio de voz. O padrão é **Permitir tráfego através do túnel**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **AirPrint:** na lista, clique em como lidar com a exceção do AirPrint. O padrão é **Permitir tráfego através do túnel**.
  - **Permitir o tráfego de folha web cativa fora do túnel VPN:** selecione se deseja permitir que os usuários se conectem a pontos de acesso públicos fora do túnel da VPN. O padrão é **Off**.
  - **Permitir o tráfego de todos os aplicativos de rede cativos fora do túnel VPN:** selecione se deseja permitir todos os aplicativos de rede do ponto de acesso fora do túnel da VPN. O padrão é **Off**.
  - **Identificadores de pacote de aplicativos de rede cativos:** para cada identificador de pacote de aplicativos de rede hotspot que os usuários têm permissão para acessar, clique em **Adicionar** e digite o **Identificador de pacote** de aplicativos de rede hotspot. Clique em **Salvar** para salvar o identificador de pacote de aplicativos.

- **VPN por aplicativo**. Definir estas configurações para tipos de conexão IKEv2.
  - **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível apenas no iOS 9.0 e versões posteriores.
  - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios Safari:** clique em **Adicionar** para adicionar um nome de domínio do Safari.
- **Configuração de proxy:** escolha como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.

Configurar o protocolo Citrix VPN para iOS

O cliente Citrix VPN está disponível na Apple Store aqui.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum.**
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você definir essa opção como I, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar 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.
- **XML personalizado:** para cada parâmetro XML personalizado que você desejar adicionar, clique em **Adicionar** e especifique os pares de chave/valor. Os parâmetros disponíveis são:
  - **disableL3:** desativa a VPN de nível de sistema. Permite somente uma VPN por aplicativo. Nenhum **valor** é necessário.
  - **useragent:** associa a esta política de dispositivo todas as políticas do NetScaler que são direcionadas a clientes de plug-in VPN. O **valor** dessa chave é anexado automaticamente ao plug-in VPN para as solicitações iniciadas pelo plug-in.

Configurar o 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. Implemente a política em dispositivos iOS.
2. Faça o upload do cliente Cisco AnyConnect de https://itunes.apple.com/us/app/cisco-anyconnect/id1135064690?mt=8, adicione o aplicativo ao XenMobile Server e implemente o aplicativo em dispositivos iOS.
3. Remova a política de dispositivo VPN antiga de dispositivos iOS.

Configurações:

- **Identificador SSL personalizado (formato DNS inverso):** defina o identificador de pacote. Para o cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de pacote de provedor:** se o aplicativo especificado em **Identificador SSL personalizado** tiver vários provedores VPN do mesmo tipo (proxy de aplicativo ou túnel de pacote), especifique esse identificador de pacote. Para o cliente Cisco AnyConnect, use

© 1999-2019 Citrix Systems, Inc. All rights reserved.

com.cisco.anyconnect.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum.**
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para iOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você definir essa opção como I, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
  - **Tipo de provedor:** um tipo de provedor indica se o provedor é um serviço de VPN ou serviço de proxy. No caso de serviço de VPN, escolha **Túnel de pacote**. No caso de serviço de proxy, escolha **Proxy de aplicativo**. No caso de cliente Cisco AnyConnect, escolha **Túnel de pacote**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.
- **XML personalizado:** para cada parâmetro XML personalizado que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do parâmetro:** digite o nome do parâmetro a ser adicionado.
  - **Valor:** digite o valor associado ao **Nome do parâmetro**.
  - Clique em **Salvar** para salvar o parâmetro ou clique em **Cancelar** para não salvar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar as opções de Ativar VPN sob demanda para iOS

- **Domínio On Demand:** para cada domínio e ação associada a ser tomada quando os usuários se conectarem a eles que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
- **Domínio:** digite o domínio a ser adicionado.
- **Ação:** na lista, clique em 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 acionará uma tentativa de conexão VPN se a resolução de nome de domínio falhar, por exemplo, 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.
- **Regras on demand**
  - **Ação:** na lista, clique na ação a ser tomada. O padrão é **EvaluateConnection**. As ações possíveis são:
    * **Permitir:** permitir que a VPN sob demanda se conecte quando acionada.
    * **Conectar:** inicie incondicionalmente uma conexão VPN.
    * **Desconectar:** remover a conexão VPN e não se reconectar sob demanda, desde que a regra seja correspondida.
    * **EvaluateConnection:** avalie a matriz ActionParameters de cada conexão.
    * **Ignorar:** manter todas as conexões VPN existentes ativas, mas não se reconectar sob demanda, desde que a regra seja correspondida.
  - **DNSDomainMatch:** para cada domínio em relação ao qual a lista de domínios de pesquisa de um dispositivo pode corresponder que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
    * **Domínio DNS**: digite o nome de domínio. Você pode usar o prefixo do caractere curinga "*" para correspondência de vários domínios. Por exemplo, *.exemplo.com corresponde a meudominio.exemplo.com, seudominio.exemplo.com e dominiodela.exemplo.com.
    * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
  - **DNSServerAddressMatch:** para cada endereço IP ao qual qualquer um dos servidores DNS especificados da rede pode corresponder que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
    * **Endereço de servidor DNS:** digite o endereço de servidor DNS que você deseja adicionar. Você pode usar o sufixo do caractere curinga "*" para correspondência de servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede da classe A.
    * Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar.
  - **InterfaceTypeMatch:** na lista, clique no tipo de hardware primário de interface de rede

© 1999-2019 Citrix Systems, Inc. All rights reserved.

em uso. O padrão é **Não especificado**. Os valores possíveis são:
    * **Não especificad:o** corresponde qualquer interface de rede de hardware. Esse é o padrão.
    * **Ethernet:** corresponde somente a hardware de interface de rede Ethernet.
    * **WiFi:** corresponde somente a hardware de interface de rede Wi-Fi.
    * **Celular:** corresponde somente a hardware de interface de rede Celular.
- **SSIDMatch:** para cada SSID a ser correspondido em relação à rede atual que você desejar adicionar, clique em **Adicionar** e faça o seguinte.
    * **SSID:** digite o SSID a ser adicionado. Se a rede não for uma rede WiFi ou se o SSID não for exibido, a correspondência falhará. Deixe essa lista vazia para corresponder a qualquer SSID.
    * Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar.
- **URLStringProbe:** digite uma URL a ser obtida. Se essa URL for obtida com êxito sem redirecionamento, essa regra será correspondida.
- **ActionParameters : Domains:** para cada domínio que EvaluateConnection verifica que você desejar adicionar, 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.
- **ActionParameters : DomainAction:** na lista, clique no comportamento da VPN dos domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
    * **ConnectIfNeeded:** o domínio acionará uma tentativa de conexão VPN se a resolução de nome de domínio falhar, por exemplo, 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.
- **ActionParameters: RequiredDNSServers:** para cada endereço IP do servidor DNS que deve ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:
    * **Servidor DNS:** válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Esse servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida na resposta. Esse servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
    * Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar.
- **ActionParameters : RequiredURLStringProbe:** opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) a ser investigada usando uma solicitação GET. Se não for possível resolver o nome de host da URL, se o servidor estiver inacessível ou se o servidor não tiver respondido com um código de status 200 HTTP, uma conexão VPN será estabelecida na resposta. Válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **OnDemandRules : XML content:** digite ou copie e cole as regras on demand da configuração XML.
    * Clique em **Verificar dicionário** para validar o código XML. Você verá XML Válido em texto verde abaixo da caixa de texto do conteúdo XML se o XML for válido; caso contrário, você verá uma mensagem de erro em texto laranja descrevendo o erro.
- **Proxy**
  - **Configuração de proxy:** na lista, clique em como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.
    * Se você ativar a opção **Manual**, configure as seguintes 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 do servidor proxy.
      · **Senha:** digite uma senha opcional do servidor proxy.
    * Se você configurar **Automático**, defina esta configuração:
      · **URL do servidor proxy:** digite a URL do servidor proxy. Este campo é obrigatório.
- **Configurações de política**
  - Em **Configurações de política**, ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

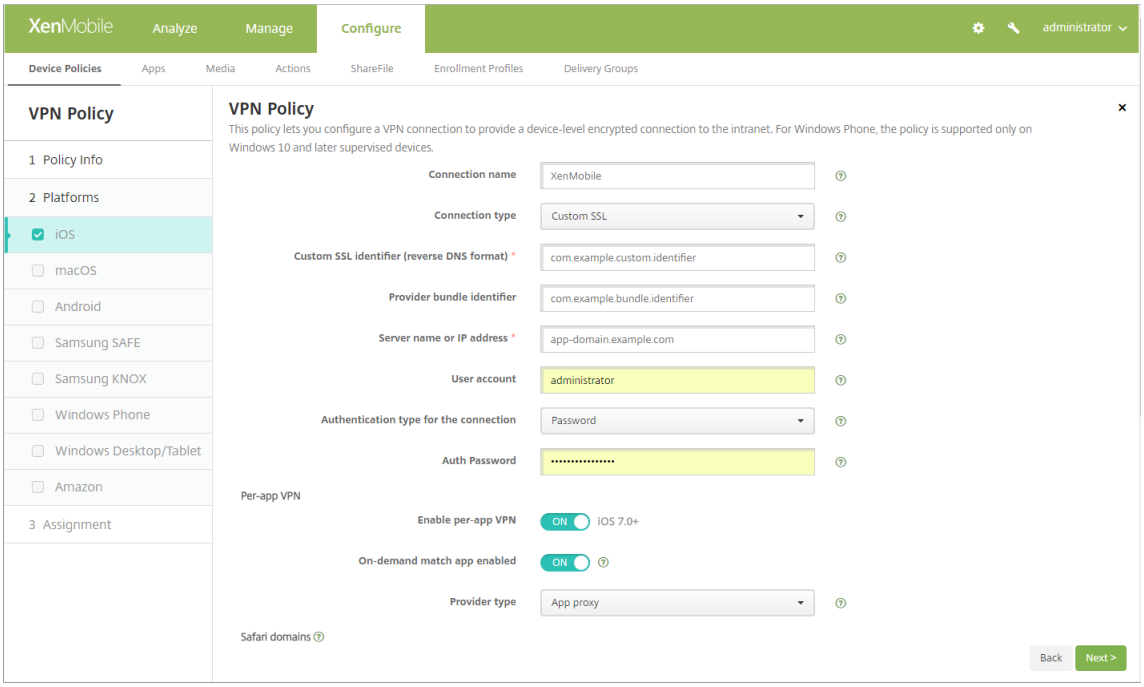
Configurar uma VPN por aplicativo

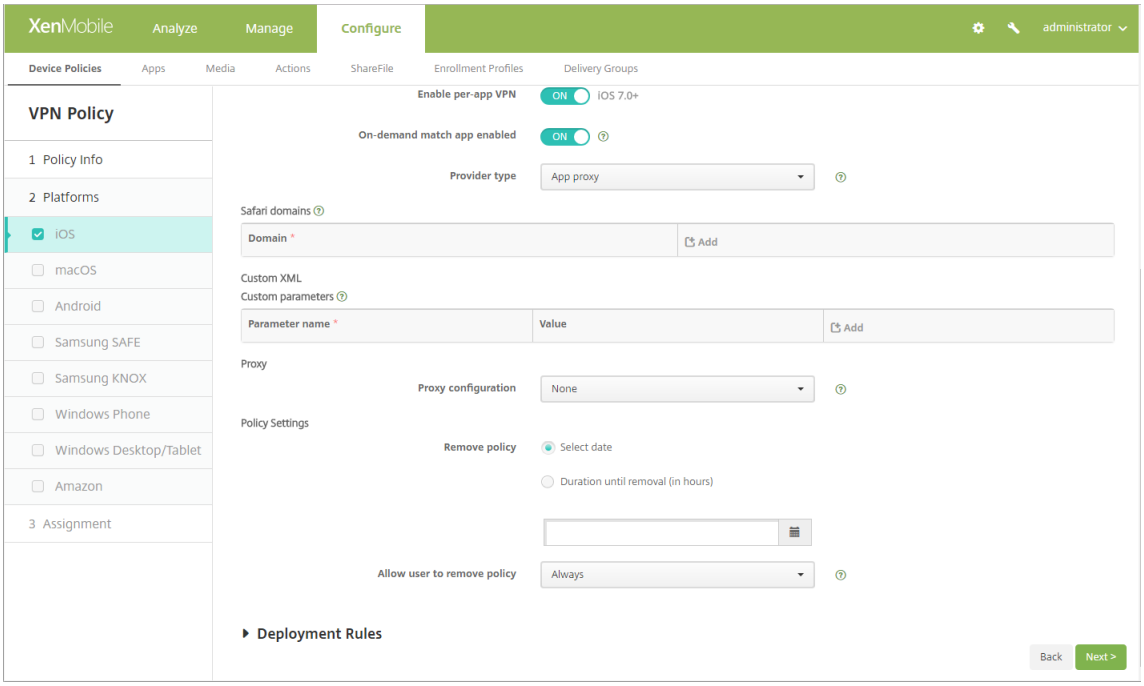
Opções de VPN por aplicativo para o iOS estão disponíveis para estes tipos de conexão: Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN e SSL personalizado.

Para configurar uma VPN por aplicativo:

1. Em **Configurar > Políticas de dispositivo**, crie uma política de VPN. Por exemplo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.





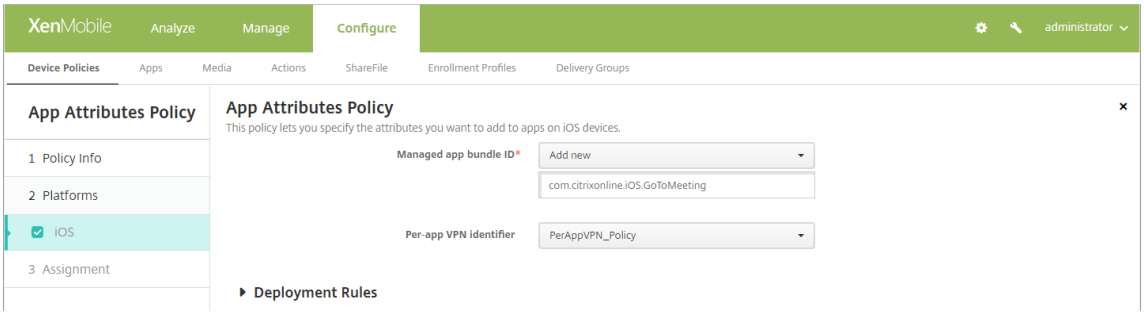
Uma política de VPN por aplicativo para o Secure Hub tem os seguintes requisitos de configuração:

- **Nome da conexão:** defina como **XenMobile**. O XenMobile usa o Nome da conexão como a descrição localizada do provedor de VPN. O Secure Hub usa a descrição localizada da VPN para diferenciar o provedor no âmbito do dispositivo do provedor por aplicativo.
- **Tipo de conexão:** defina como **SSL personalizado**.

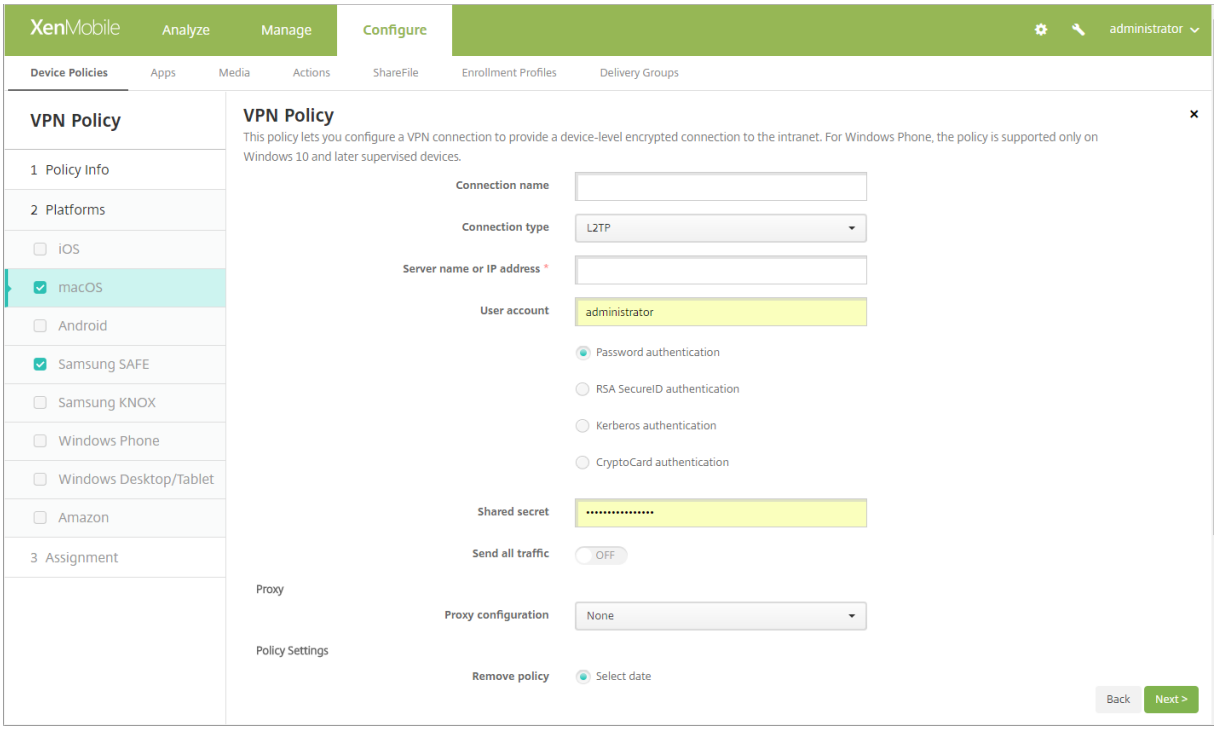
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Identificador SSL personalizado:** defina o identificador de pacote do Secure Hub.
- **Identificador de pacote de provedor:** defina como o identificador de pacote da extensão de rede do Secure Hub. Esse identificador de pacote é o identificador de pacote do Secure Hub, especificado em **Identificador de SSL personalizado**, com **.NE** acrescentado.
- **Tipo de provedor:** defina como **Túnel de pacote**.

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 criado na etapa 1. Para **ID de pacote de aplicativos gerenciados**, escolha a lista de aplicativos ou digite a ID do pacote de aplicativos. (Se você implantar um política de inventário de aplicativos iOS, a lista de aplicativos conterá aplicativos).



Configurações do macOS



- **Nome da conexão:** digite um nome para a conexão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Tipo de conexão:** na lista, clique no protocolo a ser usado para esta conexão. O padrão é L2TP.
  - **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
  - **PPTP:** Encapsulamento Ponto a Ponto.
  - **IPSec:** sua conexão VPN corporativa.
  - **Cisco AnyConnect:** cliente VPN Cisco AnyConnect.
  - **Juniper SSL:** cliente VPN Juniper Networks SSL.
  - **F5 SSL:** cliente VPN F5 Networks SSL.
  - **SonicWALL Mobile Connect:** cliente VPN unificado Dell para iOS.
  - **Ariba VIA:** cliente Ariba Networks Virtual Internet Access.
  - **Citrix VPN:** cliente Citrix VPN.
  - **SSL personalizado:** protocolo SSL personalizado.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione uma entre **autenticação de senha**, **autenticação RSA SecureID**, **autenticação Kerberos** e **autenticação CryptoCard**. O padrão é **Autenticação de senha**.
- **Segredo compartilhado:** digite a chave secreta compartilhada do IPSec.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo PPTP para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione uma entre **autenticação de senha**, **autenticação RSA SecureID**, **autenticação Kerberos** e **autenticação CryptoCard**. O padrão é **Autenticação de senha**.
- **Nível de criptografia:** selecione o nível de criptografia desejado. O padrão é **Nenhum**.
  - **Nenhum:** não use criptografia.
  - **Automático:** use o nível de criptografia mais forte compatível com o servidor.
  - **Máximo** (128 bits): use sempre criptografia de 128 bits.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o protocolo IPSec para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
  - Se você ativar a autenticação **Segredo compartilhado**, defina as seguintes configurações:
    * **Nome do grupo:** digite um nome de grupo opcional.
    * **Segredo compartilhado:** digite uma chave secreta compartilhada opcional.
    * **Usar autenticação híbrida:** selecione se a autenticação híbrida deve ser usada. Com a autenticação híbrida, o primeiro servidor autentica a si mesmo no cliente e, em seguida, o cliente autentica a si mesmo no servidor. O padrão é **Off**.
    * **Solicitar senha:** selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **Off**.
  - Se você ativar a autenticação de **Certificado**, defina estas configurações:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se os usuários serão obrigados a inserir o respectivo PIN quando se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.

Configurar o protocolo Cisco AnyConnect para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo:** digite um nome de grupo opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
        * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.
    - **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
        * **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
        * **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo SSL do Juniper para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do 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 da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
    - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
    - Se você ativar a opção **Certificado**, configure as seguintes definições:
        * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
        * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
        * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ativar essa opção, defina estas configurações:

- **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
- **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo F5 SSL para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar o protocolo SonicWALL para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo ou domínio de login:** digite um grupo ou domínio de login opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo Ariba VIA para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
        * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
        * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.
- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
  - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Configurar o protocolo Citrix VPN para macOS

O cliente Citrix VPN está disponível na Apple Store aqui.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum.**
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Disponível somente no iOS 7.0 e versões posteriores. Se você ativar essa opção, defina estas configurações:
  - **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar 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.
- **XML personalizado:** para cada parâmetro XML personalizado que você desejar adicionar, clique em **Adicionar** e especifique os pares de chave/valor. Os parâmetros disponíveis são:
  - **disableL3:** desativa a VPN de nível de sistema. Permite somente uma VPN por aplicativo. Nenhum **valor** é necessário.
  - **useragent:** associa a esta política de dispositivo todas as políticas do NetScaler que são direcionadas a clientes de plug-in VPN. O **valor** dessa chave é anexado automaticamente ao plug-in VPN para as solicitações iniciadas pelo plug-in.

Configurar o protocolo SSL personalizado para macOS

- **Identificador SSL personalizado (formato DNS inverso):** digite o identificador SSL no formato de DNS inverso. Este campo é obrigatório.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN. Este campo é obrigatório.
- **Conta de usuário:** digite uma conta de usuário opcional.
  - **Tipo de autenticação da conexão:** na lista, clique em **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
  - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
  - Se você ativar a opção **Certificado**, configure as seguintes definições:
    * **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum.**
    * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
    * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda para macOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
    * **Correspondência sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do 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 desejar 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.
- **XML personalizado:** para cada parâmetro XML personalizado que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do parâmetro:** digite o nome do parâmetro a ser adicionado.
  - **Valor:** digite o valor associado ao **Nome do parâmetro**.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar as opções de Ativar VPN sob demanda para macOS

- **Domínio On Demand:** para cada domínio e ação associada a ser tomada quando os usuários se conectarem a eles que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Domínio:** digite o domínio a ser adicionado.
  - **Ação:** na lista, clique em 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 acionará uma tentativa de conexão VPN se a resolução de nome de domínio falhar, por exemplo, 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.
- **Regras on demand**
  - **Ação:** na lista, clique na ação a ser tomada. O padrão é **EvaluateConnection**. As ações possíveis são:
    * **Permitir:** permitir que a VPN sob demanda se conecte quando acionada.
    * **Conectar:** inicie incondicionalmente uma conexão VPN.
    * **Desconectar:** remover a conexão VPN e não se reconectar sob demanda, desde que a regra seja correspondida.
    * **EvaluateConnection:** avalie a matriz **ActionParameters** de cada conexão.
    * **Ignorar:** manter todas as conexões VPN existentes ativas, mas não se reconectar sob demanda, desde que a regra seja correspondida.
  - **DNSDomainMatch:** para cada domínio em relação ao qual a lista de domínios de pesquisa

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de um dispositivo do usuário pode corresponder que você desejar adicionar, clique em **Adicionar** e faça o seguinte:

  * **Domínio DNS**: digite o nome de domínio. Você pode usar o prefixo do caractere curinga "*" para correspondência de vários domínios. Por exemplo, *.exemplo.com corresponde a meudominio.exemplo.com, seudominio.exemplo.com e dominiodela.exemplo.com.
  * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

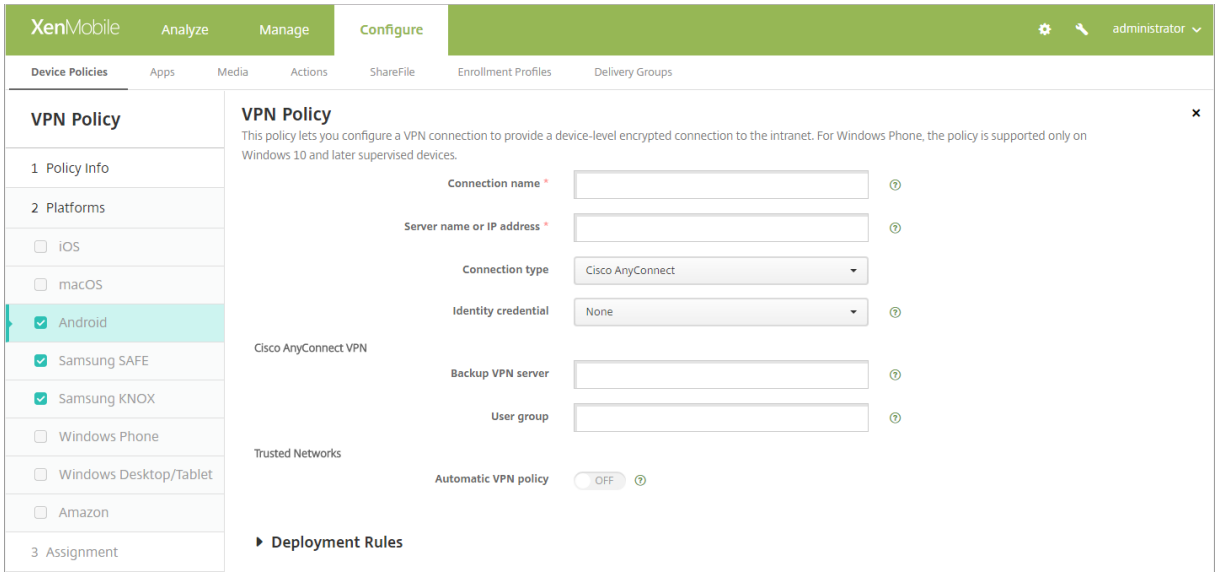
- **DNSServerAddressMatch:** para cada endereço IP ao qual qualquer um dos servidores DNS especificados da rede pode corresponder que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  * **Endereço de servidor DNS:** digite o endereço de servidor DNS que você deseja adicionar. Você pode usar o sufixo do caractere curinga "*" para correspondência de servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede da classe A.
  * Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar.
- **InterfaceTypeMatch:** na lista, clique no tipo de hardware primário de interface de rede em uso. O padrão é **Não especificado**. Os valores possíveis são:
  * **Não especificad:o** corresponde qualquer interface de rede de hardware. Esse é o padrão.
  * **Ethernet:** corresponde somente a hardware de interface de rede Ethernet.
  * **WiFi:** corresponde somente a hardware de interface de rede Wi-Fi.
  * **Celular:** corresponde somente a hardware de interface de rede Celular.
- **SSIDMatch:** para cada SSID a ser correspondido em relação à rede atual que você desejar adicionar, clique em **Adicionar** e faça o seguinte.
  * **SSID:** digite o SSID a ser adicionado. Se a rede não for uma rede WiFi ou se o SSID não for exibido, a correspondência falhará. Deixe essa lista vazia para corresponder a qualquer SSID.
  * Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar.
- **URLStringProbe:** digite uma URL a ser obtida. Se essa URL for obtida com êxito sem redirecionamento, essa regra será correspondida.
- **ActionParameters : Domains:** para cada domínio que EvaluateConnection verifica que você desejar adicionar, 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.
- **ActionParameters : DomainAction:** na lista, clique no comportamento da VPN dos domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
  * **ConnectIfNeeded:** o domínio acionará uma tentativa de conexão VPN se a resolução

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de nome de domínio falhar, por exemplo, 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.
  - **ActionParameters: RequiredDNSServers:** para cada endereço IP do servidor DNS que deve ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:
    * **Servidor DNS:** válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Esse servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida na resposta. Esse servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
    * Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar.
  - **ActionParameters : RequiredURLStringProbe:** opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) a ser investigada usando uma solicitação GET. Se não for possível resolver o nome de host da URL, se o servidor estiver inacessível ou se o servidor não tiver respondido com um código de status 200 HTTP, uma conexão VPN será estabelecida na resposta. Válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
  - **OnDemandRules : XML content:** digite ou copie e cole as regras on demand da configuração XML.
    * Clique em **Verificar dicionário** para validar o código XML. Você verá XML Válido em texto verde abaixo da caixa de texto do conteúdo XML se o XML for válido; caso contrário, você verá uma mensagem de erro em texto laranja descrevendo o erro.
- **Proxy**
  - **Configuração de proxy:** na lista, clique em como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.
    * Se você ativar a opção **Manual**, configure as seguintes 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 do servidor proxy.
      · **Senha:** digite uma senha opcional do servidor proxy.
    * Se você configurar **Automático**, defina esta configuração:
      · **URL do servidor proxy:** digite a URL do servidor proxy. Este campo é obrigatório.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android



Configurar o protocolo Citrix VPN para Android

- **Nome da conexão:** digite um nome para a conexão VPN. Este campo é obrigatório.
- **Nome ou endereço IP do servidor:** digite o FQDN endereço IP do NetScaler Gateway.
- **Tipo de autenticação da conexão:** escolha um tipo de autenticação e preencha qualquer um dos campos que são exibidos 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:** é exibida para os **Tipos de autenticação** de **Certificado** ou **Senha e certificado**.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. Se você não ativar VPN por aplicativo, todo o tráfego passa pelo do túnel do Citrix VPN. Se você ativar VPN por aplicativo, especifique as configurações a seguir. O padrão é **Off**.
  - **Lista branca** ou **Lista negra**: escolha uma configuração. Se **Lista branca**, todos os aplicativos em lista branca passam pelo túnel através dessa VPN. Se for **Lista negra**, todos os aplicativos, exceto os que estão na lista negra, passarão pelo túnel através dessa VPN.
  - **Lista de aplicativos:** especifique os aplicativos em lista branca ou lista negra. Clique em **Adicionar** e, em seguida, digite uma lista separada por vírgulas de nomes de pacote de aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **XML personalizado:** clique em **Adicionar** e, em seguida, digite parâmetros personalizados. O XenMobile é compatível com estes parâmetros para Citrix VPN:
  - **disableL3Mode:** opcional. Para ativar esse parâmetro, digite **Sim** para o **Valor**. Se ativado, o XenMobile não exibirá conexões de VPN adicionadas pelo usuário, e o usuário não poderá adicionar uma nova conexão. Essa restrição é global e se aplica a todos os perfis de VPN.
  - **userAgent:** um valor de cadeia de caracteres. Você pode especificar uma cadeia de caracteres de Agente do Usuário personalizada para enviar em cada solicitação HTTP. A cadeia de caracteres do agente de usuário especificado é acrescentada ao agente de usuário existente do Citrix VPN.

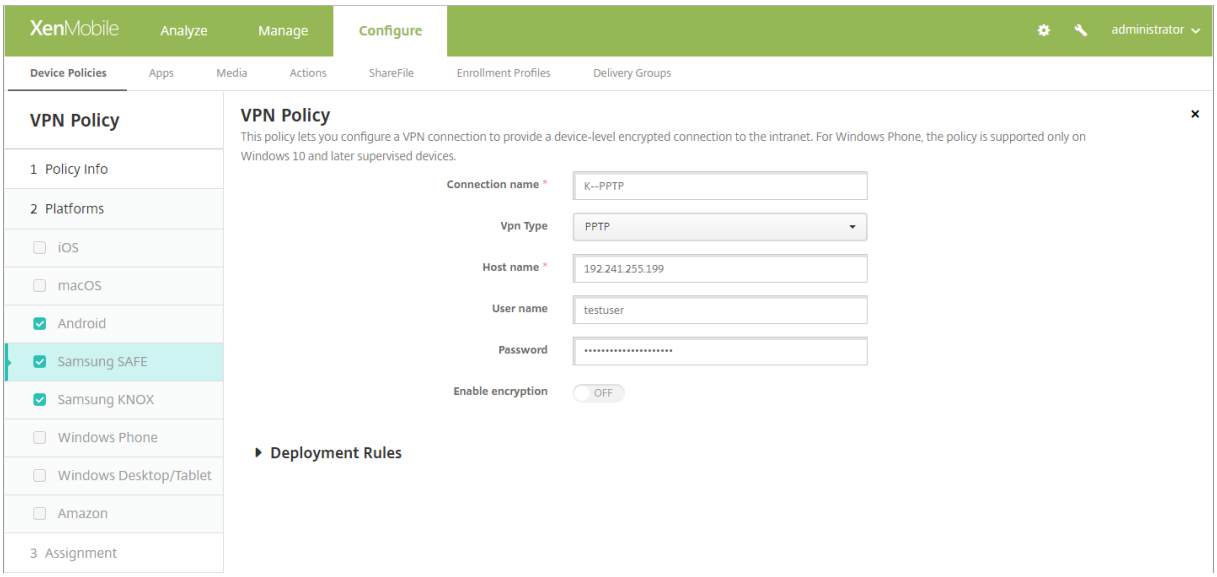
Configurar o protocolo Cisco AnyConnect VPN para Android

- **Nome da conexão:** digite um nome para a conexão VPN do Cisco AnyConnect. Este campo é obrigatório.
- **Nome do host ou endereço IP:** digite o nome ou endereço IP do servidor de VPN. Este campo é obrigatório.
- **Servidor VPN de backup:** digite as informações do servidor VPN de backup.
- **Grupo de usuários:** digite as informações do grupo de usuários.
- **Credencial de identidade:** na lista, selecione uma credencial de identidade.
- **Redes Confiáveis**
  - **Política VPN automática:** ative ou desative essa opção para definir a forma como o VPN reage a redes confiáveis e não confiáveis. Se essa opção estiver ativada, defina as seguintes configurações:
    * **Política de rede confiável:** na lista, clique na política desejada. O padrão é **Desconectar**. As opções possíveis são:
      · **Desconectar:** o cliente encerra a conexão VPN na rede confiável. Esse é o padrão.
      · **Conectar:** o cliente inicia uma conexão VPN na rede confiável.
      · **Não fazer nada:** o cliente não toma nenhuma ação.
      · **Pausar:** suspende a sessão de VPN (em vez de desconectá-la) quando um usuário insere uma rede configurada como confiável após o estabelecimento de uma sessão VPN fora da rede confiável. Quando o usuário deixa a rede confiável novamente, a sessão é retomada. Isso elimina a necessidade de estabelecer uma nova sessão VPN após a saída de uma rede confiável.
    * **Política de rede não confiável:** na lista, clique na 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 conectada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Domínios confiáveis:** para cada sufixo de domínio que a interface de rede pode ter 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.
- **Servidores confiáveis:** para cada endereço de servidor que uma interface de rede pode ter 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.

Definir as configurações do Samsung SAFE



- **Nome da conexão:** digite um nome para a conexão.
- **Tipo de VPN:** na lista, clique no protocolo a ser usado para essa conexão. O padrão é **L2TP com chave pré-compartilhada**. As opções possíveis são:
  - **L2TP com chave pré-compartilhada:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada. Essa é a configuração padrão.
  - **L2TP com certificado:** protocolo de encapsulamento de camada 2 com certificado.
  - **PPTP:** Encapsulamento Ponto a Ponto.
  - **IPSec:** sua conexão VPN corporativa. Aplicável a versões de SAFE anteriores à versão 2.0.
  - **Genérico:** uma conexão VPN genérica. Aplicável à versão 2.0 de SAFE ou superiores.

Configure o L2TP com o protocolo de chave pré-compartilhada para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Senha:** digite uma senha opcional.
- **Chave pré-compartilhada:** digite a chave pré-compartilhada. Essa opção é necessária.

Configurar o L2TP com o protocolo de certificado para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.

Configurar o protocolo PPTP para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Ativar criptografia:** selecione se a criptografia deve ser ativada na conexão VPN.

Configurar o protocolo da Empresa para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar servidor de backup:** selecione se um servidor VPN de backup deve ser ativado. Se ativado, no **servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
  - **Nome de usuário:** digite um nome de usuário.
  - **Senha:** digite a senha de usuário.
- **Nome do grupo:** digite um nome de grupo opcional.
- **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. As opções possíveis são:
  - **Certificado:** use a autenticação de certificado. Esse é o padrão. Se selecionado, na lista de Credenciais de identidade, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo Chave pré-compartilhada, digite a chave secreta compartilhada.
  - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
  - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
  - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
- **Certificado de CA:** na lista, clique no certificado a ser usado. O padrão é **Nenhum**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN. O padrão é **Off**.
- **Ativar a autenticação de cartão inteligente:** selecione se os usuários têm permissão para autenticar usando cartões inteligentes. O padrão é **Off**.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada. O padrão é **Off**.
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, clique na força da chave a ser usada. O padrão é 0.
- **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. O padrão é **Automático**. As opções possíveis são:
  - **Automático:** o túnel dividido é usado automaticamente.
  - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
  - **Desativado:** o túnel dividido não é usado.
- **SuiteB Type:** na lista, clique no nível de criptografia NSA Suite B a ser usado. O padrão é **GCM-128.** As opções possíveis são:
  - **GCM-128:** use a criptografia AES-GCM de 128 bits.
  - **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
  - **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
  - **Nenhum:** não use criptografia.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Configurar o protocolo genérico para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se ativado, em **Senha**, digite a senha do usuário.
- **Nome de usuário:** digite um nome de usuário.
- **Agente de nome de pacote VPN:** o nome ou o ID do pacote da VPN instalada no dispositivo; por exemplo, Mocana ou Pulse Secure.
- **Tipo de conexão VPN:** na lista, clique em **IPSEC** ou **SSL** para o tipo de conexão a ser usado. O padrão é **IPSEC**. As seções a seguir descrevem as definições de configuração de cada tipo de conexão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Definir configurações de tipo de conexão IPSEC para Samsung SAFE

- **Identidade:** digite um identificador opcional para essa configuração.
- **Tipo de ID de grupo IPsec:** na lista, clique no tipo de ID de grupo IPsec a ser usado. O padrão é **Padrão**. As opções possíveis são:
  - **Padrão**
  - **Endereço IPv4**
  - **Nome de domínio totalmente qualificado (FQDN)**
  - **FQDN do Usuário**
  - **ID de chave IKE**
- **Versão de IKE:** na lista, clique na versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.
- **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
  - **Certificado:** use a autenticação de certificado. Se selecionado, na lista de **Credenciais de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
  - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
  - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
  - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
  - **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Certificado de CA:** na lista, clique no certificado a ser usado.
- **Ativar detecção de perda de conexão:** selecione se você deseja entrar em contato com um par para garantir que ele permaneça ativo. O padrão é **Off**.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Vida útil ike em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, clique na força da chave a ser usada. O padrão é **0**.
- **Modo de troca de chaves IKE Phase 1:** selecione **Principal** ou **Agressivo** para o modo de negociação do IKE Phase 1. O padrão é **Principal**.
  - **Principal:** nenhuma informação é exposta a potenciais invasores durante a negociação, mas é mais lento do que o modo **Agressivo**.
  - **Agressivo:** algumas informações (por exemplo, a identidade dos pares de negociação)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

são expostas a potenciais invasores durante a negociação, mas é mais rápido do que o modo **Principal**.

- **Valor com Perfect forward secrecy (PFS):** selecione se PFS deve ser usado para exigir que uma nova troca de chaves renegocie uma conexão.
- **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. As opções possíveis são:
  - **Automático:** o túnel dividido é usado automaticamente.
  - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
  - **Desativado:** o túnel dividido não é usado.
- **Algoritmo de criptografia IPSEC:** uma configuração de VPN que o protocolo IPSec usa.
- **Algoritmo de criptografia IKE:** uma configuração de VPN que o protocolo IPSec usa.
- **Algoritmo de integridade IKE:** uma configuração de VPN que o protocolo IPSec usa.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do KNOX.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **VPN por Aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

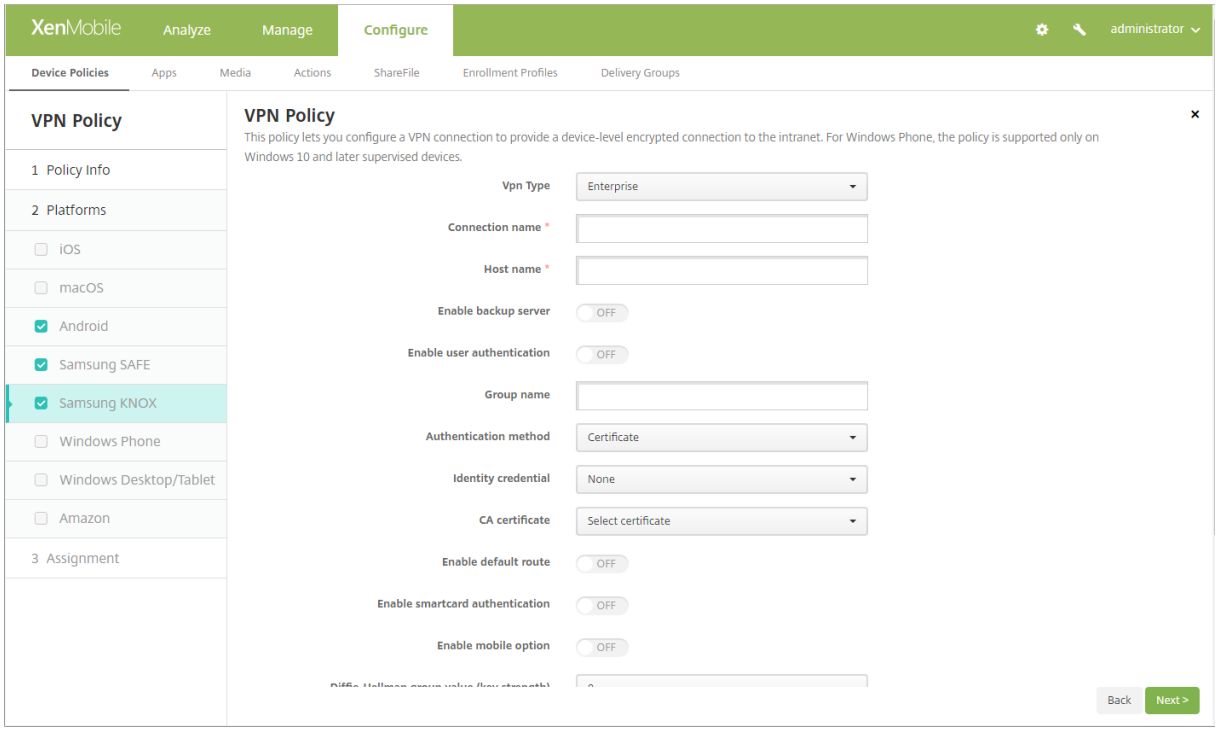
Definir configurações de tipo de conexão SSL para o Samsung SAFE

- **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. O padrão é **Não aplicável**. As opções possíveis são:
  - **Não Aplicável**
  - **Certificado:** use a autenticação de certificado. Se selecionado, na lista de **Credenciais de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Certificado de CA:** na lista, clique no certificado a ser usado.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. As opções possíveis são:
  - **Automático:** o túnel dividido é usado automaticamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
  - **Desativado:** o túnel dividido não é usado.
- **Algoritmo SSL:** digite o algoritmo SSL a ser usado para a negociação cliente-servidor.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do KNOX.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **VPN por Aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Definir as configurações do Samsung KNOX



Quando você configura qualquer política para o Samsung KNOX, ela se aplica somente no contêiner do Samsung KNOX.

- **Tipo de VPN:** na lista, clique em **Empresarial** (aplicável a versões do KNOX anteriores à 2.0) ou em **Genérico** (aplicável à versão 2.0 do KNOX ou superior). O padrão é **Empresarial**.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar protocolo Empresarial para o Samsung KNOX

- **Nome da conexão:** digite um nome para a conexão. Este campo é obrigatório.
- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar servidor de backup:** selecione se um servidor VPN de backup deve ser ativado. Se ativado, no **servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
  - **Nome de usuário:** digite um nome de usuário.
  - **Senha:** digite a senha de usuário.
- **Nome do grupo:** digite um nome de grupo opcional.
- **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. As opções possíveis são:
  - **Certificado:** use a autenticação de certificado. Para autenticação de certificado, selecione também a credencial a ser usada na lista de **Credenciais de identidade**.
  - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo Chave pré-compartilhada, digite a chave secreta compartilhada.
  - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
  - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
  - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
- **Certificado de CA:** na lista, clique no certificado a ser usado.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar a autenticação de cartão inteligente:** selecione se os usuários têm permissão para autenticar usando cartões inteligentes. O padrão é **Off**.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, clique na força da chave a ser usada. O padrão é **0**.
- **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. As opções possíveis são:
  - **Automático:** o túnel dividido é usado automaticamente.
  - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
  - **Desativado:** nenhum túnel dividido é usado.
- **SuiteB Type:** na lista, clique no nível de criptografia NSA Suite B a ser usado. As opções possíveis são:
  - **GCM-128:** use a criptografia AES-GCM de 128 bits, que é padrão.
  - **GCM-256:** use a criptografia AES-GCM de 256 bits.
  - **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
  - **GMAC-256:** use a criptografia AES-GMAC de 256 bits.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Nenhum:** não use criptografia.
- **Rotas de encaminhamento:** clique em **Adicionar** para adicionar qualquer rota de encaminhamento opcional se o servidor VPN corporativo for compatível com várias tabelas de roteamento.

Configurar o protocolo genérico para o Samsung KNOX

- **Nome da conexão:** digite um nome para a conexão. Este campo é obrigatório.
- **Agente de nome de pacote VPN:** o nome ou o ID do pacote da VPN instalada no dispositivo; por exemplo, Mocana ou Pulse Secure.
- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
  - **Nome de usuário:** digite um nome de usuário.
  - **Senha:** digite a senha de usuário.
- **Identidade:** digite um identificador opcional para essa configuração. Aplica-se somente quando **Tipo de conexão VPN = IPSEC.**
- **Tipo de conexão VPN:** na lista, clique em **IPSEC** ou **SSL** para o tipo de conexão a ser usado. O padrão é **IPSEC**. As seções a seguir descrevem as definições de configuração de cada tipo de conexão.
- **Definir as configurações de conexão IPSEC**
  - **Identidade:** digite um identificador opcional para essa configuração.
  - **Tipo de ID de grupo IPsec:** na lista, clique no tipo de ID de grupo IPsec a ser usado. O padrão é **Padrão**. As opções possíveis são:
    * **Padrão**
    * **Endereço IPv4**
    * **Nome de domínio totalmente qualificado (FQDN)**
    * **FQDN do Usuário**
    * **ID de chave IKE**
  - **Versão de IKE:** na lista, clique na versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.
  - **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
    * **Certificado:** use a autenticação de certificado. Se essa opção estiver selecionada, na lista **Credencial de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
    * **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
    * **RSA híbrido:** use a autenticação híbrida usando certificados RSA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

    * **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
    * **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
    * **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Certificado de CA:** na lista, clique no certificado a ser usado.
- **Ativar detecção de perda de conexão:** selecione se você deseja entrar em contato com um par para garantir que ele permaneça ativo. O padrão é **Off**.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Vida útil ike em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
- **Vida útil ipsec em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, clique na força da chave a ser usada. O padrão é **0**.
- **Modo de troca de chaves IKE Phase 1:** selecione **Principal** ou **Agressivo** para o modo de negociação do IKE Phase 1. O padrão é **Principal**.
    * **Principal:** nenhuma informação é exposta a potenciais invasores durante a negociação, mas é mais lento do que o modo **Agressivo**.
    * **Agressivo:** algumas informações (por exemplo, a identidade dos pares de negociação) são expostas a potenciais invasores durante a negociação, mas é mais rápido do que o modo **Principal**.
- **Valor com Perfect forward secrecy (PFS):** selecione se PFS deve ser usado para exigir que uma nova troca de chaves renegocie uma conexão.
- **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. As opções possíveis são:
    * **Automático:** o túnel dividido é usado automaticamente.
    * **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
    * **Desativado:** o túnel dividido não é usado.
- **SuiteB Type:** na lista, clique no nível de criptografia NSA Suite B a ser usado. O padrão é **GCM-128**. As opções possíveis são:
    * **GCM-128:** use a criptografia AES-GCM de 128 bits.
    * **GCM-256:** use a criptografia AES-GCM de 256 bits.
    * **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
    * **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
    * **Nenhum:** não use criptografia.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Algoritmo de criptografia IPSEC:** uma configuração de VPN que o protocolo IPSec usa.
- **Algoritmo de criptografia IKE:** uma configuração de VPN que o protocolo IPSec usa.
- **Algoritmo de integridade IKE:** uma configuração de VPN que o protocolo IPSec usa.
- **Knox:** configurações somente do Samsung KNOX.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do KNOX.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
  - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

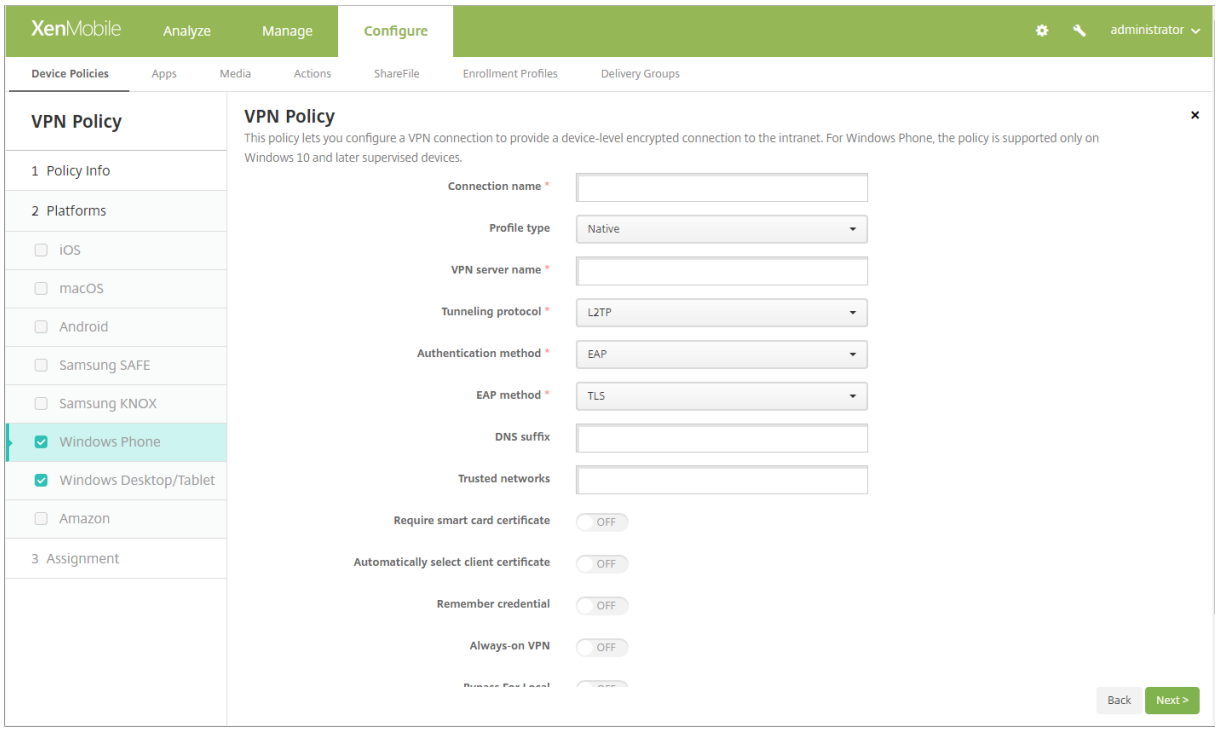
- **Definir as configurações de conexão SSL**
  - **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. As opções possíveis são:
    - **Não aplicável:** nenhum método de autenticação é aplicado. Esse é o padrão.
    - **Certificado:** use a autenticação de certificado. Esse é o padrão. Se selecionado, na lista de Credenciais de identidade, clique na credencial a ser usada. O padrão é Nenhum.
    - **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
  - **Certificado de CA:** na lista, clique no certificado a ser usado.
  - **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
  - **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
  - **Tipo de túnel dividido:** na lista, clique no tipo de túnel dividido a ser usado. As opções possíveis são:
    - **Automático:** o túnel dividido é usado automaticamente.
    - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados.
    - **Desativado:** nenhum túnel dividido é usado.
  - **SuiteB Type:** na lista, clique no nível de criptografia NSA Suite B a ser usado. O padrão é GCM-128. As opções possíveis são:
    - **GCM-128:** use a criptografia AES-GCM de 128 bits.
    - **GCM-256:** use a criptografia AES-GCM de 256 bits.
    - **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
    - **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
    - **Nenhuma: não usar criptografia.** Digite o algoritmo SSL a ser usado para a negoci-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ação cliente-servidor.

- **Algoritmo SSL:** digite o algoritmo SSL a ser usado para a negociação cliente-servidor.
- **Knox:** configurações somente do Samsung KNOX.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do KNOX.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  * **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  * Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  * **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
  * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurações do Windows Phone



Essas configurações são compatíveis somente em telefones supervisionados com Windows 10 e versões posteriores.

- **Nome da conexão:** insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil:** na lista, clique em **Nativo** ou **Plug-in**. O padrão é **Nativo**. As seções a seguir descrevem as configurações de cada uma dessas opções.

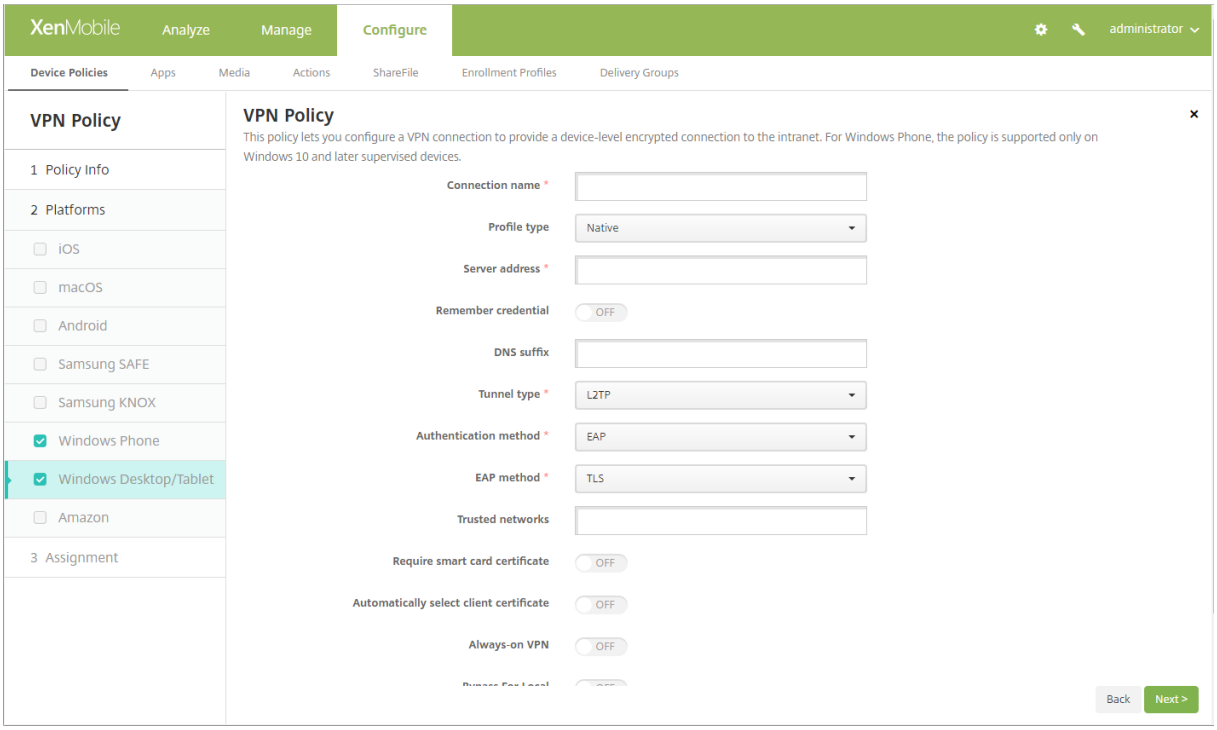
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Configurações de tipo de perfil nativo:** essas configurações se aplicam à VPN interna nos telefones com Windows dos usuários.
  - **Nome do servidor VPN:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
  - **Protocolo de encapsulamento**: na lista, clique no tipo de túnel VPN a ser usado. O padrão é **L2TP**. As opções possíveis são:
    * **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
    * **PPTP:** Encapsulamento Ponto a Ponto.
    * **IKEv2:** Internet Key Exchange versão 2.
  - **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. O padrão é **EAP**. As opções possíveis são:
    * **EAP:** Extended Authentication Protocol.
    * **MSChapV2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua. Esta opção não está disponível quando você seleciona IKEv2 para o tipo de túnel. Quando você seleciona MSChapV2, uma opção **Usar credenciais do Windows automaticamente** aparece; o padrão é **O**.
  - **Método EAP:** na lista, clique no método EAP a ser usado. O padrão é o **TLS**. Esse campo não está disponível quando a autenticação MSChapV2 está ativada. As opções possíveis são:
    * **TLS:** Transport Layer Security
    * **PEAP:** Protected Extensible Authentication Protocol
  - **Sufixo DNS:** digite o sufixo DNS.
  - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
  - **Exigir um certificado de cartão inteligente:** determine se deve ser exigido um certificado de cartão inteligente. O padrão é O.
  - **Selecionar o certificado cliente automaticamente:** Selecione se o certificado cliente a ser usado para autenticação deve ser escolhido automaticamente. O padrão é O. Essa opção não está disponível quando Exigir um certificado de cartão inteligente está ativado.
  - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é O. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
  - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é O. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
  - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Configurar o tipo de protocolo do plugin:** essas configurações se aplicam a plug-ins de VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
  - **Endereço de servidor:** digite a URL, o nome de host ou o endereço IP do servidor VPN.
  - **ID de aplicativo cliente:** digite o nome de família do pacote do plug-in de VPN.
  - **XML de Perfil de Plug-in:** selecione o perfil de plug-in de VPN personalizado para ser usado clicando em Procurar e navegando até a localização do arquivo. Entre em contato com o provedor do plug-in para obter o formato e os detalhes.
  - **Sufixo DNS:** digite o sufixo DNS.
  - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
  - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é O. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
  - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é O. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
  - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.

Configurações do Windows Desktop/Tablet



© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Nome da conexão:** insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil:** na lista, clique em **Nativo** ou **Plug-in**. O padrão é **Nativo**.
- **Configure Native profile type:** essas configurações se aplicam à VPN interna nos dispositivos Windows dos usuários.
  - **Endereço de servidor:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
  - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é **Off**. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
  - **Sufixo DNS:** digite o sufixo DNS.
  - **Tipo de túnel:** na lista, clique no tipo de túnel VPN a ser usado. O padrão é **L2TP**. As opções possíveis são:
    - **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
    - **PPTP:** Encapsulamento Ponto a Ponto.
    - **IKEv2:** Internet Key Exchange versão 2.
  - **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. O padrão é **EAP**. As opções possíveis são:
    - **EAP:** Extended Authentication Protocol.
    - **MSChapV2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua. Esta opção não está disponível quando você seleciona **IKEv2** para o tipo de túnel.
  - **Método EAP:** na lista, clique no método EAP a ser usado. O padrão é o **TLS**. Esse campo não está disponível quando a autenticação MSChapV2 está ativada. As opções possíveis são:
    - **TLS:** Transport Layer Security
    - **PEAP:** Protected Extensible Authentication Protocol
  - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
  - **Exigir um certificado de cartão inteligente:** determine se deve ser exigido um certificado de cartão inteligente. O padrão é **Off**.
  - **Selecionar o certificado cliente automaticamente:** selecione se o certificado cliente a ser usado para autenticação deve ser escolhido automaticamente. O padrão é **Off**. Essa opção não está disponível quando você ativa **Exigir um certificado de cartão inteligente**.
  - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é **Off**. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
  - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos

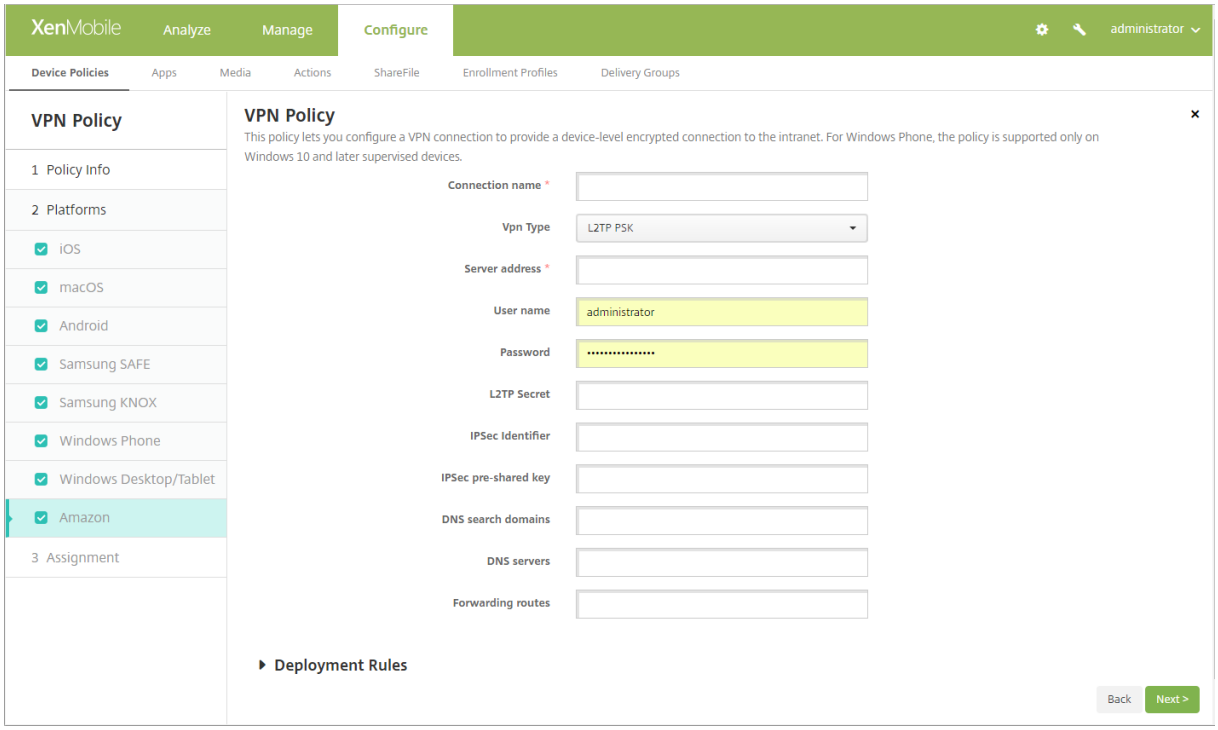
© 1999-2019 Citrix Systems, Inc. All rights reserved.

locais ignorem o servidor proxy.

- **Configure Plugin profile type:** essas configurações se aplicam a plug-ins de VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
  - **Endereço de servidor:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
  - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é **Off**. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
  - **Sufixo DNS:** digite o sufixo DNS.
  - **ID de aplicativo cliente:** digite o nome de família do pacote do plug-in de VPN.
  - **XML de Perfil de Plug-in:** selecione o perfil de plug-in de VPN personalizado para ser usado clicando em **Procurar** e navegando até a localização 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 vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
  - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é **Off**. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
  - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Definir as configurações do Amazon



- **Nome da conexão:** insira um nome para a conexão.
- **Tipo de VPN**: clique no tipo de conexão. As opções possíveis são:
  - **L2TP PSK:** protocolo de encapsulamento de camada 2 com autenticação de chave pré-compartilhada. Esse é o padrão.
  - **L2TP RSA:** protocolo de encapsulamento de camada 2 com autenticação RSA.
  - **IPSEC XAUTH PSK:** Internet Protocol Security com chave pré-compartilhada e autenticação estendida.
  - **IPSEC HYBRID RSA:** Internet Protocol Security com autenticação RSA híbrida.
  - **PPTP:** Encapsulamento Ponto a Ponto.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Definir as configurações do L2TP PSK para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **L2TP secreto:** digite a chave secreta compartilhada.
- **Identificador IPSec:** digite o nome da conexão VPN que os usuários veem nos respectivos dispositivos quando se conectam.
- **Chave pré-compartilhada IPSec:** digite a chave secreta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações do L2TP RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **L2TP secreto:** digite a chave secreta compartilhada.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Certificado CA:** na lista, clique no certificado de AC a ser usado.
- **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC XAUTH PSK para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Identificador IPSec:** digite o nome da conexão VPN que os usuários veem nos respectivos dispositivos quando se conectam.
- **Chave pré-compartilhada IPSec:** digite a chave secreta compartilhada.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC AUTH RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Certificado CA:** na lista, clique no certificado de AC a ser usado.
- **Credencial de identidade:** na lista, clique na credencial de identidade a ser usada.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC HYBRID RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Certificado CA:** na lista, clique no certificado de AC a ser usado.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de PPTP para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Criptografia PPP (MPPE):** selecione se a criptografia de dados deve ser ativada com o Microsoft Point-to-Point Encryption (MPPE). O padrão é **Off**.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
  - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
  - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Política de dispositivo de papel de parede

April 15, 2019

Você pode adicionar um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio ou na tela inicial de um dispositivo iOS, ou em ambas. Disponível no iOS 7.1.2 e versões posteriores. Para usar papéis de parede diferentes em iPads e iPhones, você precisa criar políticas diferentes de papéis de parede e implantá-las nos usuários apropriados.

A tabela a seguir lista a recomendação da Apple para dimensões de imagem para dispositivos iOS.

Dispositivo	Dimensões da imagem em pixels
iPhone 5, 5c, 5s	640 x 1136
iPhone 6, 6s	750 x 1334
iPhone 6 Plus	1080 x 1920
iPad Air, 2	1536 x 2048
iPad 4, 3	1536 x 2048

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dispositivo	Dimensões da imagem em pixels
iPad Mini 2, 3	1536 x 2048

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de 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 deverá ser exibido.
- **Arquivo de papel de parede:** selecione o arquivo de papel de parede clicando em **Procurar** e navegando até a localização do arquivo.

Política de dispositivo de filtro de conteúdo Web

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para filtrar conteúdo Web nos dispositivos iOS usando a função de filtro automático da Apple em conjunto com sites específicos que você adiciona a listas brancas e listas negras. Essa política está disponível somente nos dispositivos iOS 7.0 e versões 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.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Tipo de filtro:** na lista, clique em **Interno** ou **Plug-in**, e siga os procedimentos a seguir da opção que você escolher. O padrão é **Interno**.

Tipo de filtro interno

- **Filtro de conteúdo Web**
  - **Filtro automático ativado:** se a função de filtro automático da Apple deve ou não ser usada para analisar sites de conteúdo impróprio. O padrão é **Off**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **URLs permitidas:** essa lista será ignorada quando a opção **Filtro automático ativado** estiver definida como **O**. Quando **Filtro automático ativado** estiver definido como **I**, os itens nessa lista estarão sempre acessíveis, mesmo que o filtro automático permita ou não o acesso. Para cada URL que você desejar adicionar à lista branca, 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 branca ou clique em **Cancelar** para não salvá-lo.
  - **URLs na lista negra:** os itens nessa lista são sempre bloqueados. Para cada URL que você desejar adicionar à lista negra, clique em **Adicionar** e faça o seguinte:
    * Digite a 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 negra ou clique em **Cancelar** para não salvá-lo.
- **Lista branca de indicadores**
  - **Lista branca de indicadores:** especifica os sites que os usuários podem acessar. Para ativar o acesso a sites da web, adicione a URL.
    * **URL:** a URL de cada site que os usuários podem acessar. Por exemplo, para habilitar o acesso ao armazenamento do Secure Hub, adicione a 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 indicadores:** digite um nome de pasta de indicadores opcional. Se esse campo for deixado em branco, o marcador será adicionado ao diretório de marcadores padrão.
    * **Título:** digite um título descritivo para o site. Por exemplo, digite "Google" para a URL `https://google.com`.
    * Clique em **Salvar** para salvar o site na lista branca ou clique em **Cancelar** para não salvá-lo.

Tipo de filtrode plug-in

- **Nome do filtro:** insira um nome exclusivo para o filtro.
- **Identificador:** insira o ID de 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 de host ou URL.
- **Nome de usuário:** insira um nome de usuário opcional para o serviço.
- **Senha:** insira uma senha opcional para o serviço.
- **Certificado:** na lista, clique em um certificado de identidade opcional a ser usado para auten-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ticar o usuário no serviço. O padrão é **Nenhum**.

- **Filtrar o tráfego de WebKit:** selecione se o tráfego de WebKit deve ser filtrado.
- **Filtrar o tráfego de soquete:** selecione se o tráfego de soquete deve ser filtrado.
- **Dados personalizados:** para cada chave personalizada que você desejar adicionar ao filtro da Web, clique em **Adicionar** e 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.

Política de dispositivo de clipe Web

April 15, 2019

Você pode inserir atalhos ou clipes Web em sites para que apareçam junto aos aplicativos nos dispositivos de usuários. Você pode especificar seus próprios ícones para representar os clipes Web para dispositivos iOS, Mac OS X e Android; o Tablet Windows requer somente um rótulo e uma URL.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações de iOS

- **Rótulo:** digite o rótulo que deve ser exibido com o clipe Web.
- **URL:** digite a URL associado ao clipe Web. A URL deve começar com um protocolo, por exemplo, `https://server`.
- **Removível:** selecione se os usuários podem remover o clipe Web. O padrão é **Off**.
- **Ícone a ser atualizado:** selecione o ícone a ser usado para o clipe Web clicando em **Procurar** e navegando até a localização do arquivo.
- **Ícone pré-composto:** selecione se o ícone tem efeitos (cantos arredondados, sombra e brilho reflexivo) aplicados a ele. O padrão é **O**, o que adiciona os efeitos.
- **Tela inteira:** selecione se a página da Web vinculada é aberta no modo de tela inteira. O padrão é **Off**.

Configurações do macOS

- **Rótulo:** digite o rótulo que deve ser exibido com o clipe Web.
- **URL:** digite a URL associado ao clipe Web. A URL deve começar com um protocolo, por exemplo, `https://server`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Ícone a ser atualizado:** selecione o ícone a ser usado para o clipe Web clicando em Procurar e navegando até a localização do arquivo.

Configurações do Android

- **Regra:** selecione se essa política adiciona ou remove um clipe Web. O padrão é **Adicionar**.
- **Rótulo:** digite o rótulo que deve ser exibido com o clipe Web.
- **URL:** digite a URL associado ao clipe Web.
- **Definir um ícone:** selecione se um arquivo de ícone deve ser usado. O padrão é **Off**.
- **Arquivo de ícone:** se a opção **Definir um ícone** estiver definida como **I**, selecione o arquivo de ícone a ser usado clicando em **Procurar** e navegando até a localização do arquivo.

Configurações do Windows Desktop/Tablet

- **Nome:** digite o rótulo que deve ser exibido com o clipe Web.
- **URL:** digite a URL associado ao clipe Web.

Política de dispositivo de WiFi

April 15, 2019

Crie políticas de dispositivo de WiFi novas ou existentes no XenMobile usando a página **Configurar > Políticas de dispositivo**. Políticas de WiFi permitem gerenciar como os usuários conectam seus dispositivos a redes WiFi, definindo os itens a seguir:

- Nomes e tipos de redes
- Políticas de autenticação e segurança
- Uso de servidores proxy
- Outros detalhes relacionados a WiFi

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Pré-requisitos

Antes de criar uma política, conclua estas etapas:

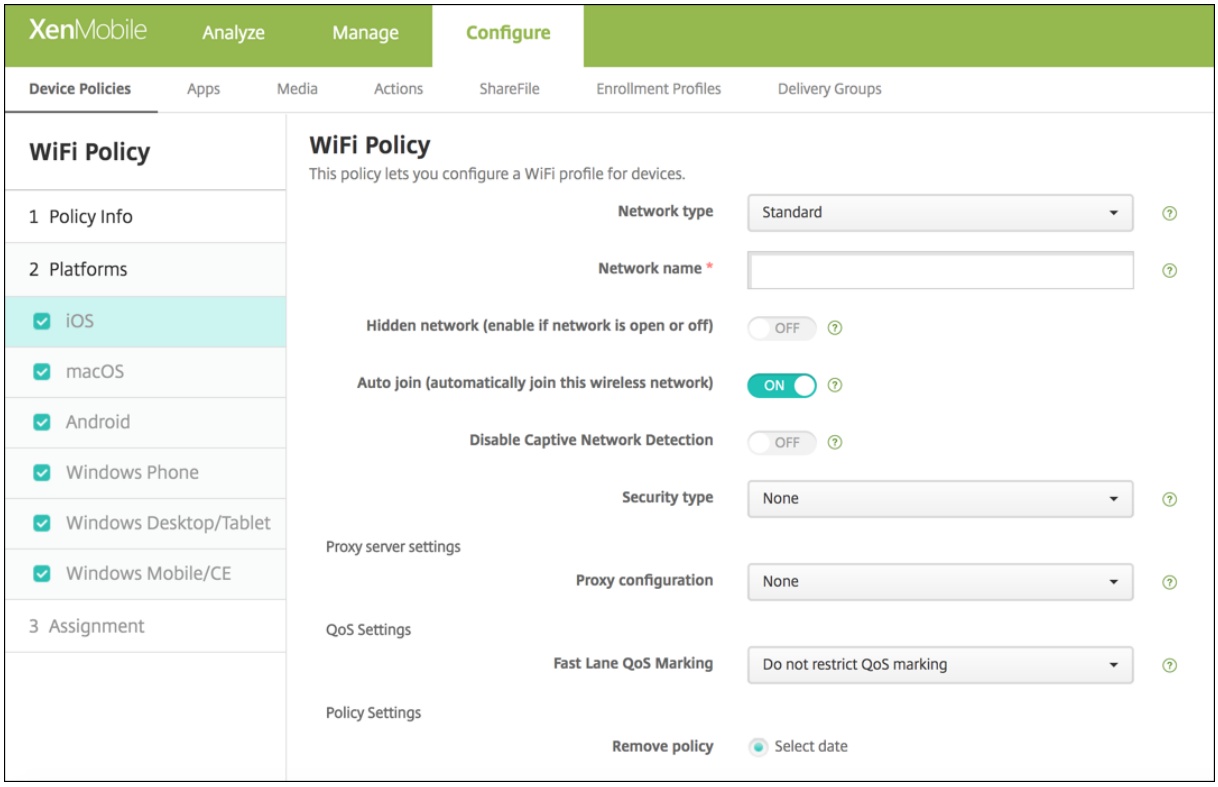
- Crie os grupos de entrega que você planeja usar.
- Conheça o nome e o tipo de rede.
- Conheça os tipos de autenticação ou segurança que você planeja usar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Conheça as informações do servidor proxy que podem ser necessárias.
- Instale todos os certificados AC necessários.
- Tenha as chaves compartilhadas necessárias.
- Crie a entidade PKI de autenticação baseada em certificado.
- Configure os provedores de credenciais.

Para obter mais informações, consulte Autenticação e os sub-artigos.

Configurações de iOS



- **Tipo de rede:** na lista, clique em **Padrão**, **Ponto de acesso legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da rede:** digite o SSID que é exibido na lista de redes disponíveis do dispositivo. Não se aplica ao **Hotspot 2.0**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Ingressar automaticamente (ingressar automaticamente nesta rede sem fio):** escolha se o ingresso na rede é automático. O padrão é **On**.
- **Tipo de segurança:** na lista, clique no tipo de segurança que você planeja usar. Não se aplica ao **Hotspot 2.0**.
  - Nenhum - não requer configuração adicional.
  - WEP

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - WPA/WPA2 Pessoal
  - Qualquer (Pessoal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP. Em seguida, o XenMobile pode enviar o certificado a dispositivos para autenticação no servidor WiFi. Para configurar o SCEP, vá para a página Distribuição de **Configurações > Provedores de credenciais**. Para obter mais informações, consulte Provedores de credenciais.
  - Qualquer (Enterprise)

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações WPA, WPA Pessoal, Qualquer (pessoal) para iOS

Senha: digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

Configurações WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para iOS

Quando você escolhe qualquer uma dessas configurações, as respectivas configurações são listadas após **Configurações do servidor proxy**.

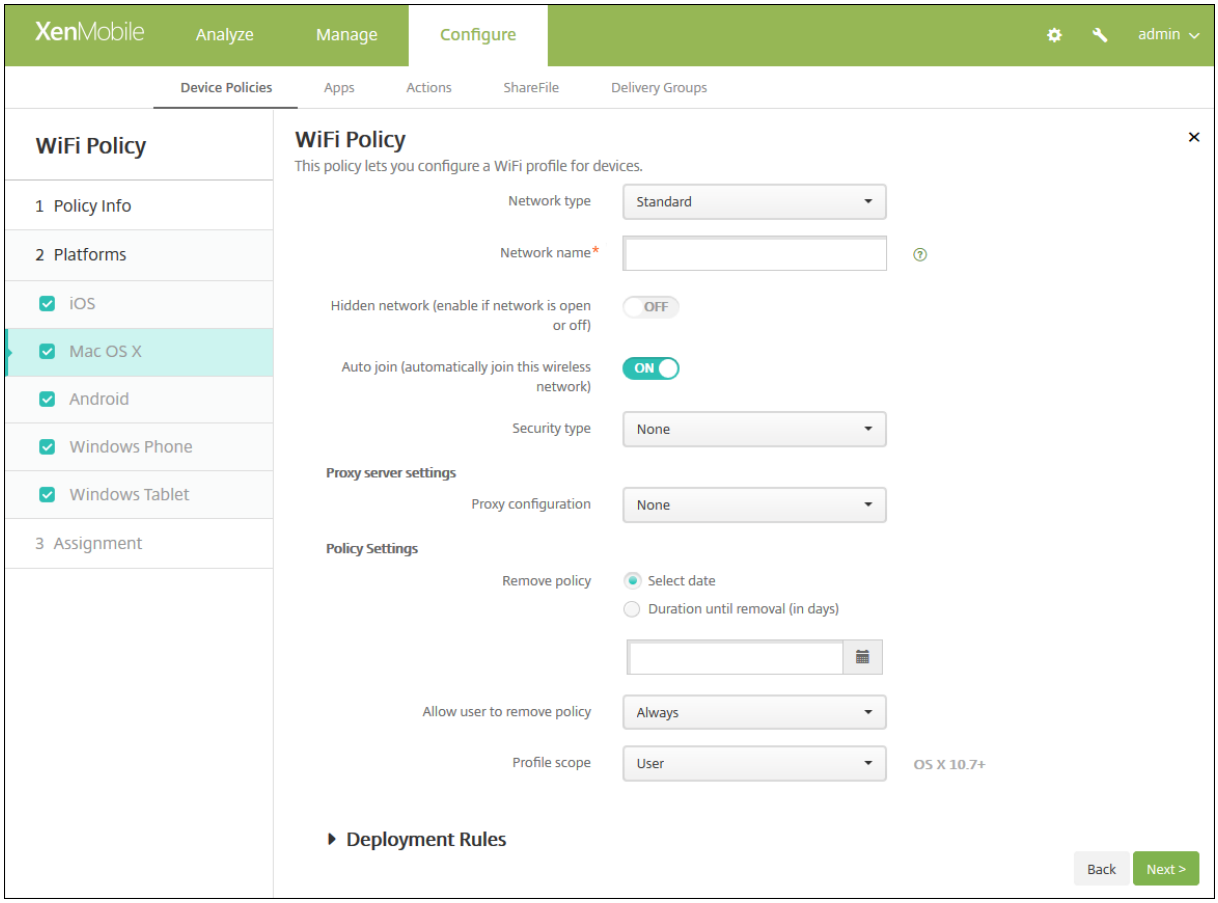
- **Protocolos, tipos de EAP aceitos:** ative os tipos de EAP aos quais você deseja dar suporte e defina as configurações associadas. O padrão é **Off** para cada tipo de EAP disponível.
- **Autenticação interna (TTLS):** *obrigatório somente quando você ativa TTLS*. Na lista, escolha método de autenticação interno a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** escolha se deseja usar as credenciais de acesso protegido (PACs).
  - Se você escolher **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
    * Se você escolher **Provisionamento de PAC**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
      · **Provisionamento de PAC anônimo**
- **Autenticação:**
  - **Nome de usuário:** digite um nome de usuário.
  - **Senha por conexão:** escolha se deve ser exigida uma senha toda vez que os usuários fizerem login.
  - **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.
  - **Credencial de identidade (keystore ou credencial PKI):** na lista, escolha o tipo de credencial de identidade. O padrão é **Nenhum**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - **Identidade externa:** *obrigatório somente quando você ativa* **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 do usuário não possa ser visto.
  - **Exigir um certificado TLS:** escolha se deseja exigir o certificado TLS.
- **Confiança**
  - **Certificados confiáveis:** para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que você deseja adicionar, faça o seguinte:
    * **Aplicativo:** na lista, escolha o aplicativo que você deseja adicionar.
    * Clique em **Salvar** para salvar o certificado ou em **Cancelar**.
  - **Nomes de certificados de servidor confiáveis:** para adicionar nomes comuns de certificado de servidores confiáveis, clique em **Adicionar** e, para cada nome que você deseja adicionar, adicione o seguinte:
    * **Certificado:** digite o nome do certificado do servidor. Você pode usar curingas para especificar o nome, como wpa.*.exemplo.com.
    * Clique em **Salvar** para salvar o nome do certificado ou em **Cancelar**.
- **Permitir exceções de confiança:** escolha se a caixa de diálogo de confiança do certificado será exibida nos dispositivos de usuários quando um certificado não for confiável. O padrão é **On**.
- **Configurações do servidor proxy**
  - **Configuração de proxy:** na lista, escolha **Nenhum**, **Manual** ou **Automático** para definir como a conexão VPN cria rotas em um servidor proxy e configure todas as opções adicionais. O padrão é **Nenhum**, que não requer configuração adicional.
  - Se você escolher **Manual**, defina as seguintes configurações:
    * **Nome do host/endereço IP:** digite o nome do host ou endereço IP do servidor proxy.
    * **Porta:** digite o número de porta do servidor proxy.
    * **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
    * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
  - Se você escolher **Automático**, defina as seguintes configurações:
    * **URL do servidor:** digite a URL do arquivo PAC que define a configuração de proxy.
    * **Permitir conexão direta se o PAC estiver inacessível:** escolha se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do macOS



- **Tipo de rede:** na lista, clique em **Padrão**, **Ponto de acesso legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da rede:** digite o SSID que é exibido na lista de redes disponíveis do dispositivo. Não se aplica ao **Hotspot 2.0**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Ingressar automaticamente (ingressar automaticamente nesta rede sem fio):** escolha se o ingresso na rede é automático. O padrão é **On**.
- **Tipo de segurança:** na lista, clique no tipo de segurança que você planeja usar. Não se aplica ao **Hotspot 2.0**.
  - Nenhum - não requer configuração adicional.
  - WEP
  - WPA/WPA2 Pessoal
  - Qualquer (Pessoal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Qualquer (Enterprise)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações WPA, WPA Pessoal, Qualquer (Pessoal) para macOS

- **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

Configurações WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para macOS

Quando você escolhe qualquer uma dessas configurações, as respectivas configurações são listadas após **Configurações do servidor proxy**.

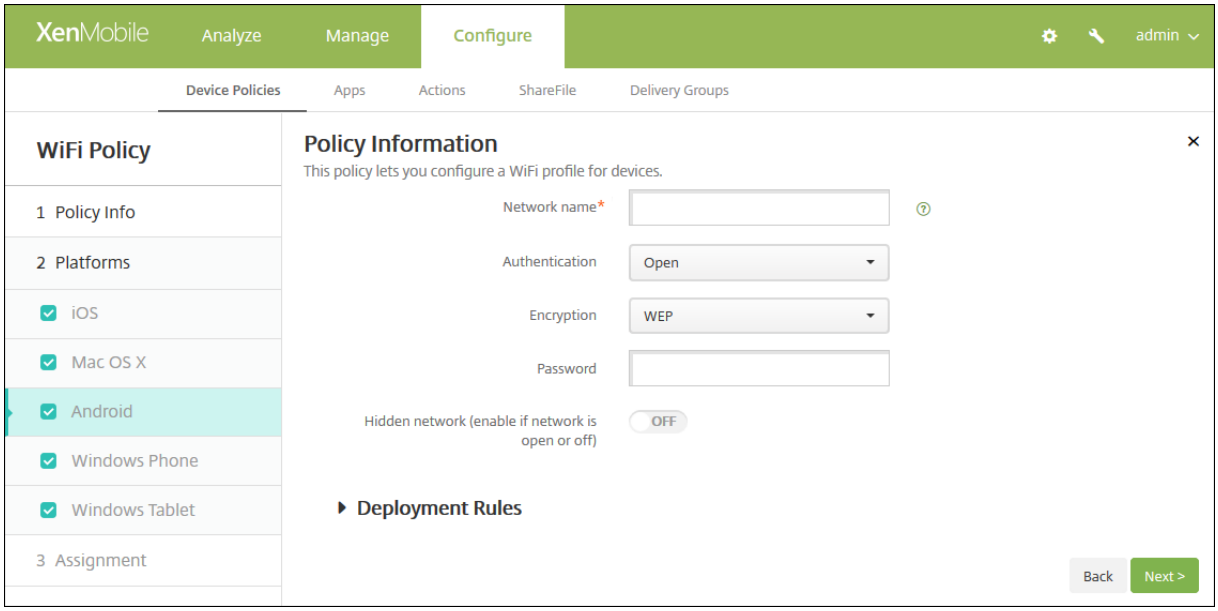
- **Protocolos, tipos de EAP aceitos:** ative os tipos de EAP aos quais você deseja dar suporte e defina as configurações associadas. O padrão é **Off** para cada tipo de EAP disponível.
- **Autenticação interna (TTLS):** *obrigatório somente quando você ativa TTLS*. Na lista, escolha método de autenticação interno a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** escolha se deseja usar as credenciais de acesso protegido (PACs).
  - Se você selecionar **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
    * Se você escolher **Provisionamento de PAC**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
      · **Provisionamento de PAC anônimo**
- **Autenticação:**
  - **Nome de usuário:** digite um nome de usuário.
  - **Senha por conexão:** escolha se deve ser exigida uma senha toda vez que os usuários fizerem login.
  - **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.
  - **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 ativa* **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 do usuário não possa ser visto.
  - **Exigir um certificado TLS:** escolha se deseja exigir o certificado TLS.
- **Confiança**
  - **Certificados confiáveis:** para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que você deseja adicionar, faça o seguinte:
    * **Aplicativo:** na lista, escolha o aplicativo que você deseja adicionar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

        * Clique em **Salvar** para salvar o certificado ou em **Cancelar**.
    - **Nomes de certificados de servidor confiáveis:** para adicionar nomes comuns de certificado de servidores confiáveis, clique em **Adicionar** e, para cada nome que você deseja adicionar, adicione o seguinte:
        * **Certificado:** digite o nome do certificado do servidor que você deseja adicionar. Você pode usar curingas para especificar o nome, como wpa.*.exemplo.com.
        * Clique em **Salvar** para salvar o nome do certificado ou em **Cancelar**.
- **Permitir exceções de confiança:** escolha se a caixa de diálogo de confiança do certificado será exibida nos dispositivos do usuário quando um certificado não for confiável. O padrão é **On**.
- **Usar como configuração de janela de login:** escolha se deseja usar as mesmas credenciais que inseriu 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 cria rotas em um servidor proxy e configure todas as opções adicionais. O padrão é **Nenhum**, que não requer configuração adicional.
    - Se você escolher **Manual**, defina as seguintes configurações:
        * **Nome do host/endereço IP:** digite o nome do host ou endereço IP do servidor proxy.
        * **Porta:** digite o número de porta do servidor proxy.
        * **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
        * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
    - Se você escolher **Automático**, defina as seguintes configurações:
        * **URL do servidor:** digite a URL do arquivo PAC que define a configuração de proxy.
        * **Permitir conexão direta se o PAC estiver inacessível:** escolha se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Android



- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão de WiFi.
  - Aberto
  - Compartilhado
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

As seções a seguir listam as opções de configuração de 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

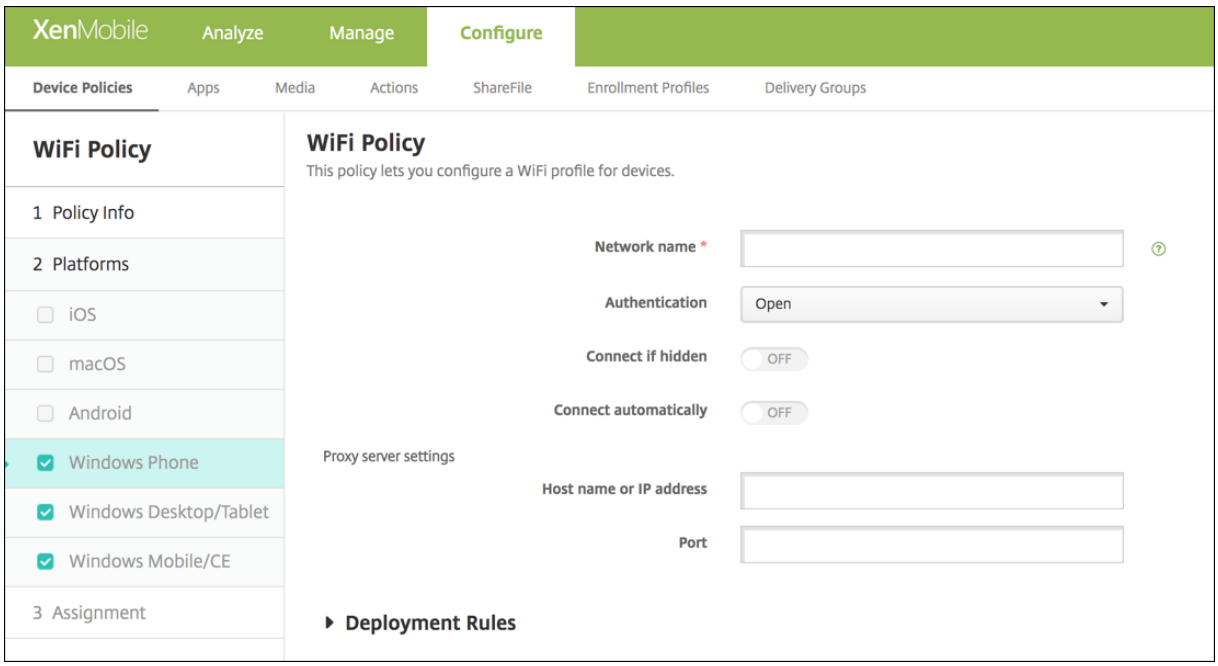
- **Criptografia:** na lista, escolha **TKIP** ou **AES**. O padrão é **TKIP**.
- **Senha:** digite uma senha opcional.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações 802.1x para Android

- **Tipo de EAP:** na lista, escolha **PEAP**, **TLS** ou **TTLS**. O padrão é **PEAP**.
- **Senha:** digite uma senha opcional.
- **Autenticação fase 2:** na lista, clique em **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, visível externamente. Você pode aumentar a segurança digitando um termo genérico como “anônimo” para que o nome do usuário não possa ser visto.
- **Certificado de 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 (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.

Configurações do Windows Phone



- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão de WiFi.
  - Aberto
  - WPA Pessoal
  - WPA-2 Pessoal
  - WPA-2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP. A configuração de SCEP permite que o XenMobile envie

© 1999-2019 Citrix Systems, Inc. All rights reserved.

o certificado a dispositivos para autenticação no servidor WiFi. Para configurar o SCEP, vá para a página **Distribuição** de **Configurações > Provedores de credenciais**. Para obter mais informações, consulte Provedores de credenciais.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows Phone

- **Conectar se a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows Phone

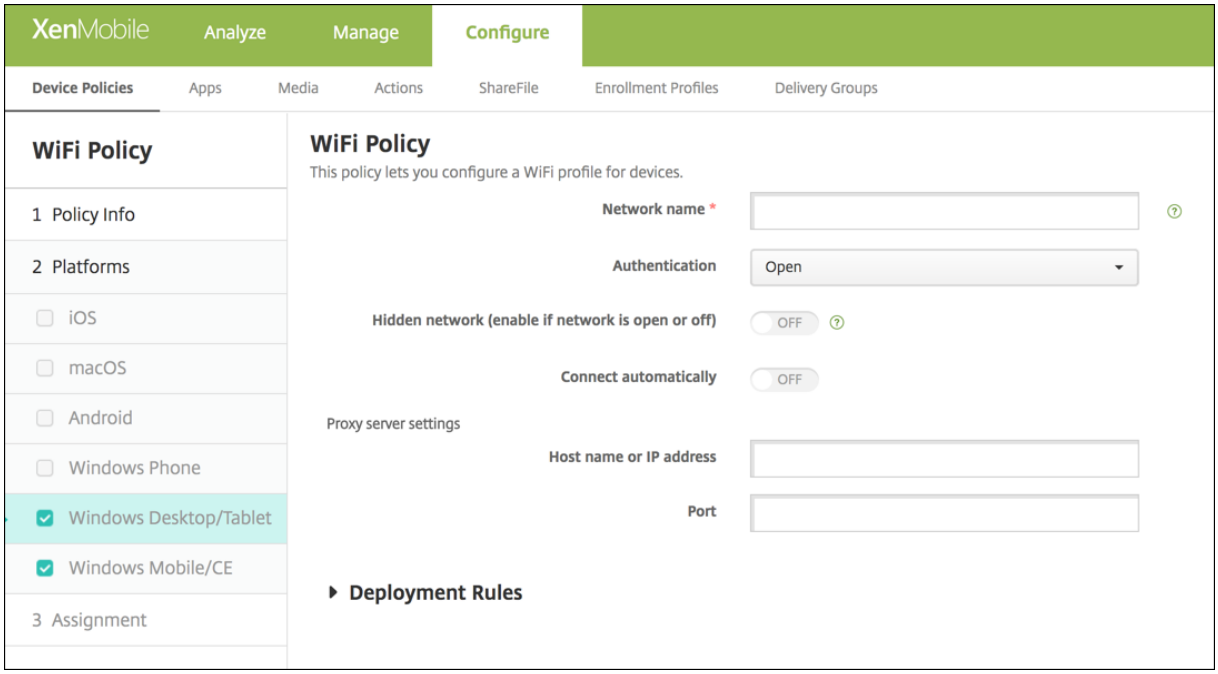
- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Conectar se a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows Phone

- **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 a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários via protocolo SCEP.
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.
- **Configurações do servidor proxy**
  - **Nome do host ou endereço IP:** digite o nome ou endereço IP do servidor proxy.
  - **Porta:** digite o número da porta do servidor proxy.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows 10



- **Autenticação:** na lista, clique no tipo de segurança para usar com a conexão de WiFi.
  - Aberto
  - WPA Pessoal
  - WPA-2 Pessoal
  - WPA Enterprise
  - WPA-2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP. A configuração de SCEP permite que o XenMobile envie o certificado a dispositivos para autenticação no servidor WiFi. Para configurar o SCEP, vá para a página **Distribuição** de **Configurações > Provedores de credenciais**. Para obter mais informações, consulte Provedores de credenciais.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows 10

- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows 10

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.

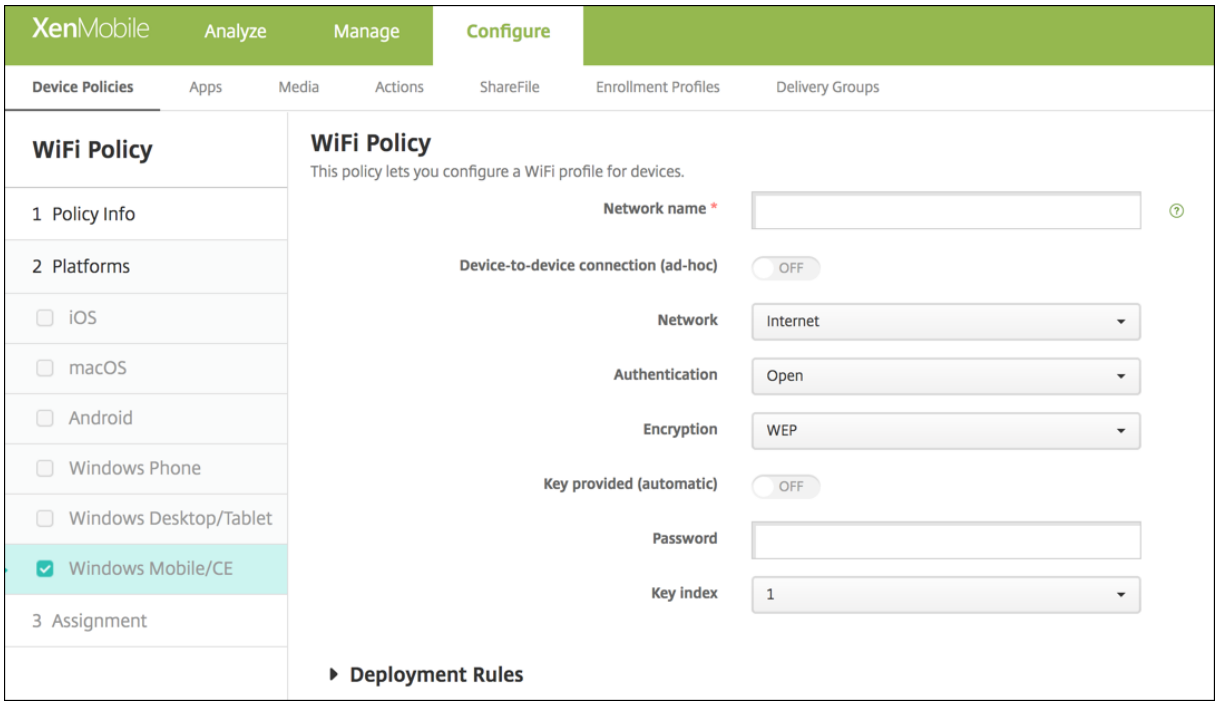
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows 10

- **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 a rede estiver oculta:** escolha se a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários usando o protocolo SCEP.
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.

Configurações do Windows Mobile/CE



- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Conexão de dispositivo a dispositivo (ad-hoc):** permite que dois dispositivos se conectem diretamente. O padrão é **Desativado**.
- **Rede:** escolha se o dispositivo está conectado a uma fonte de internet externa ou a uma intranet de escritório.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão de WiFi.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Aberto
- WPA Pessoal
- WPA-2 Pessoal
- WPA-2 Enterprise

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows Mobile/CE

- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows Mobile/CE

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows Mobile/CE

- **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 a rede estiver oculta:** escolha se a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários usando o protocolo SCEP.
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.
- **Chave fornecida (automática):** escolha se a chave fornecida é automaticamente ou não. O padrão é **Desativado**.
- **Senha:** digite a senha nesse campo.
- **Índice de chave:** escolha o índice de chave. As opções disponíveis são **1**, **2**, **3** e **4**.

Política de dispositivo do certificado do Windows CE

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Você pode criar uma política de dispositivo no XenMobile para criar e fornecer certificados do Windows Mobile/CE de uma PKI externa para os dispositivos de usuários. Para obter mais informações sobre certificados e entidades PKI, consulte Certificados.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows CE

- **Provedor de credenciais:** na lista, clique no provedor de credenciais. O padrão é **Nenhum**.
- **Senha gerada no formato PKCS#12:** digite a senha usada para criptografar as credenciais.
- **Pasta de destino:** na lista, clique na pasta de destino da credencial ou em **Adicionar novo** para adicionar uma pasta ainda não presente na lista. As opções predefinidas são:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Nome do arquivo de destino:** digite o nome do arquivo de credencial.

Política de dispositivo Proteção de informações do Windows

April 15, 2019

A Proteção de informações do Windows (WIP), conhecida anteriormente como proteção de dados empresariais (EDP), é uma tecnologia do Windows que oferece proteção contra o possível vazamento de dados corporativos. Vazamentos de dados podem ocorrer por meio do compartilhamento de dados empresariais com aplicativos protegidos não corporativos, entre aplicativos ou fora da rede da sua organização. Para obter mais informações, consulte Proteger os dados empresariais usando a Proteção de Informações do Windows (WIP) no Microsoft TechNet.

Você pode criar uma política de dispositivo no XenMobile para especificar os aplicativos que requerem Proteção de informações do Windows no nível de execução que você definir. A política Proteção de informações do Windows é para telefones, tablets e desktops supervisionados Windows 10 versão 1607 e posteriores.

O XenMobile inclui alguns aplicativos comuns, e você pode adicionar outros. Especifique para a política um nível de execução que afete a experiência do usuário. Por exemplo, você pode:

- Bloquear qualquer compartilhamento de dados impróprio.
- Avisar sobre o compartilhamento de dados impróprio e permitir que os usuários substituam a política.

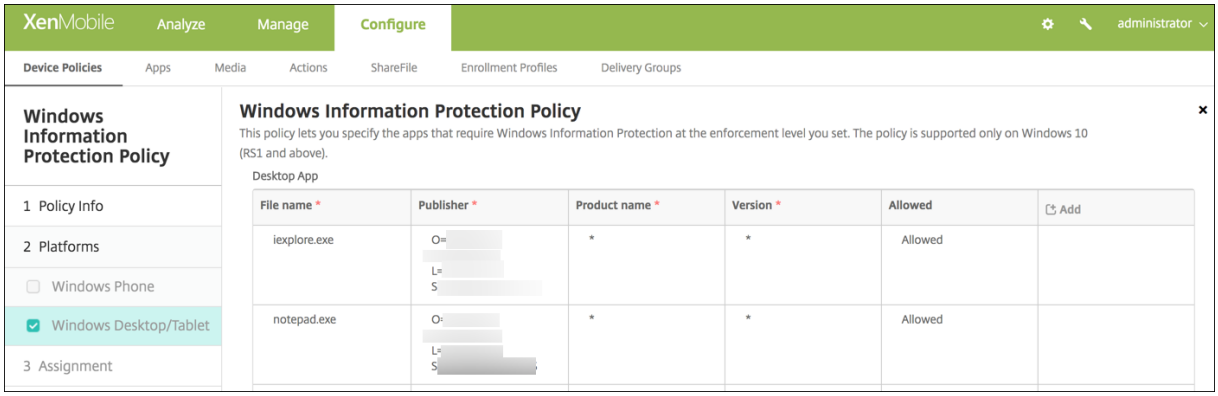
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Execute o WIP silenciosamente enquanto registra o log e permite o compartilhamento de dados impróprios.

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 essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Configurações do Windows 10



- **Aplicativo de área de trabalho** (Tablet Windows 10), **Aplicativo da loja** (telefone e tablet Windows 10): o XenMobile inclui alguns aplicativos comuns, como mostra o exemplo acima. 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 que apresentam problemas de compatibilidade com a WIP. Para excluir esses aplicativos da WIP, clique em **Procurar** para carregar a lista. O XenMobile combina o AppLocker XML carregado e os aplicativos de área de trabalho e loja configurados na política enviada ao dispositivo. Para obter mais informações, consulte Recommended deny list for Windows Information Protection.
  - **Nível de execução:** selecione uma opção para especificar como você deseja que a Proteção de informações do Windows proteja e gerencie o compartilhamento de dados. O padrão é **Desativado**.
    * **0-Desl.:** A WIP está desativada e não protege ou audita seus dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

    * **1-Silencioso:** A WIP é executada silenciosamente, registra o compartilhamento impróprio de dados e não bloqueia nada. Você pode acessar os logs por meio de Reporting CSP.
    * **2-Substituir:** A WIP avisa os usuários sobre o compartilhamento de dados potencialmente não seguros. Os usuários podem substituir avisos e compartilhar os dados. Esse modo registra ações, incluindo substituições de usuários, no log de auditoria.
    * **3-Bloquear:** A WIP impede que os usuários concluam o compartilhamento de dados potencialmente não seguros.

- **Nomes de domínio protegidos:** os domínios que a sua empresa utiliza para identidades de usuários. Essa lista de domínios de identidade gerenciados, junto com o domínio primário, compõem a identidade da sua corporação de gerenciamento. O primeiro domínio da lista é a identidade corporativa principal usada na interface de usuário do Windows. Use "|" para separar itens de lista. Por exemplo: `domain1.com | domain2.com`
- **Certificado de recuperação de dados:** clique em **Procurar** e depois selecione um certificado de recuperação para uso na recuperação de dados de arquivos criptografados. Esse certificado é o mesmo que o certificado do agente de recuperação de dados (DRA) do sistema de arquivos de criptografia (EFS), entregue somente por meio do MDM em vez de pela 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 constituem os limites da empresa. A WIP protege todo o tráfego para os domínios totalmente qualificados nessa lista. Essa configuração, junto com a configuração **Faixa de IP**, detecta se um ponto de extremidade de rede é corporativo ou pessoal em redes privadas. Use uma vírgula para separar itens de lista. Por exemplo: corp.example.com,region.example.com
- **Faixa de IP:** uma lista das faixas de IPv4 e IPv6 corporativos que definem os computadores na rede corporativa. A WIP considera esses locais um destino seguro para o compartilhamento de dados corporativos. Use uma vírgula para separar itens de lista. Por exemplo:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **A lista de faixas de IP é determinante:** para impedir a detecção automática de intervalos IP pelo Windows, altere essa configuração para **Ativado**. O padrão é **Desativado**.
- **Servidores proxy:** uma lista de servidores proxy que a empresa pode usar para recursos corporativos. Essa configuração será necessária se você usar um proxy na rede. Sem um

© 1999-2019 Citrix Systems, Inc. All rights reserved.

servidor proxy, os recursos corporativos poderão ficar indisponíveis quando um cliente estiver atrás de um proxy. Por exemplo, recursos podem estar indisponíveis em determinados pontos de acesso WiFi em hotéis e restaurantes. Use uma vírgula para separar itens de lista. Por exemplo:

```
proxy.example.com:80;157.54.11.118:443
```

- **Servidores proxy internos:** uma lista de servidores proxy pelos quais os seus dispositivos passam para acessar seus recursos de nuvem. Usar esse tipo de servidor indica que os recursos de nuvem com os quais você está se conectando são recursos corporativos. Não inclua nessa lista nenhum dos servidores na configuração de **Servidores proxy** que sejam usados para o tráfego não protegido pela WIP. Use uma vírgula para separar itens de lista. Por exemplo:

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- **Recursos de nuvem:** uma lista de recursos de nuvem protegidos pela WIP. Para cada recurso de nuvem, você também pode especificar um servidor proxy na lista de **Servidores proxy** para rotear o tráfego para esse recurso de nuvem. Todo o tráfego roteado através de **Servidores proxy** é tratado como tráfego corporativo. Use uma vírgula para separar itens de lista. Por exemplo:

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- **Definir exigência de proteção após travamento:** somente para telefones Windows 10. Se for **Ativado**, a política de dispositivo de código secreto também será necessária. Caso contrário, a implantação da política de Proteção de informações do Windows falhará. Além disso, se essa política for **Ativada**, a configuração **Exigir proteção durante bloqueio** será exibida. O padrão é **Desativado**.

- **Exigir proteção durante bloqueio:** somente para telefones Windows 10. Especifica se é preciso criptografar dados corporativos usando uma chave protegida por um PIN de funcionário em um dispositivo bloqueado. Aplicativos não podem ler dados corporativos em um dispositivo bloqueado. O padrão é **Ativado**.

- **Revogar o certificado WIP ao cancelar registro:** especifica se as chaves de criptografia locais de um dispositivo de usuário serão ou não revogadas quando seu registro for cancelado da Proteção de informações do Windows. Depois que as chaves de criptografia forem revogadas, um usuário não poderá acessar dados corporativos criptografados. Se for **Desativado**, as chaves não serão revogadas, e o usuário continuará a ter acesso a arquivos protegidos após o cancelamento do registro. O padrão é **Ativado**.

- **Exibir ícones de sobreposição:** especifica se é necessário incluir a sobreposição de ícones da Proteção de informações do Windows em arquivos corporativos no Explorer e em blocos de aplicativos somente corporativos no menu Iniciar. O padrão é **Desativado**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Criar um certificado de recuperação de dados

Um certificado de recuperação de dados é necessário para ativar a política de **Proteção de informações do Windows**.

1. No XenMobile Server, abra um prompt de comando e navegue até uma pasta (diferente de Windows\System32) na qual você deseja criar um certificado.
2. Execute este comando:

   ```
   cipher /r:ESFDRA
   ```

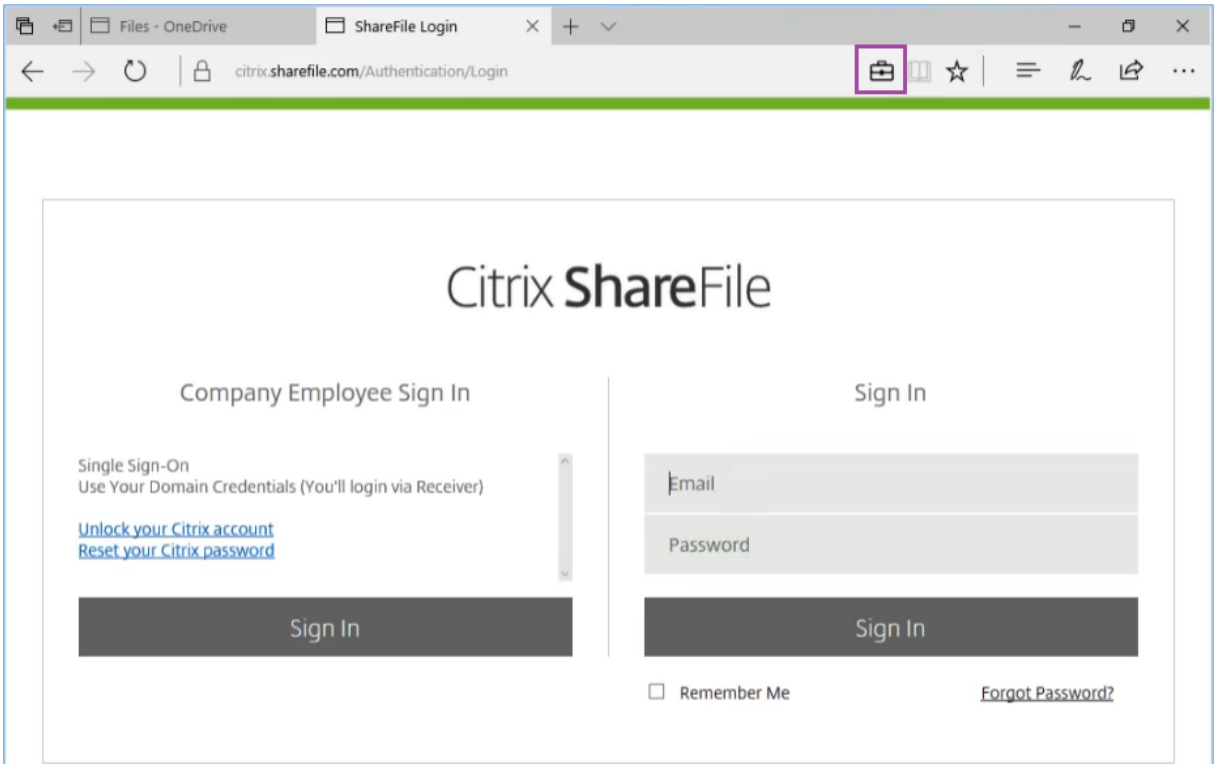
3. Quando solicitado, insira uma senha para proteger o arquivo de chave privada.

   O comando cipher cria um arquivo .cer e .pfx.

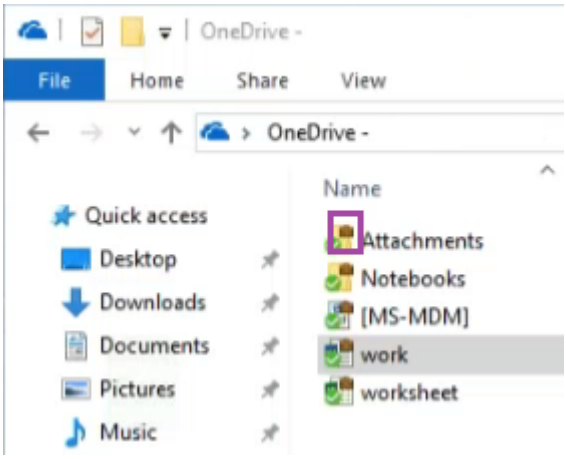
4. No console XenMobile, vá para **Configurações > Certificados** e importe o arquivo .cer, que se aplica a tablets e telefones Windows 10.

Experiência do usuário

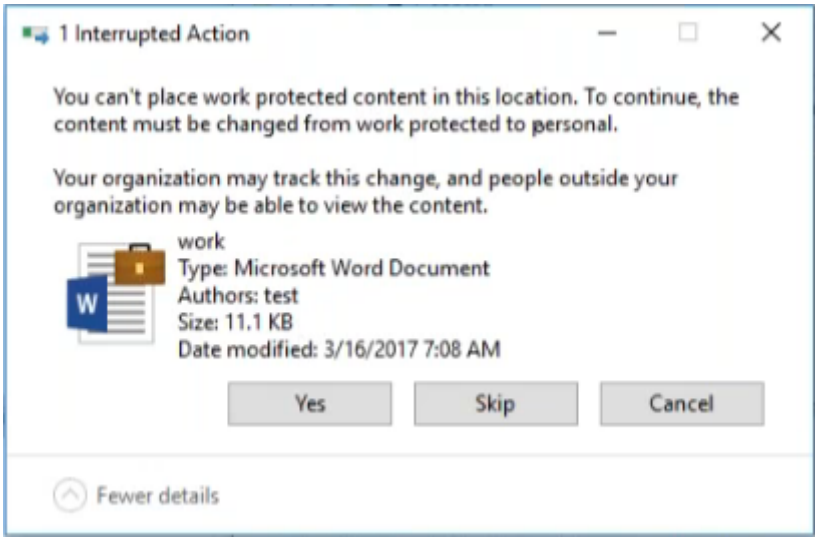
Quando a Proteção de informações do Windows está em vigor, aplicativos e arquivos incluem um ícone:



© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se um usuário copiar ou salvar um arquivo protegido em um local não protegido, a seguinte notificação será exibida, dependendo do nível de execução configurado.



Políticas de dispositivo das opções de XenMobile

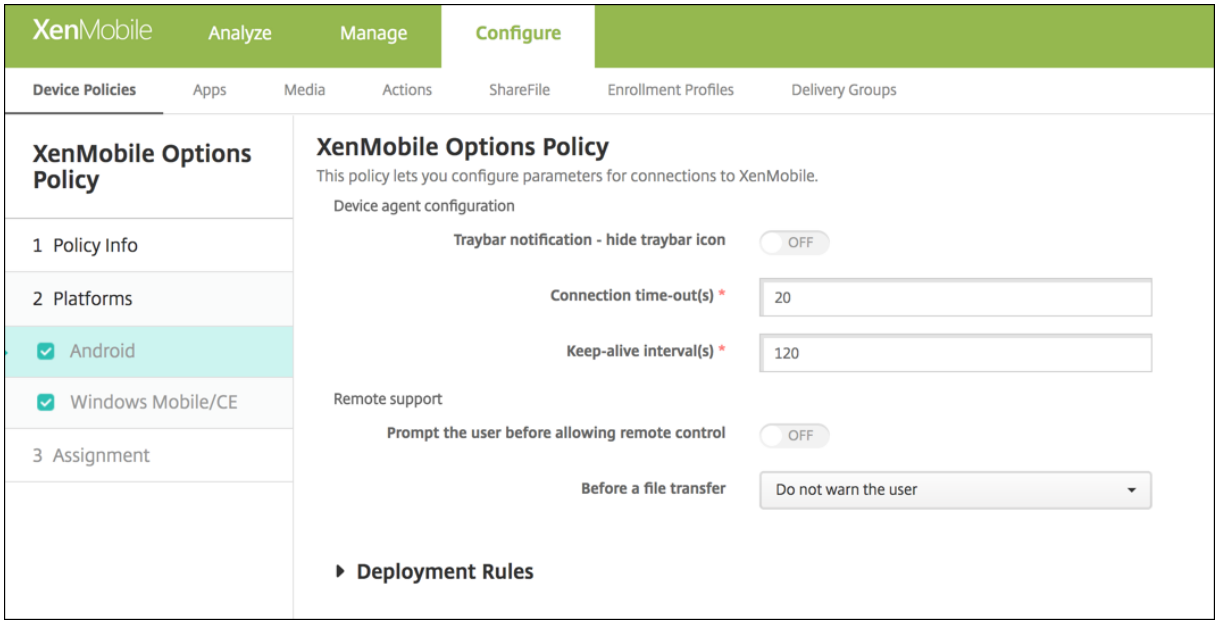
April 15, 2019

Adicione uma política de opções do XenMobile para configurar o comportamento do Secure Hub quando ele se conecta ao XenMobile de dispositivos Android e Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

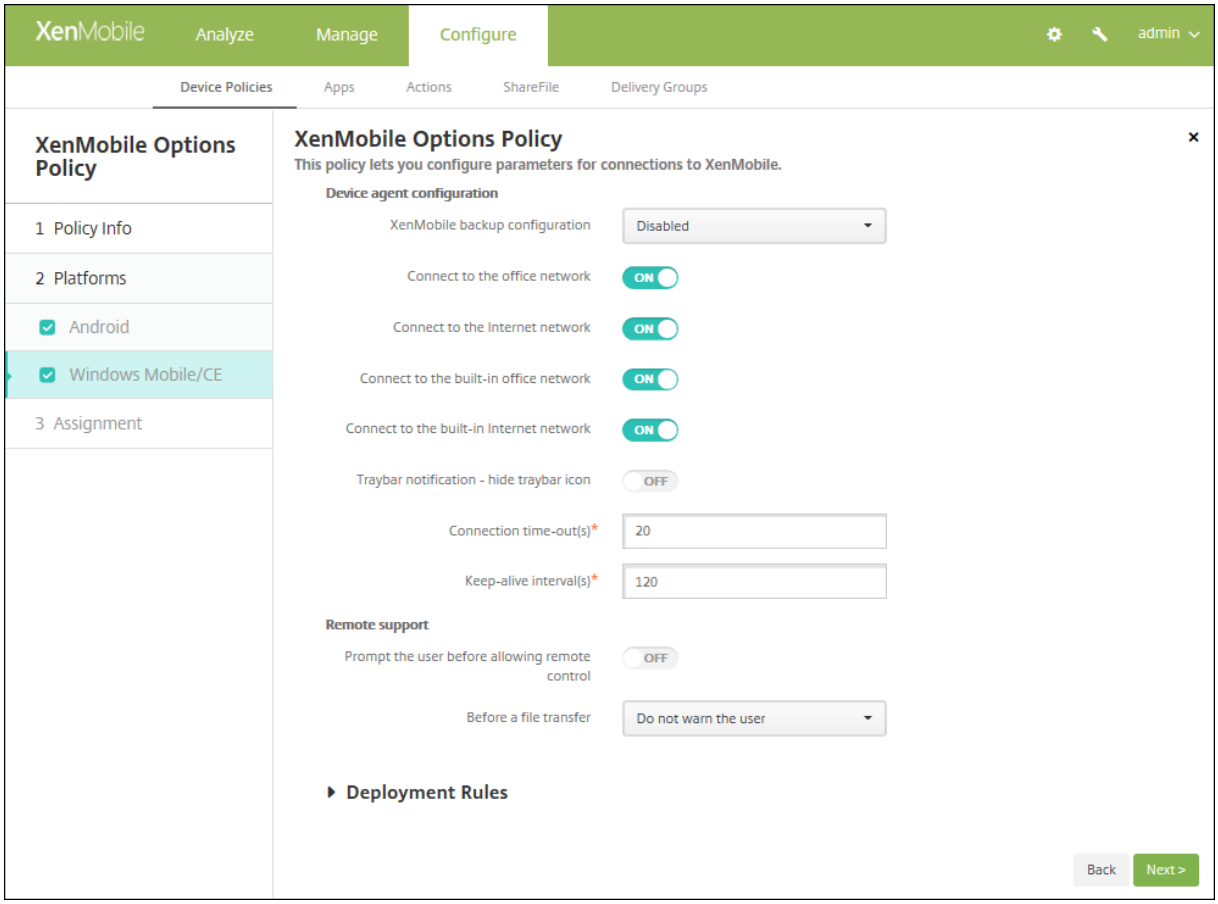
Configurações do Android



- **Notificação da barra da bandeja - ocultar ícone da barra da bandeja:** selecione se o ícone da barra da bandeja está visível ou oculto. O padrão é **Off**.
- **Tempos limites de conexão:** digite o período de tempo, em segundos, que uma conexão pode ficar inativa antes que ela atinja o tempo limite. O padrão é 20 segundos.
- **Intervalos de persistência de conexões:** digite o período de tempo, em segundos, durante o qual uma conexão deve ser mantida aberta. O padrão é 120 segundos.
- **Avisar ao usuário antes de permitir o controle remoto:** selecione se o usuário deve ser perguntado antes de permitir o controle de suporte remoto. O padrão é **Off**.
- **Antes da transferência de um arquivo:** na lista, clique para selecionar se o usuário deve ser alertado sobre uma transferência de arquivo ou se a permissão do usuário deve ser pedida. Valores disponíveis: **Não avisar ao usuário**, **Avisar ao usuário** e **Pedir permissão do usuário**. O padrão é **Não avisar ao usuário**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do Windows Mobile/CE



- **Configuração de agente de dispositivo**
  - **Configuração de backup do XenMobile:** na lista, clique em uma opção para fazer backup da configuração do XenMobile nos dispositivos dos usuários. O padrão é **Desativado**. As opções disponíveis são:
    * Desativado
    * Na primeira conexão após a instalação do XenMobile
    * Na primeira conexão após a reinicialização de cada dispositivo
  - **Conectar à rede do escritório**
  - **Conectar à rede de Internet**
  - **Conectar à rede interna do escritório:** quando essa opção é definida como **I**, o XenMobile detecta automaticamente a rede.
  - **Conectar à rede de Internet interna:** quando essa opção é definida como **I**, o XenMobile detecta automaticamente a rede.
  - **Notificação da barra da bandeja - ocultar ícone da barra da bandeja:** selecione se o ícone da barra da bandeja está visível ou oculto. O padrão é **Off**.
  - **Tempos limites de conexão:** digite o período de tempo, em segundos, que uma conexão

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pode ficar inativa antes que ela atinja o tempo limite. O padrão é 20 segundos.
  - **Intervalos de persistência de conexões:** digite o período de tempo, em segundos, durante o qual uma conexão deve ser mantida aberta. O padrão é 120 segundos.
- **Suporte remoto**
  - **Avisar ao usuário antes de permitir o controle remoto:** selecione se o usuário deve ser perguntado antes de permitir o controle de suporte remoto. O padrão é **Off**.
  - **Antes da transferência de um arquivo:** na lista, clique para selecionar se o usuário deve ser alertado sobre uma transferência de arquivo ou se a permissão do usuário deve ser pedida. Valores disponíveis: **Não avisar ao usuário**, **Avisar ao usuário** e **Pedir permissão do usuário**. O padrão é **Não avisar ao usuário**.

Política de dispositivo de desinstalação do XenMobile

April 15, 2019

Você pode adicionar uma política de dispositivo no XenMobile para desinstalar o XenMobile dos dispositivos Android e Windows Mobile/CE. Quando implantada, essa política remove o XenMobile de todos os dispositivos no grupo de implantação.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte Políticas de dispositivo.

Definir as configurações do Android e do Windows Mobile/CE

- **Desinstalar XenMobile dos dispositivos:** selecione se o XenMobile deve ser desinstalado de cada dispositivo no qual você implantar essa política. O padrão é **Off**.

Adicionar aplicativos

April 15, 2019

Você adiciona aplicativos ao XenMobile para gerenciamento. Você pode adicionar os aplicativos ao console XenMobile, onde pode organizar os aplicativos em categorias e implantar os aplicativos para usuários.

Você pode adicionar os seguintes tipos de aplicativos ao XenMobile:

- **MDX.** Esses aplicativos são preparados com o MDX Toolkit. Implante os aplicativos MDX que você obtém de lojas internas e públicas.
- **Loja de aplicativos pública.** Estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como o iTunes ou o Google Play. Por exemplo, o GoToMeeting.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Web e SaaS.** Esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). Você pode criar seus próprios aplicativos ou escolher de um conjunto de conectores de aplicativo para autenticação de logon único em aplicativos Web existentes. Por exemplo, GoogleApps_SAML.
- **Enterprise.** Estes aplicativos são aplicativos nativos não preparados com o MDX Toolkit e que não contêm as políticas associadas a aplicativos MDX.
- **Link da Web.** Esses aplicativos são endereços Web (URLs) para sites públicos ou privados ou para aplicativos Web que não exigem logon único.

Sobre instalações silenciosas

A Citrix oferece suporte à instalação silenciosa de aplicativos iOS e Android da Samsung. A instalação silenciosa significa que os usuários não são solicitados a instalar aplicativos que você implanta no dispositivo. Os aplicativos são instalados silenciosamente em segundo plano.

Pré-requisitos para implementar a instalação silenciosa:

- Para aplicativos iOS, coloque o dispositivo iOS gerenciado no modo supervisionado. Para obter detalhes, consulte Política de dispositivo de importação do perfil de iOS e macOS.
- Para aplicativos Android, ative políticas para Samsung for Enterprise (SAFE) ou KNOX no dispositivo.

  Para fazer isso, você define a política de dispositivo de chave de licença MDM Samsung para gerar as chaves de licença ELM Samsung e KNOX. Para obter detalhes, consulte Políticas de dispositivo de chave de licença MDM Samsung.

Como funcionam os aplicativos móveis e MDX

O XenMobile dá suporte aos aplicativos para iOS e Android, incluindo aplicativos móveis de produtividade, como Secure Hub, Secure Mail e Secure Web, e ao uso de políticas do MDX. Usando o console XenMobile, você pode carregar aplicativos e fornecer os aplicativos para dispositivos de usuário. Além dos aplicativos móveis de produtividade, você pode adicionar os seguintes tipos de aplicativos:

- Os aplicativos que você desenvolve para seus usuários.
- Os aplicativos em que você deseja permitir ou restringir os recursos de dispositivo usando as políticas do MDX.

Para distribuir aplicativos móveis de produtividade, siga estas etapas gerais:

1. Baixe os arquivos MDX da loja pública em https://www.citrix.com/downloads/xenmobile/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html.
2. Carregue esses arquivos no console XenMobile (**Configurar > Aplicativos**), atualizando as políticas MDX conforme necessário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Carregue os arquivos MDX nas lojas de aplicativos públicas. Para obter mais informações, consulte Acrescentar um aplicativo MDX neste artigo.

   O MDX Toolkit prepara aplicativos para dispositivos com iOS e Android com a lógica e as políticas da Citrix. A ferramenta pode preparar de forma segura um aplicativo que foi criado dentro da sua organização ou um aplicativo criado fora da empresa.

Sobre aplicativos obrigatórios e opcionais

Quando você adiciona aplicativos a um grupo de entrega, escolha se eles são opcionais ou necessários. Para aplicativos marcados como necessários, os usuários podem receber atualizações imediatamente em situações como:

- Carregue um novo aplicativo e marque-o conforme necessário.
- Marque um aplicativo existente conforme necessário.
- Quando o usuário exclui um aplicativo necessário.
- Está disponível uma atualização do Secure Hub.

Requisitos para a implantação forçada dos aplicativos necessários

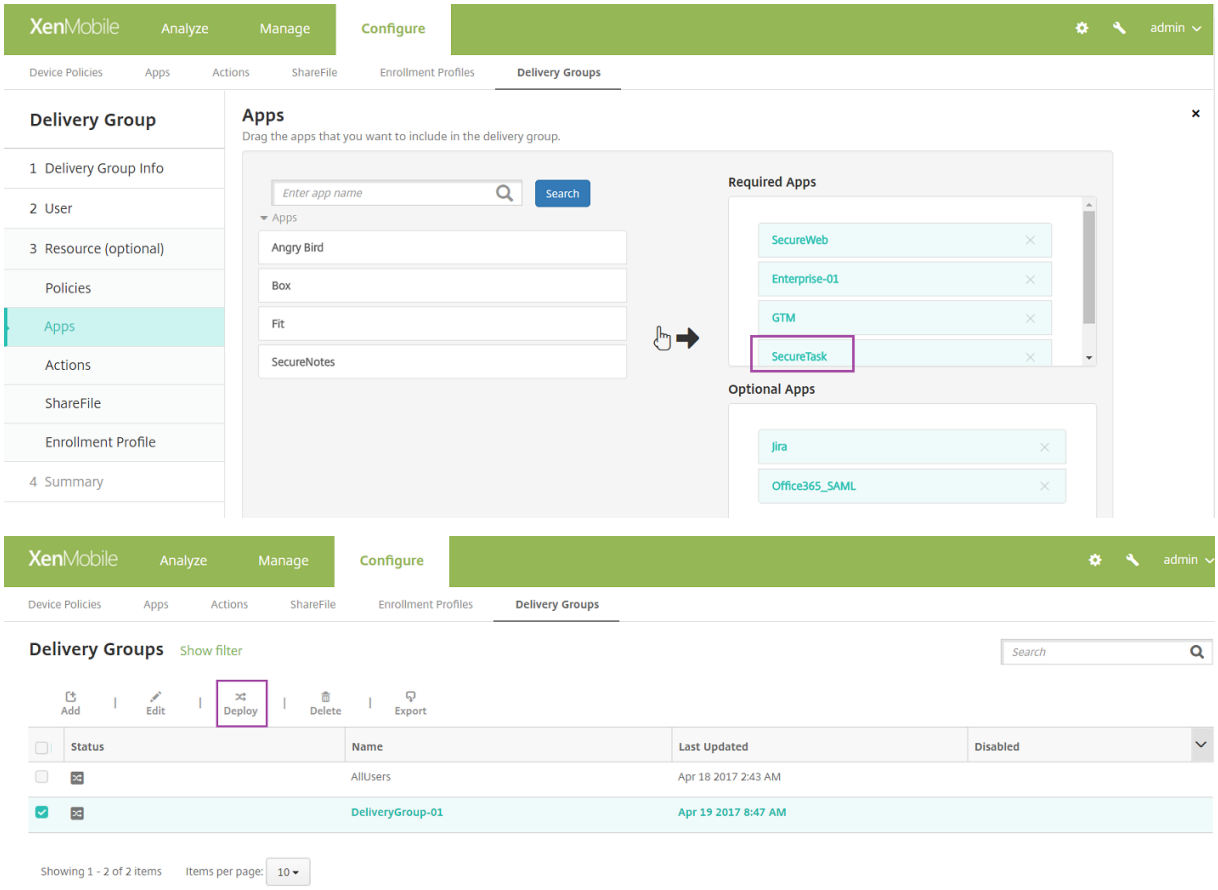
- XenMobile Server 10.6 (versão mínima)
- Secure Hub 10.5.15 para iOS e 10.5.20 para Android (versões mínimas)
- MDX Toolkit 10.6 (versão mínima)
- Propriedade personalizada de servidor, force.server.push.required.apps

  A implantação forçada dos aplicativos necessários está desativada por padrão. Para ativar o recurso, crie uma propriedade personalizada de servidor principal. Defina a **Chave** e o **Nome de exibição** para **force.server.push.required.apps** e defina o **Valor** como **verdadeiro**.
- Após a atualização do XenMobile Server e do Secure Hub: os usuários com dispositivos registrados devem fazer logoff e, em seguida, fazer logon no Secure Hub, uma vez, para obter as atualizações necessárias de implantação de aplicativos.

Exemplos

Os exemplos a seguir mostram a sequência de adicionar o aplicativo Secure Tasks a um grupo de entrega e, em seguida, implantar o grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Depois que o aplicativo de exemplo, o Secure Tasks, implanta o dispositivo do usuário, o Secure Hub avisa ao usuário para instalar o aplicativo.

> Importante:
>
> Os aplicativos necessários habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, atualizam-se imediatamente, mesmo que você configure uma política MDX para um período de carência de atualização de aplicativo e o usuário opte por atualizar o aplicativo mais tarde.

Fluxo de trabalho do aplicativo necessário do iOS para aplicativos empresariais e de lojas públicas

1. Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Atualize o aplicativo no console XenMobile.
3. Use o console XenMobile para implantar os aplicativos necessários.
4. O aplicativo na tela inicial é atualizado. E, para aplicativos da loja pública, a atualização é iniciada automaticamente. Os usuários não são solicitados a atualizar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Os usuários abrem o aplicativo a partir da tela inicial. Os aplicativos são atualizados imediatamente, mesmo se você definir um período de tolerância de atualização de aplicativo e o usuário tocar para atualizar o aplicativo mais tarde.

Fluxo de trabalho do aplicativo necessário exigido pelo Android para aplicativos empresariais

1. Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Use o console XenMobile para implantar os aplicativos necessários.
3. O aplicativo está atualizado. (Os dispositivos Nexus solicitam para instalar atualizações, mas dispositivos Samsung fazem uma instalação silenciosa).
4. Os usuários abrem o aplicativo a partir da tela inicial. Os aplicativos são atualizados imediatamente, mesmo se você definir um período de tolerância de atualização de aplicativo e o usuário tocar para atualizar o aplicativo mais tarde. (Os dispositivos Samsung fazem uma instalação silenciosa.)

Fluxo de trabalho do aplicativo necessário do Android para aplicativos de lojas públicas

1. Implante os XenMobile Apps durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Atualize o aplicativo no console XenMobile.
3. Use o console XenMobile para implantar os aplicativos necessários. Ou abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.
4. A atualização do aplicativo começa imediatamente. (Os dispositivos Nexus solicitam que os usuários instalem a atualização.)
5. Abra o aplicativo a partir da tela inicial. O aplicativo está atualizado. Os usuários não são avisados sobre um período de tolerância. (Os dispositivos Samsung fazem uma instalação silenciosa.)

Como funcionam os aplicativos SaaS e da Web

O XenMobile vem com um conjunto de conectores de aplicativos, que são modelos que você pode configurar para logon único em aplicativos Web e SaaS. Às vezes, você pode configurar os modelos para gerenciamento e criação de contas de usuário. O XenMobile inclui os conectores Security Assertion Markup Language (SAML). Os conectores SAML são usados para aplicativos Web que dão suporte ao protocolo SAML para gerenciamento de conta de usuário e de SSO. O XenMobile dá suporte a SAML 1.1 e a SAML 2.0.

Você também pode criar seus próprios conectores SAML.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Como funcionam os aplicativos empresariais

Os aplicativos geralmente residem na sua rede interna. Os usuários podem se conectar aos aplicativos usando o Secure Hub. Quando você adiciona um aplicativo empresarial, o XenMobile cria o conector de aplicativo para ele.

Como funciona a loja de aplicativos pública

Você pode definir as configurações para obter nomes de aplicativo e descrições da Apple App Store e do Google Play. Quando você obtém as informações de aplicativo da loja, o XenMobile substitui o nome existente e a descrição.

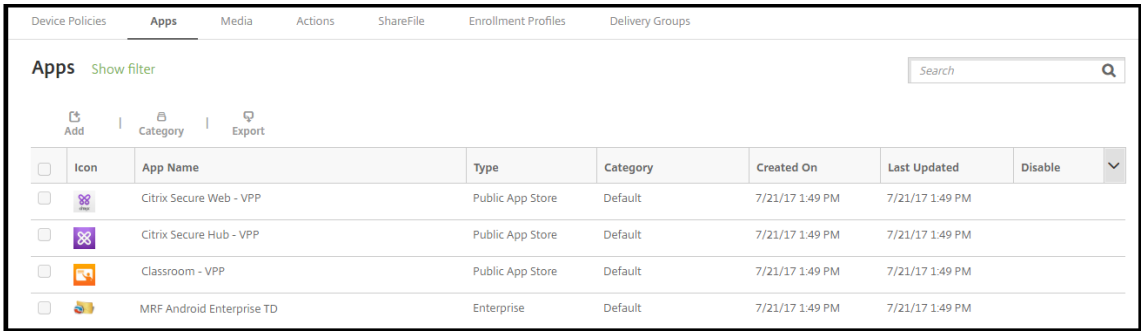
Como funcionam os links da Web

Um link da Web é um endereço Web para um site da Internet ou intranet. Um link da Web também pode apontar para um aplicativo Web que não requer SSO. Quando você termina de configurar um link da Web, o link é exibido como um ícone na XenMobile Store. Quando os usuários fazem login no Secure Hub, o link é exibido com a lista de aplicativos e áreas de trabalho disponíveis.

Acrescentar um aplicativo MDX

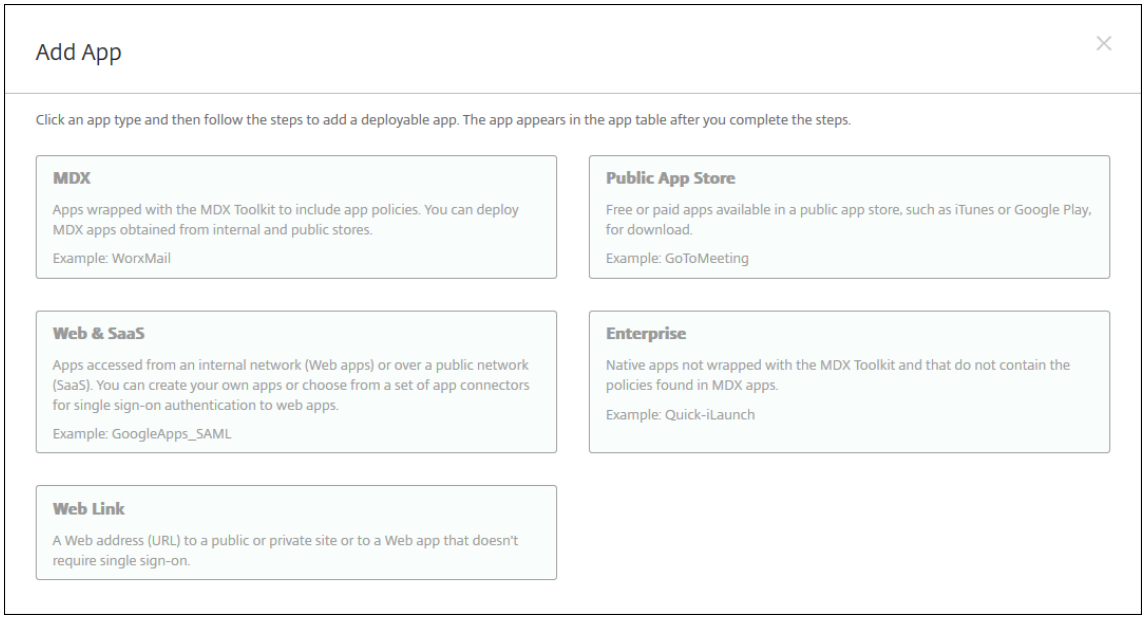
Quando você recebe um aplicativo móvel do MDX preparado para um dispositivo iOS ou Android, você pode carregar o aplicativo para o XenMobile. Depois de carregar o aplicativo, você pode configurar os detalhes do aplicativo e as configurações de política. Para obter mais informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte Resumo das políticas do MDX. Aquela seção também contém descrições detalhadas da política.

1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
   - **Descrição:** digite uma descrição opcional para o 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 Criar categorias de aplicativos.
5. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

   Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 11 para saber como definir as regras de implantação dessa plataforma.
7. To select an MDX file to upload, click **Upload** and navigate to the file location.
   - Se você adicionar um aplicativo iOS VPP B2B, clique em **Seu aplicativo é um aplicativo de VPP B2B?**. Em seguida, na lista, clique na conta de VPP B2B a ser usada.
8. Clique em **Avançar**. A página **Detalhes do Aplicativo** é exibida.
9. Defina estas configurações:
   - **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
   - **Descrição do aplicativo:** digite uma descrição para o aplicativo.
   - **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

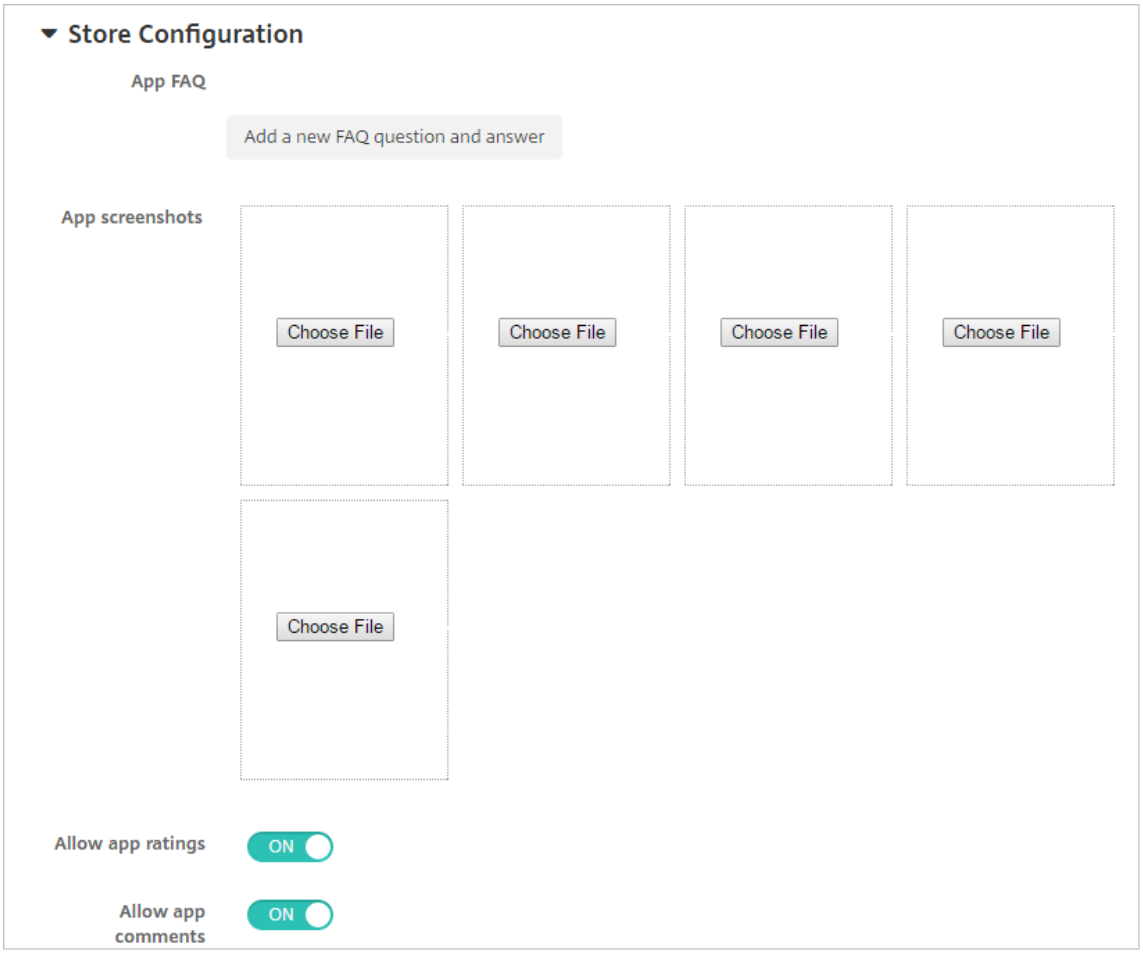
- **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
- **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
- **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 o aplicativo deve ser removido de um dispositivo quando o perfil MDM é removido. O padrão é **I**.
- **Evitar o backup de dados do aplicativo:** selecione se deseja impedir que usuários façam backup de dados do aplicativo. O padrão é **I**.
- **Forçar aplicativo a ser gerenciado:** selecione se, quando o aplicativo está instalado e não é gerenciado, os usuários devem ser solicitados a permitir que o aplicativo seja gerenciado em dispositivos não supervisionados. O padrão é **I**. Disponível no iOS 9.0 e versões posteriores.
- **Aplicativos implantados por meio de VPP:** selecione se você deseja implantar o aplicativo usando o VPP. Se estiver **ON** e você implantar uma versão do MDX do aplicativo e usar VPP para implantar o aplicativo, o Secure Hub mostra somente a instância VPP. O valor padrão é **Desativado**.

10. Configure as **Políticas de MDX**. As políticas de MDX variam por plataforma e incluem opções para áreas de política, como Autenticação, Segurança do dispositivo, Criptografia, Interação de aplicativo e Restrições de aplicativo. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política.

    Para obter mais informações sobre políticas de aplicativos para aplicativos MDX, consulte Resumo das políticas do MDX. Esse artigo inclui uma tabela que mostra quais políticas se aplicam a cada plataforma.

11. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.
12. Expanda **Configuração da XenMobile Store**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



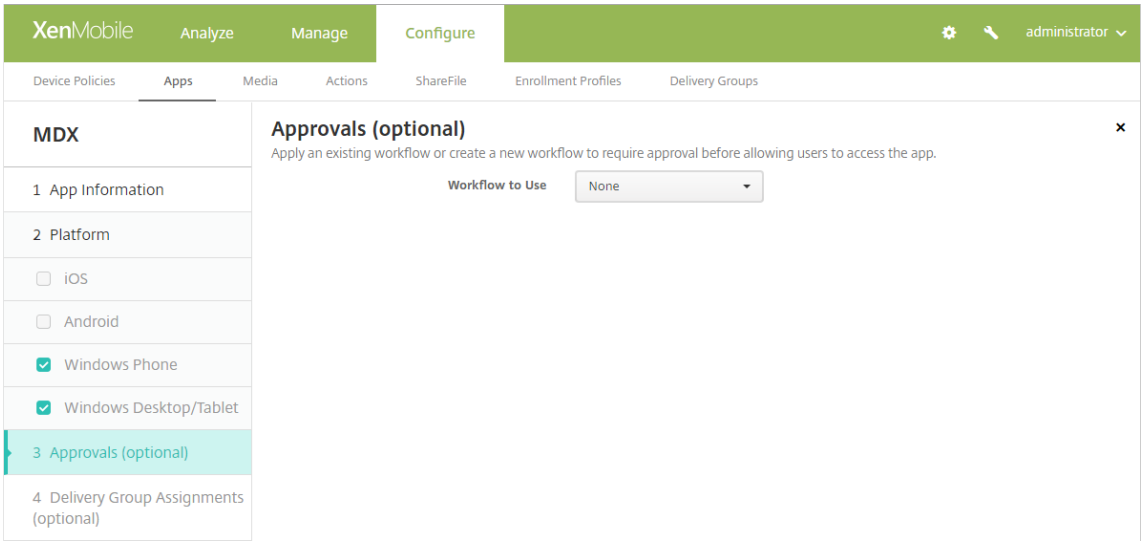
Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- Defina estas configurações:
  - **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
  - **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
  - **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.

    Permitir comentários do aplicativo: selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

13. Clique em **Avançar**. A página **Aprovações** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 15.

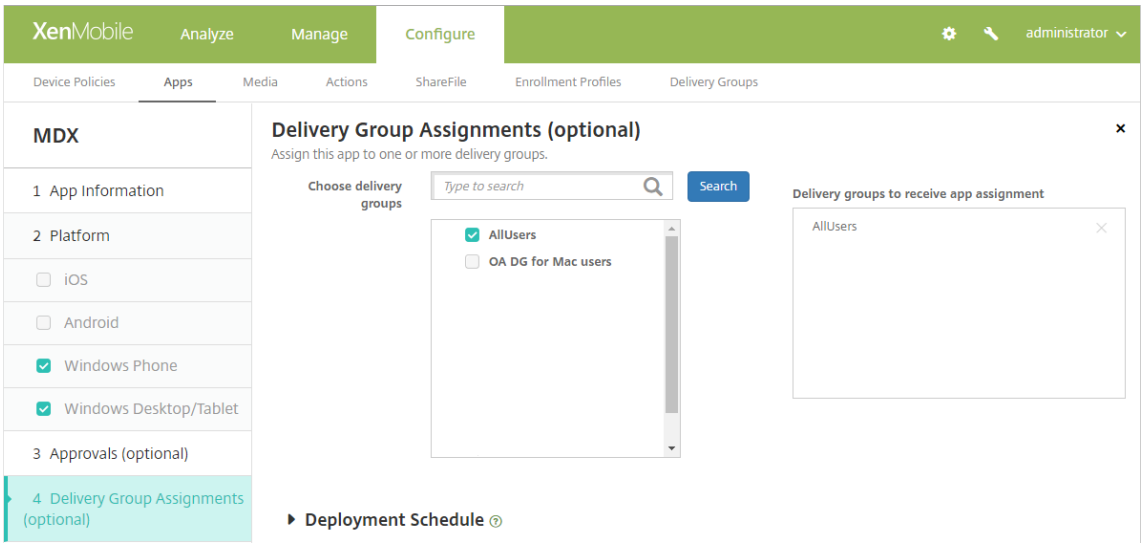
Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** 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**, defina essas configurações. Para obter mais informações, consulte Criar e gerenciar 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 de email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
  - Não é Necessário
  - 1 nível
  - 2 níveis
  - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:
  * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
  * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
  * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

14. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.



15. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

16. Expanda **Cronograma de implantação** e defina estas configurações:

    - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
    - Ao lado de Cronograma de implantação, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
    - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
    - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
    - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
>
> O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

17. Clique em **Salvar**.

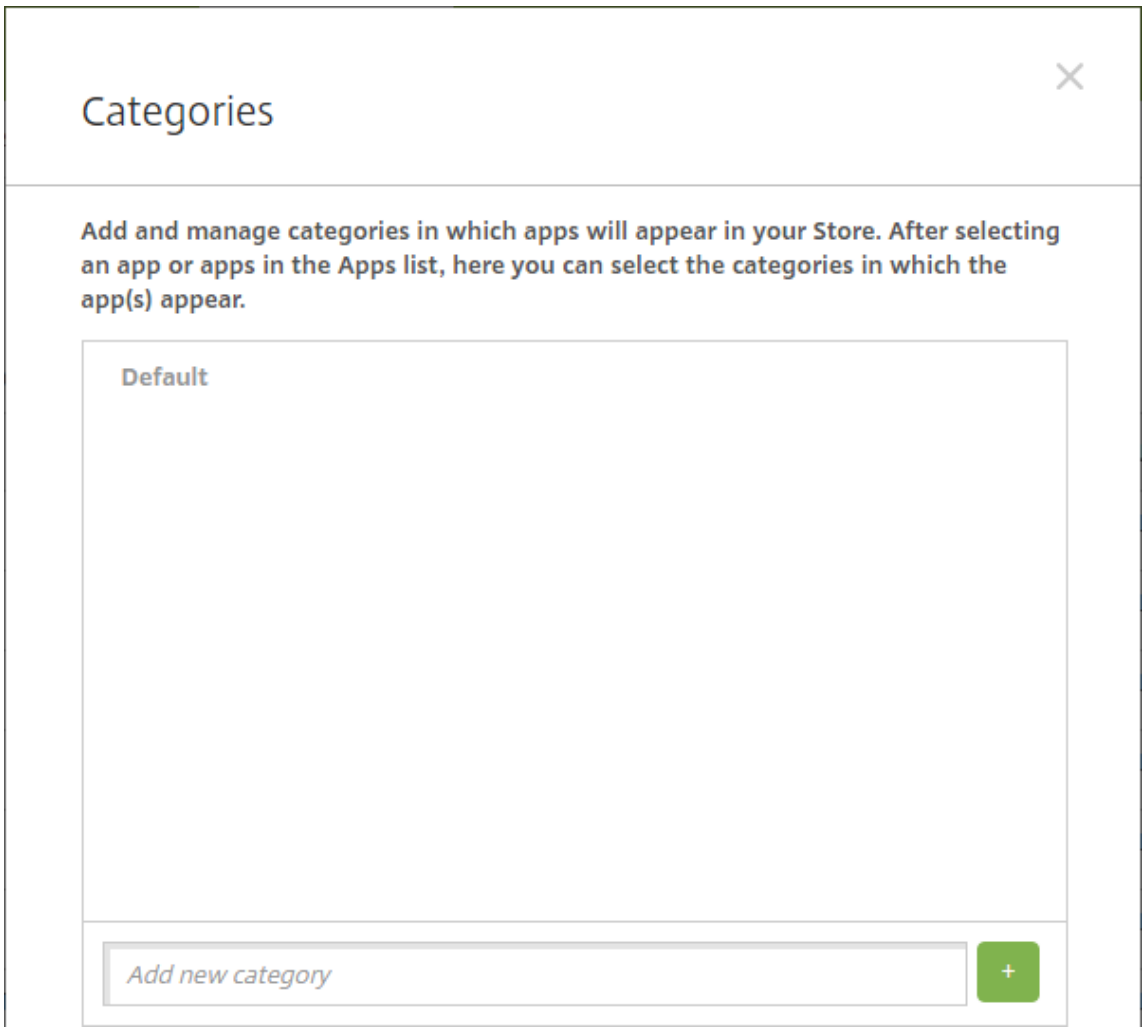
Criar categorias de aplicativos

Quando os usuários fazem login no Secure Hub, eles recebem uma lista dos aplicativos, links da Web e lojas que você configurou no XenMobile. É possível usar categorias de aplicativos para permitir que os usuários acessem somente determinados aplicativos, lojas ou links da Web. Por exemplo, você pode criar uma categoria Finanças e adicionar à categoria os aplicativos que pertencem somente a finanças. Ou pode configurar uma categoria Vendas à qual atribuir os aplicativos de vendas.

Configure as categorias na página **Aplicativos** do console XenMobile. Em seguida, quando você adicionar ou editar um aplicativo, link da Web ou loja, poderá adicionar o aplicativo a uma ou mais das categorias configuradas.

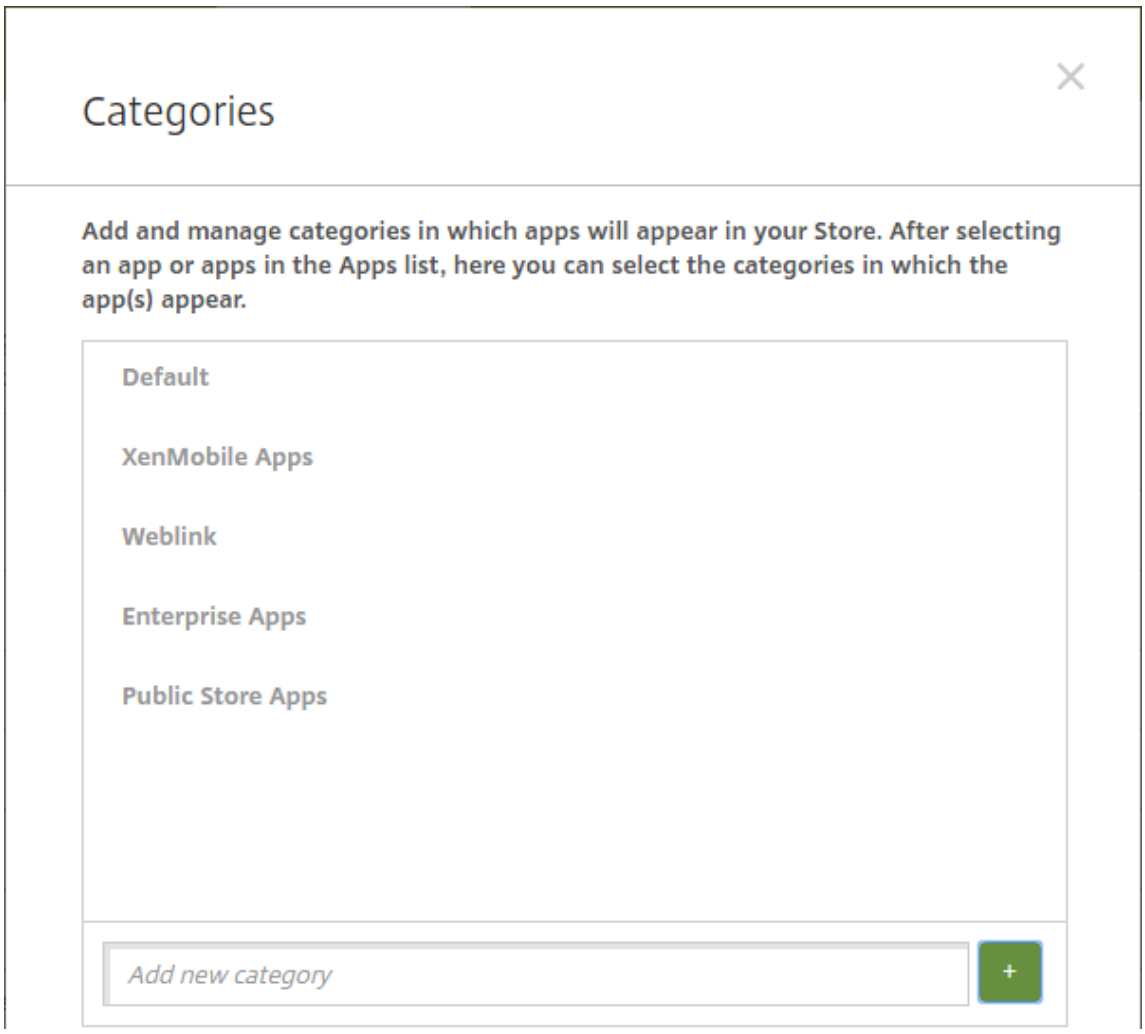
1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.
2. Clique em **Categoria**. A caixa de diálogo **Caregorias** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Para cada categoria que você desejar adicionar, faça o seguinte:
   - Digite o nome da categoria que você deseja adicionar no campo **Adicionar uma nova categoria** na parte inferior da caixa de diálogo. Por exemplo, você pode digitar Aplicativos corporativos para criar uma categoria de aplicativos corporativos.
   - Clique no sinal de adição (+) para adicionar a categoria. A categoria recém-criada é adicionada e aparece na caixa de diálogo **Categorias**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Quando terminar de adicionar categorias, feche a caixa de diálogo **Categorias**.
5. Na página **Aplicativos**, você pode colocar um aplicativo existente em uma nova categoria.
   - Selecione o aplicativo que você deseja categorizar.
   - Clique em **Edit**. A página **Informações do Aplicativo** é exibida.
   - Na lista **Categoria do aplicativo**, aplique a nova categoria marcando a caixa de seleção da categoria. Desmarque as caixas de seleção das categorias existentes que você não deseja aplicar ao aplicativo.
   - Clique na guia **Atribuições do grupo de entrega** ou em **Avançar** em cada uma das páginas seguintes para percorrer as páginas de configuração de aplicativo restantes.
   - Clique em **Salvar** na página **Atribuições do grupo de entrega** para aplicar a nova categoria. A nova categoria é aplicada ao aplicativo e é exibida na tabela **Aplicativos**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

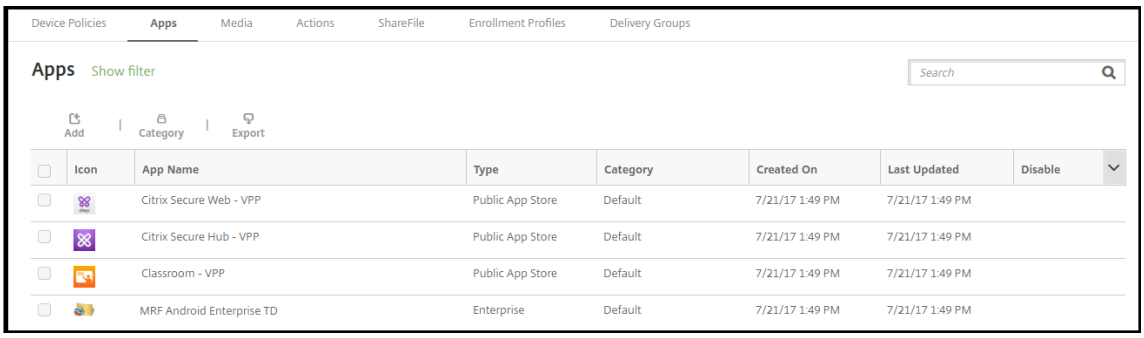
Acrescentar um aplicativo de loja de aplicativos pública

Você pode adicionar ao XenMobile aplicativos gratuitos ou pagos que estão disponíveis em uma loja de aplicativos pública, como o iTunes ou o Google Play.

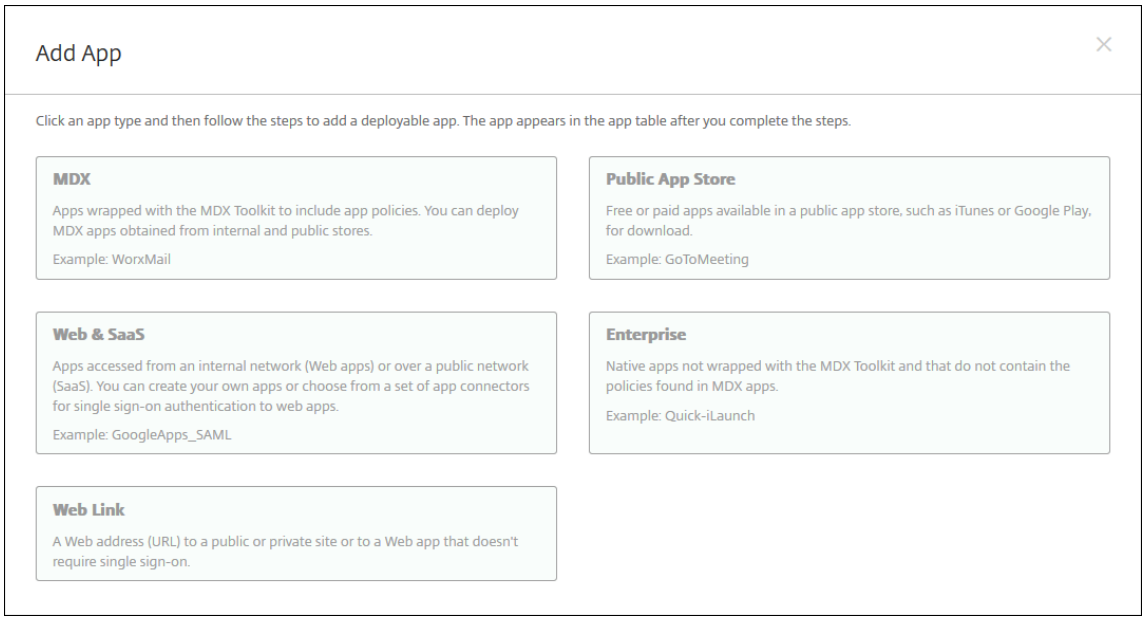
Quando você adiciona um aplicativo de loja de aplicativos pública pago para Android for Work, pode verificar o status do licenciamento da compra em massa. Esse status é o número total de licenças disponíveis, o número em uso no momento e o endereço de email de cada usuário que consome as licenças. O plano de Compra em Massa do Android for Work simplifica o processo de localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Configure as informações do aplicativo e escolha plataformas para entregar o aplicativo a:

1. No console 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 **Loja de aplicativos pública**. A página **Informações do Aplicativo** é exibida.
4. No painel **Informações do aplicativo**, digite as seguintes informações:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Nome:** digite um nome descritivo para o aplicativo. Esse nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
- **Descrição:** digite uma descrição opcional para o 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 Criar categorias de aplicativos.

5. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

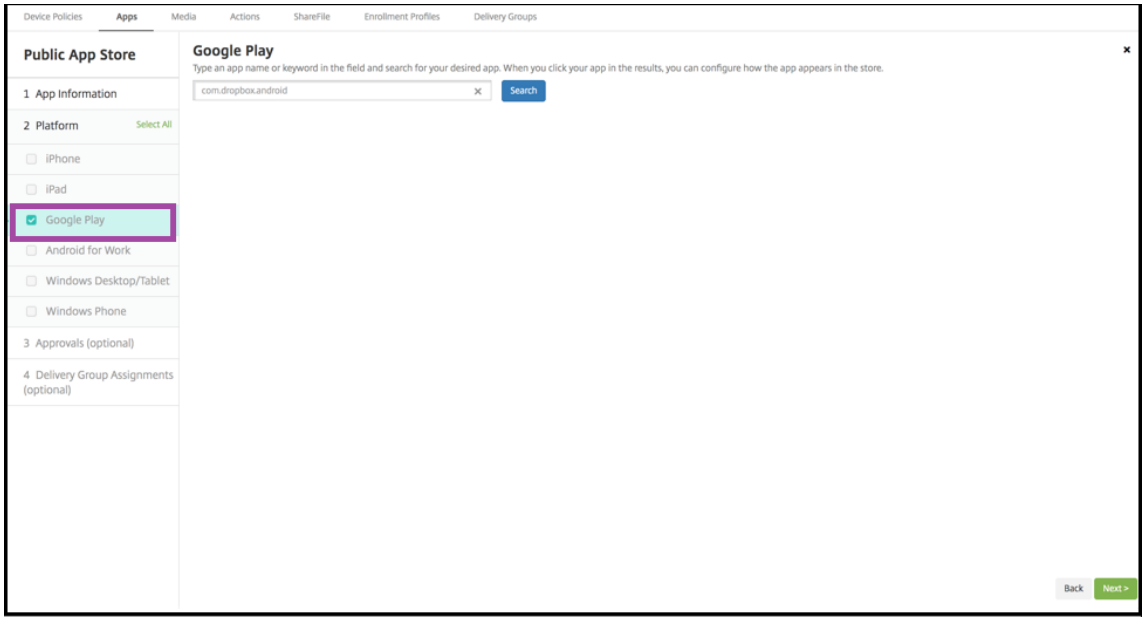
   Em seguida, defina as configurações do aplicativo para cada plataforma. Quando terminar de definir as configurações de uma plataforma, defina as regras de implantação e a configuração de armazenamento da plataforma.

   Em seguida, defina as configurações do aplicativo para cada plataforma. Quando terminar de definir as configurações de uma plataforma, defina as regras de implantação e a configuração de armazenamento da plataforma.

> **Importante:** a definição de configurações de aplicativos da Google Play Store requer etapas diferentes das de aplicativos de outras plataformas. Você deve configurar manualmente as informações do aplicativo da Google Play Store.

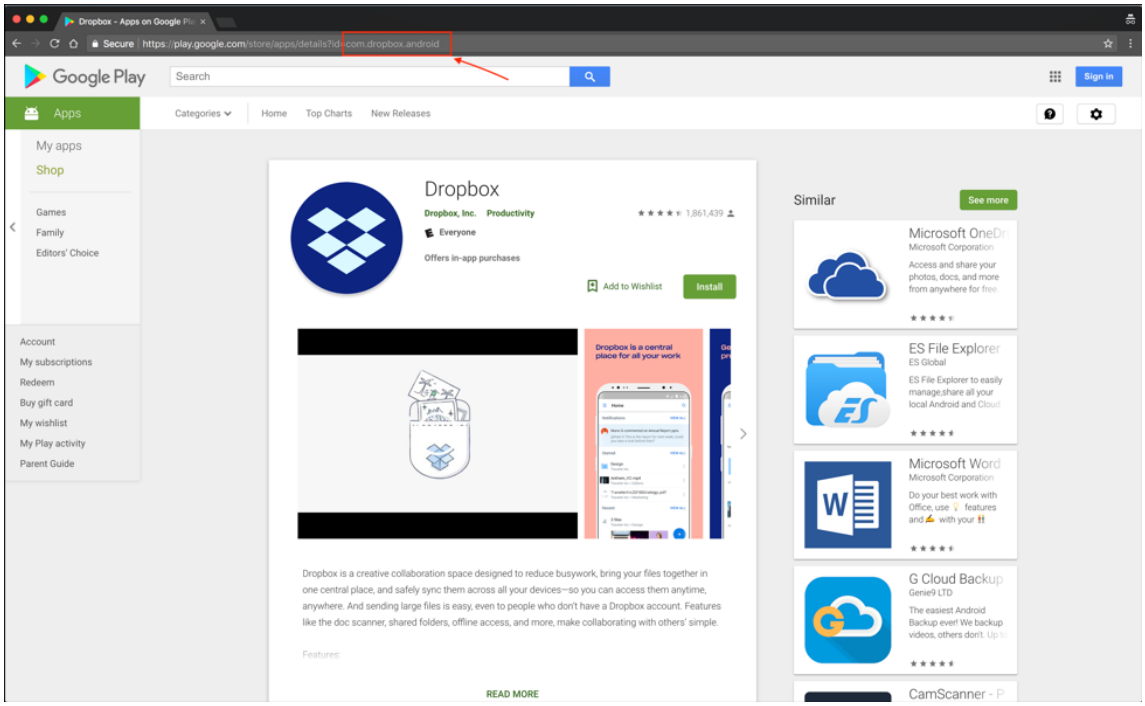
Configurar as definições do aplicativo para as aplicações do Google Play

1. Verifique se **Google Play** está selecionado em **Plataformas**.

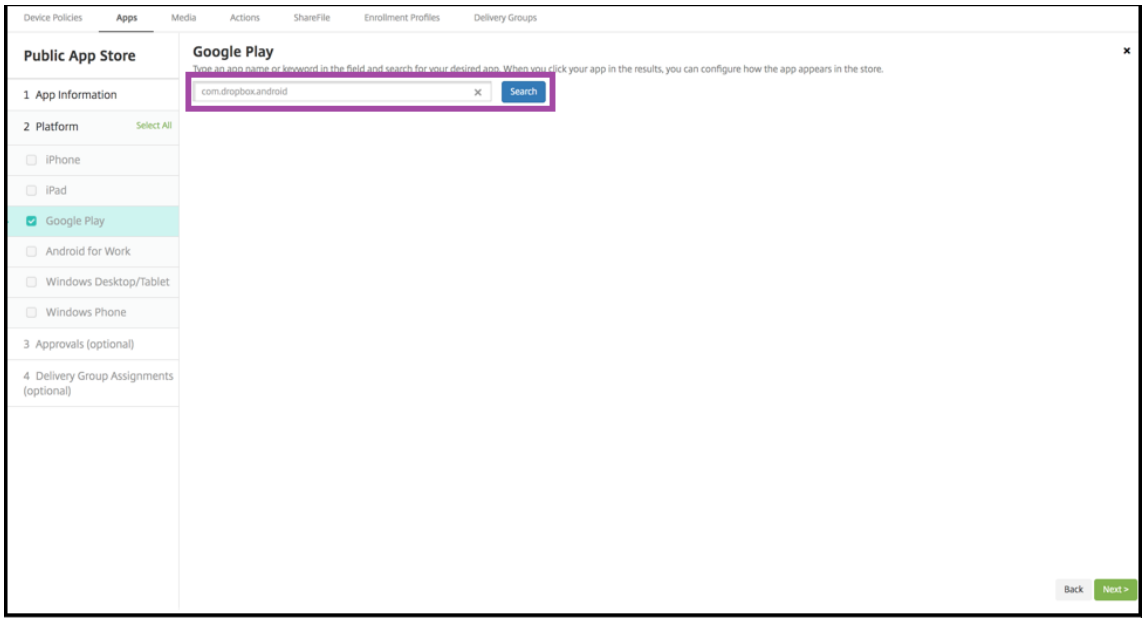


© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Vá para a loja de aplicativos do Google Play. Na Google Play Store, copie o ID do pacote. O ID pode ser encontrado na URL do aplicativo.

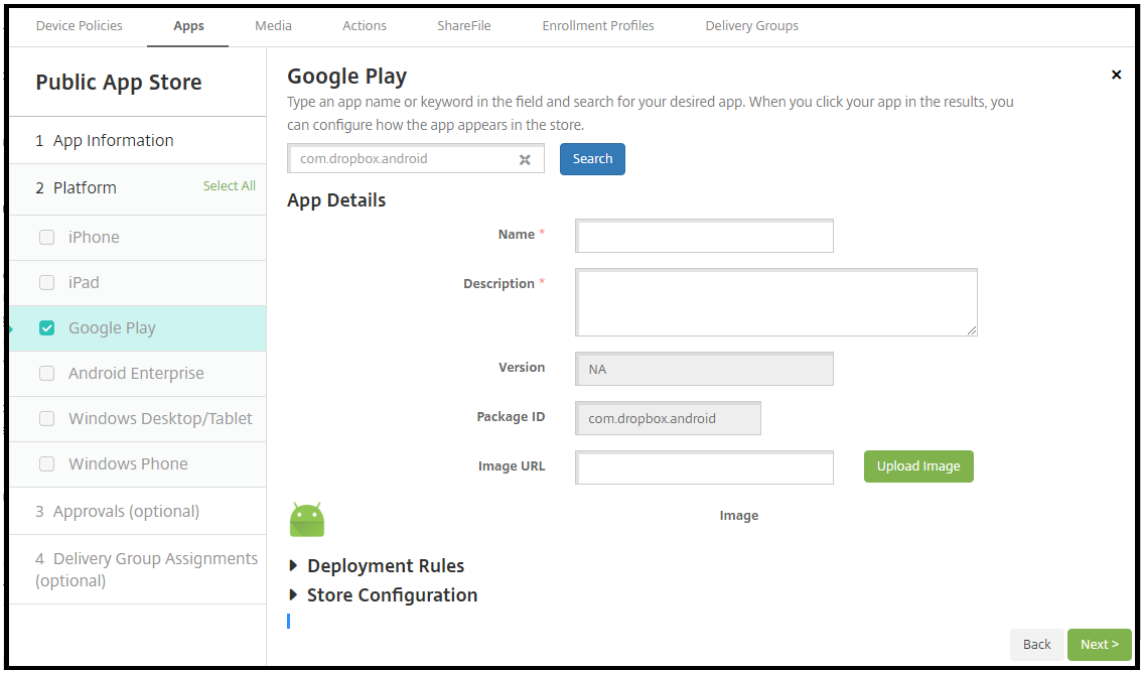


3. Ao adicionar um aplicativo da Loja Pública ao console Citrix Endpoint Management, cole o ID do pacote na barra de pesquisa. Clique em **Pesquisar**.



4. Se o ID do pacote for válido, uma interface do usuário será exibida, permitindo que você insira detalhes do aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Você pode configurar a URL para que a imagem apareça com o aplicativo na loja. Para usar a imagem da Google Play Store:

    a) Vá para a loja de aplicativos do Google Play. 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**.

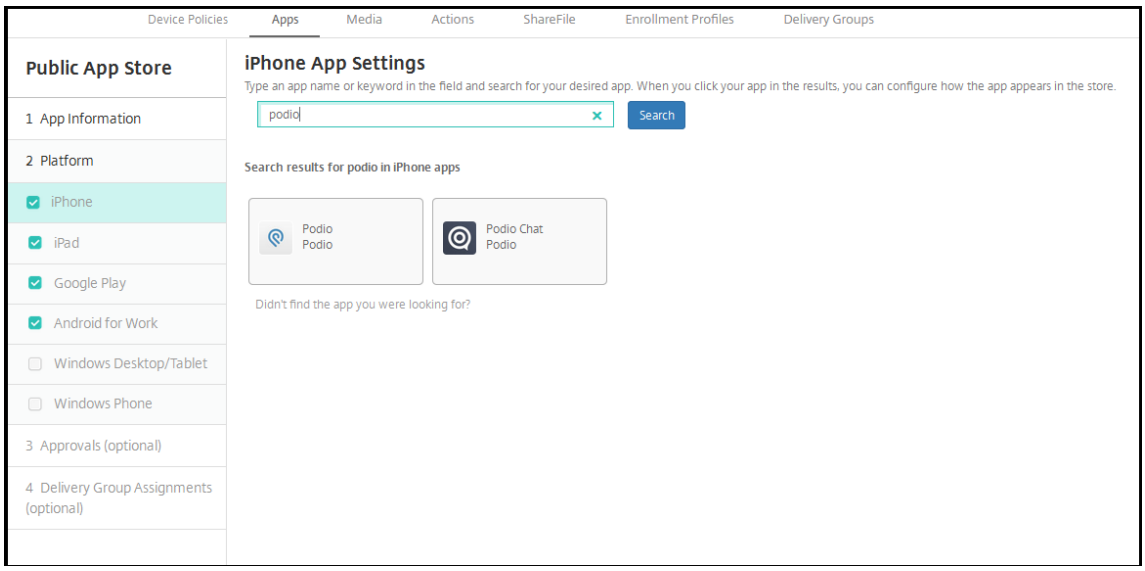
    c) Clique em **Carregar imagem**. A imagem aparece ao lado de **Imagem**.

Se você não configurar uma imagem, a imagem genérica do Android aparecerá com o aplicativo.

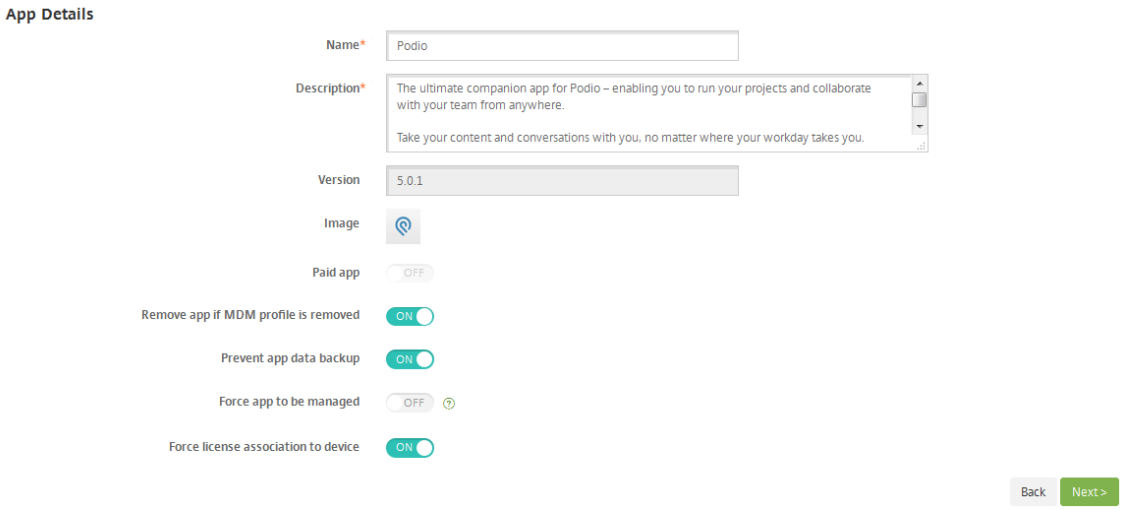
Configurar parâmetros do aplicativo para plataformas diferentes do Google Play

1. Selecione um aplicativo a ser adicionado digitando o respectivo nome na caixa Pesquisar e clicando em **Pesquisar**. Os aplicativos que correspondem aos critérios de pesquisa são exibidos. A figura a seguir mostra o resultado da pesquisa por **podio**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Clique no aplicativo que você deseja adicionar. Preencha os campos de **Detalhes do aplicativo** com informações relacionadas ao aplicativo escolhido (incluindo nome, descrição, número da versão e imagem associada).



3. Defina estas configurações:

   - Se necessário, altere o nome e a descrição do aplicativo.
   - **Aplicativo pago:** esse campo é configurado previamente e não pode ser alterado.
   - **Remover aplicativo se o perfil MDM for removido:** selecione se o aplicativo deverá ser removido quando o perfil MDM for removido. O padrão é **I**.
   - **Evitar o backup de dados do aplicativo:** selecione se o aplicativo deve ser impedido de realizar o backup de dados. O padrão é **I**.
   - **Forçar aplicativo a ser gerenciado:** selecione se, quando o aplicativo está instalado e não é gerenciado, os usuários devem ser solicitados a permitir que o aplicativo seja gerenciado em dispositivos não supervisionados. O padrão é **O**. Disponível no iOS 9.0 e versões

© 1999-2019 Citrix Systems, Inc. All rights reserved.

posteriores.

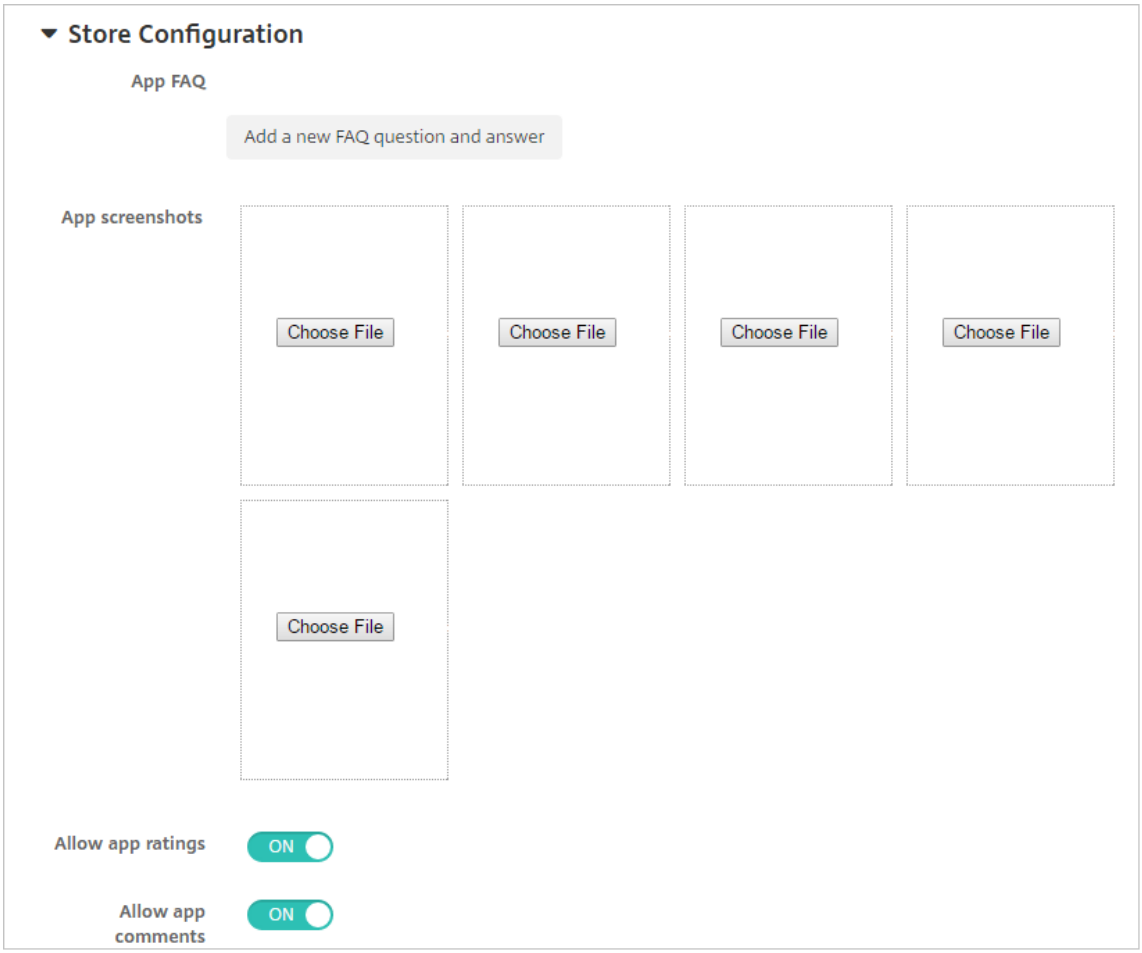
- **Forçar associação de licença ao dispositivo:** selecione se um aplicativo que foi desenvolvido com a associação de dispositivo ativada deve ser associado a um dispositivo em vez de a um usuário. Disponível no iOS 9 e versões posteriores. Se o aplicativo que você escolheu não for compatível com a atribuição a um dispositivo, esse campo não poderá ser alterado.

Configure as regras de implantação

Para obter informações, consulte Implantar recursos.

Defina a configuração da loja de aplicativos

1. Expanda **Configuração da XenMobile Store**.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Defina estas configurações:
  - **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
  - **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
  - **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é I.
  - **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado.

2. Expanda **Volume Purchase Program** ou, para o Android for Work, expanda **Compra em Massa**.

   Para o Volume Purchase Program, conclua as seguintes etapas.

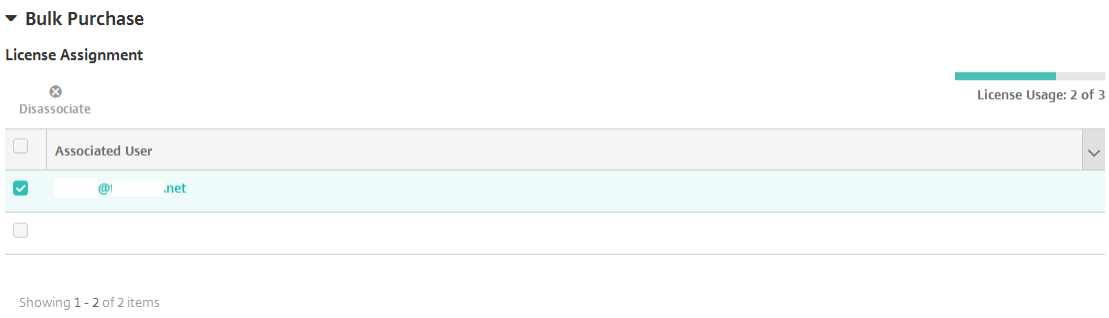
   a) Na lista **Licença do VPP**, clique **Carregar um arquivo de licença do VPP** se você desejar ativar o XenMobile para aplicar uma licença de VPP ao aplicativo.

   b) Na caixa de diálogo que é exibida, importe a licença.

   Para a compra em massa do Android for Work, expanda a seção **Compra em massa**.

   A tabela de Atribuição de licenças mostra o número de licenças em uso para o aplicativo, do total de licenças disponíveis.

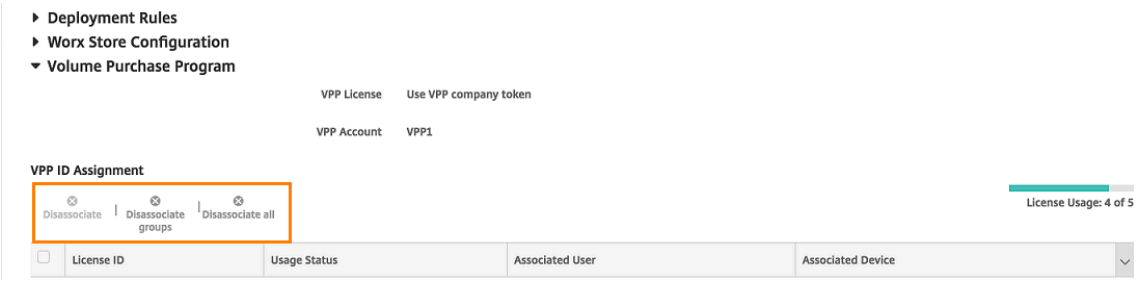
   Para o Android for Work, você pode selecionar um usuário e clicar em **Desassociar** para encerrar a respectiva atribuição de licença e liberar uma licença para outro usuário. No entanto, você poderá desassociar a licença somente se o usuário não fizer parte de um grupo de entrega que contém o aplicativo específico.



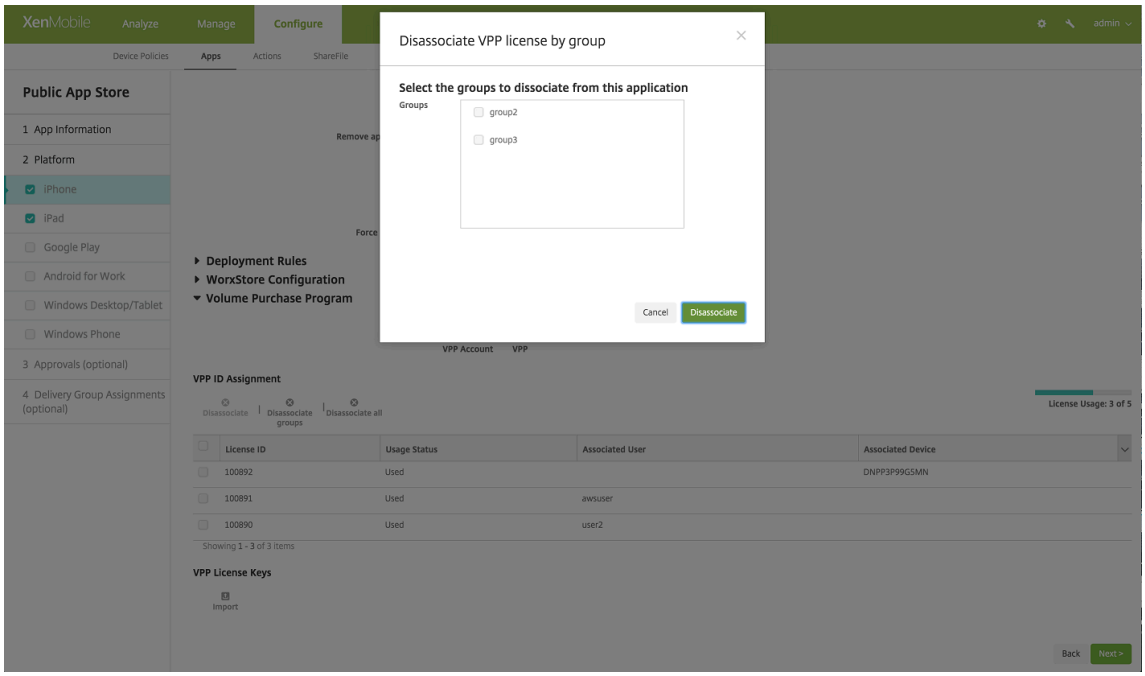
   Para o Android for Work, você poderá desassociar uma licença somente se o usuário não fizer parte de um grupo de entrega que contém o aplicativo específico.

   Para o iOS, você poderá desassociar licenças do Programa de Compra por Volume para usuários individuais, grupos de usuários ou todas as atribuições. Isso encerra as atribuições de licença e libera licenças.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Clicar em **Desassociar grupos** abre uma caixa de diálogo na qual você pode selecionar grupos.



3. Depois que você concluir o **Volume Purchase Program** ou as configurações de **Compra em massa**, clique em **Avançar**. A página **Aprovações** é exibida.

   Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, poderá pular para a próxima etapa.

   Configure estas definições se você precisar atribuir ou criar um fluxo de trabalho:

   - **Fluxo de trabalho a ser usado:** 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**, defina essas 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 email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
     - **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação

© 1999-2019 Citrix Systems, Inc. All rights reserved.

do gerente necessários para esse fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
  * Não é Necessário
  * 1 nível
  * 2 níveis
  * 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
  * Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:
  * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
  * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
  * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

4. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
5. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.
6. Expanda **Cronograma de implantação** e defina estas configurações:
   - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
   - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
   - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
   - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
   - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O.

> Nota:
>
> Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
>
> O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

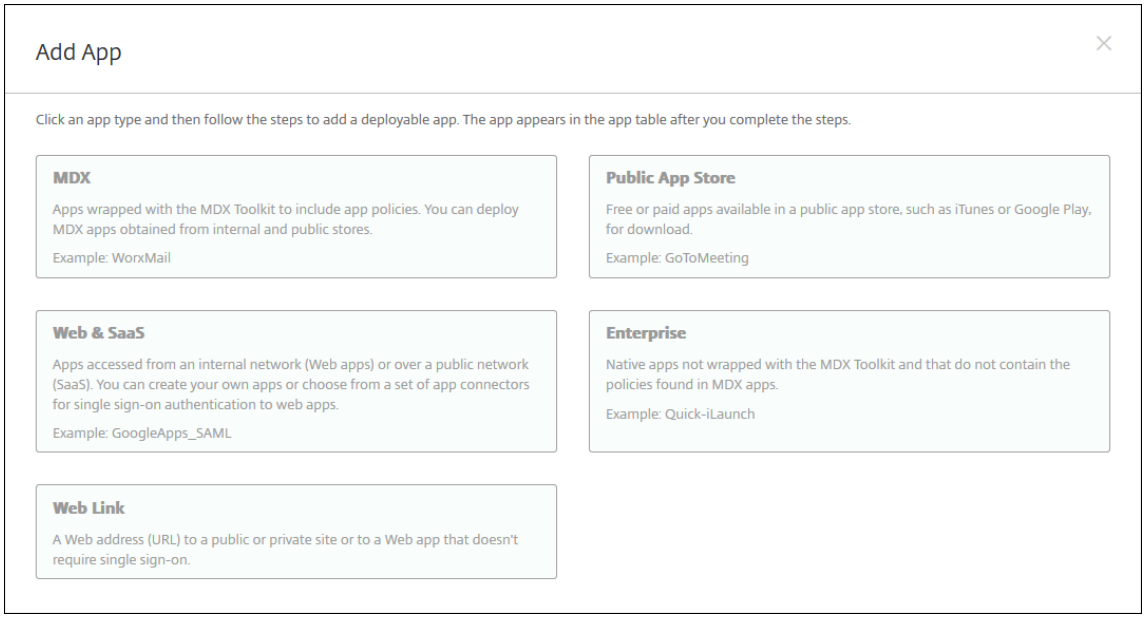
7. Clique em **Salvar**.

Acrescentar um aplicativo Web ou SaaS

Usando o console XenMobile, você pode oferecer aos usuários a autorização de logon único (SSO) aos seus aplicativos móveis, empresariais, Web e SaaS. Você pode ativar aplicativos para SSO usando modelos de conector de aplicativo. Para obter uma lista dos tipos de conectores 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.

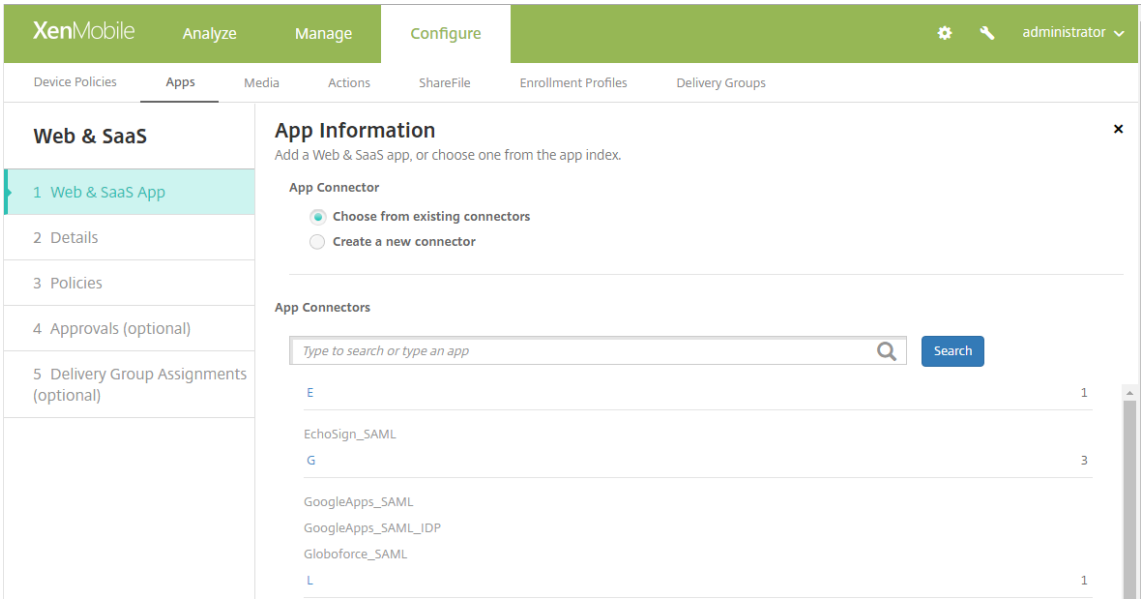
Se um aplicativo estiver disponível somente para SSO, depois que você salvar as configurações, o aplicativo será exibido na guia **Aplicativos** do console XenMobile.

1. No console 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 **Web e SaaS**. A página **Informações do Aplicativo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Configure um aplicativo existente ou novo conector, da seguinte maneira.

Para configurar um conector de aplicativo existente

1. Na página **Informações do aplicativo**, **Escolher dos conectores existentes** já está selecionado, como mostrado acima. Clique no conector que você deseja usar na lista **Conectores de aplicativos**. As informações de conector de aplicativo são exibidas.
2. Defina estas configurações:
   - **Nome do aplicativo:** aceite o nome preenchido previamente ou digite um novo nome.
   - **Descrição do aplicativo:** aceite a descrição preenchida previamente ou digite uma.
   - **URL:** aceite o URL preenchido previamente ou digite o endereço Web do aplicativo. Dependendo do conector que você escolher, esse campo poderá conter um espaço reservado que você deve substituir antes que possa continuar para a página seguinte.
   - **Nome de domínio:** se aplicável, digite o nome de domínio do aplicativo. Esse campo é obrigatório.
   - **O aplicativo está hospedado na rede interna:** selecione se o aplicativo está em execução em um servidor na sua rede interna. Se os usuários se conectarem de uma localidade remota a um aplicativo interno, eles deverão se conectar por meio do NetScaler Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do NetScaler Gateway. O padrão é **O**.
   - **Categoria do aplicativo:** na lista, clique em uma categoria opcional a ser aplicada ao aplicativo.
   - **Provisionamento de conta de usuário:** selecione se contas de usuário devem ser criadas para o aplicativo. Se você usar o conector Globoforce_SAML, deverá ativar essa opção para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

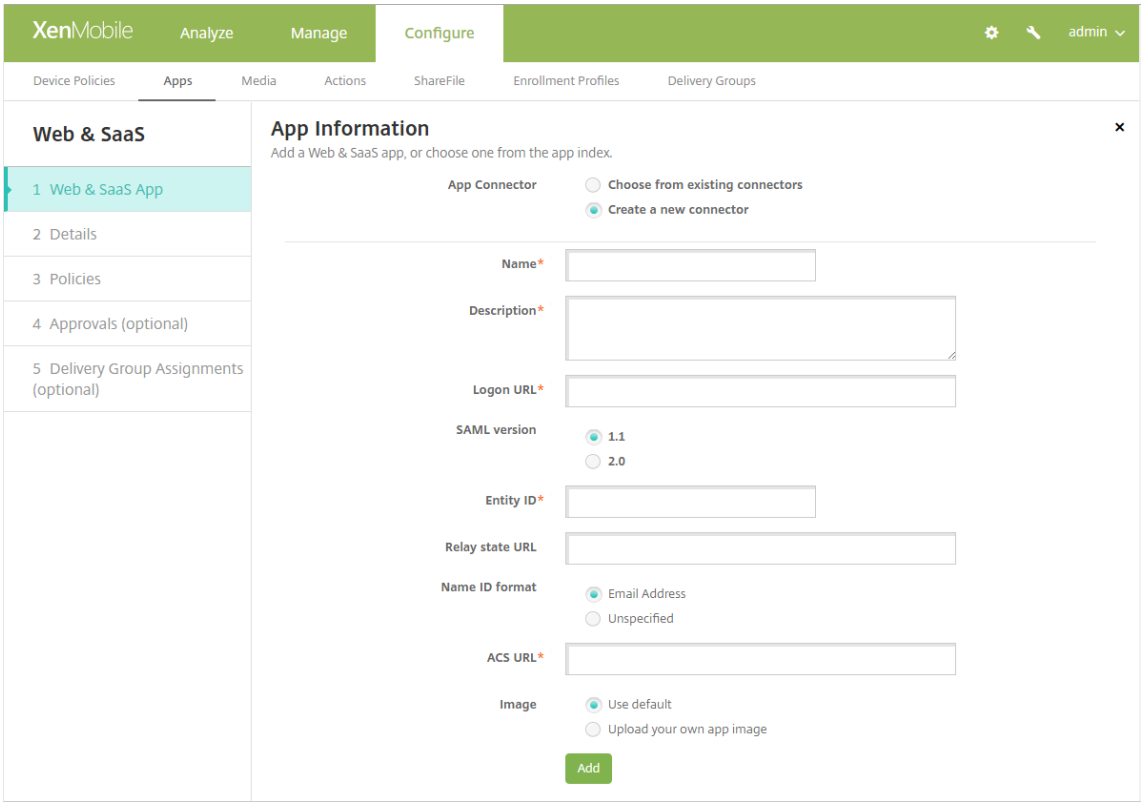
garantir a integração perfeita do SSO.

- Se você ativar o **Provisionamento de conta de usuário**, defina estas configurações:
  - **Conta de serviço**
    - **Nome de usuário:** digite o nome do administrador do aplicativo. Este campo é obrigatório.
    - **Senha:** digite a senha de administrador do aplicativo. Este campo é obrigatório.
  - **Conta de usuário**
    - **Quando termina o direito do usuário:** na lista, clique na ação a ser tomada quando os usuários não tiverem mais acesso ao aplicativo. O padrão é **Desativar conta**.
  - **Regra de nome de usuário**
    - Para cada regra de nome do usuário que você desejar adicionar, faça o seguinte:
      - **Atributos do 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 do usuário. O padrão é **Tudo**.
      - **Regra:** cada atributo de usuário que você adiciona é automaticamente acrescentado à regra de nome do usuário.
- **Requisito de senha**
  - **Comprimento:** digite o comprimento mínimo da senha do usuário. O padrão é **8**.
- **Vencimento de senha**
  - **Validade (dias):** digite o número de dias durante os quais a senha é válida. Os valores válidos são **0** a **90**. O padrão é 90.
  - **Redefinir a senha automaticamente depois de expirar:** selecione se a senha deve ser redefinida automaticamente quando ela expira. O padrão é **O**. Se você não ativar esse campo, os usuários não poderão abrir o aplicativo após a expiração das senhas.

Para configurar um novo conector de aplicativo

1. Na página **Informações do aplicativo**, selecione **Criar um novo conector**. Os campos de conector de aplicativo são exibidos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



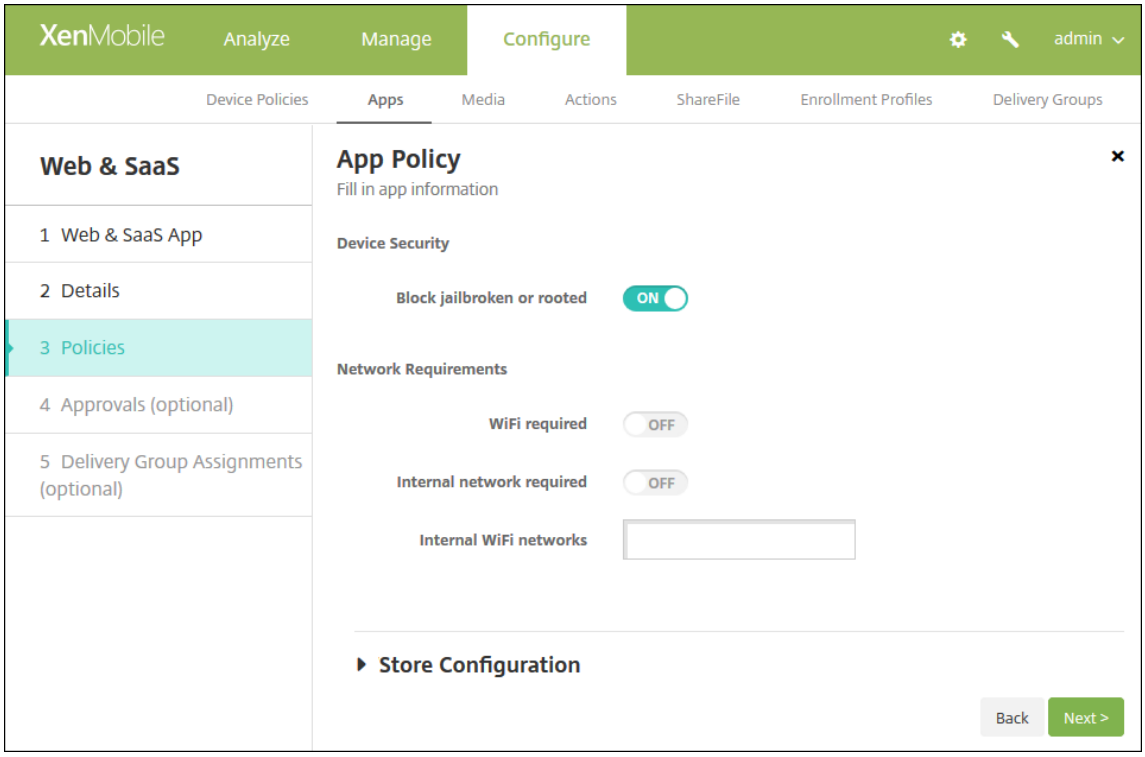
2. Defina estas configurações:

   - **Nome:** digite um nome para o conector. Este campo é obrigatório.
   - **Descrição:** digite uma descrição para o conector. Este campo é obrigatório.
   - **URL de login:** digite ou copie e cole a URL a qual os usuários usam para fazer login 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 login do aplicativo. Por exemplo, a página pode ser `https://www.example.com/logon`. Este campo é obrigatório.
   - **Versão do SAML:** selecione **1.1** ou **2.0**. O padrão é **1.1**.
   - **ID da entidade:** digite a identidade do aplicativo SAML.
   - **URL do estado do relé:** digite o endereço da Web do aplicativo de SAML. A URL do estado do relé é a URL de resposta do aplicativo.
   - **Formato de ID do nome:** selecione **Endereço de email** ou **Não especificado**. O padrão é **Endereço de e-mail**.
   - **URL de ACS:** digite a URL do Serviço do Consumidor de Asserção do provedor de identidade ou do provedor de serviços. A URL de ACS oferece aos usuários a capacidade de SSO.
   - **Imagem:** selecione se a imagem padrão da Citrix deve ser usada ou se a imagem do próprio aplicativo deve ser carregada. O padrão é Usar padrão.
     - Para carregar sua própria imagem, clique em **Procurar** e navegue até o local do arquivo. O arquivo deve ser um arquivo .PNG. Não é possível carregar um arquivo JPEG

© 1999-2019 Citrix Systems, Inc. All rights reserved.

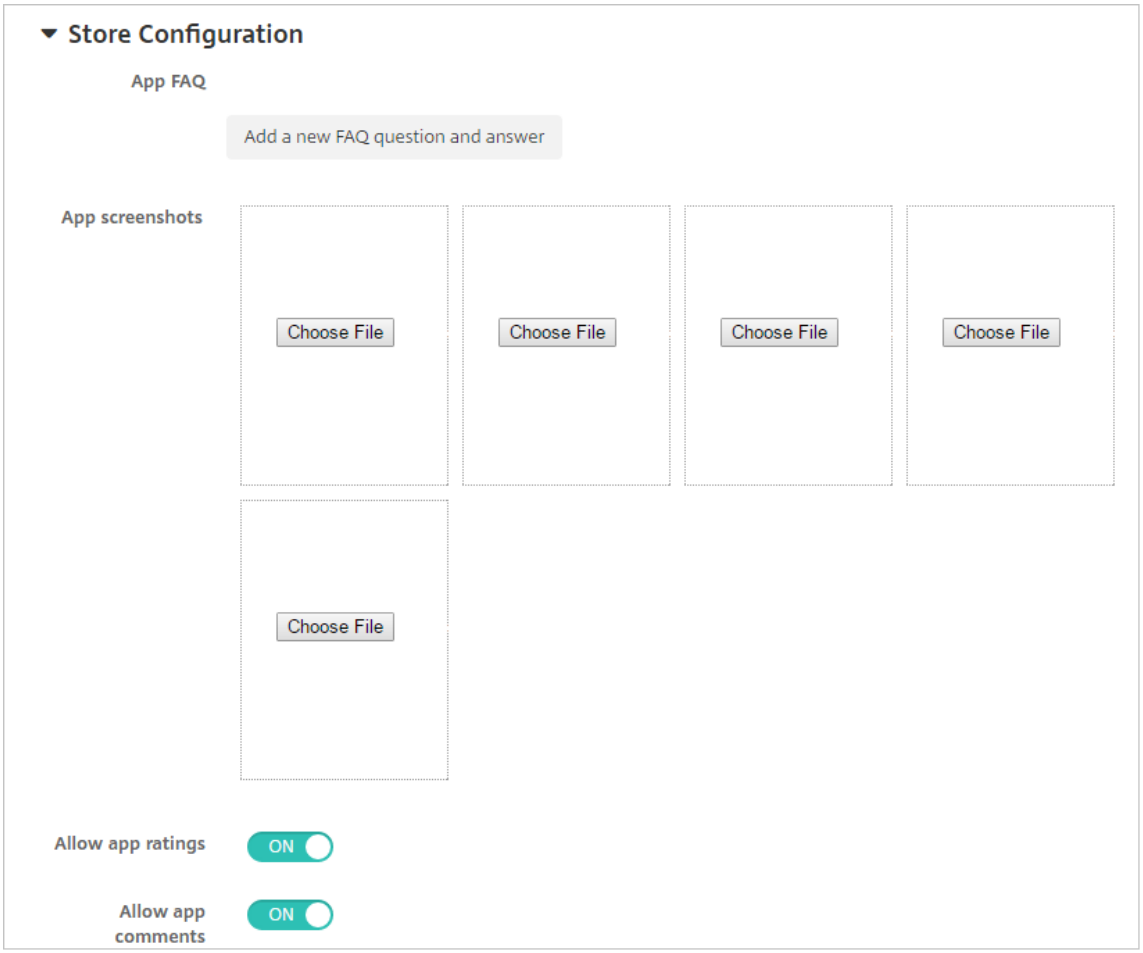
ou GIF. Quando você adicionar um gráfico personalizado, não poderá alterá-lo depois.

3. Quando terminar, clique em **Adicionar**. A página **Detalhes** é exibida.
4. Clique em **Avançar**. A página **Política de aplicativo** é exibida.



5. Defina estas configurações:
   - **Segurança do dispositivo**
   - **Bloquear com jailbreak ou com root:** selecione se os dispositivos com jailbreak ou root têm o acesso ao aplicativo bloqueado. O padrão é **I**.
   - **Requisitos de rede**
   - **Requer WiFi:** selecione se uma conexão WiFi é necessária para executar o aplicativo. O padrão é **O**.
   - **Requer rede interna:** selecione se uma rede interna é necessária para executar o aplicativo. O padrão é **O**.
   - **Redes de WiFi internas:** se você tiver ativado a opção Requer WiFi, digite as redes WiFi internas a serem usadas.
6. Expanda **Configuração da loja**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

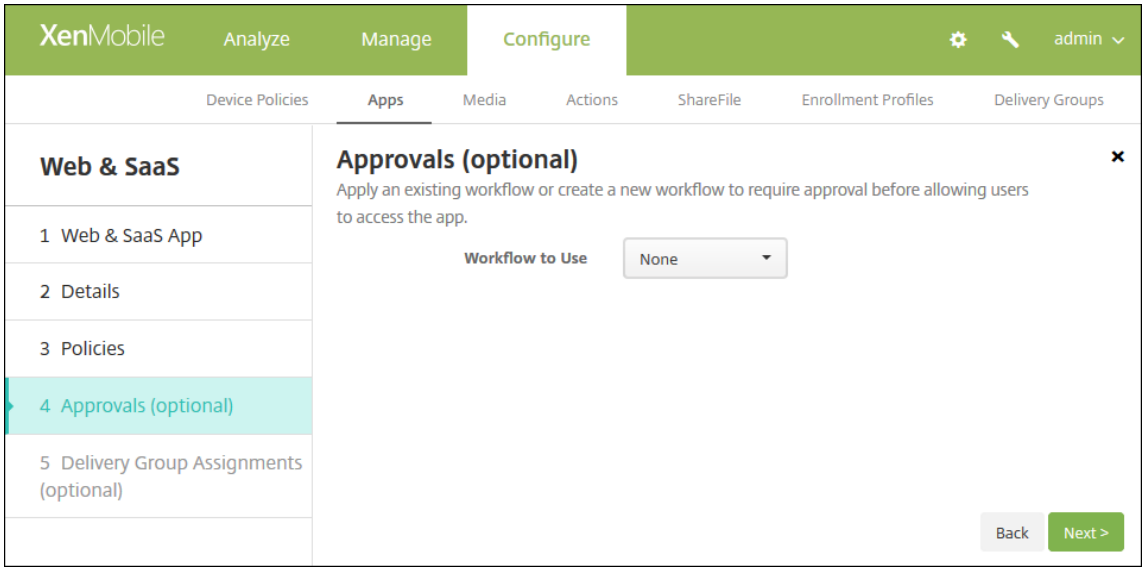


Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- Defina estas configurações:
  - **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
  - **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
  - **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.
  - **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

7. Clique em **Avançar**. A página **Aprovações** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 8.

Configure estas definições se você precisar atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** 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**, defina essas 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 email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
  - Não é Necessário
  - 1 nível
  - 2 níveis
  - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:
  * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
  * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
  * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

8. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
9. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecionar um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.
10. Expanda **Cronograma de implantação** e defina estas configurações:
    - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
    - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
    - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
    - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
    - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

    > Nota:
    >
    > Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
    >
    > O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

11. Clique em **Salvar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

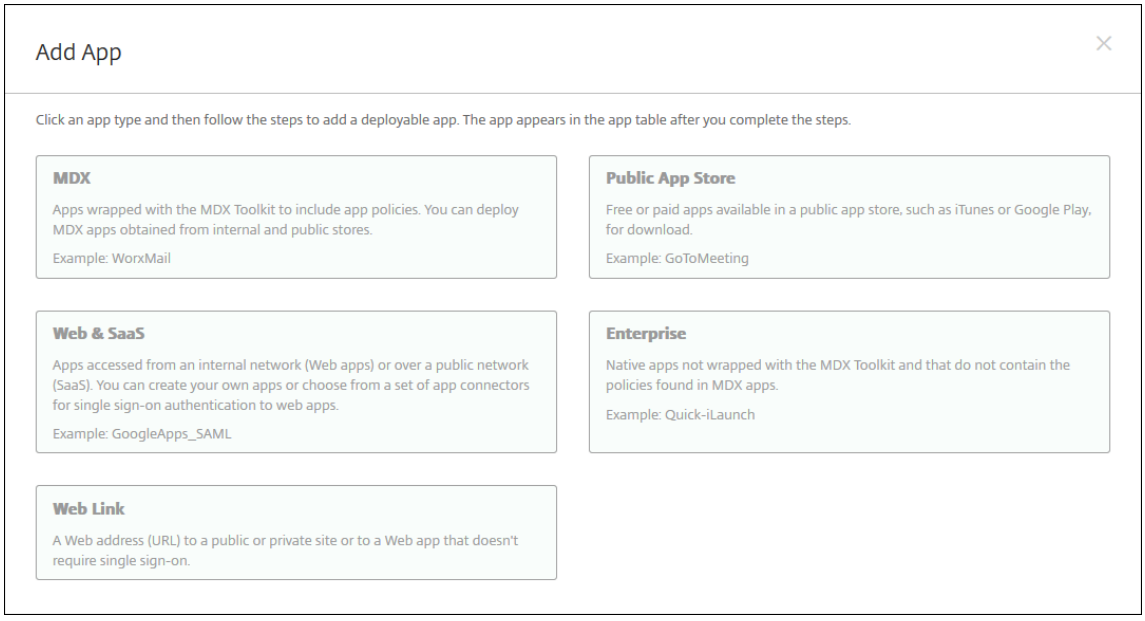
Acrescentar um aplicativo empresarial

Os aplicativos empresariais no XenMobile representam aplicativos nativos que não são preparados com o MDX Toolkit e não contêm as políticas associadas a aplicativos do MDX. Você pode carregar um aplicativo empresarial na guia **Aplicativos** no console XenMobile. Os aplicativos empresariais são compatíveis com as seguintes plataformas (e tipos de arquivo correspondentes):

- iOS (arquivo .ipa)
- Android (arquivo .apk)
- Samsung KNOX (arquivo. apk)
- Android for Work (arquivo. apk)

> Nota:
>
> A adição de aplicativos baixados da Google Play Store como aplicativos corporativos não é suportada. Portanto, adicione aplicativos da Google Play Store como aplicativos da loja de aplicativos pública. Veja Acrescentar um aplicativo de loja de aplicativos pública.

1. No console 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**. A página **Informações do Aplicativo** é exibida.
4. No painel **Informações do aplicativo**, digite as seguintes informações:
   - **Nome:** digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
   - **Descrição:** digite uma descrição opcional para o aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 Criar categorias de aplicativos.

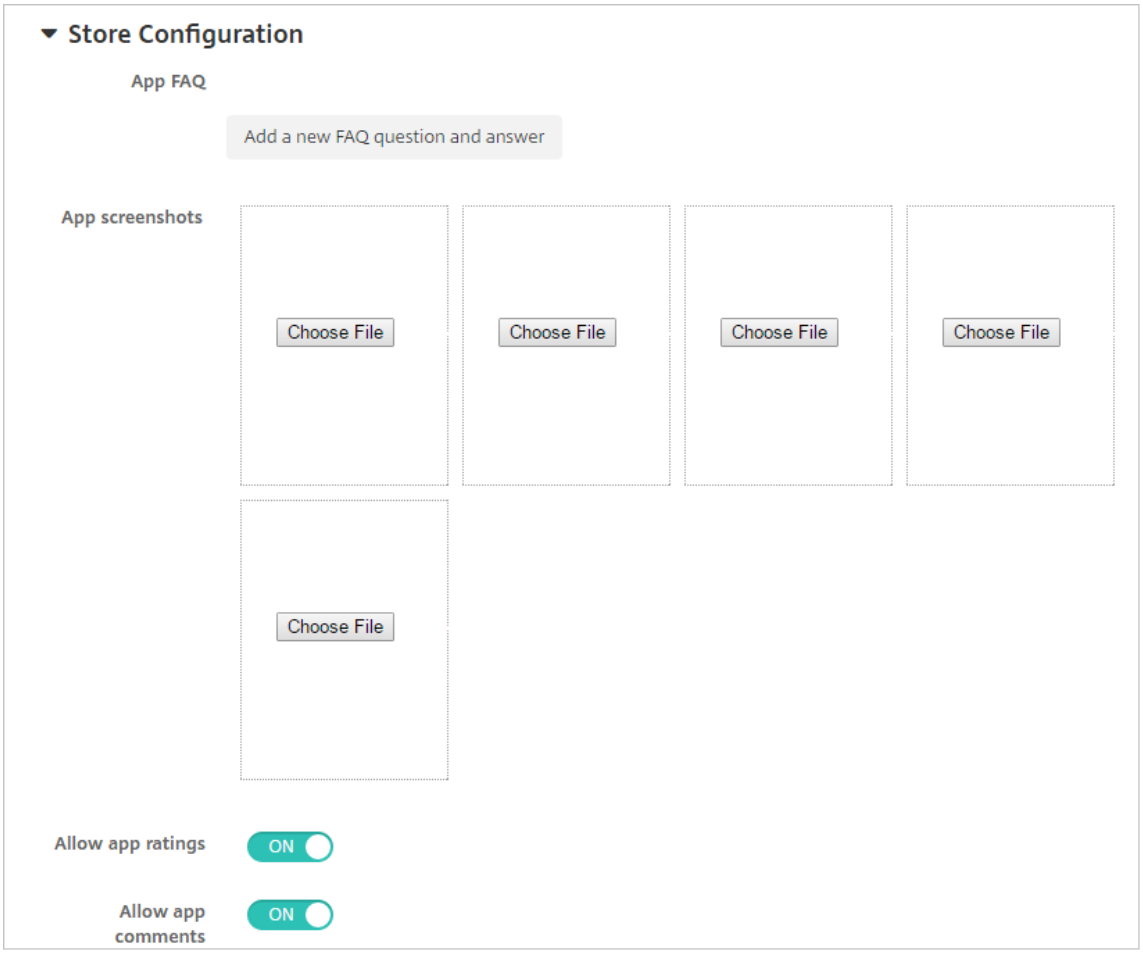
5. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

   Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 10 para saber como definir as regras de implantação dessa plataforma.
7. Para cada plataforma que você selecionou, selecione o arquivo a ser carregado clicando em **Procurar** e navegando até a localização do arquivo.
8. Clique em **Avançar**. A página de informações do aplicativo da plataforma é exibida.
9. Defina as configurações do 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 esse campo.
   - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
   - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional 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 o aplicativo deve ser removido de um dispositivo quando o perfil MDM é removido. O padrão é **I**.
   - **Evitar o backup de dados do aplicativo:** selecione se o aplicativo deve ser impedido de realizar o backup de dados. O padrão é **I**.
   - **Forçar aplicativo a ser gerenciado:** se você estiver instalando um aplicativo não gerenciado, selecione **I** se quiser que os usuários em dispositivos não supervisionados sejam solicitados a permitir o gerenciamento do aplicativo. Essa configuração se aplica aos dispositivos iOS 9.x.

10. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.
11. Expanda **Configuração da XenMobile Store**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

Defina estas configurações:

- **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
- **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
- **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.
- **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

12. Clique em **Avançar**. A página **Aprovações** é exibida.

    Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 13.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configure estas definições se você precisar atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** 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**, defina essas 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 email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
  - **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
    * Não é Necessário
    * 1 nível
    * 2 níveis
    * 3 níveis
  - **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
  - **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
  - Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
    * Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:
      · Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
      · Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
      · As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

13. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
14. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

15. Expanda **Cronograma de implantação** e defina estas configurações:
    - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
    - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
    - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
    - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
    - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

    > Nota:
    >
    > Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
    >
    > O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

16. Clique em **Salvar**.

Adicionar um link da Web

No XenMobile, você pode estabelecer um endereço da Web (URL) para um site público ou privado ou para um aplicativo Web que não requer logon único (SSO).

Você pode configurar os links da Web na guia **Aplicativos** do console XenMobile. Quando você termina de configurar um link da Web, o link é exibido como um ícone de link na lista da tabela **Aplicativos**. Quando os usuários fazem login no Secure Hub, o link é exibido com a lista de aplicativos e áreas de trabalho disponíveis.

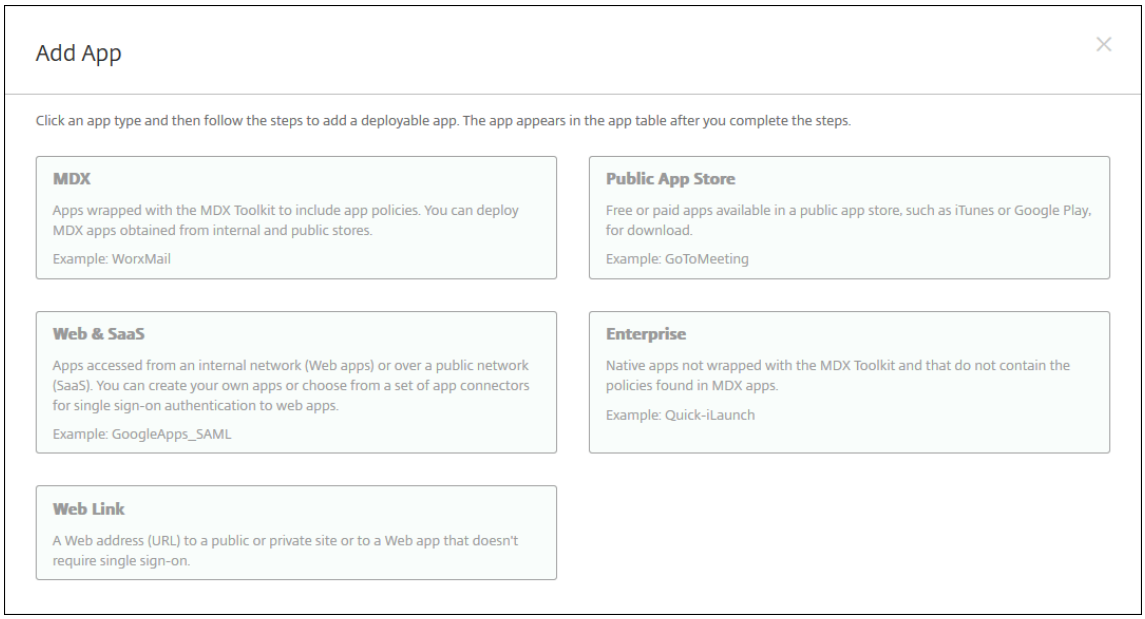
Para adicionar o link, forneça as seguintes informações:

- Nome do link
- Descrição do link
- Endereço da Web (URL)
- Categoria
- Função
- Imagem no formato .png (opcional)

1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.

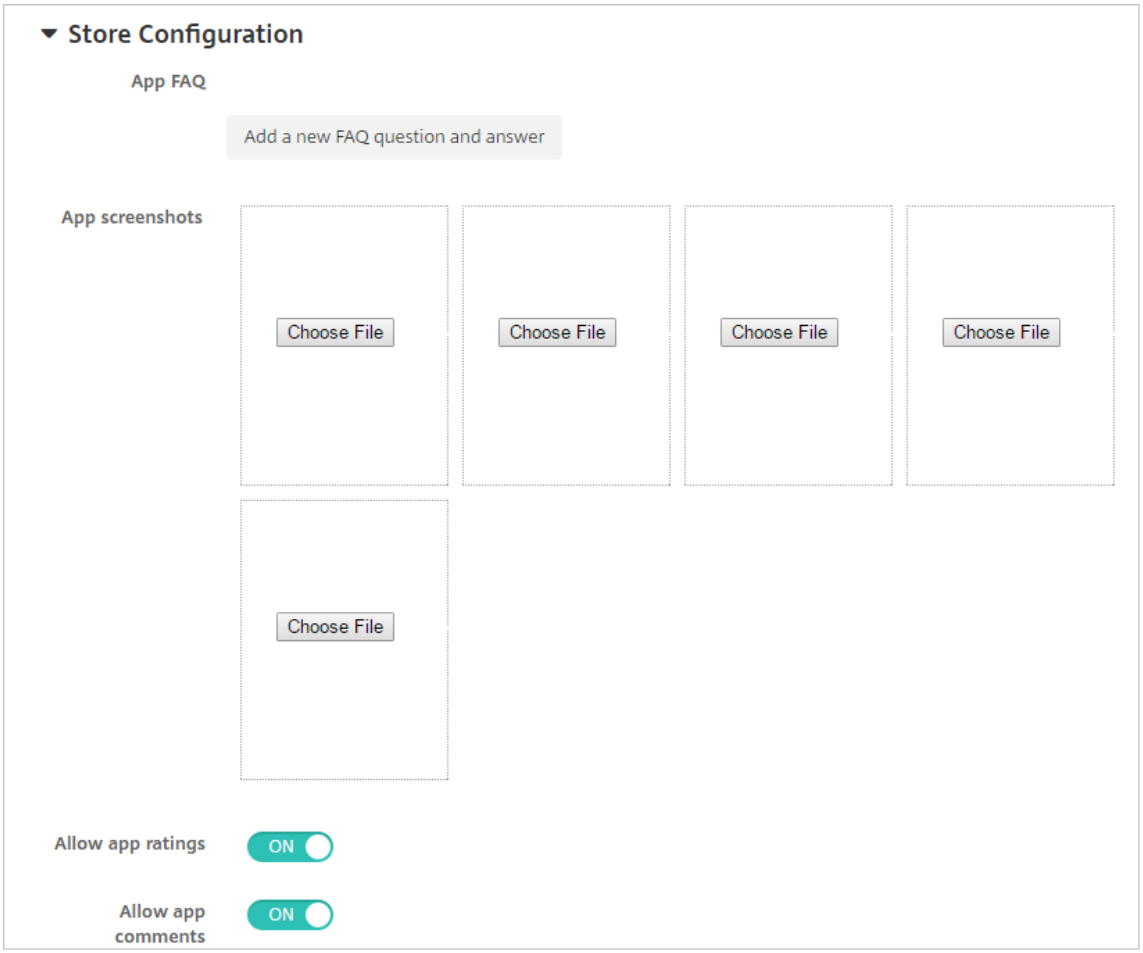
© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



3. Clique em **Link da Web**. A página **Informações do Aplicativo** é exibida.
4. Defina estas configurações:
   - **Nome do aplicativo:** aceite o nome preenchido previamente ou digite um novo nome.
   - **Descrição do aplicativo:** aceite a descrição preenchida previamente ou digite uma.
   - **URL:** aceite o URL preenchido previamente ou digite o endereço Web do aplicativo. Dependendo do conector que você escolher, esse campo poderá conter um espaço reservado que você deve substituir antes que possa continuar para a página seguinte.
   - **O aplicativo está hospedado na rede interna:** selecione se o aplicativo está em execução em um servidor na sua rede interna. Se os usuários se conectarem de uma localidade remota a um aplicativo interno, eles deverão se conectar por meio do NetScaler Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do NetScaler Gateway. O padrão é **O**.
   - **Categoria do aplicativo:** na lista, clique em uma categoria opcional a ser aplicada ao aplicativo.
   - **Imagem:** selecione se a imagem padrão da Citrix deve ser usada ou se a imagem do próprio aplicativo deve ser carregada. O padrão é Usar padrão.
     - Para carregar sua própria imagem, clique em **Procurar** e navegue até o local do arquivo. O arquivo deve ser um arquivo .PNG. Não é possível carregar um arquivo JPEG ou GIF. Quando você adicionar um gráfico personalizado, não poderá alterá-lo depois.
5. Expanda **Configuração da XenMobile Store**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

Defina estas configurações:

- **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
- **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
- **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.
- **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

6. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
7. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

receberão a atribuição de aplicativos.

8. Expanda **Cronograma de implantação** e defina estas configurações:
   - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
   - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
   - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
   - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
   - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

   > Nota:
   >
   > Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.
   >
   > O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

9. Clique em **Salvar**.

Ativar aplicativos do Microsoft Office 365

Você pode abrir o contêiner do MDX para permitir que o Secure Mail, Secure Web e ShareFile transfiram documentos e dados para aplicativos do Microsoft Office 365. Para obter detalhes, consulte Permitindo Interação Segura com Aplicativos do Office 365.

Criar e gerenciar fluxos de trabalho

Você pode usar fluxos de trabalho para gerenciar a criação e a remoção de contas de usuário. Antes de poder usar um fluxo de trabalho, identifique as pessoas em sua organização que têm a autoridade para aprovar solicitações de conta de usuário. Em seguida, você pode usar o modelo de fluxo de trabalho para criar e aprovar solicitações de conta de usuário.

Quando você configura o XenMobile pela primeira vez, define as configurações de email de fluxo de trabalho, o que deve ocorrer antes de você poder usar os fluxos de trabalho. Você pode alterar as configurações de email de fluxo de trabalho a qualquer momento. Essas configurações incluem o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

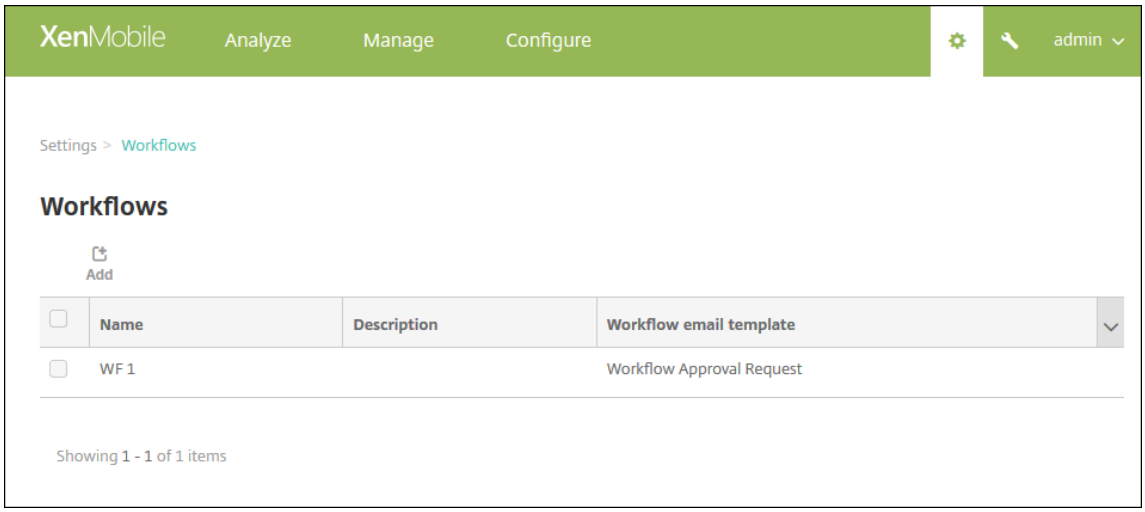
servidor de email, a porta, o endereço de email, e se a solicitação para criar a conta de usuário requer aprovação.

Você pode configurar os fluxos de trabalho em dois lugares no XenMobile:

- Na página Fluxos de trabalho no console XenMobile. Na página Fluxos de trabalho, você pode configurar vários fluxos de trabalho para serem usados com as configurações do aplicativo. Ao configurar fluxos de trabalho na página Fluxos de trabalho, você pode selecionar o fluxo de trabalho durante a configuração do aplicativo.
- Ao configurar um conector de aplicativo, forneça um nome de fluxo de trabalho e configure os indivíduos que podem aprovar a solicitação de conta de usuário.

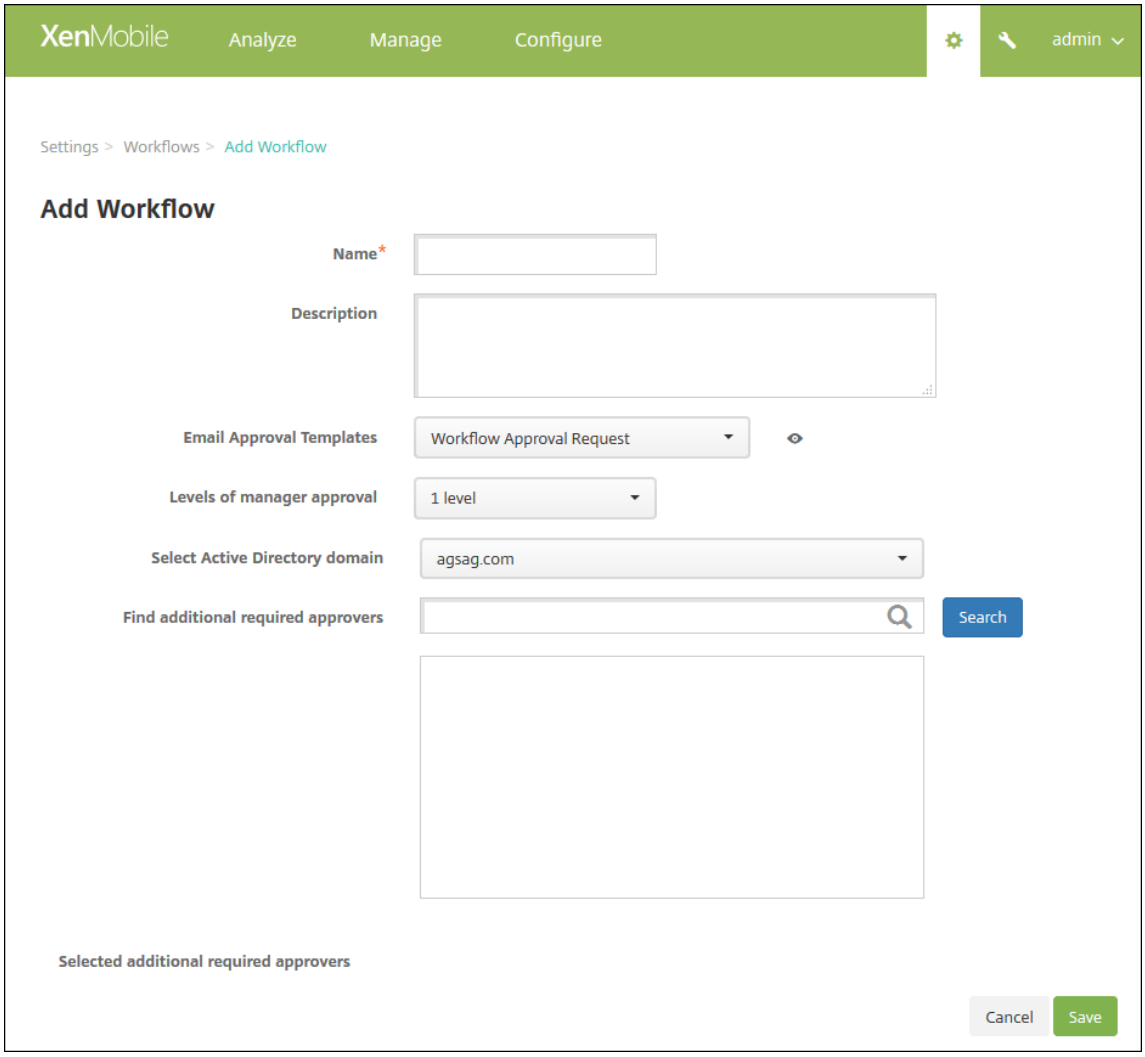
Você pode atribuir até três níveis à aprovação do gerente de contas de usuário. Se você precisar que outras pessoas aprovem a conta de usuário, poderá procurar e selecionar pessoas por nome ou endereço de email. Quando o XenMobile encontrar a pessoa, adicione-a ao fluxo de trabalho. Todos os indivíduos do fluxo de trabalho recebem emails para aprovar ou negar a nova conta de usuário.

1. No console 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.

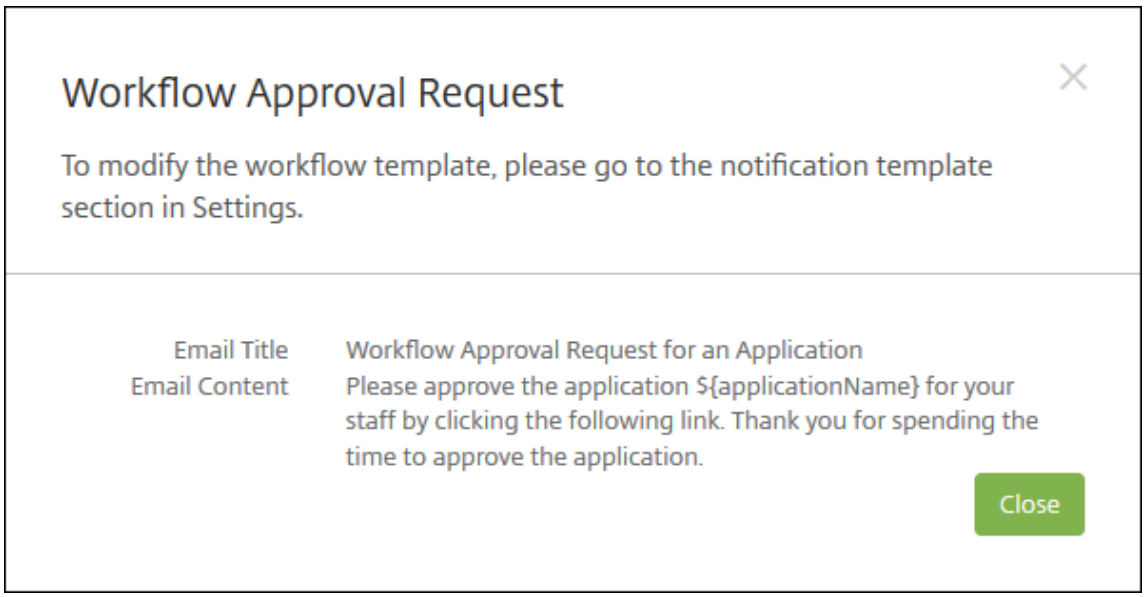
© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Defina 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 email:** na lista, selecione o modelo de aprovação a ser atribuído. Você pode criar modelos de emails na seção Modelos de notificação sob Configurações no console XenMobile. Quando você clica no ícone de olho à direita deste campo, a caixa de diálogo abaixo é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
  - Não é Necessário
  - 1 nível
  - 2 níveis
  - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
- Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:
  - Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
  - Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
  - As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você desejar remover.

5. Clique em **Salvar**. O fluxo de trabalho criado é exibido na página **Fluxos de trabalho**.

   Depois de criar o fluxo de trabalho, você pode exibir os detalhes do fluxo de trabalho, exibir os aplicativos associados a ele ou excluí-lo. Você não pode editar um fluxo de trabalho depois de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tê-lo criado. Se você precisar de um fluxo de trabalho com níveis diferentes de aprovação ou aprovadores diferentes, deverá criar outro fluxo de trabalho.

Para ver detalhes e excluir um fluxo de trabalho

1. Na página **Fluxos de trabalho**, selecione um fluxo de trabalho clicando na linha da tabela ou marcando 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:
   >
   > Você não pode desfazer essa operação.

Tipos de conector de aplicativo

August 24, 2018

A tabela a seguir lista os conectores e os tipos de conectores que estão disponíveis no XenMobile quando você adiciona um aplicativo da 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 é compatível com o gerenciamento de conta de usuário, o que permite criar novas contas automaticamente ou usando um fluxo de trabalho.

Nome do conector	SSO SAML	Dá suporte ao gerenciamento de conta de usuário
EchoSign_SAML	S	S
Globoforce_SAML		**Nota:** quando você usar esse conector, ative a opção User Management for Provisioning para garantir a integração perfeita do SSO.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome do conector	SSO SAML	Dá suporte ao gerenciamento de conta de usuário
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

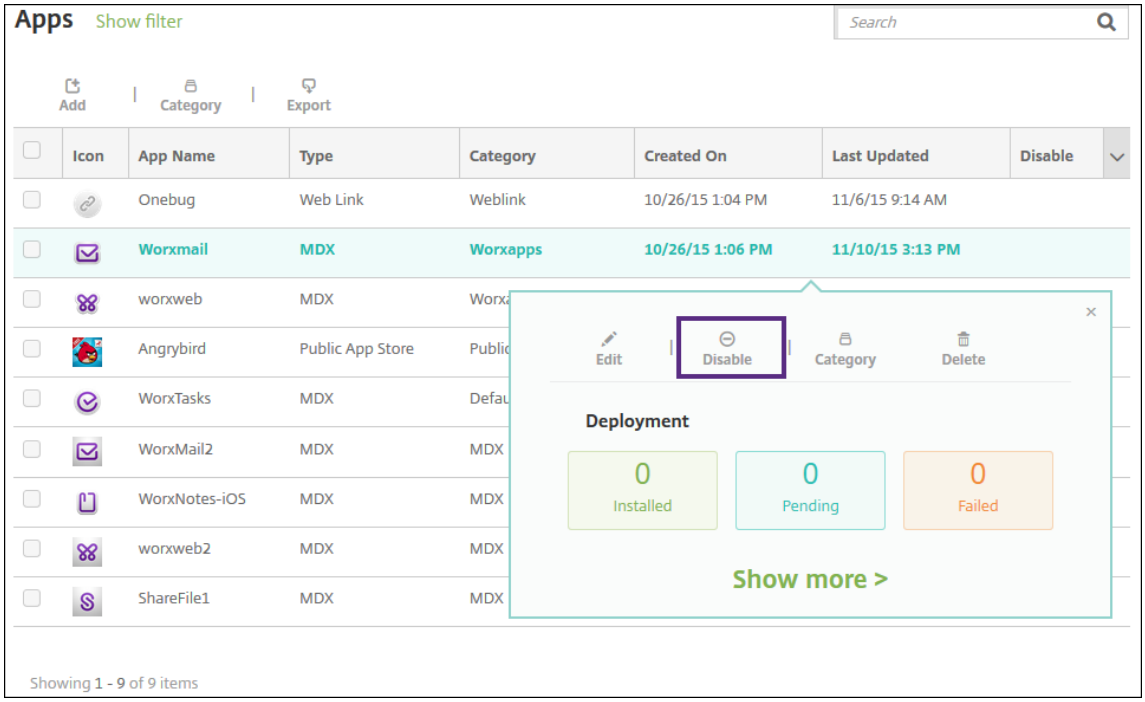
Atualizar aplicativos MDX ou empresariais

March 6, 2019

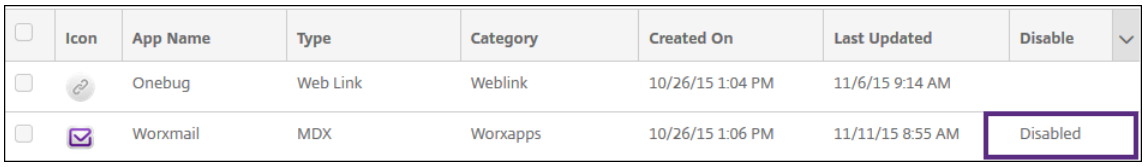
Para atualizar um aplicativo MDX ou Empresarial no XenMobile, desative o aplicativo no console do XenMobile e carregue a nova versão do aplicativo.

1. No console 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 para fins de gerenciamento de aplicativos empresariais), faça o seguinte:
   - Na tabela **Aplicativos**, marque a caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.
   - Clique em **Desativar** no menu que aparece.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Clique em **Desativar** na caixa de diálogo de confirmação. *Desativado* é exibido na coluna **Desativar** do aplicativo.



> Nota:
>
> Desativar um aplicativo coloca o aplicativo no modo de manutenção. Enquanto o aplicativo está desativado, os usuários não podem se reconectar ao aplicativo depois que fazem logoff. Desativar um aplicativo é uma configuração opcional, mas recomendamos desativar o aplicativo para evitar problemas com a funcionalidade dele. Os problemas podem resultar de atualizações da política, por exemplo, ou quando os usuários solicitam um download ao mesmo tempo que você está carregando o arquivo para o XenMobile.

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 exibido. A página **Informações do aplicativo** é exibida com as plataformas que você escolheu originalmente para o aplicativo selecionado.
5. Defina 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Clique em **Avançar**. A primeira página selecionada da plataforma é exibida. Faça o seguinte para cada plataforma selecionada:
    - Escolha o arquivo de substituição que você quer carregar clicando em **Carregar** e navegue para a localização do arquivo. O aplicativo é carregado para o XenMobile.
    - Opcionalmente, altere os detalhes de aplicativo e as configurações de política para a plataforma.
    - Opcionalmente, configure as regras de implantação e as configurações da XenMobile Store. Para obter informações, consulte Adicionar um aplicativo MDX em Adicionar aplicativos.
7. Clique em **Salvar**. A página **Aplicativos** é exibida.
8. Se você tiver desativado o aplicativo na Etapa 2, faça o seguinte:
    - Na tabela **Aplicativos**, clique para selecionar o aplicativo atualizado e, no menu exibido, clique em **Ativar**.
    - Na caixa de diálogo de confirmação exibida, clique em **Ativar**. Os usuários agora podem acessar o aplicativo e recebem um aviso de notificação solicitando que eles atualizem o aplicativo.

Resumo das políticas de aplicativos MDX

August 31, 2018

Para obter uma tabela que lista as políticas de aplicativos MDX para iOS e Android com anotações sobre restrições e recomendações da Citrix, consulte Resumo das políticas de aplicativos MDX na documentação do MDX Toolkit.

Identidade visual do XenMobile Store e do Citrix Secure Hub

April 15, 2019

Você pode definir a forma como os aplicativos aparecem na loja e adicionar um logotipo para identificar o Secure Hub e a XenMobile Store. Esses recursos de identidade visual estão disponíveis para dispositivos iOS e Android.

> Nota:
>
> Antes de começar, verifique se a imagem personalizada está pronta e acessível.

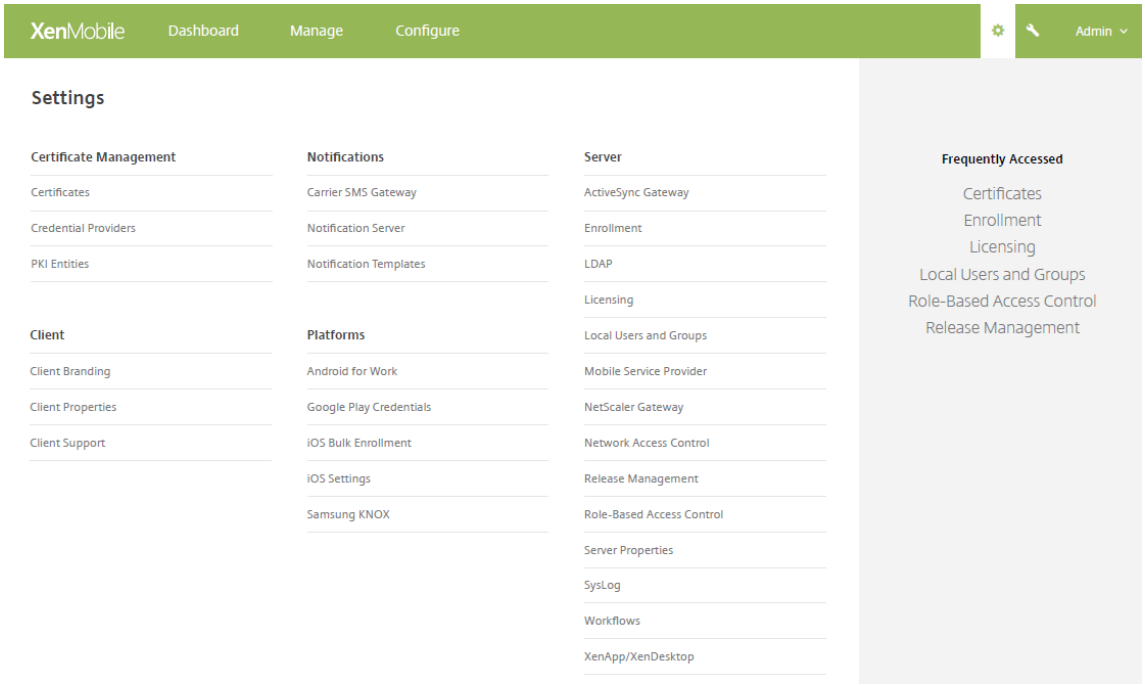
A imagem personalizada deve atender a estes requisitos:

- O arquivo deve estar no formato .png

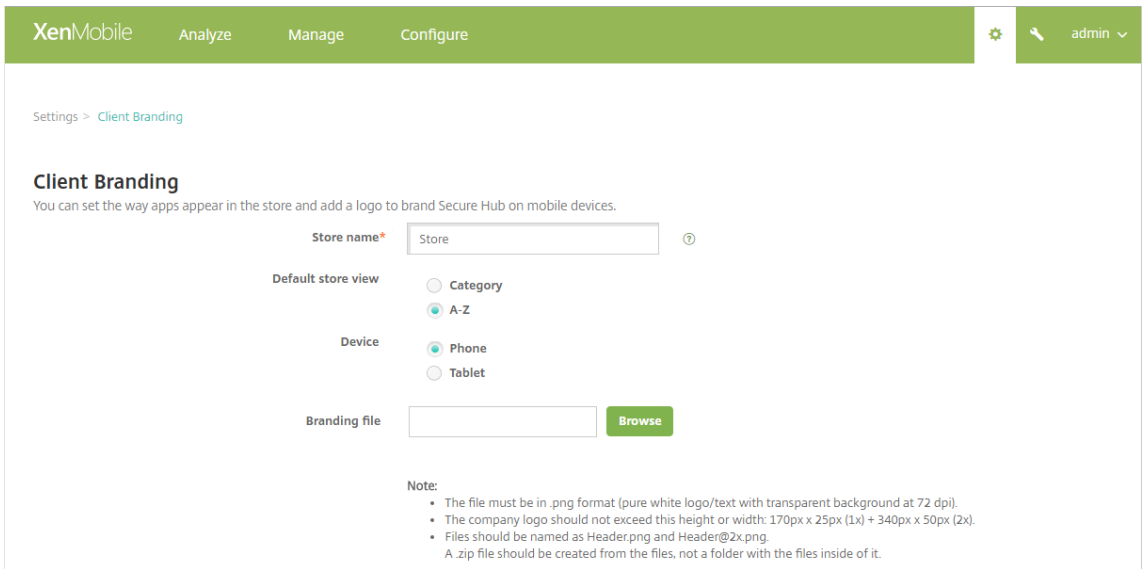
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Use um logotipo em branco puro ou texto com um fundo transparente em 72 ppp.
- O logotipo da empresa não deve exceder esta altura ou largura: 170 pixels x 25 pixels (1x) e 340 pixels x 50 pixels (2x).
- Dê os seguintes nomes aos arquivos: Header.png e Header@2x.png.
- Crie um arquivo .zip com os arquivos, não uma pasta que contenha os arquivos.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.



2. Em **Cliente**, clique em **Identidade visual do cliente**. A página **Identidade Visual do Cliente** é exibida.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Faça as seguintes configurações:

- **Nome do armazenamento:** o nome do armazenamento será exibido nas informações de conta do usuário. Alterar o nome também altera a URL usada para acessar os serviços de armazenamento. Geralmente, não é necessário alterar o nome padrão.

  > **Importante:**
  >
  > O nome da loja só pode conter caracteres alfanuméricos.

- **Exibição de armazenamento padrão:** selecione **Categoria** ou **A-Z**. O padrão é **A-Z**
- **Dispositivo:** selecione **Telefone** ou **Tablet**. O padrão é **Telefone**.
- **Arquivo de identidade visual:** selecione uma imagem ou um arquivo .zip de imagens a ser usado para a identidade visual clicando em **Procurar** e navegando até a localização do arquivo.

3. Clique em **Salvar**.

Para implantar esse pacote em dispositivos de usuários, crie um pacote de implantação e implante o pacote.

Citrix Launcher

April 15, 2019

O Citrix Launcher permite que você personalize a experiência do usuário para dispositivos Android implantados pelo XenMobile. A versão mínima do Android com suporte para o gerenciamento do Secure Hub do Citrix Launcher é o Android 4.0.3. O Citrix Launcher e a política do 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:

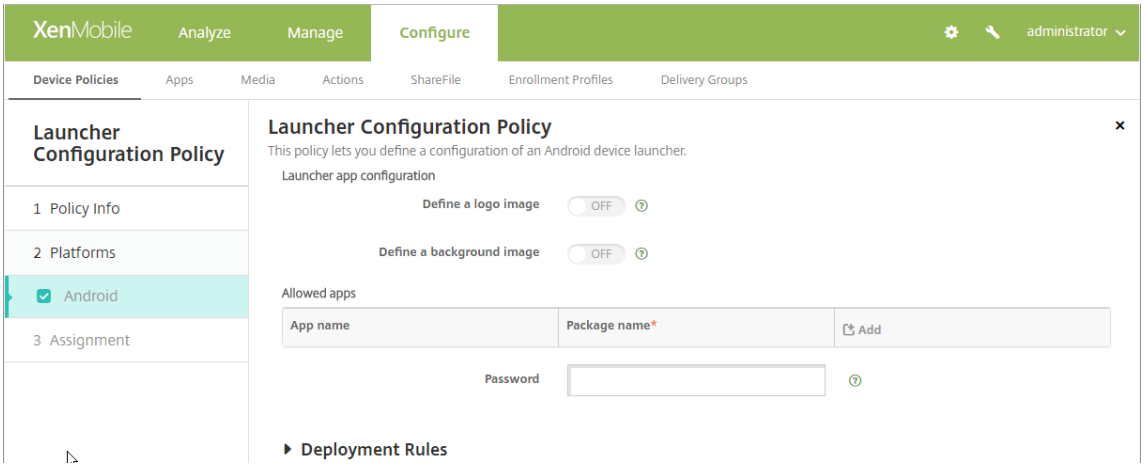
- Gerenciar dispositivos Android para que os usuários possam acessar somente os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizado para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizado para o Citrix Launcher.
- Especifique uma senha que os usuários devem digitar para sair do Launcher.

Embora o Citrix Launcher permita aplicar essas restrições em nível de dispositivo, o iniciador concede aos usuários acesso incorporado a configurações de dispositivos, como configurações de Wi-Fi, Bluetooth e de código secreto de dispositivo. O Citrix Launcher não foi criado com a intenção de ser uma camada extra de segurança além da que a plataforma de dispositivo já fornece.

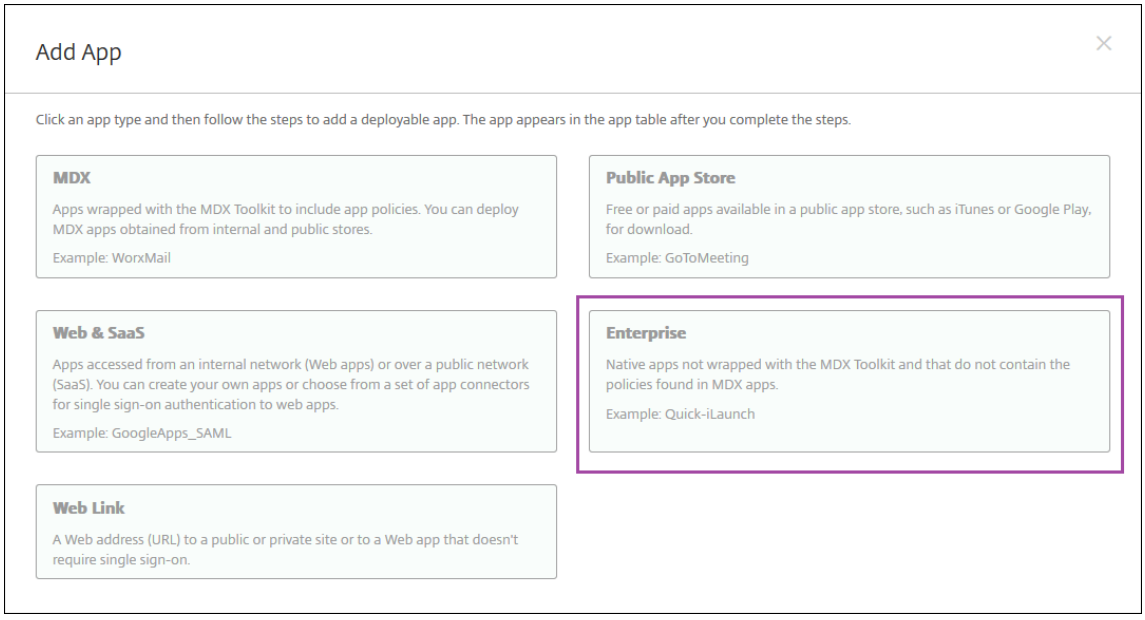
Para fornecer o Citrix Launcher para dispositivos Android, siga estes procedimentos gerais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Baixe o aplicativo Citrix Launcher da página de Transferências do Citrix XenMobile para obter sua edição do XenMobile. O nome do arquivo é CitrixLauncher.apk. O arquivo está pronto para carregar no XenMobile e não requer preparação.
2. Adicione a política de dispositivo **Política de Configuração do Launcher**. Vá até **Configurar > Políticas de dispositivo**, clique em **Adicionar** e, na caixa de diálogo **Adicionar uma nova política**, comece a digitar **Launcher**. Para obter mais informações, consulte Política de configuração do Launcher.



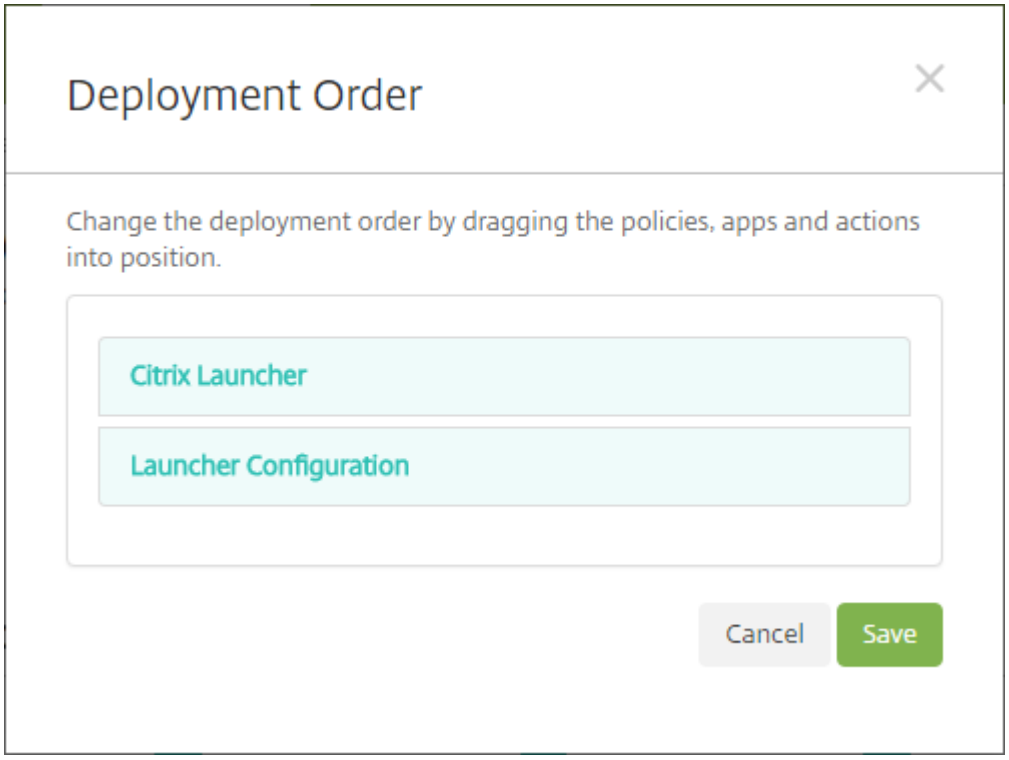
3. Adicione o aplicativo Citrix Launcher ao XenMobile como um aplicativo corporativo. Em **Configurar > Aplicativos**, clique em **Adicionar** e, em seguida, clique em **Empresarial**. Para obter mais informações, consulte Acrescentar um aplicativo empresarial.



4. Crie um grupo de entrega para o Citrix Launcher com a configuração a seguir em **Configurar > Grupos de entrega**.
    - Na página **Políticas**, adicione a **Política de configuração do Launcher**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Na página **Aplicativos**, arraste **Citrix Launcher** até **Aplicativos obrigatórios**.
- Na página **Resumo**, clique em **Ordem de implantação** e verifique se o aplicativo **Citrix Launcher** precede a política **Configuração do Launcher**.



Para obter mais informações, consulte Implantar recursos.

Programa de compra por volume do iOS

April 15, 2019

Você pode gerenciar o licenciamento de aplicativos iOS usando o Apple iOS Volume Purchase Program (VPP). O VPP simplifica o processo para localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Com VPP, você pode usar o XenMobile para distribuir aplicativos de loja de aplicativos pública. Não há suporte para VPP para aplicativos móveis de produtividade ou para aplicativos preparados por meio do MDX Toolkit. Embora você possa distribuir os aplicativos de loja pública do XenMobile com o VPP, a implantação não é otimizada. São necessários mais melhorias no XenMobile Server e no armazenamento do Secure Hub para resolver as limitações. Para obter uma lista de problemas conhecidos com a implantação do XenMobile aplicativos de loja pública por meio de VPP e possíveis soluções alternativas, consulte este artigo no Citrix knowledge center.

Com VPP, você pode distribuir os aplicativos aplicáveis diretamente para os dispositivos. Ou você

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pode atribuir conteúdo para seus usuários usando códigos resgatáveis. Você pode fazer as configurações específicas do VPP do iOS no XenMobile.

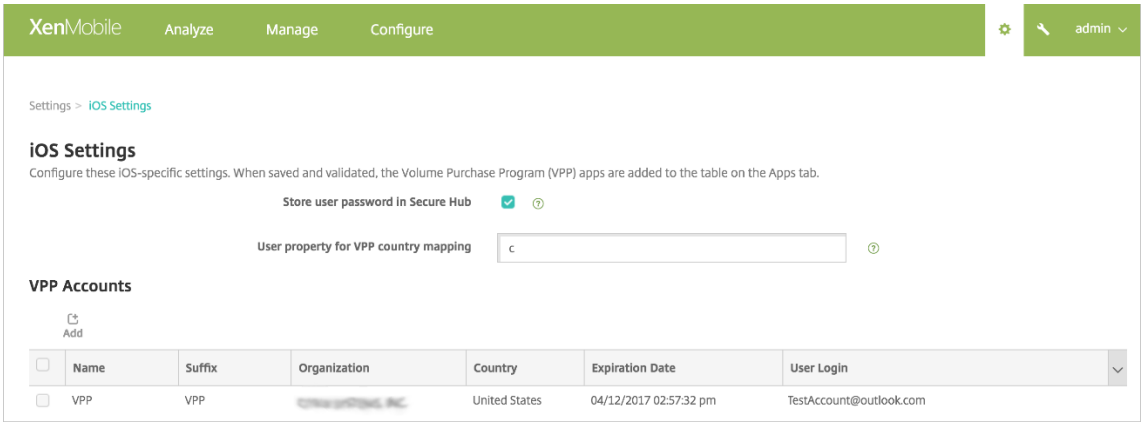
O XenMobile reimporta periodicamente as licenças do VPP da Apple para garantir que elas reflitam todas as alterações. Essas alterações incluem quando você exclui manualmente um aplicativo importado do VPP. Por padrão, o XenMobile atualiza a linha de base da licença do VPP no mínimo a cada 720 minutos. Você pode alterar o intervalo de linha de base por meio da propriedade de servidor, intervalo de linha de base do VPP (vpp.baseline). Para obter informações, consulte Propriedades do servidor.

Este artigo aborda usando VPP com licenças gerenciadas, o que permite que você usar o XenMobile para distribuir aplicativos. Se você atualmente usa códigos de resgate e deseja mudar para distribuição gerenciada, consulte o documento do Suporte da Apple sobre Como migrar dos códigos de resgate para a distribuição gerenciada com o Volume Purchase Program.

Para obter informações sobre o VPP do iOS, consulte.https://vpp.itunes.apple.com/us/store Para se inscrever no VPP, vá para https://deploy.apple.com/qforms/open/register/index/avs. Para acessar sua loja VPP no iTunes, vá para https://vpp.itunes.apple.com/?l=en.

Depois que você salva as configurações de VPP do iOS no XenMobile, os aplicativos comprados aparecem na página **Configurar > Aplicativos** no console XenMobile.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Plataforma**, clique em **Configurações de iOS**. A página de configuração **Configurações de iOS** é exibida.

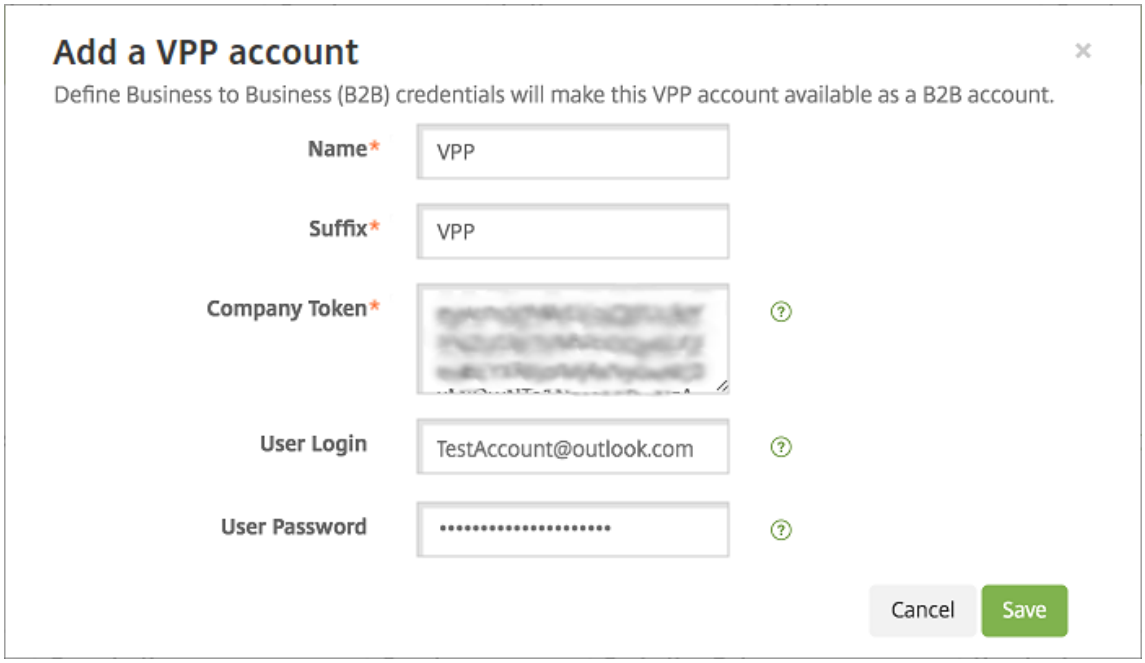


3. Defina estas configurações:
   - **Armazenar a senha de usuário no Secure Hub:** Selecione se um nome do usuário e uma senha devem ser armazenados no Secure Hub para a autenticação do XenMobile. O padrão é armazenar as informações seguras usando este método de segurança.
   - **Propriedade de usuário para mapeamento de país do VPP:** Digite um código para permitir que os usuários baixem aplicativos de lojas de aplicativos específicas de cada país.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O XenMobile usa esse mapeamento para escolher o pool de propriedades do VPP. Por exemplo, se a propriedade do usuário for Estados Unidos, ele não poderá baixar aplicativos se o código VPP do aplicativo for para o Reino Unido. Contate o administrador do plano VPP para obter mais informações sobre o código de mapeamento do país.

4. Para cada conta VPP que você desejar adicionar, clique em **Adicionar**. A caixa de diálogo **Adicionar conta VPP** é exibida.



5. Defina estas configurações para cada conta que você adicionar:

> Nota:
>
> Se você estiver usando o Apple Configurator 1, carregue um arquivo de licença: vá até **Configurar > Aplicativos**, vá para uma página da plataforma e expanda **Volume Purchase Program**.

- **Nome:** Digite o nome da conta VPP.
- **Sufixo:** Digite o sufixo a ser exibido com os nomes dos aplicativos obtidos usando a conta VPP. Por exemplo, se você inserir **VPP**, o aplicativo Secure Mail é exibido na lista de aplicativos, como **Secure Mail - VPP**.
- **Token da empresa:** Digite ou copie e cole o token de serviço de VPP obtido da Apple. Para obter o token: Na página **Account Summary** do portal do Apple VPP, clique no botão **Download** para gerar e baixar o arquivo de VPP. O arquivo contém o token de serviço e outras informações, como o código do país e a expiração. Salve o arquivo em um local seguro.
- **Login de usuário:** Digite um nome opcional de administrador de conta de VPP autorizada usado para importar aplicativos B2B personalizados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

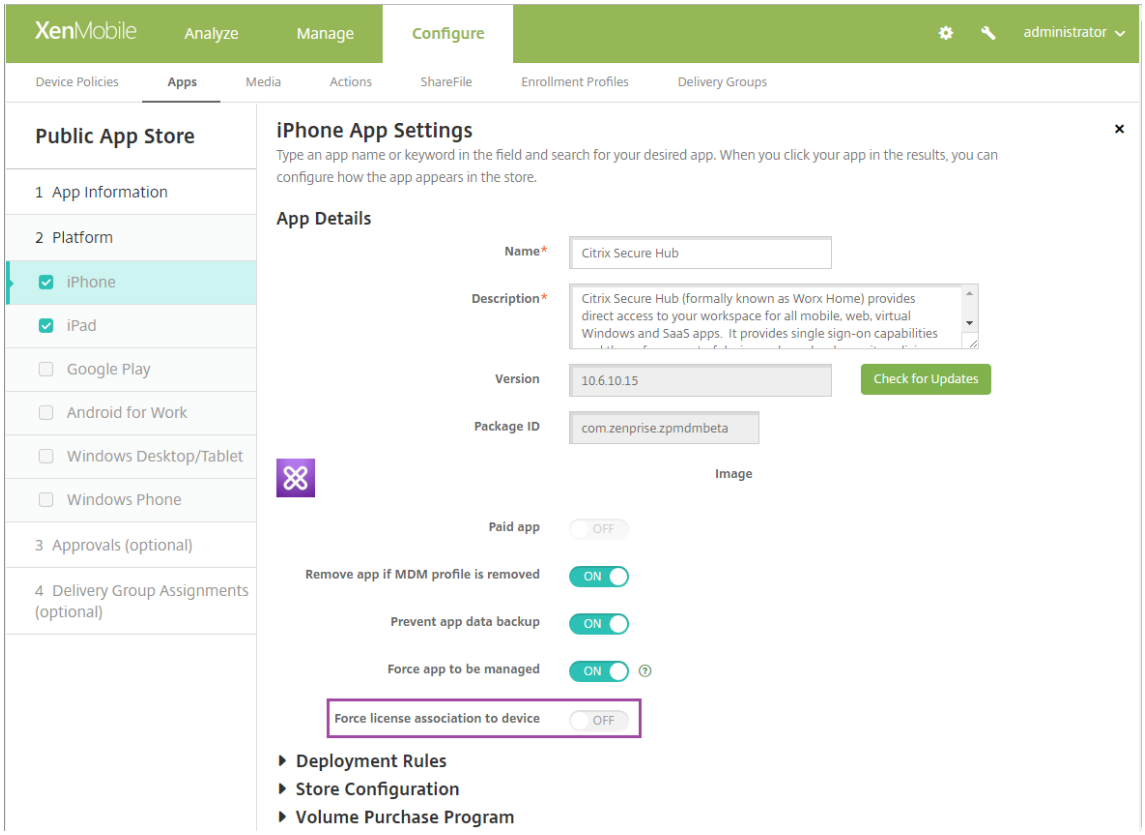
- **Senha de usuário:** Digite a senha de administrador de conta de VPP.

6. Clique em **Salvar** para fechar a caixa de diálogo.
7. Clique em **Salvar** para salvar as configurações do iOS.

   É exibida uma mensagem que informa que o XenMobile adiciona os aplicativos à página **Configurar > Aplicativos**. Naquela página, observe que os nomes dos aplicativos da sua conta do VPP contêm o sufixo que você forneceu na configuração acima.

Você pode agora definir as configurações de aplicativo VPP e, em seguida, ajustar as entrega grupo e o dispositivo as configurações de política para aplicativos VPP. Depois de concluir essas configurações, os usuários podem registrar seus dispositivos. A seguir indica fornecem considerações para esses processos.

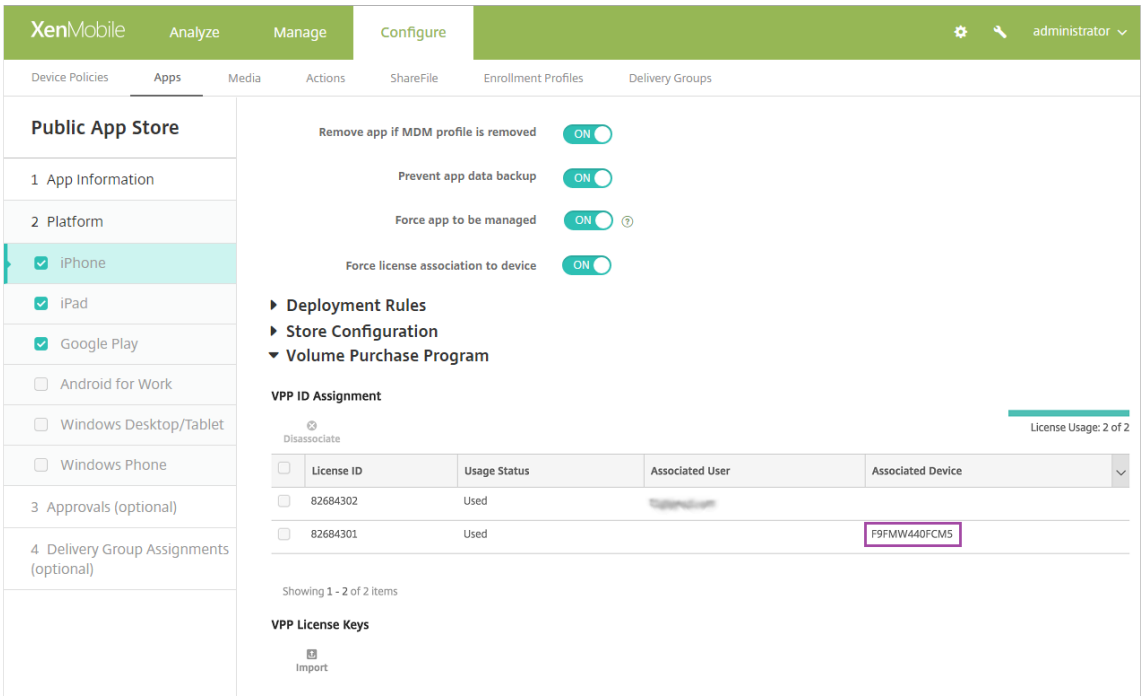
- Ao definir as configurações de aplicativo VPP (**Configurar > Aplicativos**), ativar **Forçar associação de licença ao dispositivo**. Uma vantagem de usar o Apple VPP e DEP com dispositivos supervisionados: a capacidade de usar o XenMobile para atribuir o aplicativo no nível de dispositivo (em vez de usuário). Desse modo, você não precisa usar um dispositivo com Apple ID. Além disso, os usuários não recebem um convite para participar do programa VPP. Os usuários também podem baixar aplicativos sem entrar na respectiva conta do iTunes.



Para exibir as informações VPP para esse aplicativo, expanda **Volume Purchase Program**. Na tabela **Atribuição de ID de VPP**, note que a licença é associada a um dispositivo. O número de

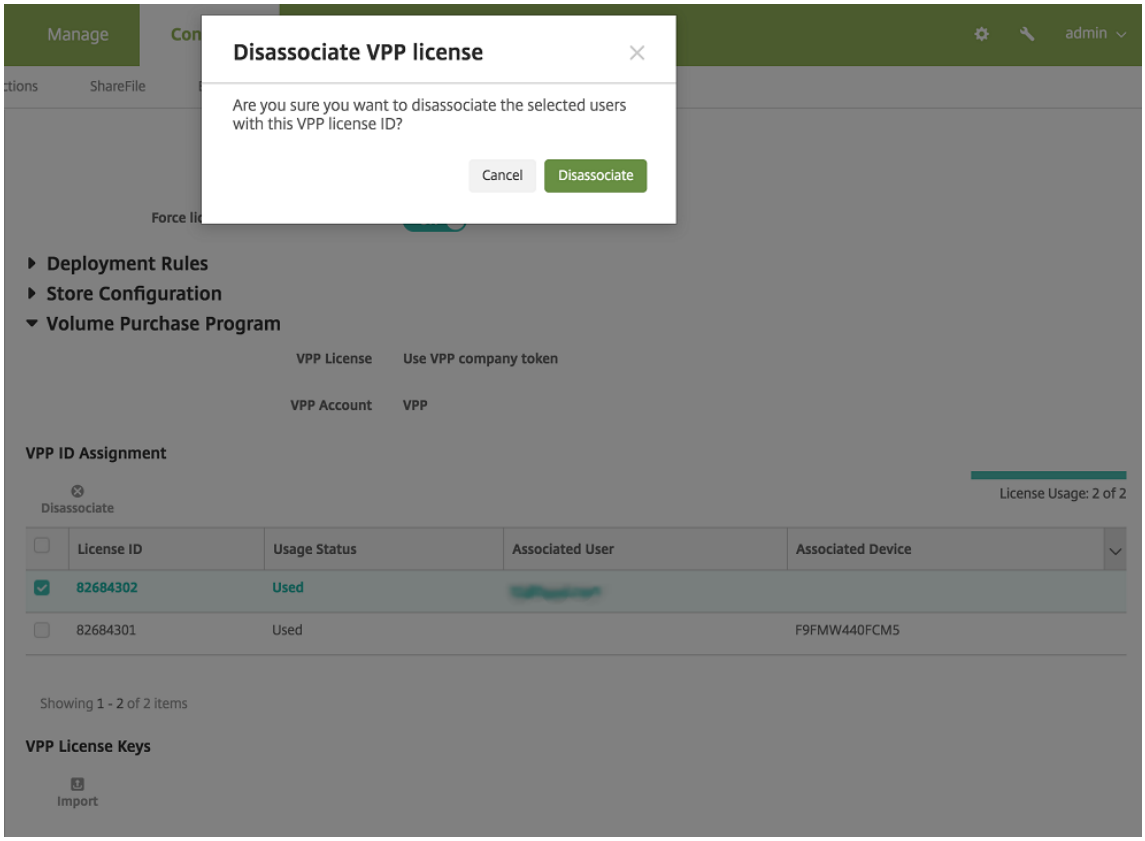
© 1999-2019 Citrix Systems, Inc. All rights reserved.

série do dispositivo é exibido na coluna **Dispositivo associado**. Se o usuário remove o token e, em seguida, importa-o novamente, a palavra **Oculto** é exibida em vez do número de série, devido a restrições de privacidade da Apple.



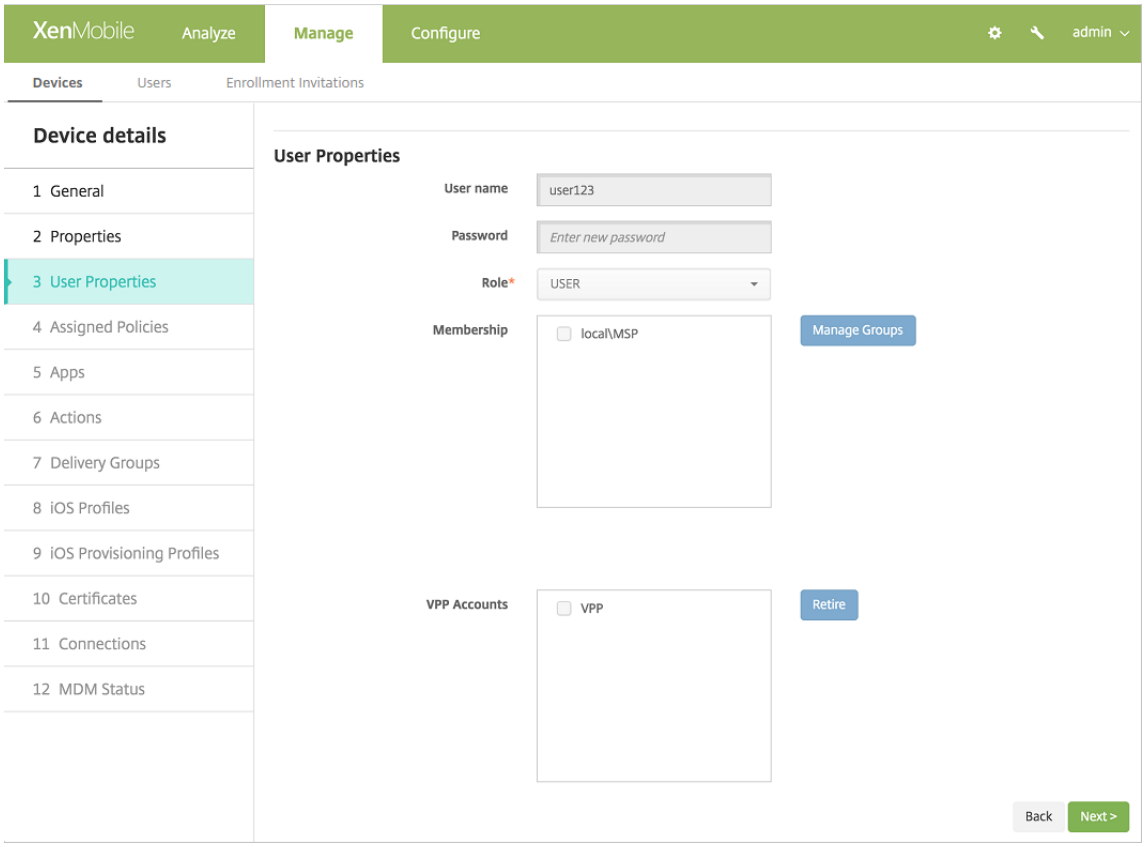
Para desassociar uma licença, clique na linha da licença e clique em **Desassociar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



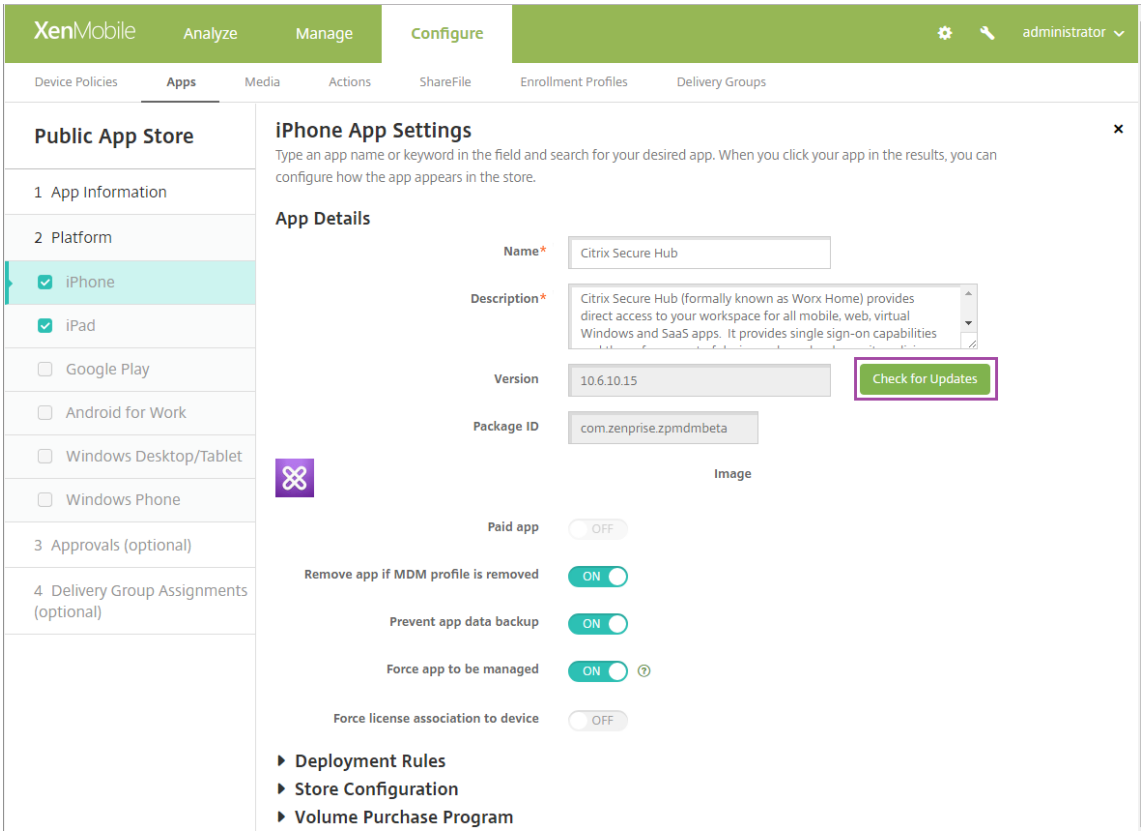
Se você associar licenças de VPP usuários, XenMobile integra os usuários em sua conta VPP e associa sua ID do iTunes com a conta VPP. A ID do iTunes dos usuários nunca é visível para a sua empresa para o XenMobile Server. Apple transparente cria a associação para manter a privacidade do usuário. Você pode desativar um usuário do programa VPP, para desassociar a todas as licenças da conta de usuário. Para desativar um usuário, vá para **Gerenciar > Dispositivos**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

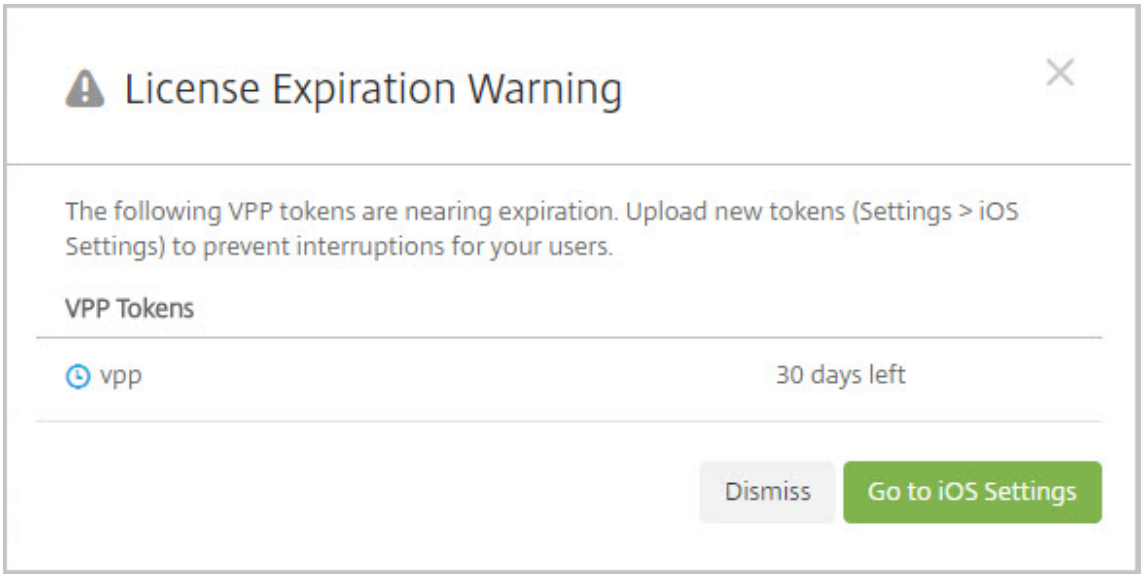


- Quando você atribuir um aplicativo a um grupo de entrega, como padrão, o XenMobile identifica o aplicativo como um aplicativo opcional. Para garantir que o XenMobile implante um aplicativo em dispositivos, vá até **Configurar > Grupos de entrega.** Na página **Aplicativos**, mova o aplicativo para a lista **Aplicativos obrigatórios**.
- Quando uma atualização de um aplicativo de loja de aplicativos pública está disponível: quando o VPP envia o aplicativo, o aplicativo não é atualizado automaticamente nos dispositivos até que você verifique se há atualizações e as aplique. Para enviar uma atualização para o Secure Hub quando atribuídas ao dispositivo e não a um usuário, faça o seguinte: Na página **Configurar > Aplicativos**, em uma página de plataforma, clique em **Verificar se há atualizações** e aplique a atualização.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



O XenMobile exibe um Aviso de Expiração de Licença quando os tokens Apple VPP estão prestes a expirar ou expiraram.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

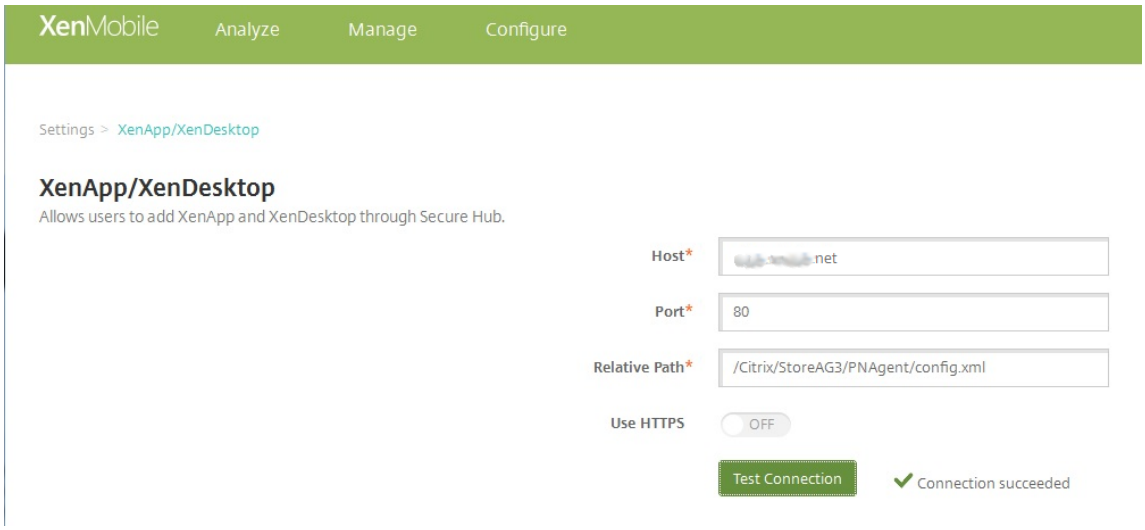
XenApp e XenDesktop através do Citrix Secure Hub

August 24, 2018

O XenMobile pode coletar aplicativos do XenApp e do XenDesktop e disponibilizá-los para usuários de dispositivos móveis no XenMobile Store. Os usuários assinam os aplicativos diretamente no XenMobile Store e os iniciam do Secure Hub. O Citrix Receiver deve estar instalado nos dispositivos do usuário para iniciar os aplicativos, mas não precisa ser configurado.

Para configurar essa definição, você precisa do nome de domínio totalmente qualificado (FQDN) ou do endereço IP, e do número de porta do site Web Interface ou StoreFront.

1. No console da Web XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Clique em **XenApp/XenDesktop**. A página **XenApp/XenDesktop** é exibida.



3. Defina estas configurações:
   - **Host:** digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do site Web Interface ou do StoreFront.
   - **Porta:** digite o número de porta do site Web Interface ou do StoreFront. O padrão é 80.
   - **Caminho relativo:** digite o caminho. Por exemplo, /Citrix/PNAgent/config.xml
   - **Usar HTTPS:** selecione se a autenticação segura entre o site Web Interface ou do StoreFront e o dispositivo de cliente deve ser ativada. O padrão é **O**.
4. Clique em **Testar conexão** para verificar se o XenMobile pode se conectar ao servidor XenApp e XenDesktop especificado.
5. Clique em **Salvar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Uso do ShareFile com o XenMobile

April 15, 2019

O XenMobile tem duas opções para integração com o ShareFile: ShareFile Enterprise e StorageZone Connectors. A integração com o ShareFile Enterprise ou com os StorageZone Connectors requer o XenMobile Enterprise Edition.

ShareFile Enterprise

Se você tem o XenMobile Enterprise Edition, pode configurar o XenMobile para fornecer acesso à sua conta do ShareFile Enterprise. Essa configuração:

- Permite que usuários móveis acessem o conjunto completo de recursos do ShareFile, como StorageZone Connectors, sincronização de arquivos e compartilhamento de arquivos.
- Pode fornecer ao ShareFile autenticação de logon único de usuários de XenMobile Apps, provisionamento de contas de usuário com base no AD e políticas abrangentes de controle de acesso.
- Fornece configuração, monitoramento de nível de serviço e monitoramento do uso de licenças do ShareFile por meio do console XenMobile.

Para obter mais informações sobre como configurar o XenMobile para o ShareFile Enterprise, consulte SAML para login único com o ShareFile.

Conectores StorageZone

Você pode configurar o XenMobile para fornecer acesso somente a StorageZone Connectors que você cria por meio do console XenMobile. Essa configuração:

- Fornece aos usuários acesso móvel em repositórios de armazenamento no local existentes, como sites do SharePoint e compartilhamentos de arquivos de rede.
- Não requer que você configure um subdomínio do ShareFile, provisione usuários para o ShareFile ou hospede dados do ShareFile.
- Fornece aos usuários acesso móvel aos seus dados armazenados por meio dos aplicativos móveis de produtividade ShareFile para iOS e Android. Os usuários podem editar documentos do Microsoft Office. Os usuários também podem visualizar e fazer anotações em arquivos Adobe PDF em dispositivos móveis.
- Está em conformidade com restrições de segurança contra vazamento de informações de usuários fora da rede corporativa.
- Fornece a configuração simples de StorageZone Connectors por meio do console XenMobile. Se mais tarde você decidir usar a funcionalidade completa do ShareFile com o XenMobile, poderá alterar a configuração no console XenMobile.

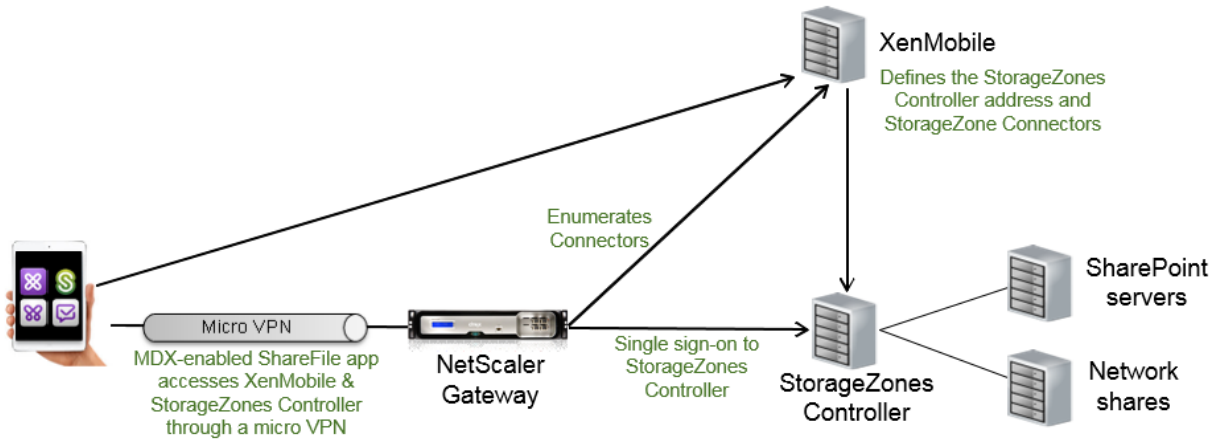
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Requer o XenMobile Enterprise Edition.

Apenas para uma XenMobile integração com conectores StorageZone:

- O ShareFile usa sua configuração de logon único para o NetScaler Gateway para autenticar com o StorageZones Controller.
- O XenMobile não se autentica via SAML porque o plano de controle do ShareFile não é usado.

O diagrama a seguir mostra a arquitetura de alto nível para o uso do XenMobile com StorageZone Connectors.



Requisitos

- Versões mínimas dos componentes:
  - XenMobile Server 10.5 (no local)
  - ShareFile para iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - ShareFile StorageZones Controller 5.0
    Este artigo contém instruções sobre como configurar o ShareFile StorageZones Controller 5.0
- Verifique se o servidor que deverá executar o StorageZones Controller atende aos requisitos de sistema. Para obter requisitos, consulte Requisitos do sistema.

Os requisitos de StorageZones para dados do ShareFile e StorageZones restritas não se aplicam a uma integração de XenMobile apenas com StorageZone Connector.

O XenMobile não dá suporte a conectores Documentum.

- Para executar scripts do PowerShell:
  - Execute os scripts na versão de 32 bits (x86) do PowerShell.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tarefas de instalação

Execute as tarefas a seguintes, na ordem apresentada para instalar e configurar o StorageZones Controller. Estes passos são específicos para uma XenMobile integração com conectores StorageZone: Alguns desses artigos estão na documentação do StorageZones Controller.

1. Configurar o NetScaler for StorageZones Controller

   Você pode usar o NetScaler como um proxy DMZ para StorageZones Controller.

2. Instalar um certificado SSL

   Um StorageZones Controller que hospeda zonas padrão requer um certificado SSL. Um StorageZones Controller que hospeda zonas restritas e usa um endereço interno não requer um certificado SSL.

3. Prepare seu servidor

   É necessário instalar o IIS e ASP.NET para conectores de StorageZone.

4. Instalar o StorageZones Controller
5. Prepare o StorageZones Controller para uso somente com os conectores StorageZone
6. Especifique um servidor proxy para StorageZones

   O console do StorageZones Controller permite que você especifique um servidor proxy para StorageZones Controllers. Você também pode especificar um servidor proxy usando outros métodos.

7. Configure o controlador de domínio para confiar no StorageZones Controller para delegação

   Configure o controlador de domínio para oferecer suporte à autenticação NTLM ou Kerberos em compartilhamentos de rede ou sites do SharePoint.

8. Junte um StorageZones Controller secundário a um StorageZone

   Para configurar uma StorageZone para alta disponibilidade, conecte pelo menos dois StorageZones Controllers a ele.

Instalar o StorageZones Controller

1. Baixe e instale o software StorageZones Controller:

   a) Na página de download do ShareFile em https://www.citrix.com/downloads/sharefile.html, faça login e baixe o instalador do StorageZones Controller mais recente.

   b) A instalação do StorageZones Controller altera o site padrão no servidor para o caminho de instalação do controlador. Ativar a **Autenticação anônima** no site da Web padrão.

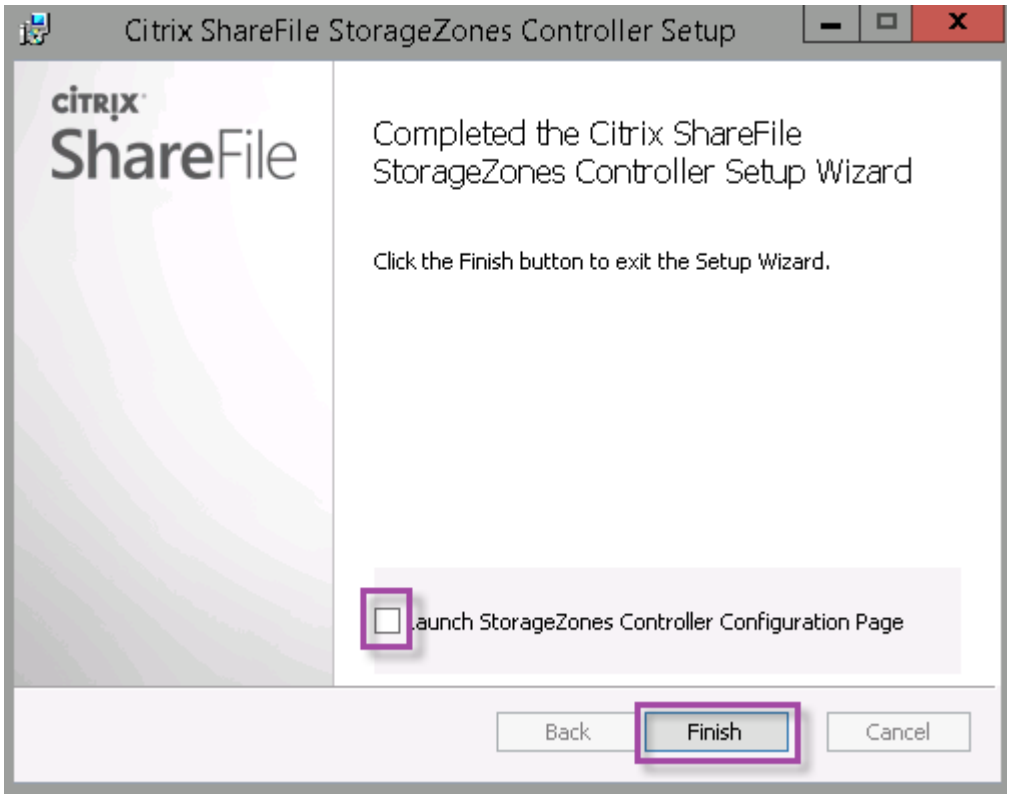
© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. No servidor em que você deseja instalar o StorageZones Controller, execute StorageCenter.msi.

   Inicia o Assistente de instalação do ShareFile StorageZones Controller.

3. Responda às solicitações:

   - Na página **Destination Folder**, se os serviços de informações da Internet (IIS) estiverem instalados no local padrão, mantenha as configurações padrão. Caso contrário, navegue até o local de instalação do IIS.
   - Quando a instalação for concluída, desmarque a caixa de seleção **Launch StorageZones Controller Configuration Page** e, em seguida, clique em **Finish**.



4. Quando solicitado, reinicie o StorageZones Controller.
5. Para testar se a instalação foi bem sucedida, navegue para `https://localhost/`. Se a instalação for bem-sucedida, o logotipo do ShareFile é exibida.

   Se o logotipo do ShareFile não for exibido, limpe o cache do navegador e tente novamente.

   > Importante:
   >
   > Se você planeja clonar o StorageZones Controller, capture a imagem de disco antes de continuar configurando o StorageZones Controller.

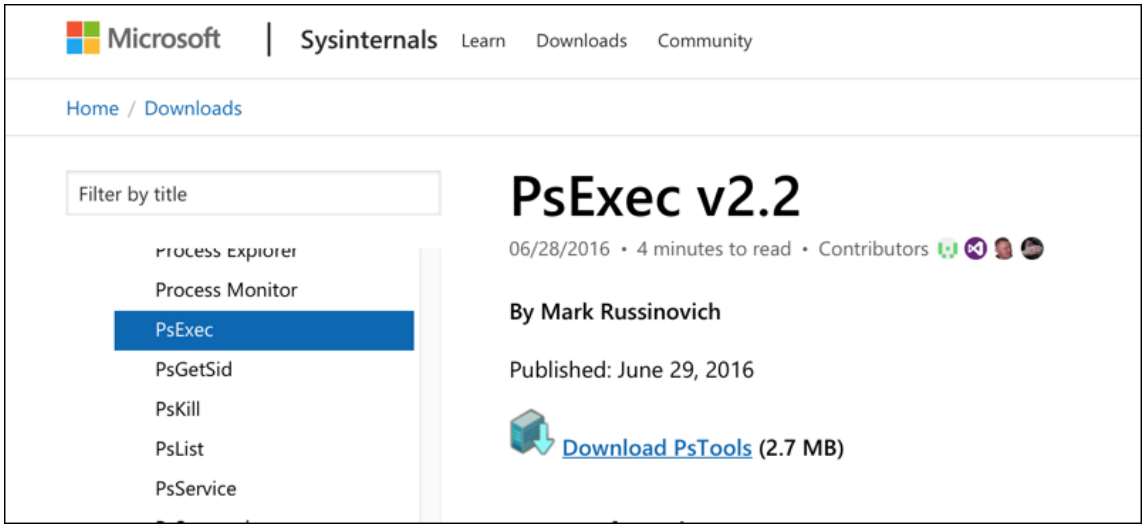
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Prepare o StorageZones Controller para uso somente com os conectores StorageZone

Para uma integração somente com conectores StorageZone, você não usa o console administrativo StorageZones Controller. Aquela interface requer uma conta de administrador do ShareFile, o que não é necessário para esta solução. Como resultado, você pode executar um script do PowerShell para preparar o StorageZones Controller para uso sem plano de controle do ShareFile. O script faz o seguinte:

- Registra o StorageZones Controller atual como um StorageZones Controller primário. Mais tarde você pode juntar StorageZones Controllers secundários ao controlador primário.
- Cria uma zona e define a senha para ela.

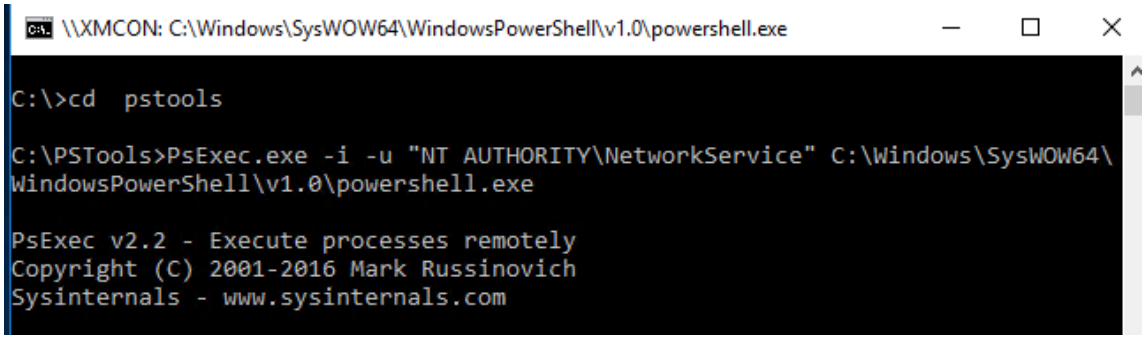
1. No seu servidor de StorageZone Controller, baixe a ferramenta PsExec: Navegue até Microsoft Windows Sysinternals e, em seguida, clique em **Download PsTools**. Extraia a ferramenta para a raiz da unidade C.



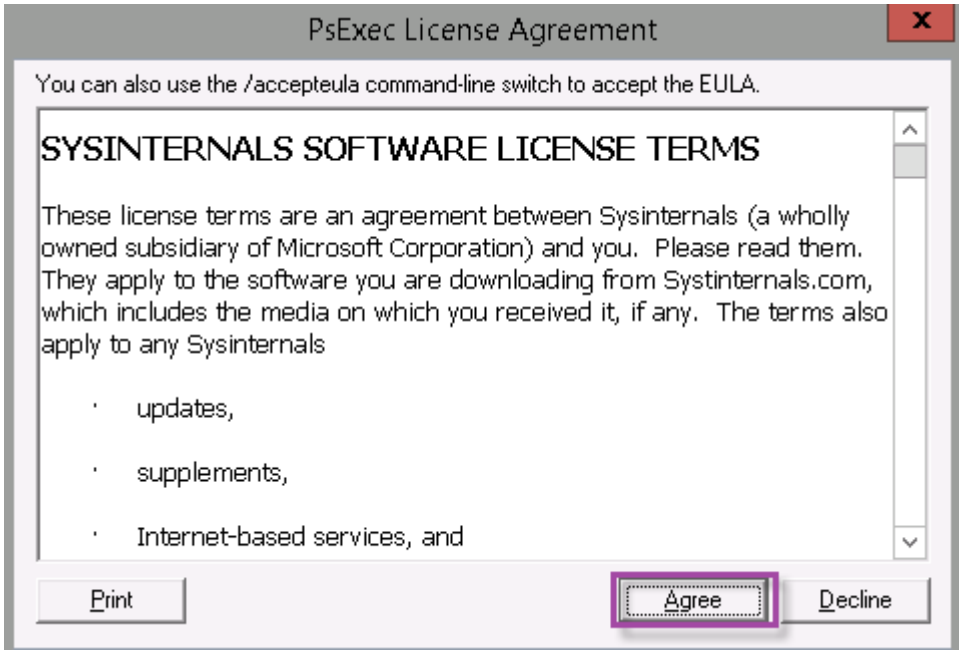
2. Execute a ferramenta PsExec: Abra o aviso de comando como o usuário de administrador e, em seguida, digite o seguinte:

```
```
cd c:\pstools
PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
```
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Quando solicitado, clique em **Concordar** para executar a ferramenta Sysinternals.



É aberta uma janela do PowerShell.

4. Na janela do PowerShell, digite o seguinte:

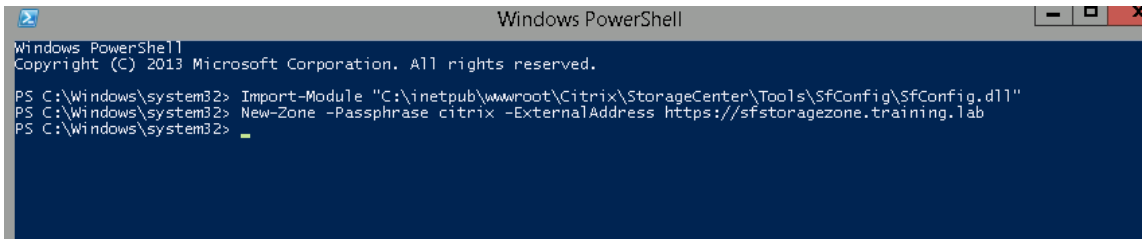
```
‘‘‘
Import-Module ”C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll”
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
‘‘‘
```

Onde:

Passphrase: é a senha que você deseja atribuir o site. Anote-a. Não é possível recuperar a senha por meio do controlador. Se você perder a senha, não poderá reinstalar StorageZones, juntar mais StorageZones Controllers à StorageZone nem recuperar a StorageZone se o servidor falhar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ExternalAddress: é o nome de domínio totalmente qualificado externo do servidor StorageZones Controller.



Seu StorageZones Controller primário agora está pronto.

Antes de fazer logon no XenMobile para criar StorageZone Connectors: conclua a configuração a seguir, se aplicável:

Especifique um servidor proxy para StorageZones

Configure o controlador de domínio para confiar no StorageZones Controller para delegação

Junte um StorageZones Controller secundário a um StorageZone

Para criar StorageZone Connectors, consulte Definir conexões do StorageZones Controller no XenMobile.

Junte um StorageZones Controller secundário a um StorageZone

Para configurar uma StorageZone para alta disponibilidade, conecte pelo menos dois StorageZones Controllers a ele. Para juntar um StorageZones Controller secundário a uma zona, instale o StorageZones Controller em um segundo servidor. Em seguida, junte esse controlador à zona do controlador principal.

1. Abra uma janela do PowerShell no servidor StorageZones Controller que você deseja juntar ao servidor primário.
2. Na janela do PowerShell, digite o seguinte:

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

   Por exemplo:

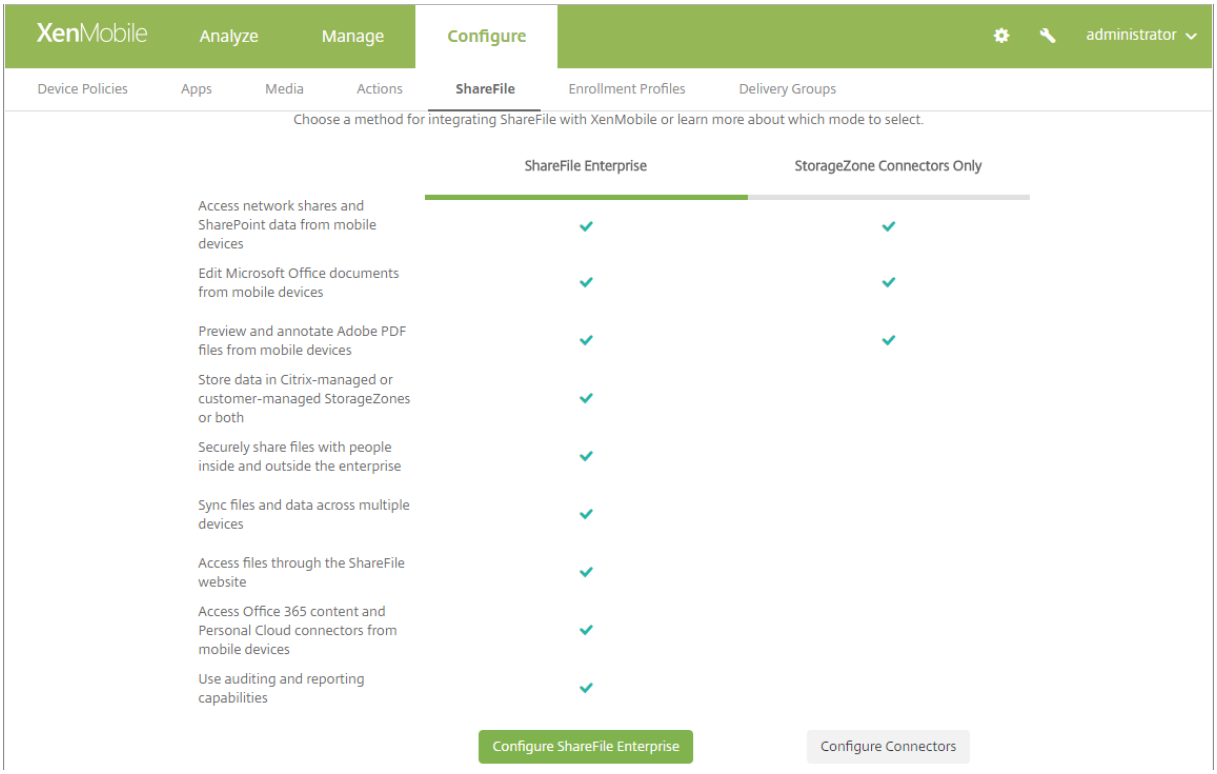
   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

Definir conexões do StorageZones Controller no XenMobile

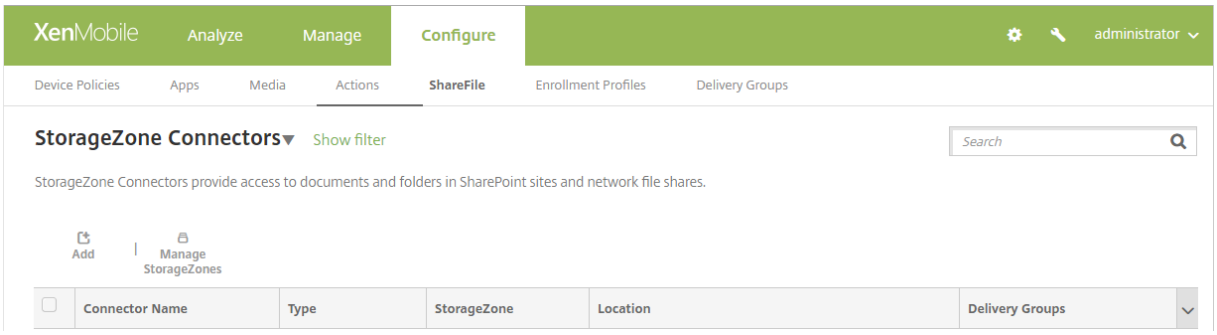
Antes de adicionar StorageZone Connectors, configure informações de conexão para cada StorageZones Controller ativado para StorageZone Connectors. Você pode definir StorageZones Controllers conforme descrito nesta seção ou ao adicionar um conector.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

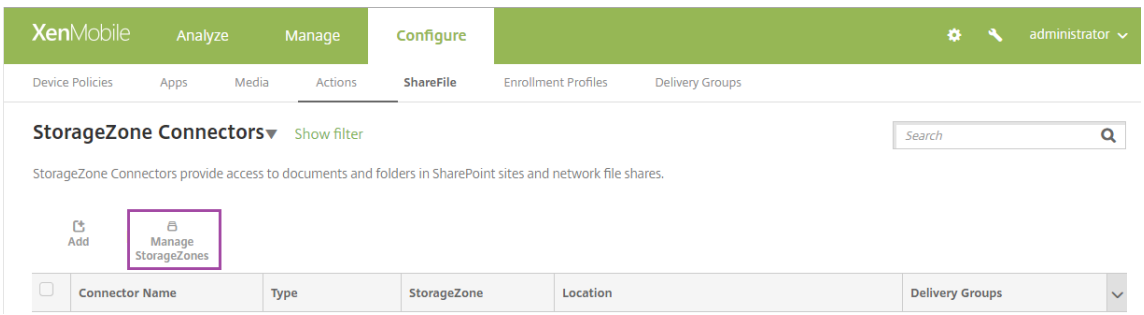
Na sua primeira visita à página **Configurar > ShareFile**, a página resume as diferenças entre o uso do XenMobile com o ShareFile Enterprise e StorageZone Connectors.



Clique em **Configurar conectores** para continuar com as etapas de configuração neste artigo.

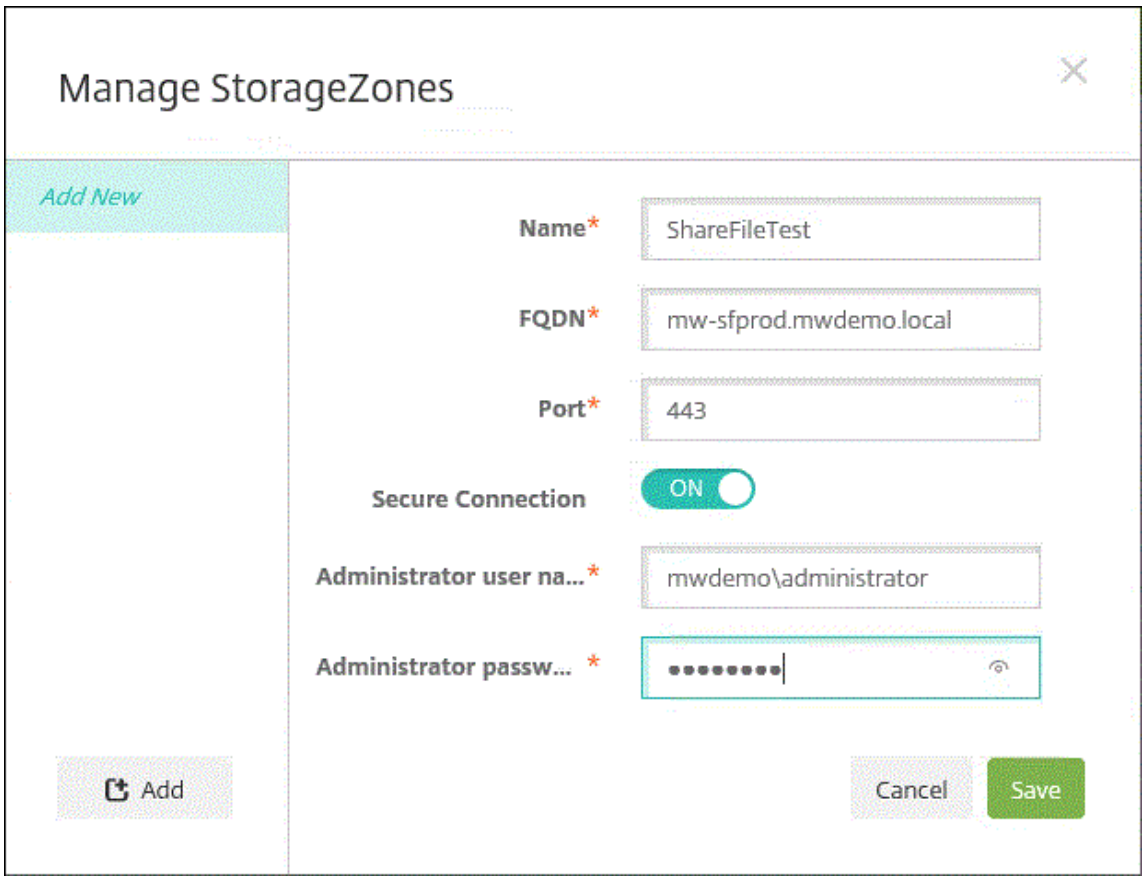


1. Em **Configurar > ShareFile**, clique em **Gerenciar StorageZones**.



2. Em **Gerenciar StorageZones**, adicione as informações de conexão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Nome:** um nome descritivo para o StorageZone, usado para identificar o StorageZone no XenMobile. Não inclua espaços ou caracteres especiais no nome.
- **FQDN e porta:** o nome de domínio totalmente qualificado e o número da porta do StorageZones Controller que pode ser alcançada a partir do XenMobile Server.
- **Conexão segura:** se você usar SSL para conexões com o StorageZones Controller, use a configuração padrão, I. Se você não usar SSL para conexões, altere essa configuração para O.
- **Nome de usuário do administrador** e **Senha do administrador:** um nome de usuário da conta de serviço de administrador (no formato domínio\administrador) e a respectiva senha. Como alternativa, uma conta de usuário com permissões de leitura e gravação nos StorageZones Controllers.

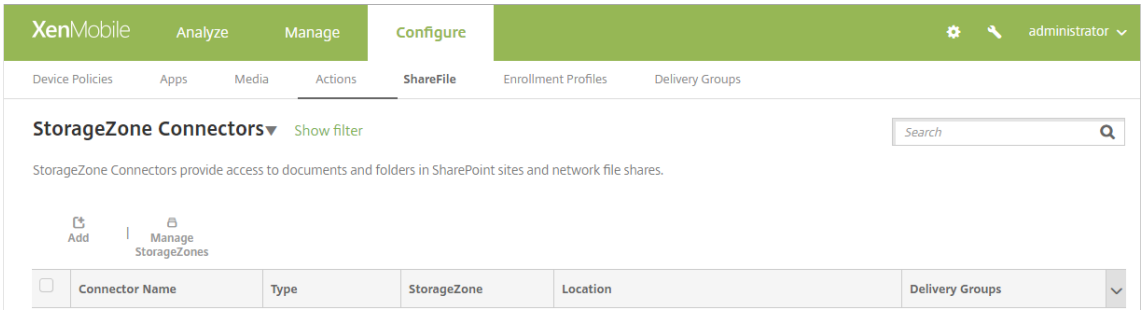
3. Clique em **Salvar**.
4. Para testar a conexão, verifique se o XenMobile Server pode alcançar o nome de domínio totalmente qualificado do StorageZones Controller na porta 443.
5. Para definir outra conexão com o StorageZones Controller, clique no botão **Adicionar** em **Gerenciar StorageZones**.

   Para editar ou excluir as informações de uma conexão do StorageZones Controller, selecione o nome da conexão em **Gerenciar StorageZones**. Em seguida, clique em **Editar** ou **Excluir**.

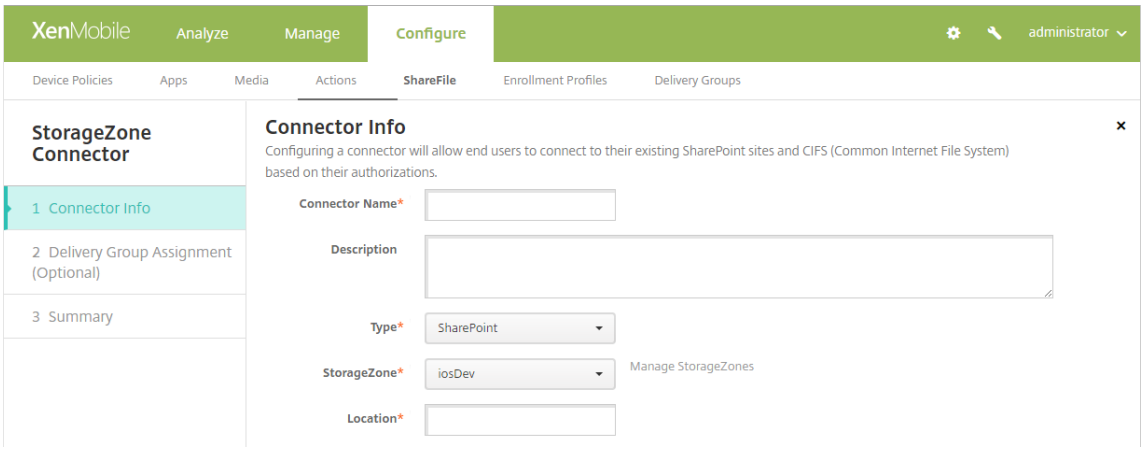
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Adicionar um StorageZone Connector no XenMobile

1. Vá até **Configurar > ShareFile** e clique em **Adicionar**.



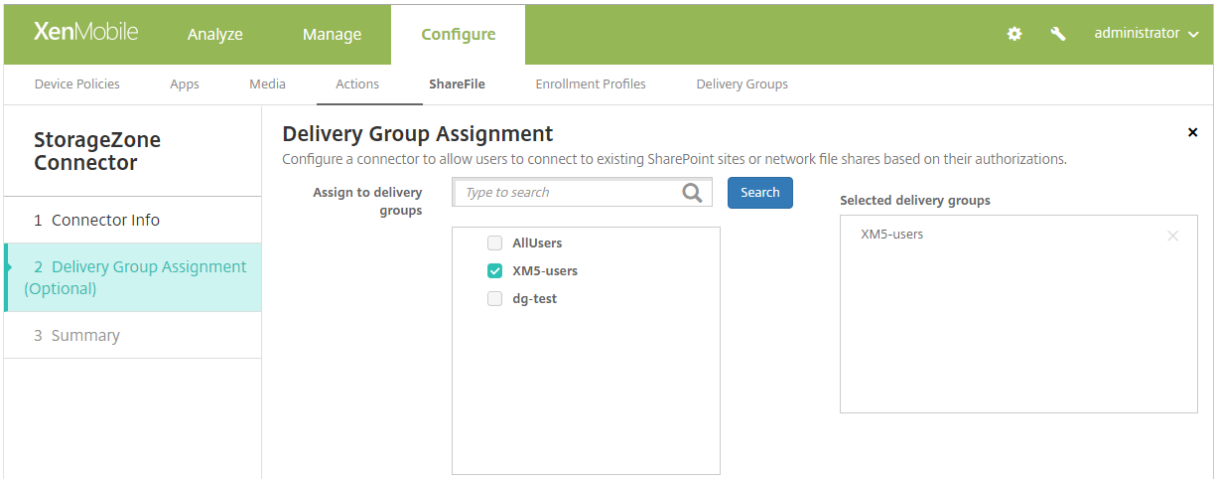
2. Na página **Informações do Connector**, defina estas configurações:



   - **Nome do conector:** um nome que identifica o StorageZone Connector no XenMobile.
   - **Descrição:** observações opcionais sobre esse Connector.
   - **Tipo:** escolha **SharePoint** ou **Rede**.
   - **StorageZone:** escolha o StorageZone associado ao Connector. Se o StorageZone não estiver na lista, clique em **Gerenciar StorageZones** para definir o StorageZones Controller.
   - **Localização:** para o SharePoint, especifique o URL do site de nível raiz, o conjunto de sites ou a biblioteca de documentos do SharePoint, no formato `https://sharepoint.company.com`. Para um compartilhamento de rede, especifique o nome de domínio totalmente qualificado do caminho UNC (Uniform Naming Convention), no formato \\servidor\compartilhamento.

3. Na página **Atribuição de grupo de entrega**, atribua opcionalmente o Conector a grupos de entrega. Como alternativa, você pode associar conectores a grupos de entrega usando **Configurar > Grupos de entrega**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



1. Na página **Resumo**, você pode rever as opções configuradas. Para ajustar a configuração, clique em **Voltar**.
2. Clique em **Salvar** para salvar o Conector.
3. Teste o conector:

    a) Ao preparar os clientes do ShareFile, faça o seguinte:

    - Defina a política de Acesso à rede como **Com túnel para a rede interna**.

    Nesse modo de operação, o framework XenMobile MDX intercepta todo o tráfego de rede do cliente do ShareFile. O tráfego é redirecionado por meio do NetScaler Gateway por meio de uma micro VPN específica para o aplicativo.

    - Defina a política de modo VPN preferido como **Com túnel - SSO de Web**.

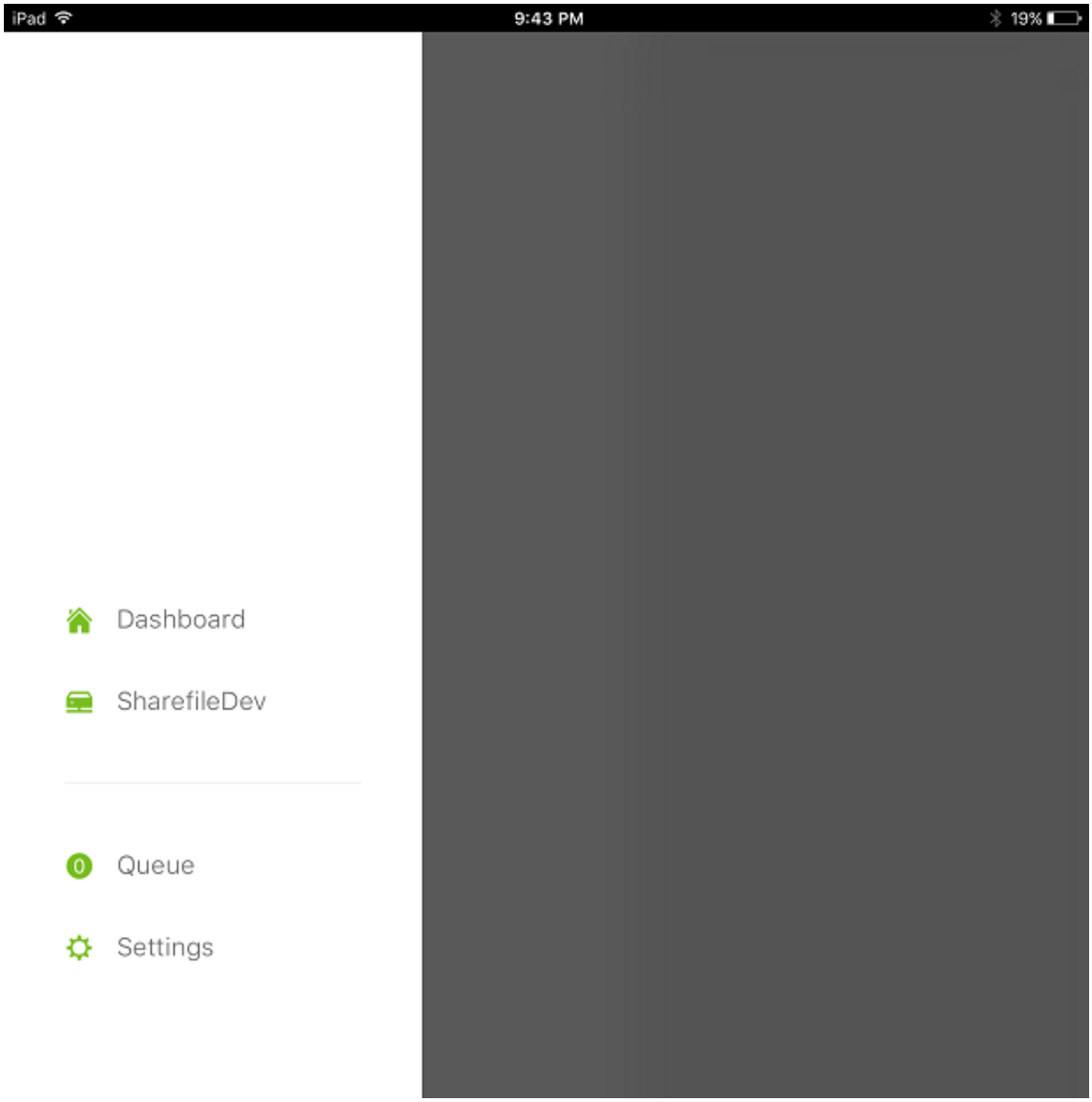
    Nesse modo de criação de túneis, o framework MDX termina o tráfego SSL/HTTP a partir de um aplicativo MDX. O MDX depois inicia novas conexões para conexões a conexões internas em nome do usuário. Essa configuração de política permite que o framework de MDX detecte e responda aos desafios de autenticação emitidos por servidores da web.

    b) Adicione clientes ShareFile ao XenMobile. Para obter detalhes, consulte Integração e fornecimento de clientes do Citrix Files Endpoint Management.

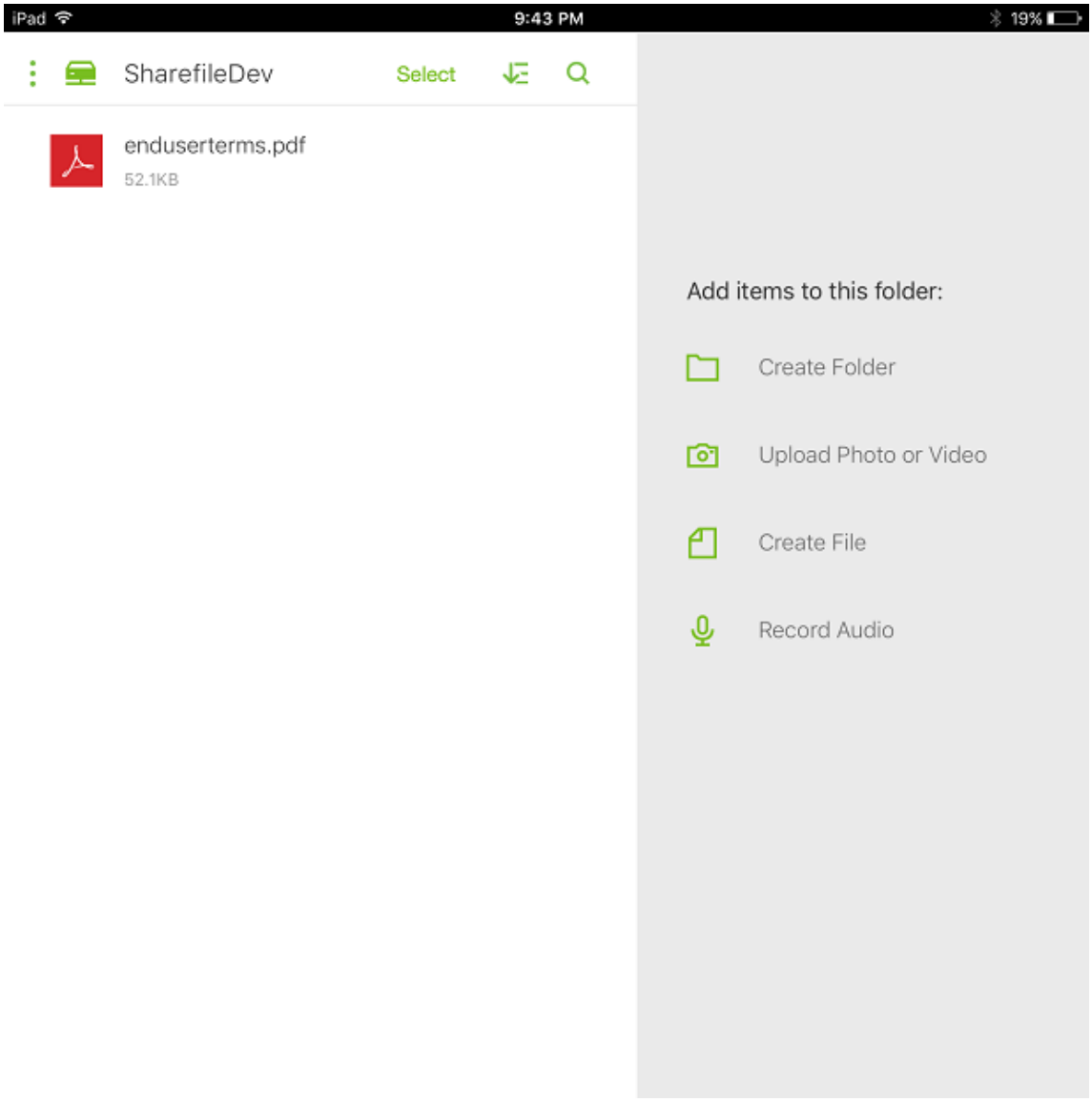
    c) A partir de um dispositivo com suporte, verifique o logon único para o ShareFile e conectores.

    Nos exemplos a seguir, SharefileDev é o nome de um conector.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

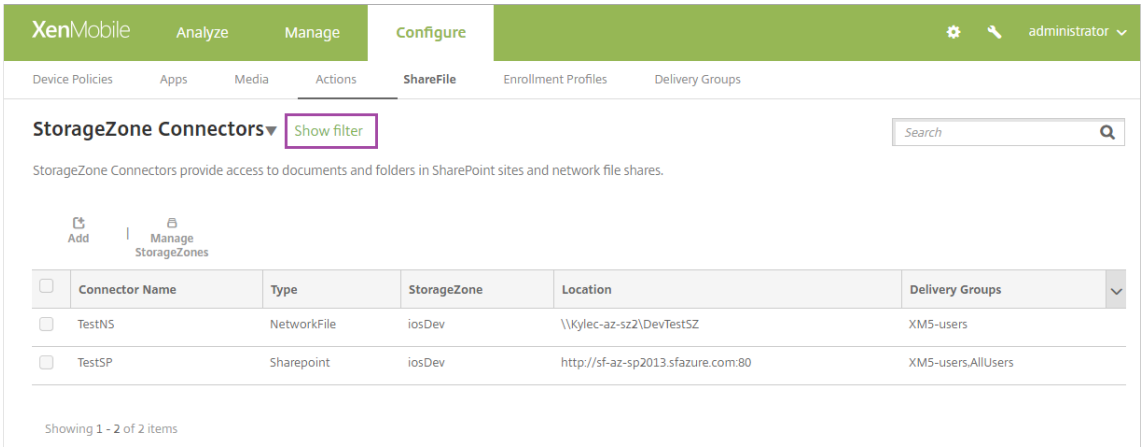


Filtrar a lista de StorageZone Connectors

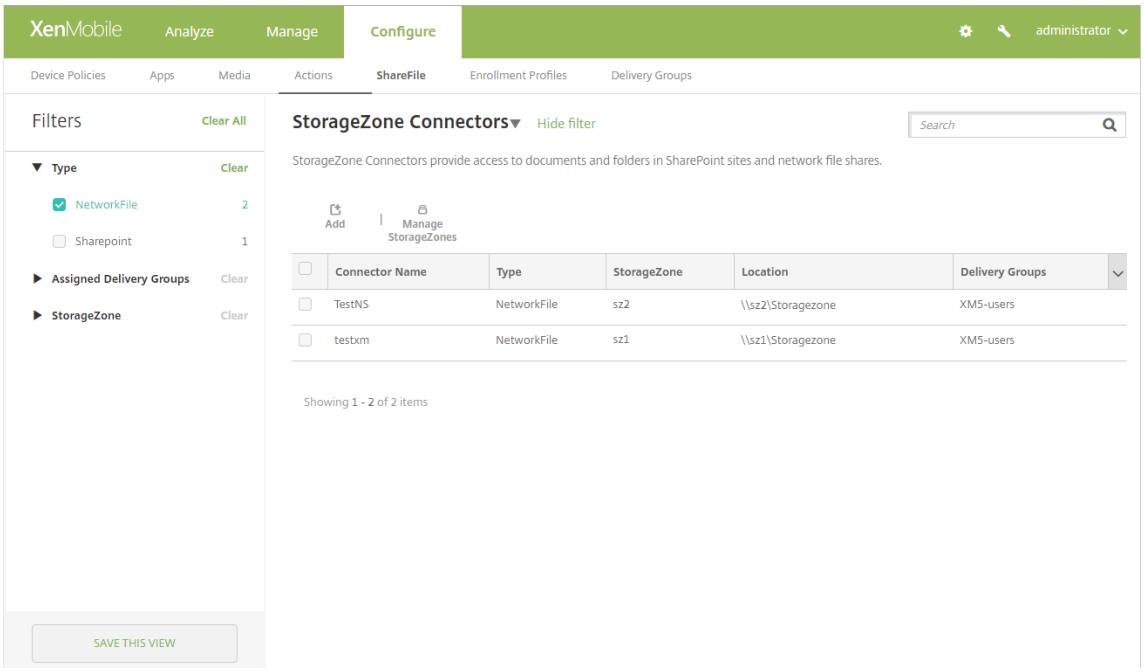
Você pode filtrar a lista de StorageZone Connectors por tipo de Conector, grupos de entrega atribuídos e StorageZone.

1. Vá até **Configurar > ShareFile** e clique em **Mostrar filtro**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

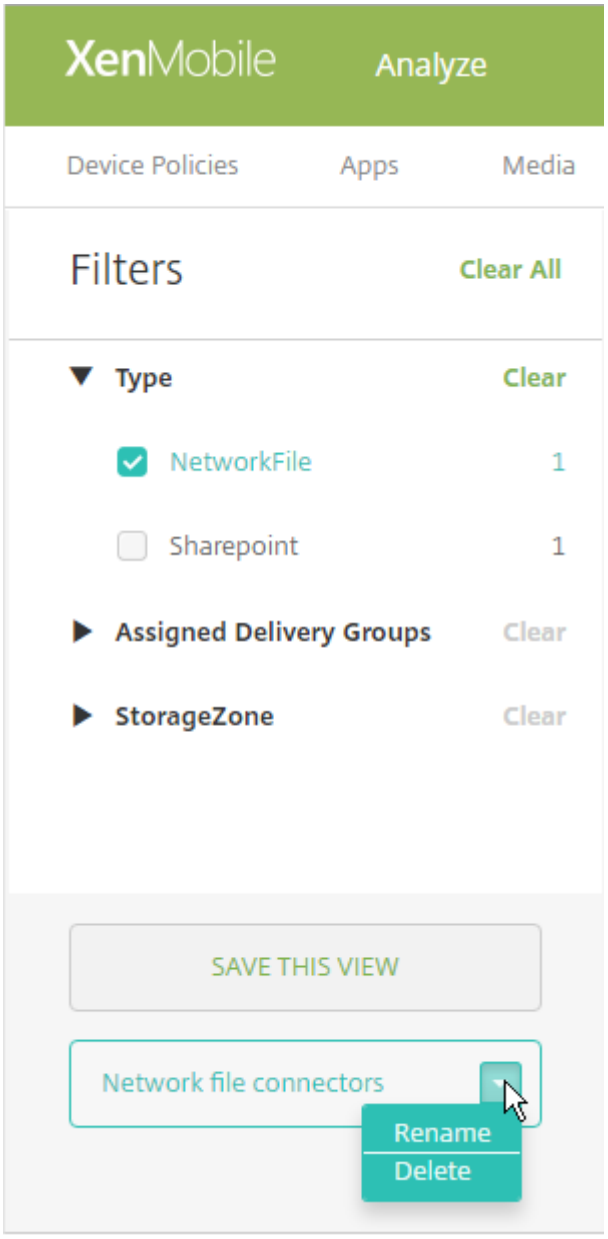


2. Expanda os títulos de filtro para fazer seleções. Para salvar um filtro, clique em **Salvar esta exibição**, digite o nome do filtro e clique em **Salvar**.



3. Para renomear ou excluir um filtro, clique no ícone de seta ao lado do nome do filtro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

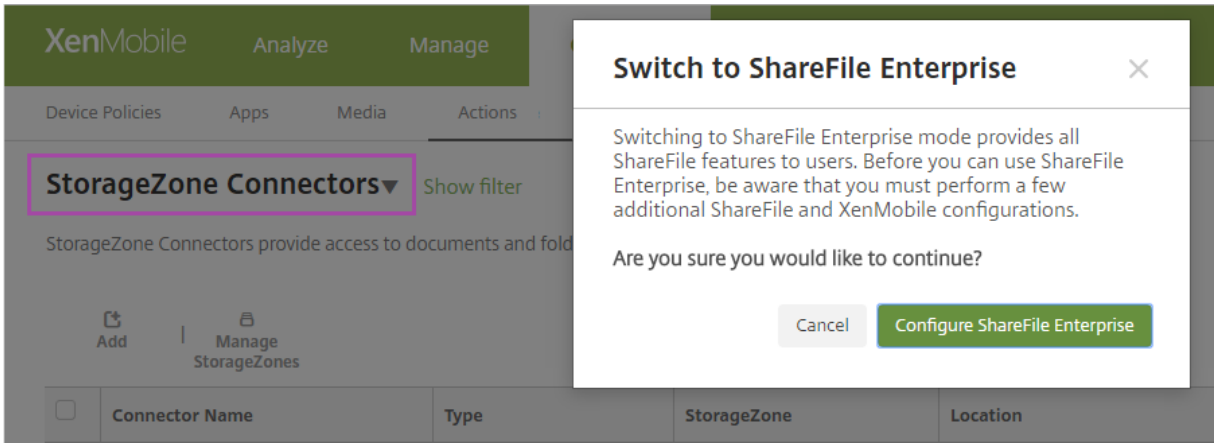


Mudar para o ShareFile Enterprise

Depois de integrar os StorageZone Connectors ao XenMobile, você pode mudar posteriormente para o conjunto completo de recursos do ShareFile Enterprise. O uso do conjunto de recursos do ShareFile Enterprise requer o XenMobile Enterprise Edition. O XenMobile mantém as configurações de integração existentes do StorageZone Connector.

Vá até **Configurar > ShareFile**, clique no menu suspenso **StorageZone Connectors** e clique em **Configurar ShareFile Enterprise**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para obter informações sobre como configurar o ShareFile Enterprise, consulte SAML para login único com o ShareFile.

SmartAccess para aplicativos HDX

August 24, 2018

Esse recurso permite controlar o acesso a aplicativos HDX com base nas propriedades do dispositivo, nas propriedades do usuário de um dispositivo ou nos aplicativos instalados em um dispositivo. Use esse recurso definindo ações automatizadas para marcar o dispositivo como fora de conformidade, para negar acesso a esse dispositivo. Os aplicativos HDX usados com esse recurso são configurados no XenApp e no XenDesktop usando uma política SmartAccess que nega acesso a dispositivos fora de conformidade. O XenMobile comunica o status do dispositivo ao StoreFront usando uma marca assinada e criptografada. Em seguida, o StoreFront permite ou nega o acesso com base na política de controle de acesso do aplicativo.

Para usar esse recurso, a implantação requer:

- XenApp e XenDesktop 7.6
- StoreFront 3.7 ou 3.8
- O XenMobile Server configurado reúne os aplicativos HDX a partir de um servidor StoreFront
- XenMobile Server configurado com um certificado SAML a ser usado para assinar e criptografar marcas. O mesmo certificado sem a chave privada é carregado no servidor StoreFront.

Para começar a usar este recurso:

- Configure o certificado do XenMobile Server para o repositório do StoreFront
- Configure pelo menos um grupo de entrega do XenApp e do XenDesktop com a política SmartAccess necessária
- Defina a ação automatizada no XenMobile

© 1999-2019 Citrix Systems, Inc. All rights reserved.

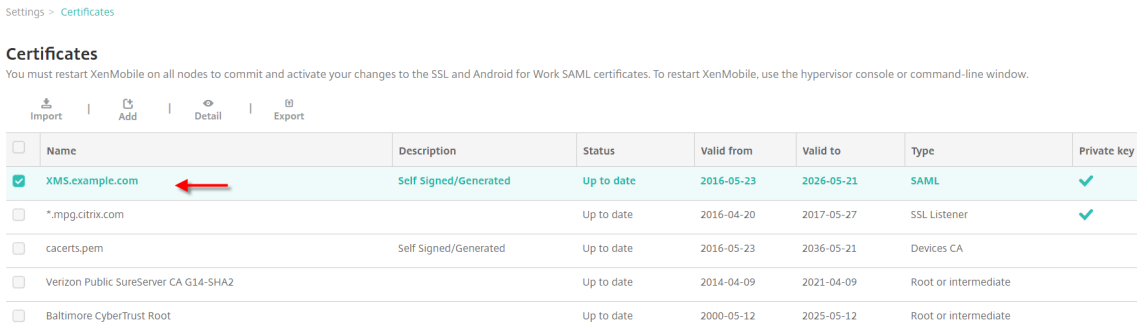
Exporte e configure o certificado do XenMobile Server e carregue-o no repositório do StoreFront

O SmartAccess usa marcas assinadas e criptografadas para se comunicar entre os servidores XenMobile e StoreFront. Para ativar essa comunicação, adicione o certificado do XenMobile Server ao repositório do StoreFront.

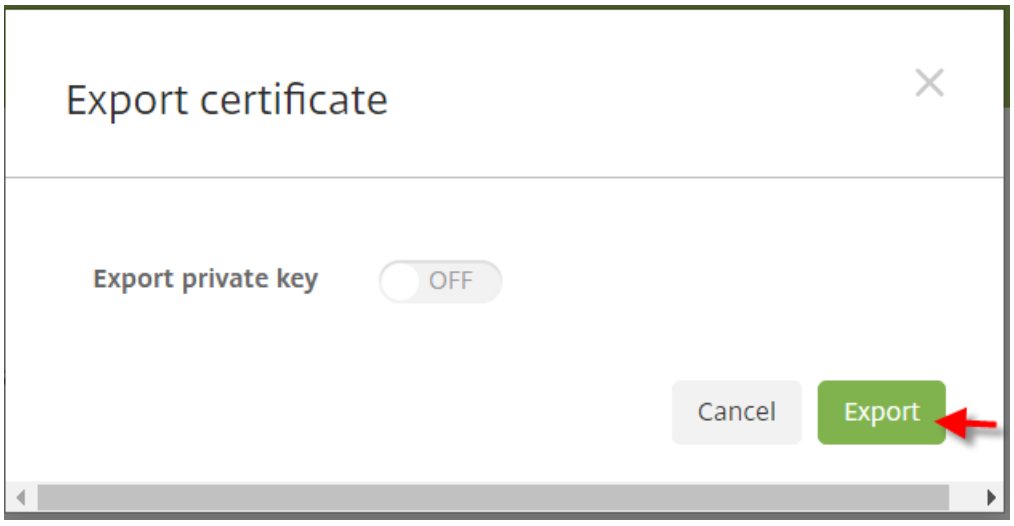
Para obter mais informações sobre como integrar o StoreFront e o XenMobile quando o XenMobile estiver ativado com autenticação baseada em domínio e em certificado, consulte o Support Knowledge Center.

Exportar o certificado SAML do XenMobile Server

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida. Clique em **Certificados**.
2. Localize o certificado SAML do XenMobile Server.

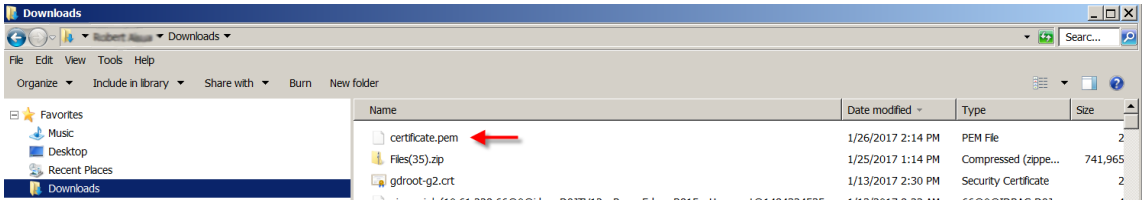


3. Verifique se a opção **Exportar chave privada** está definida como **O**. Clique em **Exportar** para exportar o certificado para o diretório de download.



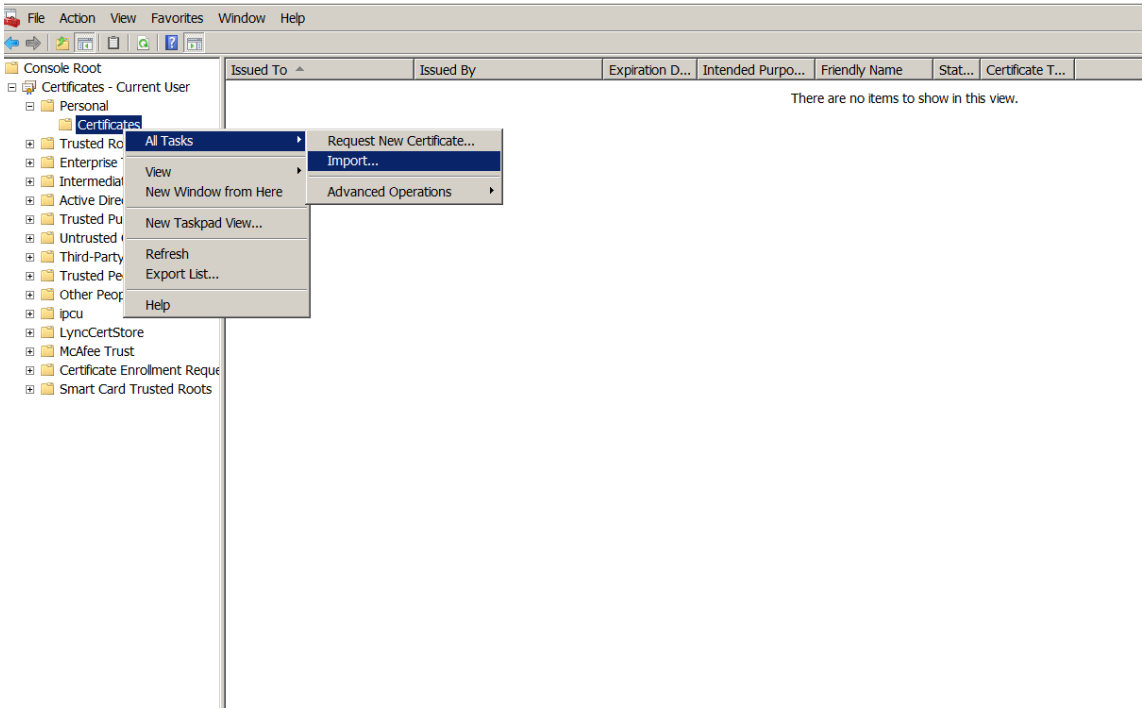
© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Localize o certificado no diretório de download. O certificado está no formato PEM.



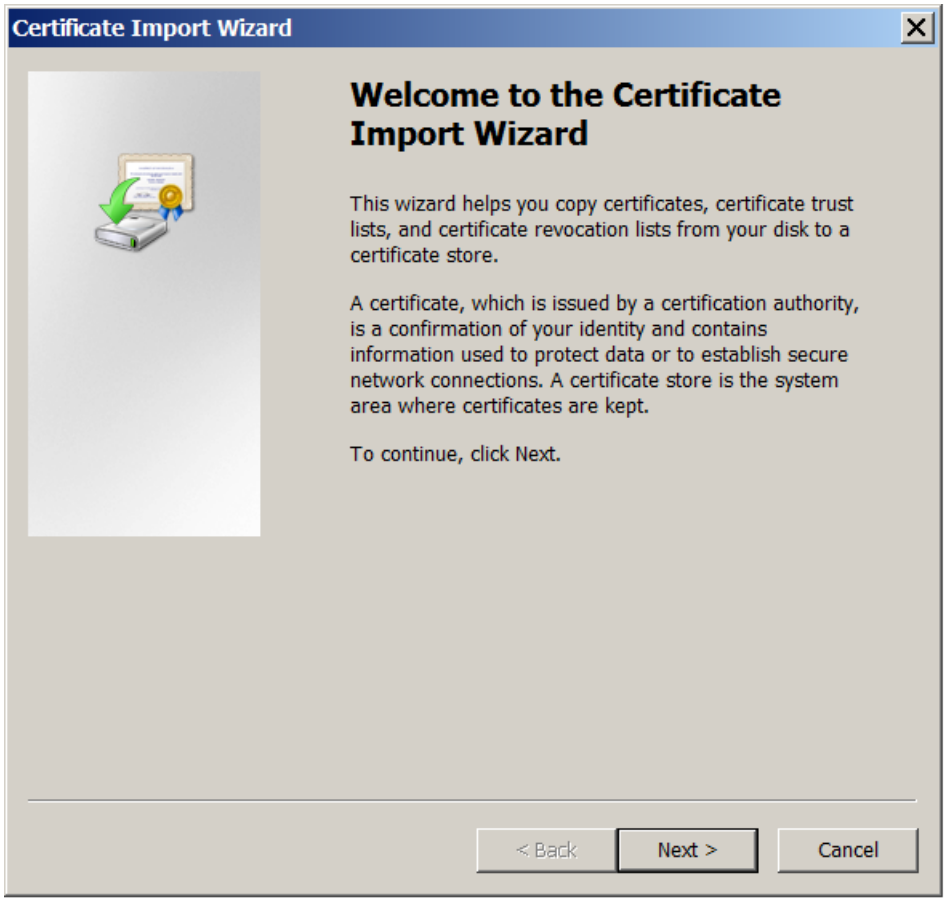
Converter o certificado de PEM para CER

1. Abra o Console de Gerenciamento Microsoft (MMC) e clique com o botão direito do mouse em **Certificados > Todas as tarefas > Importar**.



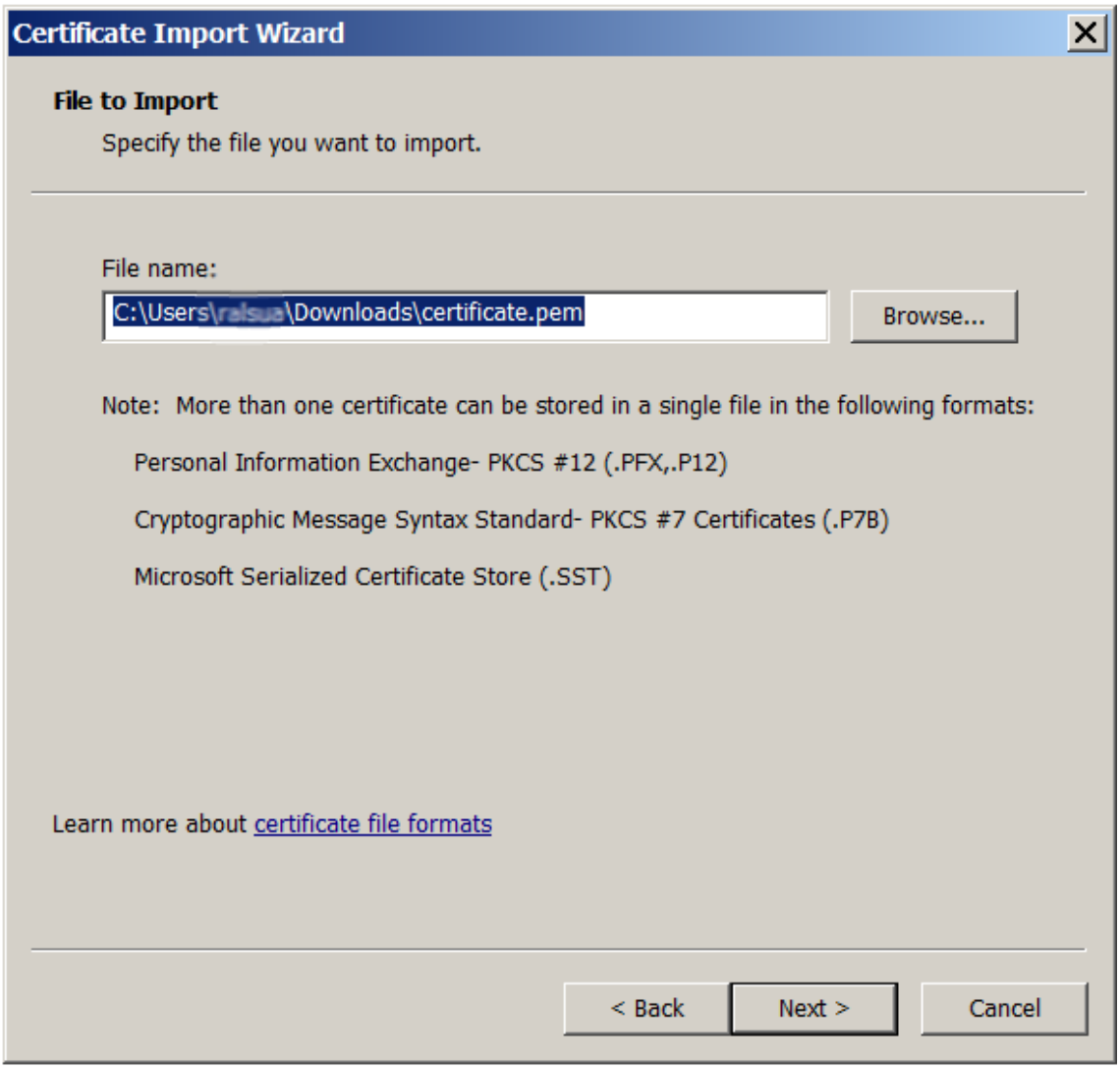
2. Quando o assistente de importação de certificado for exibido, clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



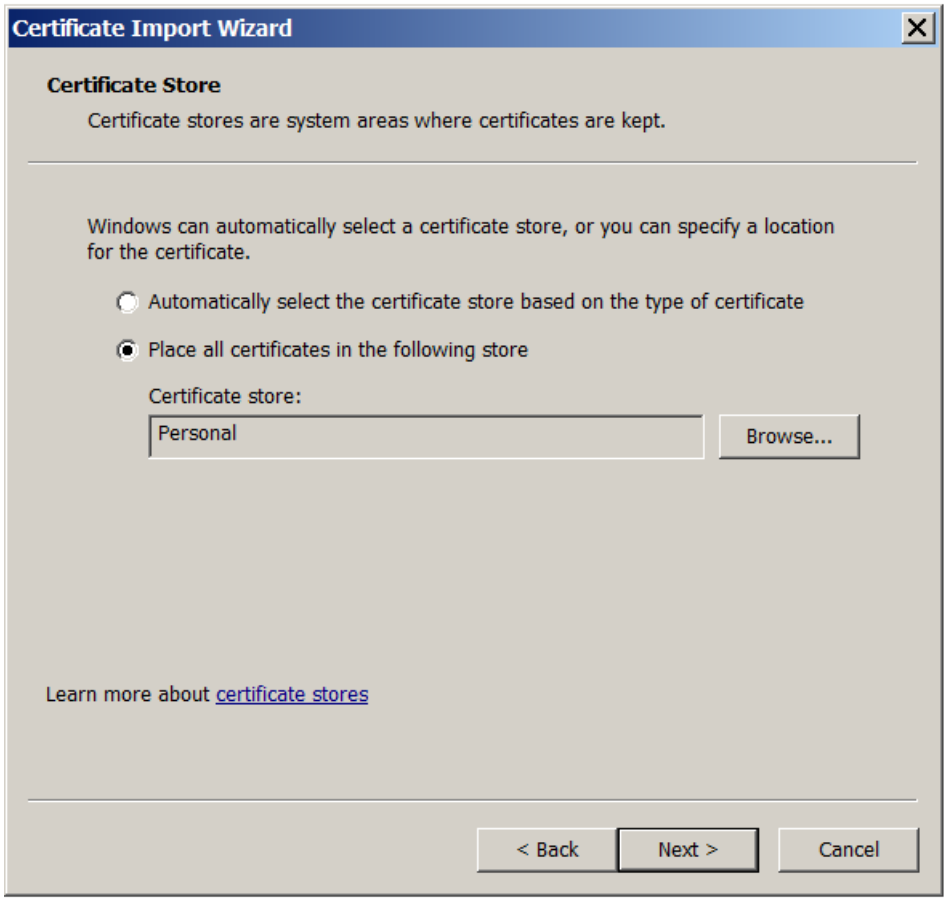
3. Navegue até o certificado no diretório de download.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

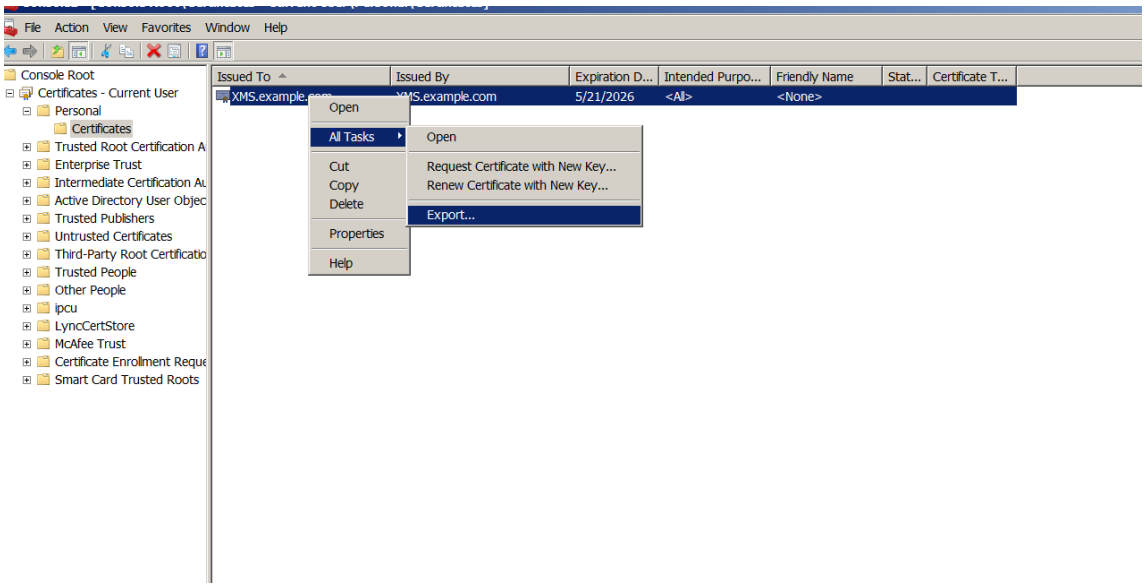


4. Selecione **Colocar todos os certificados no repositório a seguir** e selecione **Pessoal** como o repositório de certificados. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Revise suas seleções e clique em **Concluir**. Clique em **OK** na janela de confirmação.
6. No MMC, clique com o botão direito do mouse no certificado e escolha **Todas as tarefas > Exportar**.



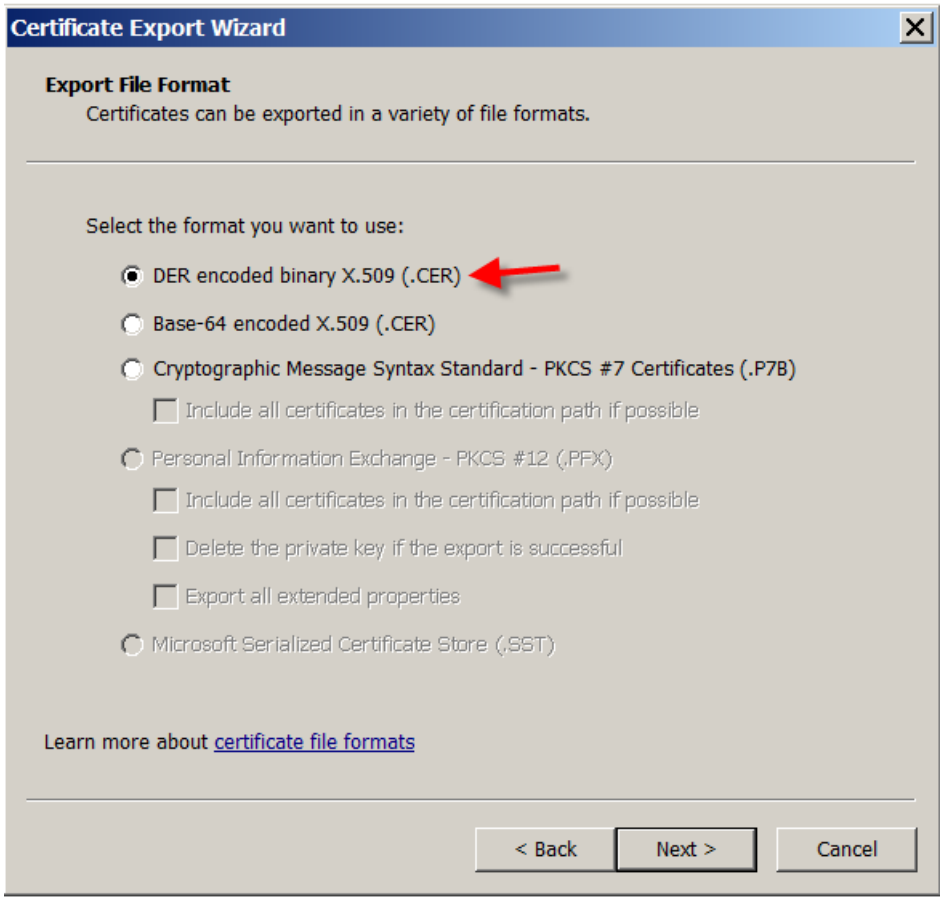
7. Quando o assistente de exportação de certificado for exibido, clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



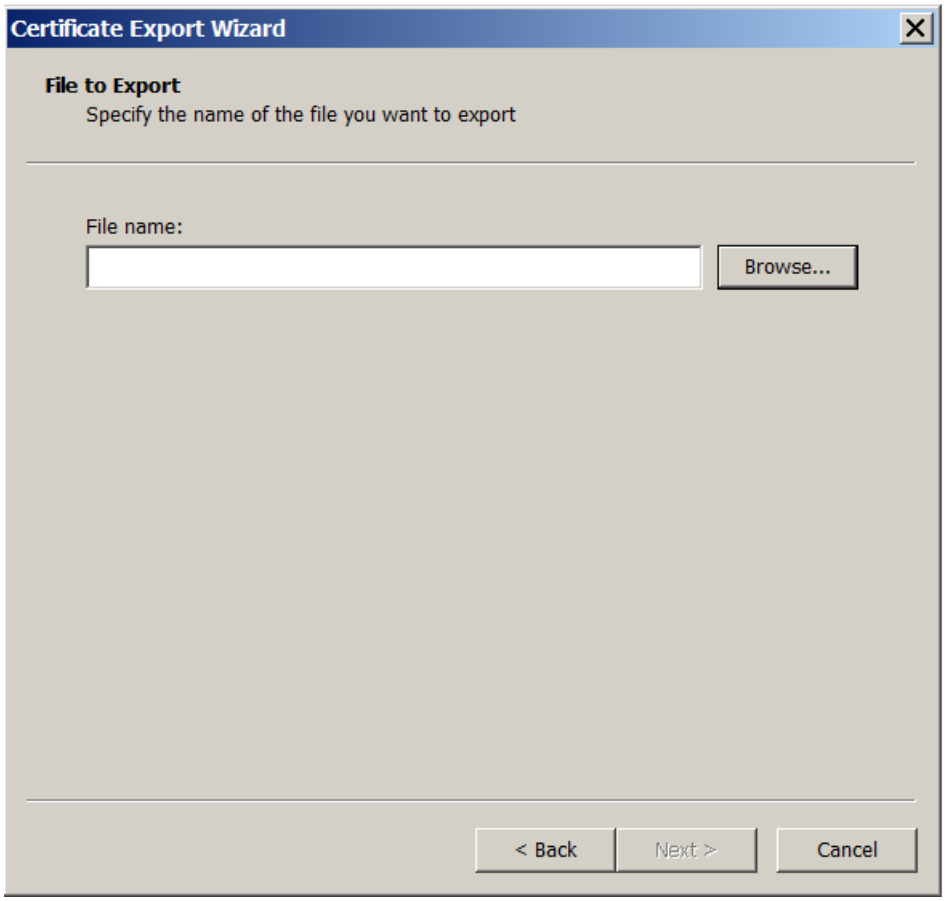
8. Escolha o formato **x.509 binário codificado por DER (.CER)**. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

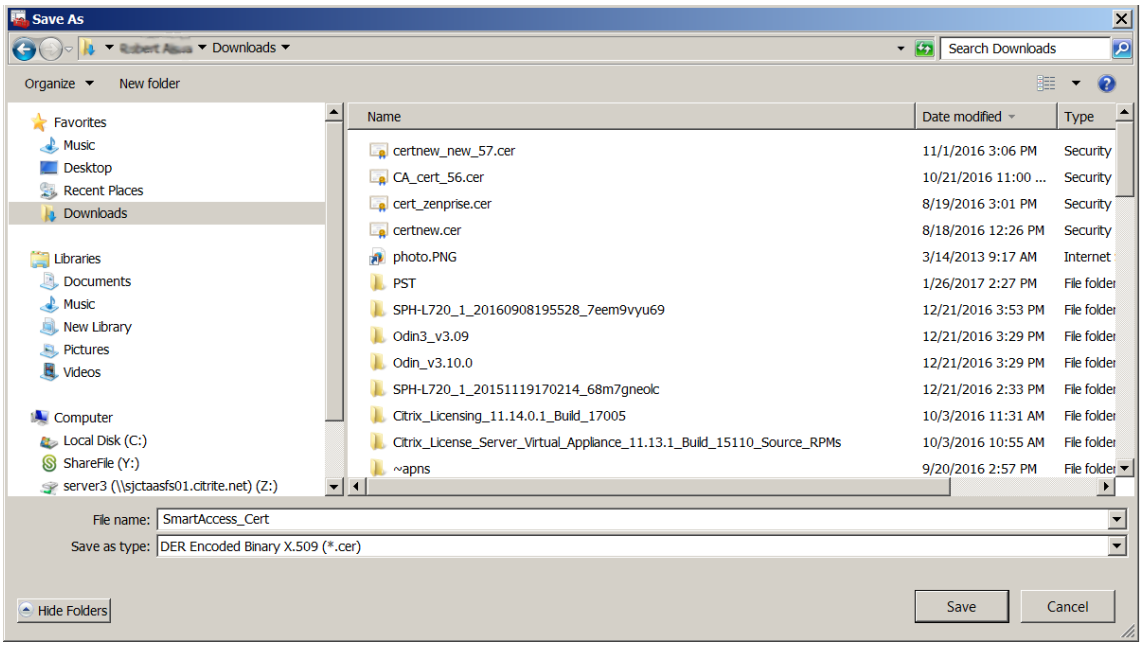


9. Procure o certificado. Digite um nome para o certificado e clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

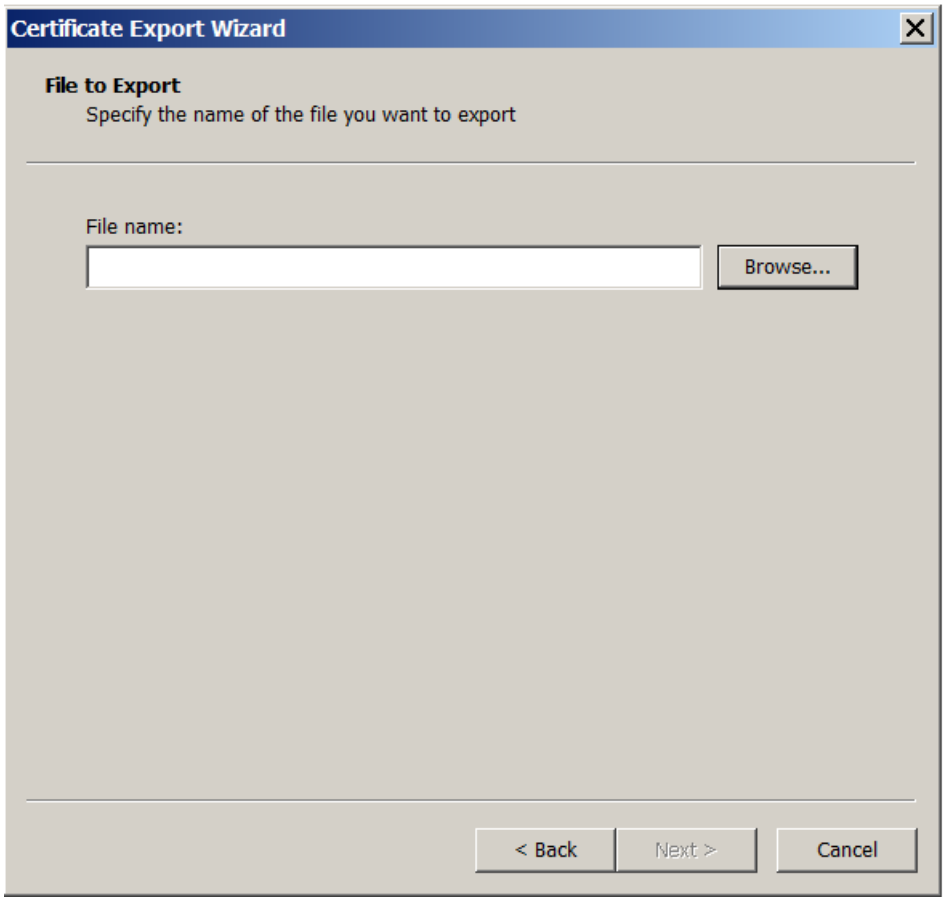


10. Salve o certificado.



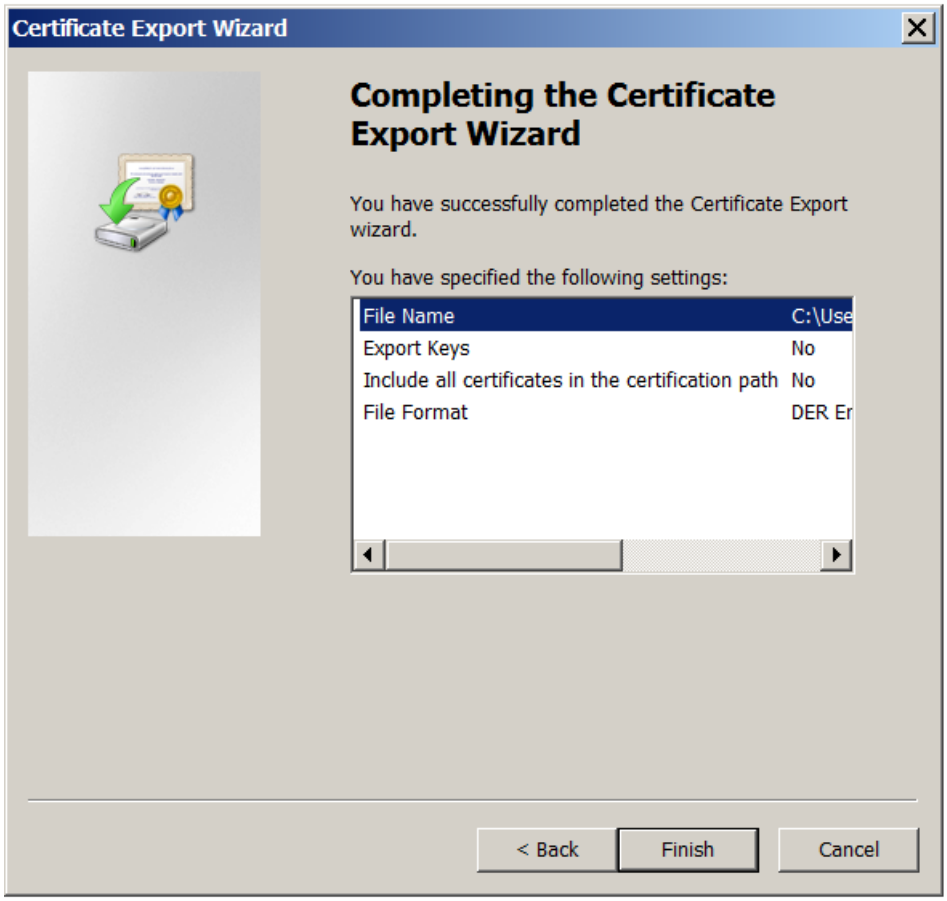
11. Procure o certificado e clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

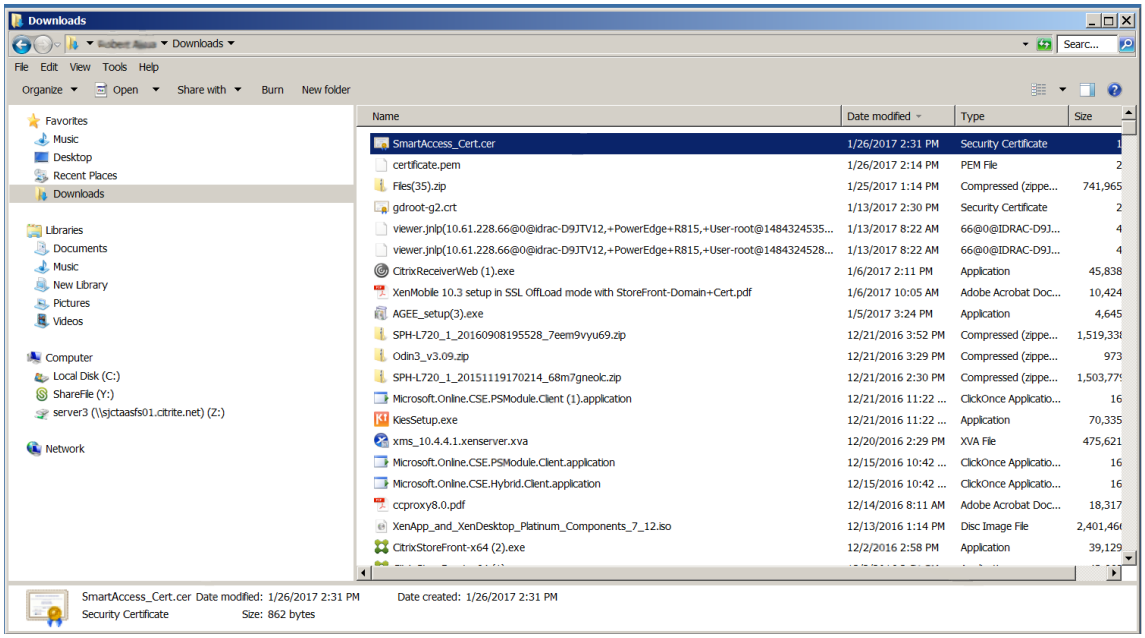


12. Revise suas seleções e clique em **Concluir**. Clique em **OK** na janela de confirmação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



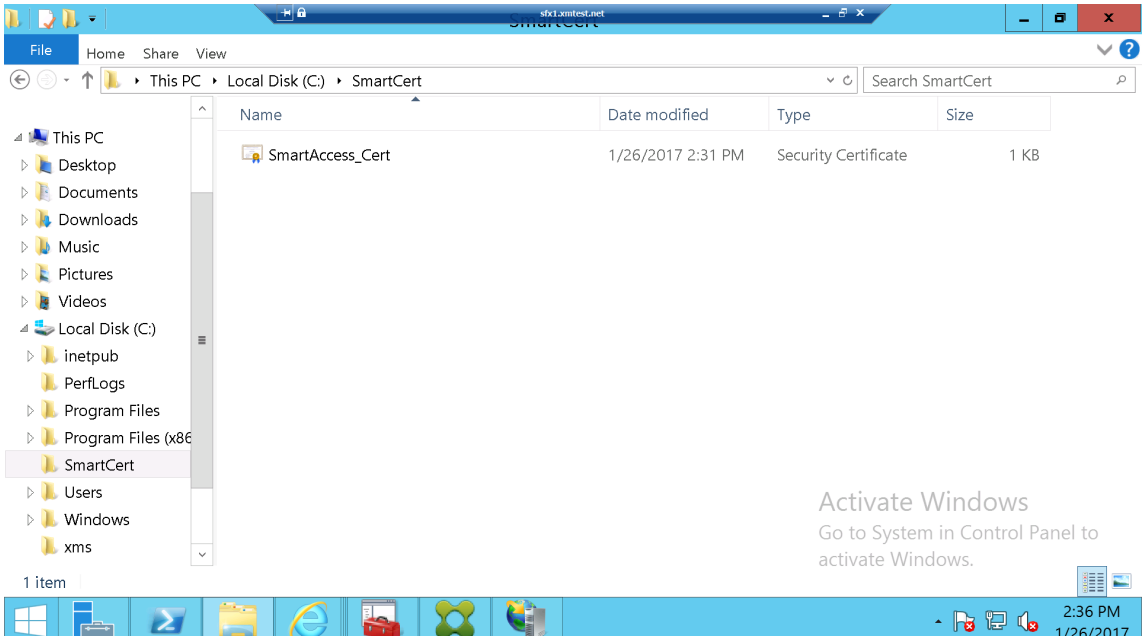
13. Localize o certificado no diretório de download. Observe que o certificado está no formato CER.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Copie o certificado para o Servidor StoreFront

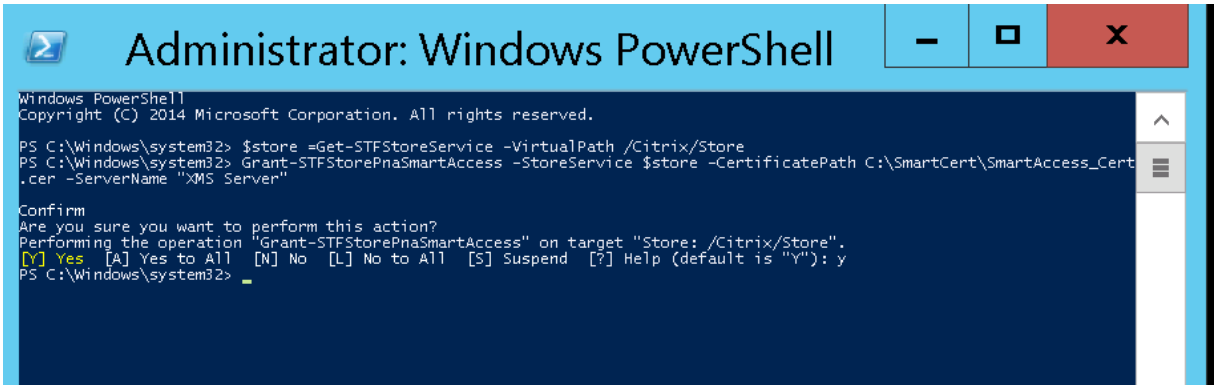
1. No servidor StoreFront, crie uma pasta chamada **SmartCert**.
2. Copie o certificado para a pasta **SmartCert**.



Configure o certificado no repositório do StoreFront

No servidor StoreFront, execute este comando do PowerShell para configurar o certificado do XenMobile Server convertido no repositório:

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
```



Se houver algum certificado existente no repositório StoreFront, execute este comando do PowerShell para revogá-lo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
Revoke-STFStorePnaSmartAccess -StoreService $store -All
```



Como alternativa, você pode executar qualquer um desses comandos do PowerShell no servidor StoreFront para revogar certificados existentes no repositório 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 "1094821dec7834d5d42
    bb456329efe4fca86c60b"
```

- Revogar por objeto de servidor:

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess -StoreService $store

Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess
    $access.AccessConditionsTrusts[0]
```

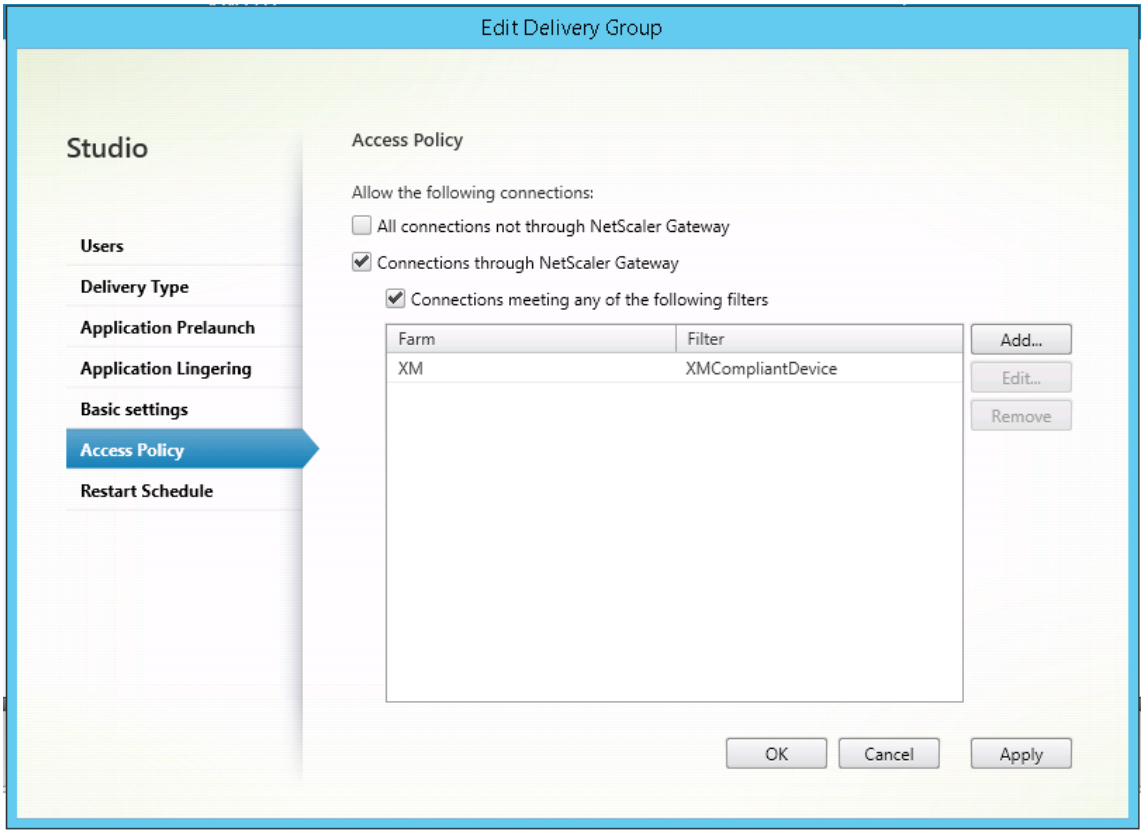
Configure a política SmartAccess para o XenApp e o XenDesktop

Para adicionar a política SmartAccess necessária ao grupo de entrega que fornecer o aplicativo HDX:

1. No XenApp e no XenDesktop Server, abra o Citrix Studio.
2. Selecione **Grupos de entrega** no painel de navegação do Studio.
3. Selecione um grupo de entrega para o aplicativo ou os aplicativos aos quais você deseja controlar o acesso. Em seguida, selecione **Editar grupo de entrega** no painel **Ações**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Na página **Política de acesso**, selecione **Conexões por meio do NetScaler Gateway** e **Conexão que atende a qualquer um dos seguintes**.
5. Clique em **Adicionar**.
6. Adicione uma política de acesso em que **Farm** seja **XM** e **Filtro** seja **XMCompliantDevice**.

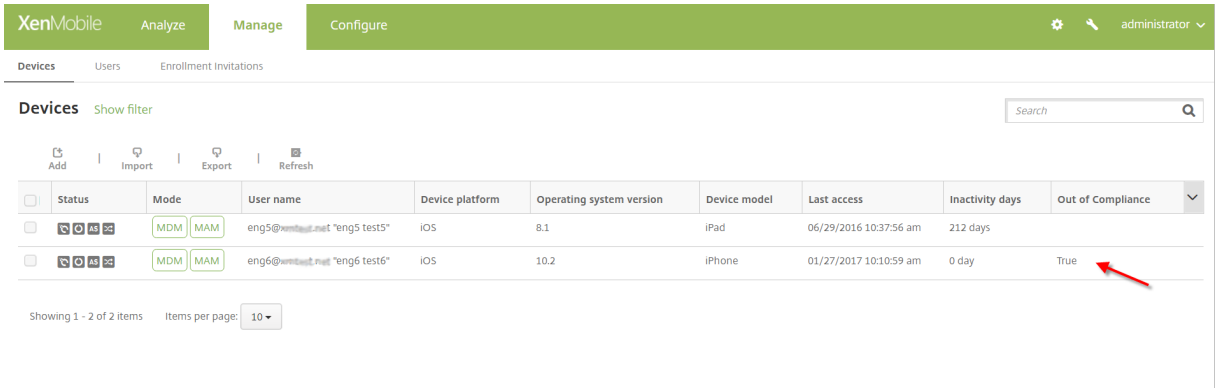


7. Clique em **Aplicar** para aplicar as alterações feitas e deixar a janela aberta ou clique em **OK** para aplicar as alterações e fechar a janela.

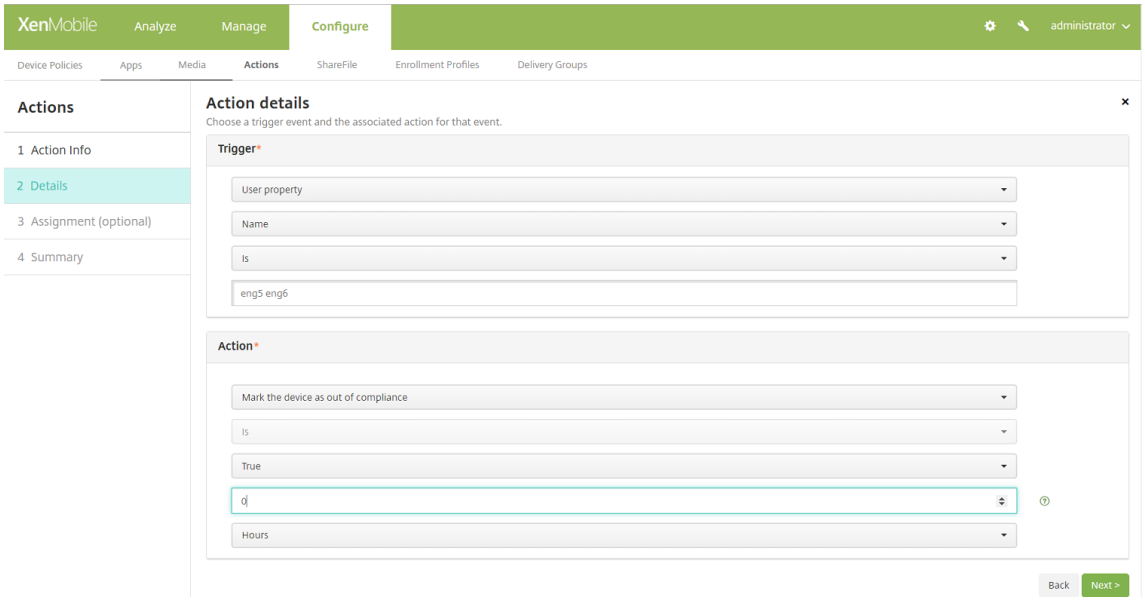
Definir ações automatizadas no XenMobile

A política SmartAccess que você define no grupo de entrega de um aplicativo HDX nega o acesso a um dispositivo quando esse dispositivo está fora de conformidade. Use ações automatizadas para marcar o dispositivo como fora de conformidade.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações sobre a ação** é exibida.
3. Na página **Informações sobre a 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, é criado um gatilho que marca imediatamente os dispositivos como fora de conformidade quando eles têm o nome de propriedade do usuário **eng5** ou **eng6**.



5. Na lista **Gatilho**, escolha **Propriedade do dispositivo**, **Propriedade do usuário** ou **Nome do aplicativo instalado**. O SmartAccess não dá suporte a gatilhos de evento.
6. Na lista **Ação**:
   - Escolha **Marcar o dispositivo como fora de conformidade.**
   - Escolha **Is**.
   - Escolha **True**.
   - Para definir a ação de marcar o dispositivo como fora de conformidade imediatamente quando a condição de gatilho for atendida, defina o período de tempo como **0**.

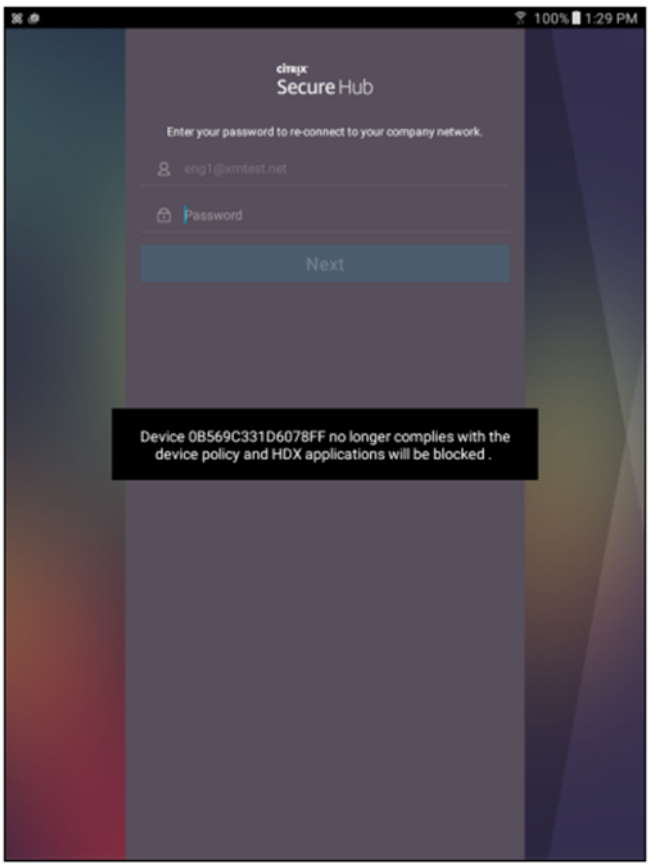
© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. Escolha o grupo ou os grupos de entrega do XenMobile aos quais aplicar essa ação.
8. Reveja o resumo da ação.
9. Clique em **Avançar** e em **Salvar**.

Quando o dispositivo está marcado como fora de conformidade, os aplicativos HDX deixam de ser exibidos no repositório do Secure Hub. O usuário deixa de estar inscrito aos aplicativos. Nenhuma notificação é enviada ao dispositivo e nada no repositório do Secure Hub indica que os aplicativos HDX estavam disponíveis anteriormente.

Se quiser que os usuários sejam notificados quando um dispositivo estiver marcado como fora de conformidade, crie uma notificação e, em seguida, crie uma ação automatizada para enviar essa notificação.

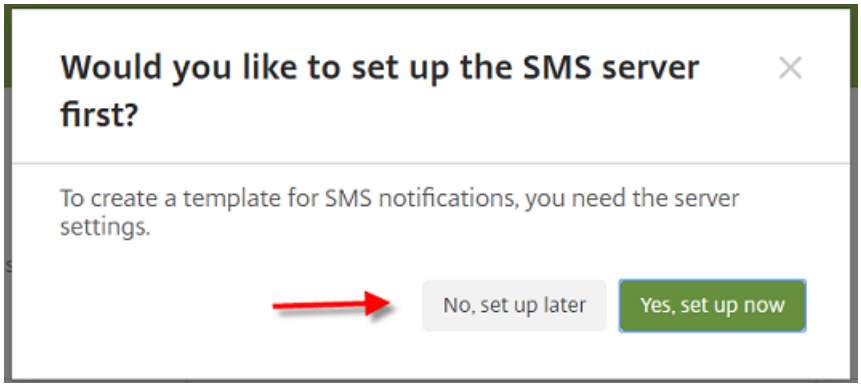
Esse exemplo cria e envia essa notificação quando um dispositivo está marcado como fora de conformidade: “O número de série do dispositivo ou o número de telefone não está mais em conformidade com a política do dispositivo, e os aplicativos HDX serão bloqueados”.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

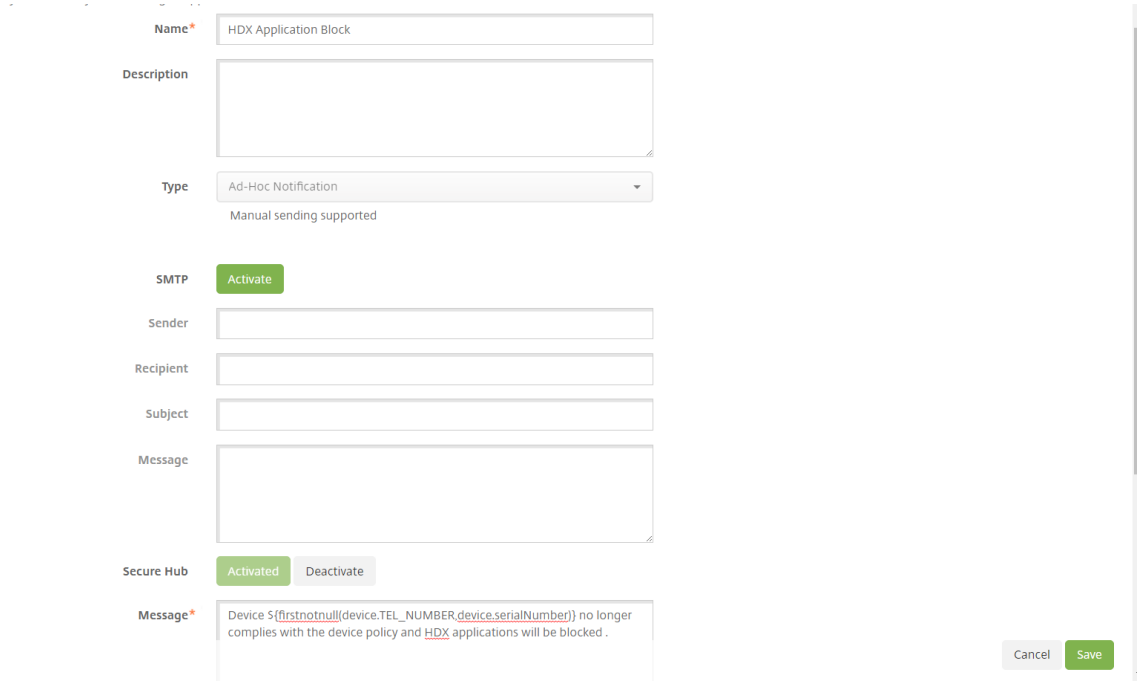
Criar a notificação que os usuários veem quando um dispositivo está marcado como fora de conformidade

1. No console 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 acrescentar à página **Modelos de notificação**.
4. Quando solicitado a configurar primeiro o servidor SMS, clique em **Não, configurar mais tarde**.



5. Defina estas configurações:
   - **Nome:** bloqueio de aplicativos HDX
   - **Descrição:** notificação do agente quando o 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 de dispositivo, e os aplicativos HDX serão bloqueados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

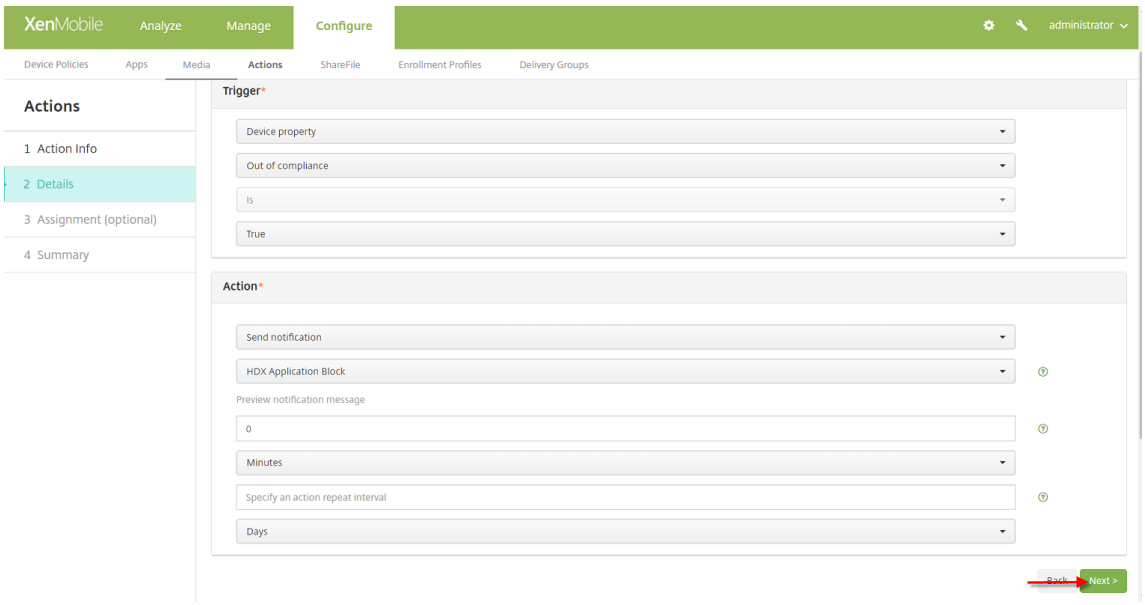


6. Clique em **Salvar**.

Crie a ação que envia a notificação quando um dispositivo está marcado como fora de conformidade

1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações sobre a ação** é exibida.
3. Na página **Informações sobre a 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 **Is**.
   - Escolha **True**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Na lista **Ação**, especifique as ações que ocorrem quando o gatilho é atendido:
   - Escolha **Enviar notificação**
   - Escolha **Bloco de aplicativos HDX, a notificação que você criou**.
   - Escolha **0**. Definir esse valor como 0 faz com que a notificação seja enviada assim que a condição do gatilho é atendida.
7. Selecione o grupo ou os grupos de entrega do XenMobile aos quais aplicar essa ação. Neste exemplo, escolha **AllUsers**.
8. Reveja o resumo da ação.
9. Clique em **Avançar** e em **Salvar**.

Para obter mais informações sobre como definir ações automatizadas, consulte Ações automatizadas.

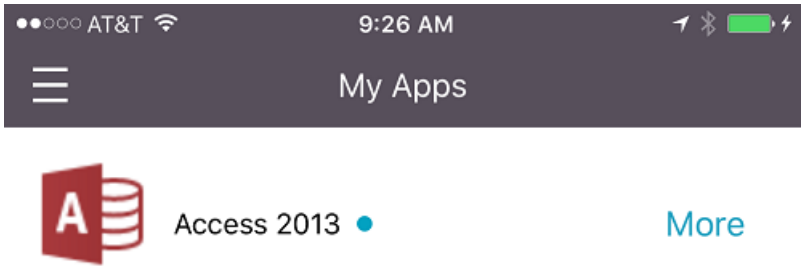
Como os usuários recuperam o acesso a aplicativos HDX

Os usuários podem acessar aplicativos HDX novamente depois que o dispositivo é recolocado em conformidade:

1. No dispositivo, vá até a loja do Secure Hub para atualizar os aplicativos na loja.
2. Vá até o aplicativo e toque em **Adicionar** ao aplicativo.

Depois que o aplicativo for adicionado, ele aparecerá em Meus aplicativos com um ponto azul ao lado, pois é um aplicativo recém-instalado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Adicionar mídia

April 15, 2019

Você adiciona mídia ao XenMobile para poder implantar a mídia em dispositivos de usuário. Você pode usar o XenMobile para implantar iBooks que obtém por meio do Programa Apple Volume Purchase (VPP).

Depois de configurar uma conta VPP no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura iBooks para implantação em dispositivos iOS escolhendo grupos de entrega e especificando regras de implantação.

A primeira vez que um usuário recebe um iBook e aceita a licença VPP, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple iBook. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala iBooks como mídia necessária. Se um usuário exclui um livro instalado do seu dispositivo, o livro permanece no aplicativo iBook, pronto para download.

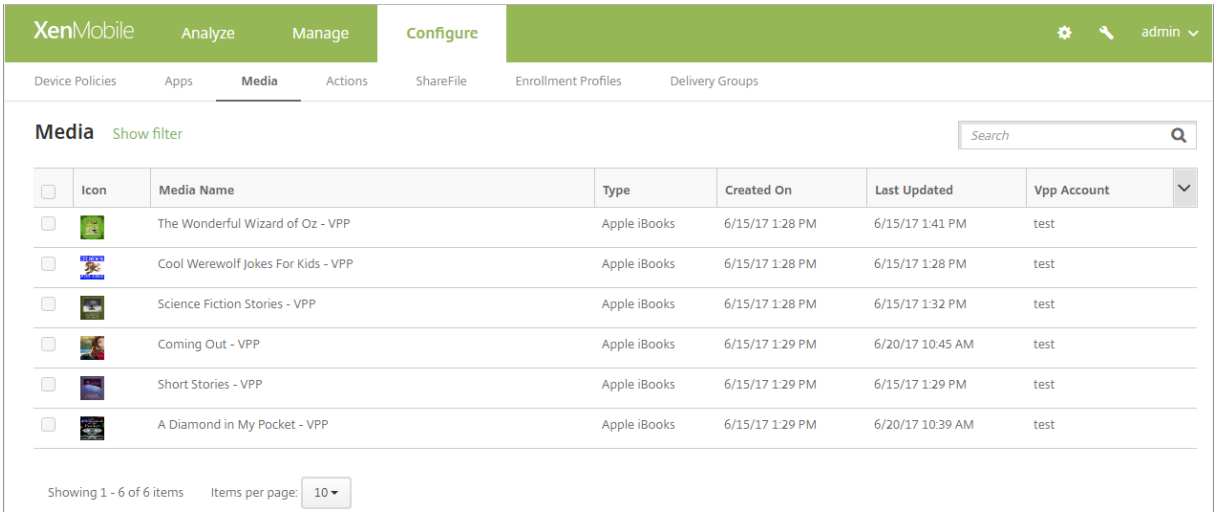
Pré-requisitos

- Dispositivos iOS (versão mínima iOS 8)
- Configure iOS VPP no XenMobile, como descrito em Volume Purchase Plan do iOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

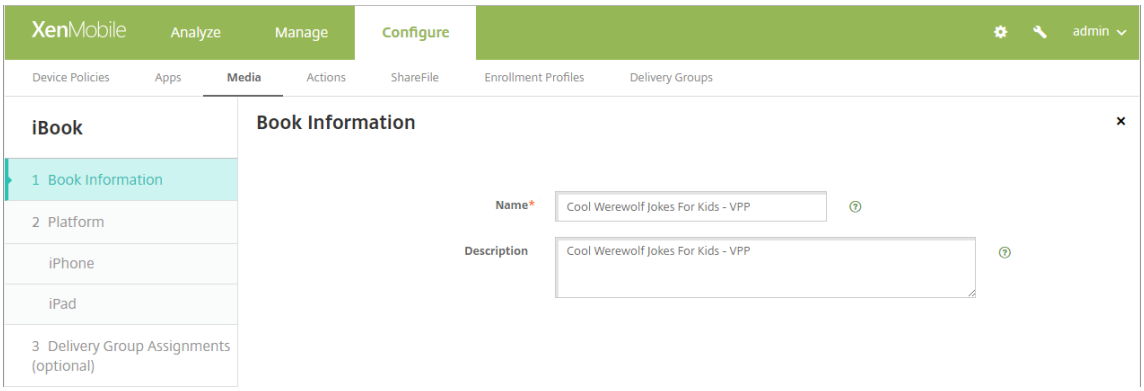
Configurar iBooks

Os iBooks obtidos através do VPP aparecem na página **Configurar > Mídia**.



Para configurar um iBook para implantação

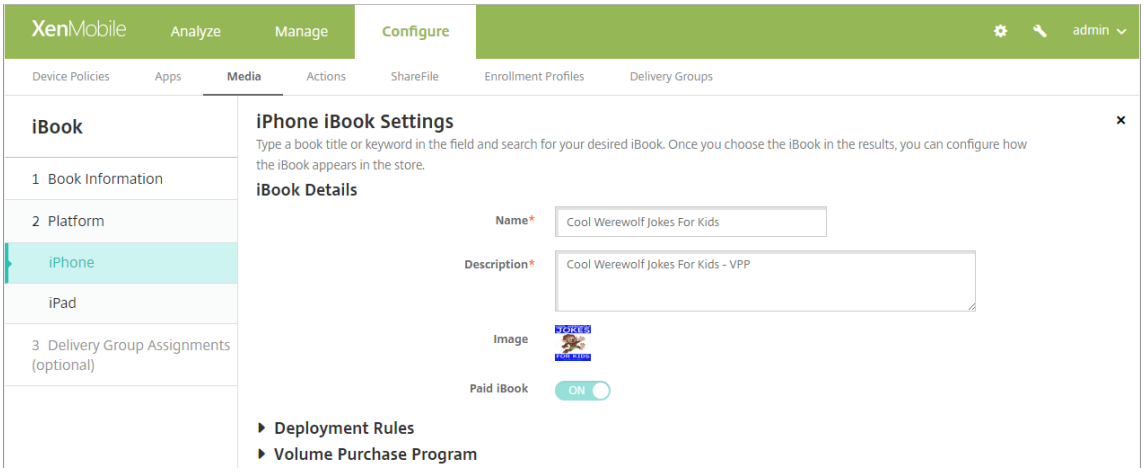
1. Em **Configurar > Mídia**, selecione um iBook e clique em **Editar**. A página **Informações do livro** é exibida.



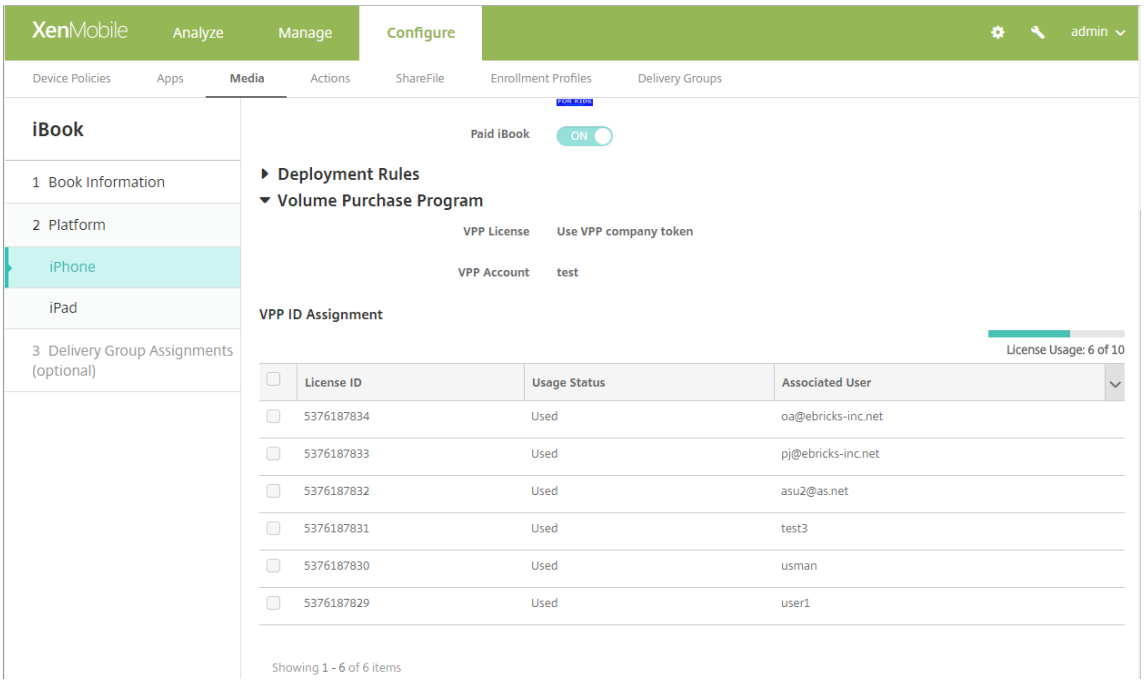
   O **Nome** e **Descrição** são exibidos somente no console XenMobile e logs.

2. Nas páginas de **Configurações iPhone iBook** e **Configurações iPad iBook**: ainda que possa opcionalmente alterar o nome e a descrição do iBook, a Citrix recomenda que você não altere essas configurações. A imagem é para sua informação e não é editável. **iBook pago** indica que um iBook é adquirido através do VPP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

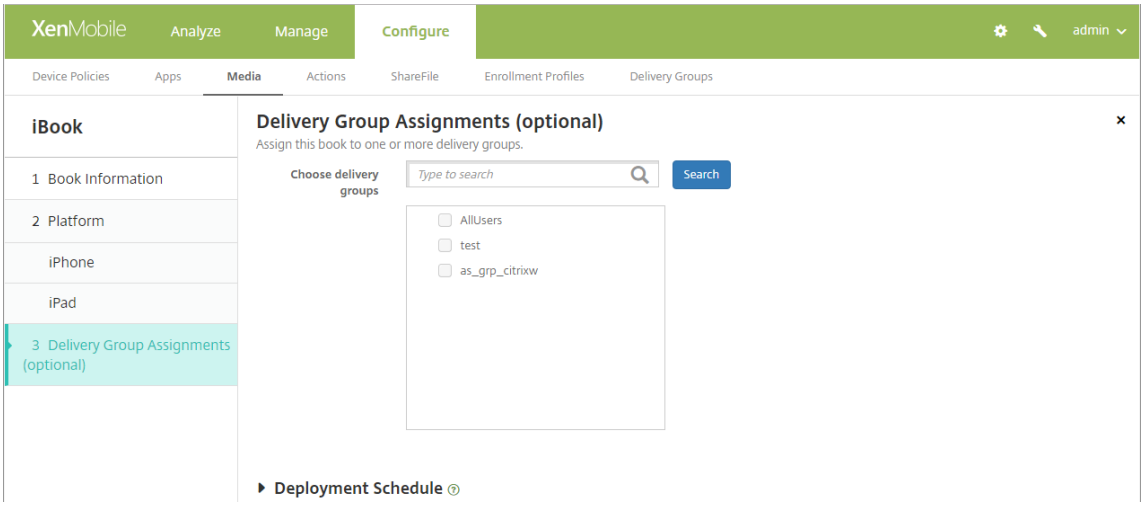


Você também pode especificar regras de implantação ou visualizar informações de VPP.

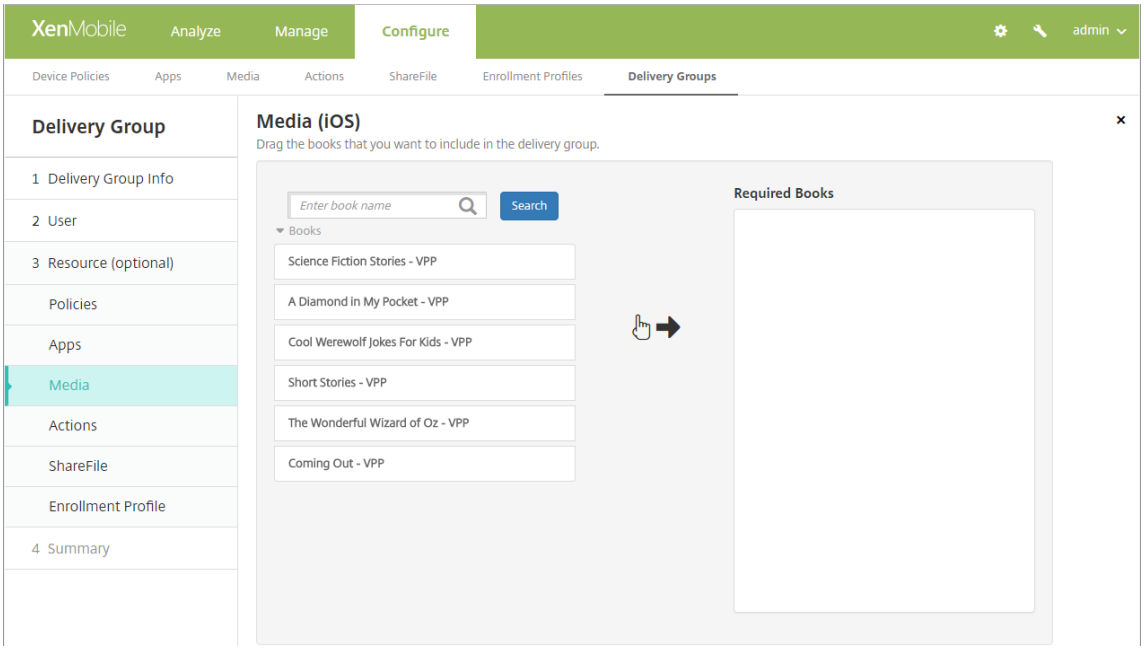


3. Opcionalmente, atribua o iBook aos grupos de entrega e defina um cronograma de implantação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

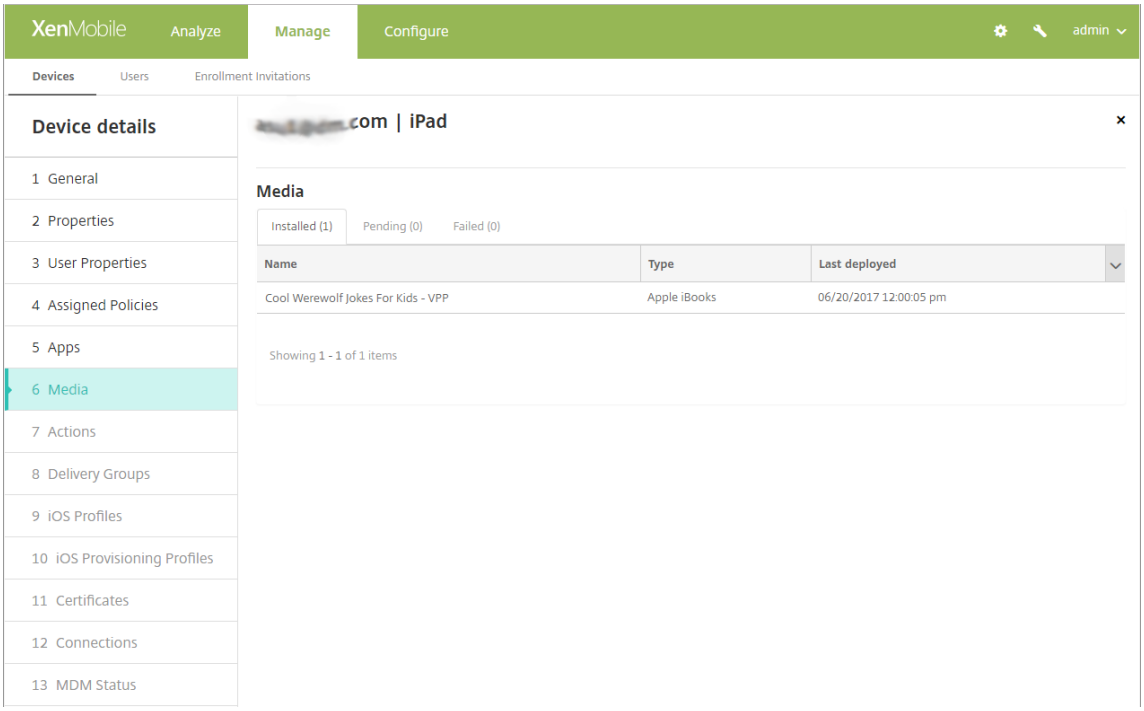


Você também pode atribuir iBooks a grupos de entrega na guia **Mídia** em **Configurar > Grupos de entrega**. Atualmente, o XenMobile suporta apenas a implantação de livro necessária.



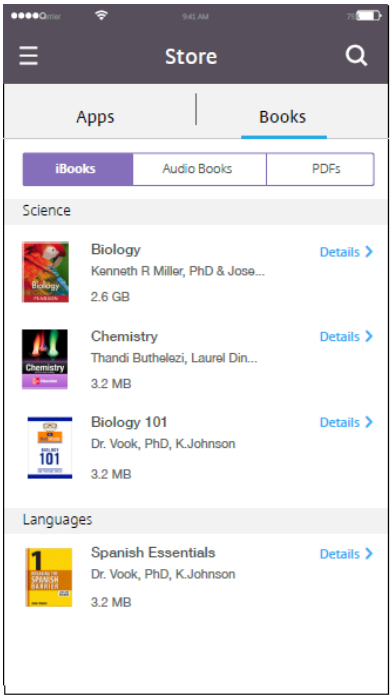
4. Use a guia **Mídia** em **Gerenciar > Dispositivos** para visualizar o status da implantação.

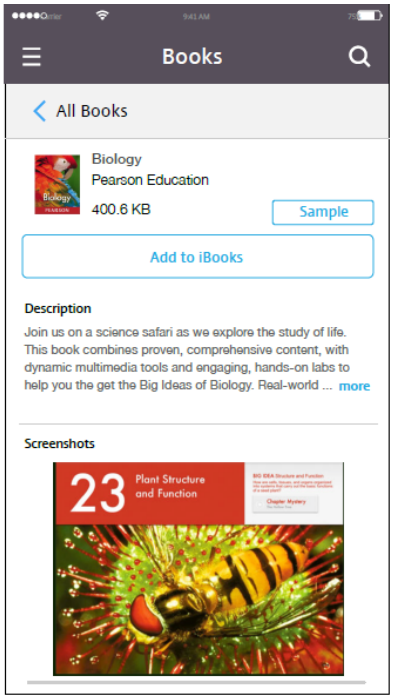
© 1999-2019 Citrix Systems, Inc. All rights reserved.

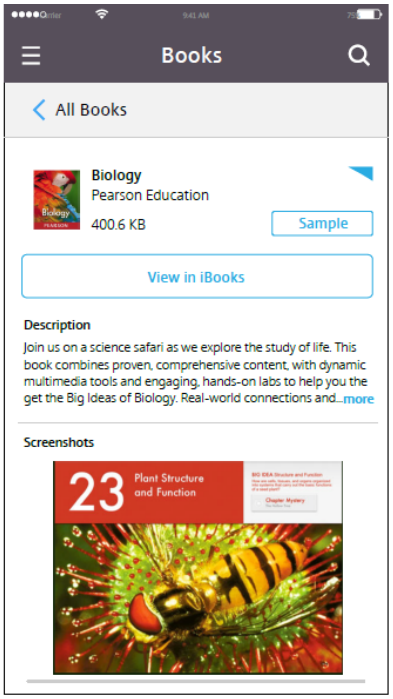


> Nota:
>
> Na página **Configurar > Mídia**, se você selecionar um livro e clicar em **Excluir**, o XenMobile remove o livro da lista. No entanto, na próxima vez que o XenMobile se sincronizar com o VPP, o livro reaparecerá na lista, a menos que tenha sido removido do VPP. A exclusão de um livro da lista não remove o livro dos dispositivos.

Os iBooks são exibidos nos dispositivos dos usuários, como mostrado nestes exemplos.







© 1999-2019 Citrix Systems, Inc. All rights reserved.

Implantar recursos

March 6, 2019

A configuração e o gerenciamento do dispositivo geralmente envolvem a criação de recursos (políticas, aplicativos e mídias) e ações no console XenMobile e, em seguida, o empacotamento deles usando grupos de entrega. A ordem na qual o XenMobile envia recursos e ações para os dispositivos em um grupo de entrega 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 têm políticas duplicadas ou conflitantes.

Os grupos de entrega especificam a categoria dos usuários em cujos dispositivos você implanta combinações de políticas, aplicativos, mídias e ações. A inclusão de um grupo de entrega é normalmente baseada nas características dos usuários, como empresa, país, departamento, endereço do escritório, cargo etc. Os grupos de entrega fornecem um maior controle sobre quem recebe quais recursos e quando isso ocorre. Você pode implantar um grupo de entrega para todos ou para um grupo de usuários definido de forma mais restrita.

Implantar em um grupo de entrega significa enviar uma notificação por push a todos os usuários com dispositivos iOS e Windows compatíveis. Esses usuários devem pertencer ao grupo de entrega para reconectarem-se ao XenMobile. Você pode reavaliar os dispositivos e implantar políticas, aplicativos, mídias e ações que fazem parte de um grupo de entrega.

Para usuários com dispositivos Android: se eles já estiverem conectados, receberão os recursos imediatamente. Caso contrário, com base em suas políticas de agendamento, eles receberão recursos da próxima vez em 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 os usuários do Active Directory. Você não pode excluir o grupo AllUsers, mas pode desativá-lo quando não desejar enviar recursos por push para todos os usuários.

Ordem de implantação

Ordem de implantação é a sequência na qual o XenMobile envia recursos para os dispositivos. A ordem de implantação é compatível somente com o modo MDM.

Quando você determina a ordem de implantação, o XenMobile aplica filtros e critérios de controle, como as regras de implantação e o cronograma de implantação, a políticas, aplicativos, mídias, ações e grupos de entrega. Antes de adicionar grupos de entrega, considere como as informações nesta seção se relacionam às suas metas de implantação.

Este é um resumo dos principais conceitos relacionados à ordem de implantação:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Ordem de implantação:** a sequência na qual o XenMobile envia recursos (políticas, aplicativos e mídias) e ações para um dispositivo. A ordem de implantação de algumas políticas, como Termos e Condições e Inventário de Software, não afeta outros recursos. A ordem na qual as ações são implantadas não afeta outros recursos, portanto, a respectiva 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 de dispositivo para filtrar as políticas, os aplicativos, as mídias, as ações e os grupos de entrega. Por exemplo, uma regra de implantação pode especificar o envio por push do pacote de implantação quando um nome de domínio corresponde a um determinado valor.
- **Cronograma de implantação:** o XenMobile usa o cronograma de implantação que você especificar para as políticas, aplicativos, mídias e ações para controlar a implantação desses itens. Você pode especificar que uma implantação ocorra imediatamente, em uma determinada data e hora ou de acordo com as condições de implantação.

A tabela a seguir mostra os critérios de filtro e controle para os vários tipos de objetos e recursos. As regras de implantação são baseadas nas propriedades do dispositivo.

Objeto/recurso	Plataforma do dispositivo	Regra de implantação	Cronograma de implantação	Usuário/grupos
Política de dispositivo	S	S	S	-
Aplicativo	S	S	S	-
Mídia	S	S	S	-
Ação	-	S	S	-
Grupo de entrega	-	S	-	S

É muito provável que, em um ambiente típico, vários grupos de entrega sejam atribuído a um único usuário, com os seguintes resultados possíveis:

- Existem objetos duplicados nos grupos de entrega.
- Uma política específica está configurada de forma diferente em mais de um grupo de entrega que é atribuído a um usuário.

Quando uma dessas situações ocorre, o XenMobile calcula uma ordem de implantação para todos os objetos que ele deve entregar para um dispositivo ou executar. As etapas de cálculo são independentes da plataforma do dispositivo.

Etapas de cálculo:

1. Determine todos os grupos de entrega de um usuário específico com base em filtros de usuários,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

grupos e regras de implantação.

2. Crie uma lista ordenada de todos os recursos (políticas, aplicativos, mídias e ações) dentro de grupos de entrega selecionados. A lista baseia-se nos filtros de plataforma de dispositivo, regras de implantação e agendamento de implantação. O algoritmo de ordenação é o seguinte:

    a) Coloque os recursos dos grupos de entrega que têm uma ordem de implantação definida pelo usuário antes daqueles que não a têm. A lógica desse posicionamento é descrita após estas etapas.

    b) Como fator decisivo entre grupos de entrega, ordene os recursos dos grupos de entrega por 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 no grupo de entrega por nome do recurso.

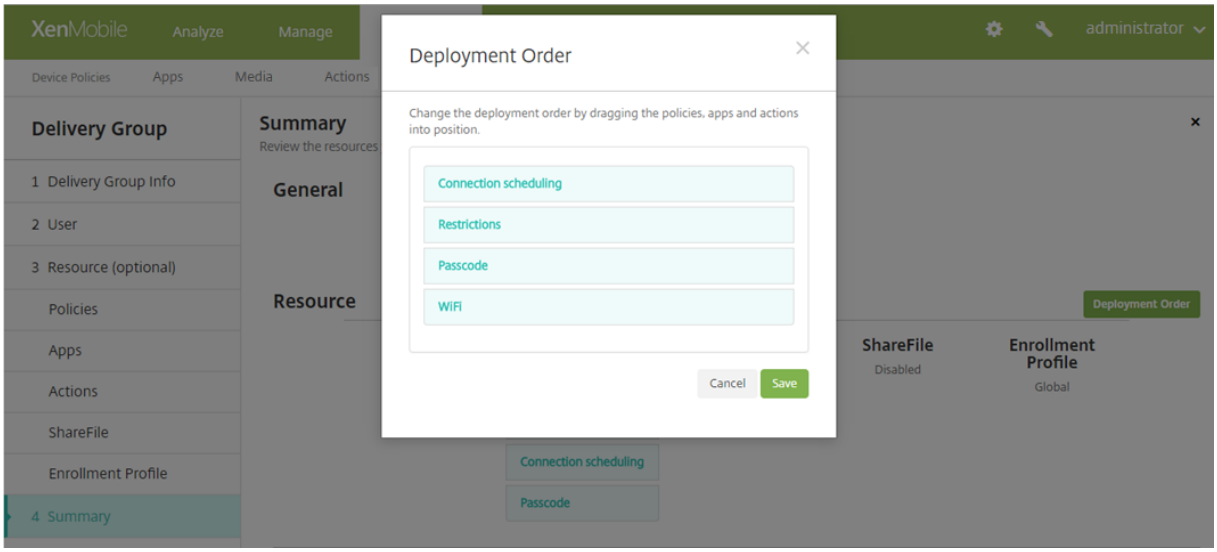
    d) Se o mesmo recurso aparece mais de uma vez, remova o recurso duplicado.

Os recursos que têm 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 ao usuário. Como indicado nas etapas acima, o algoritmo de cálculo apenas remove recursos redundantes e fornece o primeiro recurso nesta lista. Removendo recursos duplicados deste modo o XenMobile impõe a ordem definida pelo administrador do XenMobile.

Por exemplo, suponha que você tem dois grupos de entrega, desta forma:

- Grupo de entrega, Gerentes de conta 1: com ordem **não especificada** para recursos. Contém as políticas **WiFi** e **Código secreto**.
- Grupo de entrega, Gerentes de conta 2: com ordem **especificada** para recursos. Contém as políticas **Agendamento de conexão**, **Restrições**, **Código secreto** e **WiFi**. Nesse caso, você deseja fornecer a política de **Código secreto** antes de a política **WiFi**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



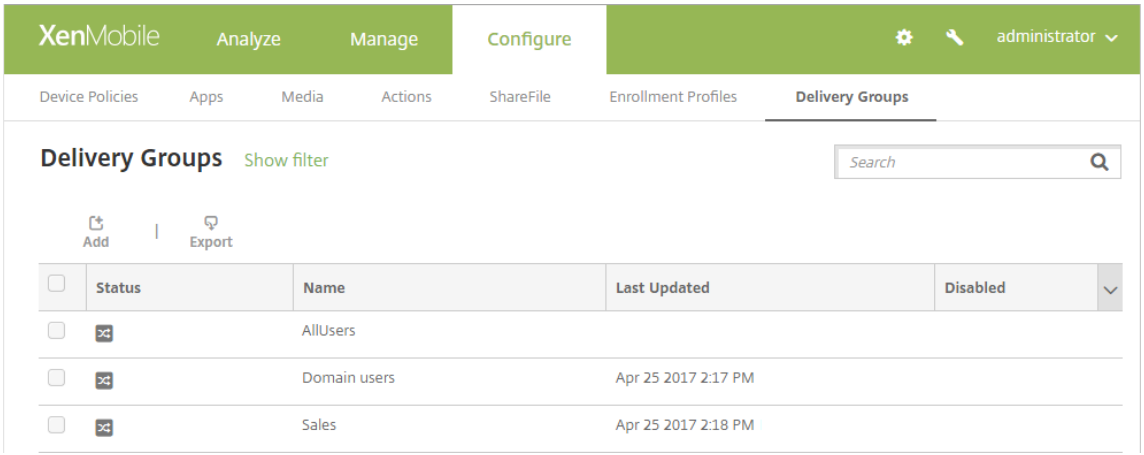
Se o algoritmo de cálculo tiver classificado grupos de implantação apenas por nome, o XenMobile realizará a implantação nessa ordem, começando com o grupo de entrega Gerentes de conta 1: **WiFi**, **Código secreto**, **Agendamento de conexão** e **Restrições**. O XenMobile ignoraria **Código secreto** e **WiFi**, os dois itens duplicados do grupo de entrega Gerentes de Conta 2.

No entanto, o grupo Gerentes de conta 2 tem uma ordem especificada pelo administrador de implantação. Portanto, o algoritmo de cálculo coloca recursos do grupo de entrega Gerentes de conta 2 mais alto na lista do que os recursos do outro grupo de entrega. Como resultado, o XenMobile implanta as políticas nesta ordem:**Agendamento de conexãoRestrição**, **Código secreto** e **WiFi**. O XenMobile ignora as políticas de **Wi-Fi** e **Código secreto** do grupo de entrega Gerentes de conta 1 porque eles são itens duplicados. Portanto, esse algoritmo não respeita a ordem especificada pelo administrador do XenMobile.

Para adicionar um grupo de entrega

1. No console XenMobile, clique em **Configurar > Grupos de entrega**. A página **Grupos de entrega** é exibida.

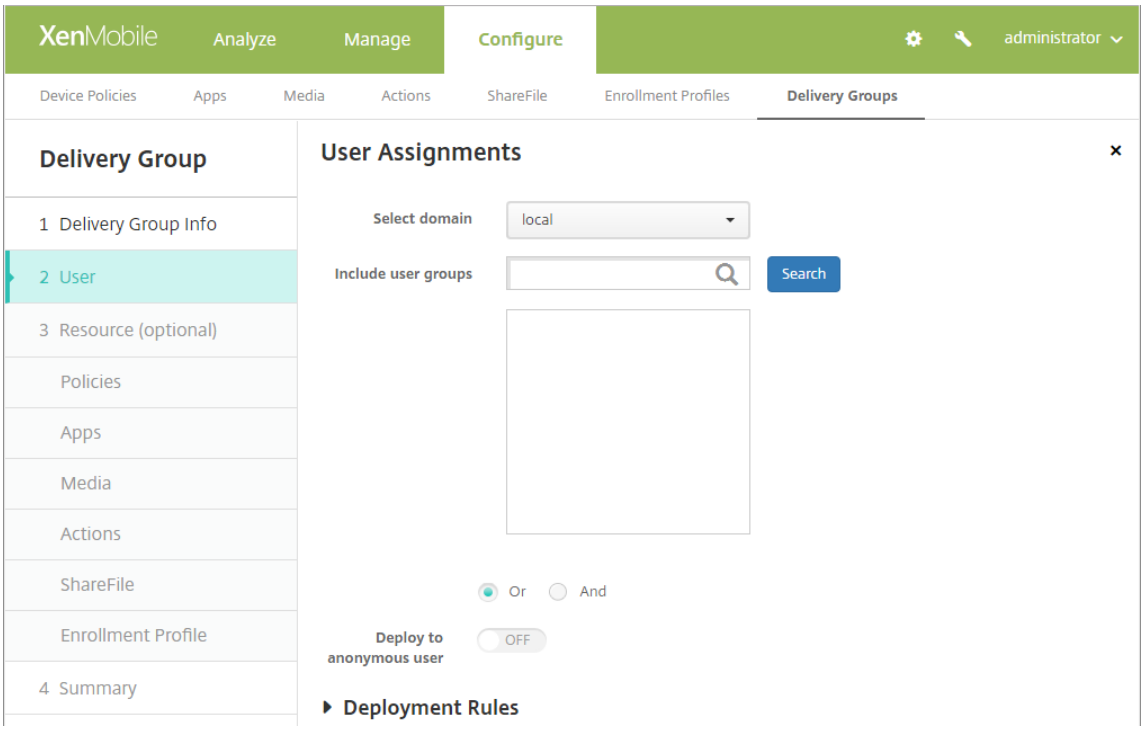
© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Na página **Grupos de entrega**, clique em **Adicionar**. Quando a página **Informações de grupo de entrega** for exibida, insira as seguintes informações:

   - **Nome:** digite um nome descritivo para o grupo de entrega.
   - **Descrição:** digite uma descrição opcional para o grupo de entrega.

3. Clique em **Avançar**. A página **Atribuições do usuário** é exibida. Defina estas configurações:



   - **Selecionar domínio:** na lista, selecione o domínio do qual escolher usuários.
   - **Incluir grupos de usuários:** você pode optar por um dos seguintes procedimentos:
     - Na lista de grupos de usuários, clique em dos grupos que você deseja adicionar. Os grupos selecionados aparecerão na lista **Grupos de usuários selecionados**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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**, você pode optar por um dos seguintes procedimentos:

- Na lista **Grupos de usuários selecionados**, clique no **X** ao lado de cada um dos grupos que você deseja remover.
- Clique em **Pesquisar** para ver uma lista de todos os grupos de usuários no domínio selecionado. Role pela lista e desmarque a caixa de seleção de cada um dos grupos que você 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 pela lista e desmarque a caixa de seleção de cada um dos grupos que você deseja remover.

- **Ou/E:** selecione se os usuários podem estar em qualquer grupo (Ou) ou se devem estar em todos os grupos (E) para que o recurso seja implantado neles.
- **Implantar para usuário anônimo:** selecione se você deseja implantar para os usuários não autenticados no grupo de entrega.

  Usuários não autenticados são usuários que você não conseguiu autenticar, mas cujos dispositivos você permitiu se conectarem ao XenMobile de qualquer maneira.

4. Configure as regras de implantação
5. Expanda **Regras de implantação** e defina estas configurações: a guia **Base** é exibida por padrão.
   - Nas listas, clique nas opções para especificar 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 **Tudo**.
   - Clique em **Nova regra** para definir as condições.
   - Nas listas, clique nas condições, como Propriedade do dispositivo e BYOD.
   - Clique em **Nova regra** novamente para adicionar mais condições.
6. Clique na guia **Avançado** para combinar as regras com as opções boolianas. As condições que você escolheu na guia **Base** são exibidas.
7. Você pode usar a lógica booliana mais avançada para combinar, editar ou adicionar regras.
   - Clique em **AND**, **OR** ou **NOT**.
   - Para adicionar a condição à regra, nas listas, selecione as condições para adicionar à regra e, em seguida, clique no sinal de mais (+) no lado direito.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A qualquer momento, clique para selecionar uma condição e, em seguida, clique em **EDITAR** para alterar a condição ou em **Excluir** para removê-la.

- Clique em **Nova regra** novamente se você desejar adicionar condições.

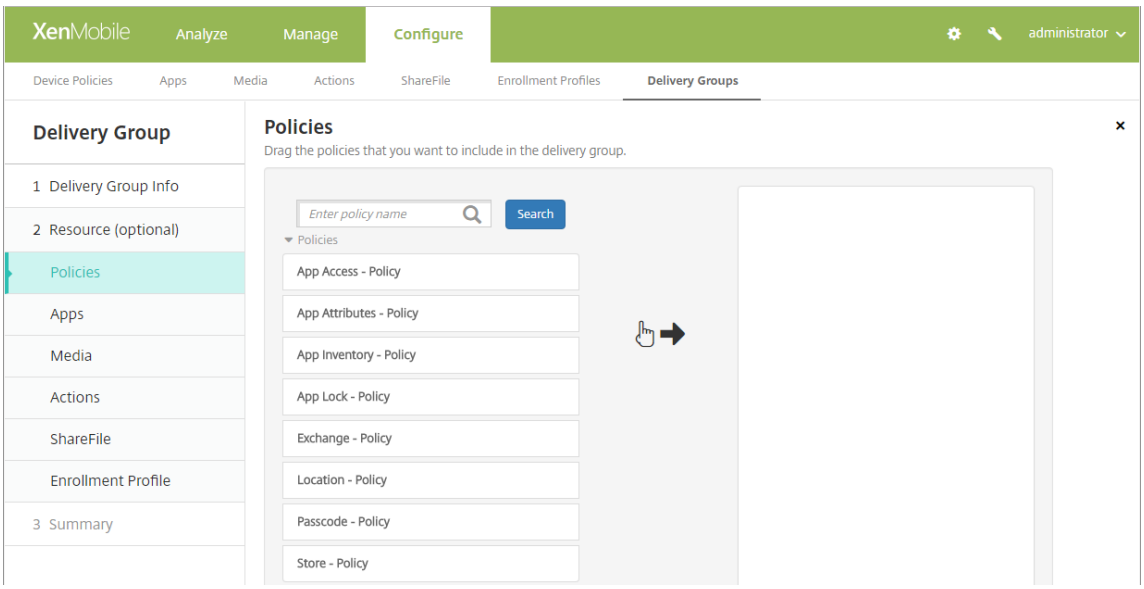
8. Clique em **Avançar**. A página de recursos de **Grupo de entrega** é exibida. Adicione opcionalmente políticas, aplicativos ou ações ao grupo de entrega aqui. Para ignorar essa etapa, em **Grupo de entrega**, clique em **Resumo** para ver um resumo da configuração do grupo de entrega.

   Para ignorar um recurso, em **Recursos (opcional)**, clique no recurso que você deseja adicionar e siga as etapas para esse recurso.

Para adicionar políticas

1. Para cada política que você desejar adicionar, faça o seguinte:
   - Role pela lista de políticas disponíveis para localizar a política que você deseja adicionar.
   - Ou, para limitar a lista de políticas, digite o nome completo ou parcial da política na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
   - Clique na política que deseja adicionar e arraste-a até 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 desejar adicionar, faça o seguinte:

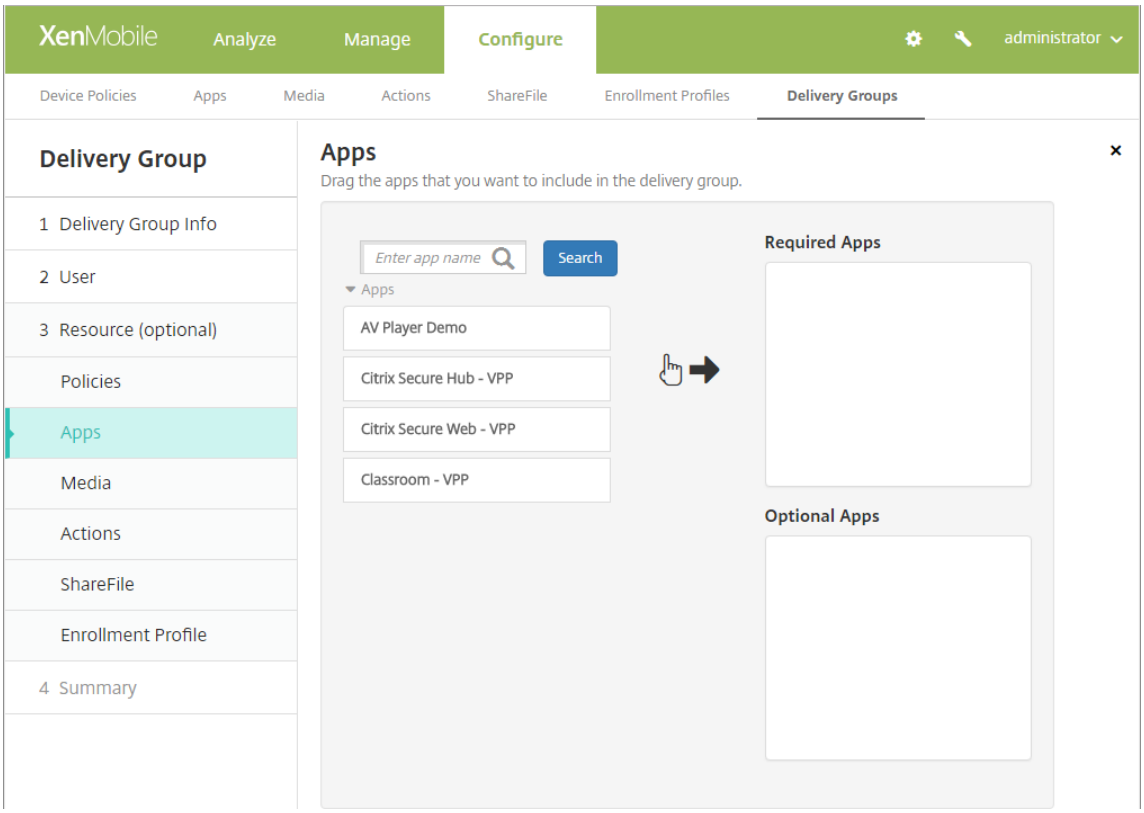
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Role pela lista de aplicativos disponíveis para localizar o aplicativo que você deseja adicionar.
- Ou, para limitar a lista de aplicativos, digite o nome completo ou parcial do aplicativo na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique no aplicativo que você deseja adicionar e arraste-o até a caixa **Aplicativos obrigatórios** ou até a caixa **Aplicativos opcionais**.

Para aplicativos marcados como necessários, os usuários podem receber atualizações imediatamente em situações como:

- Carregue um novo aplicativo e marque-o conforme necessário.
- Marque um aplicativo existente conforme necessário.
- Quando o usuário exclui um aplicativo necessário.
- Está disponível uma atualização do Secure Hub.

Para obter informações sobre a implantação forçada de aplicativos obrigatórios, incluindo como habilitar o recurso, consulte Sobre aplicativos obrigatórios e opcionais.



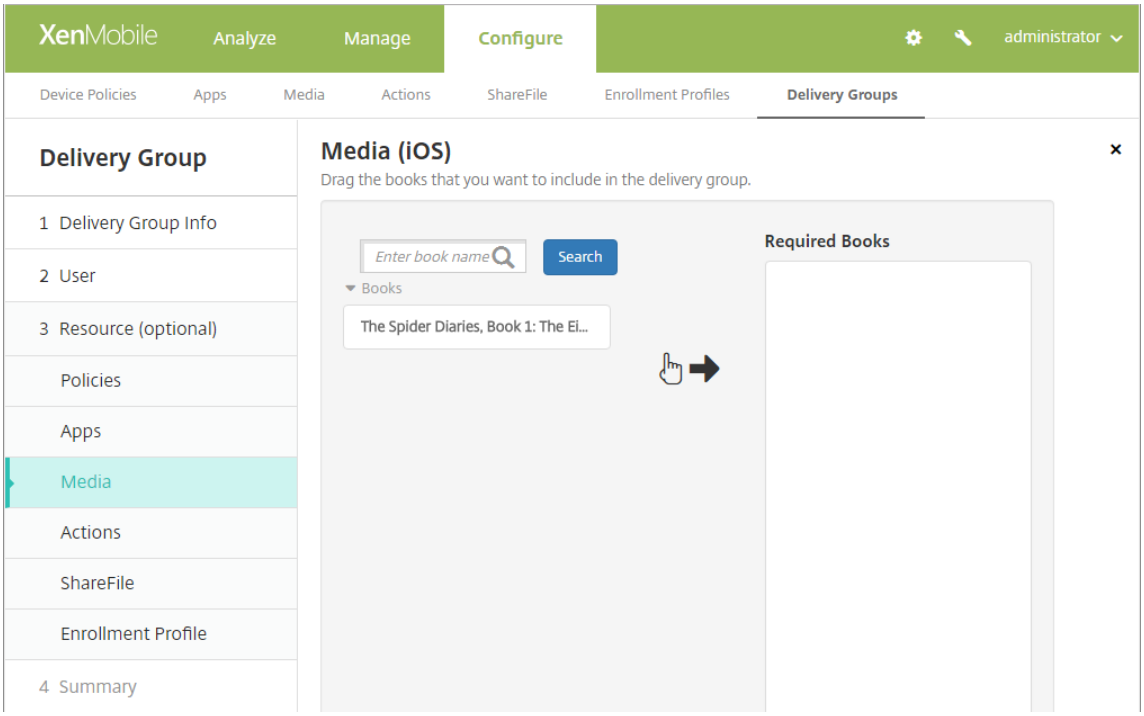
Para remover um aplicativo, clique no **X** ao lado do nome do aplicativo na caixa à direita.

2. Clique em **Avançar**. A página **Mídia** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar mídias

1. Para cada livro que você desejar adicionar, faça o seguinte:
   - Role pela lista de livros disponíveis para localizar o livro que você deseja adicionar.
   - Ou, para limitar a lista de livros, digite o nome completo ou parcial de um livro na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
   - Clique no livro que você desejar adicionar e arraste-o para a caixa **Livros obrigatórios**.



   Para livros marcados como obrigatórios, os usuários recebem atualizações imediatamente em situações como:

   - Carregue um novo livro e marque-o como necessário.
   - Marque um livro existente como necessário.
   - Quando o usuário exclui um livro necessário.
   - Está disponível uma atualização do Secure Hub.

   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.

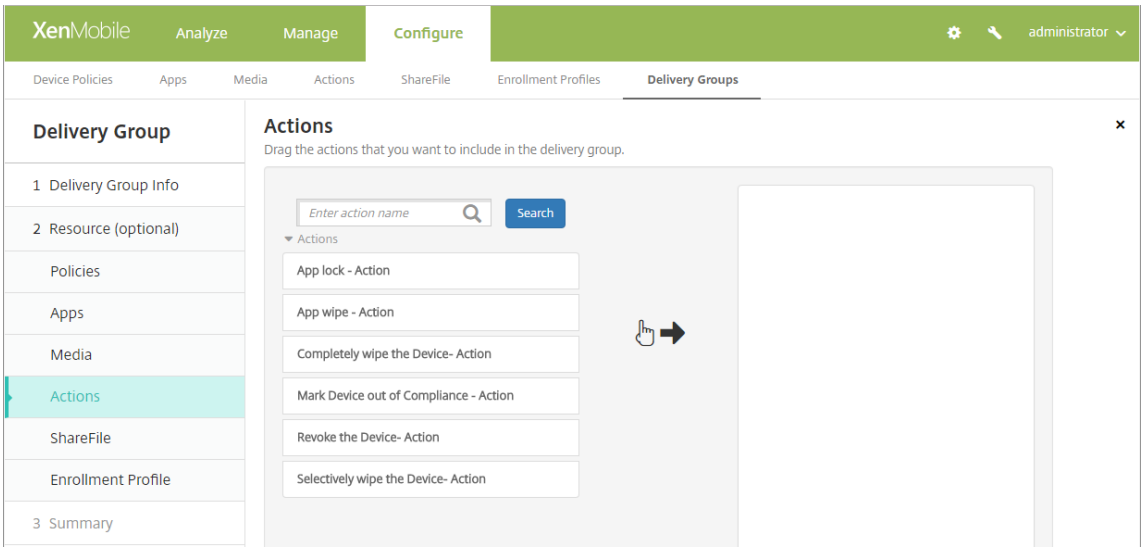
Para adicionar ações

1. Para cada ação que você desejar adicionar, faça o seguinte:
   - Role pela lista de ações disponíveis para localizar o aplicativo que você deseja adicionar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Ou, para limitar a lista de ações, digite o nome completo ou parcial da ação na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique na ação que deseja adicionar e arraste-a até a caixa à direita.

Para remover uma ação, clique no **X** ao lado do nome da ação na caixa à direita.



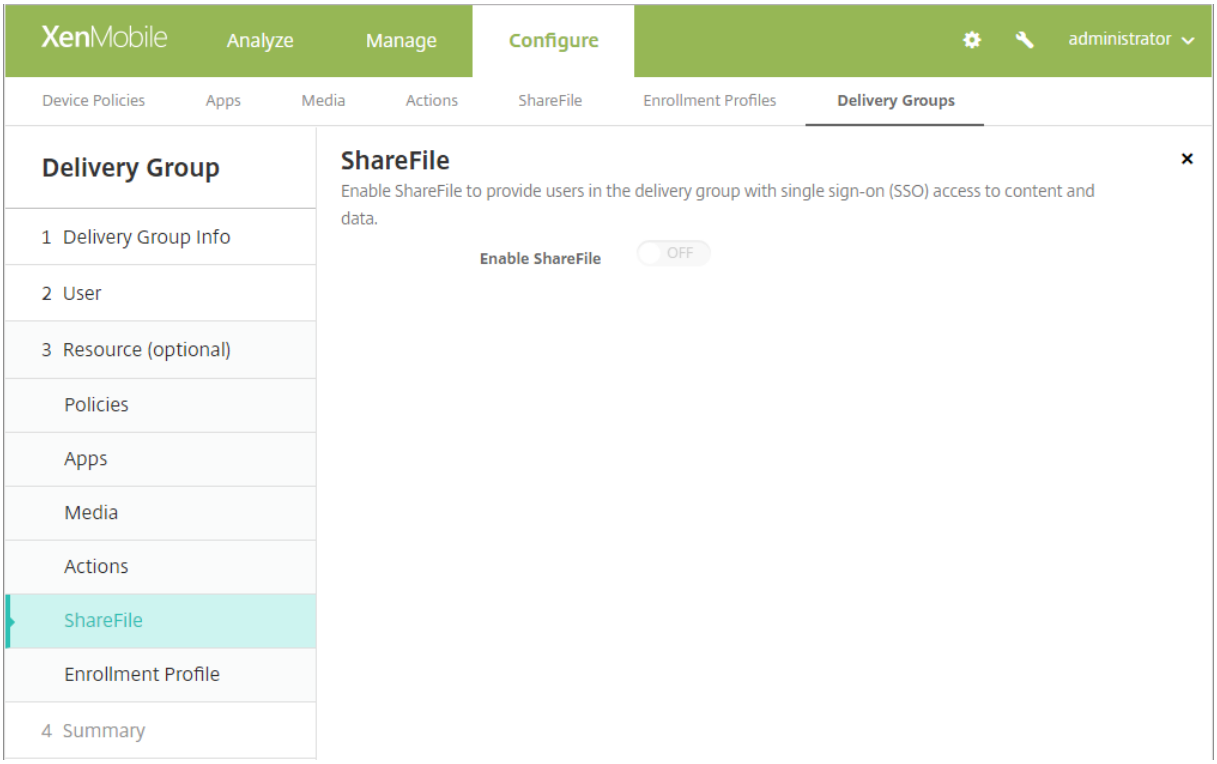
2. Clique em **Avançar**. A página **ShareFile** é exibida.

Pata aplicar a configuração ShareFile

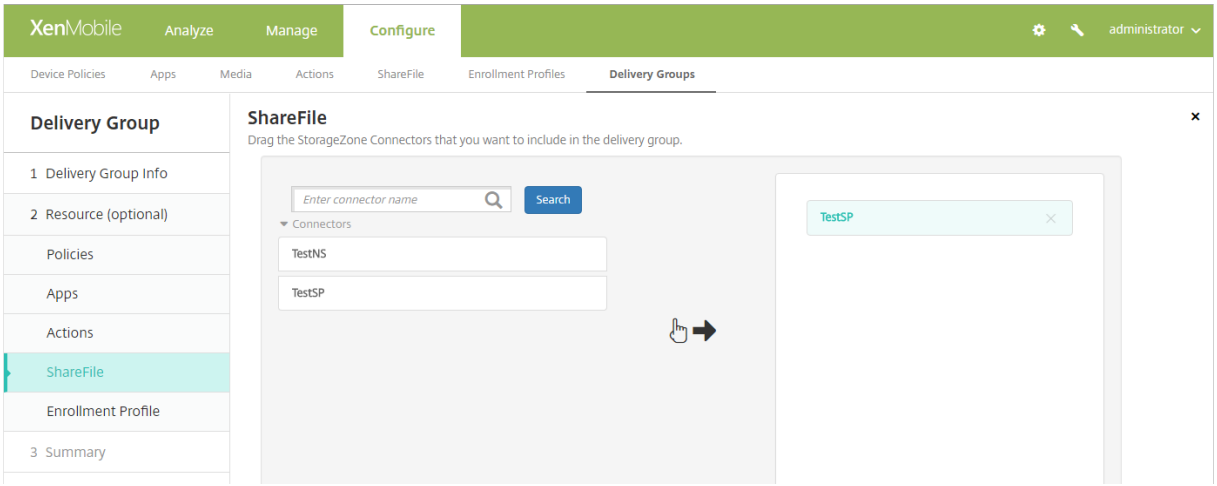
A página ShareFile difere dependendo de você ter configurado o XenMobile (**Configurar > ShareFile**) para o ShareFile Enterprise ou para os StorageZone Connectors.

Se tiver configurado o ShareFile Enterprise para uso com o XenMobile, defina **Ativar ShareFile** como **I** para fornecer de acesso de logon único ao grupo de entrega para o conteúdo e os dados do ShareFile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

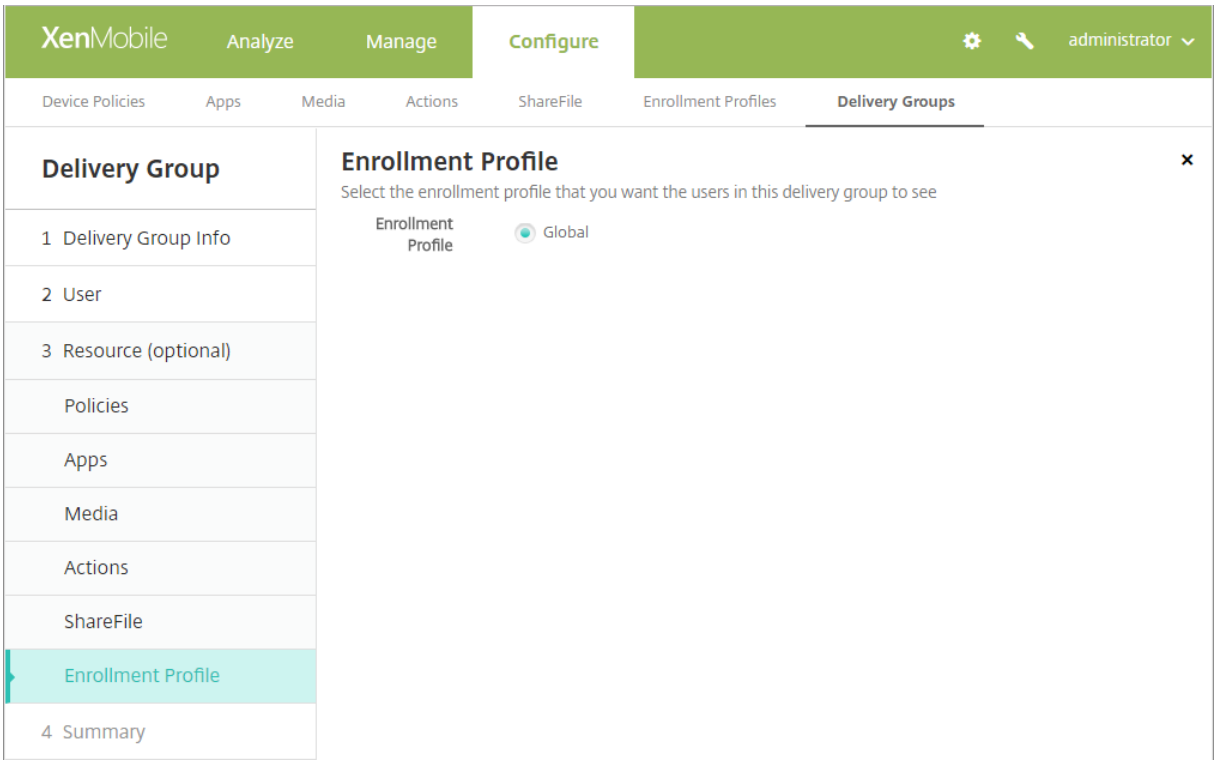


Se você tiver configurado os StorageZone Connectors para uso com o XenMobile, selecione os StorageZone Connectors que devem ser incluídos no grupo de entrega.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

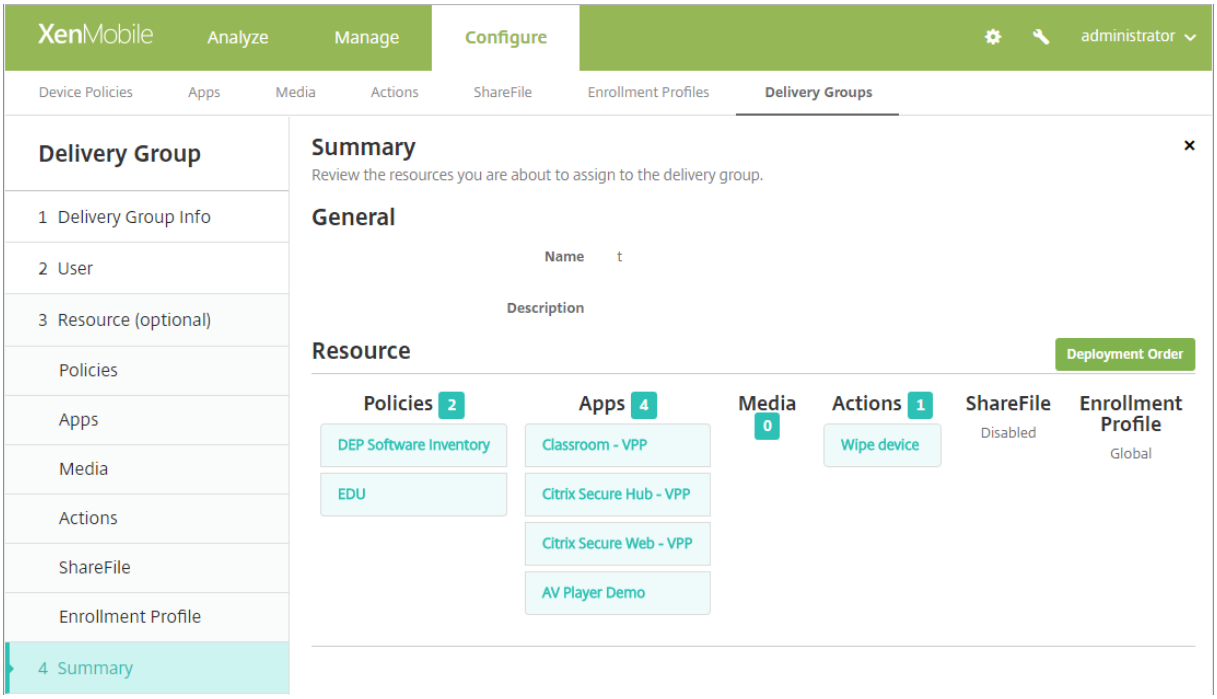
Para selecionar um perfil de registro



- **Perfil de registro:** selecione um perfil de registro. Para criar um perfil de registro, consulte Limite de registro de dispositivos.
- Clique em **Avançar**. A página **Resumo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

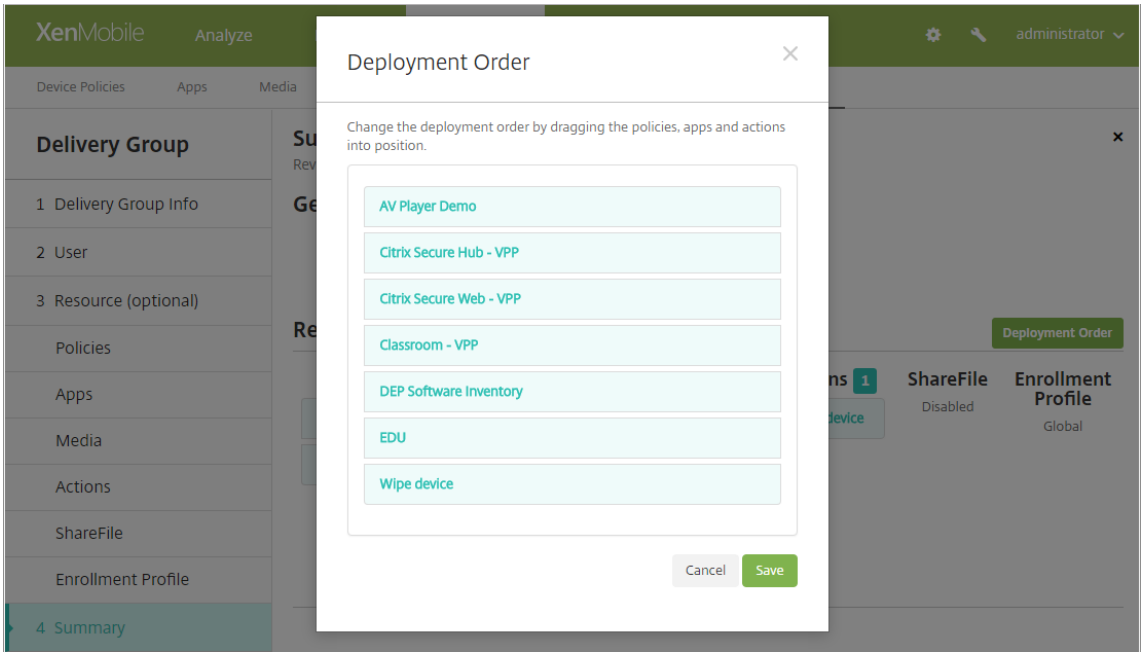
Para revisar as opções configuradas e alterar a ordem de implantação



Na página **Resumo**, você pode verificar as opções que configurou para o grupo de entrega e alterar a ordem de implantação dos recursos. A página Resumo mostra os 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 exibir a ordem de implantação ou para reordenar a implantação. A caixa de diálogo **Ordem de Implantação** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Clique em um recurso e arraste-o até a localização da qual você deseja implantá-lo. 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 ativar e desativar o grupo de entrega AllUsers

AllUsers é o único grupo de entrega que você pode ativar ou desativar.

Na página **Grupos de entrega**, escolha o grupo de entrega AllUsers marcando a caixa de seleção ao lado de **AllUsers** ou clicando na linha que contém AllUsers. Em seguida, você pode optar por um dos seguintes procedimentos:

- Clique em **Desativar** para desativar o grupo de entrega AllUsers. Esse comando estará disponível somente se AllUsers estiver ativado (o padrão). **Desativado** aparece sob o cabeçalho **Desativado** na tabela do grupo de entrega.
- Clique em **Ativar** para ativar o grupo de entrega AllUsers. Esse comando estará disponível somente se AllUsers estiver desativado. **Desativado** desaparece do cabeçalho **Desativado** na tabela do grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para implantar em grupos de entrega

Implantar em um grupo de entrega significa enviar uma notificação por push a todos os usuários com dispositivos iOS, Windows Phone e Tablet Windows. Esses usuários devem pertencer ao grupo de entrega para reconectarem-se ao XenMobile. Dessa forma, você pode reavaliar os dispositivos e implantar aplicativos, políticas e ações.

Para usuários com outros dispositivos de plataformas: se esses dispositivos já estiverem conectados ao XenMobile, eles receberão os recursos imediatamente. Caso contrário, com base em suas políticas de agendamento, eles receberão recursos da próxima vez em que se conectarem.

Para que aplicativos atualizados sejam exibidos na lista Updated Available na XenMobile Store de dispositivos Android, primeiro implante uma política de Inventário de aplicativos nos dispositivos dos usuários.

1. Na página **Grupos de entrega**, você pode optar por um dos seguintes procedimentos:
   - Para implantar em mais de um grupo de entrega por vez, marque as caixas de seleção ao lado dos grupos que você deseja implantar.
   - Para implantar em um único grupo de entrega, marque a caixa de seleção ao lado do respectivo nome ou na linha que contém o nome do grupo.
2. Clique em **Implantar**.

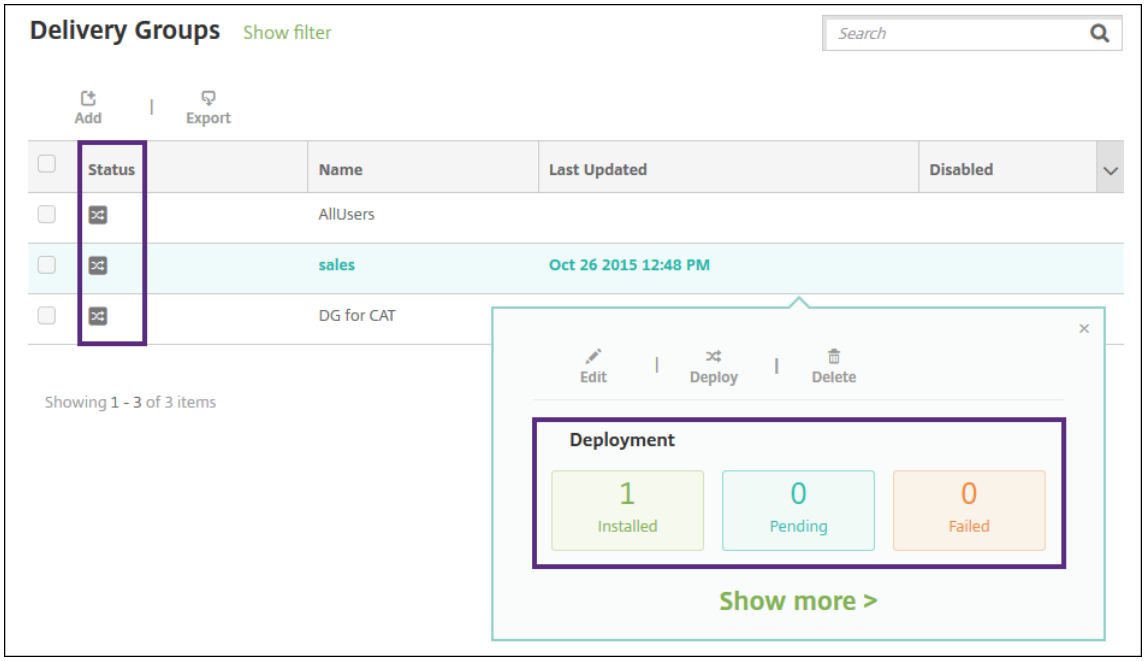
   Dependendo de como você selecionar um único grupo de entrega, o comando **Implantar** será exibido acima ou à direita do grupo de entrega.

   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 para os grupos selecionados com base na plataforma de dispositivo e política de agendamento.

   Você pode verificar o status da implantação na página **Grupos de entrega** de uma das seguintes formas:

   - Examine o ícone de implantação no cabeçalho **Status** do grupo de entrega, o 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para excluir grupos de entrega

Você não pode excluir o grupo de entrega AllUsers, mas pode desativá-lo quando não desejar enviar recursos por push para todos os usuários.

1. Na página **Grupos de entrega**, você pode optar por um dos seguintes procedimentos:
   - Para excluir em mais de um grupo de entrega por vez, marque as caixas de seleção ao lado dos grupos que você deseja excluir.
   - Para excluir um único grupo de entrega, marque a caixa de seleção ao lado do respectivo nome ou na linha que contém o nome do grupo.
2. Clique em **Excluir**. A caixa de diálogo **Excluir** é exibida.

   Dependendo de como você selecionar um único grupo de entrega, o comando **Excluir** será exibido acima ou à direita do grupo de entrega.

   > Importante:
   >
   > Você não pode 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 na tabela **Grupos de entrega** e converte-as em um arquivo .csv.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Abra ou salve o arquivo .csv, seguindo as etapas normais do seu navegador. Você também pode cancelar a operação.

Macros

March 6, 2019

O XenMobile fornece macros como uma forma de preencher dados de propriedades de usuários ou dispositivos 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 sistema ou de usuário correspondentes. Por exemplo, você pode preencher previamente o valor da caixa de correio de um usuário em um único perfil do Exchange entre milhares de usuários.

Sintaxe de macro

Uma macro pode assumir a seguinte forma:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

Coloque toda a sintaxe após o cifrão ($) entre chaves ({ }).

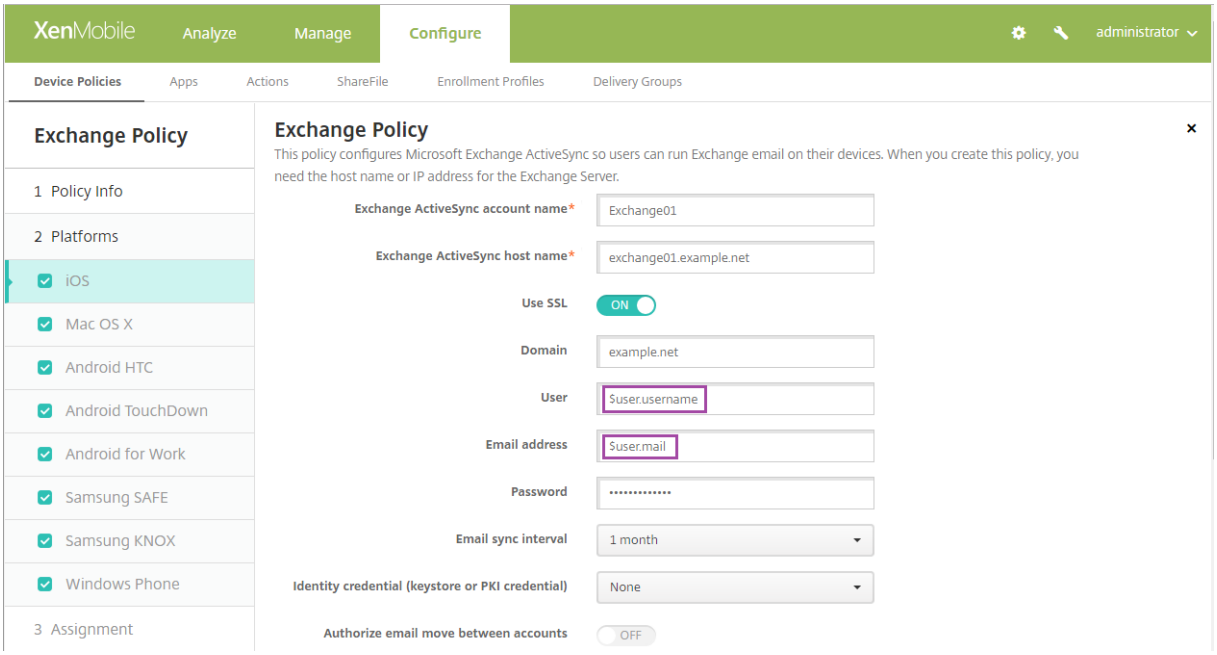
- Os nomes qualificados de propriedade fazem referência a uma propriedade de usuário, uma propriedade de dispositivo ou uma propriedade personalizada.
- Os nomes qualificados de propriedade consistem em um prefixo, seguido do nome real da propriedade.
- Propriedades do usuário do formulário `${ user.[PROPERTYNAME] (prefix="user.")} .`
- Propriedades do dispositivo do formulário `${ device.[PROPERTYNAME] (prefix="device.")} .`
- Nomes de propriedade diferenciam maiúsculas de minúsculas.
- Uma função pode ser uma lista limitada ou um link para uma referência de terceiros que define funções. A seguinte macro para uma mensagem de notificação inclui a função **firstnotnull**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` foi bloqueado...

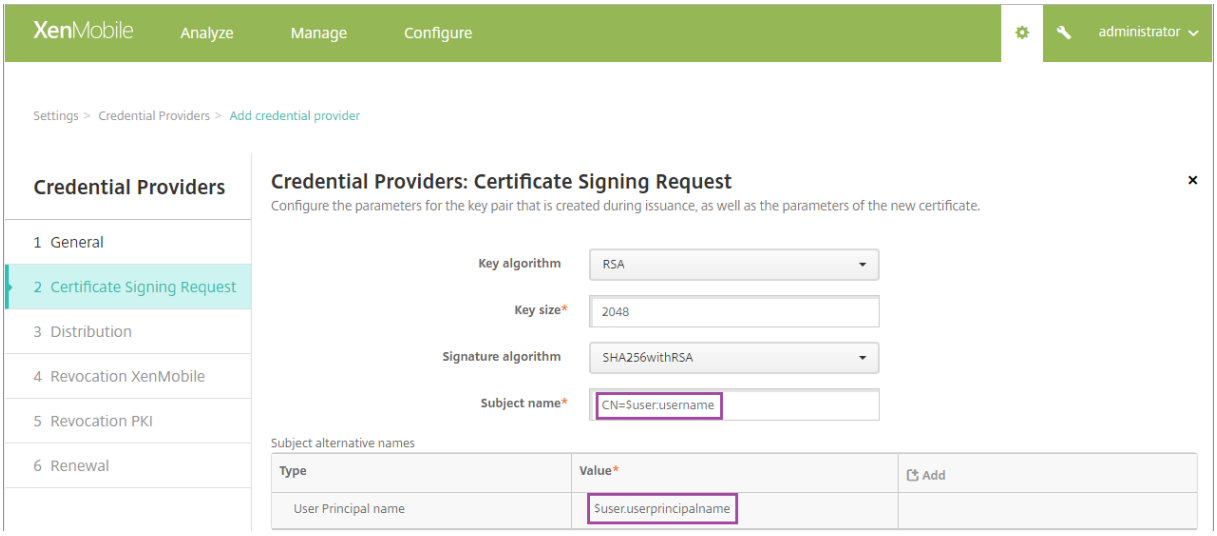
- Para macros personalizadas (propriedades que você define), o prefixo é `${ custom }` . Você pode omitir o prefixo.

Este é um exemplo de macro comum, `${ user.username }` , que preenche o valor de nome do usuário no campo de texto de uma política. Essa macro é útil para configurar perfis do Exchange ActiveSync e outros perfis usados por vários usuários. O exemplo a seguir mostra como usar macros em uma política do Exchange. A macro para o **Usuário** é **`${ user.username }`** . A macro para **Endereço de email** é **`${ user.mail }`** .



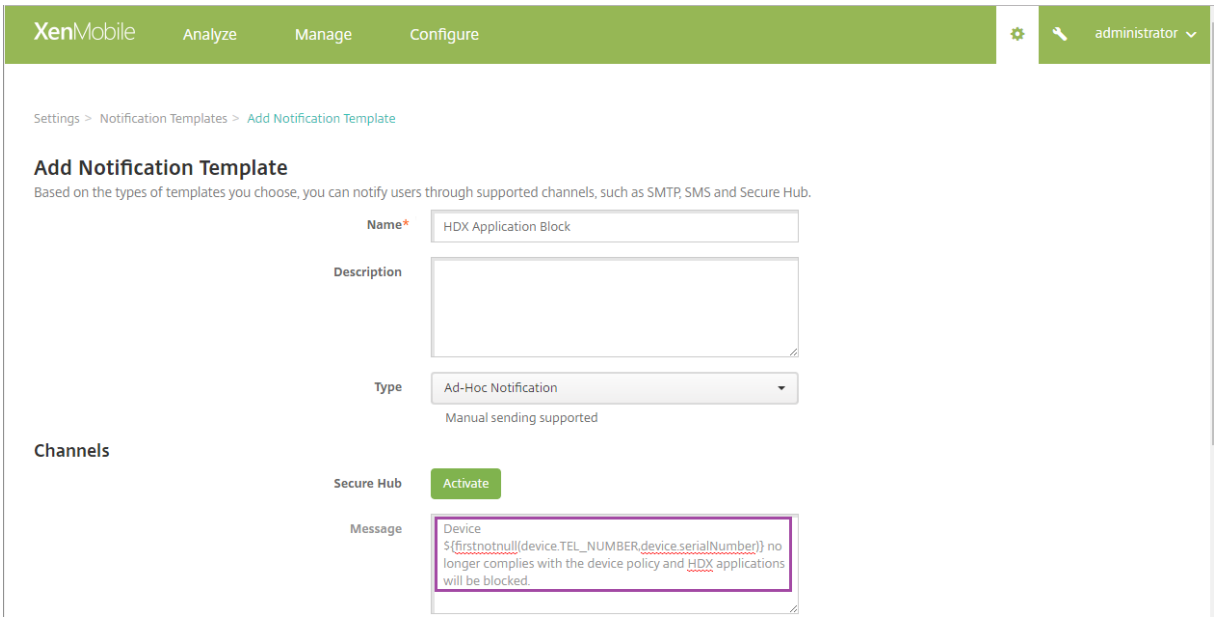
O exemplo a seguir mostra como usar macros para uma solicitação de assinatura de certificado. A macro para **Nome de entidade** é **`CN=$user.username`**. A macro para **Valor** de um **Nome de entidade alternativo** é **`$user.userprincipalname`**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 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 está mais em conformidade com a política de dispositivo, e os aplicativos HDX serão bloqueados.

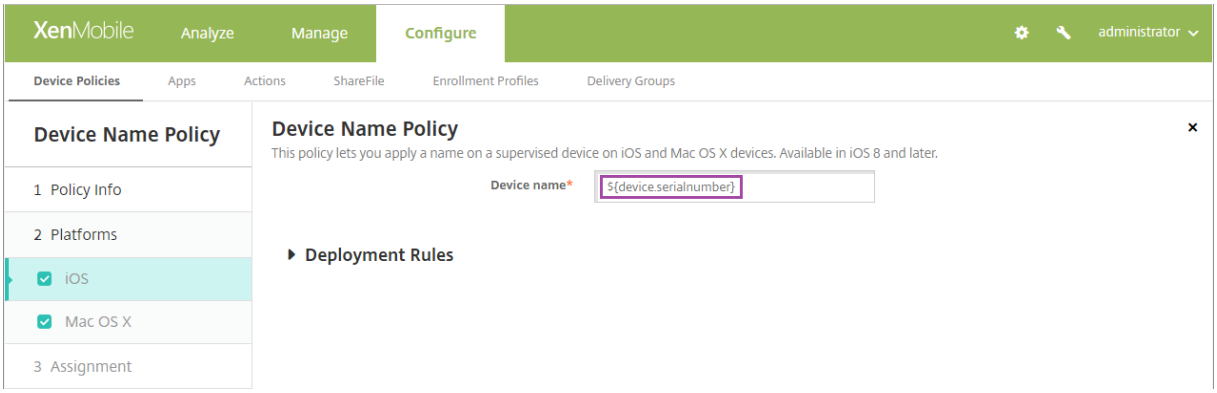


Para obter mais exemplos de macros utilizadas em notificações, vá para **Configurações > Modelos de notificação**, selecione um modelo predefinido e clique em **Editar**.

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 `${ device.serialnumber }` para definir o nome de dispositivo de acordo com o número de série de cada dispositivo. Use `${ device.`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

`serialnumber } ${ user.username }` para incluir o nome do usuário no nome do dispositivo. A política de dispositivo Nome do Dispositivo funciona em dispositivos supervisionados iOS e macOS.



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)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Macros para políticas específicas

Para a política de dispositivo de Nome do dispositivo (para iOS e macOS), você pode usar essas 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 dispositivos clip web, você pode usar esta macro para a**URL**:

- `${ webeas-url }`

Para a política de dispositivo de Chave de licença Samsung MDM, você pode usar essa macro para a **chave de licença ELM**:

- `${ elm.license.key }`

Macros para obter as propriedades internas de dispositivo

Nome de exibição	Macros
ID do dispositivo	`$device.id`
IMEI do dispositivo	`$device.imei`
Família de SO	`$device.OSFamily`
Número de série	`$device.serialNumber`

Macros para todas as propriedades de dispositivo

A lista a seguir fornece o nome de exibição, o elemento Web e as macros.

Conta suspensa?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

Código de desvio do bloqueio de ativação

- ACTIVATION_LOCK_BYPASS_CODE

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.ACTIVATION_LOCK_BYPASS_CODE

Bloqueio de ativação ativado

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

Conta do iTunes Active

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

Dispositivo ActiveSync conhecido por 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 do MDM Amazon disponível

- AMAZON_MDM
- ${device.AMAZON_MDM

ID de dispositivo do Android for Work

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

Dispositivo Android for Work ativado?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Android para o tipo de instalação de trabalho

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

Status de assinatura de antispyware

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

Status de antiSpyware

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

Status de assinatura de antivírus

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

Status do antivírus

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

Código de desvio de trava de ativação DEP ASM

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

Chave de caução DEP ASM

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

Marca do recurso

- ASSET_TAG
- ${device.ASSET_TAG

Verificar atualizações de software automaticamente

- AutoCheckEnabled
- ${device.AutoCheckEnabled

Baixar automaticamente as atualizações de software em segundo plano

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

Instalar automaticamente as atualizações de aplicativos

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

Instalar automaticamente as atualizações de SO

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Instalar automaticamente as atualizações de segurança

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

Status de 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 de firmware banda básica

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

Baregia carregando

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

Carregamento da bateria

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

Carga de bateria restante

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

Tempo de operação da bateria

- BATTERY_RUNTIME

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${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 DO BES

- BES_PIN
- ${device.BES_PIN

ID do BES servidor agente

- AGENT_ID
- ${device.AGENT_ID

Nome do servidor BES

- BES_SERVER
- ${device.BES_SERVER

Versão do servidor BES

- BES_VERSION
- ${device.BES_VERSION

Informações de 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 revisões do Gerenciador de inicialização

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

Código da operadora

- CARRIER_CODE
- ${device.CARRIER_CODE

Versão de configurações de operadora

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

URL do catálogo

- CatalogURL
- ${device.CatalogURL

Altitude do celular

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

Curso do celular

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

Precisão horizontal do celular

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

Latitude celular

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

Longitude da rede celular

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

Velocidade do celular

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

Tecnologia celular

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Timestamp celular

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

Precisão vertical do celular

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

Alterar a senha no próximo Login?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

ID de dispositivo de cliente

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

Backup de 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 revisões de integridade do código

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

Cor

- COR
- ${device.COLOR

Velocidade de CPU

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

Tipo de CPU

- CPU_TYPE
- ${device.CPU_TYPE}

Criação de regras

- GOOGLE_AW_DIRECTORY_CREATION_TIME

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${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 do país móvel atual

- CURRENT_MCC
- ${device.CURRENT_MCC

Código de rede móvel atual

- CURRENT_MNC
- ${device.CURRENT_MNC

Dados roaming permitido

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

Data do último backup 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 de DEP atribuído

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

Perfil de DEP enviado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

Perfil de DEP removido

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

Registo de DEP por

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

Data de registro de DEP

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

Descrição

- DESCRIÇÃO
- ${device.DESCRIPTION

Modelo do dispositivo

- SYSTEM_OEM
- ${device.SYSTEM_OEM

Nome do dispositivo

- NOME DO DISPOSITIVO
- ${device.DEVICE_NAME

Tipo de dispositivo

- DEVICE_TYPE
- ${device.DEVICE_TYPE

Você pode optar por 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 com criptografia

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de firewall

- DEVICE_FIREWALL_STATUS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.DEVICE_FIREWALL_STATUS

Status de firewall

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

Versão de firmware

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

Primeira sincronização

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Alias do diretório do Google

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Nome de família do Google diretório

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Nome do Google Directory

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Email principal do Google diretório

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

ID de usuário do Google diretório

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

Altitude GPS

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

Curso de GPS

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

Precisão horizontal do GPS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

Latitude de GPS

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

Longitude do GPS

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

Velocidade do GPS

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

Timestamp 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 de 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 do iTunes armazenar fez logon de conta

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

Rede da operadora inicial

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Código do país móvel local

- SIM_MCC
- ${device.SIM_MCC

Código de rede móvel local

- SIM_MNC
- ${device.SIM_MNC

Versão de API HTC

- HTC_MDM_VERSION
- ${device.HTC_MDM_VERSION

API MDM de HTC disponível

- HTC_MDM
- ${device.HTC_MDM

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 de IP

- IP_LOCATION
- ${device.IP_LOCATION

Endereço IPV4

- IP_ADDRESSV4

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.IP_ADDRESSV4

Endereço IPV6

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

Emitido em

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

Jailbroken/com raiz

- ROOT_ACCESS
- ${device.ROOT_ACCESS

Depuração de kernel ativada?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

Modo de quiosque

- IS_KIOSK
- ${device.IS_KIOSK

Último endereço IP conhecido

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

Última vez de atualização de política

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

Última data de busca

- PreviousScanDate
- ${device.PreviousScanDate

Último resultado da busca

- PreviousScanResult
- ${device.PreviousScanResult

Últimas atualizações de software programadas

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

Última mensagem de falha de atualizações de software agendadas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

Último status de 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 de 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 MDM perdido 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

NitroDesk TouchDown instalado

- TOUCHDOWN_FIND
- ${device.TOUCHDOWN_FIND

NitroDesk TouchDown licenciados por meio do MDM

- TOUCHDOWN_LICENSED_VIA_MDM
- ${device.TOUCHDOWN_LICENSED_VIA_MDM

Compilação do sistema operacional

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

Edição do sistema operacional

- OS_EDITION
- ${device.OS_EDITION

Idioma do sistema operacional (local)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

Versão do sistema operacional

- SYSTEM_OS_VERSION

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.SYSTEM_OS_VERSION

Endereço da organização

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

Email da organização

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

Magic 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

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

Código secreto em conformidade

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

Código secreto em conformidade com a configuração

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

Código secreto presente

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT

PCR0

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

Violação do 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 de plataforma API

- API_LEVEL
- ${device.API_LEVEL

Nome da política

- POLICY_NAME
- ${device.POLICY_NAME

Número de telefone principal

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

Operadora de prestadora de SIM primário

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

ICCID de SIM principal

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Principal IMEI SIM

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

IMSI de SIM principal

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

SIM principal em Roaming

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

Conformidade com roaming de SIM primário

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

Nome do produto

- PRODUCT_NAME
- ${device.PRODUCT_NAME

ID de dispositivo de fornecedor

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

Redefinir contagem

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

Reiniciar contagem

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

Modo de segurança ativado?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

API do Samsung KNOX disponível

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Versão de API do Samsung KNOX

- SAMSUNG_KNOX_VERSION

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.SAMSUNG_KNOX_VERSION

Atestado do Samsung KNOX

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Data de atualização do atestado do 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 do 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 de eixo x

- SCREEN_XDPI
- ${device.SCREEN_XDPI

Tela: Resolução do eixo Y

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- SCREEN_YDPI
- ${device.SCREEN_YDPI

Número de telefone secundário

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

Operadora de prestadora de SIM secundário

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

ICCID de SIM secundário

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

Secundário IMEI SIM

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

IMSI de SIM secundário

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

SIM secundário Roaming

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

Conformidade com roaming de SIM secundário

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

Inicialização segura ativada?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

Status de inicialização segura

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

SecureContainer ativado

- DLP_ACTIVE
- ${device.DLP_ACTIVE

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nível de patch de segurança

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

Número de série

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

Com capacidade de SMS

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

API de Enterprise Sony disponível

- SONY_MDM
- ${device.SONY_MDM

Versão da API de Enterprise Sony

- SONY_MDM_VERSION
- ${device.SONY_MDM_VERSION

Supervisionado

- SUPERVISED
- ${device.SUPERVISED

Motivo da suspensão

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

Status alterado

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

Termos e Condições

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

Termos e contrato aceitos?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

Sinalização de teste ativada?

- WINDOWS_HAS_TEST_SIGNING_ENABLED

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

Total de RAM

- MEMORY
- ${device.MEMORY

Espaço de armazenamento total

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

Versão de TPM

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

Status de controle de conta do usuário

- UAC_STATUS
- ${device.UAC_STATUS

Agente de usuário

- USER_AGENT
- ${device.USER_AGENT

Definida pelo usuário #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

Definida pelo usuário #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

Definida pelo usuário #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

Idioma do usuário (local)

- USER_LANGUAGE
- ${device.USER_LANGUAGE

Fornecedor

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- VENDOR
- ${device.VENDOR

Com capacidade 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 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 de agente do XenMobile

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Revisão de agente do XenMobile

- EW_REVISION
- ${device.EW_REVISION

Versão do agente XenMobile

- EW_VERSION
- ${device.EW_VERSION

Zebra API disponível

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Versão do MXMF Zebra

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Versão do patch Zebra

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Macros para obter as propriedades internas de usuário

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 da Web	Macros
Tentativas de login do Active Directory com falha	badpwdcount	`${ user.badpwdcount }`
Email de usuário do ActiveSync	asuseremail	`${ user.asuseremail }`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome de exibição	Elemento da Web	Macros
Origem de dados ASM	asmpersonsource	${ user.asmpersonsource }
Nome de conta DEP ASM	asmdepaccount	${ user.asmdepaccount }
ID gerenciada da Apple ASM	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
Tipo de código de acesso ASM	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ID pessoal ASM	asmpersonid	${ user.asmpersonid }
Status pessoal ASM	asmpersonstatus	${ user.asmpersonstatus }
Título pessoal ASM	asmpersontitle	${ user.asmpersontitle }
ID exclusivo pessoal ASM	asmpersonuniqueid	${ user.asmpersonuniqueid }
ID de sistema de origem ASM	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
Nível escolar de status ASM	asmpersongrade	${ user.asmpersongrade }
Email de usuário de BES	besuseremail	${ user.besuseremail }
Empresa	company	${ user.company }
Nome da empresa	companyname	${ user.companyname }
País	c	${ user.c }
Departamento	department	${ user.department }
Descrição	description	${ user.description }
Usuário desativado	disableduser	${ user.disableduser }
Nome de exibição	displayname	${ user.displayname }

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome de exibição	Elemento da Web	Macros
Nome distinto	distinguishedname	`${ user.distinguishedname }`
Nome de domínio	domainname	`${ user.domainname }`
E-mail	mail	`${ user.mail }`
Nome	givenname	`${ user.givenname }`
Endereço (residencial)	homestreetaddress	`${ user.homestreetaddress }`
Cidade (residencial)	homecity	`${ user.homecity }`
País (residencial)	homecountry	`${ user.homecountry }`
Fax (residencial)	homefax	`${ user.homefax }`
Telefone (residencial)	homephone	`${ user.homephone }`
Estado/região (residencial)	homestate	`${ user.homestate }`
CEP (residencial)	homezip	`${ user.homezip }`
Telefone IP	ipphone	`${ user.ipphone }`
Inicial do meio	middleinitial	`${ user.middleinitial }`
Segundo nome	middlename	`${ user.middlename }`
Celular	mobile	`${ user.mobile }`
Nome	cn	`${ user.cn }`
Endereço (comercial)	physicaldeliveryofficename	`${ user.physicaldeliveryofficename }`
Cidade (comercial)	l	`${ user.l }`
Número de fax (comercial)	facsimiletelephonenumber	`${ user.facsimiletelephonenumber }`
Estado/província (comercial)	st	`${ user.st }`
Endereço (comercial)	officestreetaddress	`${ user.officestreetaddress }`
Número de telefone (comercial)	telephonenumber	`${ user.telephonenumber }`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome de exibição	Elemento da Web	Macros
Código postal (comercial)	postalcode	`${ user.postalcode }`
Caixa postal	postofficebox	`${ user.postofficebox }`
Pager	pager	`${ user.pager }`
ID de grupo primário	primarygroupid	`${ user.primarygroupid }`
Conta SAM	samaccountname	`${ user.samaccountname }`
Endereço	streetaddress	`${ user.streetaddress }`
Sobrenome	sn	`${ user.sn }`
Título	title	`${ user.title }`
Nome de login do usuário	userprincipalname	`${ user.userprincipalname }`

Ações automatizadas

April 15, 2019

Você pode criar ações automatizadas no XenMobile para programar uma reação aos eventos, às propriedades do usuário ou dispositivo ou à existência de aplicativos em dispositivos de usuário. Quando você cria uma ação automatizada, os gatilhos definidos para a ação determinam o que acontece no dispositivo do usuário quando ele é conectado ao XenMobile. Quando um evento é disparado, você pode enviar uma notificação para o usuário corrigir um problema, antes que medidas mais sérias sejam necessárias.

Por exemplo, suponha que você deseja detectar um aplicativo que colocou anteriormente na lista negra (por exemplo, “Words with Friends”). Você pode especificar um disparador que define o dispositivo do usuário como fora de conformidade quando “Words with Friends” é detectado no dispositivo. A ação os notifica que eles devem remover o aplicativo para que o dispositivo esteja novamente em conformidade. Você também pode definir um limite de tempo para aguardar a conformidade dos usuários. Após esse limite de tempo, ocorre uma ação definida, como o apagamento seletivo do dispositivo.

Em casos em que o dispositivo do usuário é colocado em um estado de não conformidade e logo o usuário corrige o dispositivo, você deve configurar uma política para implantar um pacote que reinicia o dispositivo em um estado de conformidade.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Os efeitos que você define para acontecer automaticamente variam entre os seguintes:

- Limpar o dispositivo de forma total ou seletiva.
- Definir o dispositivo como fora de conformidade.
- Revogar o dispositivo.
- Enviar uma notificação para o usuário corrigir um problema, antes que medidas mais sérias sejam necessárias.

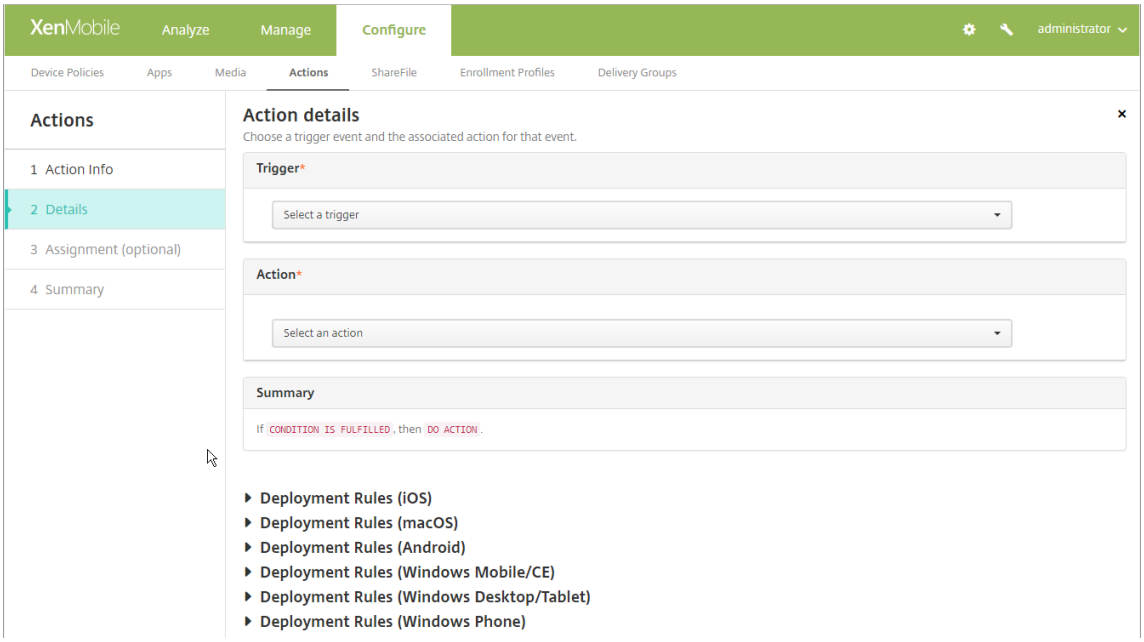
Este artigo explica como adicionar, editar e filtrar ações automatizadas e como configurar as ações de bloqueio de aplicativo e apagamento de aplicativo para o modo somente MAM

> Nota:
>
> Antes de poder notificar os usuários, você deve configurar os servidores de notificação nas configurações do XenMobile como SMTP e SMS para que o XenMobile possa enviar as mensagens. Para obter informações, consulte Notificações. Além disso, configure todos os modelos de notificação que planeja usar antes de prosseguir. Para obter detalhes, consulte Criar e atualizar modelos de notificação.

1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Na página **Ações**, siga um destes procedimentos:
   - Clique em **Adicionar** para adicionar uma ação.
   - Selecione uma ação existente para editar ou excluir. Clique na opção desejada.
3. A página **Informações sobre a ação** é exibida.
4. Na página **Informações sobre a ação**, insira ou modifique as seguintes informações:
   - **Nome:** digite um nome para identificar a ação. Este campo é obrigatório.
   - **Descrição:** descreva a finalidade da ação.
5. Clique em **Avançar**. A página **Detalhes da ação** é exibida.

   O exemplo a seguir mostra como definir um gatilho de **Evento**. Se você selecionar um gatilho diferente, as opções resultantes serão diferentes daquelas mostradas aqui.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 de dispositivo:** verifica se há um atributo no dispositivo obtido no modo do MDM e reage a ele. Para obter mais informações, consulte Nomes de propriedade do dispositivo e os valores.
   - **Propriedade do usuário:** reage a um atributo de usuário, geralmente do Active Directory.
   - **Nome do aplicativo instalado:** reage a um aplicativo que está sendo instalado. Não se aplica ao modo somente MAM. Requer que a política de inventário de aplicativos esteja ativada no dispositivo. A política de inventário de aplicativos está ativada em todas as plataformas por padrão. Para obter detalhes, consulte Política de dispositivo de inventário de aplicativos.

7. Na próxima lista, clique na resposta para o gatilho.

8. Na lista **Ação**, clique na ação a ser executada quando o critério de gatilho é atendido. Com exceção da opção **Enviar notificação**, você escolhe um período durante o qual os usuários podem resolver o problema que causou o gatilho. Se o problema não for resolvido nesse período, a ação selecionada será tomada. Para obter uma definição das ações, consulte Ações de segurança.

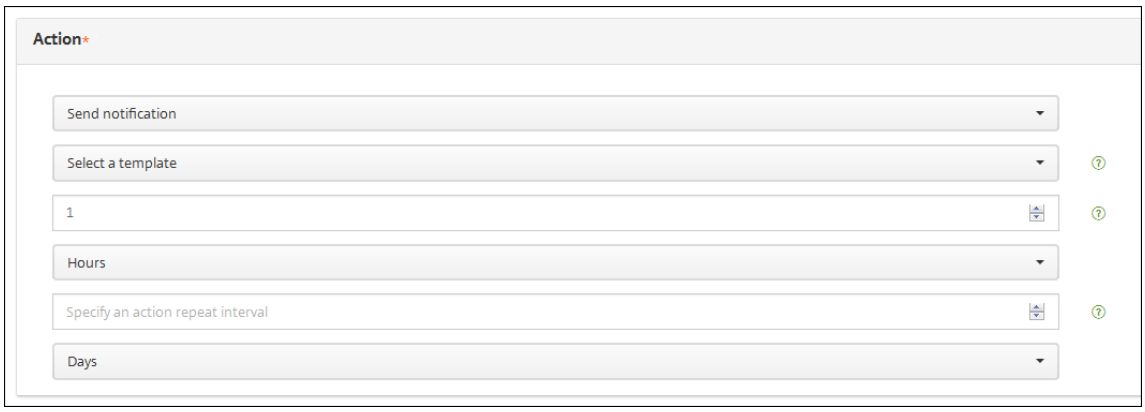
   Se você selecionar **Enviar notificação**, use as etapas a seguir para enviar uma ação de notificação.

9. Na próxima lista, selecione o modelo a ser usado para a notificação. São exibidos modelos de

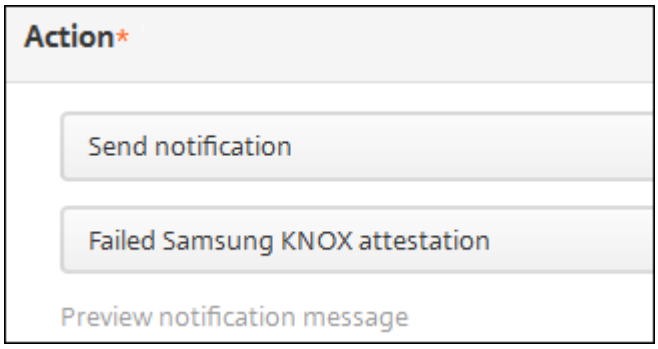
© 1999-2019 Citrix Systems, Inc. All rights reserved.

notificação relevantes para o evento selecionado, a menos que ainda não exista um modelo para o tipo de notificação. Nesse caso, você receberá um aviso para configurar um modelo com a mensagem: Nenhum modelo para este tipo de evento. Crie o modelo usando **Modelo de Notificação** em **Configurações**.

Antes de poder notificar os usuários, você deve configurar os servidores de notificação em Configurações para SMTP e SMS para que o XenMobile possa enviar as mensagens, consulte Notificações. Além disso, configure todos os modelos de notificação que planeja usar antes de prosseguir. Para obter detalhes sobre a configuração de modelos de notificação, consulte Criar e atualizar modelos de notificação.



Depois de selecionar o modelo, você poderá 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 durante o qual a ação se repete até que o usuário resolva o problema de gatilho.



11. Em **Resumo**, verifique se você criou a ação automatizada como desejado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



12. Depois de configurar os detalhes da ação, você pode configurar as regras de implantação de cada plataforma individualmente. Para fazer isso, conclua a etapa 13 para cada plataforma desejada.
13. Configure as regras de implantação Para obter informações gerais sobre como configurar as regras de implantação, incluindo ilustrações, consulte Implantar recursos.

    Para este exemplo:

    - A propriedade do dispositivo deve ser **BYOD**.
    - A criptografia local do dispositivo deve ser **True**.
    - O dispositivo deve ser compatível com código secreto.
    - O MCC do dispositivo não pode ser apenas Andorra.
14. Quando você terminar de definir as regras de implantação para a ação de plataforma, clique em **Avançar**. A página de **Atribuição de ações** é exibida, onde você pode atribuir a ação a um grupo ou grupos de entrega. Essa etapa é opcional.
15. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione grupos na lista. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.
16. Expanda Cronograma de implantação e defina estas configurações:

    - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**. Se você escolher **OFF**, nenhuma outra opção será necessária.
    - Ao lado de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
    - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
    - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
    - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

      Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, 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 Bloqueio de aplicativo e Apagamento de aplicativos do modo somente MAM

Você pode apagar ou bloquear aplicativos em um dispositivo em resposta a todas as quatro categorias de gatilhos listadas no console XenMobile: evento, propriedade de dispositivo, propriedade do usuário e o nome do aplicativo instalado.

Para configurar o apagamento ou bloqueio de aplicativos automático

1. No console XenMobile, clique em **Configurar > Ações**.
2. Na página **Ações**, clique em **Adicionar**.
3. Na página **Informações sobre a ação**, insira um nome para a ação e uma descrição opcional.
4. Na página **Detalhes da Ação**, selecione o gatilho que você desejar.
5. Em **Ação**, selecione uma ação.

   Para essa etapa, lembre-se as condições a seguir:

   Quando o tipo de gatilho é **Evento** e o valor não é de **usuário desativado do Active Directory**, as ações de **Apagamento de aplicativo** e **Bloqueio de aplicativo** não são exibidas.

   Quando o tipo de gatilho for **Propriedade do dispositivo** e o valor for **Modo MDM Perdido ativado**, não serão exibidas as seguintes ações:

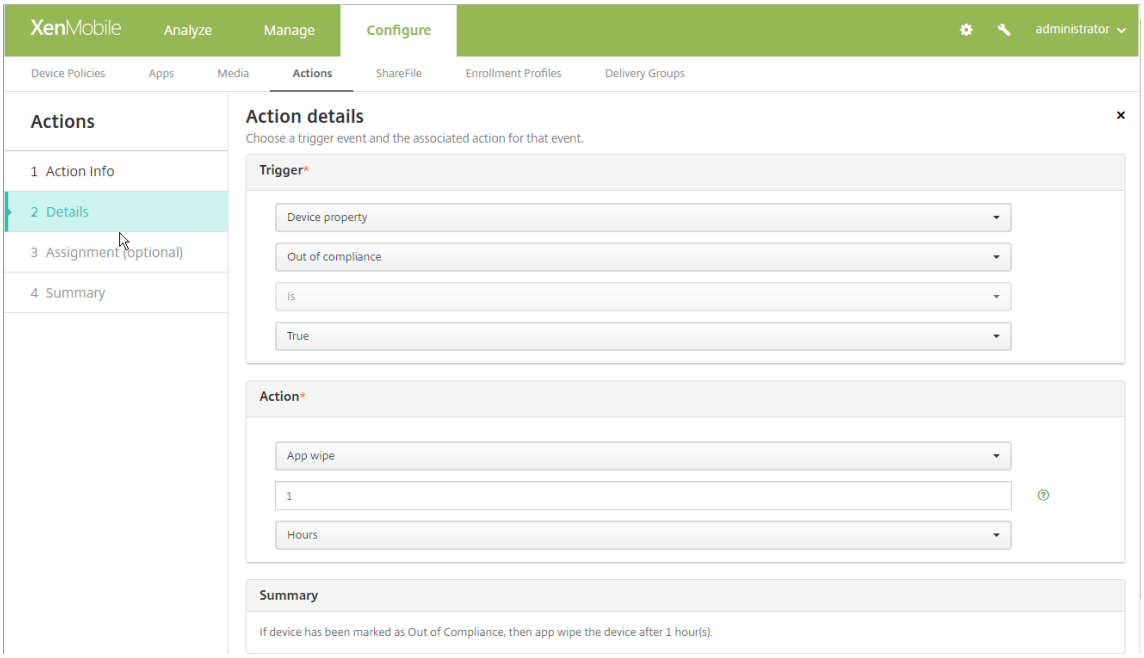
   - Apagar seletivamente o dispositivo
   - Apagar completamente o dispositivo
   - Revogar o dispositivo

   Para cada opção, um atraso de uma hora é definido automaticamente, mas você pode selecionar o período de atraso em minutos, horas ou dias. A intenção do atraso é dar aos usuários tempo para corrigir um problema antes que a ação ocorra. Para obter mais informações sobre as ações de apagamento de aplicativos e bloqueio de aplicativos, consulte Ações de segurança.

   > Nota:
   >
   > Se você definir o gatilho como **evento**, o intervalo de repetir automaticamente é um mín-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> imo de 1 hora. O dispositivo deve executar uma atualização de políticas para sincronizar com o servidor de notificação para entrar. Normalmente, um dispositivo sincroniza com o servidor quando os usuários fazem logon no ou atualizam manualmente suas políticas através do Secure Hub.
>
> Um atraso extra de aproximadamente uma hora pode ocorrer antes que qualquer ação seja realizada para permitir que o banco de dados do Active Directory seja sincronizado com o XenMobile.

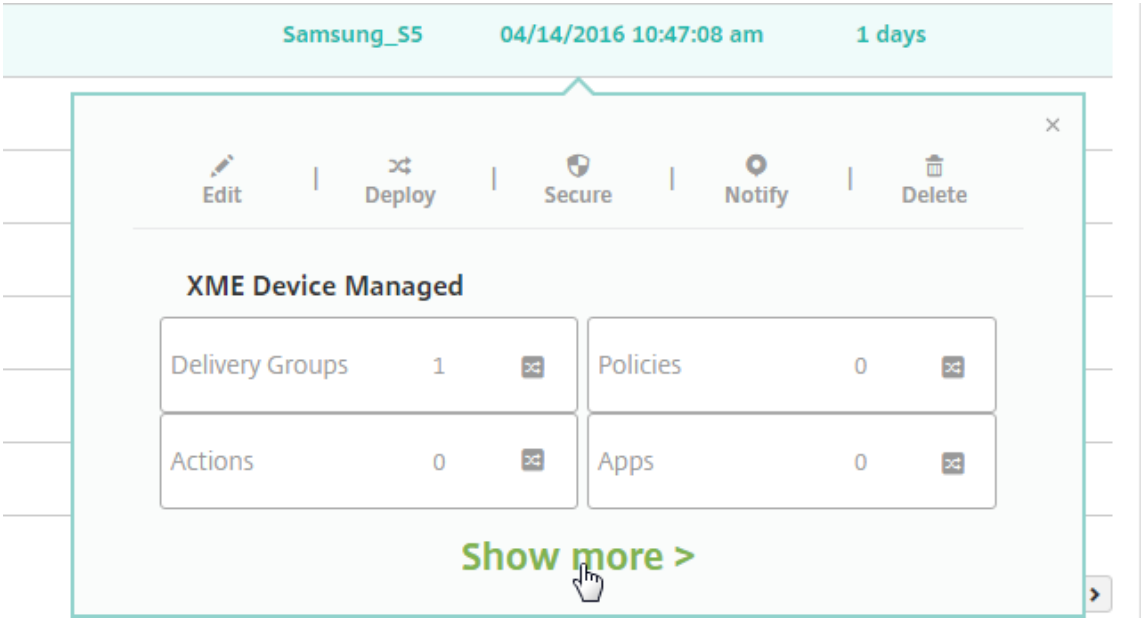


6. Configure as regras de implantação e clique em **Avançar**.
7. Configure as atribuições do grupo de entrega e um cronograma de implantação, e clique em **Avançar**.
8. Clique em **Salvar**.

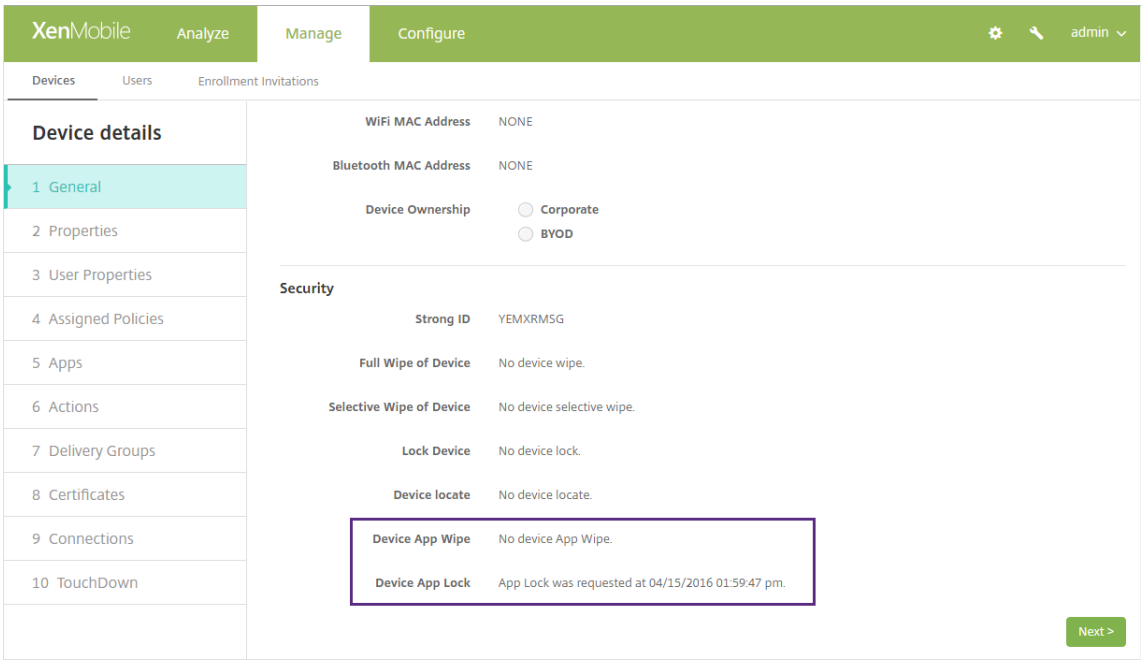
Para verificar o status do apagamento de aplicativos ou do bloqueio de aplicativo

1. Acesse **Gerenciar > Dispositivos**, clique em um dispositivo e clique em **Mostrar mais**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

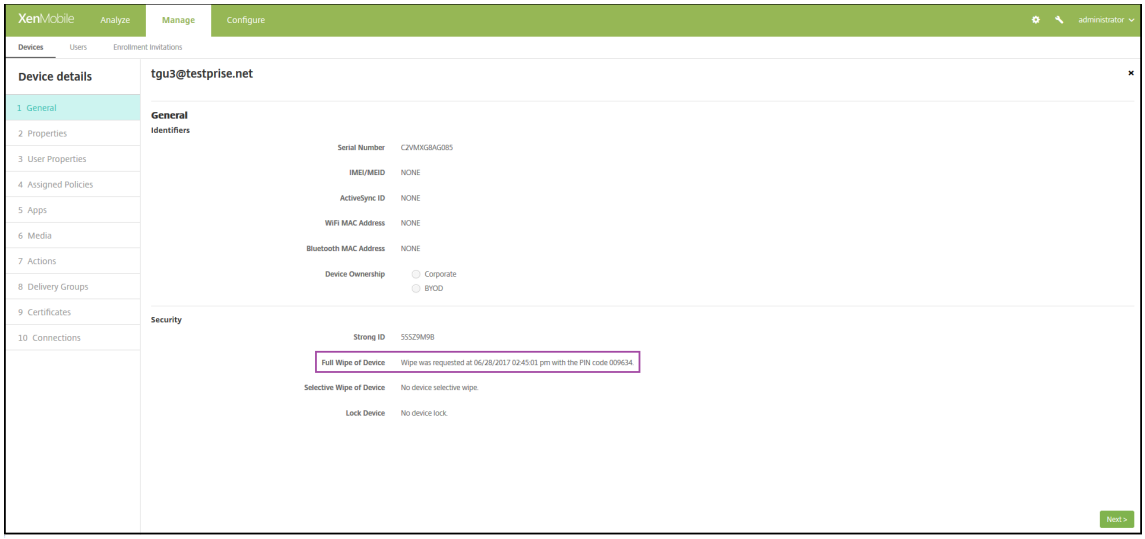


2. Role até **Apagamento de aplicativo do dispositivo** e **Bloqueio de aplicativo do dispositivo**.



Depois que um dispositivo for apagado, o usuário será solicitado a inserir um código PIN. Se o usuário esquecer o código, você pode procurá-lo nos Detalhes do dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Monitoração e suporte

April 15, 2019

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 Suporte do XenMobile para acessar informações e ferramentas relacionadas a suporte.

Para um XenMobile Server no 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 XenMobile, clique no ícone de chave inglesa no canto superior direito.



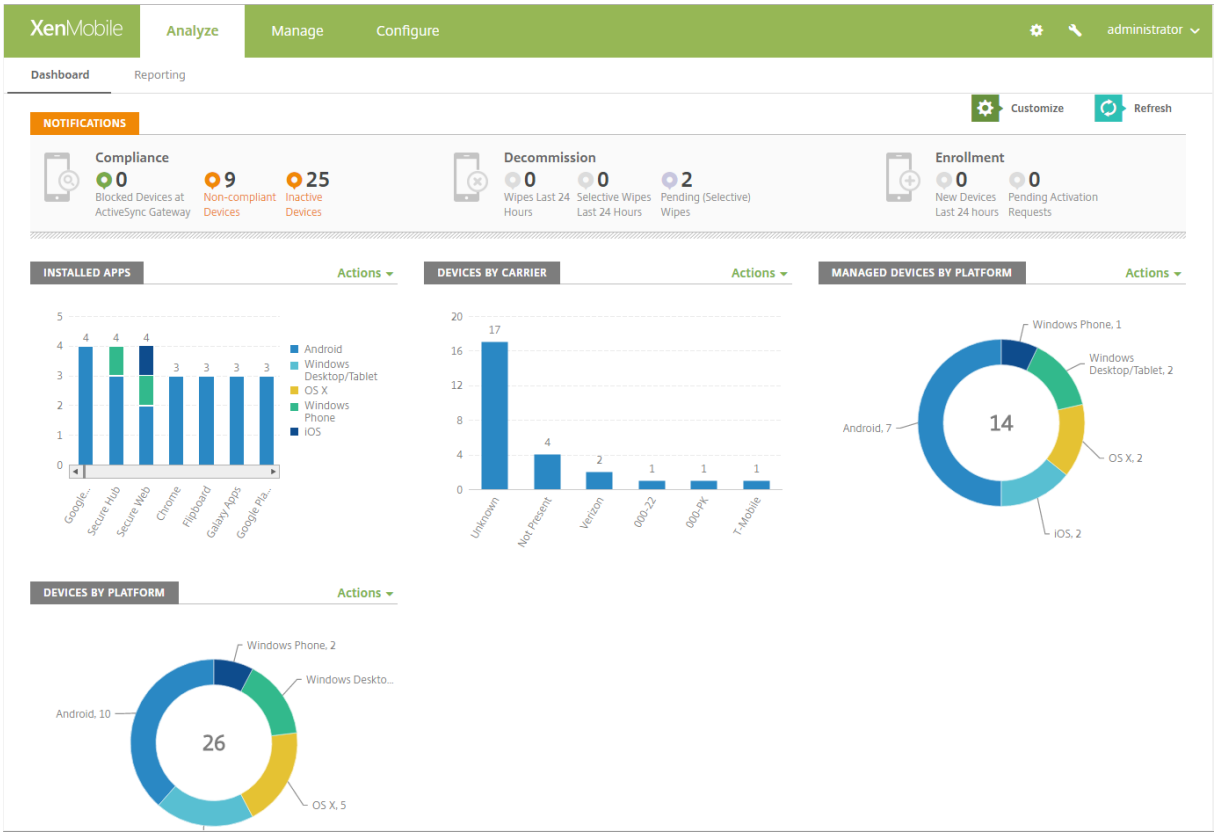
A página Solução de problemas e Suporte é exibida.

Use a página de **Suporte** do XenMobile para:

- Acessar diagnósticos.
- Criar pacotes de suporte (somente para instalações no local).
- Acessar links para a Documentação de produtos Citrix e o Knowledge Center.
- Acessar operações de log.
- Usar as opções de configuração avançada.
- Acessar um conjunto de ferramentas e utilitários.

Você também pode ver informações de resumo acessando o painel do console XenMobile. Com essas informações, você pode ver problemas e operações bem-sucedidas rapidamente usando widgets.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



O painel é geralmente a tela que aparece quando você faz logon no console 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 editar os widgets exibidos.

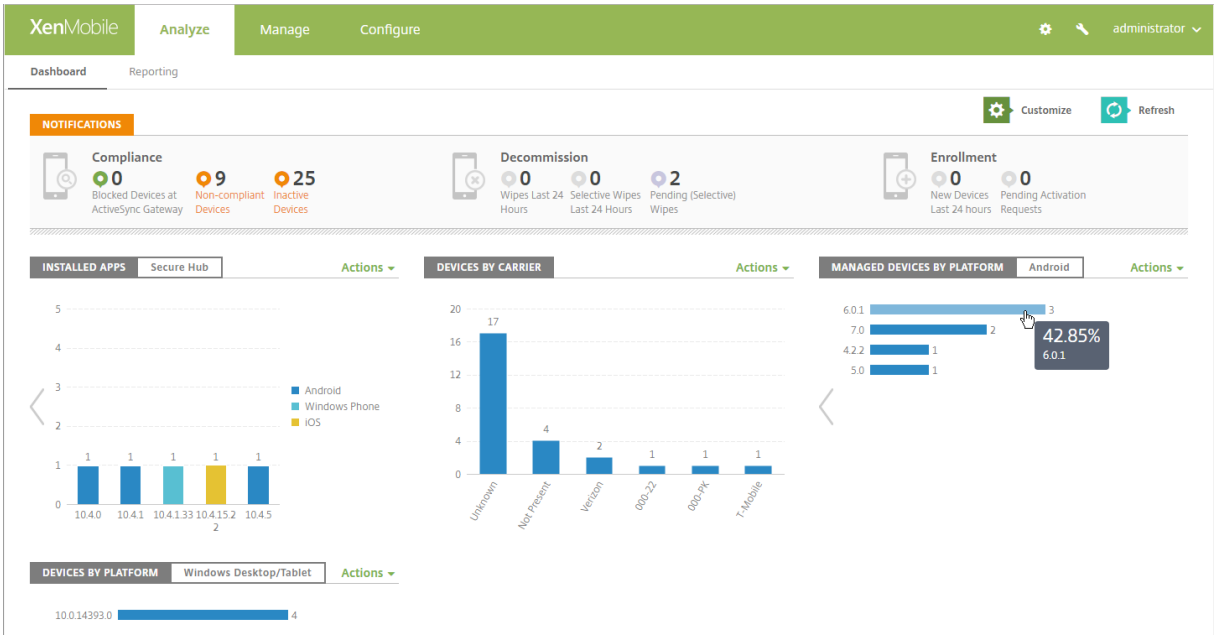
- **Meus painéis:** você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e exibir cada um selecionando o painel salvo.
- **Estilo de layout:** nessa linha você pode selecionar quantos widgets são exibidos no painel e a sua disposição.
- **Seleção de widgets:** você pode escolher as informações que aparecem no 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 não gerenciados e gerenciados por operadora. Clique em cada barra para ver um demonstrativo 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

gerenciados por plataforma. Os dispositivos exibidos nesse gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.

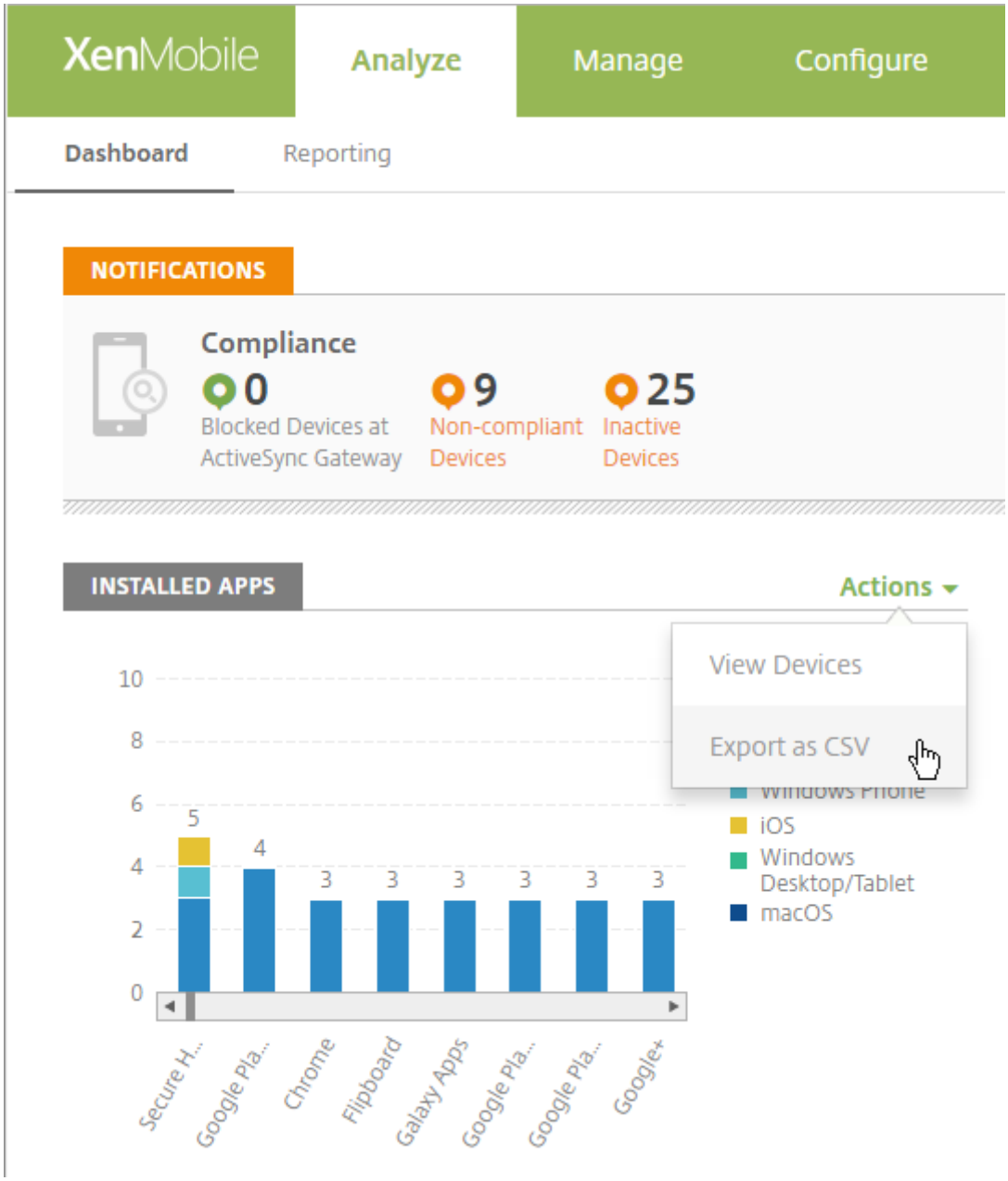
- **Dispositivos por Status do Gateway do ActiveSync:** exibe o número de dispositivos agrupados por status do ActiveSync Gateway. As informações mostram o status Desconhecido, Permitido ou Bloqueado. Você pode clicar em cada barra exibir os dados por plataforma.
- **Dispositivos por propriedade:** exibe o número de dispositivos agrupados por status de propriedade. As informações de mostram o status de propriedade de propriedade da empresa, propriedade do funcionário ou desconhecido.
- **Status de licença do android TouchDown:** exibe o número de dispositivos que têm uma licença do TouchDown.
- **Implantações de grupo de entrega com falha:** exibe o número total de falhas de implantação por pacote. Apenas os pacotes que têm falhas de implementação.
- **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 de aplicativos.
- **Uso de licenças de aplicativos de VPP:** exibe as estatísticas de uso para aplicativos do Apple Volume Purchase Program.

Em cada widget você pode clicar nas partes para analisar mais a fundo para obter mais informações.



Você também pode exportar as informações como um arquivo. csv clicando na lista suspensa **Ação**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



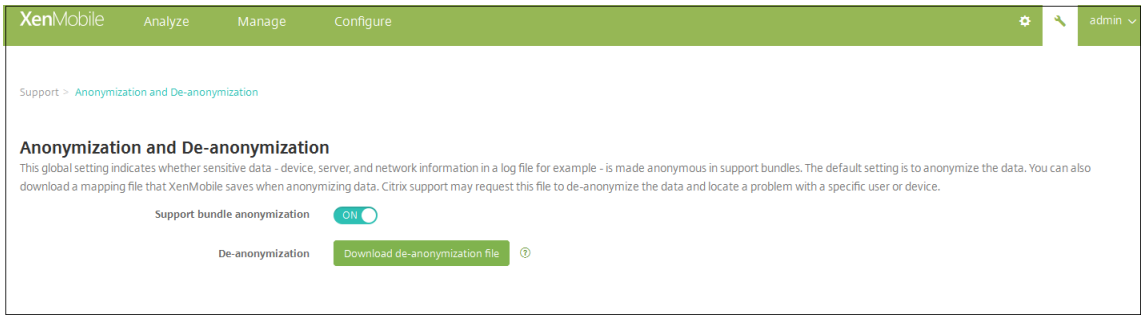
Anonimizar dados nos pacotes de suporte

August 24, 2018

Quando você cria pacotes de suporte no XenMobile, dados confidenciais do usuário, do servidor e da 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 quando anonimiza dados. O suporte da Citrix pode solicitar esse arquivo para desanonimizar os dados e localizar um problema com um usuário ou um dispositivo específico.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. No console 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 serão anonimizados. O padrão é **I**.
4. Ao lado de **Desanonimização**, clique em **Baixar o arquivo de desanonimização** para baixar o arquivo de mapeamento a ser enviado para o suporte Citrix quando eles precisarem de informações específicas do dispositivo ou do usuário para diagnosticar um problema.

Verificações de conectividade

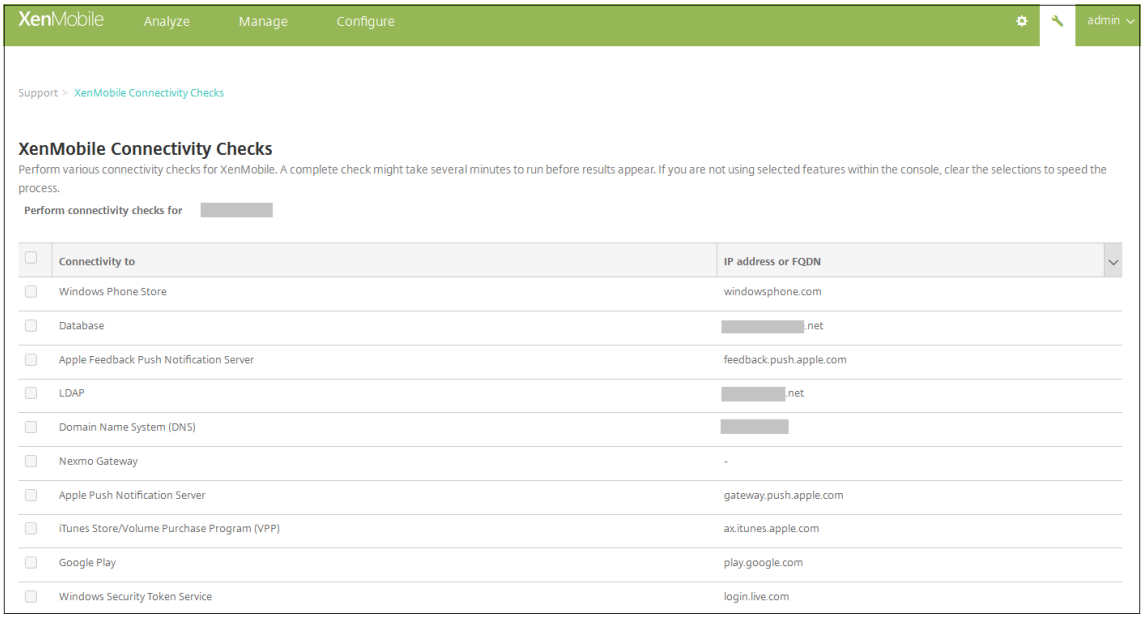
March 6, 2019

Na página **Suporte** do XenMobile, você pode verificar a conexão do XenMobile com o NetScaler Gateway e outros servidores e localizações.

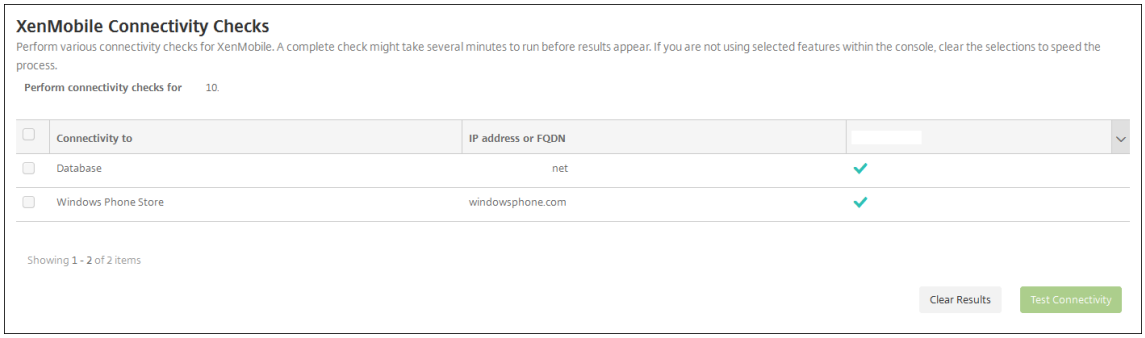
Conduzindo verificações de conectividade XenMobile

1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é exibida.
2. Em **Diagnósticos**, clique em **Verificações de Conectividade XenMobile**. A página **Verificações de conectividade XenMobile** é exibida. Se o seu ambiente do XenMobile contiver nós de cluster, todos os nós serão mostrados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

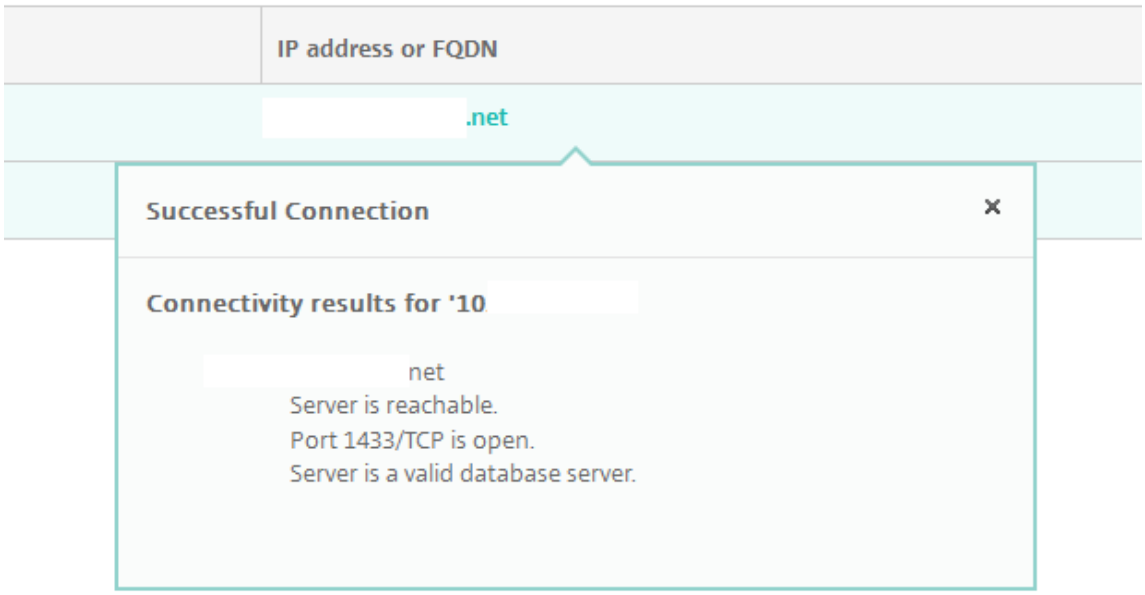


3. Selecione os servidores que você desejar incluir no teste de conectividade e clique em **Testar conectividade**. A página de resultados de teste é exibida.



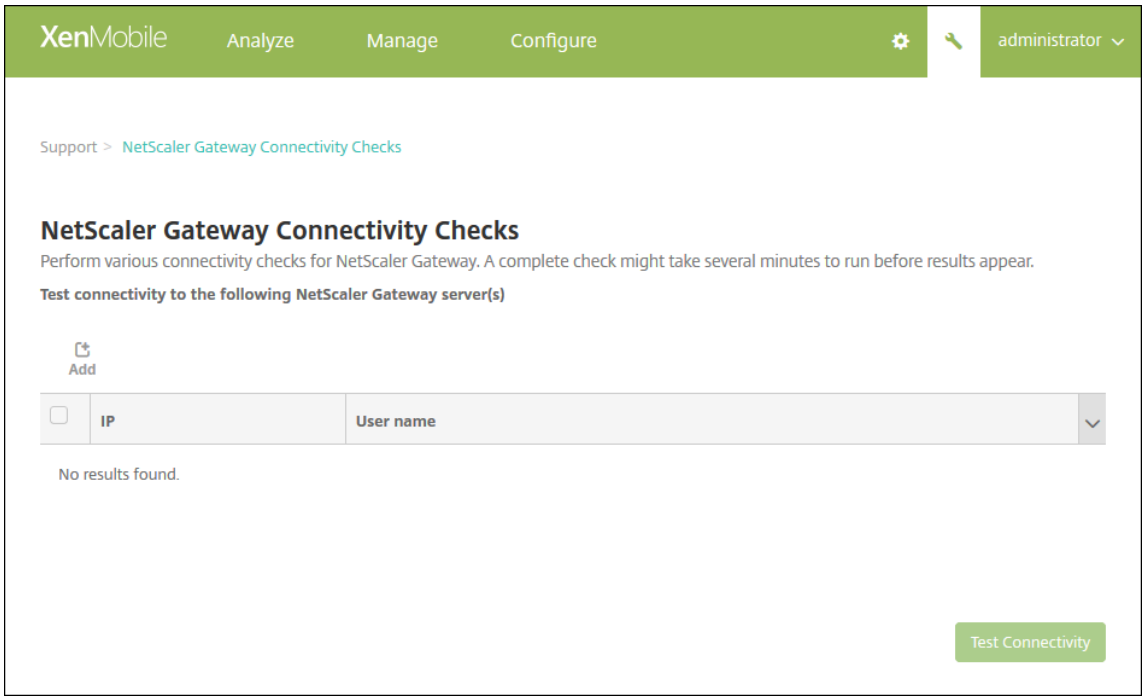
4. Selecione um servidor na tabela dos resultados do teste para ver os resultados detalhados desse servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



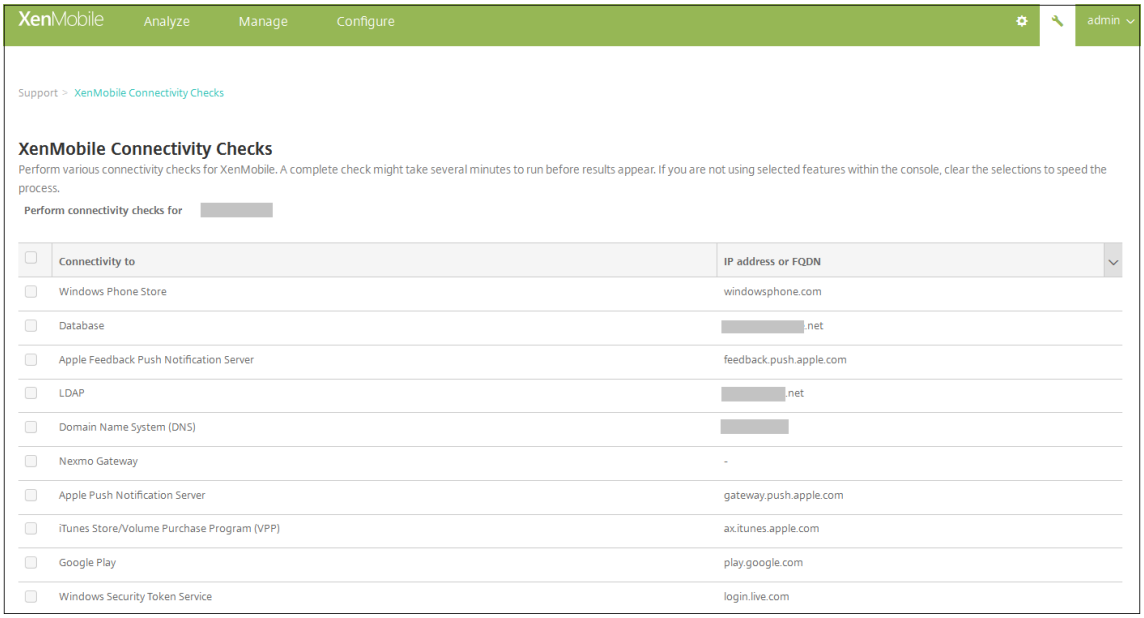
Conduzindo verificações de conectividade do NetScaler Gateway

1. Na página **Suporte**, em **Diagnósticos**, clique em **Verificações de conectividade do NetScaler Gateway**. A página **Verificações de conectividade do NetScaler Gateway** é exibida. A tabela estará vazia se você ainda não tiver adicionado nenhum servidor do NetScaler Gateway.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar servidor do NetScaler Gateway** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Em **IP de gerenciamento do NetScaler Gateway**, digite o endereço IP do servidor que executa o NetScaler Gateway que você deseja testar.

   > Nota:
   >
   > Se você estiver conduzindo uma verificação de conectividade para um servidor do NetScaler Gateway que já foi adicionado antes, o endereço IP será fornecido.

4. Digite as suas credenciais de administrador para esse NetScaler Gateway.

   > Nota:
   >
   > Se você estiver conduzindo uma verificação de conectividade para um servidor do NetScaler Gateway que já foi adicionado antes, o nome do usuário será fornecido.

5. Clique em **Adicionar**. O NetScaler Gateway é adicionado à tabela na página **Verificações de conectividade do NetScaler Gateway**.
6. Selecione o servidor do NetScaler Gateway e, em seguida, clique em **Testar conectividade**. Os resultados são exibidos em uma tabela de resultados de teste.
7. Selecione um servidor na tabela dos resultados do teste para ver os resultados detalhados desse servidor.

Programa de Melhoria de Experiência do Cliente

October 4, 2018

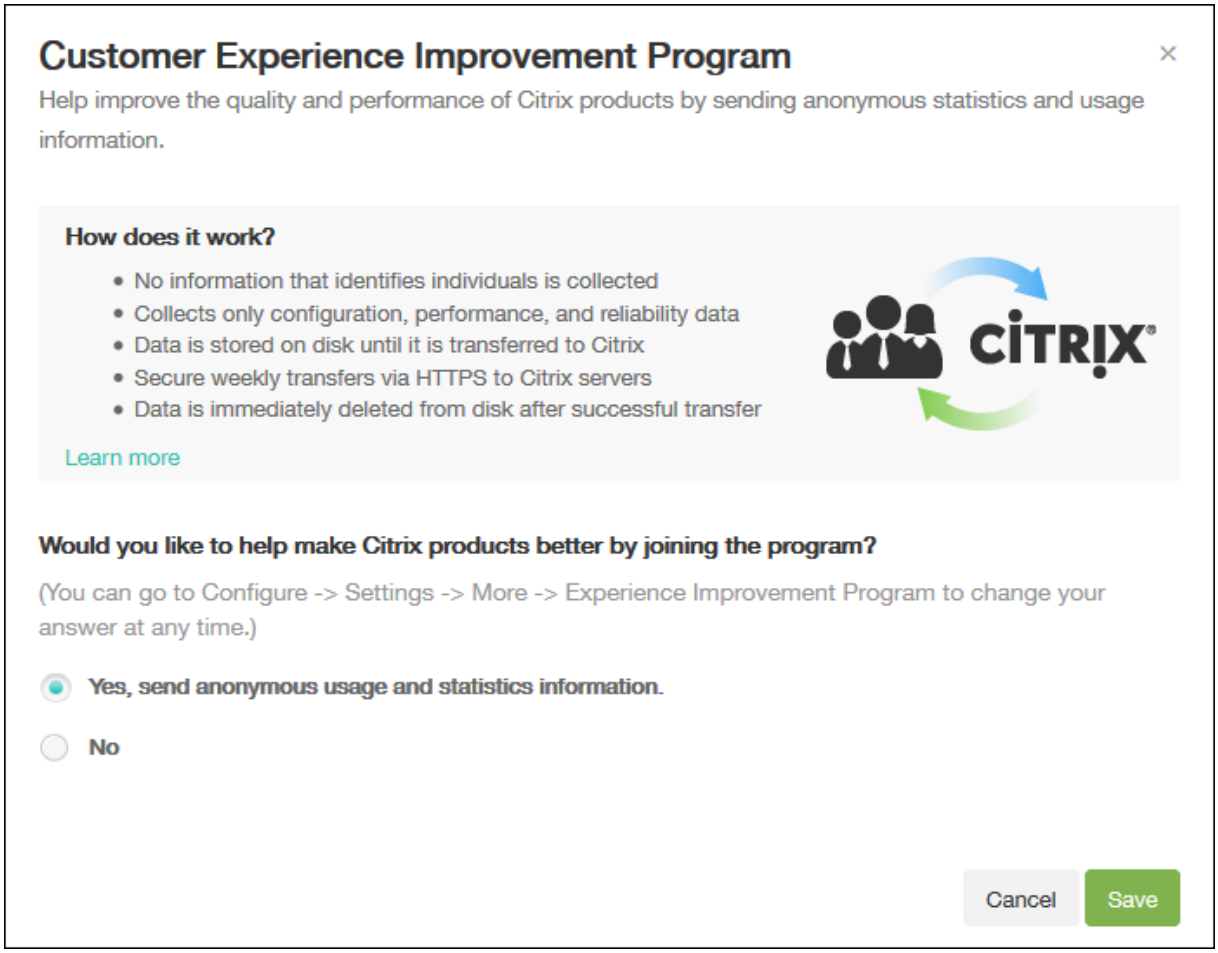
O Programa de Melhoria de Experiência do Cliente (CEIP) da Citrix reúne dados anônimos de configuração e uso do XenMobile e envia-os automaticamente para a Citrix. Esses dados ajudam a Citrix a

© 1999-2019 Citrix Systems, Inc. All rights reserved.

melhorar a qualidade, a confiabilidade e o desempenho do XenMobile. A participação no CEIP é completamente voluntária. Quando você instala o XenMobile ou uma atualização, tem a opção de participar do CEIP. Quando você opta por participar, os dados são geralmente coletados em uma base semanal, e os dados de desempenho e uso são coletados a cada hora. Os dados são armazenados em disco e transferidos com segurança usando HTTPS para a Citrix semanalmente. Você pode alterar se deseja participar do CEIP no console XenMobile. Para obter mais informações sobre o CEIP, consulte Sobre o programa de melhoria de experiência do cliente (CEIP) da Citrix.

Como optar para participar do CEIP

Na primeira vez que instalar o XenMobile ou quando fizer uma atualização, você verá a caixa de diálogo a seguir, que pergunta se você deseja participar.

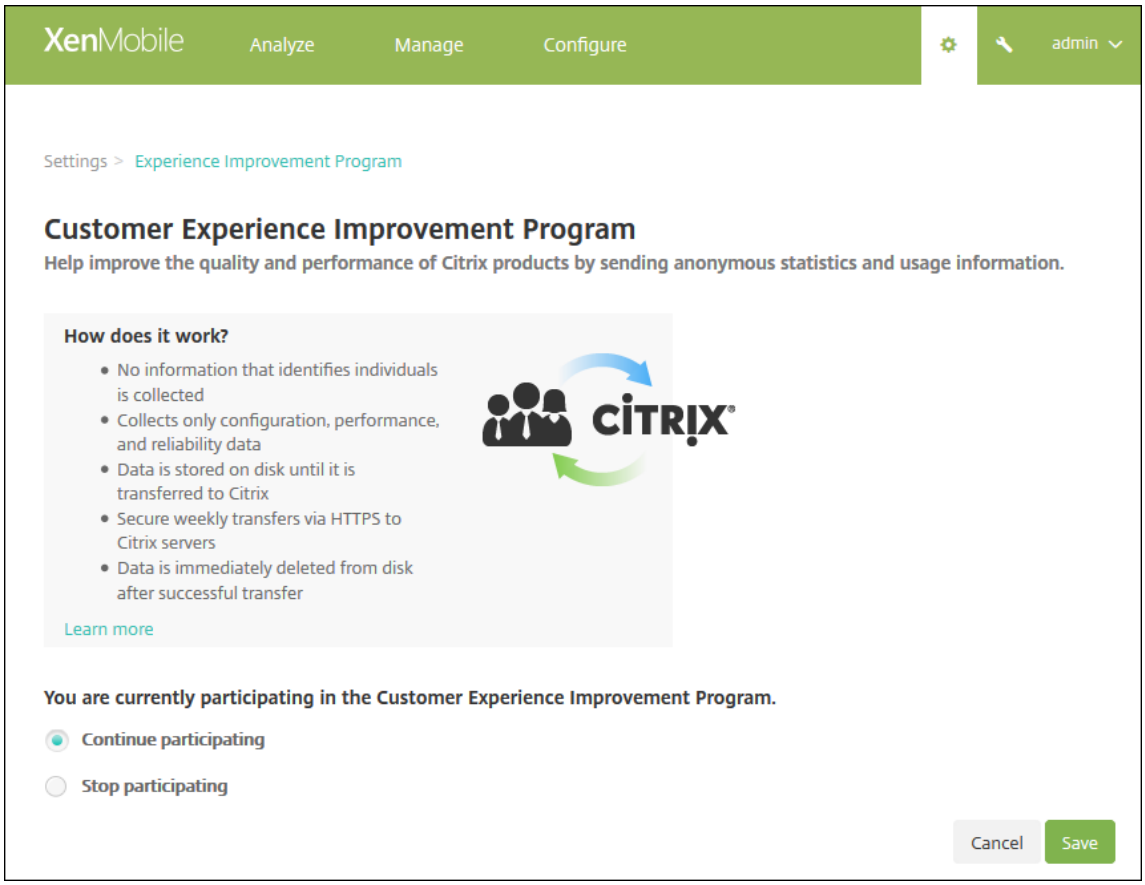


Alterar sua configuração de participação no CEIP

1. Para alterar a sua configuração de participação no CEIP, no console XenMobile, clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em **Servidor**, clique em **Programa de melhoria de experiência**. A página **Programa de melhoria de experiência do cliente** é exibida. A página exata que você vê depende de você estar ou não participando do CEIP no momento.



3. Se você participa do CEIP no momento e deseja parar, clique em **Parar participação**.
4. Se você não participa do CEIP no momento e deseja começar, clique em **Começar a participar**.
5. Clique em **Salvar**.

Logs

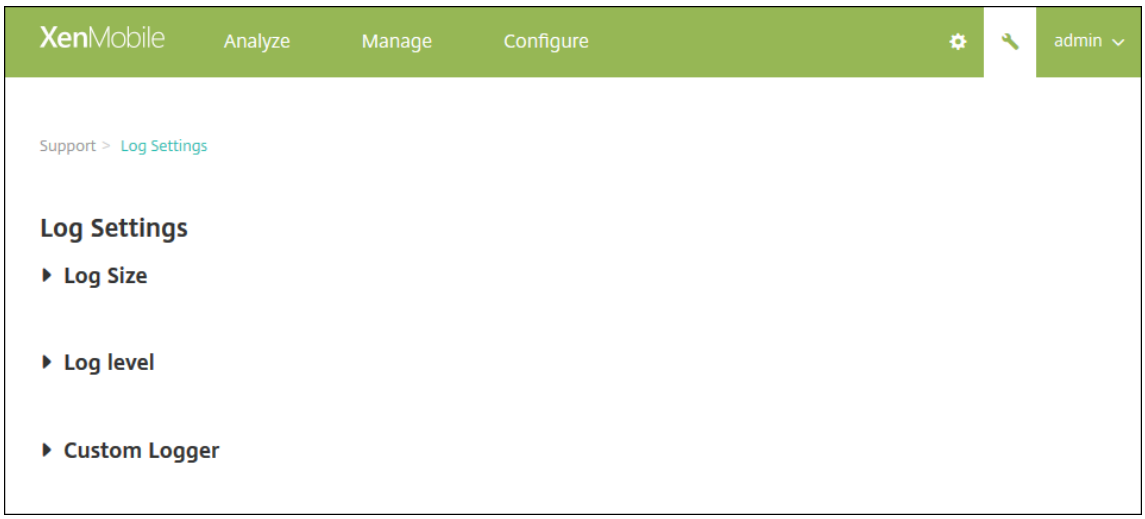
March 6, 2019

Você pode definir as configurações de log para personalizar a saída dos logs gerados pelo XenMobile. Se você tem servidores XenMobile em cluster, ao definir as configurações de log no console XenMobile, elas são compartilhadas com todos os outros servidores no cluster.

1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em **Operações de log**, clique em **Configurações de log**. A página **Configurações de log** é exibida.



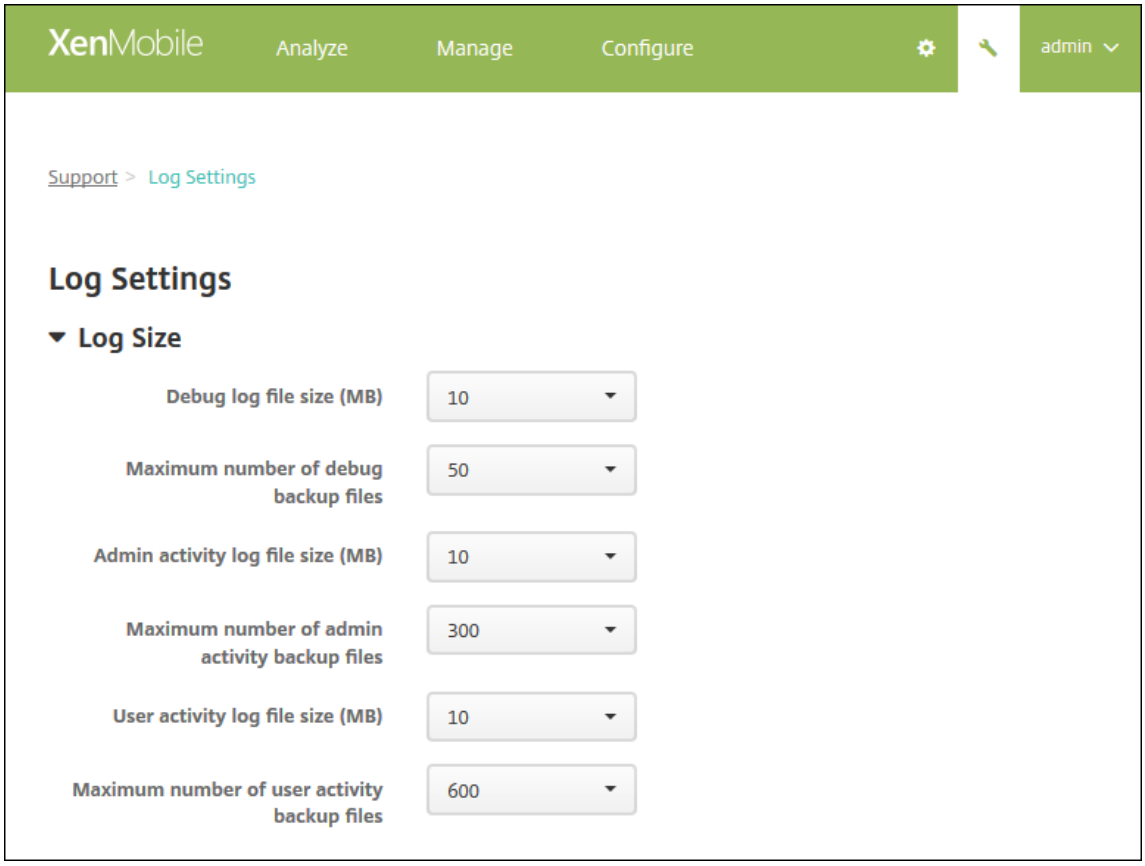
Na página **Configurações de log**, você pode acessar as seguintes opções:

- **Tamanho do log**. Use essa opção para controlar o tamanho do arquivo de log e o número máximo de arquivos de backup de log mantidos no banco de dados. O tamanho do log se aplica a cada um dos logs compatíveis com o XenMobile (log de depuração, log de atividades do administrador e log de atividades do usuário).
- **Nível de log**. Use essa opção para alterar o nível de log ou para manter as configurações.
- **Agente de log personalizado**. Use essa opção para criar um agente de log personalizado; os logs personalizados exigem um nome de classe e o nível de log.

Para configurar as opções de Tamanho do Log

1. Na página **Configurações de log**, expanda **Tamanho do log**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

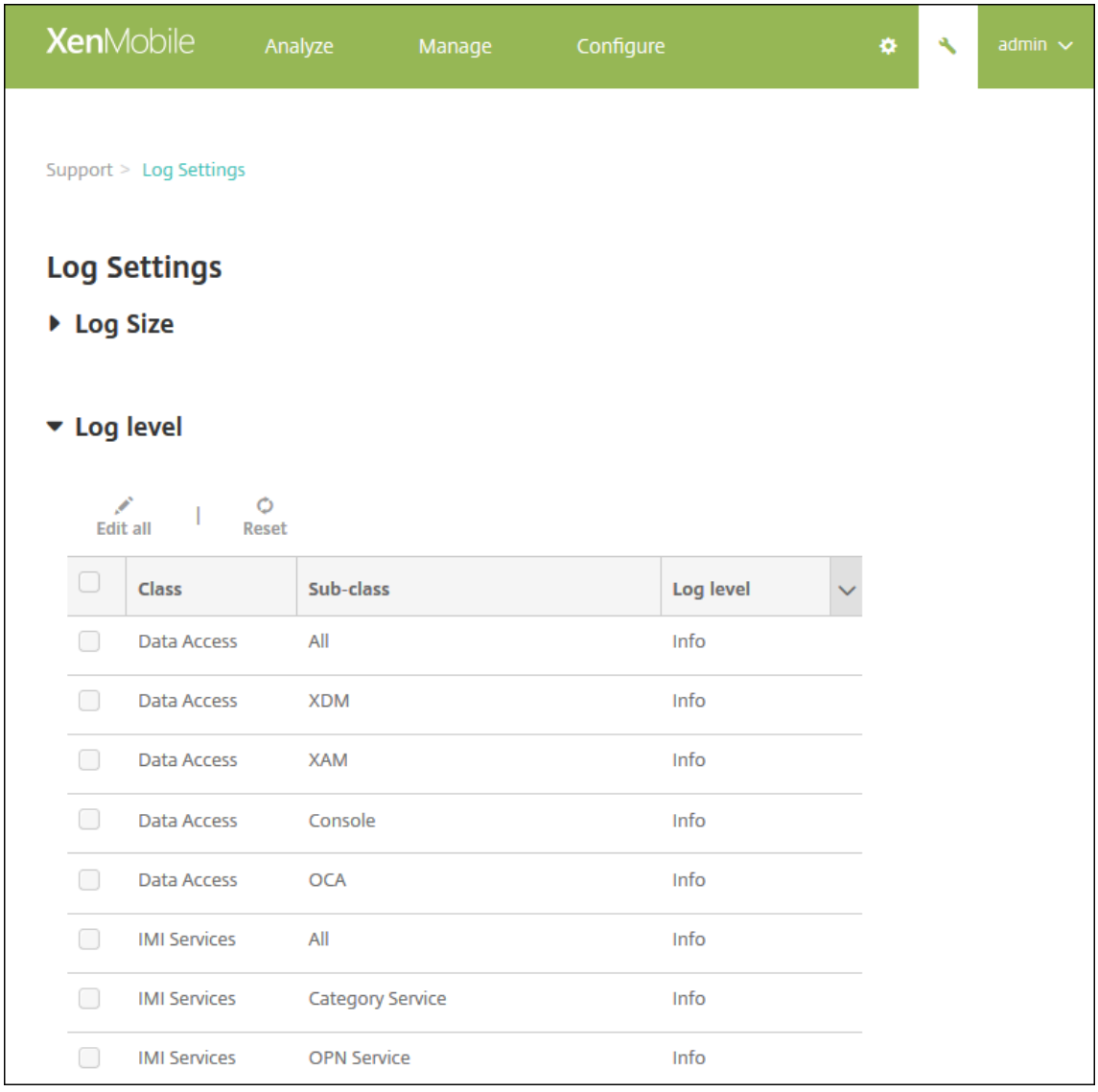
   - **Tamanho de arquivo do log de depuração (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de depuração. O tamanho do arquivo padrão é de **10 MB**.
   - **Número máximo de arquivos de backup de depuração:** na lista, clique no número máximo de arquivos de depuração mantidos pelo servidor. Por padrão, o XenMobile mantém 50 arquivos de backup no servidor.
   - **Tamanho de arquivo de log das atividades do administrador (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividades do administrador. O tamanho do arquivo padrão é de **10 MB**.
   - **Número máximo de arquivos de backup das atividades do administrador:** na lista, clique no número máximo de arquivos de atividades do administrador mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.
   - **Tamanho do arquivo de log das atividades do usuário (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividades do usuário. O tamanho do arquivo padrão é de **10 MB**.
   - **Número máximo de arquivos de backup das atividades do usuário:** na lista, clique no número máximo de arquivos de atividades do usuário mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar as opções de Nível de Log

O nível de log permite especificar quais tipos de informações o XenMobile coleta no log. Você pode definir o mesmo nível para todas as classes ou 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.

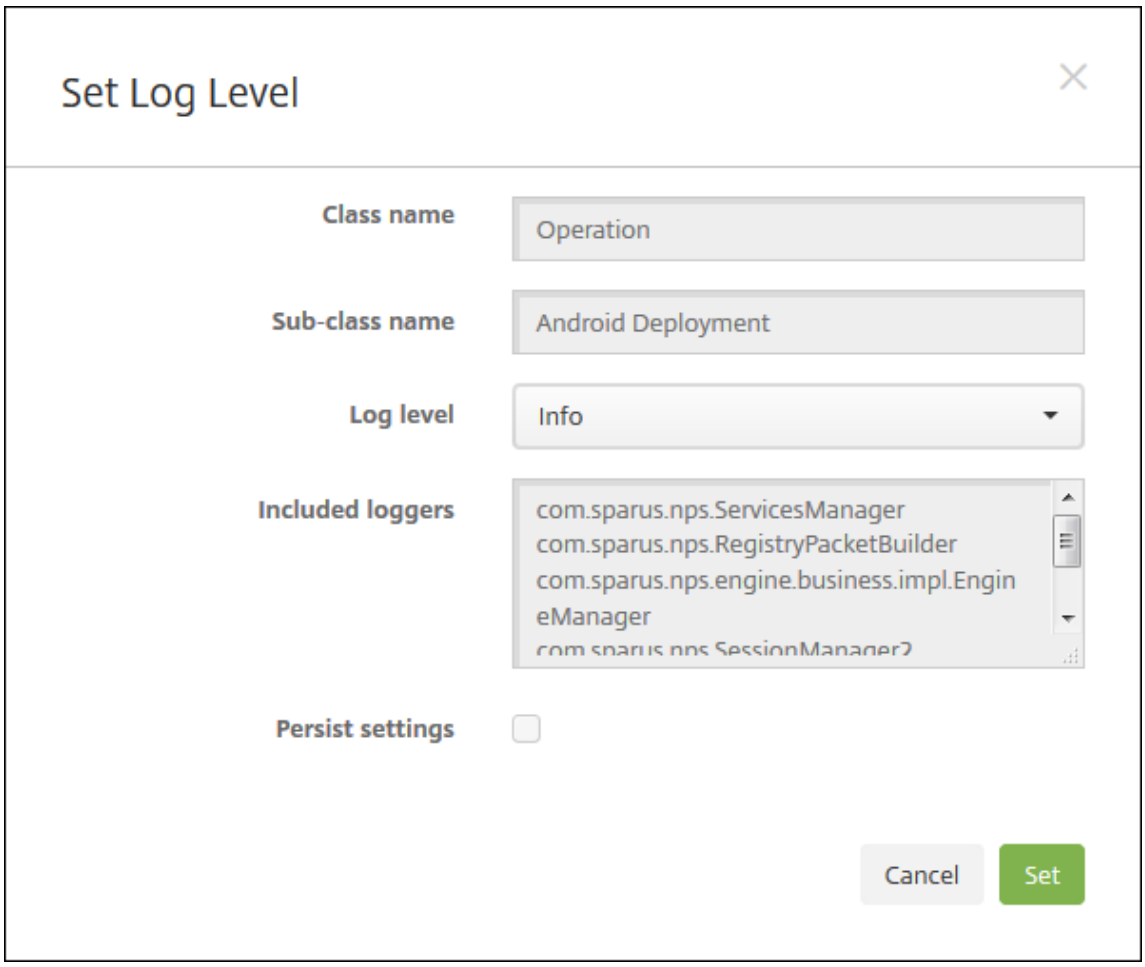


2. Você pode optar por um dos seguintes procedimentos:

   - Clique na caixa de seleção ao lado de uma Classe e, em seguida, clique em **Definir Nível** para alterar apenas o nível de registro dessa classe.
   - Clique em **Editar** tudo para aplicar a alteração no nível de log a todas as classes na tabela.

   A caixa de diálogo **Definir nível de log** é exibida, na qual você pode definir o nível de log e selecionar se as configurações no nível de log devem persistir ao reinicializar o XenMobile Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- **Nome da classe:** esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibirá o nome da classe individual; ele não é editável.
- **Nome da subclasse:** esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibirá o nome da subclasse individual; ele não é editável.
- **Nível de log:** na lista, clique em um nível de log. Os níveis de log compatíveis incluem:
  - Fatal
  - Erro
  - Aviso
  - Informações
  - Depuração
  - Rastreamento
  - Desativado
- **Agentes incluídos:** esse campo estará em branco quando você estiver alterando o nível de log de todas as classes ou exibirá os agentes de log configurados no momento para uma classe individual; ele não é editável.
- **Manter as configurações:** se você desejar que as configurações de nível de log sejam mantidas quando reiniciar o servidor, marque essa caixa de seleção. Não marcar essa caixa

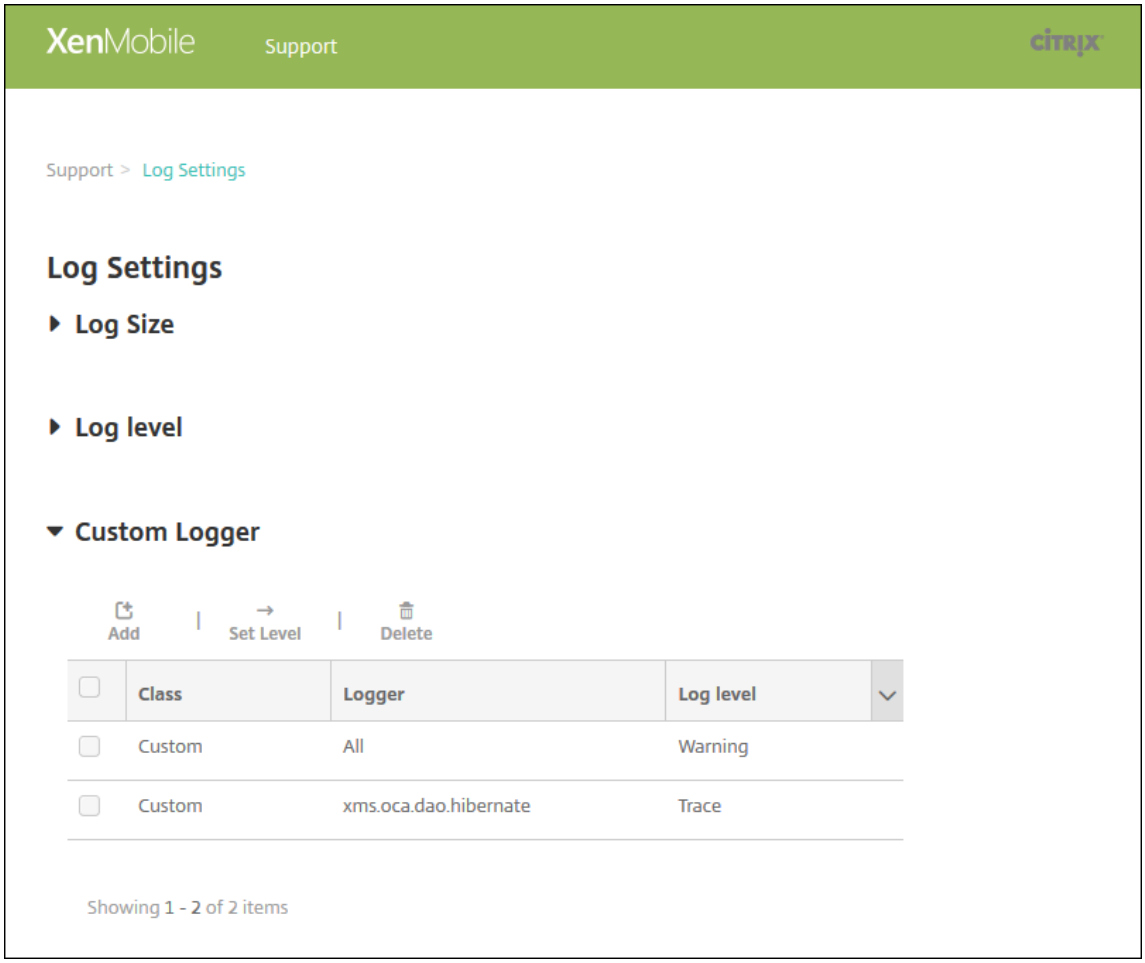
© 1999-2019 Citrix Systems, Inc. All rights reserved.

de seleção significa que as configurações de nível de log serão revertidas para o padrão quando você reiniciar o servidor.

3. Clique em **Definir** para confirmar as alterações.

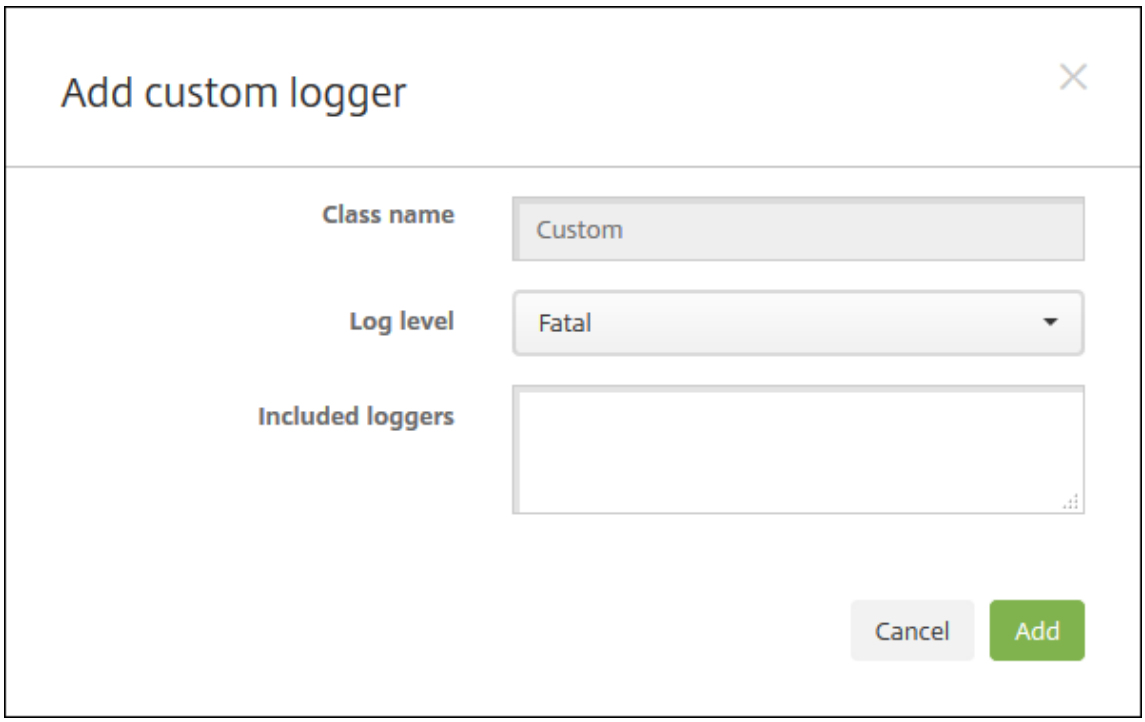
Para adicionar um Agente de Log Personalizado

1. Na página **Configurações de log**, expanda **Agente de log personalizado**. A tabela **Agente de log personalizado** é exibida. Se você ainda não tiver adicionado nenhum agente de log personalizado, a tabela estará inicialmente vazia.



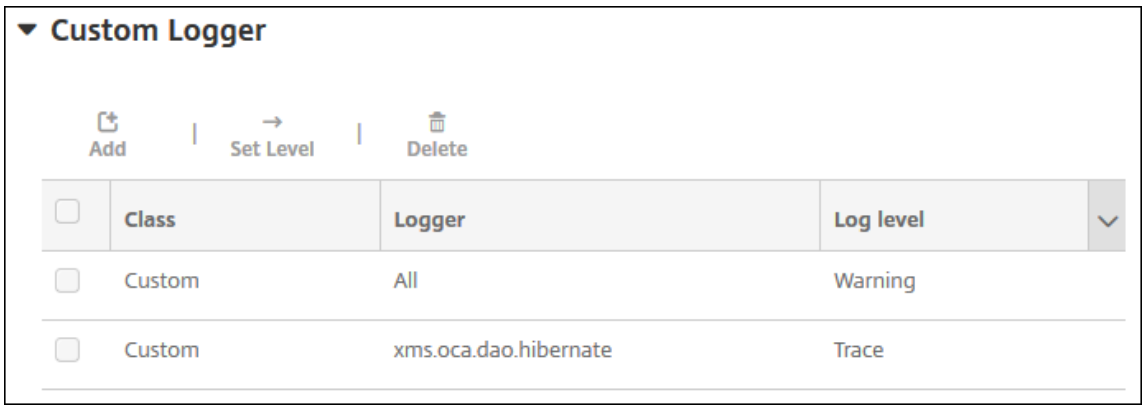
2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Defina estas configurações:
   - **Nome da classe:** esse campo exibe **Personalizado**; ele não é editável.
   - **Nível de log:** na lista, clique em um nível de log. Os níveis de log compatíveis incluem:
     - Fatal
     - Erro
     - Aviso
     - Informações
     - Depuração
     - Rastreamento
     - Desativado
   - **Agentes de log incluídos:** digite os agentes de log específicos que você desejar incluir no agente de log personalizado ou deixe o campo em branco para incluir todos os agentes de log.
4. Clique em **Adicionar**. O agente de log personalizado é adicionado à tabela **Agente de log personalizado**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para excluir um Agente de Log Personalizado

1. Na página **Configurações de log**, expanda **Agente de log personalizado**.
2. Selecione o agente de log personalizado que você deseja excluir.
3. Clique em **Excluir**. Uma caixa de diálogo será exibida perguntando se você deseja excluir o agente de log personalizado. Clique em **OK**.

> Importante:
>
> Você não pode desfazer essa operação.

Provedor de serviços móveis

October 31, 2018

Você pode ativar o XenMobile para usar a interface do Provedor de Serviços Móveis para consultar o BlackBerry e dispositivos Exchange ActiveSync e emitir operações.

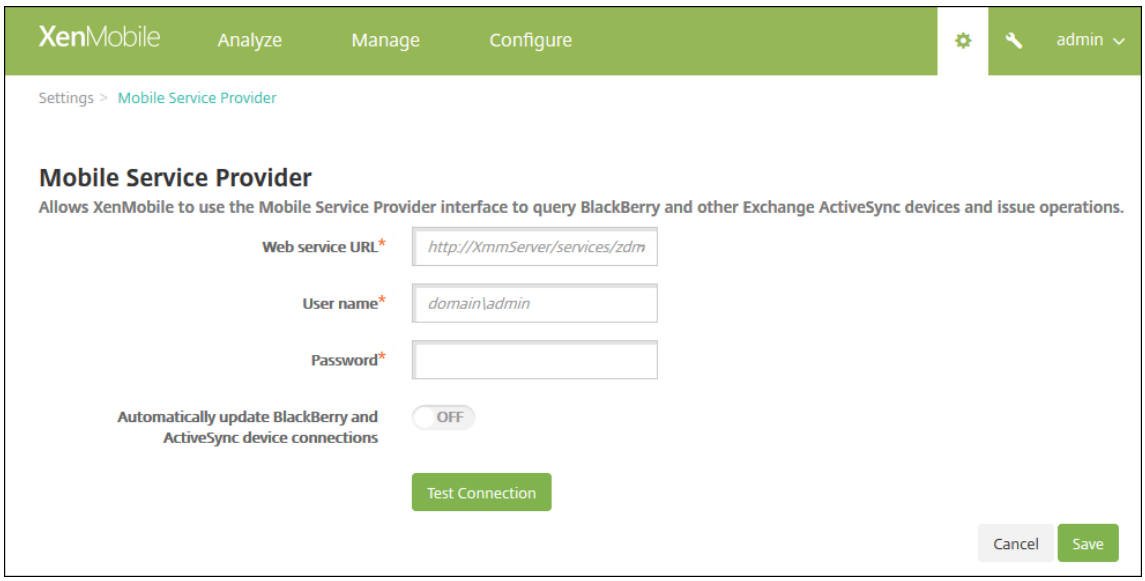
Por exemplo, sua empresa pode ter 1.000 usuários e cada usuário pode usar um ou mais dispositivos. Depois de comunicar com cada usuário que ele deve registrar seus dispositivos no XenMobile para gerenciamento, o console XenMobile indica o número de dispositivos que os usuários registram. Ao definir essa configuração, você pode determinar o número de dispositivos que se conectam ao Exchange Server. Desse modo, você pode fazer o seguinte:

- Verifique se algum usuário ainda precisaregistrar o dispositivo.
- Emita comandos para dispositivos de usuário que se conectam ao Exchange Server, como apagamentos de dados.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em **Servidor**, clique em **Provedor de serviços móveis**. A página **Provedor de serviços móveis** é exibida.



3. Defina estas configurações:

   - **URL de serviço da Web:** digite o URL do serviço da Web; por exemplo, `https://<XmmServer>/services/xdmservice`
   - **Nome de usuário:** digite o nome do usuário no formato domínio\administrador.
   - **Senha:** digite a senha.
   - **Atualizar automaticamente as conexões de dispositivo BlackBerry e ActiveSync:** selecione se as conexões do dispositivo são atualizadas automaticamente. O padrão é **O**.
   - Clique em **Testar conexão** para verificar a conectividade.

4. Clique em **Salvar**.

Relatórios

March 6, 2019

O XenMobile fornece os seguintes relatórios predefinidos que permitem analisar as implantações de aplicativo e dispositivo. Cada relatório é exibido como uma tabela e um gráfico. Você pode classificar e filtrar as tabelas por coluna. Você pode selecionar elementos em gráficos de informações mais detalhadas.

- **Total de tentativas de implantação de aplicativos:** lista aplicativos implantados que os usuários tentaram instalar em seus dispositivos.
- **Aplicativos por Plataforma:** lista os aplicativos e as versões de aplicativo por plataforma e versão do dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Aplicativos por Tipo:** lista os aplicativos por categoria, tipo e versão.
- **Registro do dispositivo:** lista todos os dispositivos registrados.
- **Dispositivos e aplicativos:** lista os dispositivos que executam os aplicativos gerenciados.
- **Dispositivos inativos:** uma lista de dispositivos que não tiveram atividades durante o número de dias especificado pela propriedade device.inactivity.days.threshold do XenMobile Server.
- **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 exibir mais detalhes.
- **Os 10 aplicativos mais usados:** falha na implantação: lista até 10 aplicativos cuja implantação falhou.
- **Aplicativos em lista negra por dispositivos e usuário:** lista de aplicativos em lista negra que os usuários têm em seus dispositivos.

Você pode exportar os dados de cada tabela para o formato .csv, que pode ser aberto por meio de programas como o Microsoft Excel. Você pode exportar o gráfico de cada relatório para o formato PDF.

Para gerar um relatório

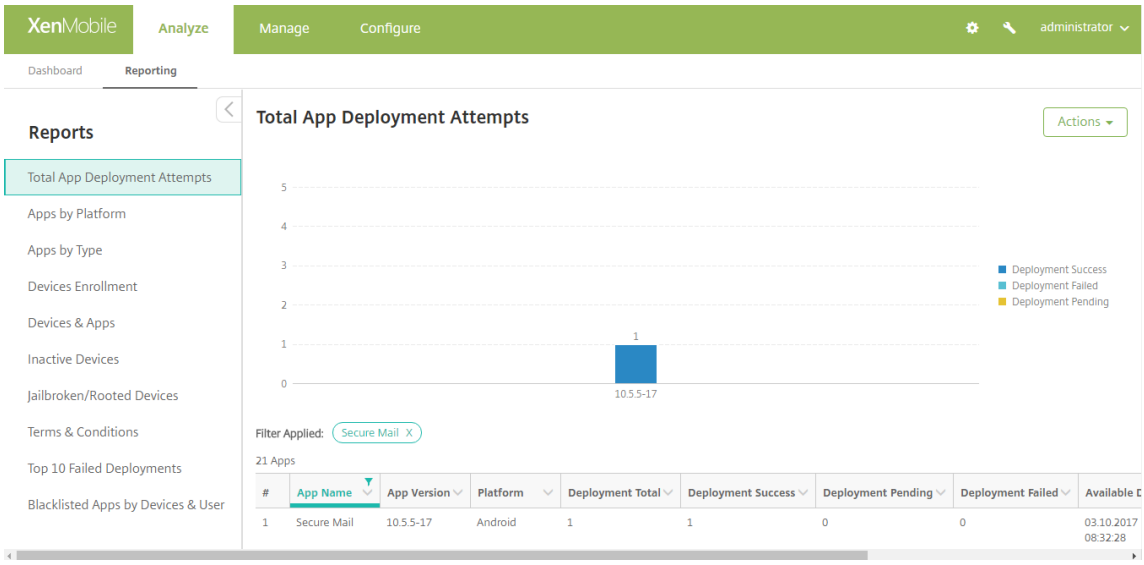
1. No console XenMobile, clique em **Analisar > Relatórios**. A página **Relatórios** é exibida.
2. Clique no relatório que você desejar gerar.



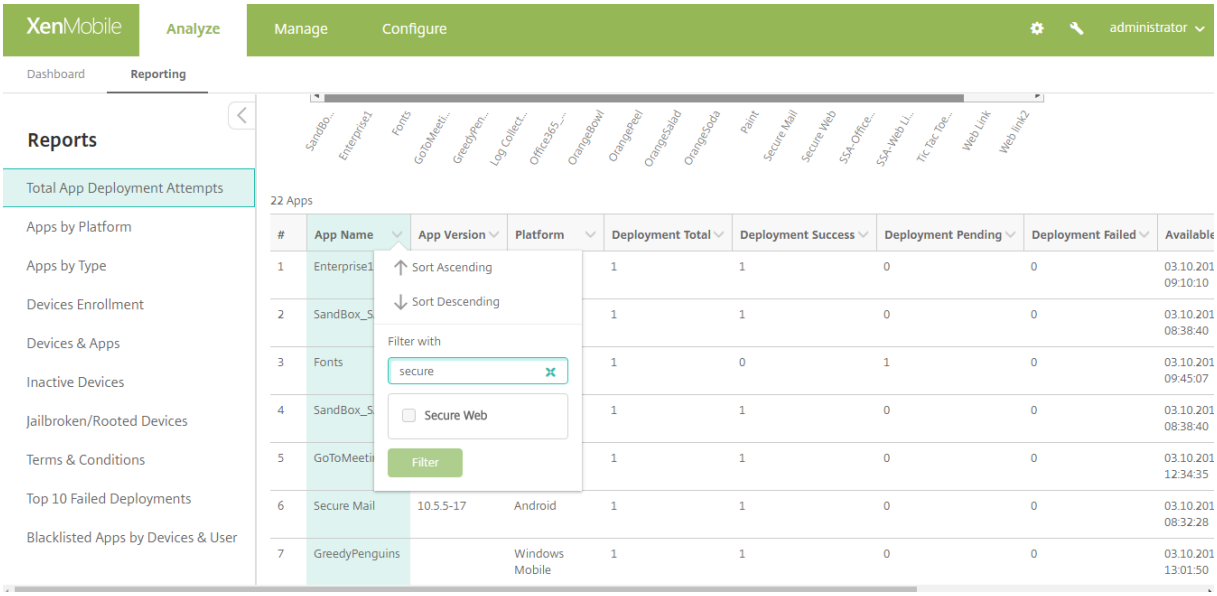
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para exibir mais detalhes de um relatório

1. Clique em áreas do gráfico para fazer uma busca detalhada e obter mais informações sobre detalhes.



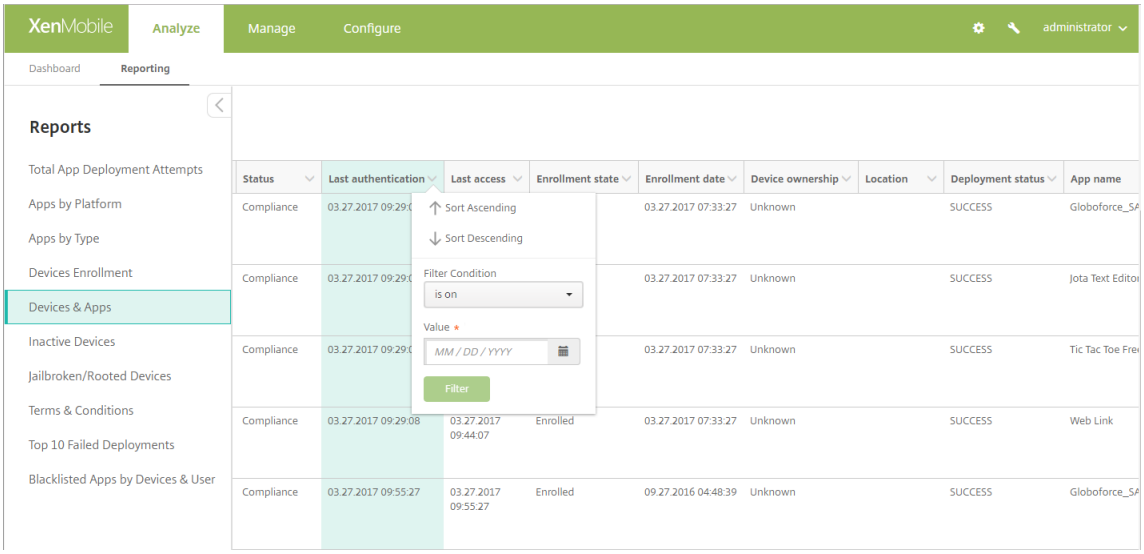
Para classificar, filtrar ou pesquisar uma coluna da tabela, clique no cabeçalho da coluna



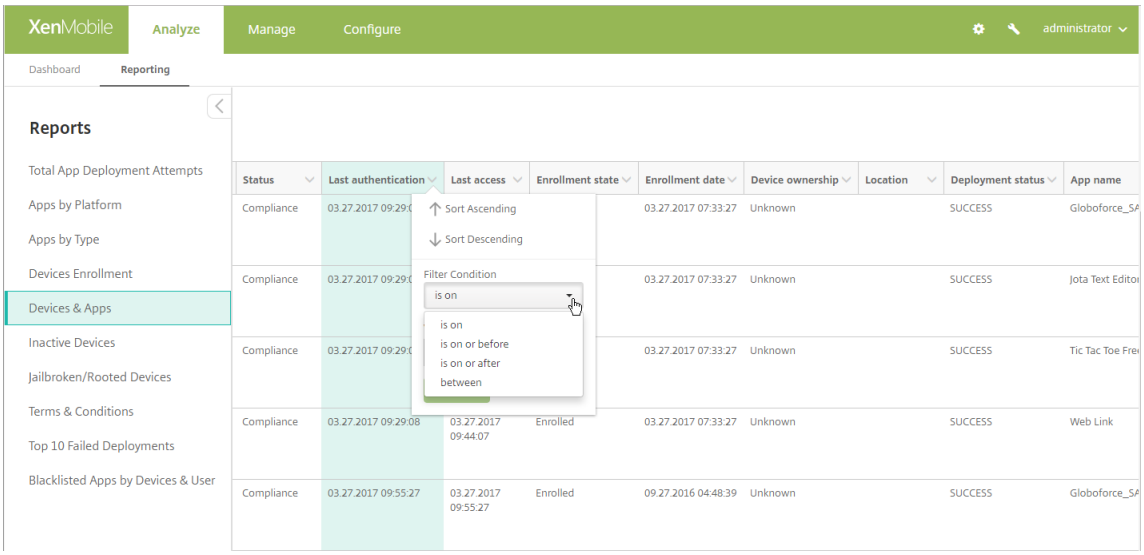
Para filtrar o relatório por data

1. Clique em um cabeçalho de coluna para exibir as configurações de filtro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

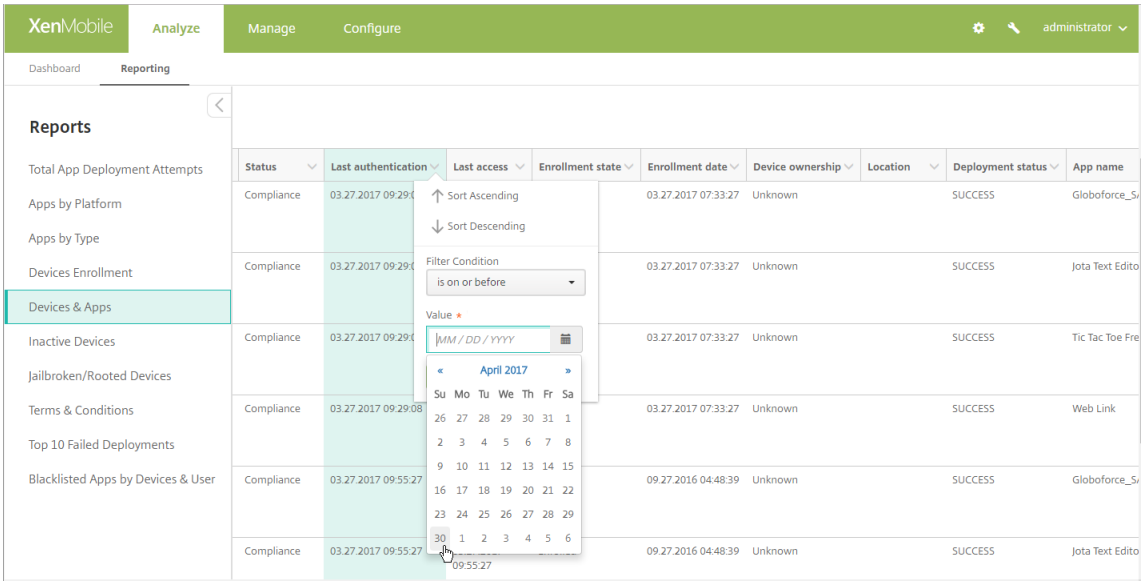


2. Em **Condição do filtro**, escolha como você deseja restringir as datas informadas.

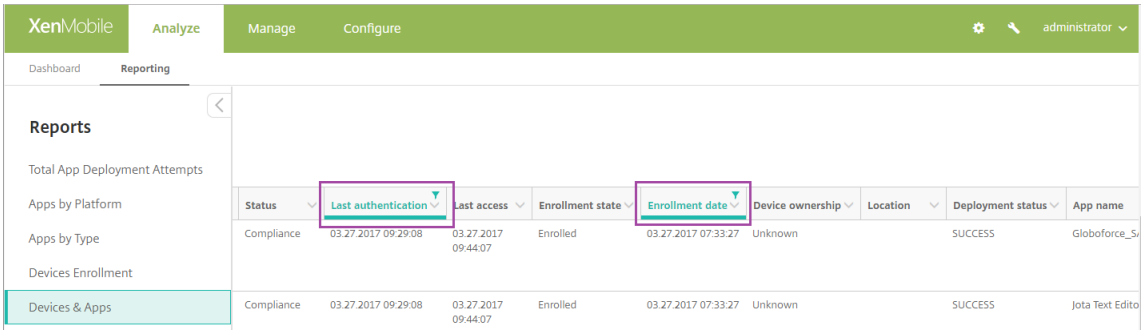


3. Use o seletor de data para especificar as datas.

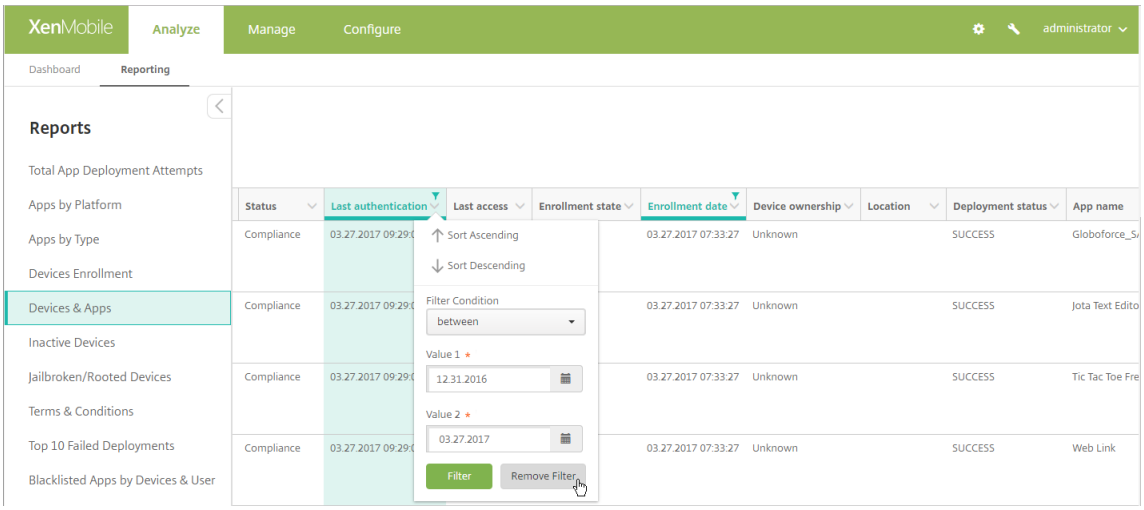
© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Uma coluna com um filtro de data é exibida conforme o exemplo a seguir.



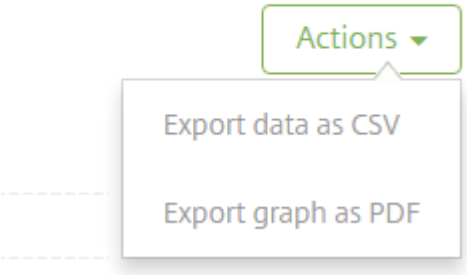
5. Para remover um filtro, clique no cabeçalho da coluna e depois em **Remover filtro**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para exportar um gráfico ou uma tabela

- Para exportar o plano no formato PDF, clique em **Ações** e em **Exportar gráfico como PDF**.
- Para exportar os dados da tabela no formato CSV, clique em **Ações** e em **Exportar dados como CSV**.



> Importante:
>
> Embora seja possível usar o SQL Server para criar relatórios personalizados, Citrix não recomenda esse método. A Citrix não publica o esquema e pode alterar o esquema sem notificação. Se você decidir tomar esse método de emissão de relatórios, certifique-se de que as consultas do SQL são executadas usando uma conta de somente leitura. Esteja ciente de que uma consulta com várias associações JOIN que leva algum tempo para executar prejudica o desempenho do XenMobile Server durante esse período.

SNMP monitoring

April 15, 2019

Você pode ativar o SNMP Monitoring no XenMobile Server para permitir que os sistemas de monitoramento consultem e obtenham informações nos nós do XenMobile. As consultas usam parâmetros, como Carga do processador, Média da carga, Uso da memória e Conectividade. Para obter mais informações sobre o SNMP v3, como especificações de autenticação e criptografia, consulte a documentação oficial do SNMP para RFC 3414.

> Nota:
>
> SNMP v3 Monitoring é compatível com o XenMobile Server 10.8 e versões posteriores.

Você pode usar vários aplicativos de monitoramento que suportam o monitoramento de SNMP, como o SCOM. Para obter detalhes sobre como configurar o SCOM, consulte este artigo do Citrix Support Knowledge Center.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos

Configure as seguintes portas TCP:

- **Porta 161 (UDP):** usada para tráfego SNMP usando o protocolo UDP. A origem é SNMP Manager e o destino é XenMobile.
- **Porta 162 (UDP):** usada para enviar alertas de interceptação SNMP ao SNMP Manager do XenMobile. A origem é XenMobile e o destino é SNMP Manager.

Para obter mais informações sobre a configuração das portas do XenMobile, consulte Requisitos de porta.

Para ver um diagrama de arquitetura de uma implantação local do XenMobile que inclui o SNMP, consulte a 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 interceptações e monitorar o XenMobile Server.
2. **Adicionar um SNMP Manager para receber interceptações:** Interceptações são alertas gerados pelo XenMobile quando o nó do XenMobile ultrapassa o limite de máximo definido pelo usuário.
3. **Configurar o SNMP Manager para interagir com o XenMobile:** O XenMobile Server usa certas bases de informações de gerenciamento (MIBs) para executar operações. Você faz o download de MIBs na página **Configurações > Configuração SNMP** no console XenMobile. Em seguida, você importa as MIBs para o SNMP Manager usando um MIB Importer.

   > Nota:
   >
   > Cada SNMP Manager possui seu próprio MIB Importer.

4. **Ativar interceptações:** Você ativa interceptações no console XenMobile e define os intervalos e limites com base em seu ambiente.
5. **Exibir interceptações no SNMP Manager de terceiros:** Para exibir interceptações, verifique o SNMP Manager. Em alguns gerenciadores, no entanto, você pode definir configurações para ativar notificações fora do Manager. Você pode configurar as notificações para aparecer, por exemplo, no email.

Você pode gerar as seguintes interceptações no XenMobile.

Nome da intercepção: Carga do processador

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.2.1.25.3.3.1.2
- **Descrição:** Monitora a carga da CPU do sistema no intervalo definido pelo usuário. Se a carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome da interceptação: Média de carga em um minuto

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.1
- **Descrição:** Monitora a carga média do sistema durante um período de um minuto no intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Média de carga em cinco minutos

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.2
- **Descrição:** Monitora a carga média do sistema durante um período de cinco minutos no intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Média de carga em 15 minutos

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.3
- **Descrição**: Monitora a carga média do sistema durante um período de 15 minutos a cada intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Memória disponível total

- **Identificador de objeto (OID) de monitoramento:** .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 de limite personalizado, o XenMobile gera a interceptação SNMP. Nota: A memória total disponível inclui RAM e memória swap (memória virtual). Para recuperar a memória swap total, você pode realizar uma consulta usando SNMP OID .1.3.6.1.4.1.2021.4.3 Para recuperar a memória swap disponível, você pode realizar uma consulta usando SNMP OID .1.3.6.1.4.1.2021.4.4

Nome de interceptação: Armazenamento em disco total usado

- **Identificador de objeto (OID) de monitoramento:** .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 de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Utilização da memória heap de Java

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Descrição:** Monitora o uso de memória heap JVM (Java virtual machine) do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Uso de metaespaço de Java

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.2.5.0

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Descrição:** Monitora o uso de metaspace Java do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor de limite, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade LDAP

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Descrição:** Monitora a conectividade entre o servidor LDAP e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade DNS

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Descrição:** Monitora a conectividade entre o servidor DNS e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Google Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Descrição:** Monitora a conectividade entre o servidor do Google Store e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do Windows Phone Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.4.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Phone Store e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do Windows Tab Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.5.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Tab Store e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Windows Security Token

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Security Token e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Windows Notification

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Notification e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome de interceptação: Conectividade do servidor do APNs (Apple Push Notification Service)

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Descrição:** Monitora a conectividade entre o servidor do APNs e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor Apple Feedback

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Descrição:** Monitora a conectividade entre o servidor do Apple Feedback e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Apple Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Descrição:** Monitora a conectividade entre o servidor do Apple Store e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Conectividade do banco de dados do XenMobile

- **Identificador de objeto (OID) de monitoramento:** .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 interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Google Cloud Messaging

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.12.0
- **Descrição:** Monitora a conectividade entre o servidor do Google Cloud Messaging e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor de licenças Citrix

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Descrição:** Monitora a conectividade entre o servidor de licença Citrix e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do NetScaler Gateway

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Descrição:** Monitora a conectividade entre o NetScaler Gateway e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome de interceptação: conectividade entre nós do XenMobile

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Descrição:** Monitora a conectividade entre nós em cluster do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do serviço de nó do XenMobile Tomcat

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Descrição:** Monitora a conectividade entre o serviço de nó do XenMobile Tomcat e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

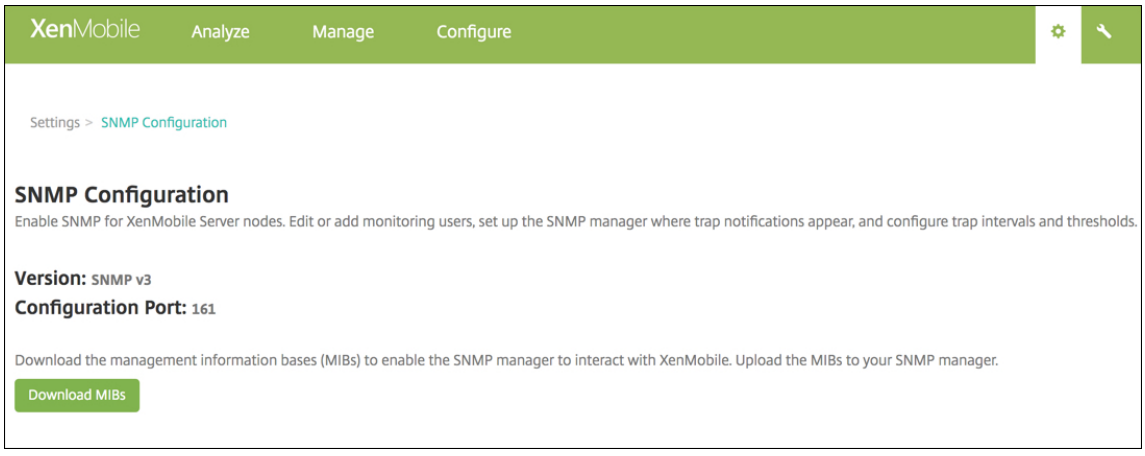
Para obter o melhor desempenho do servidor ao configurar os limites de SNMP, lembre-se dos seguintes fatores:

- Frequência de chamadas
- Dados de interceptação a serem coletados e as verificações de limite
- O mecanismo de comunicação entre nós
- Freqüência de verificações de conectividade
- Tempos limite de falhas durante as verificações

Para adicionar usuários SNMP

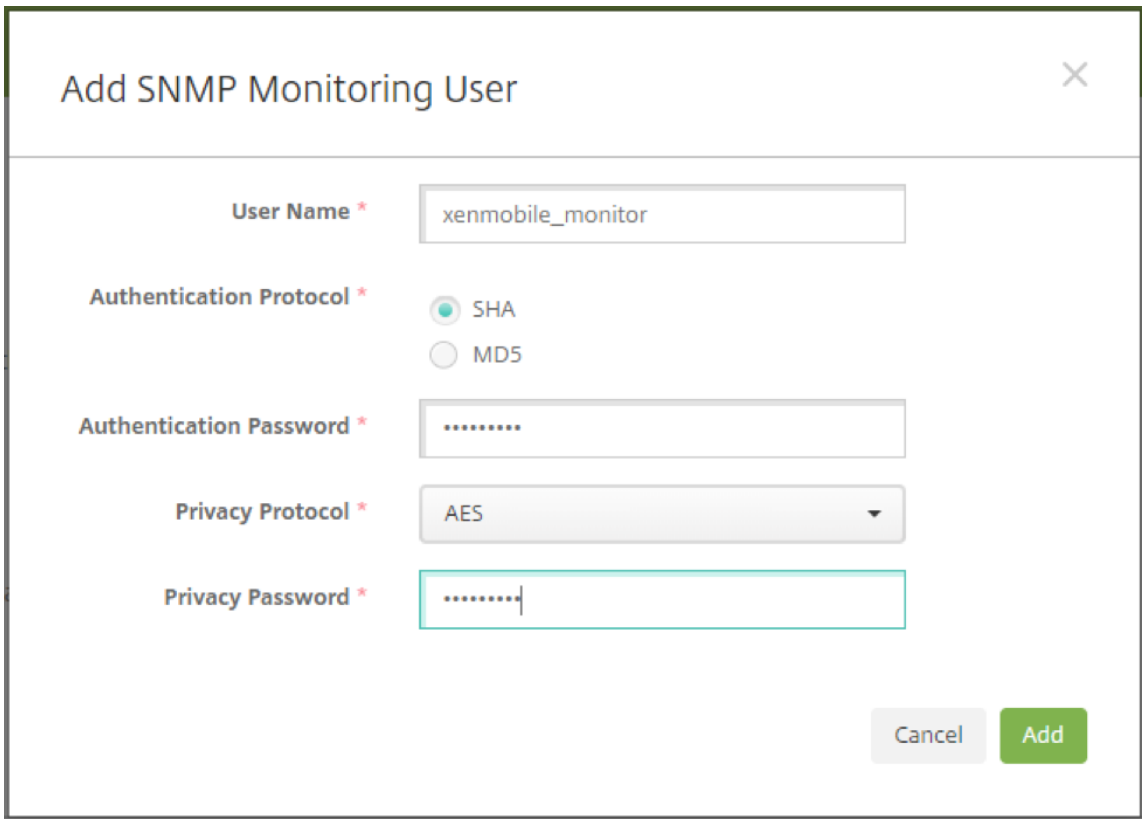
Os usuários SNMP interagem com gerenciadores SNMP e recebem interceptações.

1. No console 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 SNMP Monitoring**, clique em **Adicionar**.
4. Na caixa de diálogo **Adicionar usuário de SNMP Monitoring**, defina as seguintes configurações:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Nome de usuário: o nome do usuário usado para efetuar logon no SNMP Manager. Embora você possa usar caracteres alfanuméricos, sublinhados e hifens, não é possível usar espaços e outros caracteres especiais no 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:

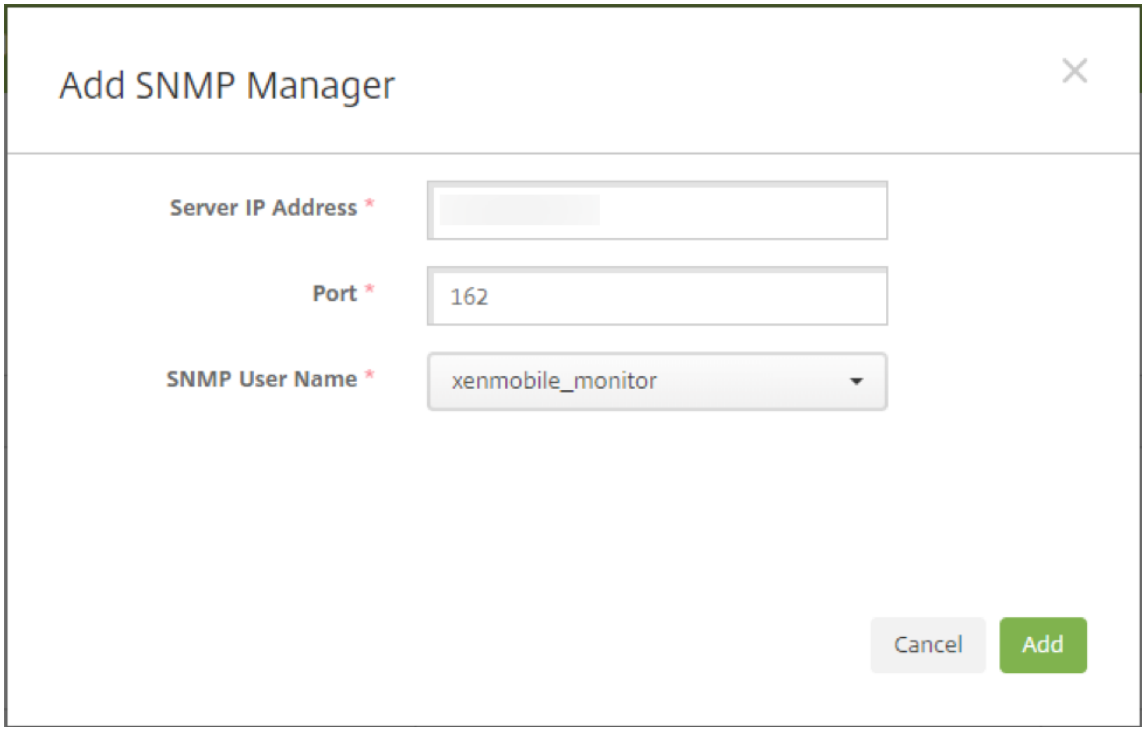
- **DES**
- **AES 128** (recomendado)

Senha de privacidade: digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para adicionar um SNMP Manager

1. Em **SNMP Managers**, clique em **Adicionar**.
2. Na caixa de diálogo **Adicionar SNMP Manager**, defina as seguintes configurações:



Endereço IP de servidor: digite o endereço IP do SNMP Manager.

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 Manager.

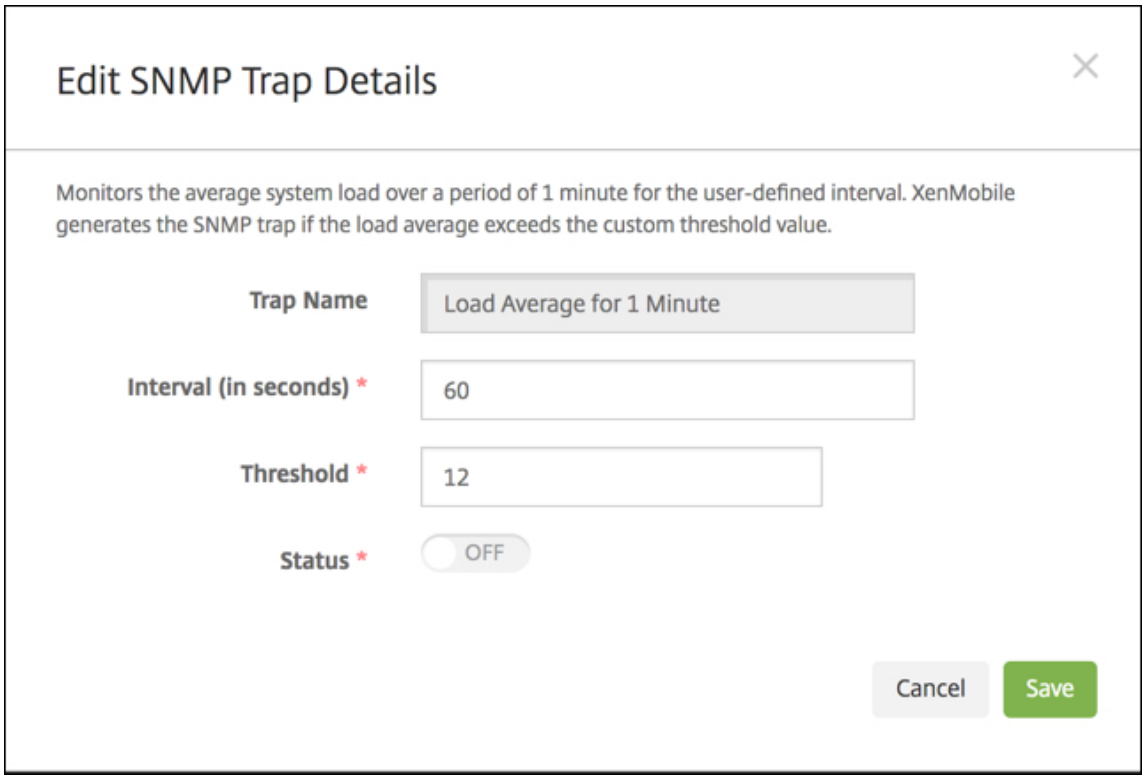
Para ativar e configurar interceptações SNMP

Para ajudar a determinar as configurações de interceptação adequadas para o seu ambiente, consulte Escalabilidade e desempenho. Por exemplo, para monitorar a média de carga do XenMobile por um minuto, você pode ativar a Média de Carga em 1 minuto e fornecer um valor de limite. Se a média de carga do XenMobile Server por 1 minuto exceder o limite especificado, você receberá uma interceptação nos SNMP Managers configurados.

1. Para ativar interceptações individuais, siga um dos destes procedimentos:
   - Marque a caixa de seleção ao lado do parâmetro e, em seguida, clique em **Ativar**.
   - Para ativar todas as interceptações da lista, marque a caixa de seleção na parte superior e clique em **Ativar**.
2. Para editar uma interceptação, selecione o parâmetro e, em seguida, clique em **Editar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Na caixa de diálogo **Editar detalhes da interceptação SNMP**, você pode editar os valores de limite para interceptações individuais.



Nome da interceptação: o nome da interceptação. Você não pode editar esse campo.

Intervalo (em segundos): o intervalo permitido é de 60 a 86400 (24 horas).

Limite: você pode alterar o limite somente para as seguintes interceptações:

- Carga do processador
- Média de carga em 1 minuto
- Média de carga em 5 minutos
- Média de carga em 15 minutos
- Memória disponível total
- Armazenamento total de disco usado
- Utilização da memória heap de Java
- Uso de metaespaço de Java

Status: selecione **I** para ativar o SNMP Monitoring para a interceptação. Selecione **O** para desativar o Monitoring.

Para obter mais informações úteis sobre o monitoramento do XenMobile usando o SNMP, consulte esta postagem no blog.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pacotes de suporte

April 15, 2019

Para notificar um problema para a Citrix ou solucionar um problema, crie um pacote de suporte. Depois, 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 padrão desses arquivos é 10 MB.

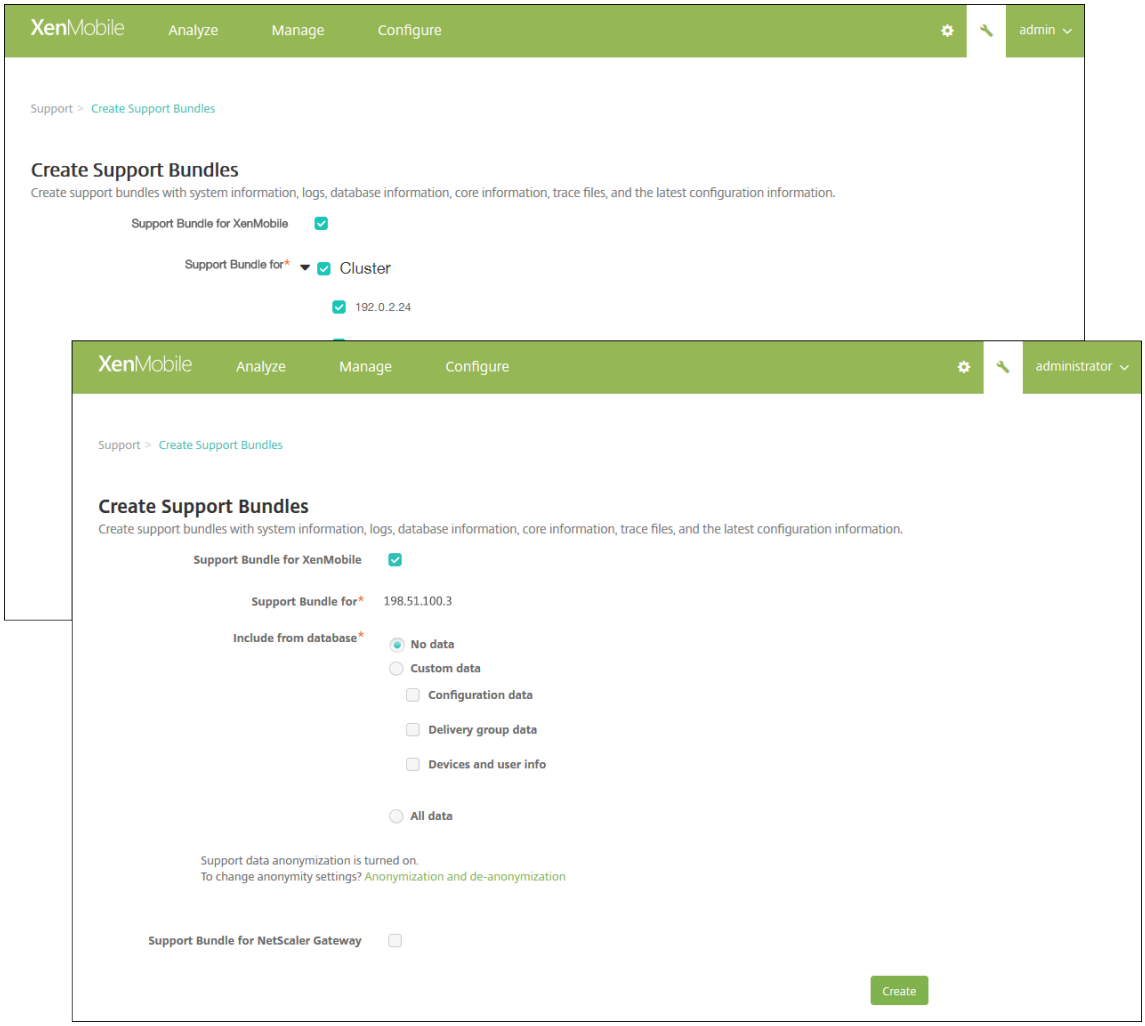
- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Quando o pacote de suporte inclui 100 arquivos de log para cada uma dessas categorias, o arquivo de log é transferido. Se você configurar um número máximo mais baixo de arquivos de log, o XenMobile excluirá imediatamente os arquivos de log externos desse 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 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 do XenMobile contiver nós de cluster, todos os nós serão mostrados.

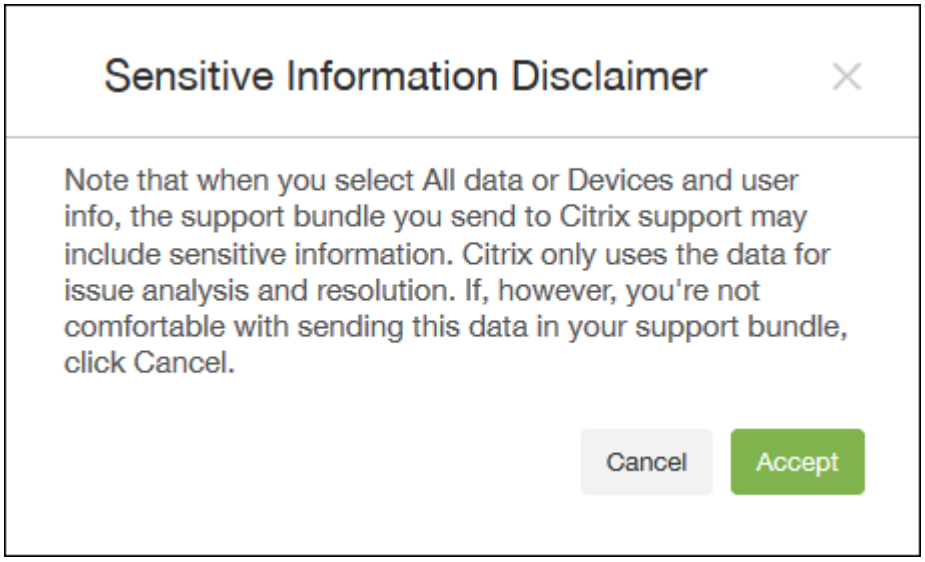
© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Verifique se a caixa de seleção **Pacote de suporte para XenMobile** está marcada.
4. Se o seu ambiente do XenMobile contiver nós de 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**, você pode optar por um dos seguintes procedimentos:
   - Clique em **Não há dados**.
   - Clique em **Dados personalizados**. Por padrão, todas essas opções estão selecionadas.
     - **Dados de configuração:** inclui configurações de certificado e políticas do gerenciador de dispositivo.
     - **Dados de grupo de entrega:** inclui informações de grupo de entrega de aplicativo que contêm detalhes de tipos de aplicativo e de política de entrega de aplicativo.
     - **Dispositivos e informações do usuário:** inclui políticas de dispositivo, aplicativos, ações e grupos de entrega.
   - Clique em **Todos os dados**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Se você escolher **Dispositivos e informações do usuário** ou **Todos os dados**, e esse for o primeiro pacote de suporte que você criou, a caixa de diálogo **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 inclui dados de usuário ou dispositivo.



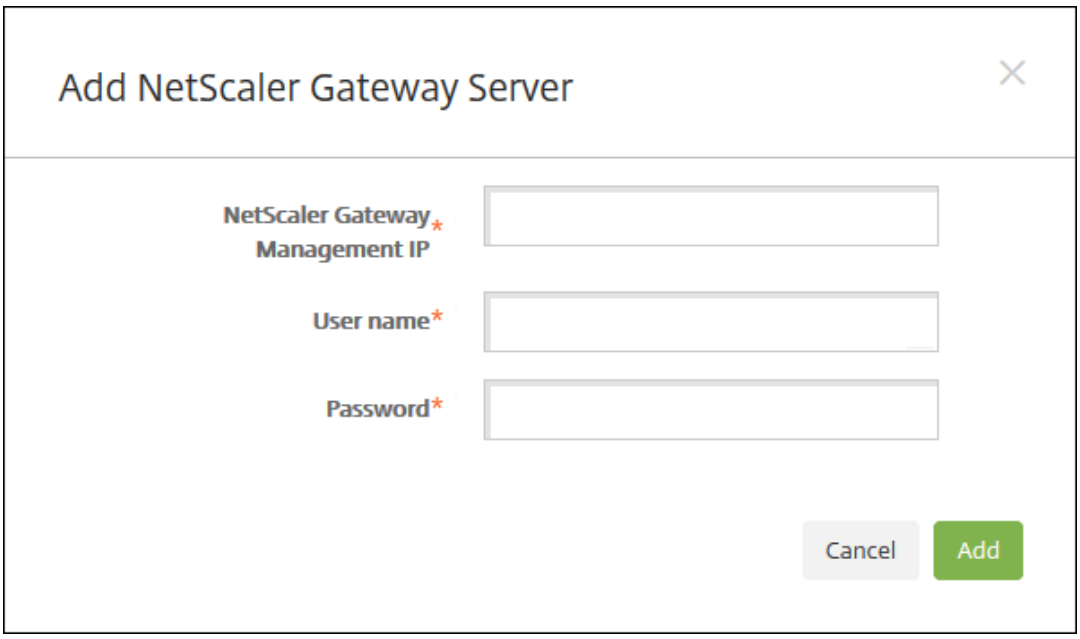
6. A opção **Anonimização de dados de suporte está ativada** indica que a configuração padrão é anonimizar os dados. A anonimização de dados significa que dados confidenciais do usuário, do servidor e da rede são feitos anônimos nos pacotes de suporte.

   Para alterar essa configuração, clique em **Anonimização e desanonimização**. Para obter mais informações sobre a anonimização de dados, consulte Anonimizando dados nos pacotes de suporte.

7. Para incluir pacotes de suporte do NetScaler Gateway: marque a caixa de seleção **Pacote de suporte para o NetScaler Gateway** e faça o seguinte:

   a) Clique em **Adicionar**. A caixa de diálogo **Adicionar servidor do NetScaler Gateway** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



b) Em **IP de Gerenciamento do NetScaler Gateway**, digite o endereço IP de gerenciamento do NetScaler do NetScaler Gateway do qual você deseja extrair os dados de pacote de suporte.

> Nota:
>
> Se você estiver criando um pacote de um servidor NetScaler Gateway que já foi adicionado, o endereço IP será fornecido.

c) Em **Nome de usuário** e **Senha**, digite as credenciais de usuário necessárias para acessar o servidor que executa o NetScaler Gateway.

> Nota:
>
> Se você estiver criando um pacote de um servidor NetScaler Gateway que já foi adicionado, o nome do usuário será fornecido.

8. Clique em **Adicionar**. O novo pacote de suporte do NetScaler Gateway é adicionado à tabela.
9. Repita a Etapa 7 para adicionar mais pacotes de suporte do NetScaler Gateway.
10. Clique em **Criar**. O pacote de suporte é criado, e dois novos botões, **Carregar em CIS** e **Baixar para o cliente** são exibidos.

Carregando pacotes de suporte para o Citrix Insight Services

Depois de criar um pacote de suporte, você poderá carregá-lo para o Citrix Insight Services (CIS) ou baixá-lo para o seu computador.

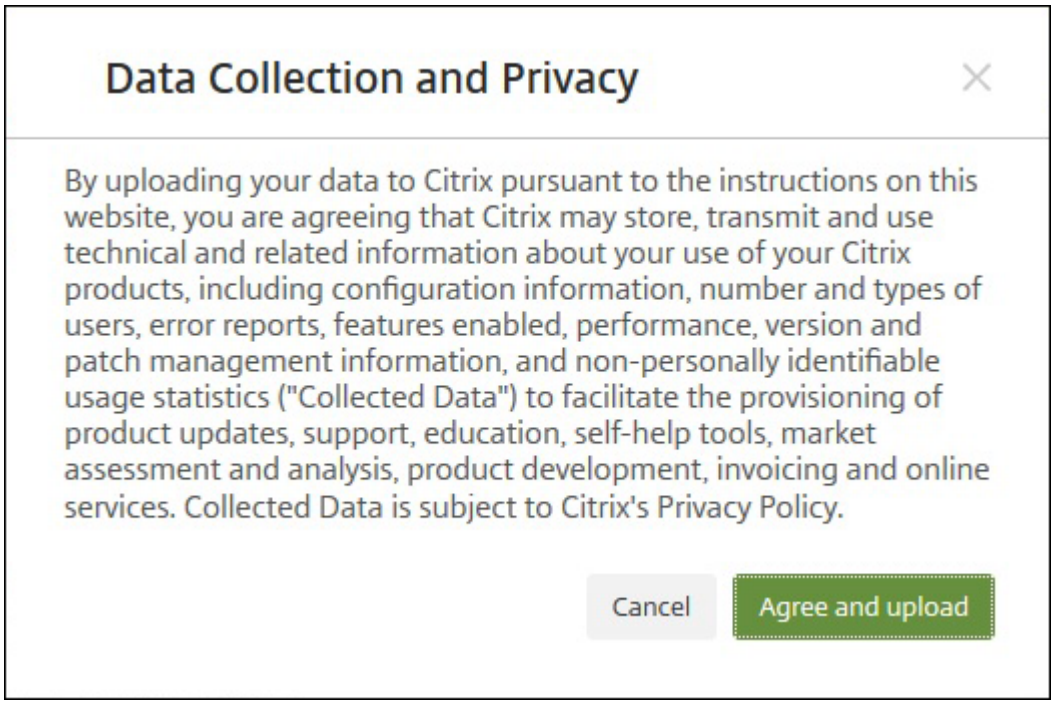
© 1999-2019 Citrix Systems, Inc. All rights reserved.

O carregamento do XenMobile para o CIS é realizado por meio de uma conexão de saída SSL. 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 o tráfego HTTPS, verifique se o proxy pode alcançar o endereço IP do servidor CIS.

Essas 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 em CIS**. A caixa de diálogo **Carregar para o Citrix Insight Services (CIS)** é exibida.
2. Em **Nome de usuário**, digite o seu ID do My Citrix.
3. Em **Senha**, digite a sua senha do My Citrix.
4. Se quiser conectar esse pacote a um número de solicitação de serviço existente, marque a caixa de seleção **Associar com nº de SR** e, nos dois novos campos que são exibidos, faça o seguinte:
   - Em **Nº de SR**, digite o número de solicitação de serviço de oito dígitos que você deseja associar a esse pacote.
   - Em **Descrição de SR**, digite uma descrição para o SR.
5. Clique em **Carregar**.

   Se essa tiver sido a primeira vez que carregou um pacote de suporte para o CIS e você não tiver criado uma conta no CIS por meio de outro produto e aceitado o acordo de Privacidade e Coleta de Dados, a seguinte caixa de diálogo é exibida. Você deve aceitar o acordo antes de começar o carregamento. Se você tiver uma conta no CEI e tiver aceitado o acordo, o pacote de suporte será carregado imediatamente.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Leia o acordo e depois 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 poderá carregá-lo para o CIS ou baixá-lo para o seu computador. Se você desejar solucionar o problema por si mesmo, baixe o pacote de suporte para o seu computador.

Na página Criar pacotes de suporte, clique em Baixar para o cliente. O pacote é baixado para o seu computador.

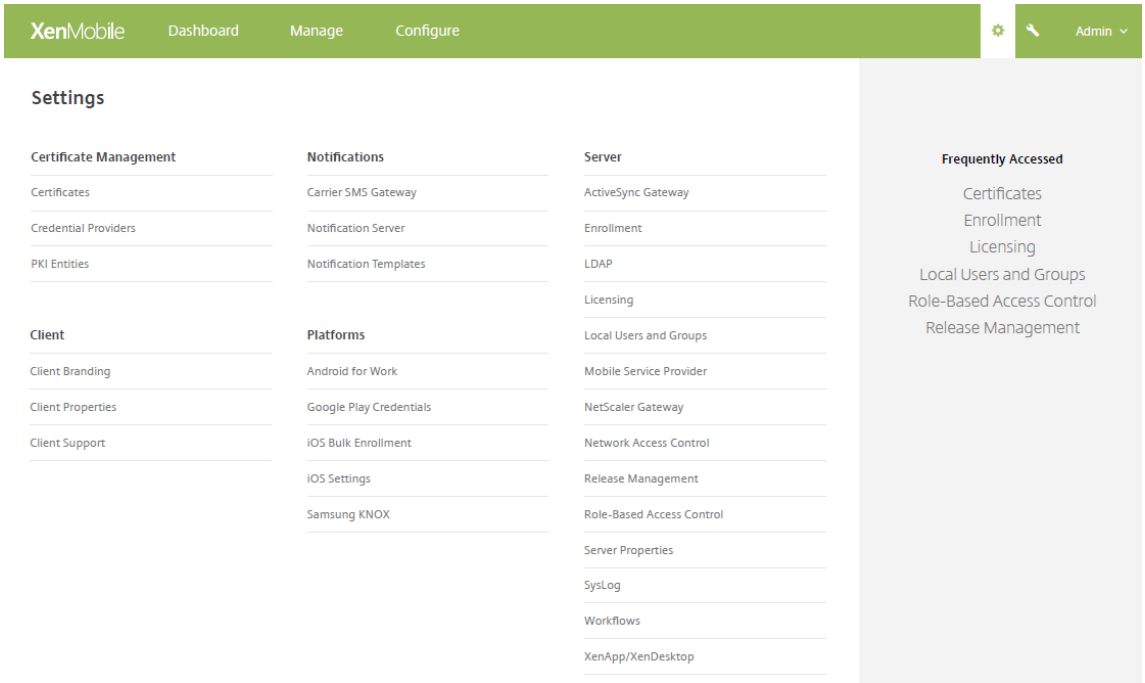
Opções de suporte e suporte remoto

April 15, 2019

Você pode fornecer um endereço de email para que os usuários entrem em contato com a equipe de suporte. Quando os usuários solicitarem assistência dos dispositivos deles, eles veem o endereço de email.

Você também pode configurar como os usuários enviam logs para o suporte técnico usando seus dispositivos. Você pode configurar os logs para que sejam enviados diretamente ou por email.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Em **Cliente**, clique em **Suporte ao cliente**. A página **Suporte ao cliente** é exibida.
3. Faça as seguintes configurações:
    - **Email de suporte (suporte técnico de TI):** digite o endereço de email do seu contato de 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 email**. O padrão é **por email**.
        - Quando você ativa **diretamente**, as configurações de Armazenar logs no ShareFile são exibidas. Se você ativar a opção Armazenar logs no ShareFile, os logs serão enviados diretamente ao ShareFile. Caso contrário, os logs serão enviados ao XenMobile e, em seguida, enviados por email para o suporte técnico. Além disso, a opção **Se o envio direto falhar, use o email**, que é ativada por padrão, aparece. Você pode desativar essa opção quando não desejar usar o email do cliente para enviar os logs se houver um problema com o servidor. Porém, quando essa opção for desativada e ocorrer um problema com o servidor, os logs não serão enviados.
        - Quando você ativa a opção **por email**, o email do cliente sempre é usado para enviar os logs.
4. Clique em **Salvar**.

Suporte remoto

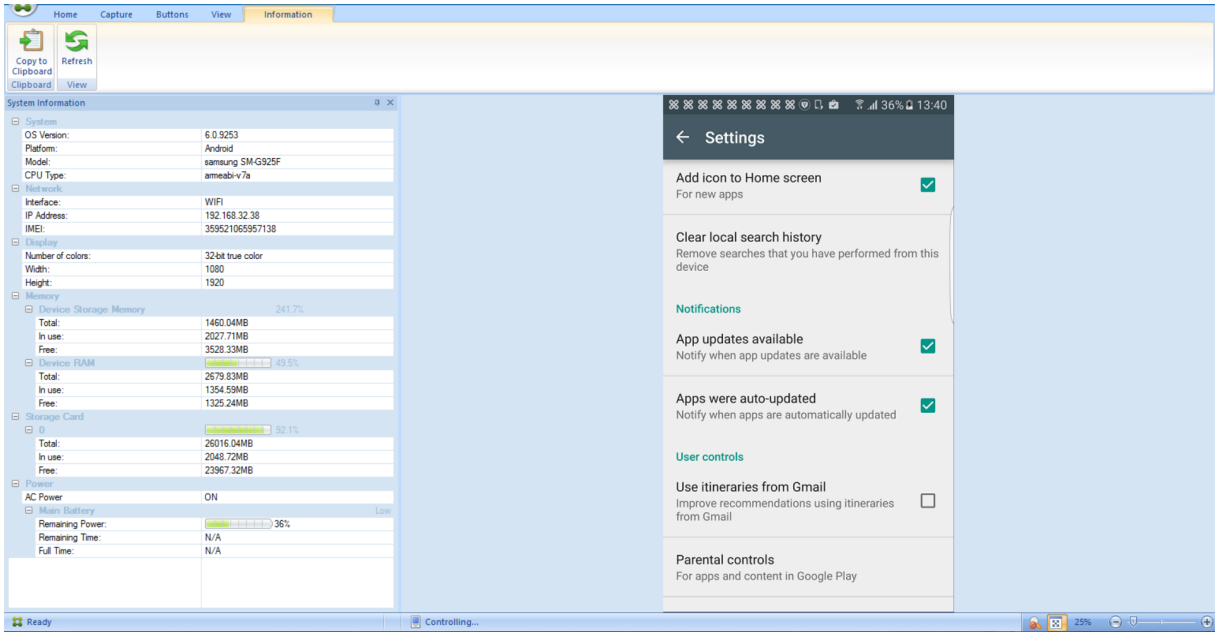
Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível com somente dispositivos Samsung KNOX.

O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

Durante uma sessão de controle remoto:

- Os usuários veem no dispositivo móvel um ícone que indica uma sessão de controle remoto está ativa.
- Os usuários do Remote Support veem a janela de aplicativo de Suporte remoto e uma janela de controle remoto que mostra uma representação do dispositivo controlado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Usando o Remote Support, você pode fazer o seguinte:

- Fazer login remotamente em um dispositivo móvel e controlar a tela. Os usuários podem assistir você navegar pela tela deles, o que também pode ser útil para fins de treinamento.
- Navegar e reparar um dispositivo remoto em tempo real. Você pode alterar as configurações, solucionar problemas de sistema operacional e desabilitar ou parar aplicativos ou processos problemáticos.
- Isolar e conter ameaças antes que se espalhem para outros dispositivos móveis desabilitando o acesso a rede, interrompendo processos danosos e removendo aplicativos ou malware.
- Habilitar remotamente o toque do dispositivo e telefonas para o telefone para ajudar o usuário a localizar o dispositivo. Quando um usuário não consegue encontrar o dispositivo, você pode apagá-lo para garantir que os dados confidenciais não sejam comprometidos.

O Suporte Remoto também permite ao pessoal de suporte:

- Exibir uma lista de todos os dispositivos conectados dentro de uma ou mais instâncias do XenMobile.
- Exibir informações do sistema do modelo de dispositivo, inclusive nível do sistema operacional, International Mobile Station Equipment Identity (IMEI), o número de série, memória e status da bateria e conectividade.
- Exibir os usuários e grupos para o XenMobile.
- Executar o gerenciador de tarefas do dispositivo, no qual você pode exibir e terminar processos ativos e reiniciar o dispositivo móvel.
- Executar transferência de arquivos remotos que inclui transferência bidirecional entre os dispositivos móveis e um servidor de arquivos.
- Baixar e instalar programas de software em lote para um ou mais dispositivos móveis.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Definir as configurações de chave de registro remotas no dispositivo.
- Otimizar o tempo de resposta por redes de celular de largura de banda estreita usando o controle remoto de tela de dispositivo em tempo real.
- Exibir a capa de dispositivo da maioria das marcas de modos de dispositivos móveis. Exibir um editor de capa para adicionar novos modelos de dispositivo e mapear chaves físicas.
- Ativar a captura, registro e reprodução de tela de dispositivo com a capacidade de capturar uma sequência de interações no dispositivo que cria um arquivo de vídeo AVI.
- Comandar reuniões compartilhadas ao vivo usando quadro de comunicações compartilhadas, comunicações de voz baseadas em VoIP e bate-papo entre usuários de dispositivos móveis e a equipe de suporte.

Requisitos de sistema do Remote Support

O software do Remote Support é instalado em computadores com base em Windows que atendem aos seguintes requisitos. Para conhecer os requisitos de porta, consulte Requisitos de porta.

Plataformas com suporte:

- Intel Xeon/Pentium 4 - 1 GHz no mínimo workstation class
- 512 MB de RAM no mínimo
- 100 MB de espaço livre em disco no mínimo

Sistemas operacionais compatíveis:

- 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
- Microsoft Windows 8
- Microsoft Windows 7

Para instalar o software de Suporte Remoto

1. Para baixar o instalador do Remote Support, vá para a Página de download do XenMobile 10 e faça login na sua conta.
2. Expanda **Ferramentas** e baixe o XenMobile Remote Support v9.
   O nome de arquivo do Remote Support é XenMobileRemoteSupport-9.0.0.35265.exe.
3. Clique duas vezes no instalador de Suporte Remoto e siga as instruções do assistente de instalação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para instalar o Suporte a partir da linha de comando

Digite o seguinte comando:

```
\*RemoteSupport\*.exe /S
```

RemoteSupport é o nome do programa de instalação. Por exemplo:

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

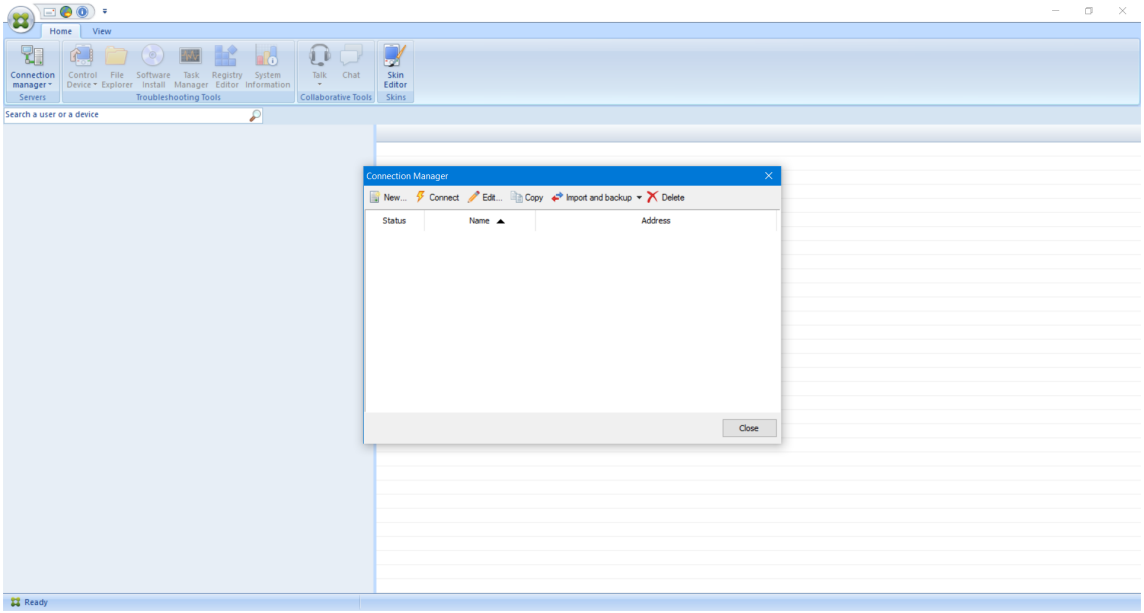
Você pode usar as variáveis a seguir ao instalar o Remote Support software:

- /S: para instalar o software do Remote Support com os parâmetros padrão.
- /D=dir: para especificar um diretório de instalação personalizado.

Para conectar-se ao Remote Support para XenMobile

Para estabelecer conexões de suporte remoto para dispositivos gerenciados, você deve adicionar uma conexão de Remote Support para um ou mais XenMobile Servers que gerenciam os dispositivos. Esta conexão é executada através de um túnel de aplicativo definido na Política de Túnel MDM, uma política para dispositivos Android e Windows Mobile/CE. Defina o túnel de aplicativo para poder conectar o Remote Support ao XenMobile. Para obter detalhes, consulte Política de dispositivo de encapsulamento de aplicativo.

1. Inicie o software do Remote Support e use suas credenciais do XenMobile para fazer login.
2. No **Connection Manager**, clique em **New**.



3. Na caixa de diálogo **Connection Configuration**, na guia **Server**, digite os seguintes valores:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a) Em **Configuration name**, digite um nome para a entrada de configuração.

b) Em **Server IP address or name**, digite o endereço IP ou o nome DNS do XenMobile Server.

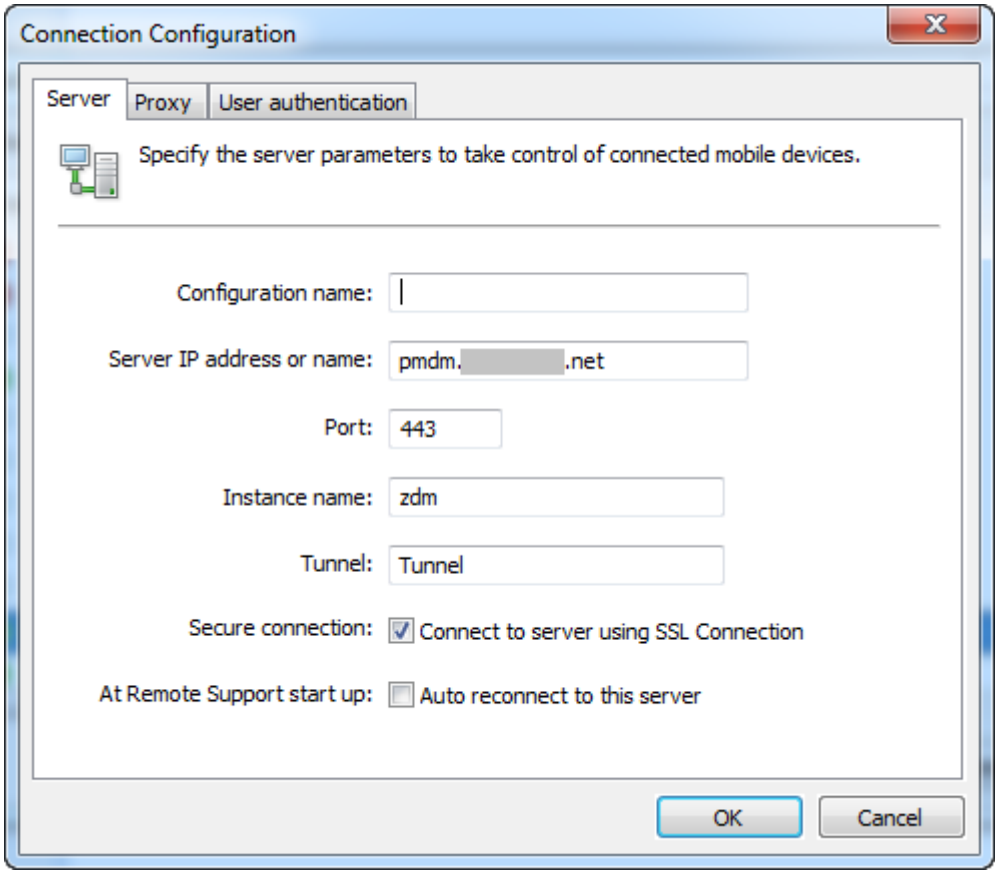
c) Em **Port**, digite um número de porta TCP, conforme definido na configuração de XenMobile Server.

d) Em **Instance name**, se o XenMobile for parte de uma implantação multilocatário, digite um nome de instância.

e) Em **Tunnel**, digite o nome da Política de Túnel.

f) Marque a caixa de seleção **Connect to server using SSL Connection**.

g) Marque a caixa de seleção **Auto reconnect to this server** para se conectar com o XenMobile Server configurado toda vez que o aplicativo Remote Support for iniciado.



4. Na guia **Proxy**, selecione **Use a http proxy server** e, em seguida, insira as seguintes informações:

a) Em **Proxy IP Address**, digite o endereço IP do servidor proxy.

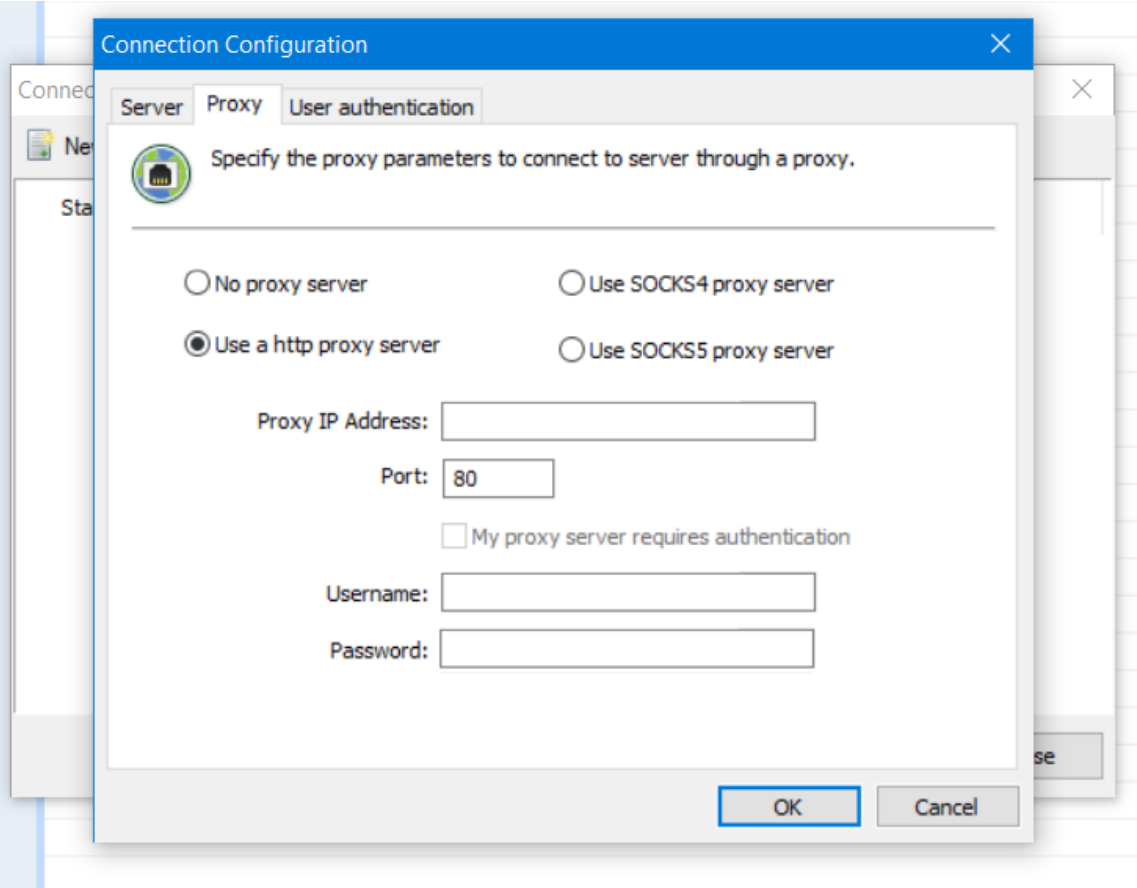
b) Em **Port**, digite um número de porta TCP usada pelo proxy.

c) Marque a caixa de seleção **My proxy server requires authentication** se o servidor proxy exigir autenticação para permitir tráfego.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

d) Em **Username**, digite o nome do usuário a ser autenticado no servidor proxy.

e) Em **Password**, digite a senha a ser autenticada no servidor proxy.



5. Na guia **User Authentication**, marque a caixa de seleção **Remember my login and password** e insira as credenciais.
6. Clique em **OK**.

Para se conectar ao XenMobile, clique duas vezes na conexão que você criou e, em seguida, digite o nome do usuário e a senha que você configurou para a conexão.

Para habilitar o suporte remoto para dispositivos Samsung KNOX

Crie uma política de Suporte Remoto no XenMobile para conceder a você acesso remoto aos dispositivos Samsung KNOX. Você pode configurar dois tipos de suporte:

- **Básico:** permite que você exiba informações de diagnóstico sobre o dispositivo. Por exemplo, informações do sistema, os processos em execução, o gerenciador de tarefas (uso de memória e da CPU) e o conteúdo da pasta do software instalado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Premium:** permite que você controle remotamente a tela de dispositivo. Por exemplo, controle de cores da janela, estabelecer uma sessão de VoIP entre o suporte técnico e o usuário e estabelecer uma sessão de bate-papo entre o suporte técnico e o usuário.

  O suporte com Premium exige que você configure a política de dispositivo de chave de licença MDM Samsung no console XenMobile. Quando você configurar essa política, selecione somente a plataforma **Samsung KNOX**. No caso da plataforma Samsung SAFE, a chave ELM é implantada automaticamente nos dispositivos Samsung quando eles se registram no XenMobile. Portanto, não selecione a plataforma Samsung SAFE no caso dessa política. Para obter detalhes, consulte Chave de licença MDM Samsung.

Para obter informações sobre como configurar a Política de Suporte Remoto, consulte Suporte remoto à política de dispositivo.

Para usar uma sessão de Remote Support

Após iniciar o Remote Support, o lado esquerdo da janela do aplicativo Remote Support apresenta grupos de usuários do XenMobile, conforme definido no console do XenMobile. Por padrão, aparecem apenas grupos que contêm usuários que estão conectados no momento. Você pode ver o dispositivo para cada usuário ao lado da entrada respectiva.

1. Para ver todos os usuários, expanda cada grupo na coluna à esquerda.
   Esses usuários conectados no momento ao XenMobile Server são indicadas por um ícone verde.
2. Para exibir todos os usuários, incluindo aqueles que não estão conectados no momento, clique em **View** e selecione **Non-connected devices**.
   Os usuários não conectados são exibidos sem o pequeno ícone verde.

Os dispositivos conectados ao XenMobile Server, mas que não foram atribuídos a um usuário, aparecem em modo anônimo. (A sequência **Anonymous** aparece na lista.) Você pode controlar esses dispositivos como o dispositivo de um usuário conectado.

Para controlar um dispositivo, selecione o dispositivo clicando na linha e, em seguida, em **Control Device**. Uma representação do dispositivo é exibida na janela do Remote Control. Você pode interagir com um dispositivo controlado das seguintes maneiras:

- Controlar a tela do dispositivo, incluindo controle com cores, na janela principal ou em janela flutuante separada.
- Criar uma sessão de Voice-over-IP (VoIP) entre o suporte técnico e o usuário. Definir as configurações do VoIP.
- Estabelecer uma sessão de bate-papo com o usuário.
- Acessar o dispositivo gerenciador de tarefas, para gerenciar itens como o uso da memória, o uso da CPU e aplicativos em execução.
- Explorar os diretórios locais do dispositivo móvel. Transferir arquivos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Editar o registro de dispositivo em dispositivos móveis do Windows.
- Exibir informações de sistema do dispositivo e todos os softwares instalados.
- Atualizar o status de conexão do dispositivo móvel com o XenMobile Server.

Syslog

April 15, 2019

Você pode configurar o XenMobile para enviar arquivos de log para um servidor de logs do sistema (syslog). Você precisa do nome do host ou do endereço IP do servidor.

Syslog é um protocolo padrão de log 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 dados de usuário (UDP) para transferência de dados. Os eventos de Administrador e os eventos de Usuário são gravados.

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 relativo ao 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 da mensagem
- O nível de log associado a um evento (Crítico, Erro, Notificação, Aviso, Informativo, Depuração, Alerta ou Emergência)
- As informações da mensagem

O XenMobile usa o log4j syslog appender para enviar mensagens de syslog formatadas RFC5424. Os dados da mensagem em uma mensagem syslog é texto simples e não tem nenhum formato específico.

Você pode usar essas informações para analisar a origem do alerta e executar a ação corretiva, se necessário.

1. No console 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. Defina estas configurações:
    - **Servidor:** digite o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do seu servidor syslog.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

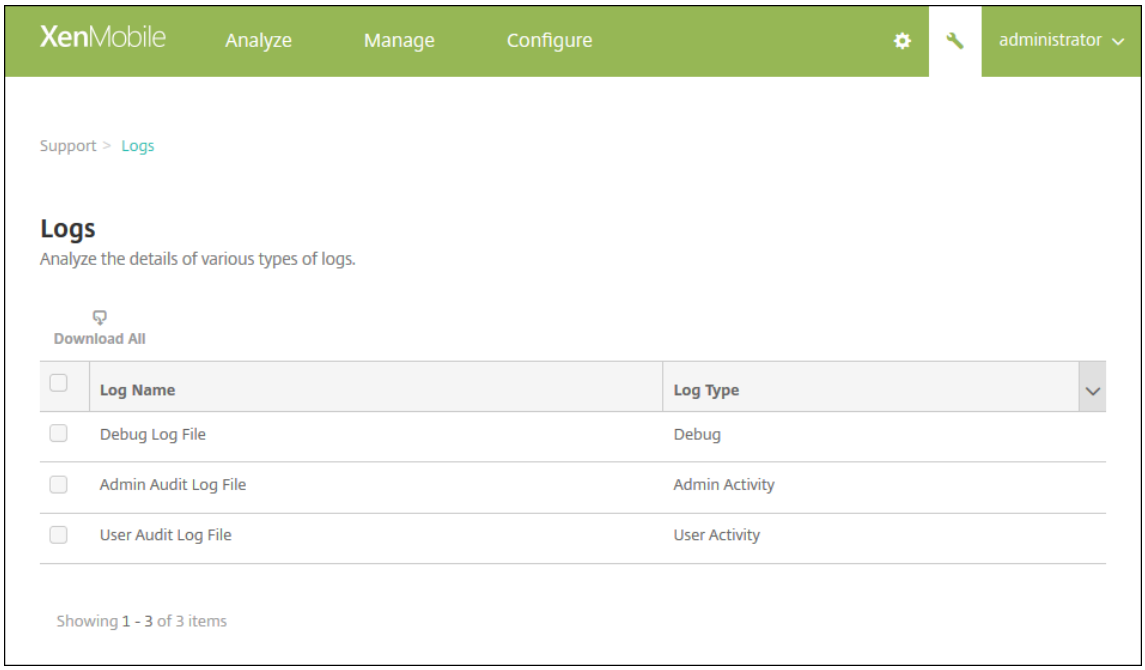
- **Porta:** digite o número da porta. Por padrão, a porta é definida como 514.
- **Informações para log:** marque ou desmarque **Logs do sistema** e **Auditoria**.
  - Logs do sistema contêm as ações realizadas pelo XenMobile.
  - Logs de auditoria contêm um registro cronológico das atividades do sistema relativo ao XenMobile.
  - Logs de depuração para o XenMobile.

4. Clique em **Salvar**.

Exibir e analisar arquivos de log no XenMobile

March 6, 2019

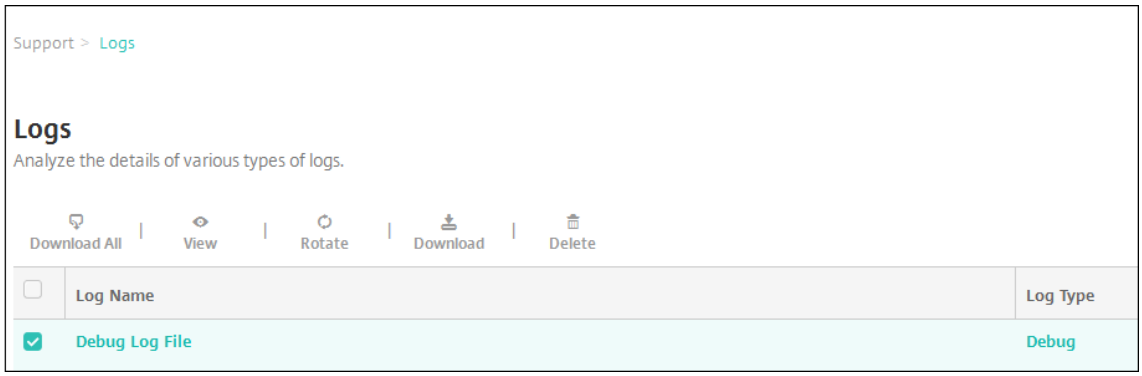
1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é aberta.
2. Em **Operações de log**, clique em **Logs**. A página **Logs** é exibida. Logs individuais são exibidos em uma tabela.



3. Selecione o log que você deseja exibir:
   - Os Arquivos de Log de Depuração contêm informações úteis para o suporte da Citrix, como mensagens de erro e ações relacionadas.
   - Os Arquivos de Log de Auditoria do Administrador contêm informações de auditoria sobre as atividades no console XenMobile.
   - Os Arquivos de Log de Auditoria do Usuário contêm informações relacionadas aos usuários configurados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Use as ações na parte superior da tabela para baixar tudo, exibir, girar, baixar um único log ou excluir o log selecionado.

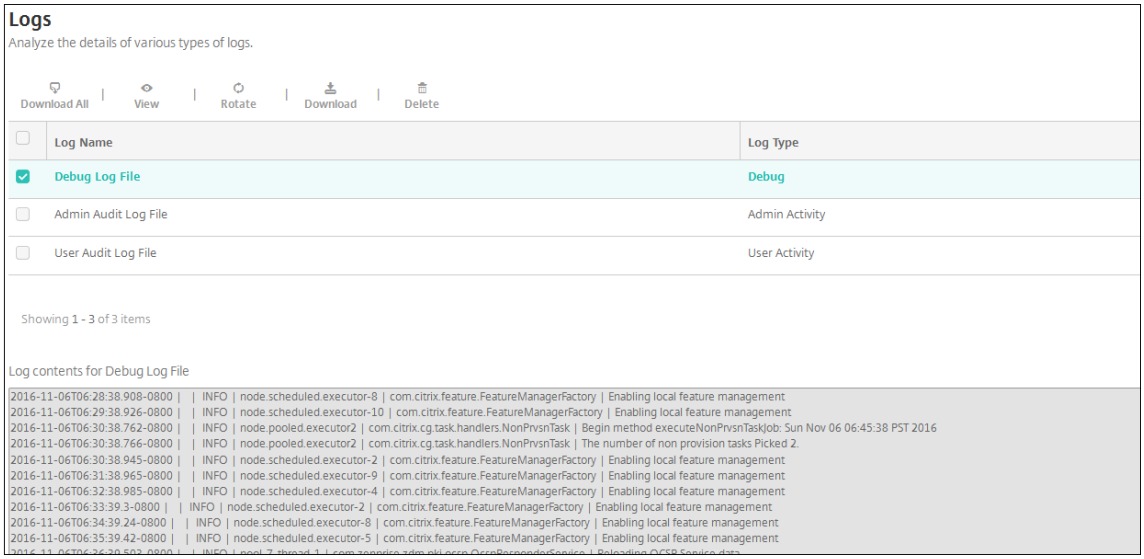


> Nota:
>
> - Se você selecionar mais de um arquivo de log, somente as opções **Baixar todos** e **Girar** estarão disponíveis.
> - Se você tiver servidores XenMobile em cluster, poderá exibir somente os logs do servidor ao qual está conectado. Para ver os logs de outros servidores, use uma das opções de download.

5. Você pode optar por um dos seguintes procedimentos:

   - **Baixar todos:** o console baixa todos os logs presentes no sistema (incluindo de depuração, auditoria de administração, auditoria de usuário, logs do servidor e assim por diante).
   - **Exibir:** mostra o conteúdo do log selecionado abaixo da tabela.
   - **Girar:** Arquiva o arquivo de log atual e cria um novo arquivo para capturar entradas de log. Uma caixa de diálogo aparece quando um arquivo de log é arquivado; clique em Girar para continuar.
   - **Baixar:** O console baixa somente o único tipo de arquivo de log selecionado; ele também baixa todos os logs arquivados desse mesmo tipo.
   - **Excluir:** Remove permanentemente os arquivos de log selecionados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Ferramenta XenMobile Analyzer

April 15, 2019

O XenMobile Analyzer é uma ferramenta baseada em nuvem que você pode usar para diagnosticar e resolver problemas relacionados do XenMobile relacionados à configuração e outros recursos. A ferramenta verifica se há registro do dispositivo ou de usuário e problemas de autenticação no seu ambiente do XenMobile.

Configure a ferramenta para apontar para o XenMobile Server e forneça informações, como tipo de implantação de servidor, plataforma móvel, tipo de autenticação e as credenciais do usuário. Em seguida, a ferramenta se conecta ao servidor e examina o ambiente quanto a problemas de configuração. Se o XenMobile Analyzer descobrir problemas, a ferramenta fornece recomendações para corrigir os problemas.

Características principais

- Microsserviço seguro e baseado em nuvem para resolver todos os problemas relativos ao XenMobile.
- Fornece recomendações precisas para resolver problemas de configuração do XenMobile.
- Menos chamadas ao suporte e solução de problemas acelerada de ambientes do XenMobile.
- Suporte de dia zero para versões para XenMobile Server.
- Agendamento de verificação de integridade com frequência diária ou semanal.
- Verificações de configuração do NetScaler.
- O Secure Web testa a acessibilidade a sites da intranet.
- Verificações de serviço de descoberta automática do Secure Mail.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

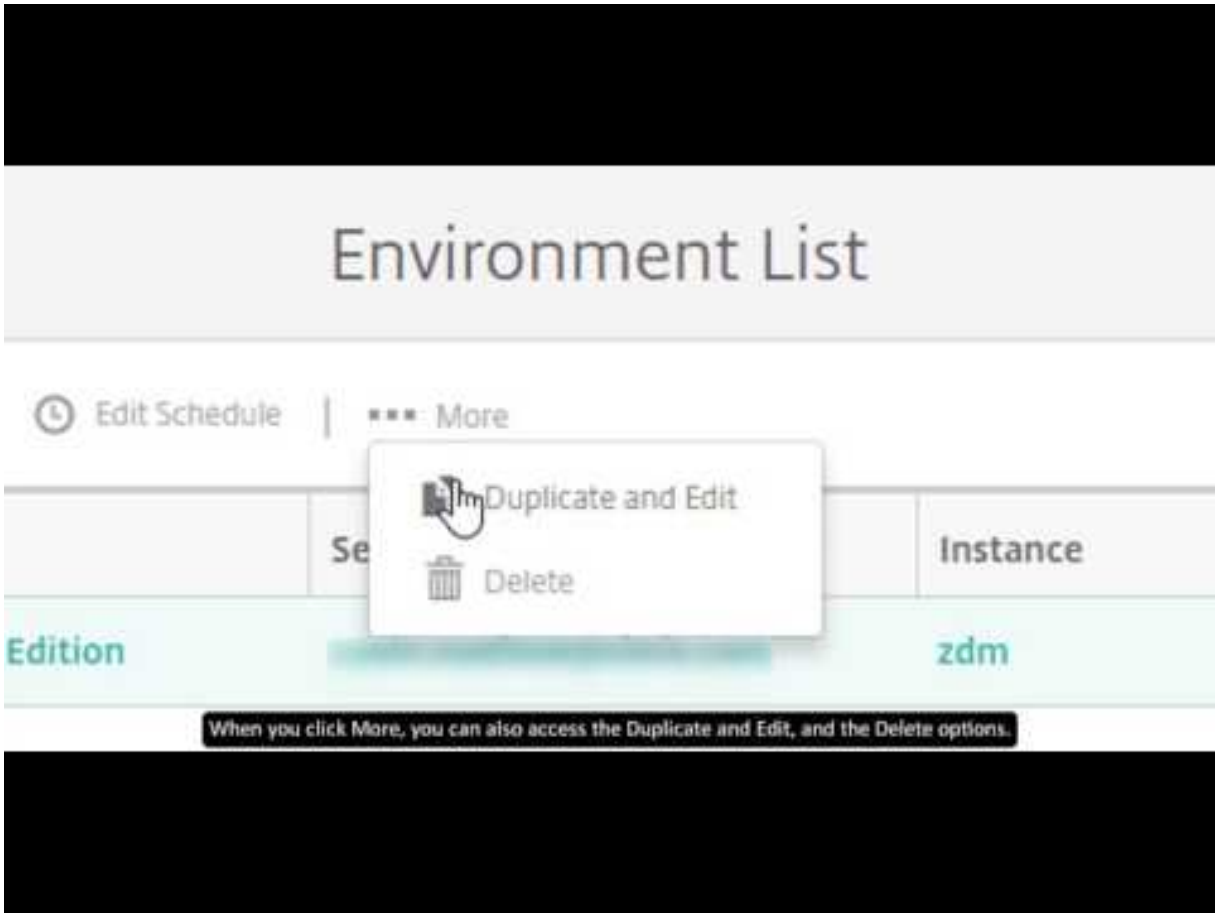
- Verificações de logon único (SSO) do ShareFile.

Novidades

- O Relatório de configuração do NetScaler exibe uma notificação de selo indicando o número de recomendações. As recomendações baseiam-se nas verificações de Configuração essencial em um NetScaler Gateway específico.
- Os ícones na barra de navegação global da página Lista do ambiente de teste foram reordenadas para uma melhor experiência do usuário.

O vídeo a seguir destaca as alterações de navegação na interface do usuário.

Citrix XenMobile Analyzer: nova interface do usuário da lista de ambientes



> Nota:
>
> Esse vídeo não contém som de áudio. Ele é melhor visualizado no modo de tela inteira.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

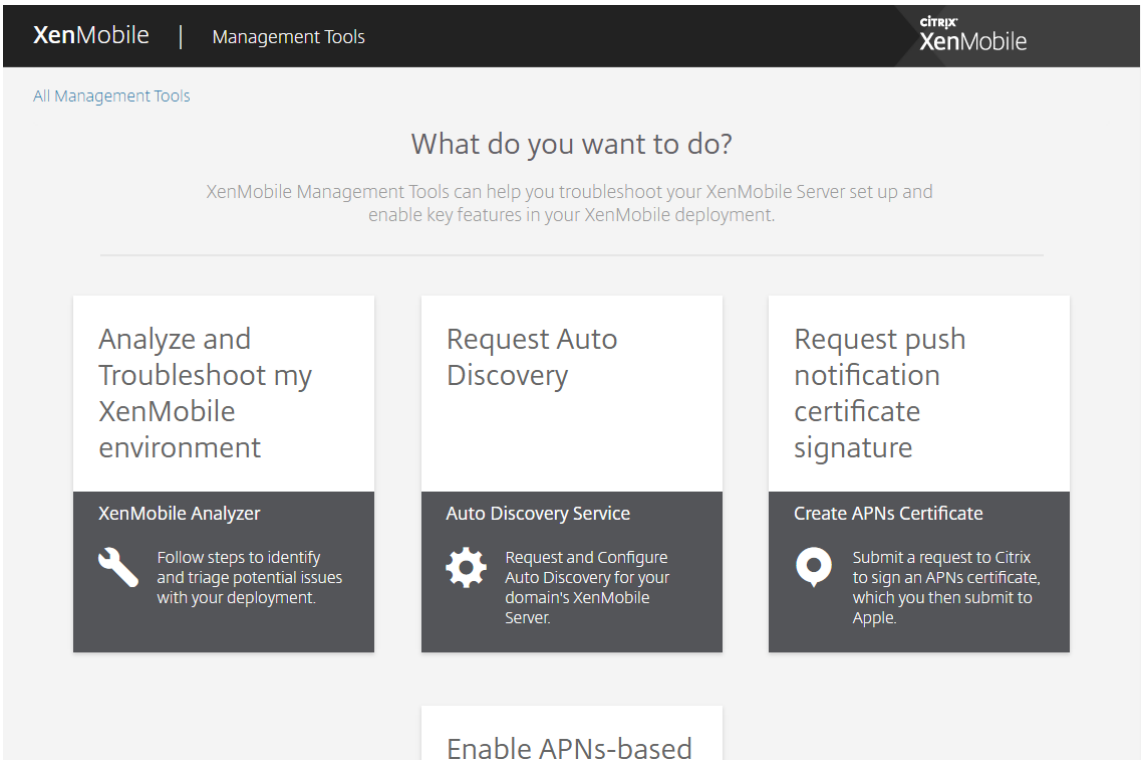
Acessar e iniciar o XenMobile Analyzer

Pré-requisitos

Produto	Versão com suporte
Servidor XenMobile	10.1.0 e posterior
NetScaler Gateway	10.5 e versões posteriores
Simulação de registro de cliente	iOS e Android

Acesse o XenMobile Analyzer usando um destes métodos:

- No console XenMobile, clique no ícone de engrenagem no canto superior direito para abrir a página **Solução de problemas e suporte**.
- Use suas credenciais My Citrix para acessar a ferramenta em https://xenmobiletools.citrix.com. Na página XenMobile Management Tools exibida, para iniciar o XenMobile Analyzer, clique em **Analyze and Troubleshoot my XenMobile Environment**.



O XenMobile Analyzer contém cinco opções criadas para guiar você durante o processo de separação e para reduzir o número de tíquete de suporte. As opções podem reduzir os custos para todos.

As opções são as seguintes:

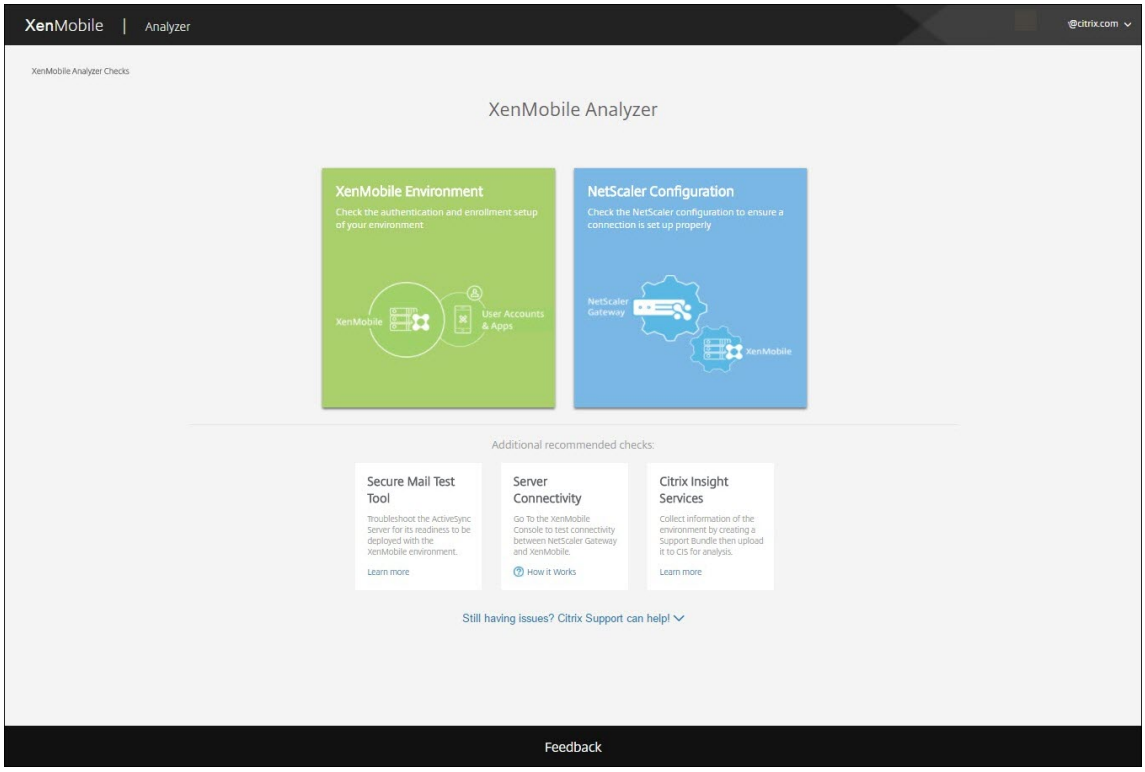
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Environment Check:** Esta etapa o orienta na configuração de testes para verificar a configuração em caso de problemas. A etapa também fornece recomendações e soluções para problemas no dispositivo, registro de usuário e autenticação.
- **NetScaler Check:** Esta etapa o orienta na verificação das suas configurações do NetScaler para preparação de implantação do XenMobile.
- **Advanced Diagnostics:** Esta etapa fornece informações sobre como usar o Citrix Insight Services para encontrar mais problemas que a verificação de ambiente possa ter deixado de detectar.
- **Secure Mail Readiness:** Esta etapa direciona você a baixar e executar o aplicativo XenMobile Exchange ActiveSync Test. O aplicativo resolve os problemas de servidores ActiveSync para que a sua prontidão seja implantada com um ambiente XenMobile.
- **Server Connectivity Checks:** Esta etapa instrui você a testar a conectividade dos seus servidores.
- **Contact Citrix Support:** Esta etapa conecta você ao site onde você poderá criar um caso de suporte da Citrix.

As seções a seguir descrevem cada opção com mais detalhes.

Execução de uma verificação de ambiente

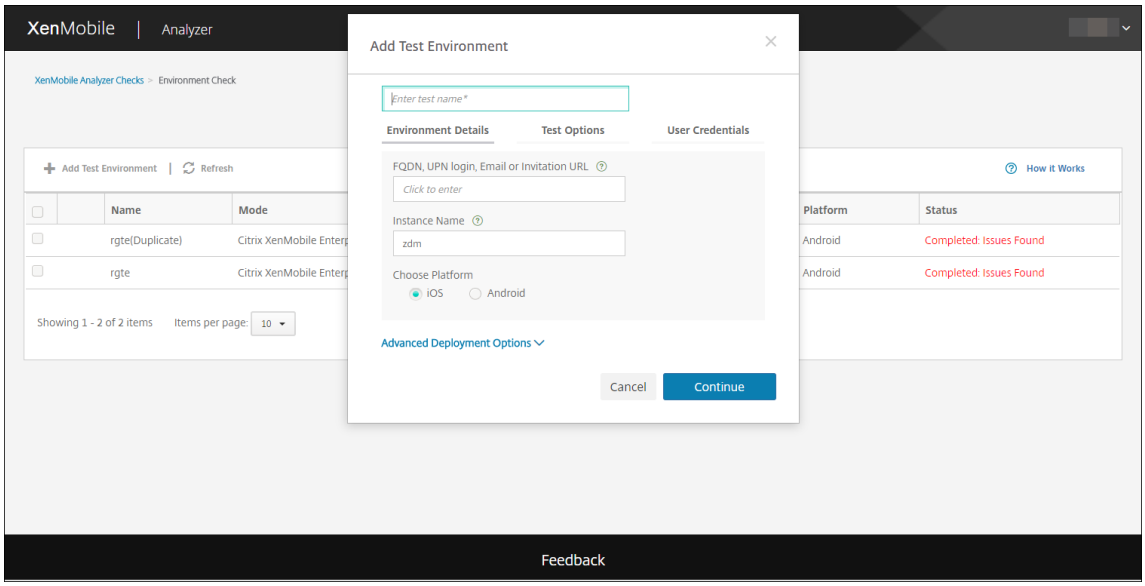
1. Faça login no XenMobile Analyzer e clique em **XenMobile Environment**.



2. Clique em **Add Test Environment**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Na caixa de diálogo **Add Test Environment**, faça o seguinte:



   a) Forneça um nome exclusivo para o teste que o ajude a identificar o teste no futuro.

   b) Em **FQDN, UPN login, Email or URL Invitation**, digite as informações usadas para acessar o servidor.

   c) Em **Instance Name**, se você usar uma instância personalizada, poderá fornecer esse valor.

   d) Em **Choose Platform**, selecione **iOS** ou **Android** como a plataforma para teste.

   e) Se você expandir **Advanced Deployment Options**, na lista **Deployment Mode**, você pode selecionar o modo de implantação do XenMobile 1. As opções disponíveis são **Enterprise (MDM + MAM)**, **App Management (MAM)** ou **Device Management (MDM)**.

   f) Clique em **Continue**.

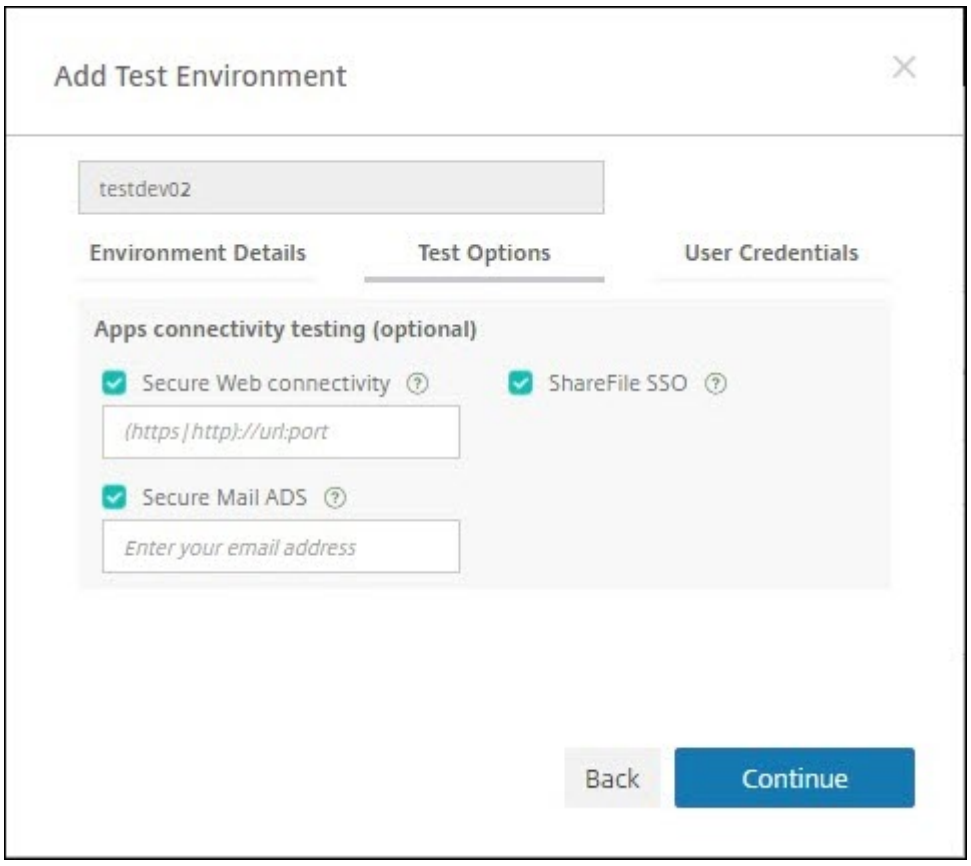
4. Na guia **Test Options**, escolha um ou mais dos seguintes testes e clique em **Continue**.

   a) **Conectividade do Secure Web**. Forneça uma URL de intranet. A ferramenta testa a acessibilidade da URL. Isso detecta se há problemas de conectividade que possam ocorrer no aplicativo Secure Web ao tentar acessar URLs de intranet.

   b) **ADS do Secure Mail**. Forneça um ID de email de usuário. Essa ID é usada para testar a detecção automática do Microsoft Exchange Server em seu ambiente XenMobile. Ele detecta se há problemas relacionados à detecção automática de Secure Mail.

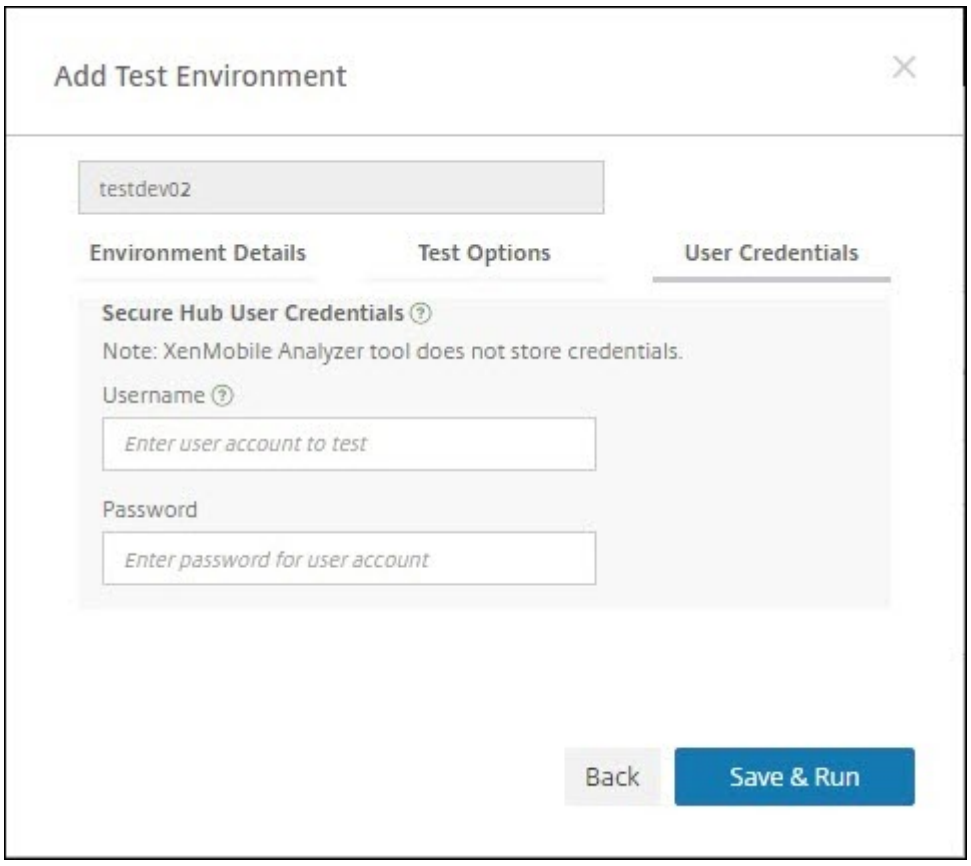
   c) **ShareFile SSO**. Se selecionado, o XenMobile Analyzer testará se a resolução DNS do ShareFile tem êxito. A ferramenta também verifica se o logon único (SSO) do ShareFile é compatível com as credenciais de usuário fornecidas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Na guia **User Credentials**, dependendo da configuração do servidor, você verá campos diferentes. Os campos possíveis são **Username**, **Username e Password** ou **Username, Password** e **Enrollment PIN**.

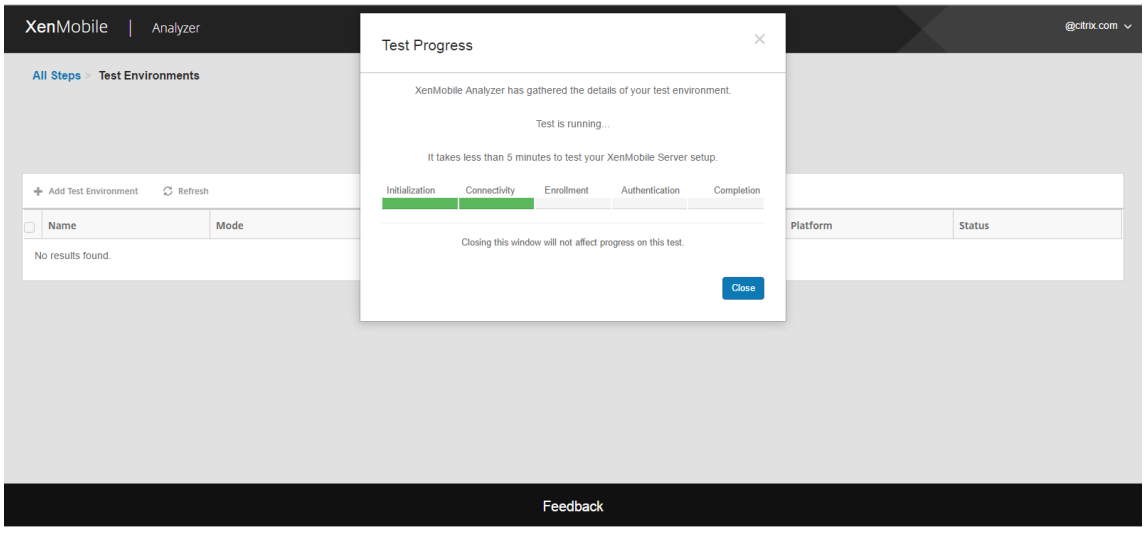
© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Clique em **Save & Run** para iniciar os testes.

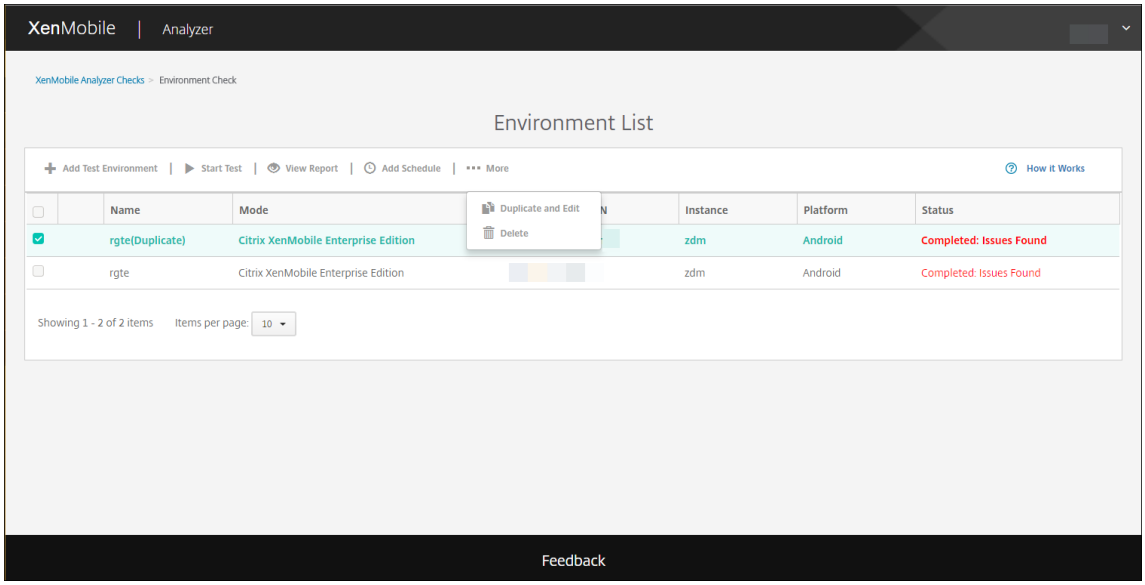
   Uma notificação de progresso é exibida. Você pode deixar a caixa de diálogo de progresso aberta ou fechar a caixa de diálogo a execução dos testes continua.

   Os testes com aprovação aparecem em verde. Testes sem aprovação aparecem em vermelho.



   Depois de fechar a caixa de diálogo de progresso, você poderá retornar à página **Environments List**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A página **Results** mostra resultados do teste, recomendações e resultados.

7. Clique no ícone **View Report** para ver resultados do teste.

   Se as recomendações tiverem um artigo da Base de Conhecimento da Citrix associado, esse artigo aparecerá nesta página.

8. Clique na guia **Results** para exibir a categoria e os testes que a ferramenta executou, com seus resultados.

   a) Para baixar o relatório, clique em **Download Report**.

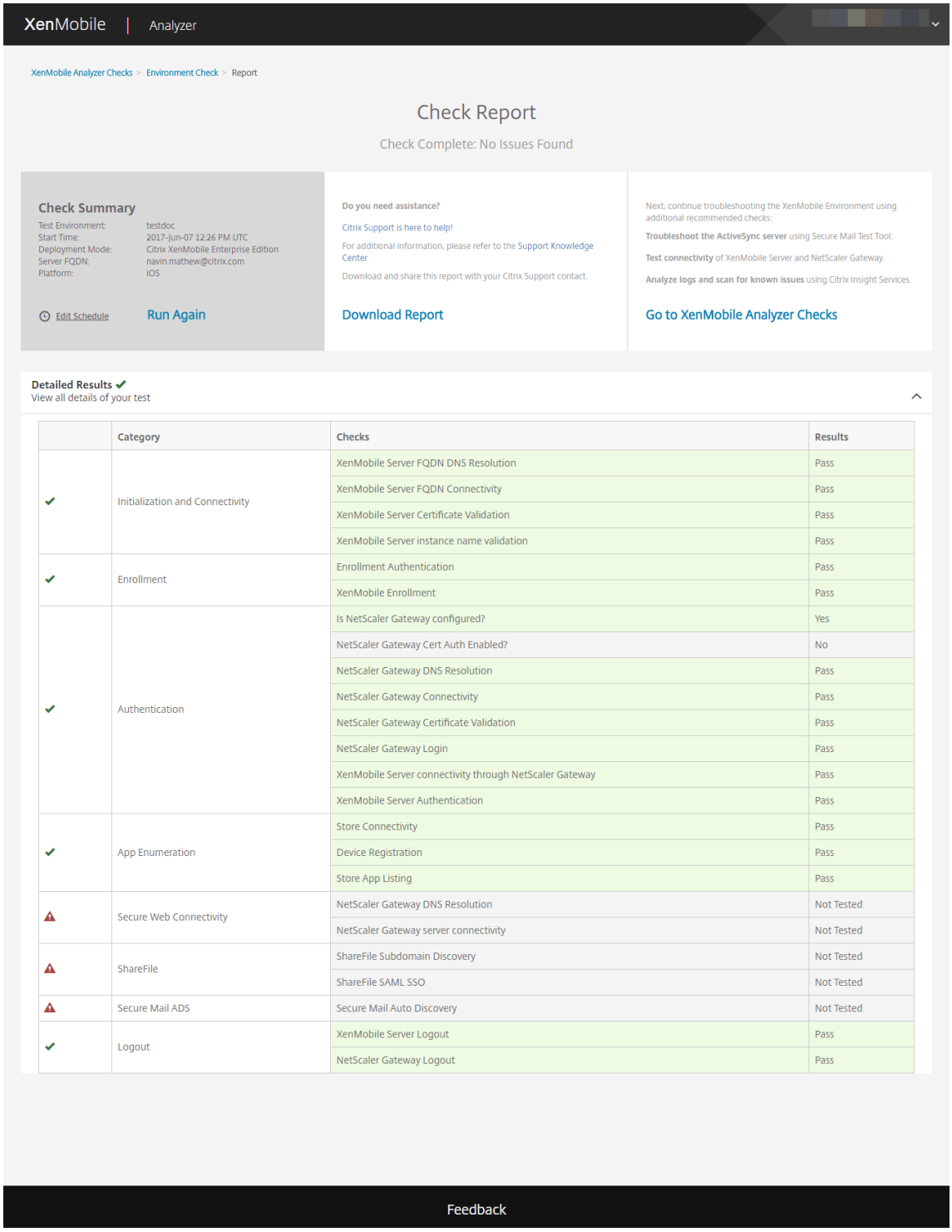
   b) Para retornar à lista de ambientes de teste, clique em **Environment Check**.

   c) Para executar novamente o mesmo teste, clique em **Run Again**.

   d) Se você deseja executar novamente outro teste, volte para **Test Environments**, selecione o teste e clique em **Start Test**.

   e) Para selecionar outra opção do XenMobile Analyzer, clique em **Go To XenMobile Analyzer Checks**.

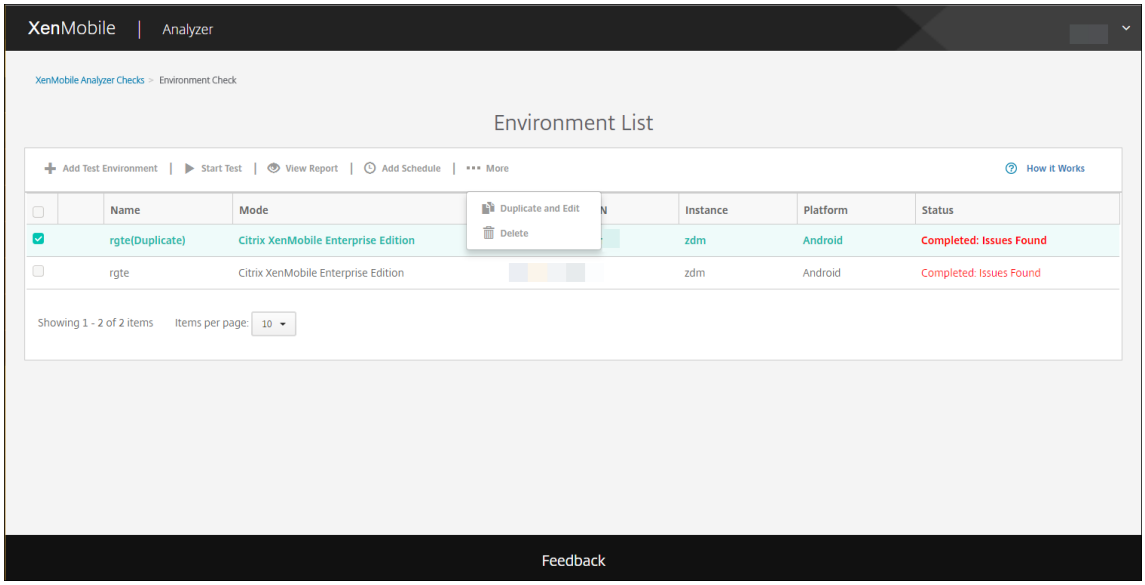
© 1999-2019 Citrix Systems, Inc. All rights reserved.

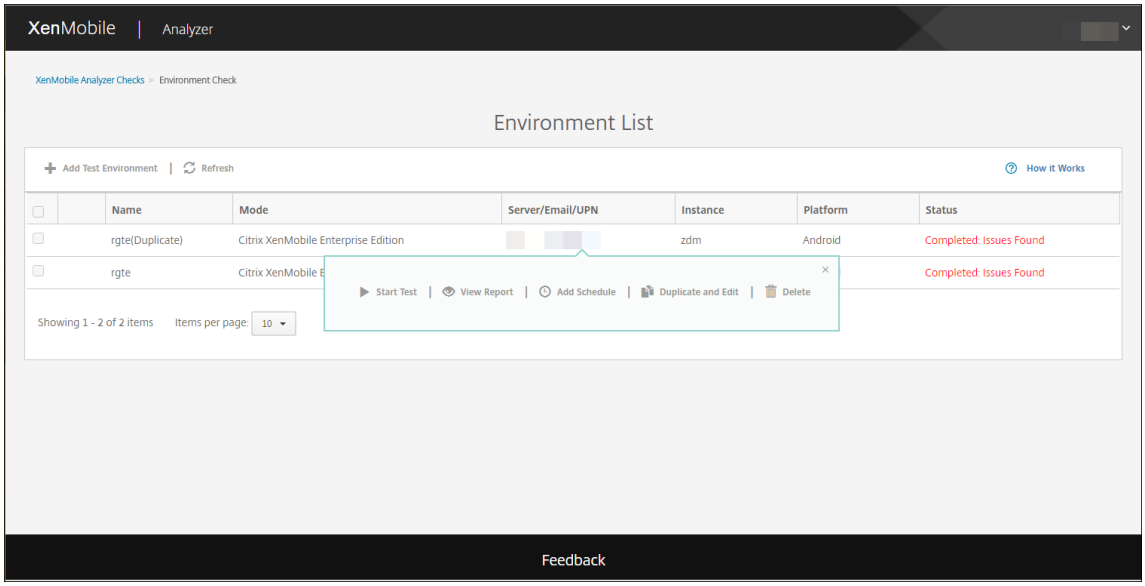


9. Na página ambientes de teste, você pode copiar e editar testes. Para fazer isso, selecione um teste e, em seguida, clique em **More** e selecione **Duplicate and Edit**.

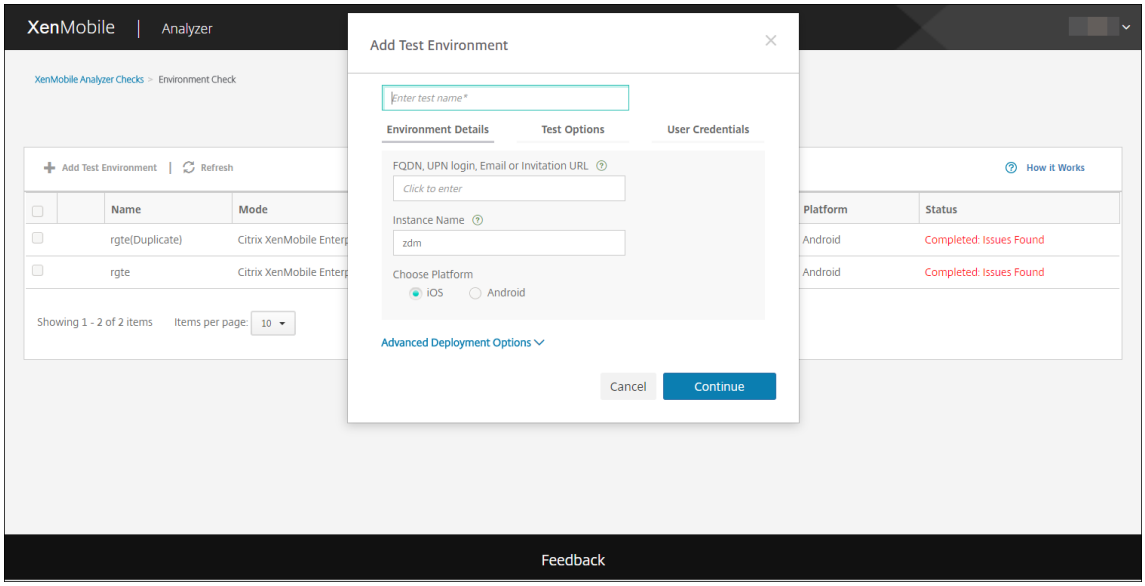
   Uma cópia do teste selecionada é criada e a caixa de diálogo Adicionar ambiente de teste é aberta, permitindo que você modifique o novo teste.

© 1999-2019 Citrix Systems, Inc. All rights reserved.





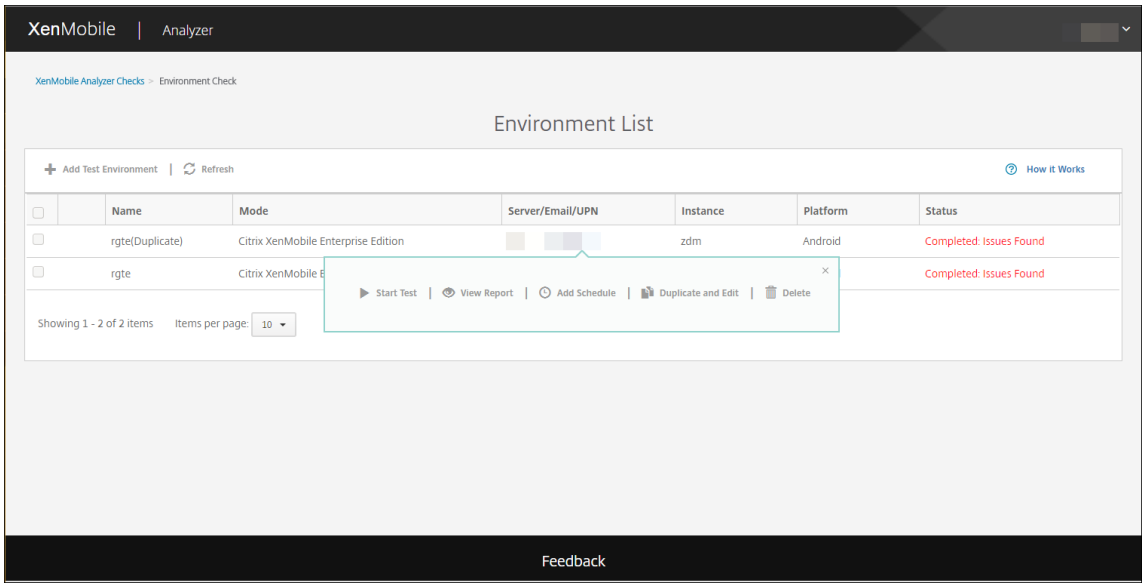
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Adicionar um agendamento para verificações de ambiente

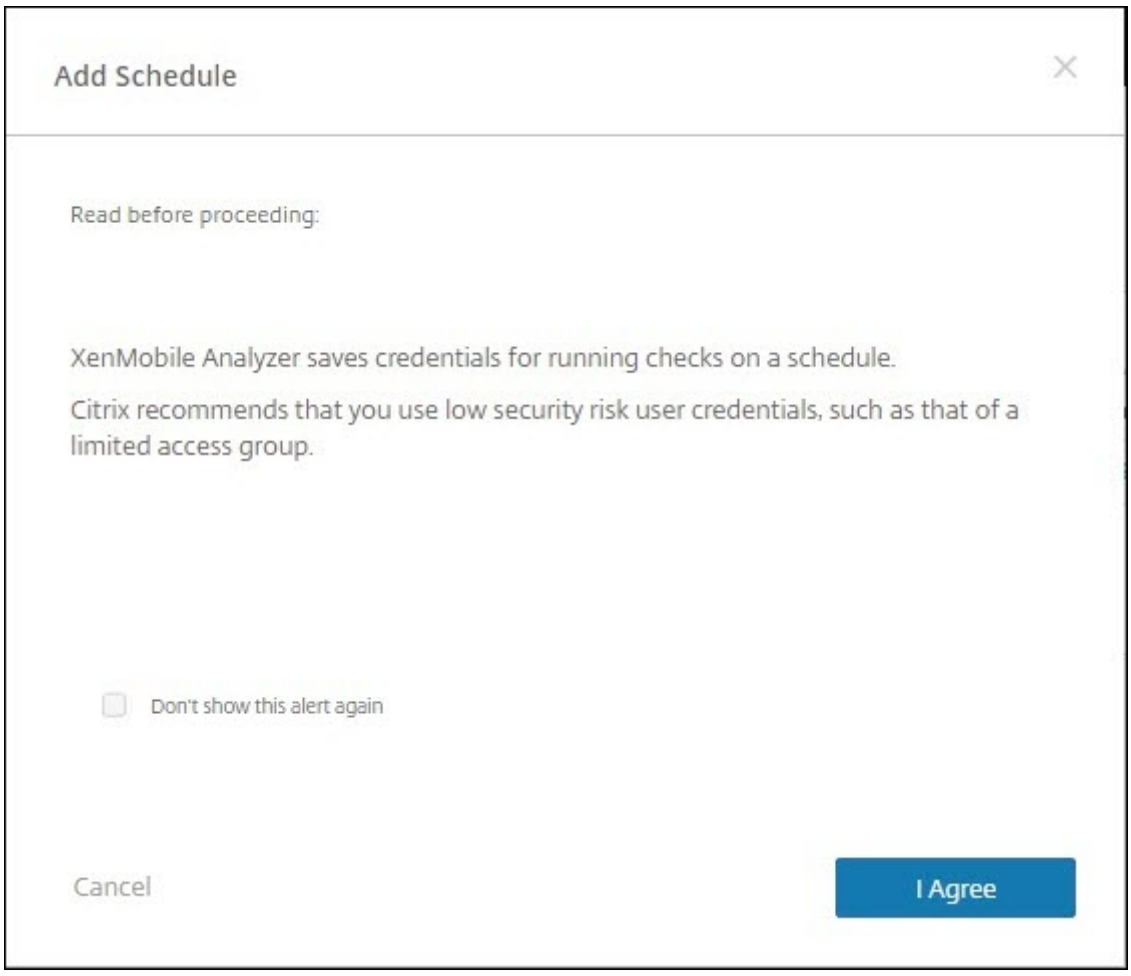
Você pode configurar testes para executar em um agendamento automático com resultados enviados para uma lista de usuários que você configura.

1. Na página **Environment List**, selecione o ambiente para a qual você deseja agendar e clique em **Add Schedule**.



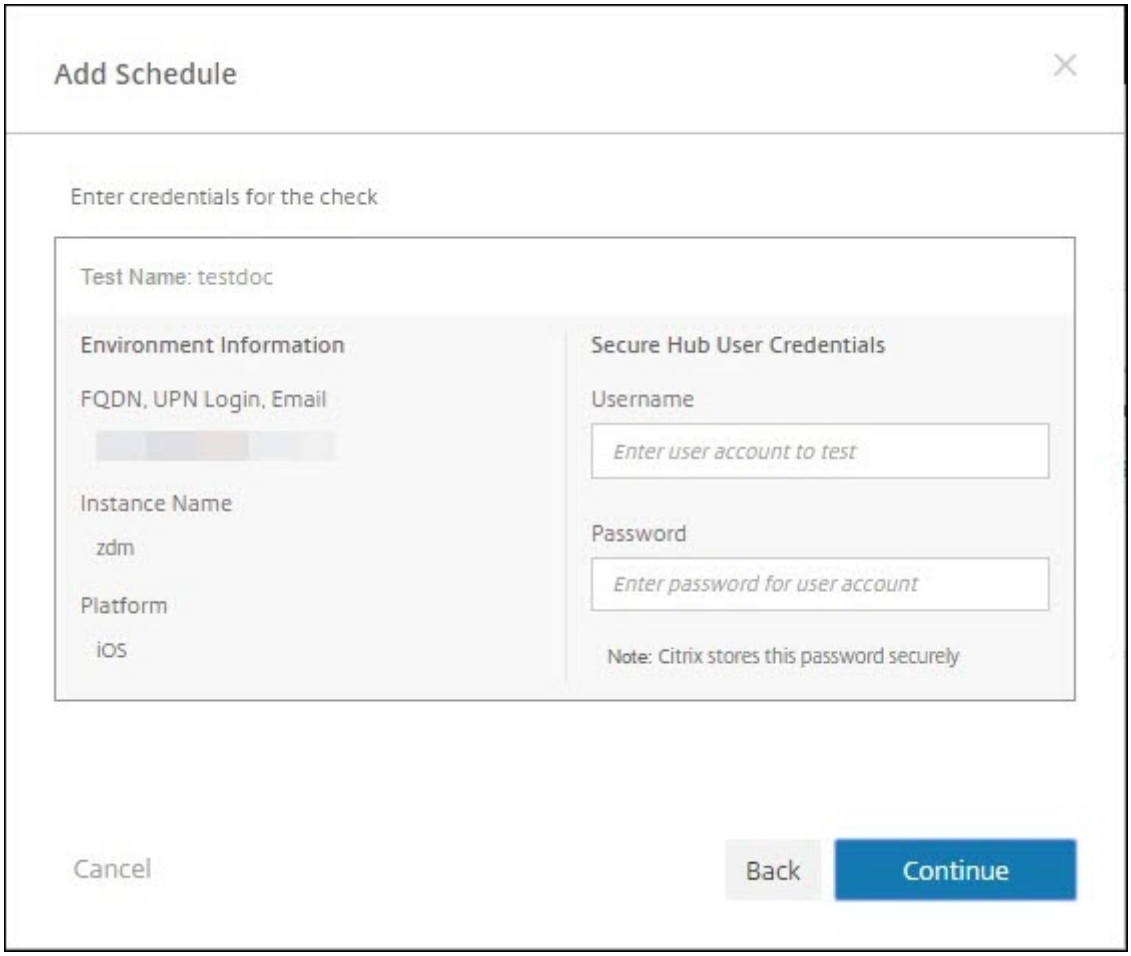
2. A janela **Add Schedule** exibe uma mensagem para avisar você que o XenMobile Analyzer salva as credenciais para executar testes em um agendamento. A Citrix recomenda que você use uma conta com acesso limitado para executar testes programados. Clique em **I Agree**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



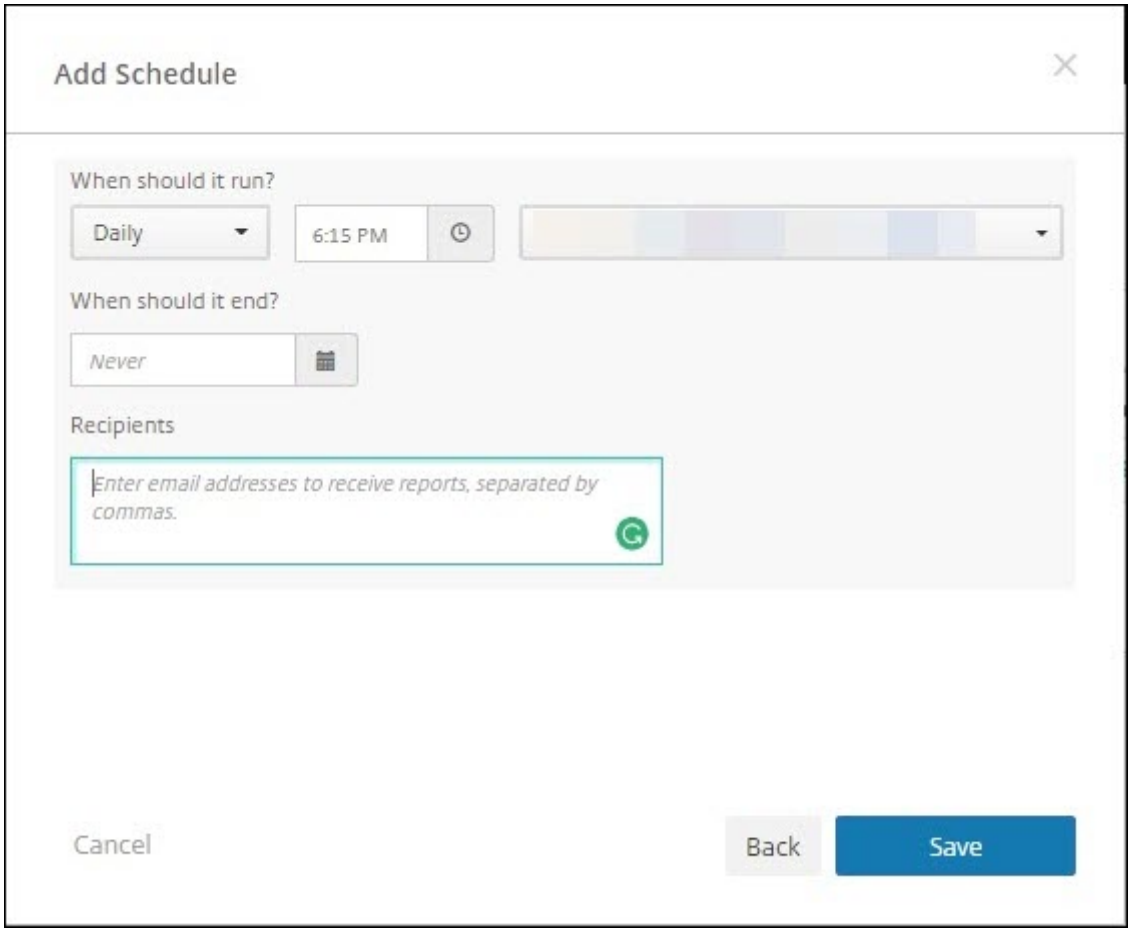
3. Digite um **Nome de usuário** e **Senha** para executar o teste.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

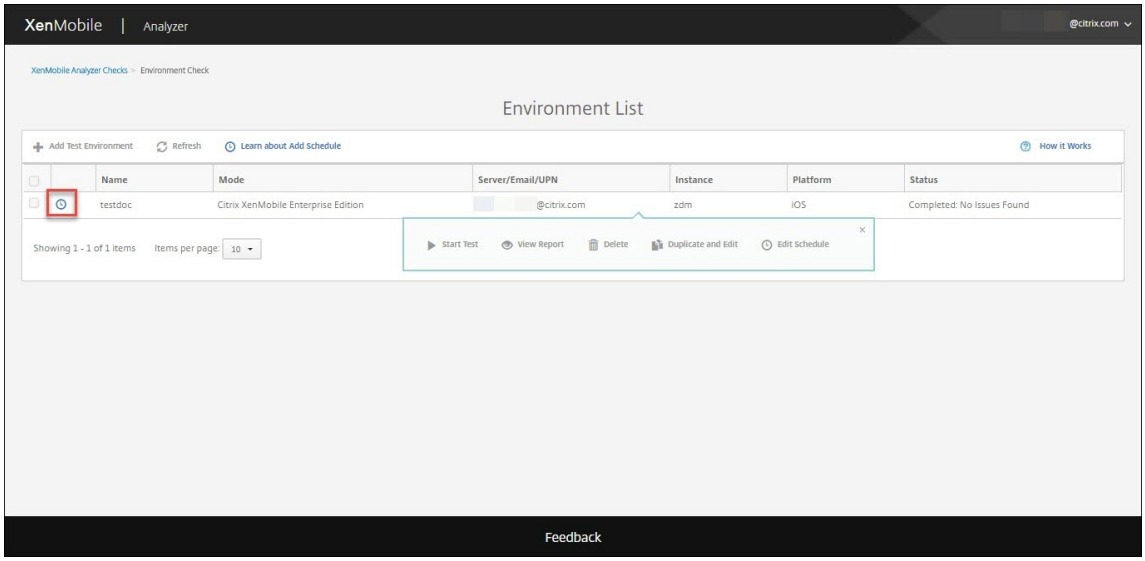


4. Configure um agendamento para execução do teste. Selecione **Daily** ou **Weekly** no menu suspenso. Selecione uma hora do dia para executar o teste e um fuso horário. Use o botão para selecionar uma data para que o teste agendado pare de ser executado ou deixe em branco para que o teste seja executado indefinidamente. Forneça uma lista de endereços de email para receber relatórios, separados por vírgulas. Clique em **Salvar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



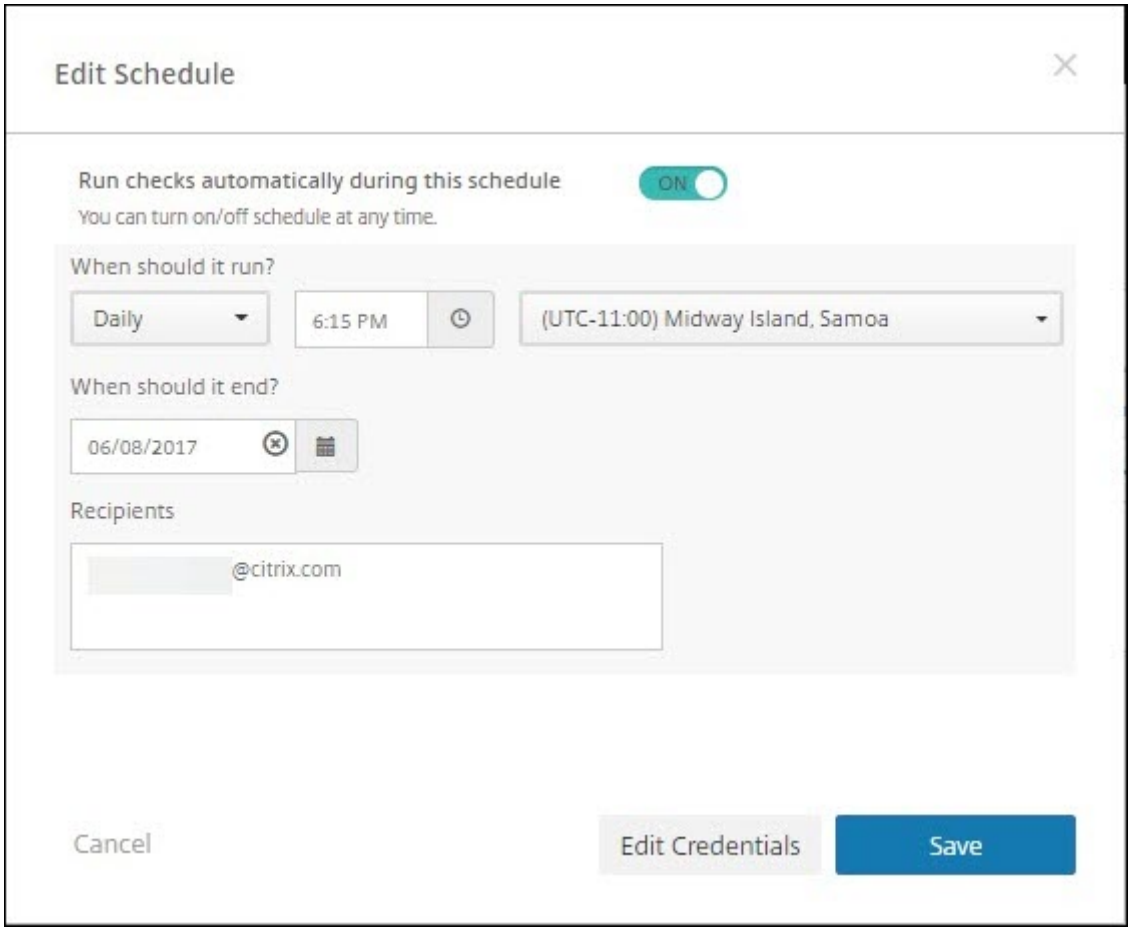
5. Um símbolo de relógio à esquerda do seu teste indica que está configurado um agendamento. Se você selecionar o seu teste, você pode clicar em **Edit Schedule** para alterar quando o teste for executado.



6. Nessa janela, você pode alterar quando o teste deve ser executado. Você também pode

© 1999-2019 Citrix Systems, Inc. All rights reserved.

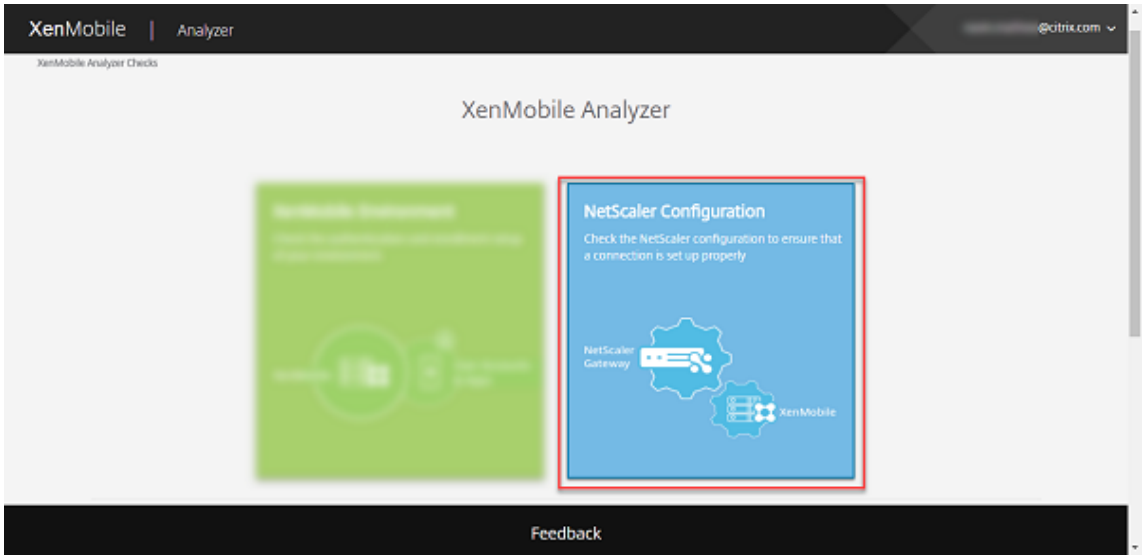
desativá-lo, clicando no botão na parte superior. Clique em **Salvar** quando terminar.



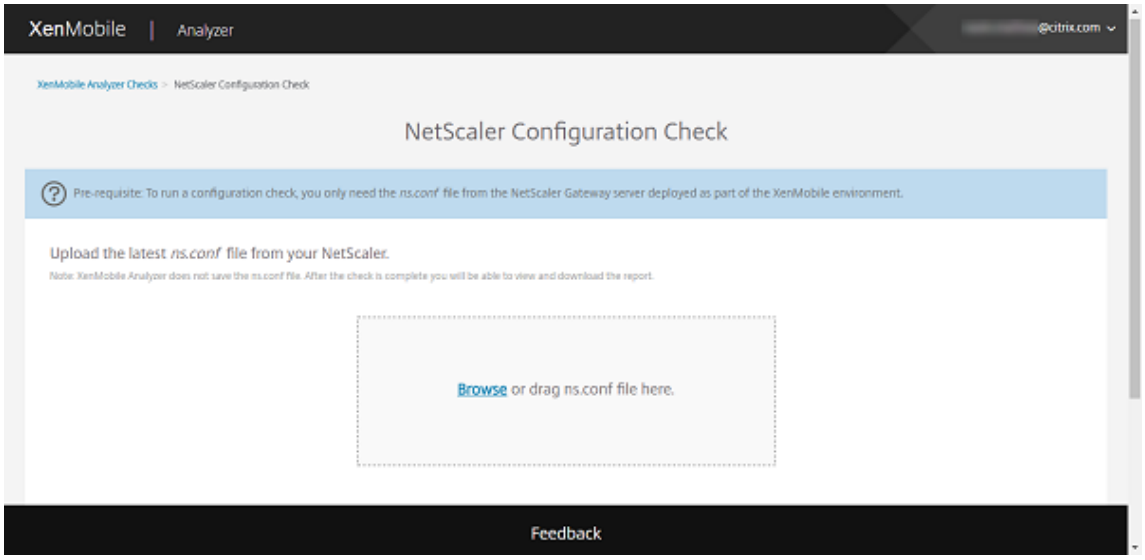
Executar uma verificação do NetScaler

1. Faça login no XenMobile Analyzer e, em seguida, clique em **Configuração do NetScaler**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



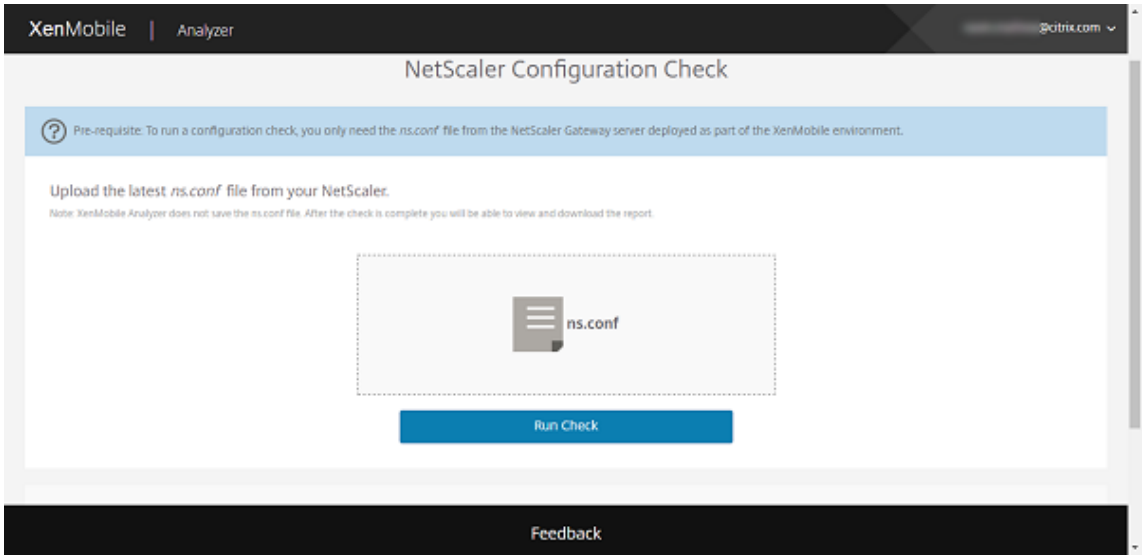
2. Carregue o arquivo ns.conf mais recente da sua instância do NetScaler. Você pode arrastar o arquivo para a caixa de upload ou clicar em **Procurar** para procurar e adicionar o arquivo ns.conf. Para obter mais informações sobre como você pode baixar o arquivo ns.conf mais recente, consulte o Support Knowledge Center.



> Nota:
>
> O XenMobile Analyzer não salva o arquivo ns.conf. Depois que a verificação estiver concluída, você pode exibir e baixar o relatório.

3. Clique em **Run Check**.

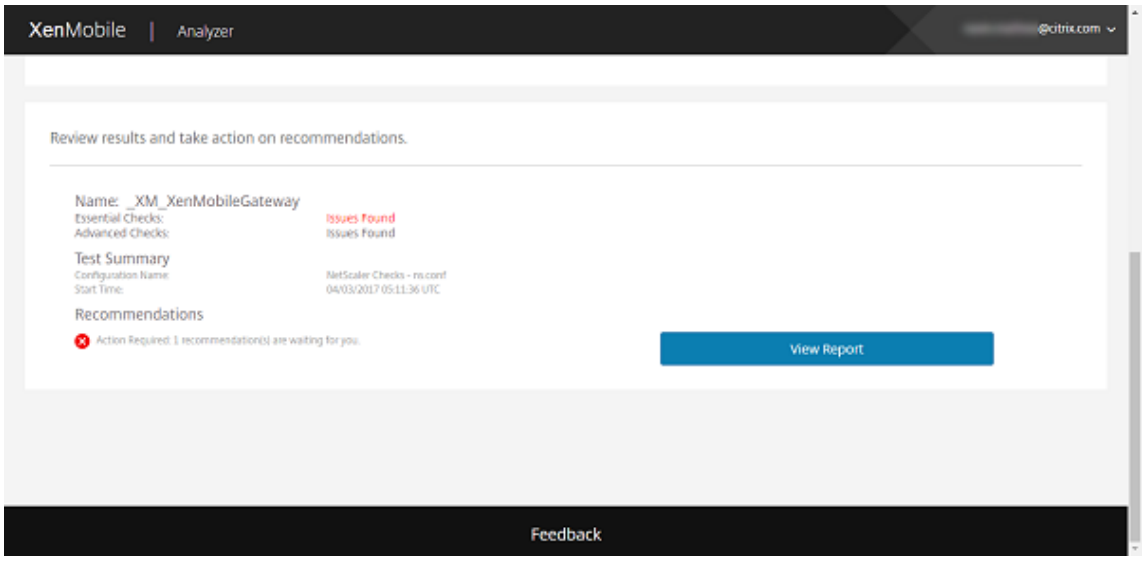
© 1999-2019 Citrix Systems, Inc. All rights reserved.



O XenMobile Analyzer executa dois tipos de verificação de configuração.

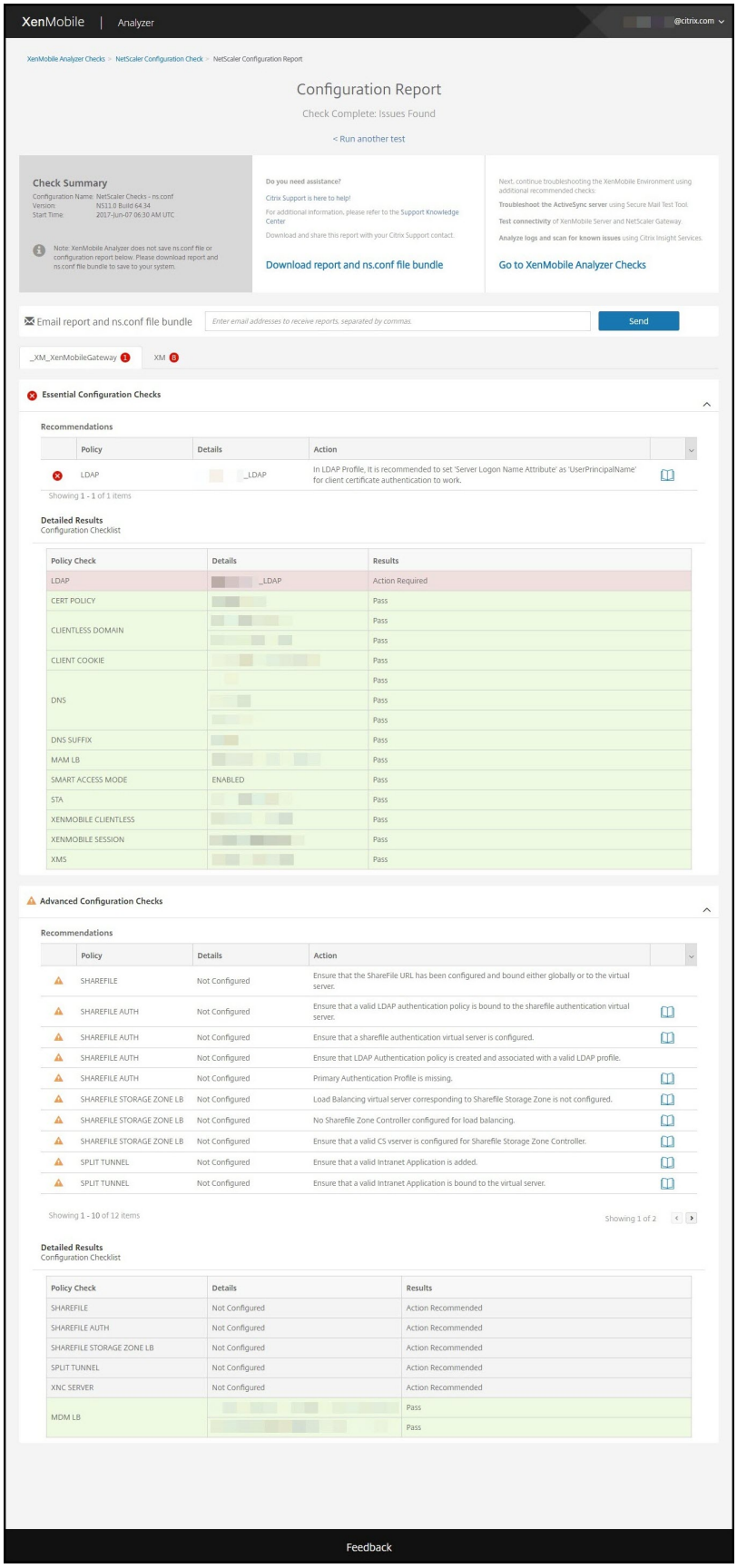
- A opção Essential Checks procura por componentes que são essenciais para uma implantação com êxito do XenMobile.
- A opção Advanced Checks procura por componentes que não são essenciais, mas complementares para implantações do XenMobile.

4. Para exibir as recomendações em Essential Checks e Advanced Checks para NetScaler, clique em **View Report**.



A página **Configuration Report** é exibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> O XenMobile Analyzer é compatível com servidores de gateway configurados por meio do Assistente do NetScaler. As instâncias do NetScaler Gateway sempre seguem a seguinte convenção de título: '_XM_*nome-usado-pelo-usuário-na-implementação'.

O status geral é Success quando as verificações de configuração essenciais tiveram dado resultado positivo.

Quando uma verificação de configuração Essential falha, a tabela de recomendações lista a **Política**, **Detalhes** e **Resultados (ação obrigatória)**.

Quando uma verificação de configuração Advanced falha, a tabela de recomendações lista a **Política**, **Detalhes** e **Resultados (ação recomendada)**.



O selo de notificação no relatório de configuração indica o número de recomendações na verificação de Configuração essencial para servidores de gateway configurados por meio do assistente do NetScaler e de Gateways configurados pelo usuário.

Na página **Configuration Report**, estão disponíveis as opções a seguir.

a) Para exibir os detalhes, clique em **Essential Configuration Checks/Advanced Configuration Checks** (ou no ícone de expandir).

b) Para executar outra verificação de configuração do NetScaler, clique em **Run another test**.

c) Para exibir outras solução de problemas e ferramentas de análise, clique em **Go to XenMobile Analyzer Checks**.

d) Para baixar um relatório dos resultados, clique em **Download report** e **ns.conf file bundle**, ou em **Email report and ns.conf bundle**, e digite seu endereço de email. Clique em **Send**.

Realizar outras verificações informativas

Você interage com a etapa Environment Check do XenMobile Analyzer diretamente para executar testes, enquanto as outras opções são informativas. Cada uma dessas opções fornece informações relativas às outras ferramentas de suporte que você pode usar para garantir que o seu ambiente do XenMobile seja configurado corretamente.

- **Advanced Diagnostics:** essa etapa instrui você a coletar informações sobre o seu ambiente e depois carregar as informações em Citrix Insight Services. A ferramenta analisa os dados e fornece um relatório personalizado com resoluções recomendadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Secure Mail Readiness:** essa etapa direciona você a baixar e executar o aplicativo XenMobile Exchange ActiveSync Test. O aplicativo resolve os problemas de servidores ActiveSync que a sua prontidão seja implantada com ambientes do XenMobile. Depois que o aplicativo for executado, você poderá exibir relatórios ou compartilhá-los com outras pessoas.
- **Server Connectivity Checks:** fornece instruções para verificar suas conexões com servidores XenMobile, Authentication e ShareFile.
- **Contact Citrix Support:** se nada mais funcionar, você poderá criar um tíquete de suporte com o suporte da Citrix.

Problemas conhecidos

Os seguintes problemas são conhecidos no XenMobile Analyzer:

- Ao realizar as verificações do conectividade do Secure Web, não é possível digitar várias URLs no caixa de texto.
- O recurso de autenticação de dispositivos compartilhados Secure Hub não tem suporte.
- O Secure Web testa somente verificar a conectividade com as URLs inserido e não a autenticação para sites correspondentes.

Problemas resolvidos

Os seguintes problemas com o XenMobile Analyzer foram corrigidos:

- Ao realizar uma verificação usando o convite para registro, passa o teste, mas o convite de registro não é trocado.

APIs REST

March 6, 2019

> Nota:
>
> Este artigo aborda as APIs REST para o XenMobile Server 10.9. Para as APIs REST para Endpoint Management, consulte APIs REST.

Com a API REST do XenMobile, você pode chamar os serviços que são expostos por meio do console XenMobile. Você pode chamar os serviços REST usando um cliente REST. A API não exige que você faça logon no console XenMobile para chamar os serviços.

Para obter o conjunto completo e atual de APIs disponíveis, baixe o PDF XenMobile Public API for REST Services.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Permissões necessárias para acessar a API REST

Você precisa de uma das seguintes permissões para acessar a API REST:

- Permissão de acesso à API pública definida como parte da configuração de acesso com base em função. Para obter informações, consulte Configuração de funções com RBAC.
- Permissão de superusuário

Para invocar os serviços da API REST

Você pode chamar os 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 de host e o número de porta para corresponder ao seu ambiente.

Login

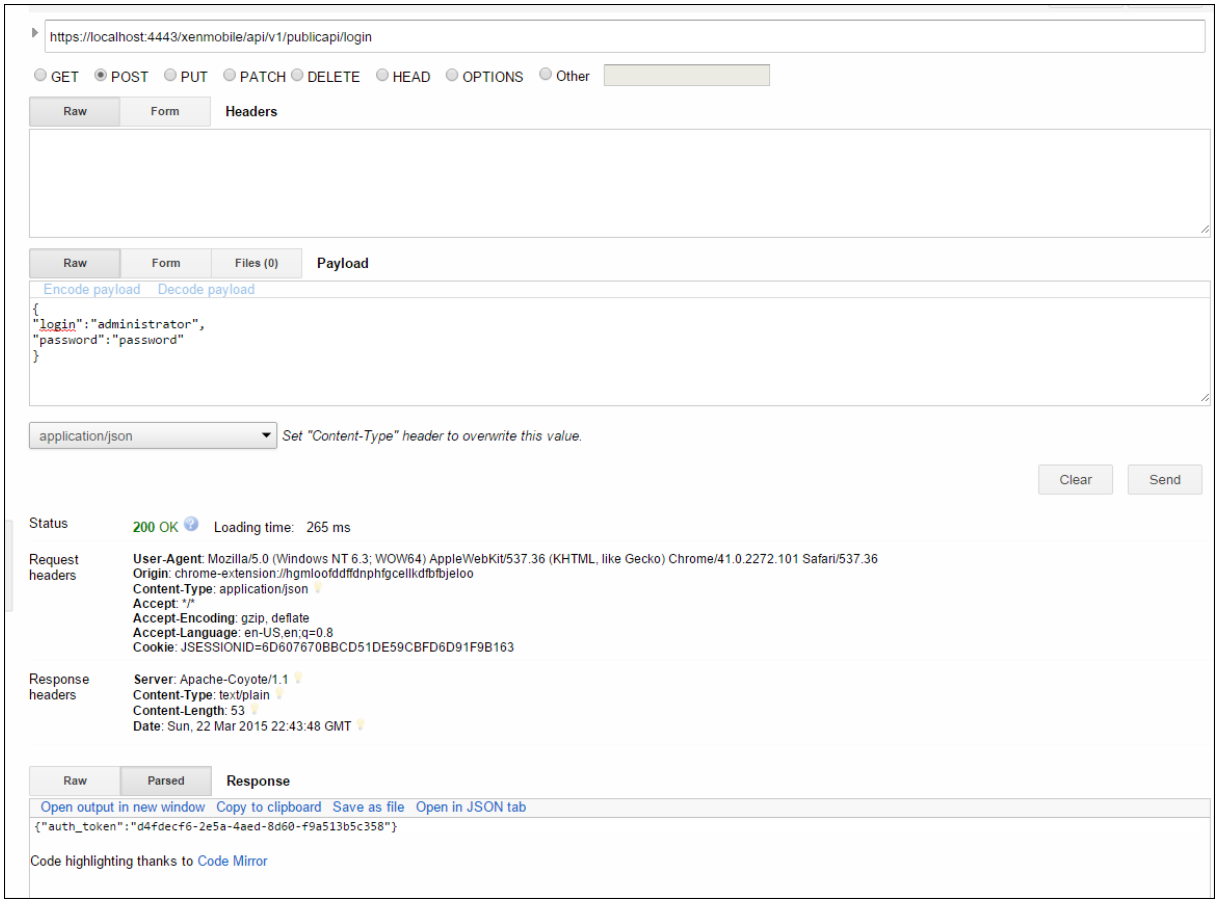
URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Solicitação: `{ "login":"administrator", "password":"password"}`

Tipo de método: POST

Tipo de conteúdo: application/json

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Informações correlatas

- API REST do XenMobile

Conector de Endpoint Management para Exchange ActiveSync

April 15, 2019

O XenMobile Mail Manager é agora o conector de Endpoint Management para Exchange ActiveSync. Para obter mais detalhes sobre o portfólio unificado da Citrix, consulte o Guia do produto Citrix.

O conector oferece a funcionalidade que estende os recursos do XenMobile das seguintes maneiras:

- Controle de Acesso Dinâmico para os dispositivos Exchange Active Sync (EAS). Os dispositivos EAS podem receber automaticamente permissão ou bloqueio de acesso aos serviços do Exchange.
- A capacidade para que o XenMobile acesse as informações de parceria do dispositivo EAS fornecidas pelo Exchange.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- A capacidade para que o XenMobile realize um EAS Wipe em um dispositivo móvel.
- A capacidade para que o XenMobile acesse informações sobre dispositivos BlackBerry e execute operações de controle, como Wipe e ResetPassword.

Para fazer o download do conector de Endpoint Management para Exchange ActiveSync, vá até a seção Server Components em XenMobile 10 Server em Citrix.com.

Novidades

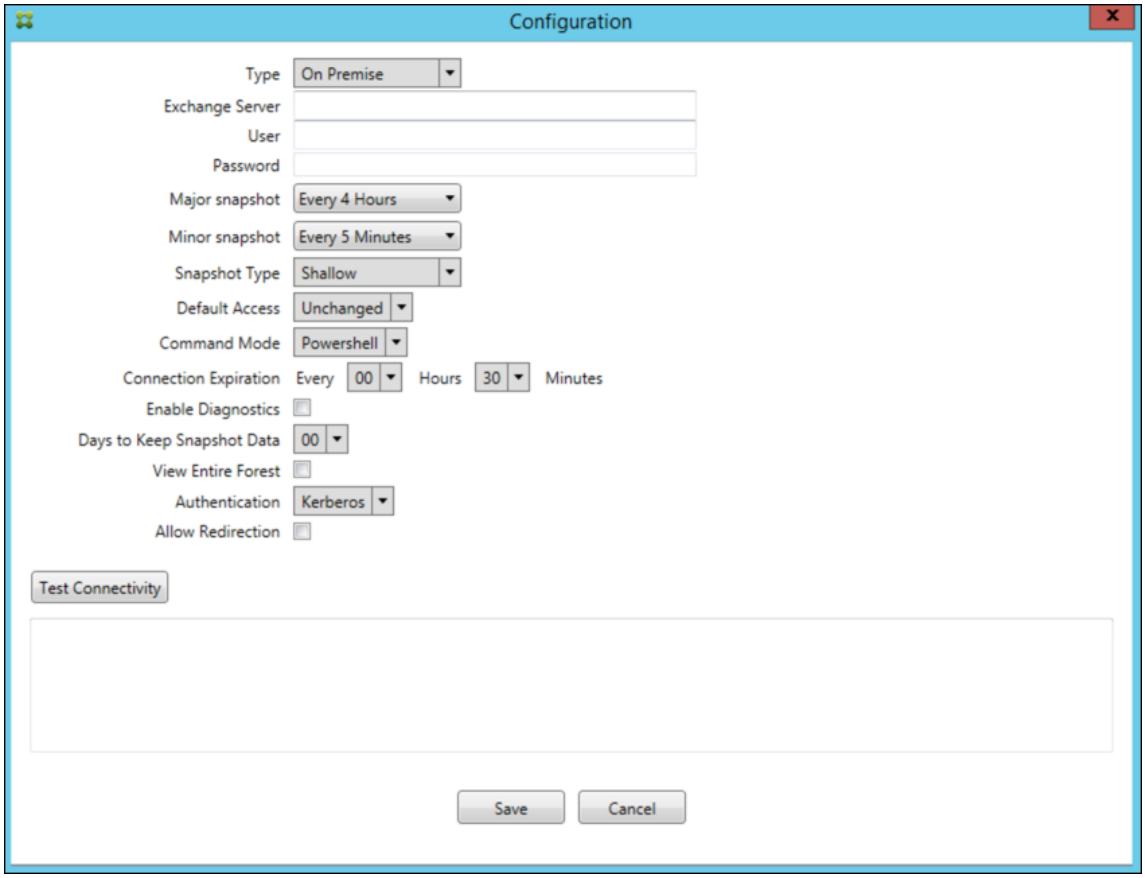
As seções a seguir listam o que há de novo nas versões atuais e anteriores do conector de Endpoint Management para Exchange ActiveSync, anteriormente XenMobile Mail Manager.

O que há de novo na versão 10.1.9

Os seguintes problemas foram resolvidos 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 todas as programações e outras infraestruturas internas são restabelecidas com novas configurações. Esse problema corrige um problema conhecido na versão 10.1.8. [CXM-47709, CXM-61330]
- Durante uma atualização, a configuração de banco de dados existente não foi mesclada com o novo arquivo de configuração. A configuração do banco de dados é agora agrupada ao arquivo de configuração atualizado. [CXM-49326]
- Nos arquivos de diagnóstico relacionados a instantâneos, os cabeçalhos de coluna estavam ausentes. Os cabeçalhos são restaurados. [CXM-62680]
- Ao atualizar a partir de uma versão anterior, a seção padrão do arquivo de configuração era substituída pela seção análoga do arquivo de configuração em uso. Esse problema impedia que adições ou melhorias na seção padrão fossem carregadas pelo serviço após a atualização. A partir desta versão, a seção padrão sempre reflete a configuração mais recente. [CXM-62681]
- Os administradores não podem mais acessar determinadas opções pressionando Shift com o aplicativo em execução. Essas opções estavam disponíveis anteriormente com permissão Citrix. Algumas opções agora estão totalmente disponíveis, como Permitir Redirecionamento, e outras, como Detecção de travamento e Correção de contagem, estão obsoletas. [CXM-62767]

© 1999-2019 Citrix Systems, Inc. All rights reserved.



O que há de novo em versões anteriores

A seção a seguir lista os novos recursos e os problemas corrigidos em versões anteriores do conector de Endpoint Management para Exchange ActiveSync.

O que há de novo na versão 10.1.8

Os seguintes problemas foram resolvidos na versão 10.1.8:

- É possível que o Exchange faça com que o conector Citrix Endpoint Management limite a emissão de comandos para o serviço Exchange ActiveSync com muita frequência. Isso é comum em conexões com o Office 365. O efeito da limitação requer que o serviço pause por um período de tempo especificado antes de enviar o próximo comando. O console Configure agora mostra o tempo restante em pausa. [CXM-48044]
- Quando são feitas modificações nas seções “Watchdog” e/ou “SpecialistsDefaults” do arquivo de configuração (config.xml), as alterações não são refletidas no arquivo de configuração após uma atualização. Nesta versão, as modificações são mescladas corretamente no novo arquivo de configuração. [CXM-52523]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Mais detalhes foram adicionados às análises enviadas ao Google Analytics, especialmente no que diz respeito aos instantâneos. [CXM-56691]
- O recurso de conectividade de teste do Exchange tentava inicializar a conexão apenas uma vez. Uma vez que as conexões do Office 365 podem ser limitadas, era possível que uma conectividade de teste parecesse falhar quando ficava limitada. O conector Citrix Endpoint Management para Exchange ActiveSync agora tenta iniciar uma conexão até três vezes. [CXM-58180]
- Para efetivar políticas no Exchange, o conector 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 volta ao seu estado de acesso padrão. Se esse estado de acesso padrão for diferente do estado desejado para um dispositivo, o dispositivo ficará fora de conformidade. Consequentemente, um usuário pode perder o acesso ao email se o estado de acesso padrão do Exchange estiver bloqueado quando deveria ser permitido. Ou, um usuário cujo acesso ao email deveria ser bloqueado pode ter o acesso permitido. O conector Citrix Endpoint Management para Exchange ActiveSync agora garante que todos os dispositivos com um estado desejado válido sejam incluídos em cada comando **Set-CasMailbox**. [CXM-61251]

O seguinte problema é conhecido na versão 10.1.8:

Se um administrador fizer uma alteração no aplicativo Configure que modifique os dados de configuração, enquanto o serviço estiver executando operações de longa duração, como uma avaliação de política ou um instantâneo, o serviço pode entrar em um estado indeterminado. Um possível sintoma seria as alterações na política não serem processadas ou os instantâneos não serem iniciados. Para retornar o serviço a um estado de funcionamento, o serviço deve ser reiniciado. Talvez seja necessário usar o gerenciador de Serviços do Windows para encerrar o processo de serviço antes de iniciar o serviço. [CXM-61330]

O que há de novo na versão 10.1.7

- O XenMobile Mail Manager é agora o conector de Endpoint Management para Exchange ActiveSync.
- Nós substituímos a opção **Desativar 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. [CXM-54593]

Os seguintes problemas foram resolvidos na versão 10.1.7:

- Na janela Histórico da Captura Instantânea, as mensagens de erro eram exibidas com pouco contexto. Agora, as mensagens de erro são prefixadas com o contexto de onde ocorreram. [CXM-49157]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- O arquivo .dll do XmmGoogleAnalytics não tinha a versão do arquivo correspondente para o lançamento. [CXM-52518]
- Para melhorar o diagnóstico, recentemente alteramos o formato da cadeia de caracteres para uma lista de IDs de dispositivos usados para definir um estado Permitido/Bloqueado da caixa de correio. Uma especificação de muitos dispositivos, no entanto, excedeu o tamanho máximo da cadeia de caracteres. Agora, usamos uma estrutura de dados de matriz interna. Essa estrutura não tem limite de tamanho e também formata os dados adequadamente para fins de diagnóstico. [CXM-52610]
- Quando detectadas políticas de dispositivo que não estão em sincronia com o Exchange, 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 os dispositivos que pertencem a suas respectivas caixas de correio. [CXM-54842]
- Em alguns ambientes, um assembly da Microsoft não está disponível. O assembly necessário agora é explicitamente instalado com o aplicativo. [CXM-55439]
- Se Nomes diferenciados para dispositivos ou caixas de correio tiverem espaços entre o nome do atributo e os iguais e/ou espaços após os iguais e antes do valor, o conector do Endpoint Management do Exchange ActiveSync podia não corresponder corretamente um dispositivo com a sua caixa de correio e vice-versa. O resultado era que alguns dispositivos e/ou caixas de correio podiam ser rejeitados durante a reconciliação de instantâneos. [CXM-56088]

> Nota:
>
> As seções a seguir se referem ao conector do Endpoint Management para Exchange ActiveSync por seu nome anterior, XenMobile Mail Manager. O nome foi alterado 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 detectadas políticas de dispositivo que não estão em sincronia com o Exchange, 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 os dispositivos que pertencem a suas respectivas caixas de correio. [CXM-54842]

O que há de novo na versão 10.1.6

O XenMobile Mail Manager versão 10.1.6 apresenta os seguintes problemas corrigidos e aprimoramentos:

- A janela de histórico do instantâneo (Snapshot History), às vezes, entrava em um estado em que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

sua atualização não era mais realizada. O mecanismo de atualização de janelas foi aprimorado para oferecer uma atualização mais confiável. [CXM-47983]

- Dois modos e caminhos de código separados eram usados para instantâneos particionados e não particionados. Como os instantâneos não particionados são equivalentes aos instantâneos particionados com uma configuração usando uma única partição "*", o modo de instantâneo não particionado foi eliminado. O modo de instantâneo padrão é agora formado de instantâneos particionados com 36 partições (0–9, A – Z). [CXM-49093]
- Na janela Snapshot History de histórico do instantâneo, as mensagens de erro eram substituídas por mensagens de status. Agora, o XenMobile Mail Manager fornece dois campos separados para que os usuários possam visualizar status e erros simultaneamente. [CXM-51942]
- Ao se conectar ao Exchange Online (Office 365), as consultas relacionadas à captura instantânea podiam resultar em um conjunto de dados truncado. Esse problema ocorria quando o XenMobile Mail Manager executava um script com pipelines de vários comandos. O comando upstream não pode passar os dados com rapidez suficiente para o comando downstream, que conclui o trabalho prematuramente; o resultado são dados incompletos. O XenMobile Mail Manager agora pode imitar o próprio pipeline e aguardar até que o comando upstream seja realizado antes de chamar o comando downstream. Essa alteração resulta em todos os dados processados e capturados. [CXM-52280]
- Se ocorre um erro não resolvível 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 resultava no envio do comando ao Exchange várias vezes. Nesta versão do XenMobile Mail Manager, um comando que resulta em um erro só é retornado para a fila de trabalho um pequeno número de vezes. [CXM-52633]
- Se a atualização de uma política de uma caixa de correio específica envolvesse a permissão ou o bloqueio de todos os dispositivos, o comando **Set-CASMailbox** emitido falhava devido à conversão da lista vazia em uma cadeia de caracteres vazia em vez de **NULL**. Os dados apropriados são enviados agora. [CXM-53759]
- Ao processar um novo dispositivo, o Exchange pode retornar o estado como "DeviceDiscovery" por um período (geralmente 15 minutos). O XenMobile Mail Manager não estava manipulando especificamente esse estado. O XenMobile Mail Manager agora manipula o estado. Na guia Monitor da interface do usuário, os usuários podem filtrar dispositivos nesse estado. [CXM-53840]
- 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 podia 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 mostrada) ou no indicador de banco de dados (passando o cursor sobre a mensagem) na parte inferior da janela principal de configuração. [CXM-54219]
- Dependendo da carga de trabalho atual, quando direcionado, o serviço XenMobile Mail Manager nem sempre parava imediatamente. Portanto, o serviço parecia estar em um estado letár-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

gico. Com as melhorias, as tarefas contínuas são interrompidas, resultando em um desligamento mais fácil. [CXM-54282]

O que há de novo na versão 10.1.5

O XenMobile Mail Manager versão 10.1.5 apresenta os seguintes problemas corrigidos:

- Quando o Exchange está aplicando a limitação à atividade do XenMobile Mail Manager, não há nenhuma 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 elimine o embargo de limitação. [CXM-49617]
- Se o XenMobile Mail Manager estiver sendo limitado pelo Exchange durante um instantâneo principal, é possível que uma quantidade insuficiente de tempo passe antes da execução da próxima tentativa de criar um instantâneo. Esse problema resulta em mais limitação e em um instantâneo com falha. Agora, o XenMobile Mail Manager aguarda o tempo mínimo especificado pelo Exchange entre as tentativas de captura instantânea. [CXM-49618]
- Quando o diagnóstico está ativado, o arquivo de comandos mostra comandos **Set-CasMailbox** com hifens ausentes antes do nome de cada propriedade. Esse problema ocorre apenas na formatação do arquivo de diagnóstico e não no comando para o Exchange. O hífen ausente impede que um usuário corte o comando e cole-o diretamente em um prompt do PowerShell para teste ou validação. Os hifens foram adicionados. [CXM-52520]
- Se a identidade de uma caixa de correio estiver no formato "sobrenome, nome", o Exchange adicionará 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. [CXM-52635]

Limitação conhecida

> Nota:
>
> A limitação a seguir está resolvida na versão 10.1.6.

O XenMobile Mail Manager possui uma limitação conhecida que pode fazer com que os comandos do Exchange falhem. Para aplicar alterações de política ao Exchange, um comando **Set_CASMailbox** é emitido pelo XenMobile Mail Manager. Esse comando pode ter 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 falhará na sua totalidade, impedindo que as políticas de caixa de correio desses

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dispositivos sejam configuradas. O erro relatado, que aparecerá nos logs do XenMobile Mail Manager, será semelhante ao seguinte. Este exemplo é de uma lista bloqueada.

"Message:'Não é possível vincular o parâmetro 'ActiveSyncBlockedDeviceIDs' ao destino. Exception setting "ActiveSyncBlockedDeviceIDs": "O comprimento da propriedade é muito longo. O comprimento máximo é 256 e o comprimento do valor fornecido é… "

Os tamanhos de ID dos dispositivos podem variar, mas, via de regra, cerca de 10 dispositivos ou mais simultaneamente Permitidos ou Bloqueados poderão exceder o limite. Embora ter muitos dispositivos associados a uma caixa de correio específica seja raro, essa é uma possibilidade. Até que o XenMobile Mail Manager seja aprimorado para lidar com esse cenário, recomendamos limitar o número de dispositivos associados a um usuário e a uma caixa de correio a 10 ou menos. [CXM-52633]

O que há de novo na versão 10.1.4

O XenMobile Mail Manager versão 10.1.4 apresenta os seguintes problemas corrigidos:

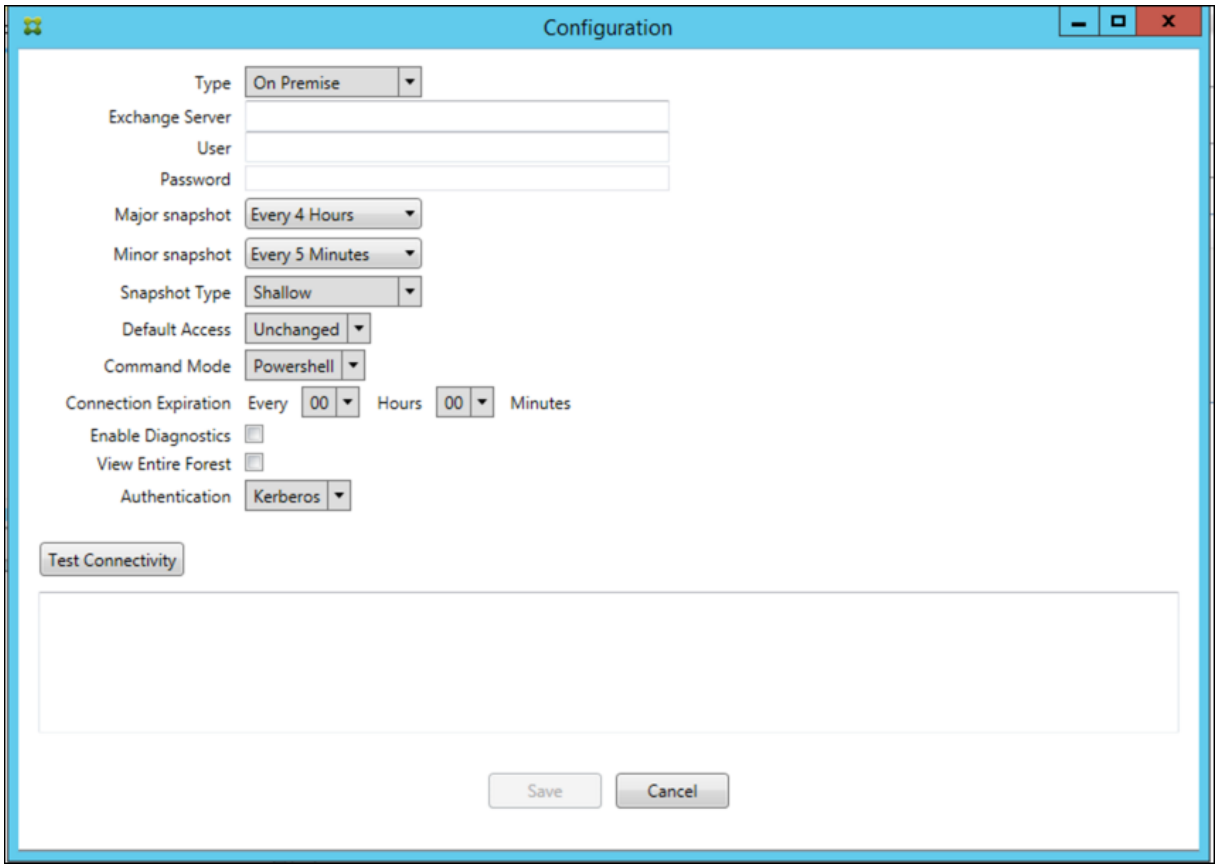
- Devido ao enfraquecimento da segurança, o TLS 1.0 está sendo suspenso pelo PCI Council. O suporte para o TLS 1.1 e 1.2 é adicionado ao XenMobile Mail Manager. [CXM-38573, CXM-32560]
- O XenMobile Mail Manager inclui um novo arquivo de diagnóstico. Quando a opção **Ativar diagnóstico** está selecionada na especificação do Exchange, um novo arquivo de Histórico de Captura Instantânea é gerado. Com cada tentativa de instantâneo, uma linha é adicionada ao arquivo com os resultados do instantâneo. [CXM-49631]
- No arquivo de diagnóstico Comandos, a lista de dispositivos permitidos ou bloqueados não foi exibida para o comando **Set-CASMailbox**. Em vez disso, o nome da classe interna foi mostrado no arquivo para os argumentos relacionados. O XenMobile Mail Manager agora mostra a lista de deviceIDs como uma lista delimitada por vírgulas. [CXM-50693]
- 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". Mais mensagens descritivas aparecem agora, como "Todas as conexões estão inoperantes", "O pool de conexões está vazio", "Todas as conexões são limitadas" e "Nenhuma conexão disponível". [CXM-50783]
- Em alguns casos, os comandos Permitir/Bloquear/Apagar são enfileirados várias vezes no cache interno do XenMobile Mail Manager. Esse problema causa um atraso no comando que está sendo enviado para o Exchange. O XenMobile Mail Manager agora só enfileira uma instância de cada comando. [CXM-51524]

O que há de novo na versão 10.1.3

- **Suporte ao Google Analytics:** queremos saber como você usa o XenMobile Mail Manager para nos concentrarmos em como podemos melhorar o produto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Configuração para ativar o diagnóstico:** uma caixa de seleção **Ativar diagnóstico** é exibida no console Configurar na caixa de diálogo **Configuração**.



Problemas resolvidos na versão 10.1.3

- Na janela **Histórico da Captura Instantânea**, as dicas de ferramentas que mostram o estado atual da captura instantânea não refletem o estado real. [CXM-5570]
  Ocasionalmente, o XenMobile Mail Manager não pode gravar no arquivo de diagnósticos de Comandos. Quando isso ocorre, o histórico de comandos não é registrado em sua totalidade. [CXM-49217]
- Quando ocorre um erro com uma conexão, a conexão não é marcada como “com erro”. Como resultado, um comando subsequente pode tentar usar a conexão e causar outro erro. [CXM-49495]
- Quando a limitação do Exchange Server ocorre, uma exceção pode ser lançada na rotina de Verificação de Integridade. Como resultado, as conexões que sofreram um erro ou expiraram podem não ser limpas. Além disso, o XenMobile Mail Manager não cria conexões até que o tempo de limitação expire. [CXM-49794].
- Quando a contagem máxima de sessões do Exchange é excedida, o XenMobile Mail Manager relata o erro “Falha na Captura do Dispositivo”, que não é uma mensagem precisa. Em vez disso,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a mensagem deve indicar que as duas sessões que o XenMobile Mail Manager normalmente usa para a comunicação do Exchange estão em uso. [CXM-49994]

O que há de novo na versão 10.1.2

- **Melhor conexão com o Exchange**: o XenMobile Mail Manager usa as sessões do PowerShell para se comunicar com o Exchange. Uma sessão do PowerShell, especialmente ao lidar com o Office 365, pode se tornar instável depois de algum tempo, impedindo o êxito dos comandos subsequentes. O XenMobile Mail Manager agora pode definir um período de expiração para conexões. Quando a conexão atinge seu tempo de expiração, o XenMobile Mail Manager encerra a sessão do PowerShell e cria uma sessão. Ao fazer isso, é menos provável que a sessão do PowerShell se torne instável, reduzindo significativamente a chance de uma falha de instantâneo.
- **Fluxo de trabalho de instantâneo aprimorado**: os principais instantâneos são uma operação demorada e de processo intenso. Se ocorrer um erro durante um instantâneo, agora o XenMobile Mail Manager tentará várias vezes (até três) concluir um instantâneo. Tentativas subsequentes não começam do início. O XenMobile Mail Manager continua de onde parou. Esse aprimoramento melhora a taxa de sucesso de instantâneos em geral, permitindo que erros transitórios passem enquanto um instantâneo ainda está em andamento.
- **Diagnóstico aprimorado**: a solução de problemas de operações de instantâneos agora ficou 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.
- **Melhor uso de memória**: agora, o XenMobile Mail Manager é mais eficiente no uso de memória. Os administradores podem agendar o XenMobile Mail Manager para reiniciar automaticamente para fornecer uma barreira limpa ao sistema.
- **Pré-requisito do Microsoft .NET Framework 4.6**: o pré-requisito para o Microsoft .NET Framework agora é a versão 4.6.

Problemas resolvidos

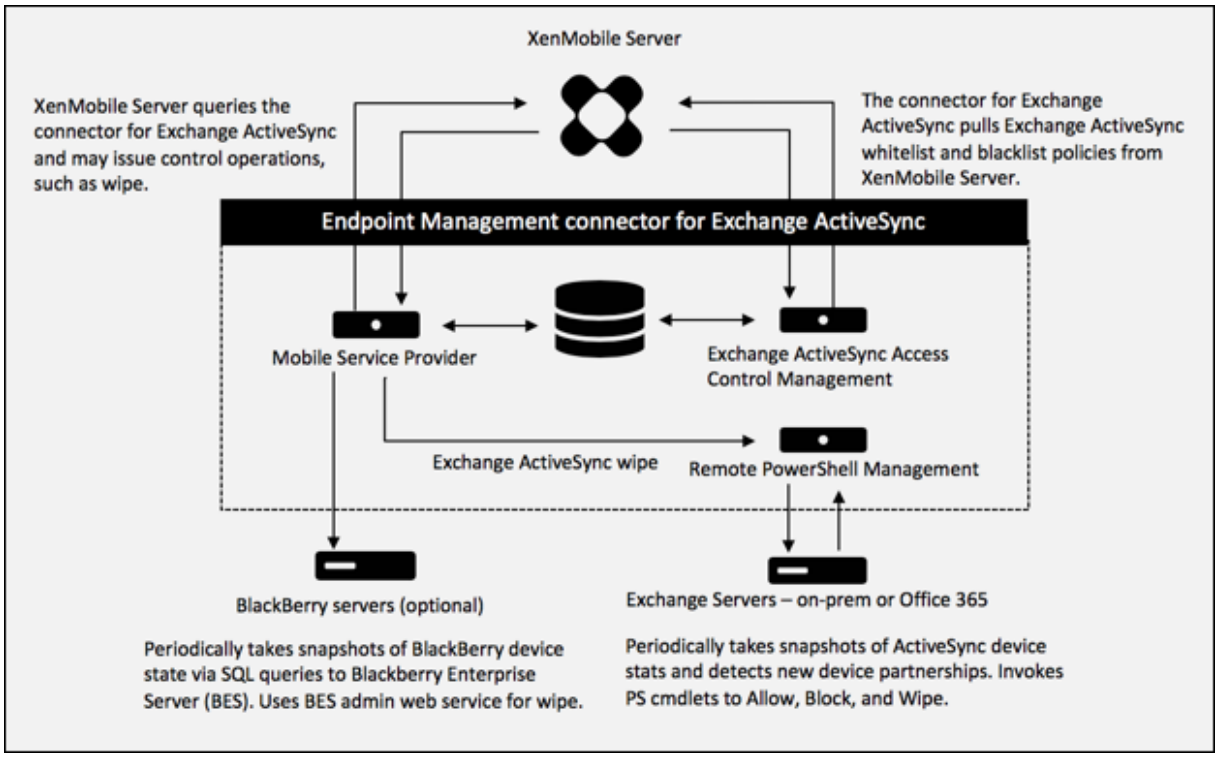
- Aviso de erro de credenciais: a instabilidade da sessão do Office 365 muitas vezes causou esse erro. O melhoria Conexão Aprimorado ao Exchange resolve esse problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Imprecisões na contagem de caixas de correio e dispositivos: o XenMobile Mail Manager possui um algoritmo aprimorado de associação de Caixa de Correio com Dispositivo. O recurso Diagnóstico Aprimorado ajuda na identificação de caixas de correio e dispositivos que o XenMobile Mail Manager considera que não estão dentro de seu domínio de responsabilidade. (XMHELP-623)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Comandos Permitir/Bloquear/Apagar não são reconhecidos: um bug foi corrigido onde, às vezes, os comandos de permissão/bloqueio/apagamento do XenMobile Mail Manager não são reconhecidos. (XMHELP-489)
- Gerenciamento de memória: melhor gerenciamento de memória e mitigação. (XMHELP-419)

Arquitetura

A figura a seguir mostra os principais componentes do conector do Endpoint Management para Exchange ActiveSync. Para um diagrama da arquitetura de referência detalhada, consulte Arquitetura.



Os três componentes principais são:

- **Exchange ActiveSync Access Control Management:** comunica-se com o XenMobile para recuperar uma política do Exchange ActiveSync do XenMobile e mesclá-la com qualquer política definida localmente para determinar os dispositivos do Exchange ActiveSync que devem ter o acesso ao Exchange permitido ou negado. A política local permite a extensão das regras da política para possibilitar o controle de acesso pelo Grupo do Active Directory, Usuário, Tipo de Dispositivo ou Agente de Usuário do Dispositivo (geralmente o número de versão de plataforma).
- **Remote PowerShell Management:** responsável pelo cronograma e invocação de comandos PowerShell remotos para impor a política compilada pelo Exchange ActiveSync Access Control Management. Tira periodicamente um instantâneo do banco de dados do Exchange ActiveSync para detectar dispositivos do Exchange ActiveSync novos ou alterados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Mobile Service Provider:** fornece uma interface de serviços da Web para que o XenMobile possa consultar o Exchange ActiveSync, consultar dispositivos Blackberry e emitir operações de controle, como o Wipe nos dispositivos Blackberry e no ActiveSync.

Requisitos do sistema e pré-requisito

Os seguintes requisitos mínimos do sistema são necessários para usar o conector de Endpoint Management para Exchange ActiveSync:

- Windows Server 2012 R2, Windows Server 2008 R2 (deve ser um servidor baseado no idioma inglês)
- Microsoft SQL Server 2016, SQL Server 2014, SQL Server 2012, SQL Server 2012 Express LocalDB ou SQL Server Express 2008
- 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
- Exchange Server 2010 SP2

Pré-requisitos

- O Windows Management Framework deve estar instalado.
  - PowerShell V5, V4 e V3
- A política de execução do PowerShell deve ser definida como RemoteSignedvia Set-ExecutionPolicy RemoteSigned.
- A porta TCP 80 deve estar aberta entre o computador que está executando o conector de Endpoint Management para Exchange ActiveSync e o Exchange Server remoto.
- **Clientes de email de dispositivos**: nem todos os clientes de email sempre retornam o mesmo ActiveSync ID para um dispositivo. Como o conector de Endpoint Management para Exchange ActiveSync espera uma ID exclusiva do ActiveSync para cada dispositivo, apenas os clientes de email que consistentemente geram a mesma ID exclusiva do ActiveSync para cada dispositivo são suportados. Esses clientes de email foram testados pela Citrix e executados sem erros:
  - Cliente de email nativo HTC
  - Cliente de email nativo Samsung
  - Cliente de email nativo iOS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - TouchDown for Smartphones

- **Exchange**: os requisitos para o computador local executando o Exchange são os seguintes:

  As credenciais especificadas na interface do usuário da Configuração do Exchange devem conseguir realizar a conexão com o Exchange Server e ter acesso total para executar os seguintes cmdlets do PowerShell específicos do Exchange.

  - **Para o Exchange Server 2010 SP2:**
    * Get-CASMailbox
    * Set-CASMailbox
    * Get-Mailbox
    * Get-ActiveSyncDevice
    * Get-ActiveSyncDeviceStatistics
    * Limpar ActiveSyncDevice
    * Get-ExchangeServer
    * Get-ManagementRole
    * Get-ManagementRoleAssignment
  - **Para o 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 de Endpoint Management para Exchange ActiveSync estiver configurado para exibir a floresta inteira, a permissão deve ter sido concedida para execução de: **Set-AdServerSettings -ViewEntireForest $true**
  - As credenciais fornecidas devem ter o direito de conexão com o Exchange Server por meio do Shell remoto. Por padrão, o usuário que instalou o Exchange tem esse direito.
  - De acordo com o artigo da Microsoft TechNet about_Remote_Requirements, para estabelecer uma conexão remota e executar comandos remotos, as credenciais devem corresponder a um usuário que seja um administrador no computador remoto. 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 a postagem do blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands.
  - O Exchange Server deve ser configurado para oferecer suporte a solicitações remotas do PowerShell por meio de HTTP. Normalmente, um administrador que executa o seguinte

© 1999-2019 Citrix Systems, Inc. All rights reserved.

comando do PowerShell no Exchange Server é só o que é necessário: WinRM QuickConfig.
  - O Exchange apresenta muitas políticas de limitação. Uma das políticas controla quantas conexões simultâneas do PowerShell 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 de Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo permitido de conexões simultâneas por meio do PowerShell que estão além do escopo desta documentação. Se você tiver interesse, investigue as políticas de limitação do Exchange relacionadas ao gerenciamento remoto com o PowerShell.

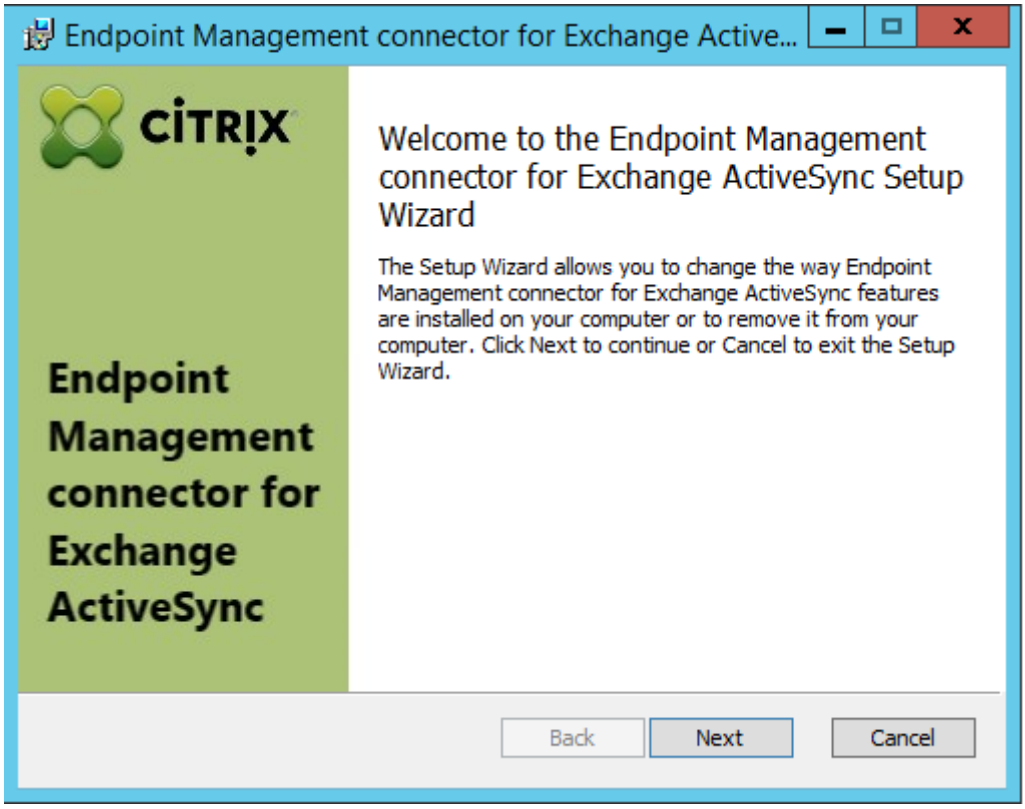
Requisitos do Office 365 Exchange

- **Permissões:** as credenciais especificadas na interface do usuário da Configuração do Exchange devem conseguir realizar a conexão com o 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 o direito de conexão com o servidor do Office 365 por meio do Shell remoto. Por padrão, o administrador online do Office 365 tem os privilégios necessários.
- **Throttling policies:** Exchange has many throttling policies. Uma das políticas controla quantas conexões simultâneas do PowerShell 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 de Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo permitido de conexões simultâneas por meio do PowerShell que estão além do escopo desta documentação. Se você tiver interesse, investigue as políticas de limitação do Exchange relacionadas ao gerenciamento remoto com o PowerShell.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Instalar e configurar

1. Clique no arquivo XmmSetup.msi e siga os prompts no instalador para instalar o conector de Endpoint Management para Exchange ActiveSync.
2. Deixe a opção **Launch the Configure utility** selecionada na última tela do assistente de configuração. Ou, no menu **Iniciar**, abra o conector de Endpoint Management para Exchange ActiveSync.

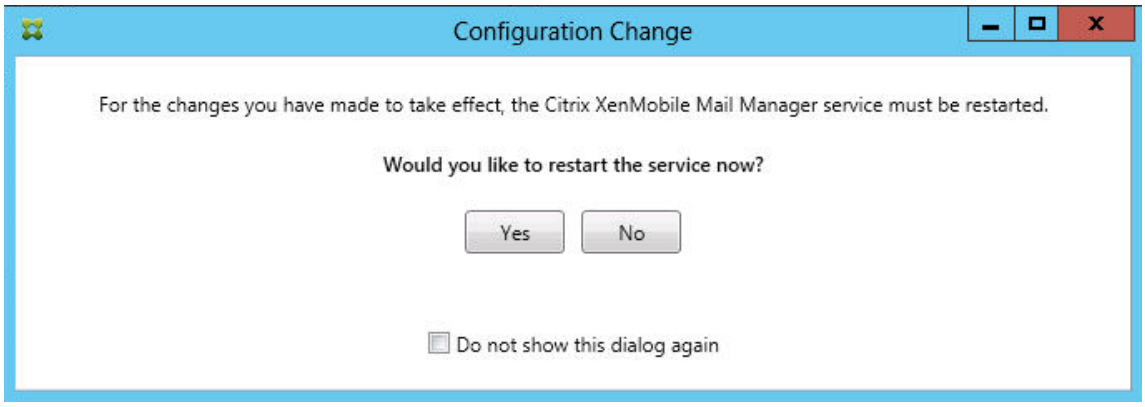


3. Configure as seguintes propriedades de banco de dados:
   - Selecione a guia **Configure > Database**.
   - Digite o nome do SQL Server (o padrão é localhost).
   - Mantenha o banco de dados como o padrão **CitrixXmm**.
4. Selecione um dos seguintes modos de autenticação usados para SQL:
   - **SQL:** digite o nome do usuário e a senha de um usuário válido do SQL.
   - **Windows Integrated:** se você selecionar essa opção, as credenciais de login do serviço conector de Endpoint Management para Exchange ActiveSync deverão 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 no serviço conector de Endpoint Management para Exchange ActiveSync e clique na guia **Logon**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

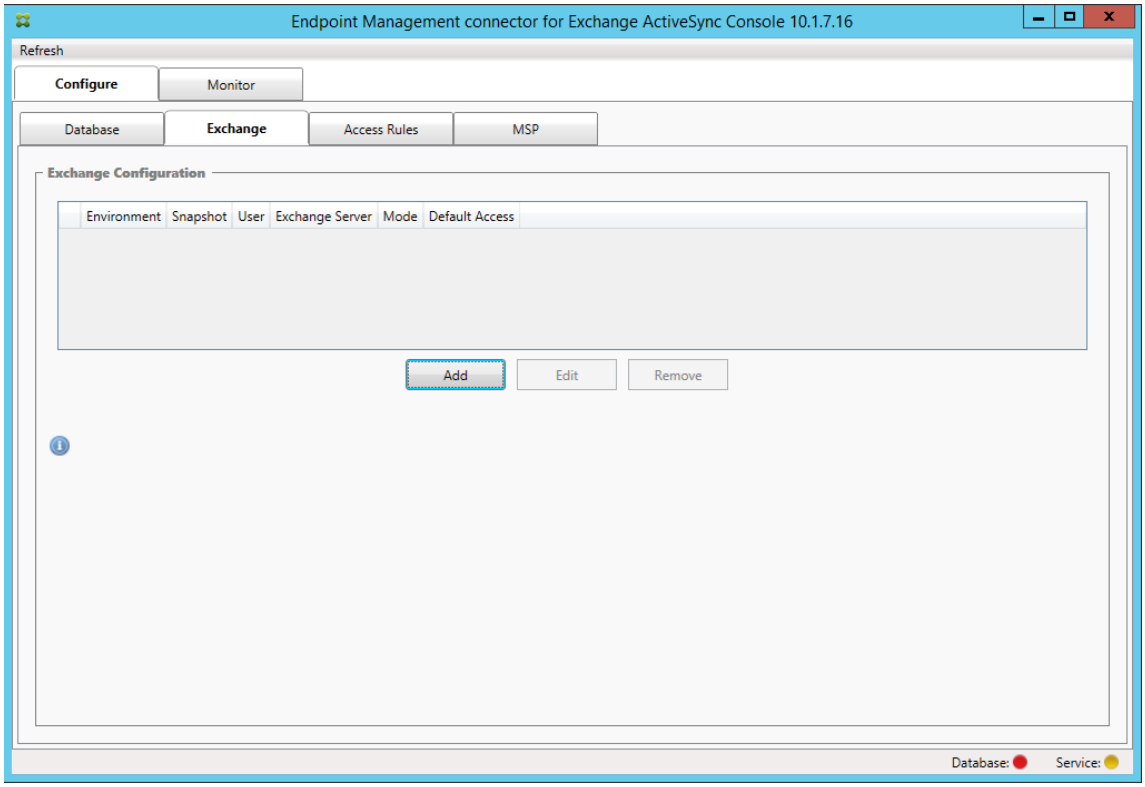
Se a opção Windows Integrated também for escolhida para a conexão de banco de dados do BlackBerry, a conta do Windows especificada aqui também deverá ter acesso ao banco de dados do BlackBerry.

5. Clique em **Test Connectivity** para verificar se uma conexão com o SQL Server pode ser realizada e clique em **Save**.
6. Uma mensagem solicita que você reinicie o serviço. Clique em **Yes**.



7. Configure um ou mais Exchange Servers:
   - Se estiver gerenciando um único ambiente do Exchange, especifique apenas um único servidor. Se estiver gerenciando vários ambientes do Exchange, especifique um único Exchange Server para cada ambiente do Exchange.
   - Clique na guia **Configure > Exchange** e, em seguida, clique em **Add**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



8. Selecione o tipo de ambiente do Exchange Server: **On Premise** ou **Office 365**.

   - Se você selecionar **On Premise**, digite o nome do Exchange Server que será usado para os comandos do Remote PowerShell.
   - Digite o **nome do usuário** de uma identidade do Windows que tenha os direitos adequados no Exchange Server, conforme especificado na seção Requisitos, e insira a **senha** do usuário.
   - Selecione o cronograma da execução de instantâneos principais. Um instantâneo principal detecta cada parceria do Exchange ActiveSync.
   - Selecione o cronograma da execução de instantâneos secundários. Um instantâneo secundário detecta parcerias do Exchange ActiveSync recém-criadas.
   - Selecione o Snapshot Type: **Deep** ou **Shallow**. Os instantâneos superficiais (Snapshot Shallow) são tipicamente muito mais rápidos e são suficientes para executar todas as funções de Controle de Acesso do Exchange ActiveSync do conector de Endpoint Management para Exchange ActiveSync. Os instantâneos profundos (Snapshot Deep) podem demorar mais tempo e serão necessários somente se o Provedor de Serviços Móveis estiver ativado para o ActiveSync. Essa opção permite que o XenMobile consulte dispositivos não gerenciados.
   - Selecione o Default Access: **Allow**, **Block** ou **Unchanged**. Essa configuração controla como todos os dispositivos diferentes dos identificados por regras explícitas do XenMobile ou Locais são tratados. Se você selecionar **Allow**, o acesso do ActiveSync a todos esses dispositivos será permitido. Se você selecionar **Block**, o acesso será negado. Se

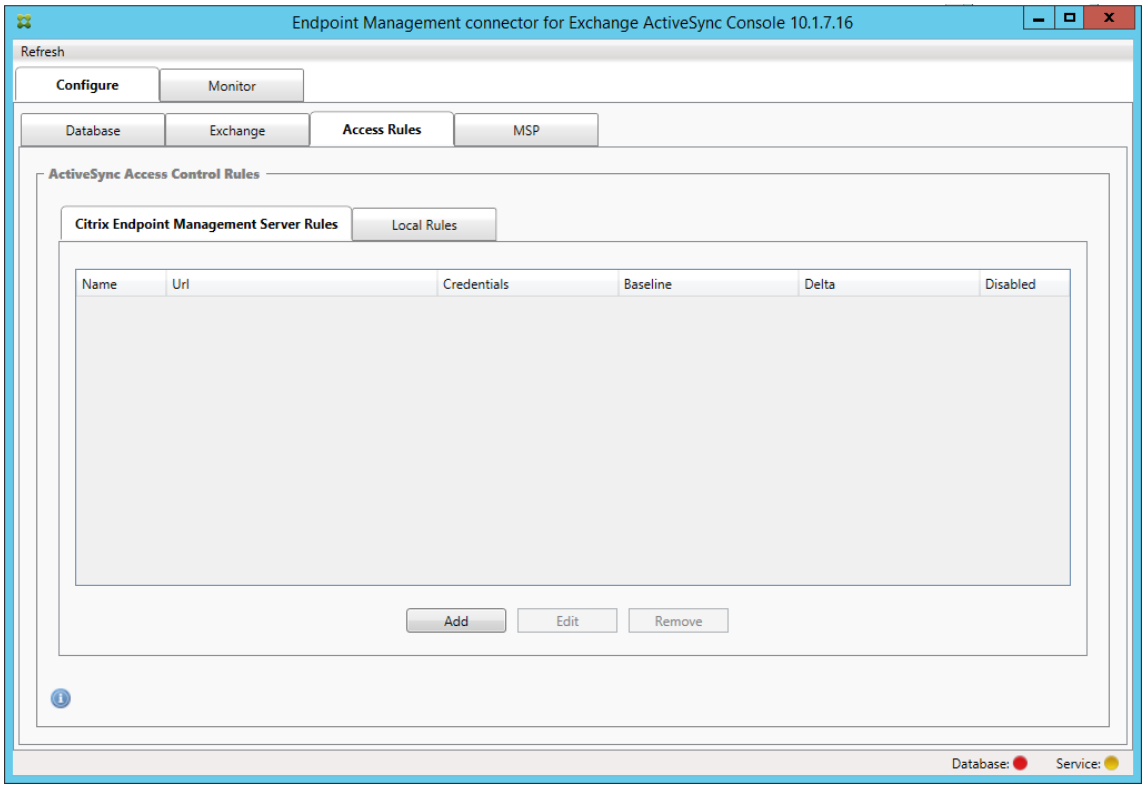
© 1999-2019 Citrix Systems, Inc. All rights reserved.

você selecionar **Unchanged**, nenhuma alteração será feita.

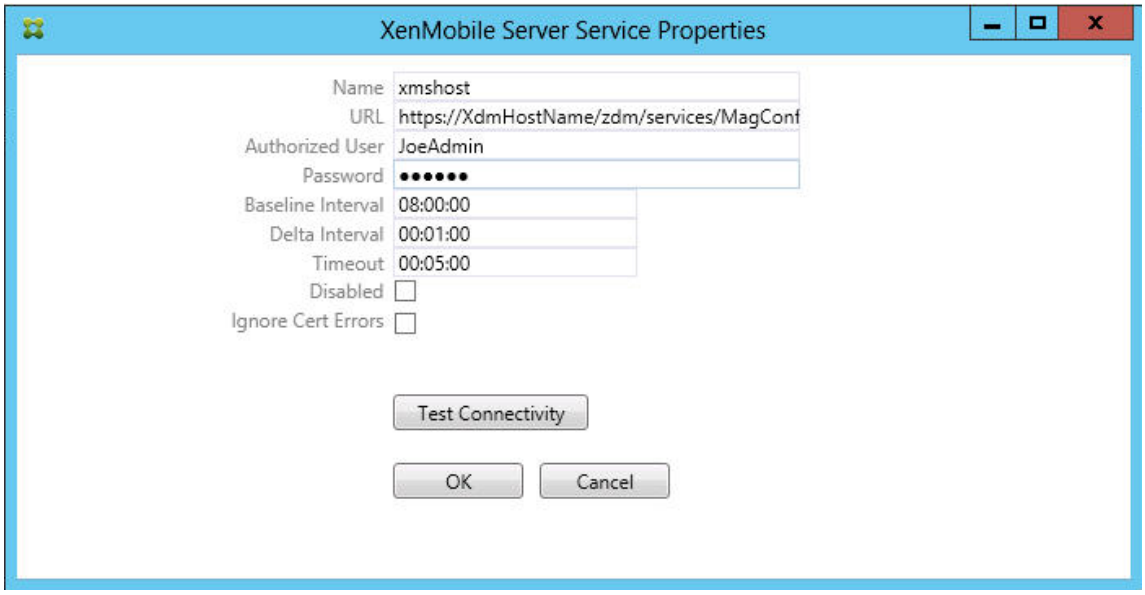
- Selecione o ActiveSync Command Mode: **PowerShell** ou **Simulation**.
- No modo **PowerShell**, o conector de Endpoint Management para Exchange ActiveSync emite comandos do PowerShell para efetuar o controle de acesso desejado. No modo Simulation, o conector de Endpoint Management para Exchange ActiveSync não emite comandos do PowerShell, mas registra o comando e os resultados pretendidos no banco de dados. No modo Simulation, o usuário pode usar a guia **Monitor** para ver o que teria acontecido se o modo PowerShell estivesse ativado.
- Em **Connection Expiration**, defina as horas e minutos para a duração de uma conexão. Quando uma conexão atinge a duração especificada, a conexão é marcada como expirada, de modo que a conexão nunca seja usada novamente. Quando a conexão expirada não é mais usada, o conector de Endpoint Management para Exchange ActiveSync encerra a conexão normalmente. Quando uma conexão é necessária novamente, uma nova conexão é inicializada se nenhuma estiver disponível. Se nenhuma for especificada, o padrão de 30 minutos será usado.
- Selecione **View Entire Forest** para configurar o conector de Endpoint Management para Exchange ActiveSync para exibir toda a floresta do Active Directory no ambiente do Exchange.
- Selecione o protocolo de autenticação: **Kerberos** ou **Basic**. O conector de Endpoint Management para Exchange ActiveSync oferece suporte à autenticação Basic para implantações locais. Isso permite que o conector de Endpoint Management para Exchange ActiveSync seja usado quando o conector de servidor Endpoint Management para Exchange ActiveSync não é membro do domínio no qual o Exchange Server reside.
- Clique em **Test Connectivity** para verificar se uma conexão com o Exchange Server pode ser realizada e clique em **Save**.
- Uma mensagem solicita que você reinicie o serviço. Clique em **Yes**.

9. Configure as regras de acesso: selecione a guia **Configure > Acess Rules**, clique na guia **XMS Rules** e, em seguida, clique em **Add**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



10. Na página de **Propriedades do servidor XenMobile Service**, modifique a sequência 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.



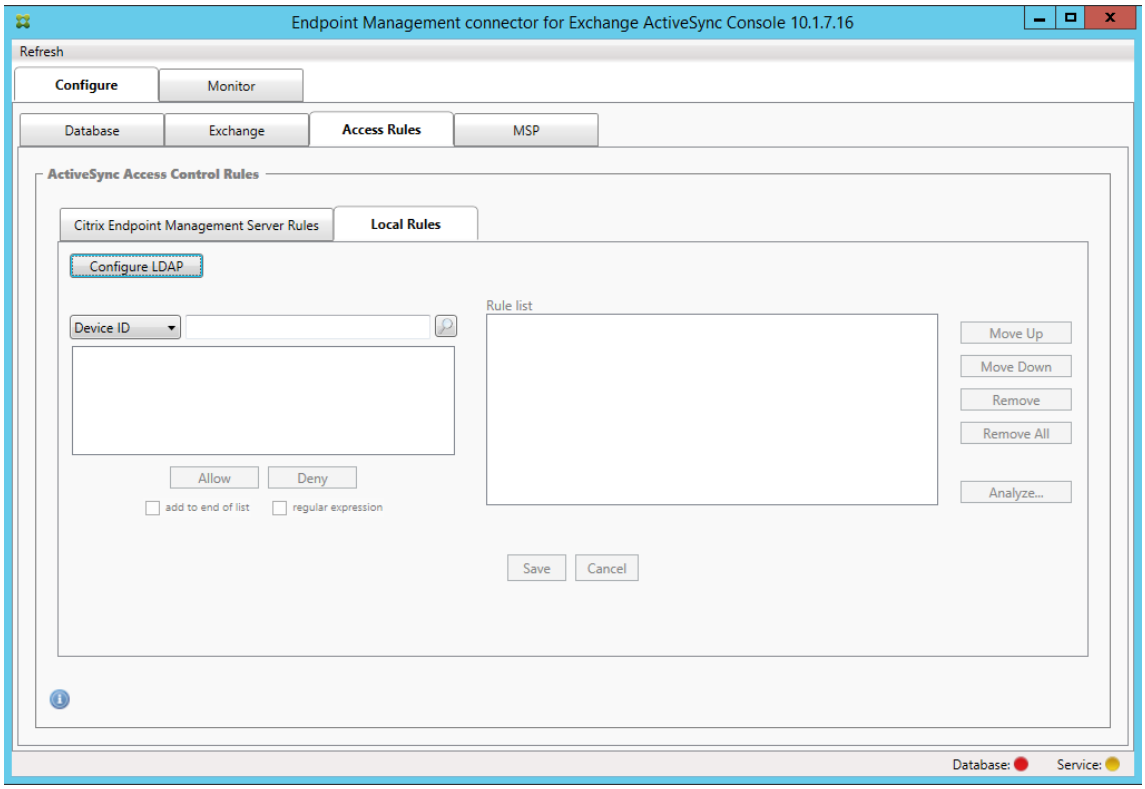
- Insira um usuário autorizado do servidor.
- Insira a senha de usuário.
- Mantenha os valores padrão de **Baseline Interval**, **Delta Interval** e **Timeout**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Clique em **Test Connectivity** para verificar a conexão com o servidor e depois clique em **OK**.

Se a caixa de seleção **Disabled** estiver marcada, o XenMobile Mail Service não coletará políticas do XenMobile.

11. Clique na guia **Local Rules**.



- Você pode adicionar regras locais com base em ActiveSync Device ID, Device Type, AD Group, User ou UserAgent de dispositivo. Na lista, selecione o tipo adequado.
- Insira texto ou fragmentos de texto na caixa de texto. Opcionalmente, clique no botão de consulta para exibir as entidades que correspondem ao fragmento.

Para todos os tipos diferentes de Group, o sistema se baseia nos dispositivos que foram encontrados em um instantâneo. Portanto, se você estiver apenas começando e ainda não tiver concluído um instantâneo, nenhuma entidade estará disponível.

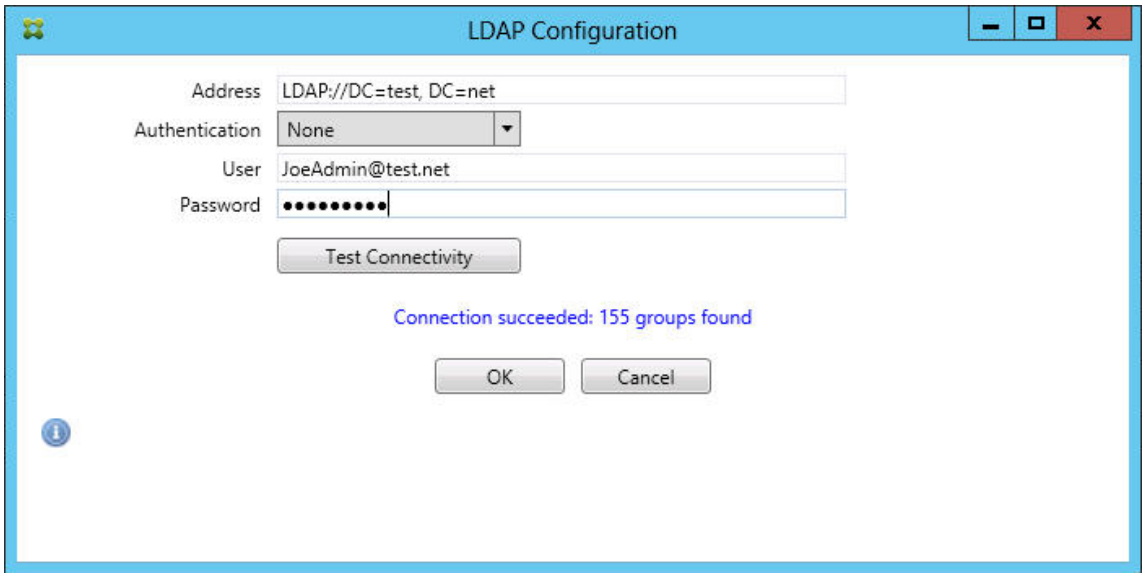
- Selecione um valor de texto e clique em **Allow** ou **Deny** para adicioná-lo ao painel **Rule List** à direita. Você pode alterar a ordem das regras ou removê-las usando os botões à direita do painel **Rule List**. A ordem é importante pois, para um determinado usuário e dispositivo, as regras são avaliadas na ordem mostrada e uma correspondência em uma regra superior (mais perto do topo) faz com que as regras subsequentes não tenham nenhum efeito. Por exemplo, se houver uma regra que permite todos os dispositivos iPad e uma regra subsequente que bloqueia o usuário Matt, o iPad de Matt ainda será permitido,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pois a regra iPad tem uma prioridade efetiva mais alta do que a regra Matt.

- Para executar uma análise das regras na lista de regras para localizar possíveis substituições, conflitos ou construções complementares, clique em **Analyze** e depois clique em **Save**.

12. Se você desejar criar regras locais que operam em Grupos do Active Directory, clique em **Configure LDAP** e, em seguida, configure as propriedades de conexão LDAP.

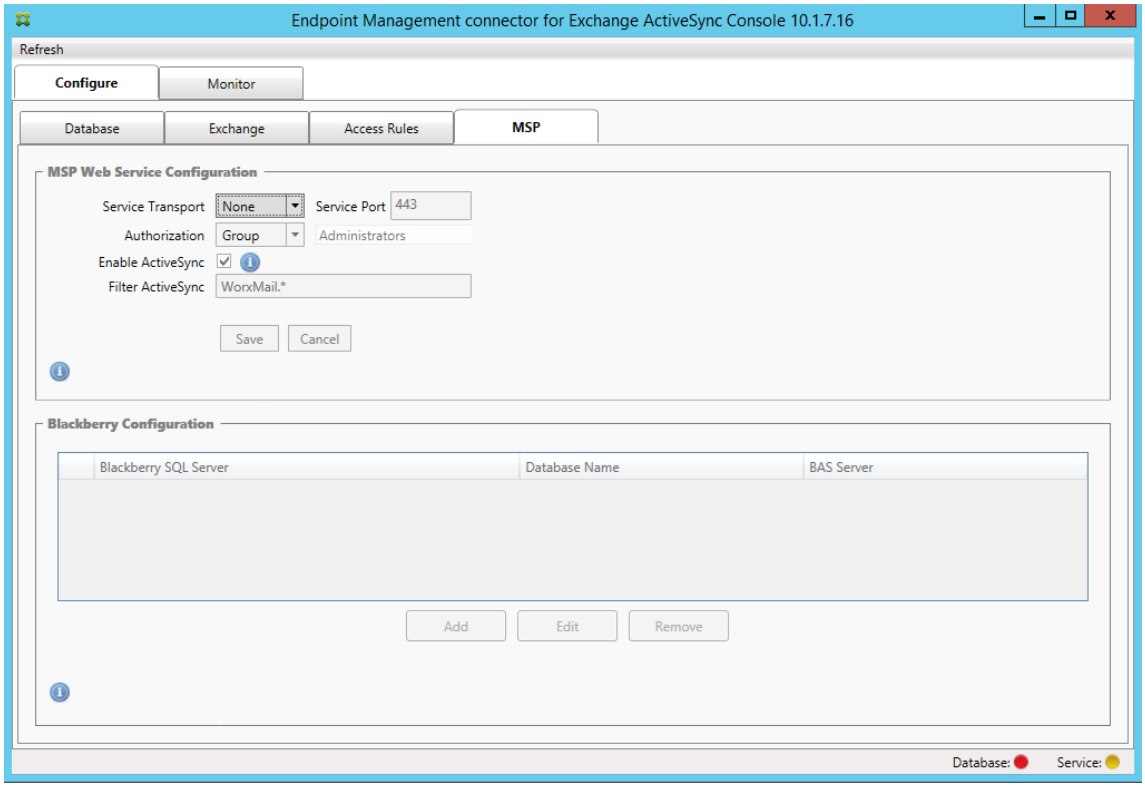


13. Configure o Provedor de Serviços Móveis.

    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**.

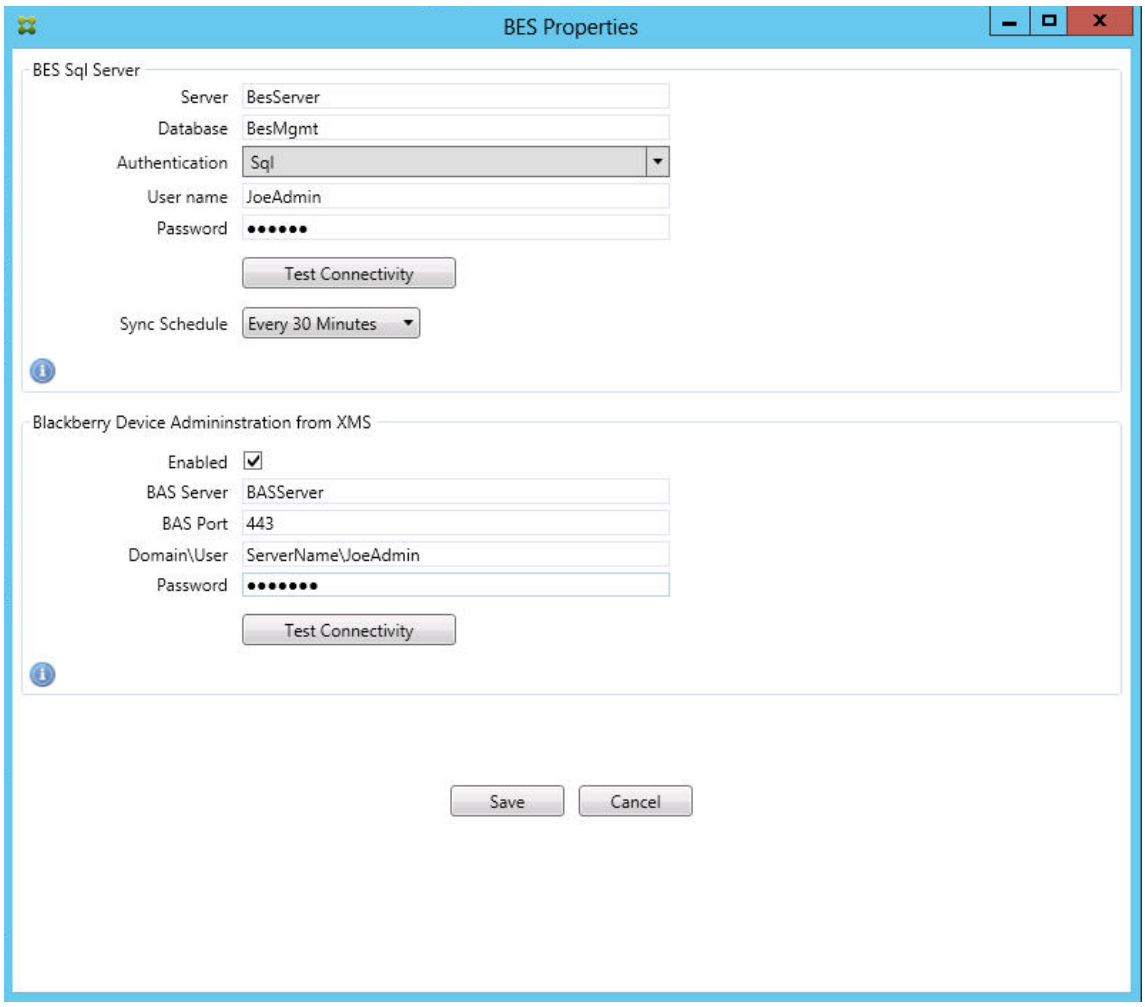
© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Defina o tipo de Service Transport, como **HTTP** ou **HTTPS**, do serviço do Provedor de Serviços Móveis.
- Defina a **Service Port** (normalmente 80 ou 443) do serviço do Provedor de Serviços Móveis. Se você usar a porta 443, ela exigirá um certificado SSL associado a ela no IIS.
- Defina o **Authorization Group** ou **User**. Isso define o usuário ou o conjunto de usuários que poderá se conectar ao serviço do Provedor de Serviços Móveis do XenMobile.
- Defina se as consultas do ActiveSync estão ativadas ou não. Se as consultas do ActiveSync estiverem ativadas para o servidor XenMobile, o tipo de instantâneo para um ou mais Exchange Servers deverá ser definido como **Deep**. Essa configuração pode ter custos de desempenho significativos para tirar instantâneos.
- Por padrão, os dispositivos ActiveSync que correspondam à expressão regular WorxMail.* não serão enviados para o XenMobile. Para alterar esse comportamento, altere o campo **Filter ActiveSync** conforme necessário.
  Em branco significa que todos os dispositivos são encaminhados ao XenMobile.
- Clique em **Salvar**.

14. Opcionalmente, configure uma ou mais instâncias do BlackBerry Enterprise Server (BES): clique em **Add** e digite o nome do servidor do BES SQL Server.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Insira o nome do banco de dados de gerenciamento do BES.
- Selecione o modo **Authentication**. Se você selecionar a autenticação Integrated do Windows, a conta de usuário do serviço conector de Endpoint Management para Exchange ActiveSync é a conta usada para conectar-se ao SQL Server do BES. Se você também escolher a conexão Integrated do Windows para a conexão do banco de dados do conector de Endpoint Management para Exchange ActiveSync, a conta do Windows especificada aqui também deverá receber acesso ao banco de dados do conector de Endpoint Management para Exchange ActiveSync.
- Se você selecionar **SQL authentication**, digite o nome do usuário e a senha.
- Defina o **Sync Schedule**. Esse é o calendário usado para conexão com o SQL Server do BES e verifica se há alguma atualização de dispositivo.
- Clique em **Test Connectivity** para verificar a conectividade com o SQL Server. Se você selecionar Windows Integrated, esse teste usará o usuário atualmente conectado e não o serviço conector do Endpoint Management para Exchange ActiveSync e, portanto, não testará com precisão a autenticação do SQL.
- Para dar suporte a Wipe ou ResetPassword de dispositivos BlackBerry a partir do XenMo-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

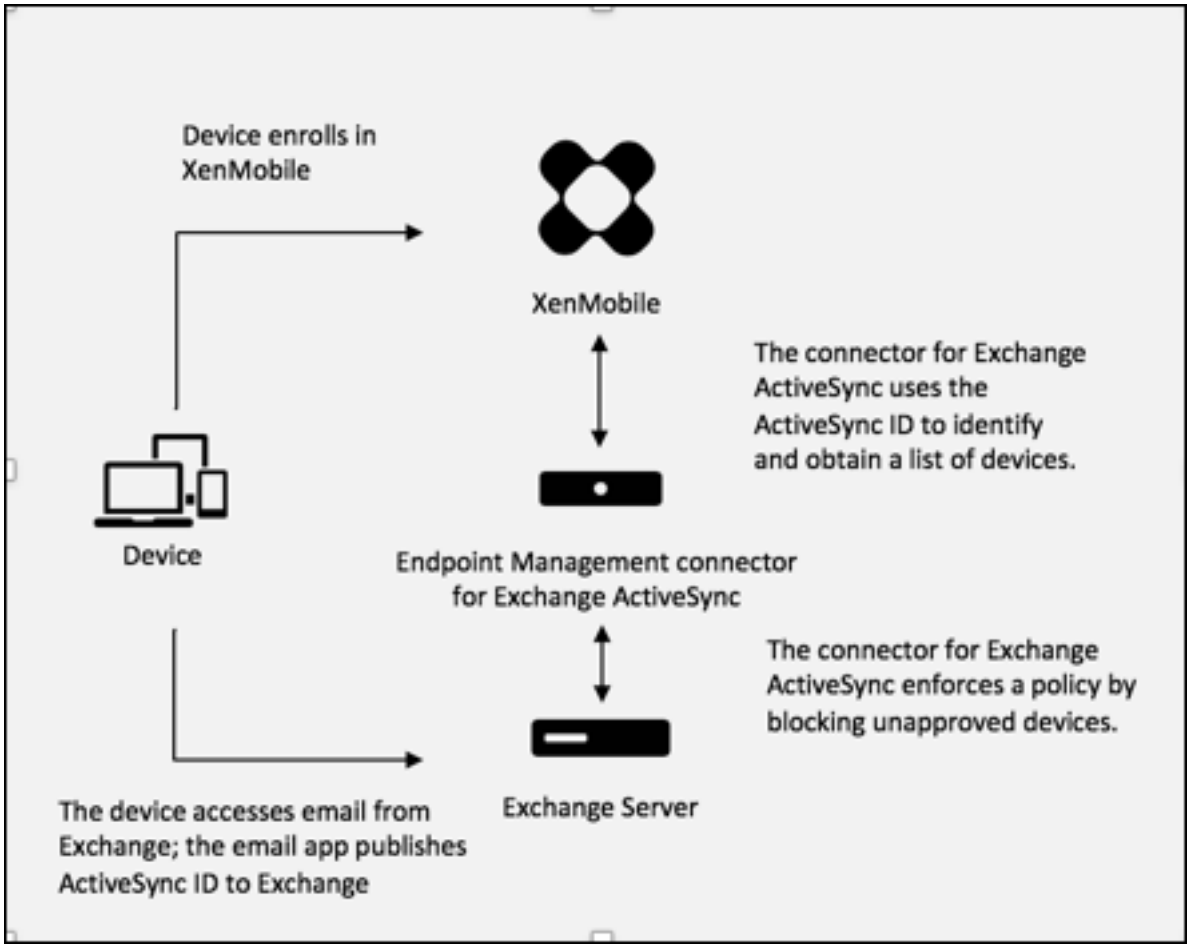
bile, marque a caixa de seleção **Enabled**.
- Insira o nome de domínio totalmente qualificado (FQDN) do BES.
- Insira a porta do BES usada para o serviço da Web de administração.
- Insira o usuário totalmente qualificado e a senha exigidos pelo serviço do BES.
- Clique em **Test Connectivity** para testar a conexão com o BES.
- Clique em **Salvar**.

Impor políticas de email com IDs do ActiveSync

Sua política de email corporativo pode ditar que determinados dispositivos não sejam aprovados para o uso de email corporativo. Para cumprir essa política, você deseja garantir que os funcionários não consigam acessar o email corporativo desses dispositivos. O conector de Endpoint Management para Exchange ActiveSync e o XenMobile trabalham em conjunto para impor essa política de email. O XenMobile define a política de acesso a email corporativo e, quando um dispositivo não aprovado se registra no XenMobile, o conector de Endpoint Management para Exchange ActiveSync impõe a política.

O cliente de email em um dispositivo se apresenta para o Exchange Server (ou o Office 365) usando o ID de dispositivo, também conhecido como o ActiveSync ID, que é usado para identificar o dispositivo. O Secure Hub obtém um identificador semelhante e o envia para o XenMobile quando o dispositivo se registra. Ao comparar os dois IDs de dispositivo, o conector de Endpoint Management para Exchange ActiveSync pode determinar se um dispositivo específico deve ter acesso a email corporativo. A figura a seguir ilustra esse conceito:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Se o XenMobile enviar ao conector de Endpoint Management para Exchange ActiveSync um ID do ActiveSync diferente do ID que o dispositivo publica no Exchange, o conector de 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 email apresenta ao Exchange. Para atenuar esse problema, você pode fazer o seguinte:

- Na plataforma Samsung SAFE, envie por push a configuração do ActiveSync do dispositivo do XenMobile.
- Em todas as outras plataformas Android, envie por push o aplicativo TouchDown e a configuração do ActiveSync do TouchDown a partir do XenMobile.

No entanto, isso não impede que um funcionário instale um cliente de email diferente do TouchDown em um dispositivo Android. Para garantir que a sua política de acesso ao email corporativo seja aplicada corretamente, você poderá adotar uma postura de segurança defensiva e configurar o conector de Endpoint Management para Exchange ActiveSync para bloquear emails definindo a política estática como Deny by default. Isso significa que se um funcionário configurar um cliente de email

© 1999-2019 Citrix Systems, Inc. All rights reserved.

diferente do TouchDown em um dispositivo Android, e se a detecção do ID do ActiveSync não funcionar corretamente, o funcionário terá o acesso ao email corporativo negado.

Regras de controle de acesso

O conector de Endpoint Management para Exchange ActiveSync fornece uma abordagem baseada em regras para configurar dinamicamente o controle de acesso a dispositivos Exchange ActiveSync. Um conector de Endpoint Management para Exchange ActiveSync consiste em duas partes: uma expressão correspondente e um estado de acesso desejado (Permitir ou Bloquear). Uma regra pode ser avaliada em relação um determinado dispositivo Exchange ActiveSync para determinar se ela é aplicável ou corresponde ao dispositivo. Existem vários tipos de expressões correspondentes; 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.

Em qualquer momento durante a adição, remoção e reorganização das regras na lista de regras, clicar no botão **Cancel** reverterá a lista de regras para o estado em que estava quando ela foi aberta pela primeira vez. A menos que você clique em **Save**, todas as alterações feitas nessa janela serão perdidas se você fechar a ferramenta Configure.

O conector do Endpoint Management for Exchange ActiveSync tem três tipos de regras: regras locais, regras do XenMobile Serfver (também conhecidas como regras XDM) e a regra de acesso padrão.

Regras locais: as regras locais têm a prioridade mais alta: se um dispositivo corresponde a uma regra local, a avaliação da regra é interrompida. Nem as regras do XenMobile nem a regra de acesso padrão serão consultadas. As regras locais são configuradas localmente para o conector de Endpoint Management para Exchange ActiveSync na guia **Configure > Access Rules > Local Rules**. A correspondência de suporte é baseada na associação de um usuário em um determinado grupo do Active Directory. A correspondência de suporte é baseada em expressões regulares para os seguintes campos:

- Active Sync Device ID
- Tipo de dispositivo ActiveSync
- Nome UPN
- ActiveSync User Agent (normalmente a plataforma do dispositivo ou o cliente de email)

Desde que um instantâneo principal tenha sido concluído e localizado dispositivos, você deverá conseguir adicionar uma regra normal ou de expressão regular. Se um instantâneo principal não tiver sido concluído, você poderá adicionar somente regras de expressão regular.

Regras do servidor XenMobile: regras do servidor XenMobile são referências a um servidor XenMobile externo que fornece regras sobre dispositivos gerenciados. O servidor XenMobile pode ser configurado com suas próprias regras de alto nível que identificam os dispositivos que devem ser permitidos ou bloqueados com base nas propriedades conhecidas do XenMobile, como se o dispositivo tem jail-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

break ou se o dispositivo contém aplicativos proibidos. O XenMobile avalia as regras de alto nível e produz um conjunto de IDs de dispositivos ActiveSync permitidos ou bloqueados, que são entregues ao conector de Endpoint Management para Exchange ActiveSync.

Regra de acesso padrão: a regra de acesso padrão é exclusiva, no sentido que ela potencialmente pode corresponder a cada dispositivo e sempre é avaliada por último. Essa regra é a regra genérica, 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 será determinado pelo estado de acesso desejado da regra de acesso padrão.

- **Default Access – Allow:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será permitido.
- **Default Access – Block:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será bloqueado.
- **Default Access - Unchanged:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server não terá seu estado de acesso modificado de qualquer forma pelo conector de Endpoint Management para Exchange ActiveSync. Se um dispositivo tiver sido colocado no modo Quarantine pelo Exchange, nenhuma ação será tomada; por exemplo, a única maneira de remover um dispositivo do modo Quarantine é ter uma regra Local ou o XDM explicitamente substituir a quarentena.

Sobre as avaliações de regra

Para cada dispositivo que o Exchange relata para o conector de Endpoint Management para Exchange ActiveSync, as regras são avaliadas em sequência, da prioridade mais alta para a mais baixa, desta forma:

- Regras locais
- Regras de servidor XenMobile
- Regra de acesso padrão

Quando uma correspondência é encontrada, a avaliação é interrompida. Por exemplo, se uma regra local corresponder a um determinado dispositivo, ele não será avaliado em relação a qualquer das regras do servidor XenMobile ou à regra de acesso padrão. Isso é verdadeiro também em um determinado tipo de regra. Por exemplo, se houver mais de uma única correspondência para um determinado dispositivo na lista de regras locais, assim que a primeira correspondência seja encontrada, a avaliação é interrompida.

O conector de Endpoint Management para Exchange ActiveSync reavalia o conjunto de regras atualmente definido quando as propriedades do dispositivo são alteradas ou quando os dispositivos são adicionados ou removidos ou quando as próprias regras são alteradas. Os instantâneos principais detectam as alterações na propriedade de dispositivo e as remoções em intervalos configuráveis. Os instantâneos secundários detectam novos dispositivos em intervalos configuráveis.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O Exchange ActiveSync também apresenta regras que regem o acesso. É importante entender como essas regras funcionam no contexto do conector de Endpoint Management para Exchange ActiveSync. O Exchange pode ser configurado com três níveis de regras: isenções pessoais, regras de dispositivo e configurações de organização. O conector de Endpoint Management para Exchange ActiveSync automatiza o controle de acesso emitindo programaticamente as solicitações remotas do PowerShell para afetar as listas de isenções pessoais. Elas são listas de IDs de dispositivo Exchange ActiveSync permitidos ou bloqueados associados a uma determinada caixa de correio. Quando implantado, o conector de Endpoint Management para Exchange ActiveSync efetivamente assume o gerenciamento do recurso de listas de isenção no Exchange. FPara obter detalhes, consulte este Artigo da Microsoft.

Analisar é especialmente útil em situações nas quais várias regras foram definidas para o mesmo campo. Você pode solucionar problemas das relações entre as regras. Execute a análise da perspectiva dos campos de regra; por exemplo, as regras são analisadas em grupos com base no campo que está sendo correspondido, como ID de dispositivo ActiveSync, tipo de dispositivo ActiveSync, Usuário, Agente do Usuário e assim por diante.

Terminologia de regra

- **Regra predominante:** uma predominância ocorre quando mais de uma única regra poderia ser aplicada ao mesmo dispositivo. Como as regras são avaliadas por prioridade na lista, as instâncias de regra de menor prioridade que podem ser aplicadas podem nunca ser avaliadas.
- **Regra conflitante:** um conflito ocorre quando mais de uma única regra poderia ser aplicada ao mesmo dispositivo, mas o acesso (Permitir/Bloquear) não é correspondente. Se as regras conflitantes não forem regras de expressão regular, um conflito sempre conotará 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 também possam ser combinadas em uma única regra de expressão regular ou que não estejam duplicando a funcionalidade. Uma regra suplementar também pode entrar em conflito no respectivo acesso (Permitir/Bloquear).
- **Regra principal:** a regra principal é a regra que foi clicada na caixa de diálogo. A regra é indicada visualmente por uma borda sólida que a contorna. A regra também terá uma ou duas setas verdes, apontando para cima ou para baixo. Se uma seta apontar para cima, ela indicará que existem regras auxiliares que precedem a regra principal. Se uma seta apontar para baixo, ela indicará que existem regras auxiliares que se seguem a regra principal. Somente uma única regra principal pode estar ativa em determinado momento.
- **Regra auxiliar:** uma regra auxiliar está relacionada de alguma forma à regra principal por meio de substituição, conflito ou uma relação suplementar. As regras são indicadas visualmente por uma borda tracejada que as contorna. Pode haver uma a muitas regras auxiliares para cada regra principal. Quando você clica em qualquer entrada sublinhada, a regra auxiliar ou as regras

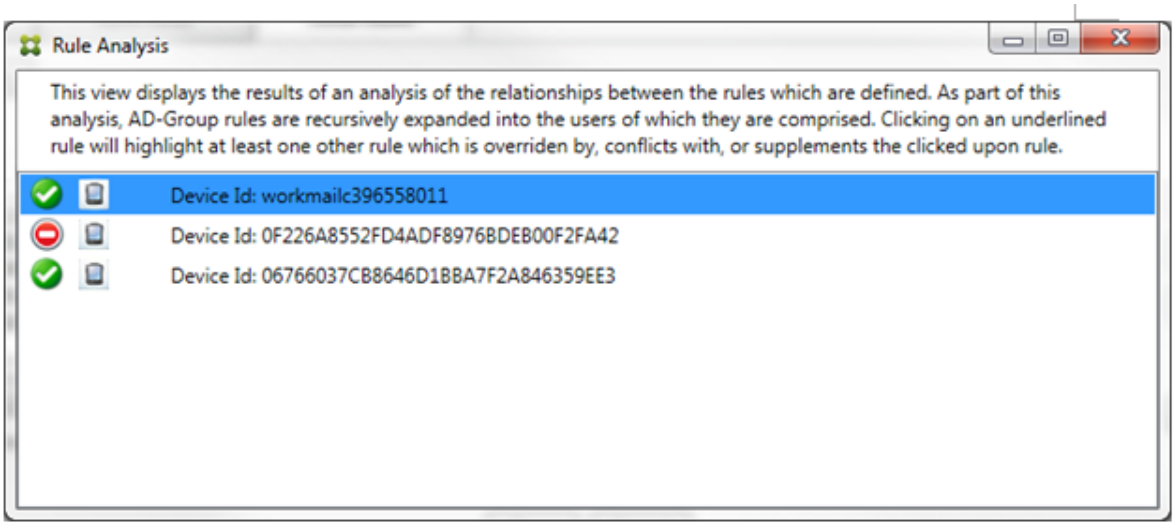
© 1999-2019 Citrix Systems, Inc. All rights reserved.

que são realçadas são sempre da perspectiva da regra principal. Por exemplo, a regra auxiliar é substituída pela regra principal e/ou a regra auxiliar entrará em conflito no respectivo acesso com a regra principal, e/ou a regra auxiliar suplementará a regra principal.

Como os tipos de regras aparecem na caixa de diálogo Rule Analysis

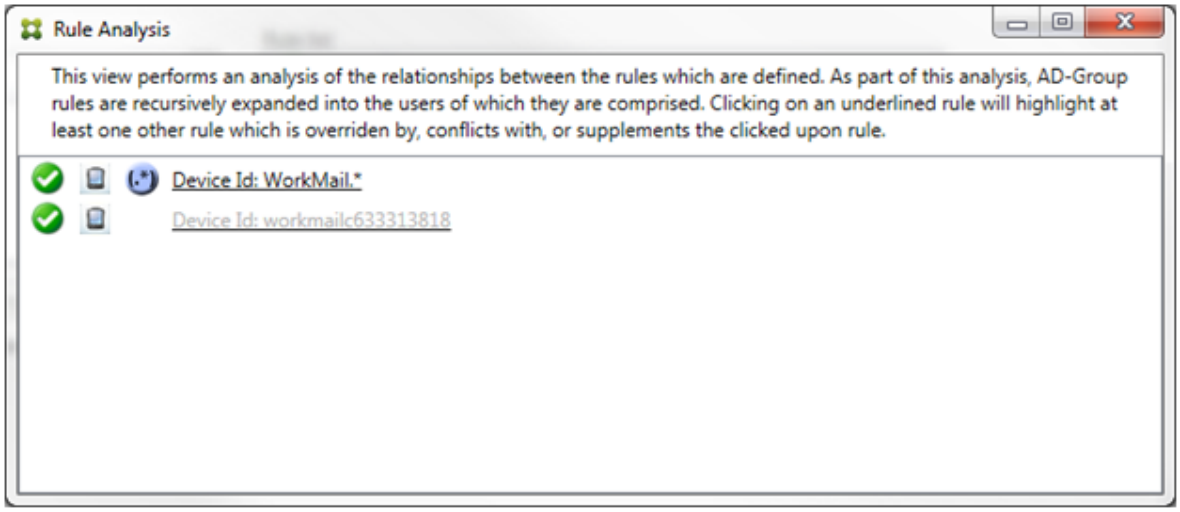
Quando não existirem conflitos, substituições ou suplementos, a caixa de diálogo Rule Analysis não apresentará entradas sublinhadas. Clicar em qualquer um dos itens não terá impacto; por exemplo, os visuais normais de item selecionado ocorrem.

A janela Análise de regras tem uma caixa de seleção que, quando selecionada, exibe somente as regras que são conflitos, substituições, redundâncias ou suplementos.

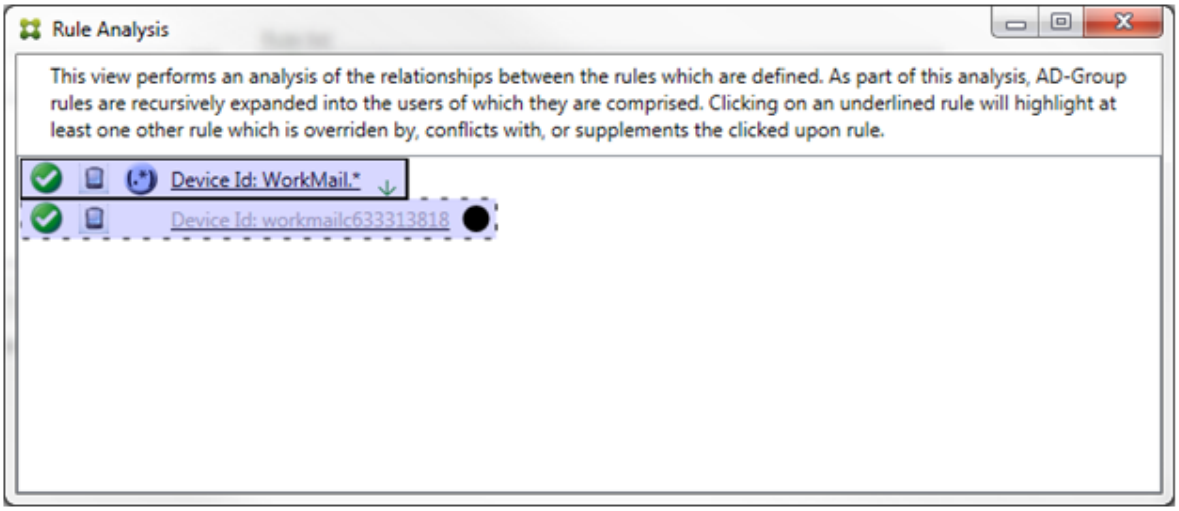


Quando ocorrer uma substituição, pelo menos duas regras serão sublinhadas: a regra principal e a regra ou as regras auxiliares. Pelo menos uma regra auxiliar é exibida em uma fonte mais fina para indicar que a regra foi substituída por uma regra de prioridade mais alta. Você pode clicar na regra predominante para descobrir qual regra ou regras a substituíram. Sempre que uma regra predominante for realçada como resultado de a regra ser a regra principal ou auxiliar, um círculo preto é exibido 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 é exibida da seguinte forma:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

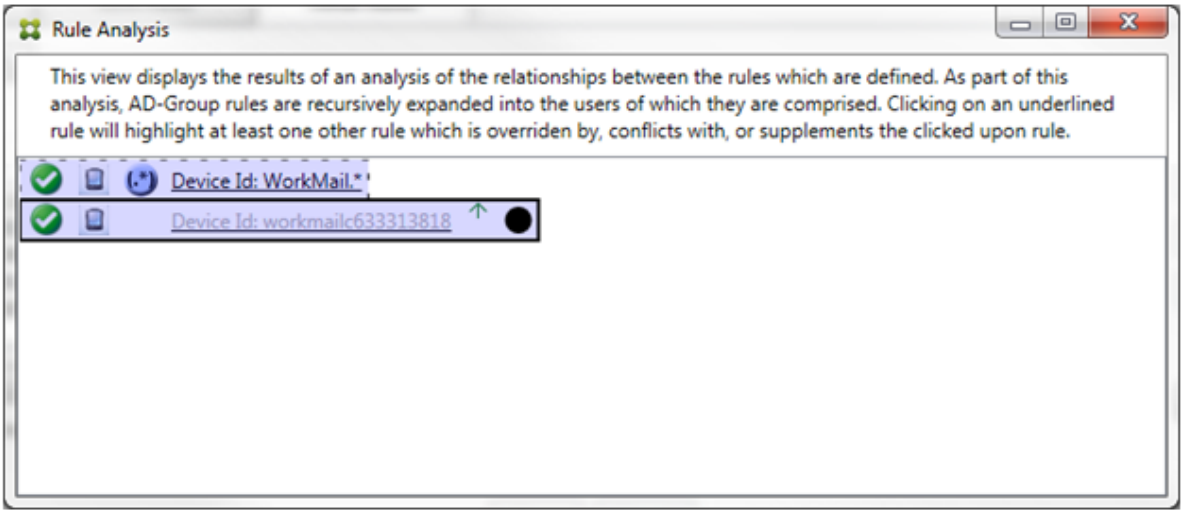


Quando você clica na regra de prioridade mais alta, a caixa de diálogo é exibida da seguinte forma:



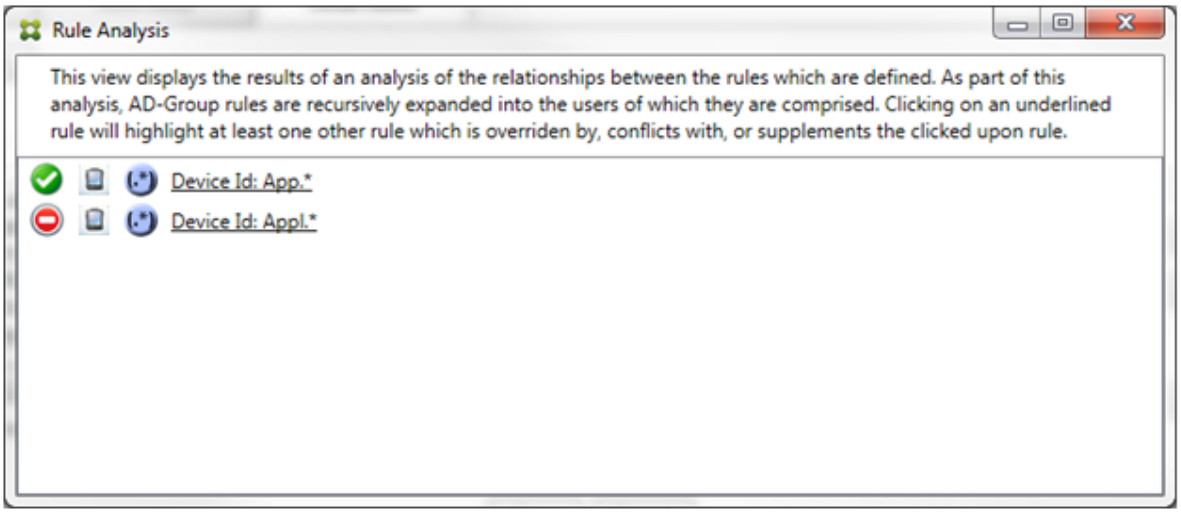
Nesse exemplo, a regra de expressão regular `WorkMail.*` é a regra principal (indicada pela borda sólida) e a regra normal `workmailc633313818` é uma regra auxiliar (indicada pela borda tracejada). O ponto preto ao lado da regra auxiliar é uma indicação visual adicional de que a regra está inativa (nunca será avaliada) devido à regra de expressão regular de prioridade mais alta que a precede. Depois de clicar na regra predominante, a caixa de diálogo é exibida da seguinte forma:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 principal (indicada pela borda sólida). Nesse 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 rapidamente identifica qual regra ou regras a substituíram.

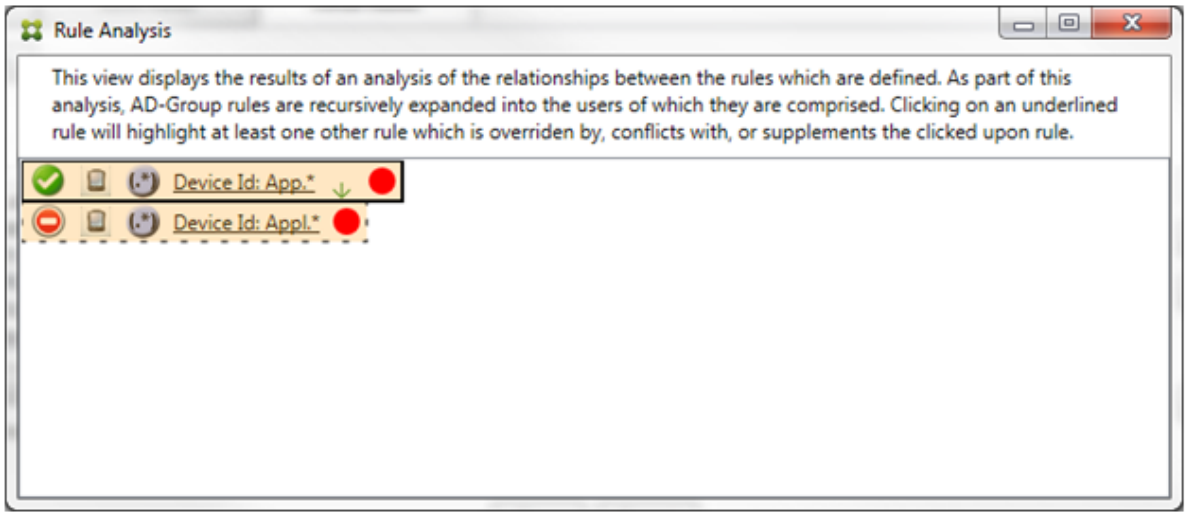
Quando ocorrer um conflito, pelo menos duas regras serão sublinhadas: a regra principal e a regra ou as regras auxiliares. As regras em conflito são indicadas por um ponto vermelho. Regras que só entram em conflito uma com a outra são possíveis somente com duas ou mais regras de expressão regular definidas. Em todos os outros cenários de conflito, não haverá somente um conflito, mas uma substituição envolvida. Antes de clicar em qualquer uma das regras em um exemplo simples, a caixa de diálogo é exibida da seguinte forma:



Quando se inspeciona as duas regras de expressão regular, fica 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, mesmo que a segunda re-

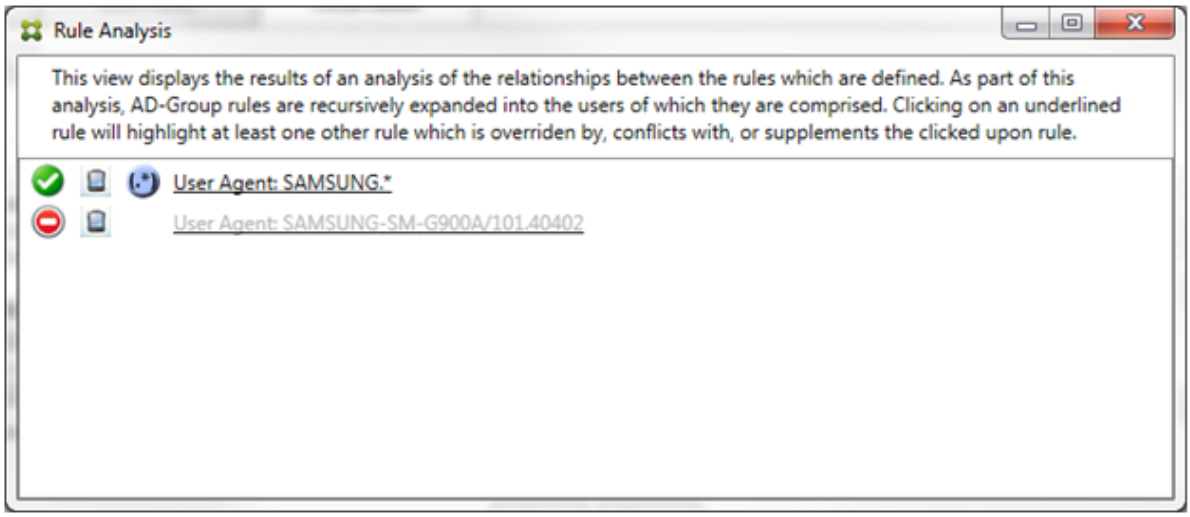
© 1999-2019 Citrix Systems, Inc. All rights reserved.

gra negue todos os dispositivos com um ID de dispositivo que contém “Appl”, nenhum dispositivo com esses critérios de correspondência jamais será negado, devido à precedência mais alta da regra permitir. Depois de clicar na primeira regra, a caixa de diálogo é exibida da seguinte forma:



No cenário anterior, tanto a regra principal (a regra de expressão regular `App.*`) quanto a regra auxiliar (a regra de expressão regular `Appl.*`) são realçadas em amarelo. Trata-se simplesmente de um aviso visual para alertar para o fato de que você aplicou mais de uma única regra de expressão regular a um único campo passível de correspondência, o que pode significar um problema de redundância ou algo mais sério.

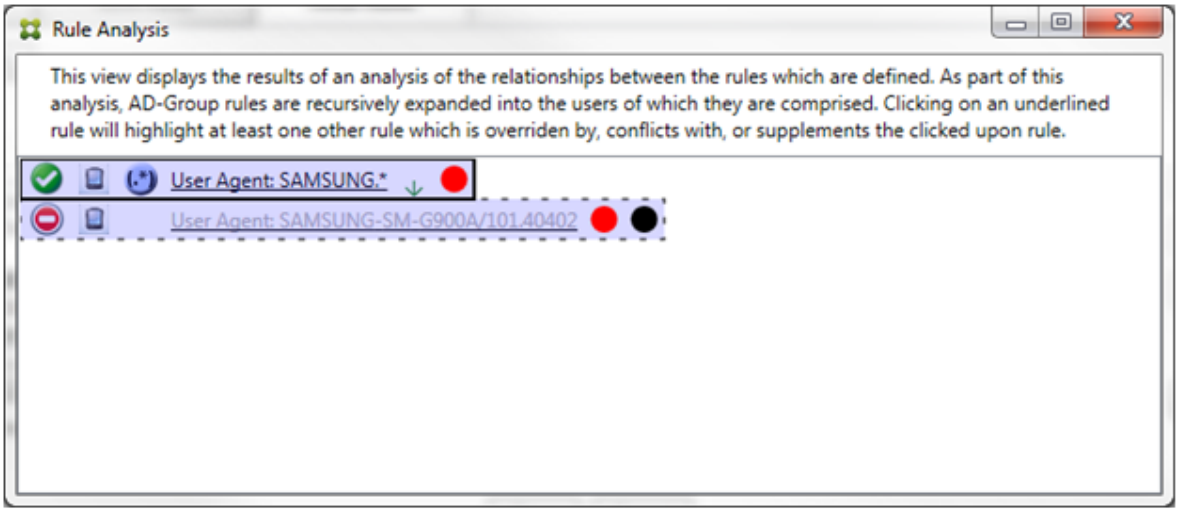
Em um cenário com um conflito e uma predominância, tanto a regra principal (a regra de expressão regular `App.*`) quanto a regra auxiliar (a regra de expressão regular `Appl.*`) são realçadas em amarelo. Trata-se simplesmente de um aviso visual para alertar para o fato de que você aplicou mais de uma única regra de expressão regular a um único campo passível de correspondência, o que pode significar um problema de redundância ou algo mais sério.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

É fácil ver, no exemplo anterior, que a primeira regra (a regra de expressão regular `SAMSUNG.*`) não somente substitui a regra seguinte (a regra normal `SAMSUNG-SM-G900A/101.40402`), mas as duas regras diferem no respectivo acesso (a principal especifica Permitir, a auxiliar especifica Bloquear). A segunda regra (a regra normal `SAMSUNG-SM-G900A/101.40402`) é exibida em um texto mais fino para indicar que ela foi substituída e, portanto, está inativa.

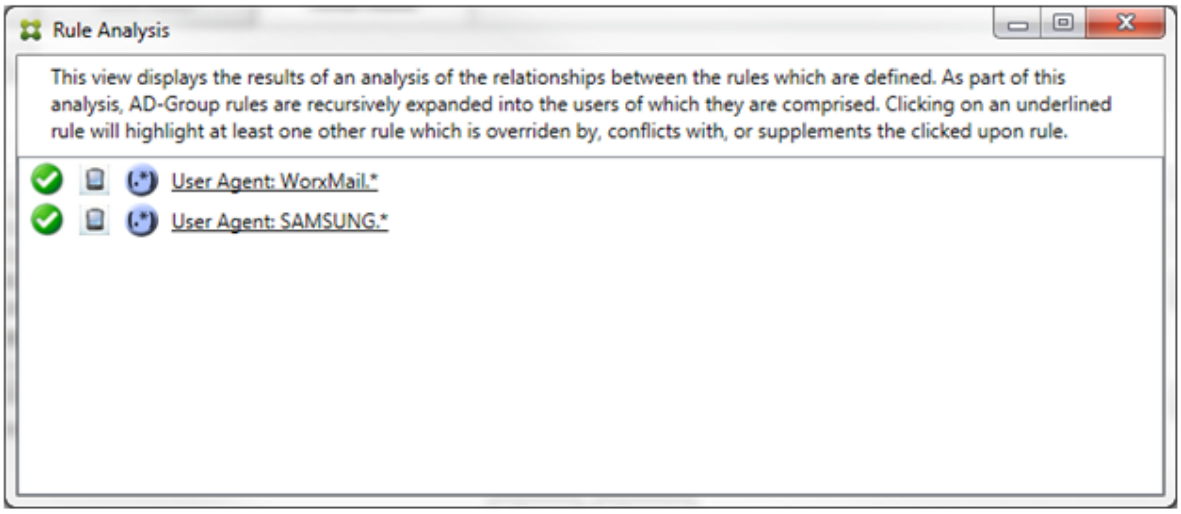
Depois de clicar na regra de expressão regular, a caixa de diálogo é exibida da seguinte forma:



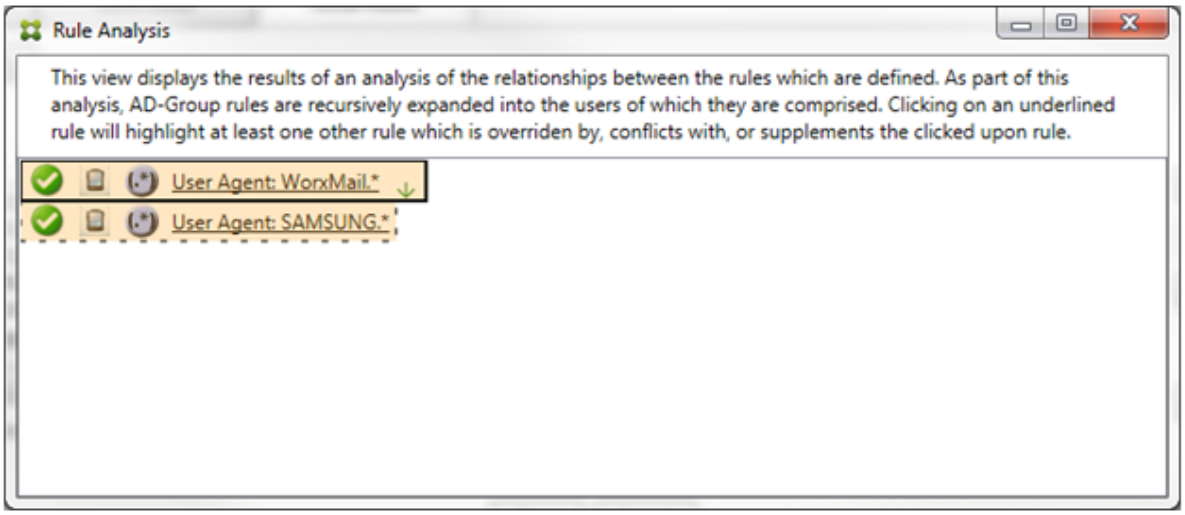
A regra principal (a regra de expressão regular `SAMSUNG.*`) é seguida por um ponto vermelho para indicar que o estado de acesso dela entra em conflito com uma ou mais regras auxiliares. A regra auxiliar (regra normal `SAMSUNG-SM-G900A/101.40402`) é seguida por um ponto vermelho para indicar que seu estado de acesso está em conflito 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 principal e a regra ou as regras auxiliares. As regras que somente suplementam uma à outra envolverão apenas regras de expressão regular. Quando regras suplementam uma à outra, elas são indicadas por uma sobreposição amarela. Antes de clicar em qualquer uma das regras em um exemplo simples, a caixa de diálogo é exibida da seguinte forma:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A inspeção visual facilmente revela que ambas as regras são regras de expressão regular que foram aplicadas ao campo de ID de dispositivo ActiveSync no conector de Endpoint Management para Exchange ActiveSync. Depois de clicar na primeira regra, a caixa de diálogo tem a seguinte aparência:

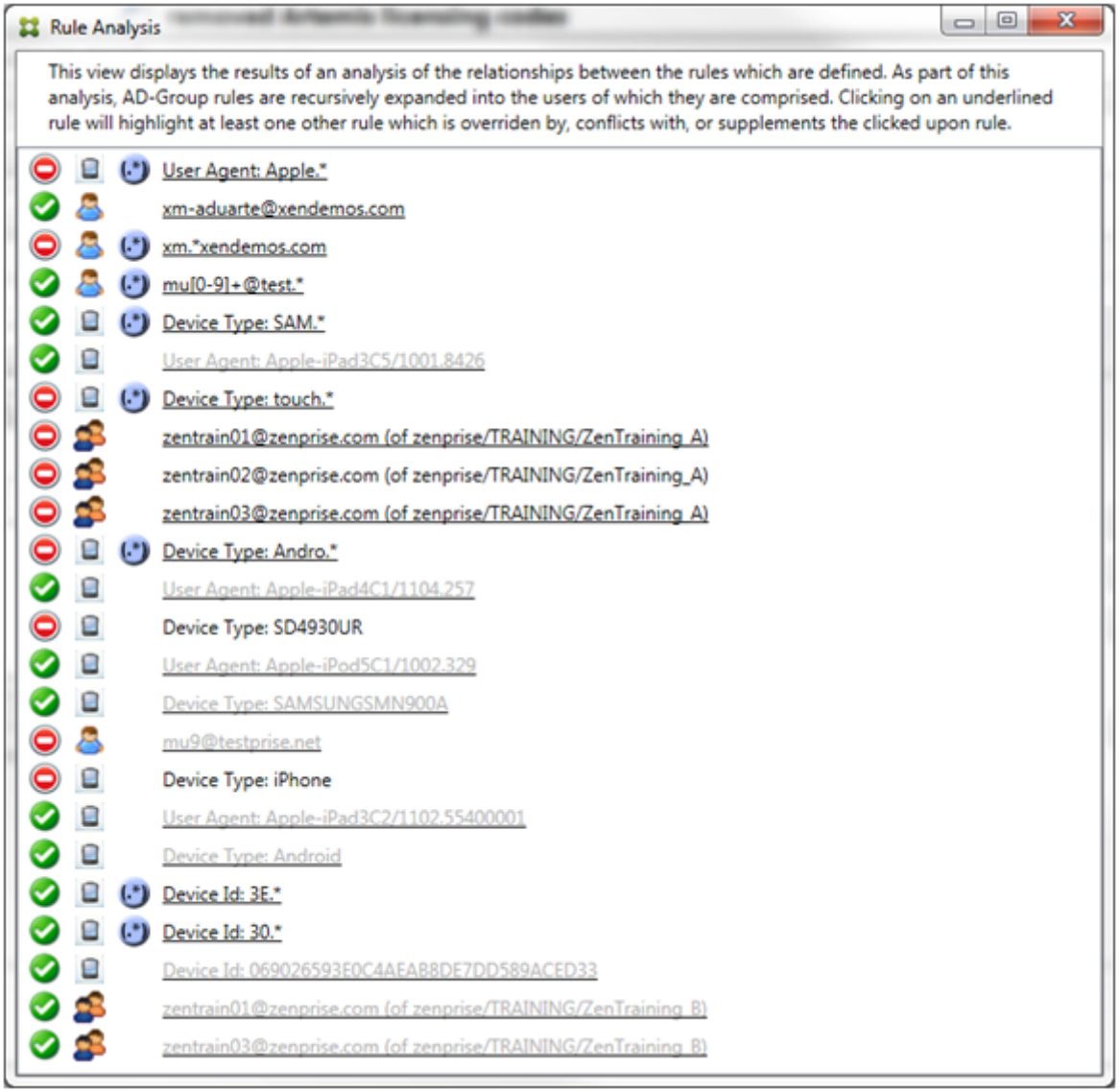


A regra principal (a regra de expressão regular `WorkMail.*`) é realçada com uma sobreposição amarela para indicar que existe pelo menos uma regra auxiliar a mais que é uma expressão regular. A regra auxiliar (a regra de expressão regular `SAMSUNG.*`) é realçada com uma sobreposição amarela para indicar que ela e a regra principal são regras de expressão regular aplicadas ao mesmo campo no conector de Endpoint Management para Exchange ActiveSync. Nesse caso, esse campo é o ID do dispositivo do ActiveSync. As expressões regulares podem ou não se sobrepor. Cabe a você decidir se as expressões regulares foram devidamente trabalhadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exemplo de uma expressão complexa

Muitas substituições, conflitos ou suplementos possíveis podem ocorrer, tornando impossível oferecer um exemplo de todos os cenários possíveis. O exemplo a seguir discute o que não fazer, servindo também para ilustrar todo o poder da construção visual de análise de regra. A maioria dos itens estão sublinhados na figura a seguir. Muitos dos itens são exibidos em uma fonte mais fina, o que indica que a regra em questão foi substituída por uma regra de prioridade mais alta de alguma maneira. Muitas regras de expressão regular também estão incluídas na lista, conforme indicado pelo ícone  .

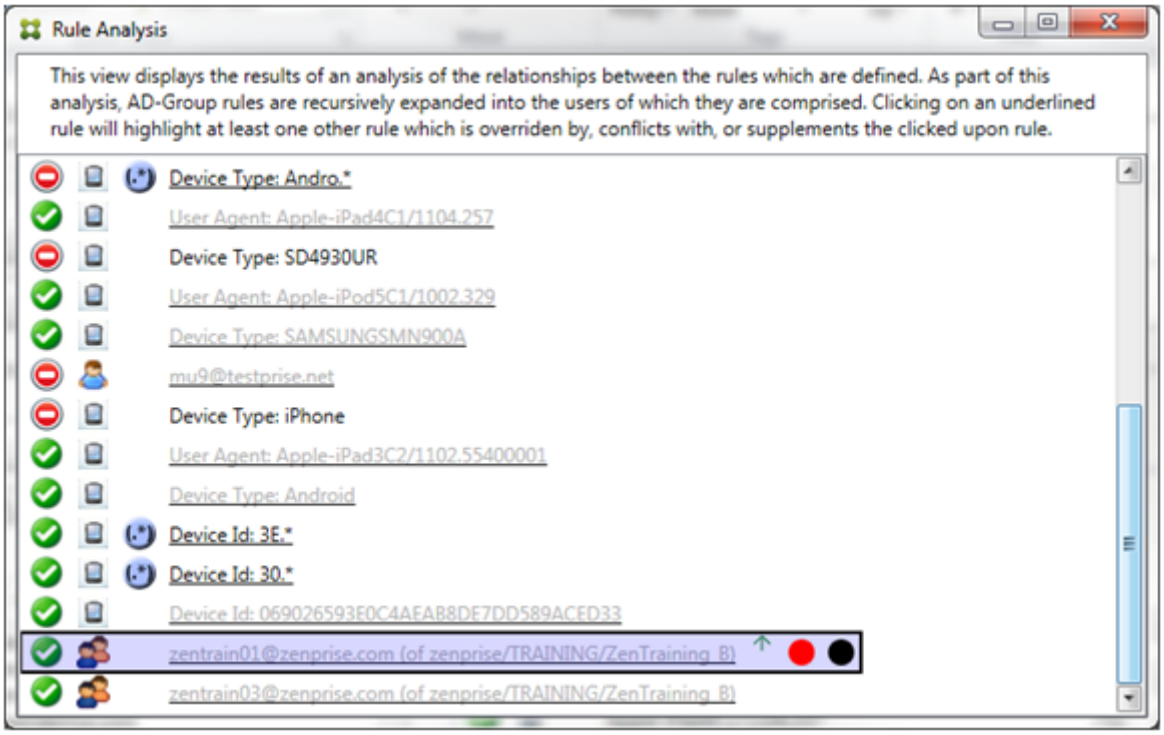


Como analisar uma substituição

Para ver qual regra ou regras substituíram uma regra específica, clique nela.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exemplo 1: Esse exemplo examina por que `zentrain01@zenprise.com` foi substituída.

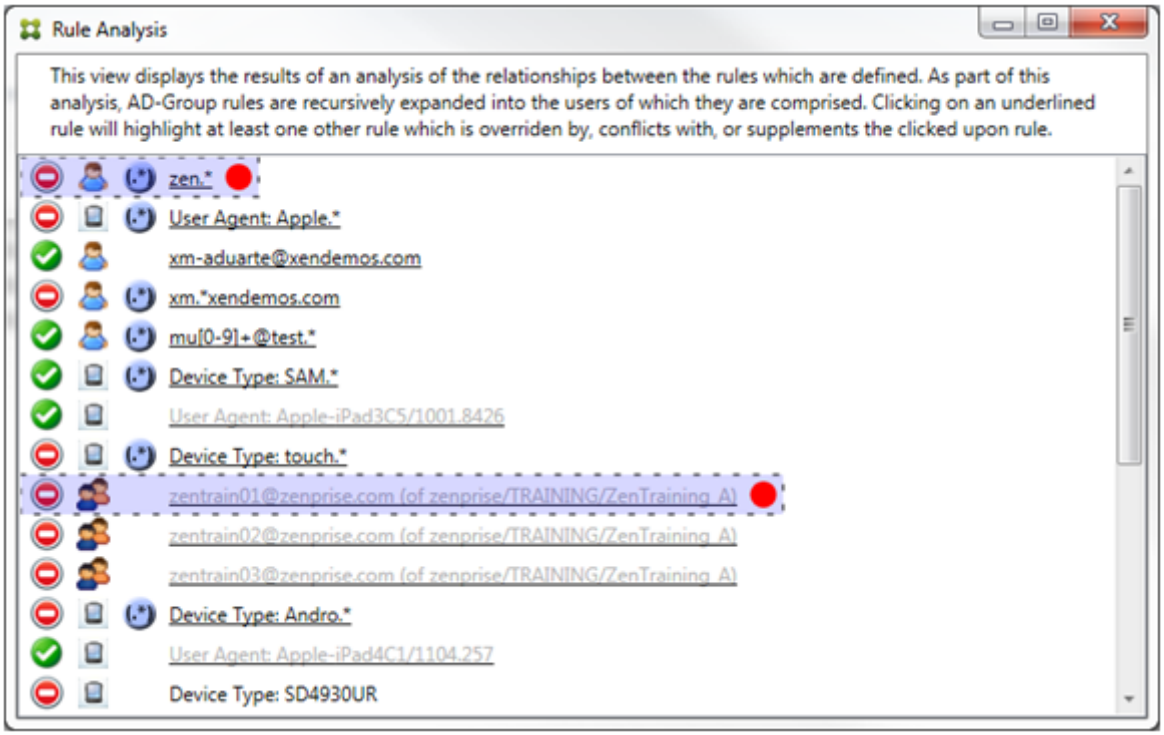


A regra principal (regra `zenprise/TRAINING/ZenTraining B`, da qual `zentrain01@zenprise.com` é um membro) apresenta as seguintes características:

- Está realçada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra ou as regras auxiliares todas se encontram acima dela).
- É seguida por um círculo vermelho e um círculo preto para indicar, respectivamente, que um ou mais regras auxiliares entram em conflito com o respectivo acesso e que a regra principal foi substituída e, portanto, está inativa.

Quando você rola para cima, vê o seguinte:

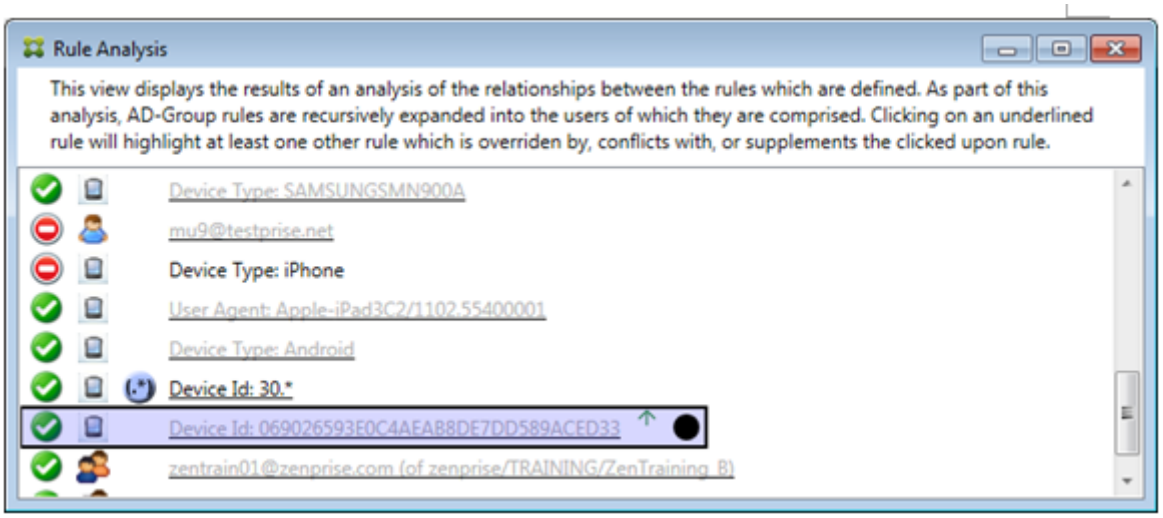
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Nesse caso, há duas regras auxiliares que substituem a regra principal: 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 mais alta do que a regra principal, a regra principal foi substituída. O acesso da regra principal é Permitir e, como o acesso da regra auxiliar é Bloquear, todas são seguidas por um círculo vermelho como indicação adicional de um conflito de acesso.

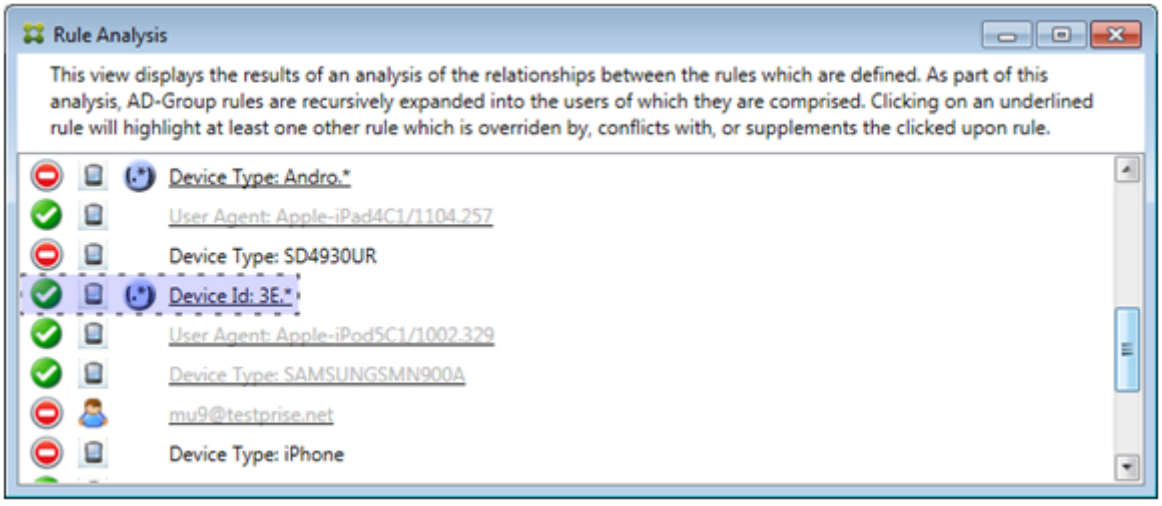
Exemplo 2: Esse exemplo mostra por que o dispositivo com um ID de dispositivo ActiveSync `069026593E0C4AEAB8DE7DD589ACED33` foi substituído:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



A regra principal (regra de ID de dispositivo normal `069026593E0C4AEAB8DE7DD589ACED33`) apresenta as seguintes características:

- Está realçada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra auxiliar se encontra acima dela).
- É seguida por um círculo preto para indicar que uma regra auxiliar substituiu a regra principal e, portanto, está inativa.



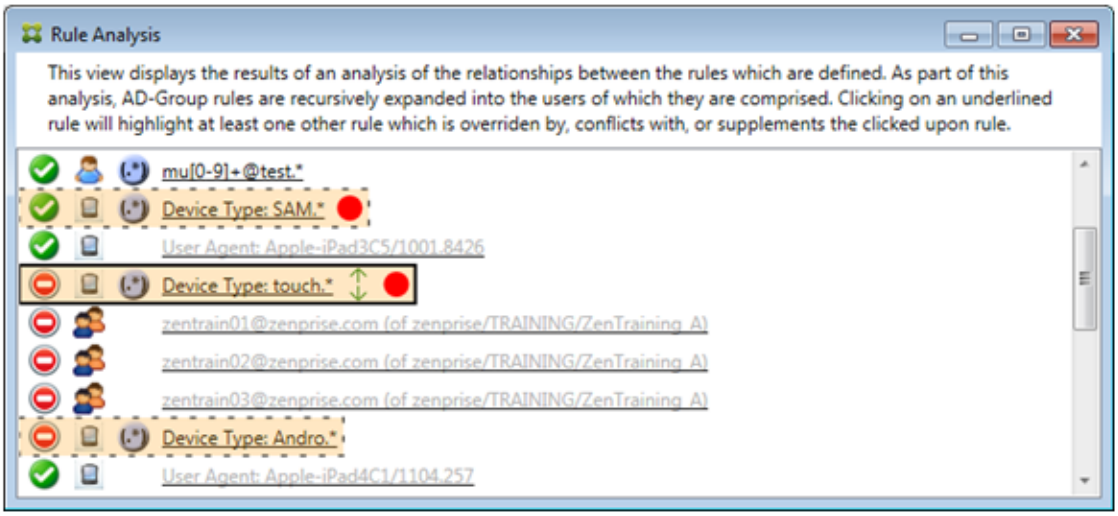
Nesse caso, uma única regra auxiliar substitui a regra principal: a regra de ID de dispositivo ActiveSync de expressão regular é `3E.*`. Como a expressão regular `3E.*` corresponderia a `069026593E0C4AEAB8DE7DD589ACED33`, a regra principal nunca será avaliada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Como analisar um suplemento e um conflito

Neste caso, a regra principal é a regra de tipo de dispositivo ActiveSync de expressão regular `touch.*`. As características são as seguintes:

- É indicada por uma borda sólida com uma sobreposição amarela, como um aviso de que há mais de uma única regra de expressão regular em funcionamento em relação a um campo de regra específico; nesse caso, o tipo de dispositivo ActiveSync.
- Duas setas apontam respectivamente para cima e para baixo, 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 dela indica que pelo menos uma regra auxiliar tem o respectivo acesso definido como Permitir, o que entra em conflito com o acesso Bloquear da regra principal
- 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 têm bordas tracejadas para indicar que são auxiliares.
- Ambas as regras auxiliares têm uma sobreposição amarela para indicar que também são aplicadas ao campo de regra do tipo de dispositivo ActiveSync.
- Em tais cenários, você deve garantir que as respectivas regras de expressão regular não sejam redundantes.



Como analisar ainda mais as regras

Este exemplo explora como as relações entre regras sempre existem na perspectiva da regra principal. O exemplo anterior mostrou como clicar na regra de expressão regular aplicada ao campo de regra do

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tipo de dispositivo com um valor de `touch.*`. Clicar na regra auxiliar `Andro.*` mostra um conjunto diferente de regras auxiliares destacadas.

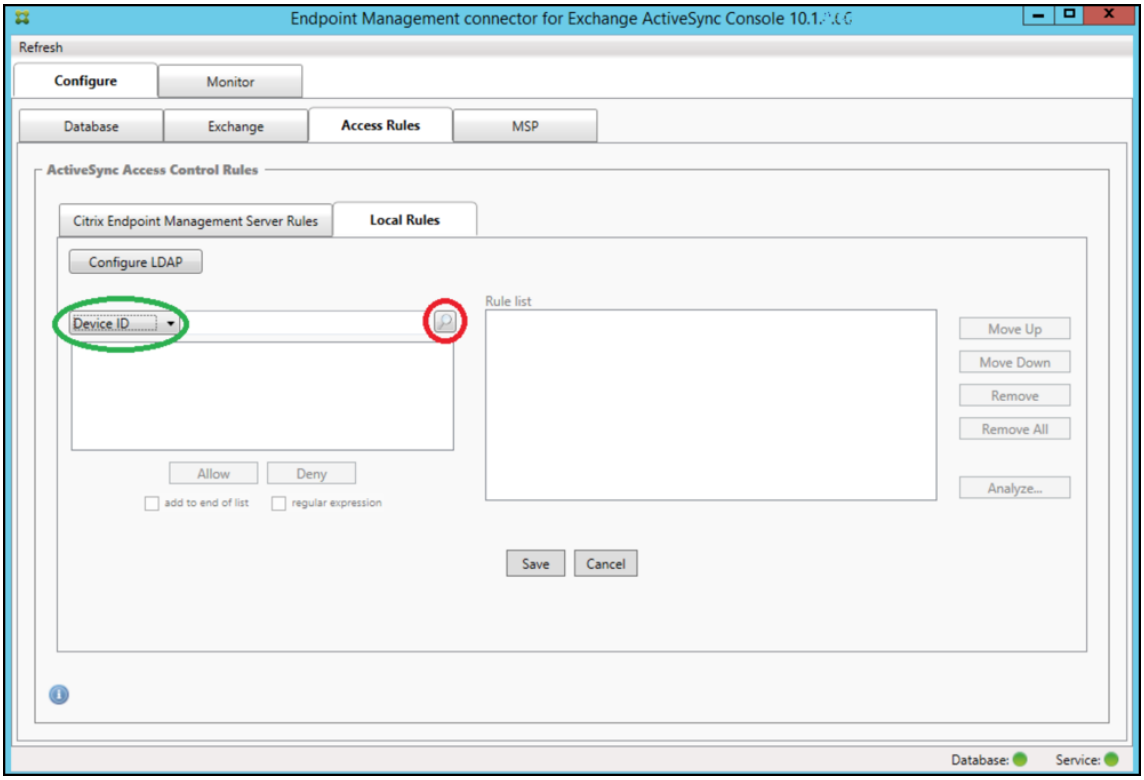


O exemplo mostra uma regra substituída que está incluída na relação de regra. Essa regra é a regra normal de tipo de dispositivo ActiveSync `Android`, que é substituída (indicada pela fonte fina e o círculo preto ao lado dela) e também entra em conflito no respectivo acesso com a regra de tipo de dispositivo ActiveSync de expressão regular da regra principal `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 era exibida como uma regra auxiliar pois, na perspectiva da regra principal naquele momento (a regra de tipo de dispositivo ActiveSync de expressão regular `touch.*`), a regra não era relacionada a ela.

Para configurar uma regra local de expressão normal

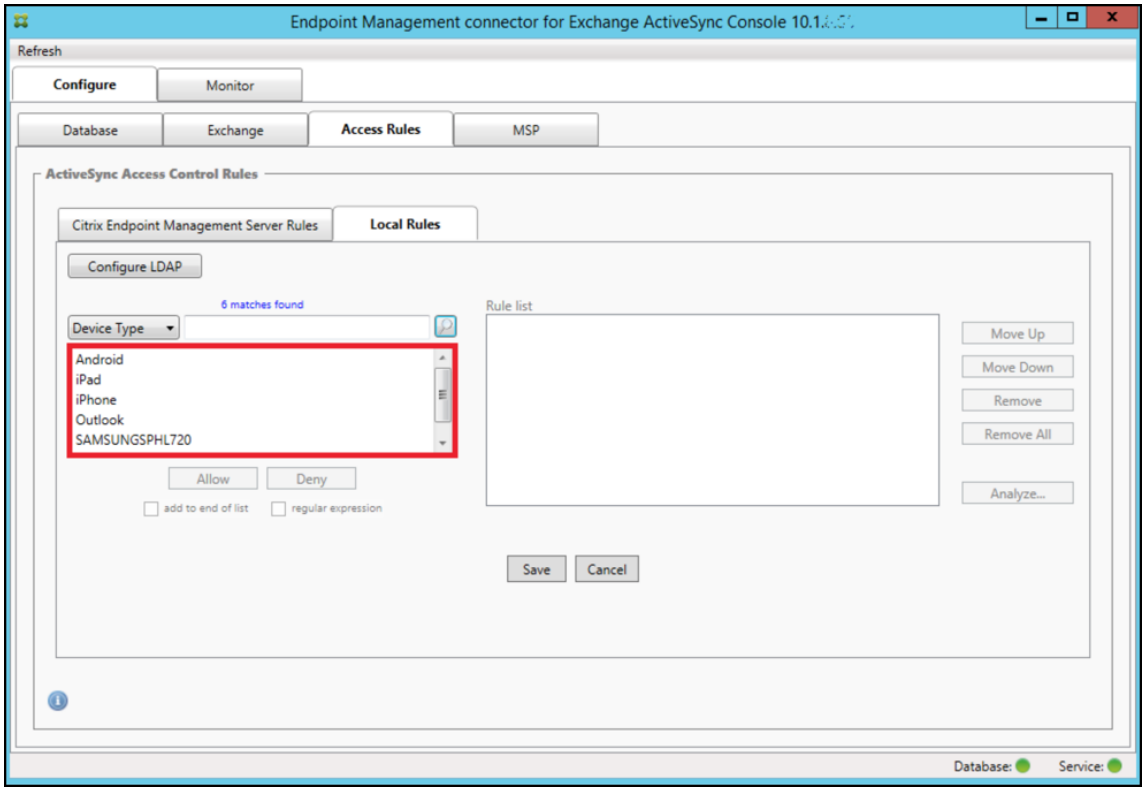
1. Clique na guia **Access Rules**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Na lista **Device ID**, selecione o campo para o qual você deseja criar uma Regra Local.
3. Clique no ícone de lupa para exibir todas as correspondências exclusivas do campo escolhido. Neste exemplo, o campo **Device Type** foi escolhido e as opções são mostradas abaixo, na caixa de lista.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

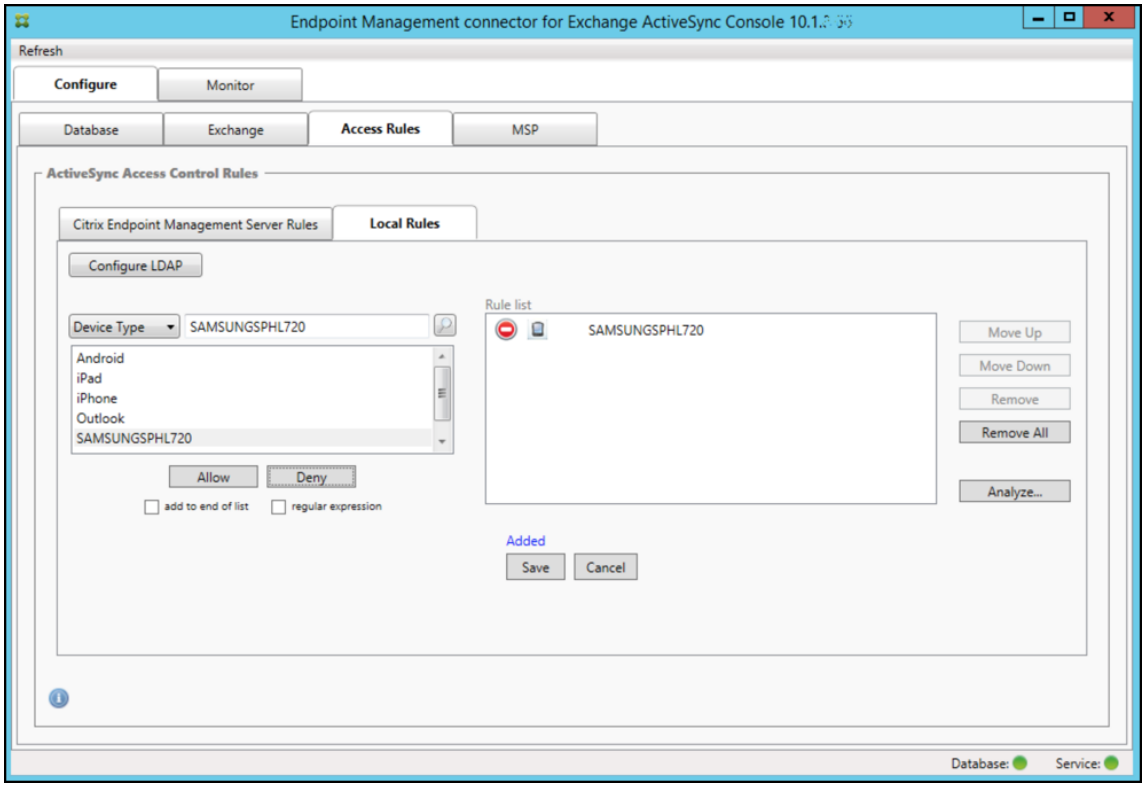


4. Clique em um dos itens na caixa de lista de resultados e, em seguida, clique em uma das seguintes opções:

   - **Allow** significa que o Exchange será configurado para permitir o tráfego do ActiveSync para todos os dispositivos correspondentes.
   - **Deny** 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 acesso negado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para adicionar uma expressão regular

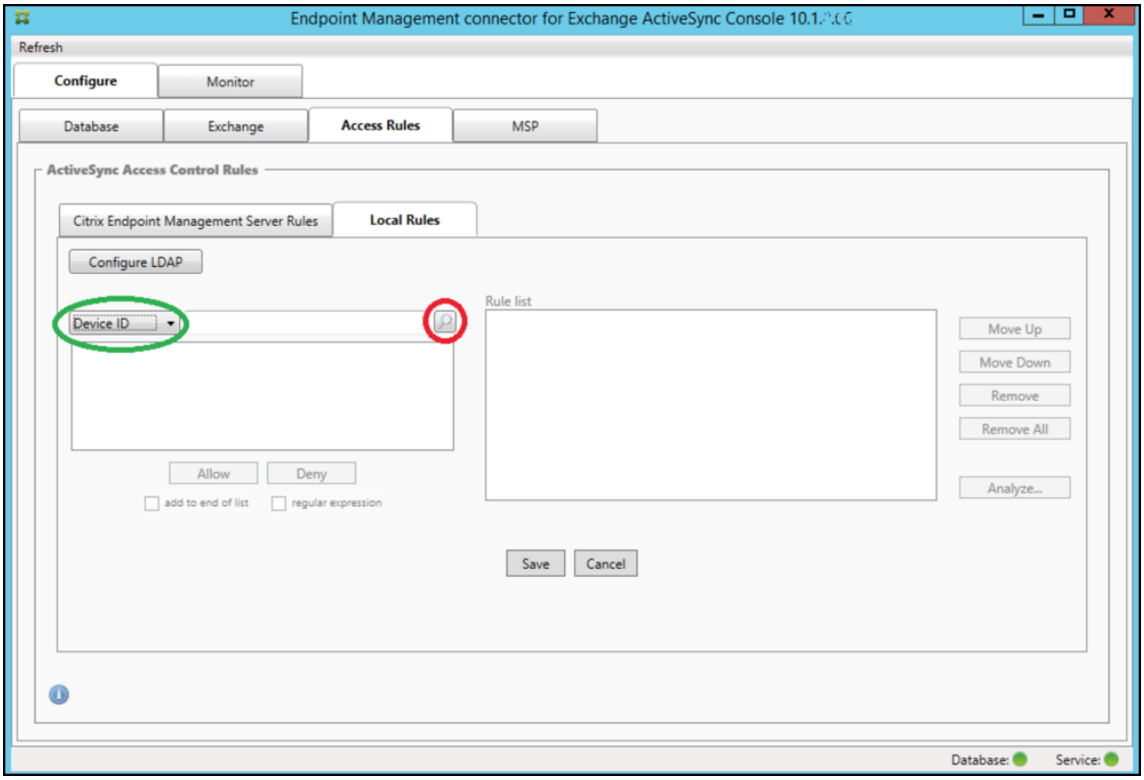
As regras locais de expressão regular podem ser distinguidas pelo ícone exibido ao lado delas -  .

Para adicionar uma regra de expressão regular, você pode criar uma regra de expressão regular com base em um valor existente na lista de resultados de um determinado campo (desde que um instantâneo principal tenha sido concluído) ou pode simplesmente digitar a expressão regular que desejar.

Para criar uma expressão regular com base em um valor de campo existente

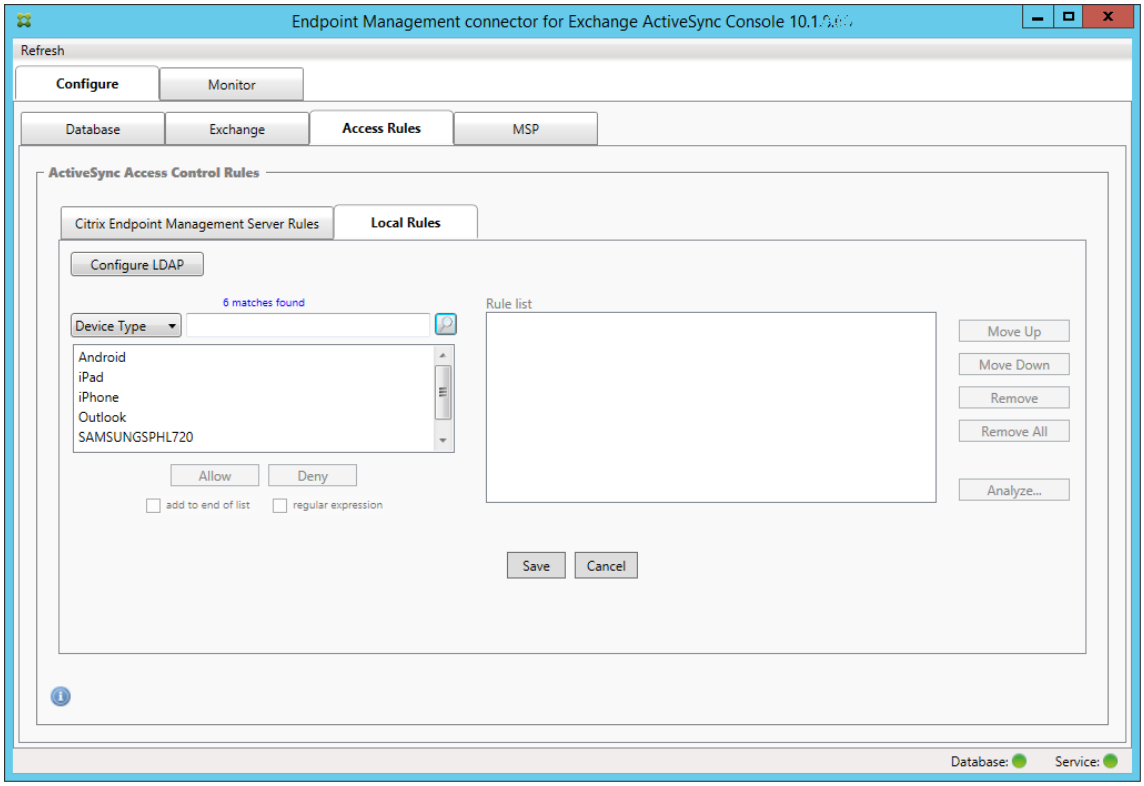
1. Clique na guia **Access Rules**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

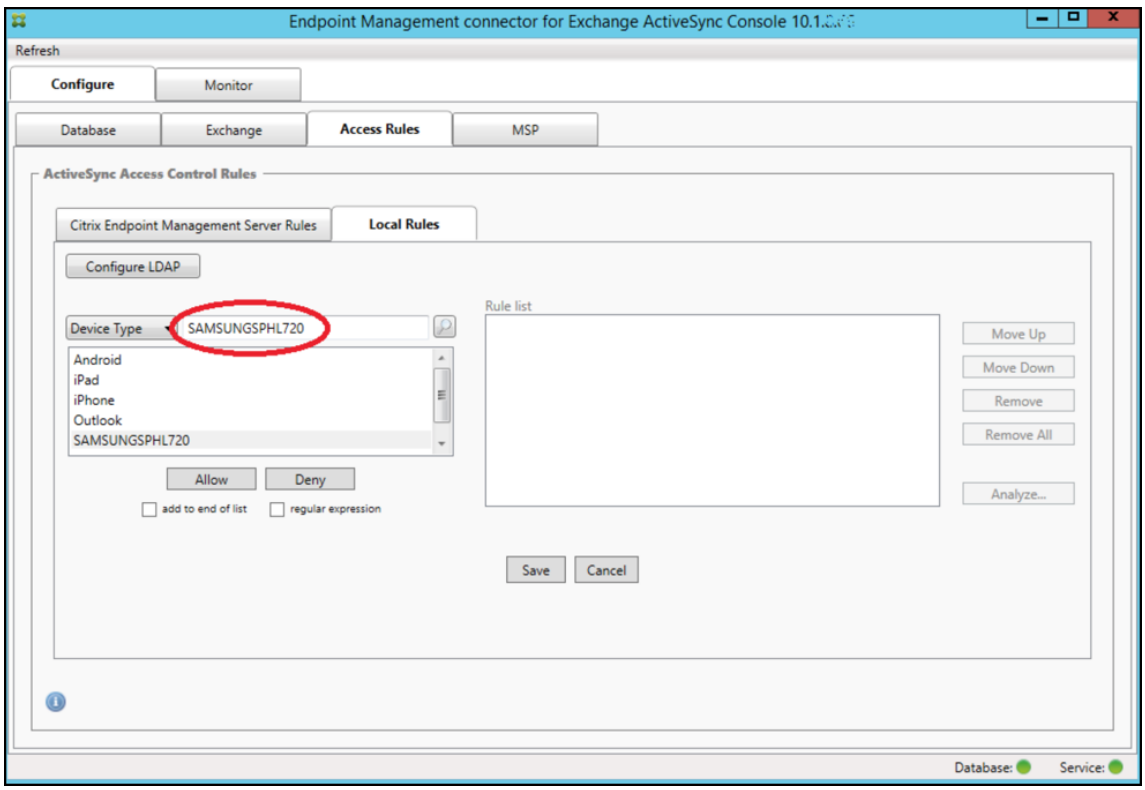


2. Na lista **Device ID**, selecione o campo para o qual você deseja criar uma Regra Local de expressão regular.
3. Clique no ícone de lupa para exibir todas as correspondências exclusivas do campo escolhido. Neste exemplo, o campo **Device Type** foi escolhido e as opções são mostradas abaixo, na caixa de lista.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Clique em um dos itens na lista de resultados. Nesse exemplo, **SAMSUNGSPHL720** foi selecionado e é exibido na caixa de texto adjacente a **Device Type**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

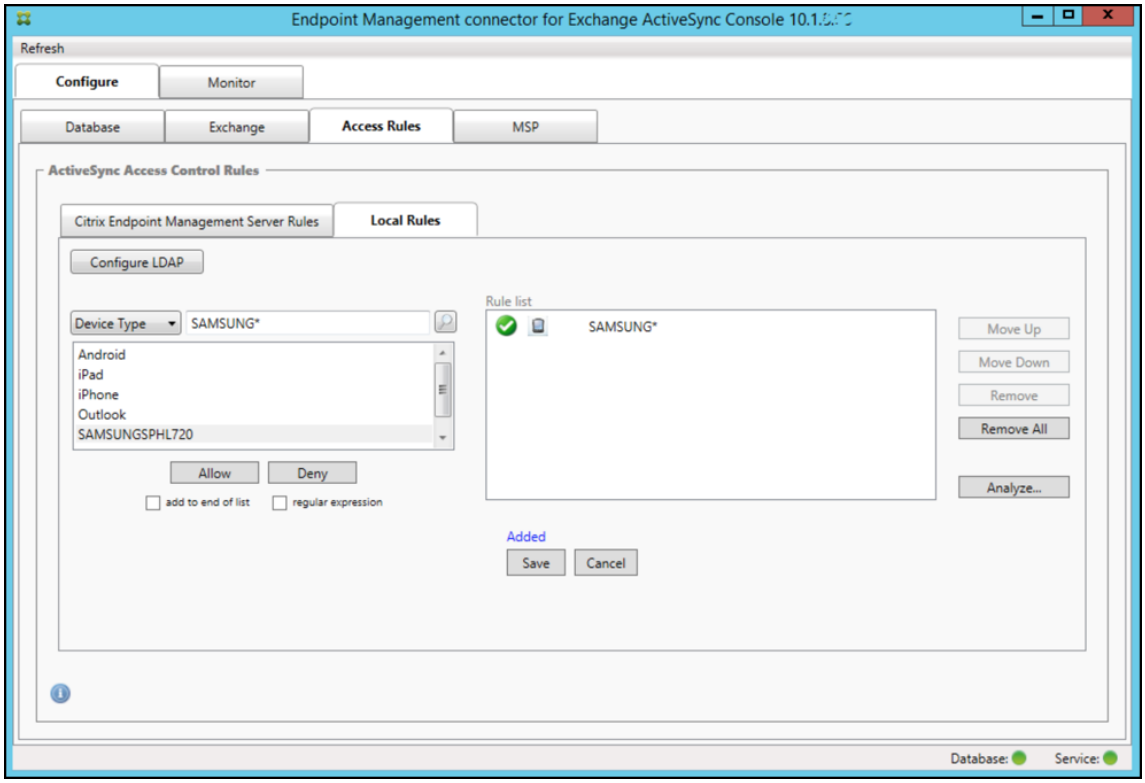
5. Para permitir todos os tipos de dispositivo que têm “Samsung” no respectivo valor de tipo de dispositivo, adicione uma regra de expressão regular seguindo estas etapas:

   a) Clique na caixa de texto do item selecionado.

   b) Altere o texto de **SAMSUNGSPHL720** para **SAMSUNG.***.

   c) Verifique se a caixa de seleção regular expression está marcada.

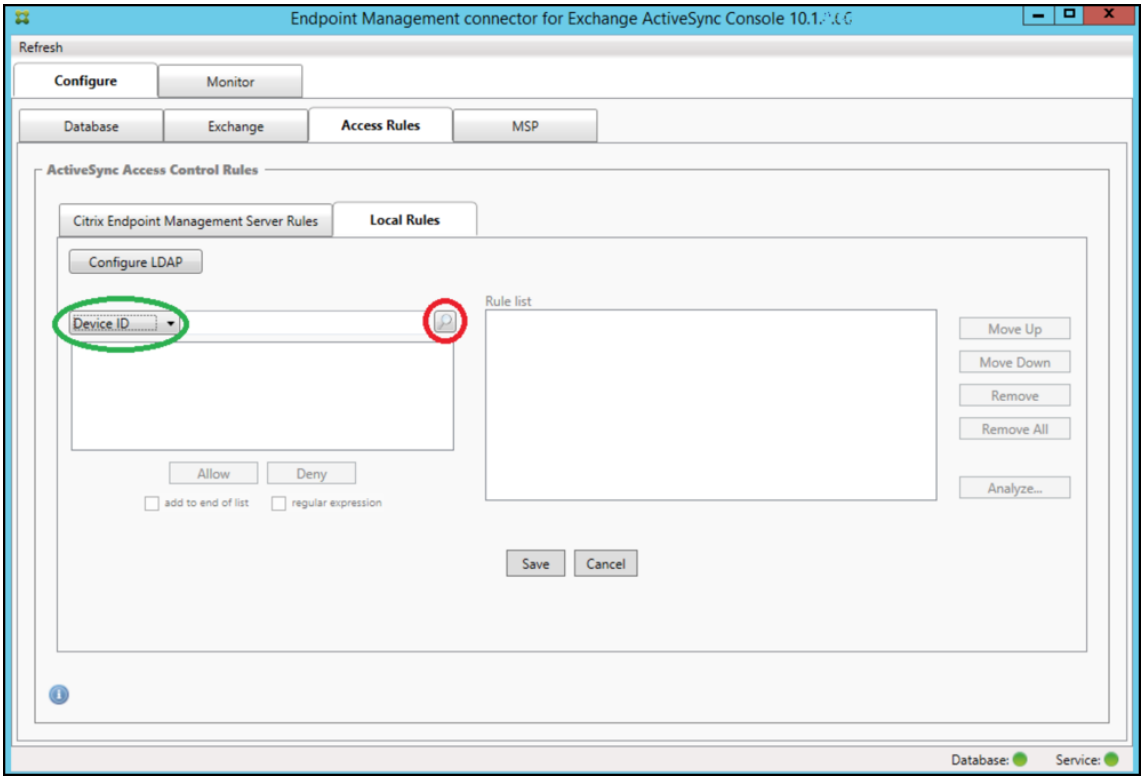
   d) Clique em **Allow**.



Para criar uma regra de acesso

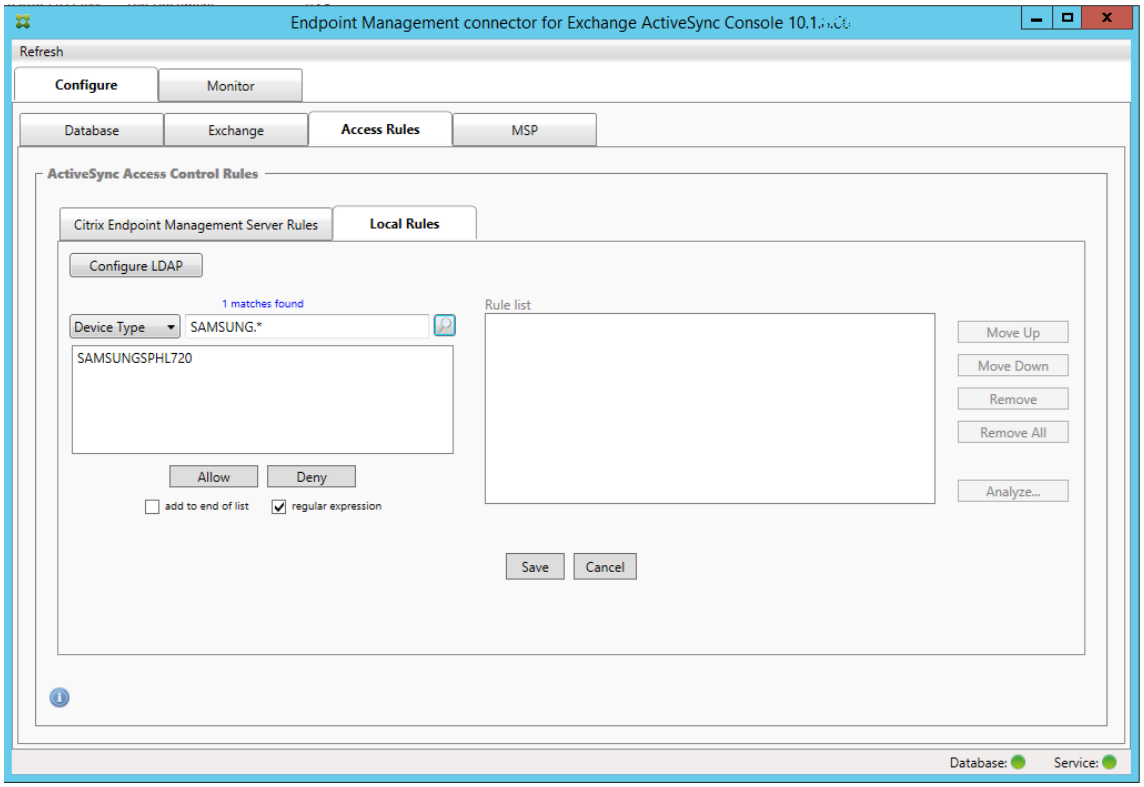
1. Clique na guia **Local Rules**.
2. Para inserir a expressão regular, você precisa usar a lista Device ID e a caixa de texto do item selecionado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Selecione o campo em relação ao qual você deseja corresponder. Esse exemplo usa Device Type.
4. Digite a expressão regular. Esse exemplo usa `samsung.*`
5. Verifique se a caixa de seleção regular expression está marcada e clique em **Allow** ou em **Deny**. Neste exemplo, a escolha é **Permitir**. O resultado final é o seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

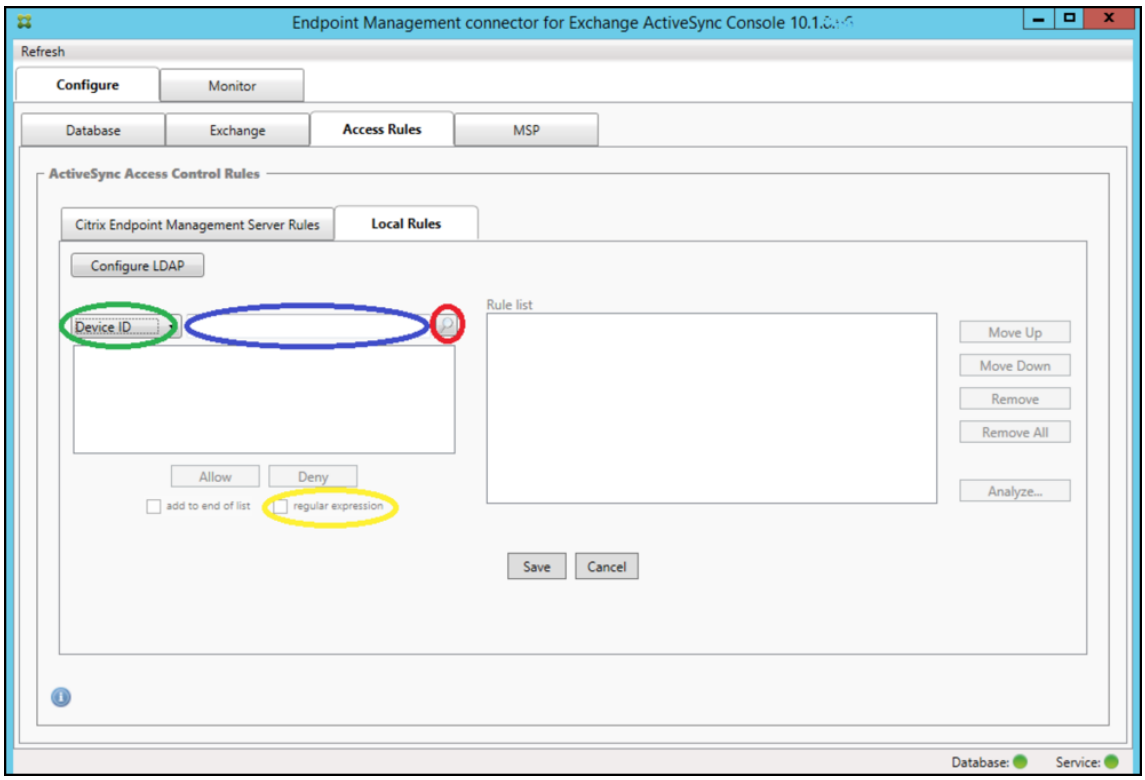


Para encontrar dispositivos

Ao marcar a caixa de seleção de expressão regular, você pode executar pesquisas para dispositivos específicos que correspondem à expressão específica. Esse recurso estará disponível somente se um instantâneo principal tiver sido concluído com êxito. Você pode usar esse recurso mesmo que não haja nenhum planejamento para usar regras de expressão regular. Por exemplo, suponha que você deseja encontrar todos os dispositivos que tenham o texto “workmail” no respectivo ID de dispositivo ActiveSync. Para fazê-lo, siga este procedimento.

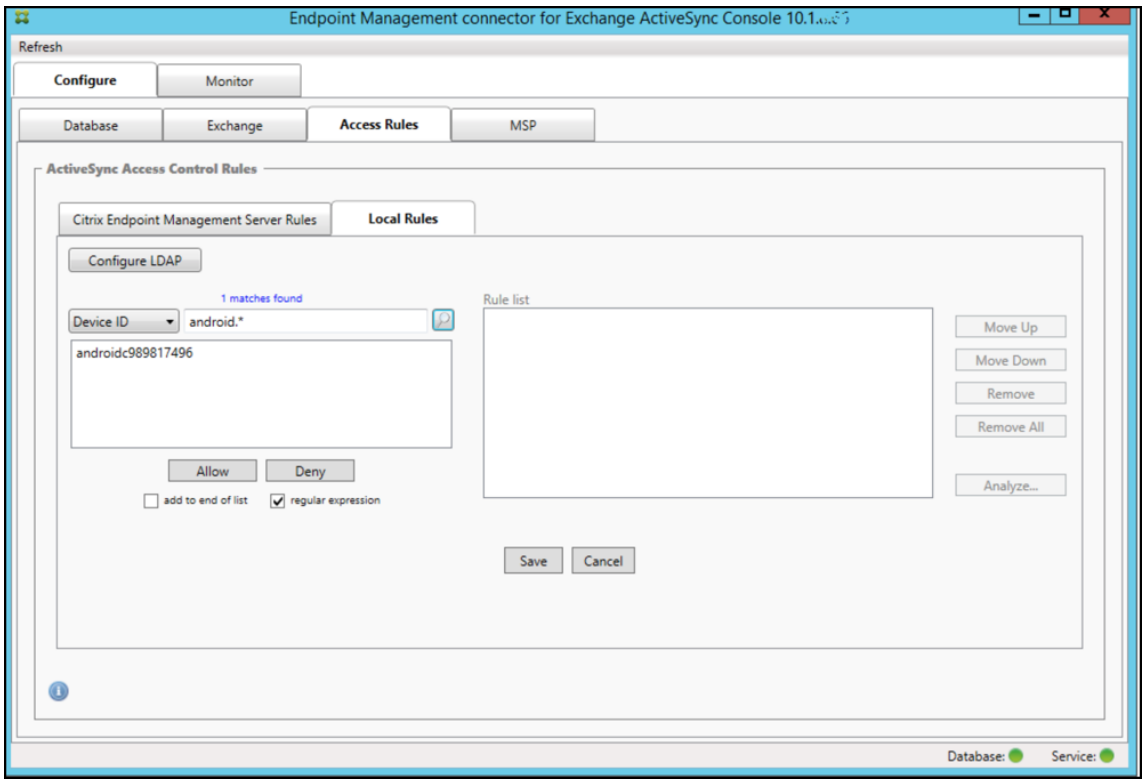
1. Clique na guia **Access Rules**.
2. Verifique se o seletor do campo de correspondência do dispositivo está definido como Device ID (o padrão).

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Clique na caixa de texto do item selecionado (conforme mostrado em azul na figura anterior) e digite `workmail.*`.
4. Confirme que a caixa de seleção regular expression esteja marcada e, em seguida, clique no ícone de lupa para exibir as correspondências, conforme mostrado na figura a seguir.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



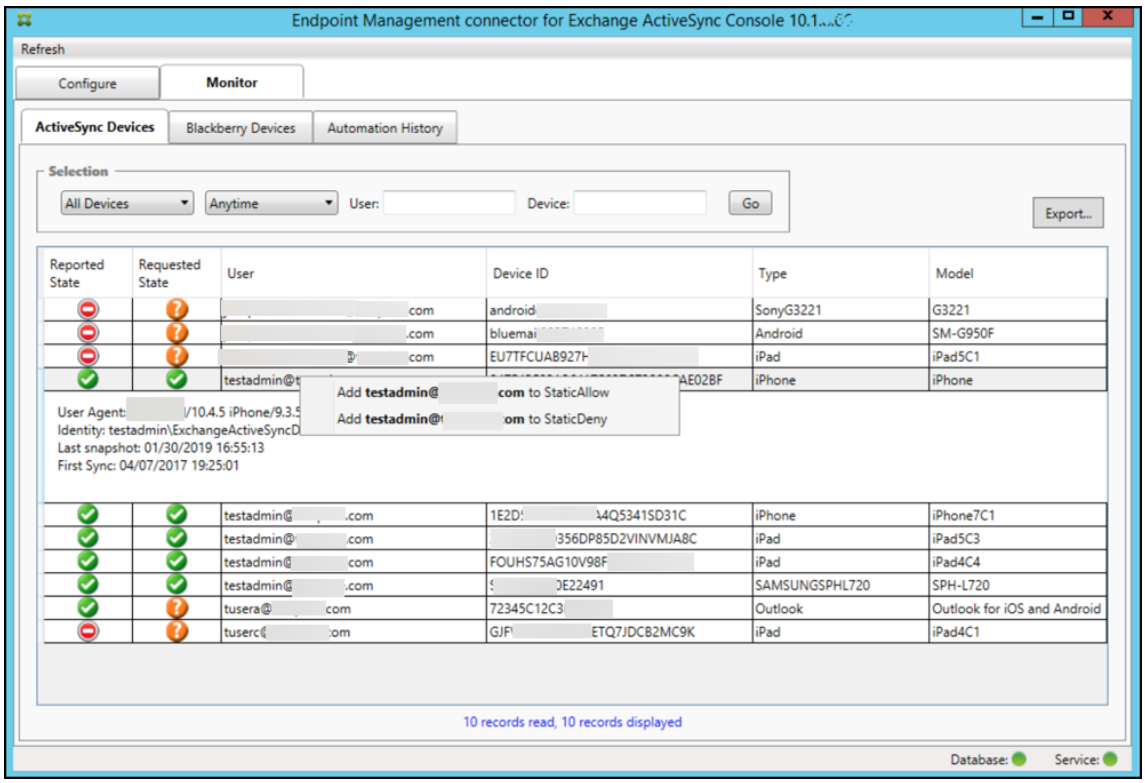
Para adicionar um usuário, um dispositivo ou um tipo de dispositivo individual a uma regra estática

Você pode adicionar regras estáticas com base no usuário, no ID de dispositivo ou no tipo de dispositivo na guia ActiveSync Devices.

1. Clique na guia **ActiveSync Devices**.
2. Na lista, clique com o botão direito em um usuário, um dispositivo ou um tipo de dispositivo e selecione se você deseja permitir ou negar a sua seleção.

   A imagem a seguir mostra a opção Allow/Deny quando user1 está selecionado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Monitoramento de dispositivo

A guia **Monitor** no conector de Endpoint Management para Exchange ActiveSync permite navegar nos dispositivos do Exchange ActiveSync e do BlackBerry que foram detectados e no histórico de comandos automatizados do PowerShell que foram emitidos. A guia **Monitor** tem as seguintes três guias:

- **ActiveSync Devices**:
  - Você pode exportar as parcerias de dispositivo do ActiveSync exibidas clicando no botão **Export**.
  - Você pode adicionar regras locais (estáticas) clicando nas colunas **User**, **Device ID** ou **Type** e selecionando o tipo de regra de permissão ou bloqueio apropriado.
  - Para recolher uma linha expandida, clique com o Ctrl pressionado na linha expandida.
- **Dispositivos BlackBerry**
- **Histórico de automação**

A guia **Configure** mostra o histórico de todos os instantâneos. O histórico de instantâneos mostra quando o instantâneo ocorreu, o tempo que levou, quantos aparelhos foram detectados e todos os erros que ocorreram:

- Na guia **Exchange**, clique no ícone de informações do Exchange Server desejado.
- Na guia **MSP**, clique no ícone de informações do BlackBerry Server desejado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Resolução de problemas e diagnósticos

O conector de Endpoint Management para Exchange ActiveSync registra erros e outras informações operacionais no respectivo arquivo de log: *pasta de instalação*\log\XmmWindowsService.log. O conector de Endpoint Management para Exchange ActiveSync também registra eventos significativos no Log de Eventos do Windows.

Para alterar o nível de log

O conector de gerenciamento de ponto de extremidade para o Exchange ActiveSync inclui os seguintes níveis de log: Erro, Informações, Aviso, Depuração e Rastreamento.

> Nota:
>
> Cada nível sucessivo gera mais detalhes (mais dados). Por exemplo, o nível Erro fornece o mínimo de detalhes, enquanto o nível de Rastreamento 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 que você preferir. Por exemplo:

```
1          <rules >
2
3          <logger name="*" writeTo="file" minlevel="Debug" />
4
5          </rules>
```

1. Salve o arquivo.

   As alterações entram em vigor imediatamente. Não é necessário reiniciar o conector do Exchange ActiveSync.

Erros comuns

A seguinte lista inclui os erros comuns:

- O serviço conector de 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 serviço conector de Endpoint Management para Exchange ActiveSync não consegue acessar o SQL Server. Isso pode ser devido a estes problemas:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

    * O serviço do SQL Server não está em execução.
    * Falha na autenticação.

  Se a autenticação Integrated do Windows estiver configurada, a conta de usuário do serviço conector de Endpoint Management para Exchange ActiveSync deve ser um login permitido do SQL. A conta do serviço conector de Endpoint Management para Exchange ActiveSync tem como padrão o Sistema Local, mas pode ser alterada para qualquer conta que tenha privilégios de administrador local. Se a autenticação de SQL estiver configurada, o login do SQL deverá ser configurado corretamente no SQL.

- A porta configurada para o Provedor de Serviços Móveis (MSP) não está disponível. Deve haver uma porta de escuta selecionada que não seja usada por outro processo no sistema.

- O XenMobile não consegue se conectar ao MSP

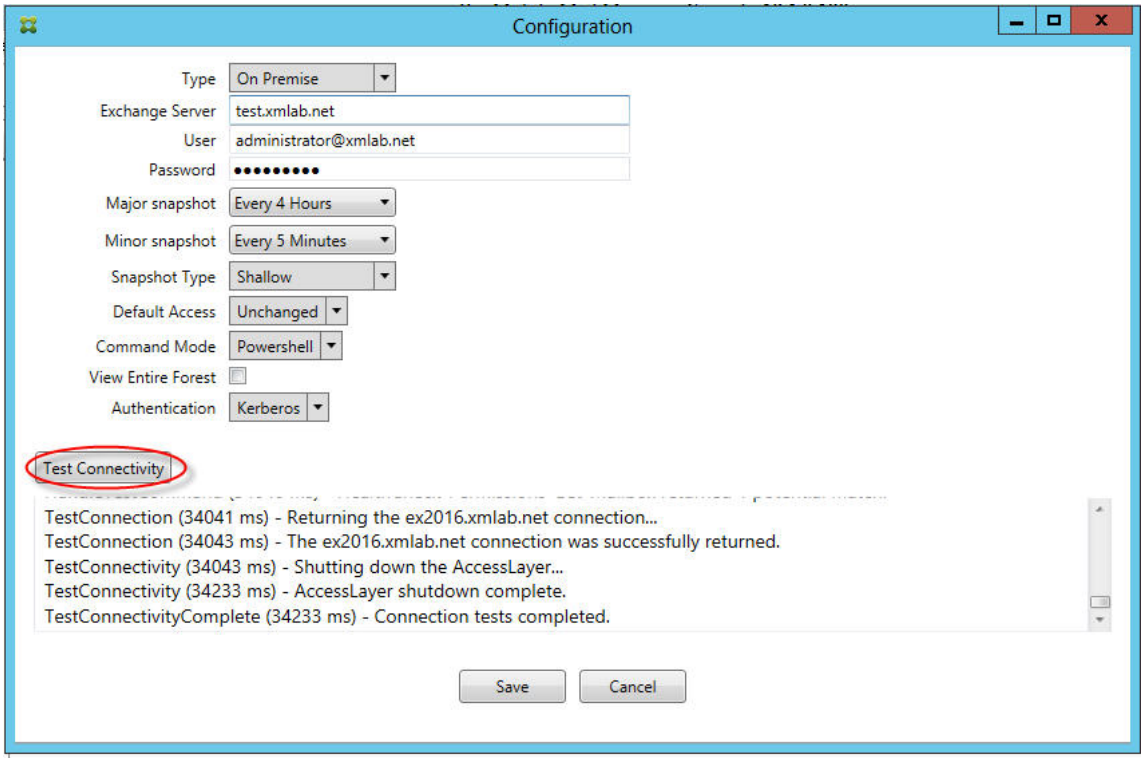
  Verifique se a porta de serviço e o transporte do MSP estão configurados corretamente na guia **Configure > MSP** do console conector de Endpoint Management para Exchange ActiveSync. Verifique se o Authorization Group ou o User está configurado corretamente.

  Se HTTPS estiver configurado, um certificado de servidor SSL válido deverá ser instalado. Se IIS estiver instalado, o Gerenciador do IIS poderá 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 como instalar os certificados.

  O conector de Endpoint Management para Exchange ActiveSync contém um programa utilitário para testar a conectividade com o serviço MSP. Execute o programa *PastadeInstalação*MspTestServiceClient.exe e defina a URL e as credenciais para uma URL e credenciais que serão configuradas no XenMobile e, em seguida, clique em **Test Connectivity**. Isso simula as solicitações de serviço da Web que o XenMobile Server emite. Observe que, se HTTPS estiver configurado, você deverá especificar o nome de host real do servidor (o nome especificado no certificado SSL).

  Quando você estiver usando **Test Connectivity**, verifique se há pelo menos um registro do ActiveSyncDevice ou o teste poderá falhar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Ferramentas de solução de problemas

Um conjunto de utilitários do PowerShell para solução de problemas está disponível na pasta Support\PowerShell.

Uma ferramenta de solução de problemas executa uma análise profunda das caixas de correio e dispositivos do usuário, detectando condições de erro e possíveis áreas de falha e análise detalhada RBAC de usuários. Pode salvar a saída bruta de todos os cmdlets para um arquivo de texto.

Conector Citrix Gateway para Exchange ActiveSync

April 15, 2019

O XenMobile NetScaler Connector é agora o conector Citrix Gateway para Exchange ActiveSync. Para obter mais detalhes sobre o portfólio unificado da Citrix, consulte o Guia do produto Citrix.

O conector para Exchange ActiveSync oferece um serviço de autorização de nível de dispositivo dos clientes ActiveSync para o NetScaler agindo como um proxy reverso para o protocolo do 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 obter mais informações, consulte ActiveSync Gateway.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para um diagrama da arquitetura de referência detalhada, consulte Arquitetura.

A versão atual do conector do Citrix Gateway para Exchange ActiveSync é a versão 8.5.2.

Novidades

As seções a seguir listam o que há de novo nas versões atuais e anteriores do conector Citrix Gateway para Exchange ActiveSync, anteriormente XenMobile NetScaler Connector.

O que há de novo na versão 8.5.3

- Esta versão adiciona suporte aos protocolos ActiveSync 16.0 e 16.1.
- Mais detalhes foram adicionados às análises enviadas ao Google Analytics, especialmente no que diz respeito aos instantâneos. [CXM-52261]

O que há de novo na versão 8.5.2

- O XenMobile NetScaler Connector é agora o 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, poderá ocorrer o seguinte problema: se um usuário tiver mais aliases, os aliases também não serão verificados ao aplicar a regra. [CXM-55355]

> Nota:
>
> A seção de novidades a seguir se refere ao conector Citrix Gateway para Exchange ActiveSync por seu nome anterior, XenMobile NetScaler Connector. O nome foi alterado a partir da versão 8.5.2.

O que há de novo na versão 8.5.1.11

- **Alteração do requisito do sistema:** a versão atual do NetScaler Connector requer o Microsoft .NET Framework 4.5.
- **Suporte ao Google Analytics:** queremos saber como você usa o XenMobile NetScaler Connector para nos concentrarmos em como podemos melhorar o produto.
- **Suporte para TLS 1.1 e 1.2:** devido ao enfraquecimento da segurança, o TLS 1.0 está sendo substituído pelo PCI Council. O suporte para TLS 1.1 e 1.2 é adicionado ao XenMobile NetScaler Connector.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Monitoramento do conector Citrix Gateway para Exchange ActiveSync

O utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync fornece registro detalhado que você pode usar para visualizar todo o tráfego que passa pelo seu Exchange Server que é permitido ou bloqueado pelo Secure Mobile Gateway.

Use a guia **Log** para visualizar o histórico das solicitações do ActiveSync encaminhadas para o conector Citrix Gateway para Exchange ActiveSync pelo NetScaler para autorização.

Além disso, para garantir que o serviço web do conector Citrix Gateway para 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 da Web está responsivo.

Para simular o tráfego do ActiveSync com o conector Citrix Gateway para Exchange ActiveSync

Você pode usar o conector Citrix Gateway para Exchange ActiveSync para simular como o tráfego do ActiveSync se parecerá em conjunto com suas políticas. No utilitário de configuração do conector, selecione a guia **Simulador**. Os resultados mostram como suas políticas serão aplicadas de acordo com as regras que você configurou.

Escolha de filtros para o conector Citrix Gateway para Exchange ActiveSync

Os filtros do conector Citrix Gateway para Exchange ActiveSync funcionam analisando um dispositivo para uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, o dispositivo será colocado em uma Lista de dispositivos. Essa lista de dispositivos não é uma lista permitir ou uma lista de bloqueio. É uma lista de dispositivos que atendem aos critérios definidos. Os filtros a seguir 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, poderia ser um usuário que foi registrado, mas de quem a senha do usuário do Active Directory expirou, ou um usuário que foi registrado com credenciais desconhecidas.
- **Falha no atestado Samsung KNOX:** os dispositivos Samsung possuem funcionalidade para segurança e diagnóstico. Este filtro fornece confirmação de que o dispositivo está configurado para o KNOX. Para obter detalhes, consulte Samsung KNOX.
- **Aplicativos proibidos:** permite ou nega dispositivos com base na Lista de dispositivos definida pelas políticas da lista negra e na presença de aplicativos da lista negra.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Permissão/Negação implícita:** cria uma Lista de dispositivos de todos os dispositivos que não atendem a qualquer um dos outros critérios de regra do filtro e permite ou nega com base nessa lista. A opção Permissão/negação implícita garante que o status do conector Citrix Gateway para Exchange ActiveSync na guia Dispositivos esteja ativado e mostre o status do conector para seus dispositivos. A opção Permissão/negação implícita também controla todos os outros filtros do conector que não foram selecionados. Por exemplo, aplicativos em listas negras serão negados (bloqueados) pelo conector, enquanto que todos os outros filtros serão permitidos, pois a opção Permissão/negação implícita está definida como **Permitir**.
- **Dispositivos inativos:** cria uma Lista de dispositivos que não se comunicaram com o XenMobile dentro de um período especificado. Esses dispositivos são considerados inativos. O filtro permite ou nega os dispositivos de acordo.
- **Aplicativos obrigatórios ausentes:** quando um usuário se registra, o usuário 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 todos os dispositivos que não têm um código secreto no dispositivo.
- **Dispositivos sem conformidade:** permite negar ou permitir dispositivos que atendam aos seus próprios critérios internos de conformidade com TI. A conformidade é uma configuração arbitrária definida pela propriedade do dispositivo chamada Sem conformidade, que é um sinalizador booliano que pode ser **True** ou **False**. (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 atender a critérios específicos.)
  - **Sem conformidade = True**. Se um dispositivo não atende aos padrões de conformidade e definições de políticas definidos pelo seu departamento de TI, o dispositivo está sem conformidade.
  - **Sem conformidade = False.** Se um dispositivo atende aos padrões de conformidade e definições de políticas definidos pelo seu departamento de TI, o dispositivo está em conformidade.
- **Status revogado:** cria uma Lista de todos os dispositivos revogados e permite ou nega com base no status de 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 com root.
- **Dispositivos não gerenciados**. Cria uma lista de dispositivos de todos os dispositivos no banco de dados do XenMobile. O Gateway de aplicativo móvel deve ser implantado em um modo de bloqueio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar uma conexão ao conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o XenMobile e outros provedores de configuração remota através de serviços do Web Secure.

1. No utilitário de configuração do conector, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Provedores de configuração**, em **Nome**, digite um nome de usuário que tenha privilégios administrativos e seja usado para autorização HTTP básica com o servidor XenMobile.
3. Em **Url**, digite o endereço da Web do XenMobile GCS, geralmente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.
4. Em **Senha**, digite a senha que será usada para a autorização básica de HTTP com o XenMobile Server.
5. Em **Gerenciamento de host**, insira o nome do servidor do conector.
6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmicas atualizado é recebido do Device Manager.
7. Em **Intervalo delta**, especifique um período de tempo para quando uma atualização de regras dinâmicas é recebida.
8. Em **Tempo limite de solicitação**, especifique o intervalo de tempo limite de solicitação do servidor.
9. Em **Provedor de configuração**, selecione se a instância do servidor do provedor de configuração fornece a configuração da política.
10. Em **Eventos ativados**, ative esta opção se desejar que o conector notifique o XenMobile quando um dispositivo estiver bloqueado. Essa opção é necessária se você estiver usando as regras do conector em qualquer uma das suas ações automatizadas do XenMobile.
11. Clique em **Salvar** e, em seguida, clique em **Testar a conectividade** para testar a conectividade do provedor de gateway para 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 **Desativado** e clique em **Salvar**.

Quando você adiciona 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 de Política definido nesta seção, uma nova política é criada.

O operador pode adicionar, remover ou modificar elementos da política, se ocorrer o seguinte: o elemento da política está em conformidade com a definição de esquema e as cadeias de caracteres de substituição padrão (colocadas entre chaves) não são modificadas. Em seguida, adicione novos grupos para o provedor e atualize a política para que inclua os novos grupos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para importar uma política do XenMobile

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Provedores de configuração**, em **Nome**, digite um nome de usuário que será usado para autorização HTTP básica com o servidor XenMobile e que tenha privilégios administrativos.
3. Em **URL**, digite o endereço da Web do XenMobile Gateway Configuration Service (GCS), geralmente no formato `https://<xdmHost>/xdm/services/<MagConfigService>`. O nome MagConfigService diferencia maiúsculas de minúsculas.
4. Em **Senha**, digite a senha que será usada para a autorização de HTTP básica com o servidor XenMobile.
5. Clique em **Testar a conectividade** para testar a conectividade do provedor de gateway para configuração. Se a conexão falhar, verifique se as configurações do firewall local permitem a conexão, ou entre em contato com o administrador.
6. Quando a conexão for bem-sucedida, desmarque a caixa de seleção **Desativado** e clique em **Salvar**.
7. Em **Gerenciamento de host**, deixe o nome DNS padrão do computador host local. Essa configuração costumava coordenar a comunicação com o XenMobile quando vários servidores do Forefront Threat Management Gateway (TMG) estavam configurados em uma matriz.

   Depois de salvar as configurações, abra o GCS.

Configuração do modo de política do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync pode ser executado nos seis modos a seguir:

- **Permitir todos**. Este modo de política concede acesso para todo o tráfego que passa pelo conector. Não são utilizadas outras regras de filtragem.
- **Negar todos**. Este modo de política bloqueia o acesso para todo o tráfego que passa pelo conector. Não são utilizadas outras regras de filtragem.
- **Regras estáticas: modo de Bloqueio**. Esse modo de política executa regras estáticas com uma instrução de negação ou bloqueio implícita no final. O conector bloqueia dispositivos que não são permitidos através de outras regras de filtro.
- **Regras estáticas: modo de Permissão**. Esse modo de política executa regras estáticas com uma instrução de permissão implícita no final. Os dispositivos que não são bloqueados ou negados por outras regras de filtro são permitidos por meio do conector.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Regras estáticas + ZDM:** modo de Bloqueio. Esse modo de política executa regras estáticas primeiro, seguido por regras dinâmicas do XenMobile com uma instrução de negação ou bloqueio implícita no final. Os dispositivos são permitidos ou negados com base nos filtros definidos e regras do Device Manager. Os dispositivos que não correspondem a regras e filtros definidos são bloqueados.
- **Regras estáticas + ZDM:** modo de Permissão. Esse modo de política executa regras estáticas primeiro, seguido por regras dinâmicas do XenMobile com uma instrução de permissão implícita no final. Os dispositivos são permitidos ou negados com base nos filtros definidos e regras do XenMobile. Os dispositivos que não correspondem a regras e filtros definidos são permitidos.

O processo do conector Citrix Gateway para Exchange ActiveSync permite ou bloqueia regras dinâmicas com base em IDs ActiveSync exclusivos para dispositivos móveis com iOS e Windows recebidos do XenMobile. Os dispositivos Android diferem no seu comportamento com base no fabricante e alguns não expõem prontamente um ID exclusivo do ActiveSync. Para compensar, o XenMobile envia informações de ID de usuário para dispositivos Android para emitir uma autorização de permissão ou bloqueio. Como resultado, se um usuário tiver apenas um dispositivo Android, as permissões e os 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 estes dispositivos pelo ActiveSyncID, se eles 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 SMG Controller Configuration, faça o seguinte:

1. Clique na guia **Filtros do caminho** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Propriedades do caminho**, selecione um modo de política na lista de **Políticas** e 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 Permitir são exibidas com marca de seleção verde. As políticas Negar são exibidas como um círculo vermelho com uma linha através dele. Para atualizar a tela e ver as regras mais atualizadas, clique em **Atualizar**. Você também pode modificar a ordem das regras no arquivo config.xml.

Para testar as regras, clique na guia **Simulador**. Especifique os valores nos campos. Estes também podem ser obtidos a partir dos logs. Uma mensagem de resultado aparecerá especificando Permitir ou Bloquear.

Para configurar regras estáticas

Insira regras estáticas com valores que o filtro ISAPI da solicitação da conexão do ActiveSync HTTP lê. As regras estáticas habilitam o conector Citrix Gateway para Exchange ActiveSync a permitir ou

© 1999-2019 Citrix Systems, Inc. All rights reserved.

bloquear o tráfego pelos seguintes critérios:

- **Usuário**. O conector Citrix Gateway para Exchange ActiveSync usa a estrutura de valor e nome de usuário autorizada que foi capturada durante o registro do dispositivo. Isso é comumente encontrado como domínio\nome de usuário como referenciado pelo servidor que executa o XenMobile conectado ao Active Directory via LDAP. A guia **Log** no 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 se for diferente.
- **Deviceid (ActiveSyncID)**. Também conhecido como o ActiveSyncID do dispositivo conectado. Esse valor é comumente encontrado na página Propriedades do dispositivo específico no console XenMobile. Esse valor também pode ser rastreado a partir da guia Log no utilitário de configuração do conector.
- **DeviceType**. 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. Tal como acontece com outros valores, o utilitário de configuração do conector pode revelar todos os tipos de dispositivos conectados que estão sendo processados para a conexão ActiveSync.
- **UserAgent**. Contém informações sobre o cliente ActiveSync que é usado. Na maioria dos casos, o valor especificado corresponde a uma compilação e versão do sistema operacional específicas para a plataforma do dispositivo móvel.

O utilitário de configuração do conector executado no servidor sempre gerencia as regras estáticas.

1. No utilitário SMG Controller Configuration, clique na guia **Regras estáticas** e clique em **Adicionar**.
2. Na caixa de diálogo **Propriedades da regra estática**, especifique os valores que você deseja usar como critérios. Por exemplo, você pode inserir um usuário para permitir o acesso inserindo o nome do usuário (por exemplo, AllowedUser) e, em seguida, desmarcando a caixa de seleção **Desativado**.
3. Clique em **Salvar**.

   A regra estática agora está em vigor. Além disso, você pode usar expressões regulares para definir valores, mas você deve habilitar o modo de processamento de regras no arquivo config.xml.

Para configurar regras dinâmicas

Políticas e propriedades de dispositivo no XenMobile definem regras dinâmicas e podem disparar um filtro dinâmico do conector Citrix Gateway para Exchange ActiveSync. Os disparadores são baseados na presença de uma violação de política ou configuração de propriedade. Os filtros do conector funcionam analisando um dispositivo para uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, o dispositivo será colocado em uma Lista de dis-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

positivos. Essa lista de dispositivos não é uma lista de permissão ou uma lista de bloqueio. Ela é uma lista de dispositivos que atende aos critérios definidos. As opções de configuração a seguir permitem que você defina se deseja permitir ou negar dispositivos na Lista de dispositivos usando o conector.

> Nota:
>
> Você deve usar o console XenMobile para configurar regras dinâmicas.

1. No console 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.
3. Em **Ativar as regras a seguir**, selecione uma ou mais regras que você desejar ativar.
4. Em Somente Android, em **Enviar usuários de domínio do Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o Secure Mobile Gateway.

   Quando essa opção está ativada, o XenMobile envia as informações do dispositivo Android para o conector Citrix Gateway para Exchange ActiveSync caso o XenMobile não tenha o identificador do ActiveSync do usuário do dispositivo Android.

Para configurar políticas personalizadas editando o arquivo XML do conector Citrix Gateway 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, você pode editar o arquivo de configuração XML do conector (config\config.xml).

1. Encontre a seção **PolicyList** no arquivo e, em seguida, 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**.

Configuração do 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 leva em consideração ao avaliar solicitações HTTP. Por padrão, o arquivo é chamado config.xml e pode ser encontrado no seguinte local: ..\Program Files\Citrix\XenMobile NetScaler Connector\config.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nós GroupRef

Os nós GroupRef definem os nomes dos grupos lógicos. Os padrões são AllowGroup e DenyGroup.

> Nota:
>
> A ordem dos nós GroupRef tal como aparecem no nó GroupRefList é importante.

O valor do ID de um nó GroupRef identifica um contêiner lógico ou uma coleção de membros que são usados para combinar contas ou dispositivos específicos de usuários. 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 corresponda a uma regra no conjunto AllowGroup "passará". Passar significa ter permissão para acessar as autoridades de certificação do Exchange, Exchange CAS. Uma conta de usuário ou dispositivo que corresponde a uma regra no conjunto DenyGroup é "rejeitado". Rejeitado significa não ter permissão para acessar as autoridades de certificação do Exchange, Exchange CAS.

Quando uma conta de usuário/dispositivo específico ou uma combinação de regras atende a 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 Allow sempre terão precedência sobre as regras para a mesma condição no grupo Deny.

Nós Group

Além disso, o config.xml define os nós do grupo Group. Esses nós vinculam os contêineres lógicos AllowGroup e DenyGroup aos arquivos XML externos. As entradas armazenadas nos arquivos externos são a base das regras do filtro.

> Nota:
>
> Nesta versão, apenas arquivos XML externos são suportados.

A instalação padrão implementa dois arquivos XML na configuração: allow.xml e deny.xml.

Configuração do conector Citrix Gateway para Exchange ActiveSync

Você pode configurar o conector Citrix Gateway para Exchange ActiveSync para seletivamente bloquear ou permitir solicitações do ActiveSync com base nas propriedades a seguir: **ID de serviço do Active Sync**, **Tipo de dispositivo**, **Agente de 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 do SMG Controller Configuration. Os grupos estáticos podem consis-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tir em categorias conhecidas de dispositivos, como todos os dispositivos que usam um determinado agente de usuário.

Uma fonte externa chamada Gateway Configuration Provider mantém grupos dinâmicos. O conector Citrix Gateway para Exchange ActiveSync conecta os grupos periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e bloqueados para o conector.

Os grupos dinâmicos são mantidos por uma fonte externa chamada Gateway Configuration Provider e coletados pelo conector Citrix Gateway para Exchange ActiveSync periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e bloqueados para o conector.

Uma Política é uma lista ordenada de grupos na qual 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 do grupo dentro de uma política é importante porque, quando uma correspondência é encontrada, a ação do grupo é realizada e os grupos subsequentes não são avaliados.

Um membro define uma maneira de combinar as propriedades de uma solicitação. Ele pode corresponder a uma única propriedade, como ID de dispositivo, ou a várias propriedades, como o agente de usuário e o tipo de dispositivo.

Escolha de 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 o 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. Toda organização que gerencia a segurança de TI pode ter uma abordagem ligeiramente diferente ou adaptada da segurança para dispositivos móveis.

A mesma lógica aplica-se à segurança do dispositivo móvel. O uso de um modelo permissivo é uma escolha fraca devido à infinidade de tipos e dispositivos móveis, dispositivos móveis por usuário e plataformas e aplicativos do sistema operacional disponíveis. Na maioria das organizações, o modelo restritivo será a escolha mais lógica.

Os cenários de configuração que a Citrix permite para integrar o conector Citrix Gateway para Exchange ActiveSync ao XenMobile são os seguintes:

Modelo Permissivo (Modo de Permissão)

O modelo de segurança permissivo opera na premissa de que a tudo é permitido ou concedido acesso por padrão. Apenas por meio de regras e filtragem algo é bloqueado e é aplicada uma restrição. O

© 1999-2019 Citrix Systems, Inc. All rights reserved.

modelo permissivo de segurança é bom para organizações que têm uma preocupação com a segurança relativamente fraca sobre dispositivos móveis. O modelo só se aplica a controles restritivos para negar o acesso quando apropriado (quando uma regra de política é falha).

Modelo Restritivo (Modo de Bloqueio)

O modelo de segurança restritivo se baseia na premissa de que a nada é permitido ou concedido acesso por padrão. Tudo 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 restritivo de segurança é bom para organizações que têm um critério de segurança relativamente rígido sobre dispositivos móveis. O modo somente concede acesso para uso e funcionalidade com os serviços de rede quando todas as regras para permitir o acesso forem aprovadas.

Gerenciamento do conector Citrix Gateway para Exchange ActiveSync

Você pode usar o conector 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 negras ou listas brancas de aplicativos e outras condições de conformidade.

Ao usar o utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, você pode criar regras dinâmicas e estáticas que impõem as políticas corporativas de e-mail, permitindo que você bloqueie os usuários que estão em violação dos padrões de conformidade. Você também pode configurar criptografia de anexos de e-mail, de modo que todos os anexos que passam pelo seu Exchange Server para dispositivos gerenciados sejam criptografados e apenas visíveis em dispositivos gerenciados por usuários autorizados.

Para desinstalar o conector 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 Citrix Gateway para Exchange ActiveSync

1. Execute o 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.

Depois de instalar o conector, manualmente reinicie o serviço de configuração do XenMobile e o serviço de notificação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Instalação do conector Citrix Gateway para Exchange ActiveSync

Você instala o conector Citrix Gateway para Exchange ActiveSync em seu próprio Windows Server.

A carga de CPU que o conector coloca em um servidor depende da quantidade de dispositivos gerenciados. Para um grande número de dispositivos (mais de 50.000), talvez seja necessário fornecer mais de um núcleo se você não tiver um ambiente em cluster. A espaço de memória do connector não é suficientemente significativo para garantir mais memória.

Requisitos de sistema do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o NetScaler sobre uma ponte SSL configurada no dispositivo NetScaler. A ponte permite que o dispositivo transmita todo o tráfego seguro diretamente para o XenMobile. O conector requer a seguinte configuração mínima do sistema:

Componente	Requisito
Computador e processador	Processador 733 MHz Pentium III de 733 MHz ou superior. Processador Pentium III de 2.0 GHz ou superior (recomendado)
NetScaler	Dispositivo NetScaler com software versão 10
Memória	1 GB
Disco rígido	Partição local formatada em NTFS com 150 MB de espaço disponível no disco rígido
Sistema operacional	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2012 R2
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.
Tela	Monitor VGA ou resolução superior

O computador host para o conector Citrix Gateway para Exchange ActiveSync requer o espaço em disco mínimo disponível seguinte:

- **Aplicativo:** 10 - 15 MB (recomendado 100 MB)
- **Registro em log:** 1 GB (recomendado 20 GB)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para obter informações sobre o suporte de plataforma para o conector Citrix Gateway para Exchange ActiveSync, consulte Sistemas operacionais compatíveis de dispositivos.

Os clientes de email do dispositivo

Nem todos os clientes de email sempre retornam a mesma ID do ActiveSync para um dispositivo. Como o conector Citrix Gateway para Exchange ActiveSync espera uma ID exclusiva do ActiveSync para cada dispositivo, aplica-se o seguinte: apenas os clientes de email que consistentemente geram a mesma ID exclusiva do ActiveSync para cada dispositivo são suportados. A Citrix testou esses clientes de email e os clientes foram executados sem erros:

- Cliente de email nativo HTC
- Cliente de email nativo Samsung
- Cliente de email nativo iOS
- TouchDown

Implantação do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync permite que você use NetScaler para proxy e balanceamento de carga de comunicação do XenMobile Server com dispositivos gerenciados XenMobile. O conector se comunica periodicamente com o XenMobile para sincronizar as políticas. O conector e o XenMobile podem ser agrupados, em conjunto ou independentemente, e podem ter a carga balanceada pelo NetScaler.

Componentes do conector Citrix Gateway para Exchange ActiveSync

- **Serviço do conector Citrix Gateway para Exchange ActiveSync:** este serviço fornece uma interface de serviço web REST que pode ser invocada pelo NetScaler para determinar se uma solicitação do ActiveSync de um dispositivo está 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 a dispositivo não autorizado para o XenMobile. Desta forma, o XenMobile pode tomar as medidas apropriadas, como notificar o usuário por que o dispositivo foi bloqueado.
- **Utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync:** este aplicativo permite ao administrador configurar e monitorar o conector.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para configurar endereços de escuta para o conector Citrix Gateway para Exchange ActiveSync

Para o conector Citrix Gateway para Exchange ActiveSync receber solicitações do NetScaler para autorizar o tráfego do ActiveSync, faça o seguinte: Especifique a porta em que o conector Citrix Gateway para Exchange ActiveSync escuta as chamadas de serviço da web do NetScaler.

1. No menu **Iniciar**, selecione o utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync.
2. Clique na guia **Serviços da Web** e, em seguida, digite os endereços de escuta para o serviço da web do conector Citrix Gateway para Exchange ActiveSync. Você pode selecionar **HTTP** ou **HTTPS** ou ambos. Se o conector for co-residente 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 da web.

Para configurar políticas de controle de acesso para dispositivos no conector Citrix Gateway para Exchange ActiveSync

Para configurar a política de controle de acesso que deseja aplicar aos seus dispositivos gerenciados, faça o seguinte:

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia**Filtros do caminho**.
2. Selecione a primeira linha, **Microsoft-Server-ActiveSync é para o ActiveSync** e, em seguida, clique em **Editar**.
3. Na lista **Política**, selecione a política desejada. Para uma política que inclua as políticas do XenMobile, selecione **Estática + ZDM: modo de Permissão ou Estática + ZDM: modo de Bloqueio**. Essas políticas combinam regras locais (ou estáticas) com as regras do XenMobile. Modo de permissão significa que todos os dispositivos que não são explicitamente identificados pelas regras têm acesso autorizado ao ActiveSync. Modo de bloqueio significa que esses dispositivos são bloqueados.
4. Depois de configurar as políticas, clique em **Salvar**.

Para configurar a comunicação com o XenMobile

Especifique o nome e as propriedades do servidor XenMobile (também conhecido como Config Provider) que você deseja usar com o conector Citrix Gateway para Exchange ActiveSync e o NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Essa tarefa pressupõe que você já instalou e configurou o XenMobile.

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Digite o nome e a URL do XenMobile Server que você está usando nessa implantação. Se você tiver vários XenMobile Servers implantados em uma implantação multilocatário, esse nome deve ser exclusivo para cada instância do servidor. Por exemplo, para **Nome**, você pode digitar **XMS**.
3. Em **Url**, digite o endereço da Web do XenMobile GlobalConfig Provider (GCP), geralmente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.
4. Em **Senha**, digite a senha que será usada para a autorização básica de HTTP com o XenMobile Server.
5. Em **Gerenciamento de host**, digite o nome do servidor em que você instalou o conector do Citrix Gateway para Exchange ActiveSync.
6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmicas atualizado é recebido do XenMobile.
7. Em **Tempo limite de solicitação**, especifique o intervalo de tempo limite de solicitação do servidor.
8. Em **Provedor de configuração**, selecione se a instância do servidor do provedor de configuração fornece a configuração da política.
9. Em **Eventos ativados**, ative esta opção se desejar que o Secure Mobile Gateway notifique o XenMobile quando um dispositivo estiver bloqueado. Esta opção é necessária se você estiver usando as regras do Secure Mobile Gateway em qualquer uma das Ações Automatizadas do Device Manager.
10. Depois de configurar o servidor, clique em **Testar Conectividade** para testar a conexão com o XenMobile.
11. Quando a conectividade for estabelecida, clique em **Salvar**.

Implantação do conector Citrix Gateway para Exchange ActiveSync para redundância e escalabilidade

Se deseja dimensionar sua implantação do conector Citrix Gateway para Exchange ActiveSync e do XenMobile, você pode instalar instâncias do conector em vários Windows Servers, todas apontando para a mesma instância XenMobile e, em seguida, usar o NetScaler para balancear a carga dos servidores.

Existem dois modos de configuração do conector Citrix Gateway para Exchange ActiveSync:

- No modo não compartilhado, cada instância do conector Citrix Gateway para Exchange

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ActiveSync se comunica com um XenMobile Server e mantém sua própria cópia privada da política resultante. Por exemplo, se você tiver um cluster de XenMobile Servers, poderá executar uma instância do conector em cada XenMobile Server e o conector obterá as políticas da instância do XenMobile local.

- No modo compartilhado, um nó do conector é designado como o nó primário e ele se comunica com o XenMobile. A configuração resultante é compartilhada entre os outros nós, seja por um compartilhamento de rede do Windows ou pela replicação do Windows (ou de terceiros).

Toda a configuração do conector está em uma única pasta (que consiste em alguns arquivos XML). O processo do conector detecta as alterações aos arquivos 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 desativado por alguns minutos (por exemplo, para reiniciar) porque a última configuração boa conhecida é armazenada em cache no processo do conector.

Conceitos avançados

April 15, 2019

> Nota:
>
> Este artigo aborda conceitos avançados para o XenMobile Server 10.9. Para obter informações avançadas sobre o Endpoint Management, consulte Conceitos avançados.

Os artigos XenMobile Advanced Concepts oferecem um mergulho mais profundo na documentação do produto XenMobile. O objetivo é ajudar a reduzir o tempo de implantação por meio de técnicas especializadas. Os artigos podem citar o especialista técnico ou especialistas que criaram o conteúdo.

Para recomendações, perguntas comuns e casos de uso para o seu ambiente XenMobile de ponta a ponta, consulte o Manual de implantação do XenMobile nesta seção.

Para fóruns de suporte de comunidade no XenMobile, consulte Citrix Discussions.

Interação do XenMobile no local com o Active Directory

April 15, 2019

Contribuição de Siddartha Vuppala

Este artigo explica a interação entre o servidor XenMobile e do Active Directory. O XenMobile Server interage com o Active Directory em linha e em segundo plano. As seções a seguir fornecem mais informações sobre operações em linha e em segundo plano que envolvem a interação do Active Directory.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Este artigo é uma visão geral da interação e não abrange os detalhes. Para obter mais informações sobre como configurar o Active Directory e LDAP no console XenMobile, consulte Configure autenticação de domínio ou de domínio de segurança.

Interações em linha

O XenMobile Server se comunica com o Active Directory usando as configurações de LDAP que um administrador configura. As configurações recuperam informações sobre os usuários e grupos. A seguir estão as operações que resultam em interação entre o XenMobile Server e o Active Directory.

1. **Configuração de LDAP.** A configuração do Active Directory em si resulta em uma interação com o Active Directory. XenMobile Server attempts to validate the information by authenticating the information with Active Directory. O servidor faz isso por meio do protocolo internet, porta e credenciais de conta de serviço fornecidas. Uma associação bem-sucedida indica que a conexão está configurada corretamente.
2. **Interações baseadas em grupo.**
   a) Pesquisar um ou mais grupos durante o Controle de Acesso Baseado em Função (RBAC) e criação de definição de grupo de entrega. O administrador do servidor XenMobile insere uma cadeia de caracteres de texto de pesquisa no console XenMobile. O XenMobile Server pesquisa no domínio selecionado todos os grupos que contêm a subcadeia de caracteres que é fornecida. Em seguida, do servidor XenMobile recupera o objectGUID, sAMAccountName e atributos de nome distinto dos grupos identificados na pesquisa.

      > Nota:
      >
      > Essas informações não são armazenadas no banco de dados do XenMobile Server.

   b) Adição ou atualização de RBAC ou de definição de grupo de implantação. O administrador do XenMobile Server seleciona grupos de interesse do Active Directory com base na pesquisa anterior e os inclui na definição de grupo de implantação. XenMobile Server searches for the specific group, one at a time, in Active Directory. XenMobile Server searches for the objectGUID attribute and retrieves selected attributes, including membership information. As informações de associação de grupo ajudam a determinar a associação entre o grupo recuperado e usuários ou grupos existentes no banco de dados do XenMobile Server. Alterações de associação de grupo resultam em RBAC e derivação de grupo de implantação para os membros de usuário afetados, o que resulta em direitos de usuário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> As alterações na definição de grupo de implantação podem levar a alteração em direitos de aplicativos e política para usuários atingidos.

c) **Convites de PIN de uso 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. Convites de OTP são enviadas para os usuários que foram identificados na etapa anterior.

> Nota:
>
> As três interações anteriores implicam que interações baseadas em grupo devem ser acionadas com base nas alterações de configuração do XenMobile Server. Quando não há nenhuma alteração de configuração, as interações implicam que não há nenhum interações com o Active Directory. Elas também implicam que não há nenhum requisito para os trabalhos de segundo plano para capturar do lado do grupo de alterações periodicamente.

3. **Interação com base no usuário.**

a) Autenticação do usuário. O fluxo de trabalho de autenticação de 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, nome diferenciado, sAMAccountName e direta filiação a grupos. Alterações à filiação ao grupo resultam na nova avaliação do aplicativo, políticas e direitos de acesso.

O usuário pode autenticar com o dispositivo ou no console do XenMobile Server. Em ambos os cenários a interação com o Active Directory segue o mesmo comportamento.

b) Acesso e atualização do App Store. Uma atualização da loja resulta em uma atualização de atributos do usuário, incluindo associações de grupo diretas. Esta ação permite uma nova avaliação de direitos de usuário.

c) Check-ins do dispositivo. Os administradores podem configurar no console XenMobile check-ins do dispositivo periodicamente. Toda vez que um dispositivo faz check-in, os atributos de usuário correspondentes são atualizados, incluindo associações de grupo diretas. Esses check-ins permitem uma nova avaliação dos direitos de usuário.

d) Convites de 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. Membros de usuário, diretos e indiretos (por causa de aninhamento), são recuperados do

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Active Directory e salvos no banco de dados do XenMobile Server. Convites de OTP são enviados para os membros do usuário que foram identificados na etapa anterior.

e) Convites de OTP por usuário. O administrador do XenMobile Server insere uma cadeia de caracteres de texto de pesquisa dentro do console XenMobile. O XenMobile Server consulta o Active Directory e retorna os registros de usuário que correspondem à cadeia de caracteres de texto de entrada. O administrador seleciona, em seguida, 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 para o usuário.

Interações de segundo plano

Uma conclusão da comunicação em linha com o Active Directory é que interações baseadas em grupo são acionadas depois de alterações de seleção para a configuração do XenMobile Server. Quando não há nenhuma alteração de configuração, isso implica que não há interações com o Active Directory para grupos.

Essa interação requer trabalhos em segundo plano que periodicamente sincronizam com o Active Directory e as alterações relevantes de atualização para os grupos interessados.

A seguir estão os trabalhos de plano de fundo 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, em grupos interessados grupos quanto a alterações do nome distinto ou atributos sAMAccountName. A solicitação de pesquisa para o Active Directory usa o objectGUID do grupo de interessados para obter os valores atuais do nome diferenciado e atributos sAMAccountName. As alterações no nome distinto ou valores de sAMAccountName para grupos interessados são atualizadas para o banco de dados.

   > Nota:
   >
   > Esta tarefa não atualiza o usuário às informações de associação ao grupo.

2. **Trabalho de sincronização de grupo aninhado**. Esse trabalho atualiza as alterações na hierarquia de aninhamento de grupos interessados. O XenMobile Server permite diretos e indiretos membros de um grupo interessado para obter direitos. A associação direta dos usuários é atualizada durante interações de usuário incorporadas. Sendo executado em segundo plano, esse trabalho controla associações indiretas. Associações indiretas ocorrem quando um usuário é um membro de um grupo que é um membro de um grupo interessado.

   Este trabalho reúne a lista de grupos do Active Directory do banco de dados do XenMobile Server. Esses grupos fazem parte do grupo de implantação ou a definição de RBAC. Para cada grupo na lista, o XenMobile Server obtém os membros do grupo. Membros de um grupo são

© 1999-2019 Citrix Systems, Inc. All rights reserved.

uma lista de nomes distintos que representam os usuários e grupos. O XenMobile Server faz outra consulta ao Active Directory para obter somente os membros de usuário do grupo interessado. A diferença entre as duas listas oferece somente os membros do grupo para o grupo interessado. As alterações em grupos membros são atualizadas no banco de dados. O mesmo processo é repetido para todos os grupos na hierarquia.

As alterações de aninhamento resulta no processamento de usuários afetados quanto a alterações de direito.

3. **Verificação de usuário desativado**. Esta tarefa é executada somente quando o administrador do XenMobile cria uma ação de verificação de usuários desativados. O trabalho é executado dentro do escopo de um trabalho de sincronização de grupo. O trabalho consulta o Active Directory para verificar o status de desativado de usuários interessados, um usuário por vez.

Perguntas frequentes

O que é a frequência padrão da execução de tarefas em segundo plano?

- Trabalhos de sincronização de grupo executado a cada cinco horas, começando às 02:00h no horário local.
- Os trabalhos de sincronização de grupo aninhado são executados uma vez por dia às meia-noite, horário local.

Por que é necessário um trabalho de sincronização de grupo?

- O atributo memberOf de um registro de usuário no Active Directory fornece a lista de grupos, da qual o usuário é um membro direto. Se um grupo se move de uma unidade Organizacional para outra, o atributo memberOf reflete o valor mais recente do nome distinto. O banco de dados do XenMobile Server também tem o valor mais recente atualizado. Qualquer discrepância entre os nomes distintos do grupo pode resultar na perda de acesso ao grupo de implantação por parte do usuário. O usuário também pode perder os aplicativos e políticas associadas a esse grupo de implantação.
- O trabalho em segundo plano mantém o atributo de nome distinto grupo atualizado no banco de dados do XenMobile Server para garantir que os usuários tenham acesso a seus direitos.
- Os trabalhos de sincronização estão programados para cada cinco horas porque de presume que as alterações de grupo do Active Directory são incomuns.

Um trabalho de sincronização de grupo pode ser desativado?

- Você pode desativar trabalhos quando sabe que grupos interessados não mudam de uma unidade Organizacional para outra.

Por que é necessário um trabalho de segundo plano de processamento de grupo aninhado?

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- As alterações de aninhamento de grupos do Active Directory não são uma ocorrência diária. Alterações à hierarquia de aninhamento de grupos interessados resultam em alterações direitos dos usuários afetados. Quando um grupo é adicionado à hierarquia, seus usuários membros passam a ter o direito às 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 executa uma vez por dia para verificar se existem alterações.

Um trabalho de processamento de grupo aninhado pode ser desativado?

- Você pode desativar trabalhos quando sabe alterações de aninhamento não ocorrem em grupos interessados.

Implantação do XenMobile

August 24, 2018

Há muito a considerar quando você está planejando uma implantação do XenMobile. Quais dispositivos você deve escolher? Como você deve gerenciá-los? Como você garante que sua rede permaneça segura e mesmo assim amigável? Qual hardware você precisa usar e como solucionar possíveis problemas? Este manual tem como objetivo ajudar a responder a essas perguntas e muito mais. Nas páginas a seguir, você encontrará casos de uso e recomendações sobre tópicos que abrangem considerações de implantação, bem como perguntas que talvez você nunca tenha pensado em fazer.

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 iniciar a implantação do XenMobile.

O manual tem três seções principais:

- **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:** Garantia do bom funcionamento do ambiente de execução.

Avaliar

Como em qualquer implantação, avaliar suas necessidades deve ser sua primeira 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 os dois. Qual o nível de segurança que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

você precisa que seu ambiente XenMobile tenha? Vejamos alguns casos de uso comuns e perguntas a serem consideradas ao planejar sua implantação.

- Modos de gerenciamento
- Requisitos de dispositivo
- Segurança e experiência do usuário
- Aplicativos
- Comunidades do usuário
- Estratégia de email
- Integração do XenMobile
- Requisitos para vários locais

Projetar e configurar

Depois de concluir a avaliação de suas necessidades de implantação, você poderá tomar decisões relacionadas ao projeto e à configuração de seu ambiente. Escolher o hardware para seu servidor, configurar políticas para aplicativos e dispositivos e registrar os usuários são apenas algumas das coisas que você precisará planejar. Esta seção inclui casos de uso e recomendações para cada um desses cenários e muito mais.

- Integração com NetScaler e NetScaler Gateway
- Considerações sobre SSO e proxy para aplicativos MDX
- Autenticação
- Arquitetura de referência para implantações locais
- Arquitetura de referência para implantações em nuvem
- Propriedades do servidor
- Políticas de dispositivos e aplicativos
- Opções de registro do usuário
- Ajuste das operações do XenMobile

Operar e monitorar

Depois que o ambiente do XenMobile estiver em funcionamento, você deverá monitorá-lo para garantir uma operação contínua. A seção de monitoramento discute onde você pode encontrar os vários logs e mensagens que o XenMobile e seus componentes geram, bem como a maneira de 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 ao XenMobile

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Monitoramento de sistemas
- Recuperação de desastres
- Processo de suporte Citrix

Modos de gerenciamento

April 15, 2019

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, às vezes também chamados de modos de implantação:

- Modo de gerenciamento de dispositivo móvel (modo MDM)
- Modo de gerenciamento de aplicativo móvel (modo MAM)
- Modo MDM+MAM (modo Empresarial)

Gerenciamento de dispositivo móvel (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 dá suporte à alteração para o modo de autenticação após o registro de 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 no nível do sistema. Você pode configurar políticas, ações e funções de segurança. Por exemplo, você pode apagar um dispositivo seletivamente se o dispositivo 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 da loja de aplicativos pública e aplicativos corporativos, nesse modo. A seguir se encontram casos de uso comuns do modo MDM:

- O MDM é uma consideração para dispositivos de propriedade corporativa em que são necessárias políticas ou restrições de gerenciamento no nível do dispositivo, como apagamento completo, apagamento seletivo ou localização geográfica.
- Quando os clientes exigem o gerenciamento de um dispositivo real, mas não exigem políticas MDX, como conteinerização de aplicativos, controles no compartilhamento de dados de aplicativos ou micro VPN.
- Quando os usuários só precisam de e-mails entregues a seus clientes de email nativos em seus dispositivos móveis, e o Exchange ActiveSync ou o Servidor de Acesso para Cliente já é acessível externamente. Nesse caso de uso, você pode usar o MDM para configurar a entrega de emails.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Quando você implanta aplicativos corporativos nativos (não MDX), aplicativos de loja de aplicativos pública ou aplicativos MDX entregues de lojas públicas. Considere que uma solução MDM sozinha não pode 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 nos aplicativos do Office 365.

Gerenciamento de aplicativo móvel (modo MAM)

O MAM protege os dados do aplicativo e permite controlar o compartilhamento de dados de 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.

Aproveitando as políticas MDX, o XenMobile fornece controle em nível de aplicativo sobre o acesso à rede (como micro VPN), interação com aplicativos e dispositivos, criptografia de dados e acesso a aplicativos.

O modo MAM geralmente é adequado para dispositivos BYO (traga o seu próprio) porque, embora o dispositivo não seja gerenciado, os dados corporativos permanecem protegidos. O MDX tem mais de 50 políticas somente para MAM que podem ser definidas sem a necessidade de um controle do MDM ou sem depender de códigos secretos de dispositivos para criptografia.

O MAM também suporta os aplicativos móveis de produtividade. Esse suporte inclui entrega segura de e-mails para o Citrix Secure Mail, compartilhamento de dados entre aplicativos móveis de produtividade protegidos e armazenamento seguro de dados no ShareFile. Para obter detalhes, consulte mobile productivity apps.

O MAM é geralmente adequado para os exemplos a seguir:

- 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)

O 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 do MDM e do MAM.

O XenMobile permite especificar se os usuários podem optar por desativar o gerenciamento de dispositivos ou se você precisa do gerenciamento de dispositivos. Essa flexibilidade é útil para ambientes

© 1999-2019 Citrix Systems, Inc. All rights reserved.

que incluem uma mistura de casos de uso. Esses ambientes podem ou não exigir o gerenciamento de um dispositivo por meio de políticas do MDM para acessar seus recursos do MAM.

O MDM+MAM é adequado para os exemplos a seguir:

- Você tem um único caso de uso no qual o MDM e o MAM são necessários. O MDM é necessário para acessar seus recursos do MAM.
- Alguns casos de uso exigem MDM, enquanto outros não.
- Alguns casos de uso exigem o MAM, enquanto outros não.

Você especifica o modo de gerenciamento do XenMobile Server por meio da propriedade Modo do Servidor. Você define a configuração no console XenMobile. O modo pode ser MDM, MAM ou ENT (para MDM+MAM).

A edição XenMobile para a qual você possui uma licença determina os modos de gerenciamento e outros recursos disponíveis, conforme mostrado na tabela a seguir.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
Recursos do MDM	Recursos do MDM	Recursos do MDM
-	Recursos do MAM	Recursos do MAM
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	Secure Tasks	Secure Tasks
-	-	ShareConnect
-	-	Secure Notes
-	-	ShareFile Enterprise Edition

Gerenciamento de dispositivos e registro do MDM

Um ambiente XenMobile Enterprise pode incluir uma mistura de casos de uso, alguns dos quais exigem gerenciamento de dispositivos por meio de políticas do MDM para permitir acesso a recursos do MAM. Antes de implantar aplicativos móveis de produtividade para os usuários, avalie completa-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

mente os casos de uso e decida se exigem o registro no MDM. Se posteriormente você decidir alterar o requisito de registro no MDM, é provável que os usuários tenham que registrar seus dispositivos novamente.

> Nota:
>
> Para especificar se é preciso ou não que os usuários se registrem no MDM, use a propriedade do XenMobile Server **Inscrição obrigatória** no console XenMobile (**Configurações > Propriedades do servidor**). Essa propriedade de servidor global se aplica a todos os usuários e dispositivos da instância do XenMobile. A propriedade se aplica somente quando o Modo do XenMobile Server é ENT.

A seguir, você encontra um resumo das vantagens e desvantagens (juntamente com as atenuações) de exigir o registro do MDM em uma implantação do modo XenMobile Enterprise.

Quando o registro no MDM é opcional

Vantagens:

- Os usuários podem acessar os recursos do MAM sem colocar seus dispositivos sob o gerenciamento do MDM. Esta opção pode aumentar a adoção do usuário.
- Capacidade acessar os recursos do MAM com segurança para proteger dados corporativos.
- Políticas de MDX, como **Código secreto de aplicativo**, podem controlar o acesso a aplicativos para cada aplicativo MDX.
- Configurar o tempo de espera do NetScaler, do XenMobile Server e por aplicativo, juntamente com o Citrix PIN, fornece uma camada extra de proteção.
- Embora as ações do MDM não se apliquem ao dispositivo, algumas políticas de MDX estão disponíveis para negar o acesso ao MAM. A negação seria baseada nas configurações do sistema, como dispositivos com jailbreak ou root.
- Os usuários podem optar por registrar seus dispositivos no MDM durante o primeiro uso.

Desvantagens:

- Os recursos do MAM estão disponíveis para dispositivos não registrados no MDM.
- As políticas e ações do MDM estão disponíveis apenas para dispositivos registrados no MDM.

Opções de atenuação:

- Solicite que os usuários concordem com os termos e condições da empresa e se responsabilizem caso decidam não atender à conformidade. Solicite que os administradores monitorem dispositivos não gerenciados.
- Gerencie o acesso e a segurança do aplicativo usando timers de aplicativos. Valores de tempo limite reduzidos aumentam a segurança, mas podem afetar a experiência do usuário.
- Um segundo ambiente XenMobile com registro no MDM é uma opção. Ao considerar essa opção, tenha em mente a sobrecarga de gerenciar dois ambientes e os recursos adicionais necessários.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Quando o registro no MDM é necessário

Vantagens:

- Capacidade de restringir o acesso a recursos do MAM apenas de dispositivos gerenciados pelo MDM.
- As políticas e ações do MDM podem ser aplicadas a todos os dispositivos no ambiente, conforme desejado.
- Os usuários não podem desativar o registro do dispositivo.

Desvantagens:

- Requer que todos os usuários se registrem no MDM.
- Pode diminuir a adoção por usuários que se opõem ao gerenciamento corporativo de seus dispositivos pessoais.

Opções de atenuação:

- Informe 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 de MAM (também chamado de modo somente MAM), para dispositivos que não precisam de gerenciamento do MDM. Ao considerar essa opção, tenha em mente a sobrecarga de gerenciar dois ambientes e os recursos adicionais necessários.

Sobre os modos MAM e MAM Legado

O XenMobile 10.3.5 introduziu um novo modo de servidor Somente MAM. Para distinguir os modos MAM anterior e novo, a documentação usa estes termos. O novo modo é chamado Somente MAM ou MA, o modo MAM anterior é chamado de modo MAM Legado.

O modo somente MAM estará em vigor quando a propriedade Modo de Servidor do XenMobile for MAM. Os dispositivos se registram no modo MAM.

A funcionalidade do MAM legado estará em vigor quando a propriedade Modo de Servidor do XenMobile for ENT e os usuários recusarem o gerenciamento de dispositivo. Nesse caso, os dispositivos se registram no modo MAM. Os usuários que optam pelo gerenciamento do MDM continuam recebendo a funcionalidade do MAM Legado.

> Nota:
>
> Anteriormente, definir a propriedade Modo de Servidor como MAM tinha o mesmo efeito que defini-la como ENT: os usuários que recusavam o gerenciamento MDM recebiam a funcionalidade do MAM legado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A seguinte tabela resume a configuração do Modo de Servidor a ser usada para um tipo específico de licença e o modo de dispositivo desejado:

Suas licenças são desta edição	Você deseja que os dispositivos se registrem neste modo	Defina a propriedade Modo de Servidor como
Enterprise/Advanced/MDM	Modo MDM	MDM
Enterprise/Advanced	Modo MAM (também chamado de modo somente MAM)	MAM
Enterprise/Advanced	Modo MDM+MAM	ENT (Os usuários que recusam o gerenciamento de dispositivo operam sob o modo MAM legado.)

O modo somente MAM suporta os seguintes recursos anteriormente disponíveis apenas para ENT. Esses recursos não estão disponíveis para o Windows Phone.

- **Autenticação baseada em certificado:** o modo somente MAM oferece suporte à autenticação baseada em certificado. Os usuários terão acesso contínuo aos aplicativos mesmo quando a senha do Active Directory expirar. Se você usa autenticação baseada em certificado para dispositivos MAM, você deve configurar seu NetScaler Gateway. Por padrão, nas **Configurações do XenMobile> NetScaler Gateway**, Entregar certificado de usuário para autenticação está **Desativado**, o que significa que a autenticação de nome e senha de usuário é usada. Altere essa configuração para **Ativado** para ativar a autenticação de certificado.
- **Portal de Autoajuda:** para permitir que os usuários executem suas próprias operações de bloqueio de aplicativo e apagamento de aplicativo. Essas ações se aplicam a todos os aplicativos no dispositivo. Você pode configurar as ações Bloqueio de aplicativo e Apagamento de aplicativos em **Configurar > Ações**.
- **Todos os modos de registro:** incluindo Alta Segurança, URL de Convite e Dois Fatores, configurados por meio de **Gerenciar > Convites de registro**.
- **Limite de registro do dispositivo para dispositivos Android e iOS:** a propriedade do servidor **Número de dispositivos por usuário** foi movida para **Configurar > Perfis de registro** e agora se aplica a todos os modos do servidor.
- **APIs somente MAM:** para dispositivos somente MAM, você pode chamar os serviços REST usando qualquer cliente REST e a API REST do XenMobile para chamar os serviços que o console XenMobile expõe.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- As APIs somente MAM permitem:
  - Enviar uma URL de convite e um PIN de uso único.
  - Emitir ações de bloqueio e apagamento de aplicativos em dispositivos.

A tabela a seguir resume as diferenças entre a funcionalidade MAM legado e somente MAM.

Cenários de registro e outros recursos	MAM legado (o modo de servidor é ENT)	Modo somente MAM (o modo de servidor é MAM)
Autenticação de certificado	Não compatível.	Compatível. Para a autenticação de certificado, o NetScaler Gateway é necessário.
Requisito de implantação	O Servidor XenMobile não precisa ser diretamente acessível dos dispositivos.	O Servidor XenMobile não precisa ser diretamente acessível dos dispositivos.
Opção de registro	Use o FQDN do NetScaler Gateway ou, ao usar o FQDN do MDM, opte por não se registrar.	Use o FQDN do Servidor XenMobile.
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 apagamento de aplicativos	Compatível.	Compatível.
Opções do Portal de Autoajuda para bloqueio e apagamento de aplicativos	Não compatível.	Compatível.
Comportamento do apagamento 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ações automatizadas para os usuários somente MAM.	As ações de evento, propriedade de dispositivo e propriedade de usuário são compatíveis. Não suporta ações automatizadas baseadas em aplicativos instaladas.	Suporta evento, propriedade de dispositivo, propriedade de usuário e algumas ações baseadas em aplicativo, incluindo apagamento de aplicativo e bloqueio de aplicativo.
Ação interna quando um usuário do Active Directory é excluído	Suporta apagamento de aplicativos.	Suporta apagamento 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 aplicativos instalados em um dispositivo	Não compatível.

***Em relação às notificações:** o SMTP é o único método suportado para enviar convites de registro.

> Importante:
>
> Para o modo somente MAM, os usuários registrados anteriormente devem registrar seus dispositivos novamente. Forneça aos usuários o FQDN do XenMobile Server que eles precisam para o registro. No modo somente MAM, como no modo ENT, os dispositivos se registram usando o FQDN do XenMobile Server. (No modo MAM legado, os dispositivos se registram usando o FQDN do NetScaler Gateway.)

Requisitos de dispositivo

April 15, 2019

Um ponto importante a ser considerado em qualquer implantação é o dispositivo que você planeja lançar. Nas plataformas iOS, Android e Windows, as opções são numerosas. Para obter uma lista de dispositivos compatíveis com o XenMobile, consulte Plataformas de dispositivo com suporte.

Em um ambiente "traga seu próprio dispositivo" (BYOD), é possível uma mistura de plataformas suportadas. No entanto, considere as limitações no artigo sobre a plataforma de dispositivos com suporte ao informar os usuários sobre os dispositivos que podem ser registrados. Mesmo se você permitir

© 1999-2019 Citrix Systems, Inc. All rights reserved.

apenas um ou dois dispositivos em seu ambiente, o XenMobile funciona de maneira um pouco diferente em dispositivos iOS, Android e Windows. Conjuntos de recursos diferentes estão disponíveis em cada plataforma.

Além disso, nem todos os designs de aplicativos segmentam os fatores de formato de tablets e de telefones. Antes de fazer alterações generalizadas, teste os aplicativos para garantir que eles se encaixem na tela do dispositivo que você deseja implantar.

Você também pode considerar fatores de registro. Apple e Google oferecem programas de registro corporativa. Por meio do Device Enrollment Program (DEP) da Apple e do Google Android for Work você pode comprar dispositivos pré-configurados e prontos para serem usados pelos funcionários. Mesmo quando você não usa esses programas, considere se deseja enviar links de convite para seus usuários por meio do SMS. Você não pode usar o SMS em tablets.

Para obter mais informações sobre registro, consulte Opções de registro do usuário.

Segurança e experiência do usuário

April 15, 2019

A segurança é importante para qualquer organização, mas você precisa encontrar um equilíbrio entre segurança e experiência do usuário. Por um lado, você pode ter um ambiente bastante seguro, mas que é muito difícil para os usuários usarem. Mas por outro lado, seu ambiente pode ser tão fácil de usar que o seu controle de acesso não se mostra tão rigoroso. As outras seções deste manual virtual abordam os recursos de segurança em detalhes, mas o objetivo deste artigo é oferecer uma visão geral das opções de segurança disponíveis para você e lhe expor as considerações comuns de segurança no XenMobile.

Aqui estão algumas considerações importantes a serem analisadas para cada caso de uso:

- Você quer proteger determinados aplicativos, o dispositivo inteiro ou ambos?
- Como você deseja que seus usuários autentiquem a identidade deles? Você usará LDAP, autenticação baseada em certificado ou uma combinação dos dois?
- Quanto tempo deve passar antes que a sessão de um usuário expire? Tenha em mente que existem diferentes valores de tempo limite para serviços em segundo plano, NetScaler e para poder acessar aplicativos enquanto estiver off-line.
- Deseja que os usuários definam um código secreto no nível do dispositivo e/ou um código secreto no nível do aplicativo? Quantas tentativas de login você deseja conceder aos usuários? Tenha em mente os requisitos adicionais de autenticação por aplicativo que podem ser implementados com o MAM e como os usuários podem interpretá-los.
- Quais outras restrições você deseja impor aos usuários? Eles devem poder acessar serviços em nuvem, como a Siri? O que eles podem fazer com cada aplicativo disponibilizado para eles e o

© 1999-2019 Citrix Systems, Inc. All rights reserved.

que eles não podem fazer? Você deve implantar políticas de Wi-Fi corporativas para impedir que os dados de planos de celular sejam consumidos enquanto estiver dentro da área do escritório?

Aplicativo versus Dispositivo

Uma das primeiras coisas que você deve considerar é se você deve proteger apenas determinados aplicativos (gerenciamento de aplicativos móveis ou MAM) ou se deseja gerenciar todo o dispositivo (gerenciamento de dispositivos móveis ou MDM). Normalmente, se você não precisar de controle no nível do dispositivo, só precisará gerenciar aplicativos para dispositivos móveis, especialmente se a sua organização trabalhar com dispositivos BYOD (Traga seu próprio dispositivo).

Em um ambiente somente MAM, os usuários podem acessar os recursos disponibilizados para eles. As políticas do MAM protegem e gerenciam os aplicativos em si.

O MDM permite proteger um dispositivo inteiro, incluindo a capacidade de fazer um inventário de todos os softwares em um dispositivo e impedir o registro se o dispositivo estiver com jailbroken ou com root, ou se contiver um software não seguro instalado. No entanto, esse nível de controle deixa os usuários desconfiados de dar tanto poder sobre seus dispositivos pessoais e pode reduzir as taxas de registro.

É possível exigir o MDM para alguns dispositivos e não para outros, mas tenha em mente que essa escolha pode envolver a configuração de dois ambientes dedicados, o que requer recursos e manutenção adicionais.

Autenticação

Autenticação é onde ocorre grande parte da experiência do usuário. Se sua organização já estiver executando o Active Directory, o uso do Active Directory é a maneira mais simples de fazer com que seus usuários acessem o sistema.

Outra grande parte da experiência do usuário em relação à autenticação é o tempo limite. Um ambiente de alta segurança pode exigir que os usuários façam login toda vez que acessarem o sistema, mas essa opção pode não ser ideal para todas as organizações. Por exemplo, fazer com que os usuários insiram suas credenciais cada vez que desejam acessar seus e-mails pode ser muito laborioso e não justificar o esforço.

Entropia de usuário

Para maior segurança, você pode ativar um recurso chamado *entropia de 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

genérico no Secure Hub. Se você habilitar a entropia de usuário através da opção **Criptografar segredos**, o XenMobile cria um novo cofre chamado UserEntropy e move as informações do cofre genérico para este novo cofre. Para que o Secure Hub ou outro aplicativo acesse os dados, os usuários devem inserir uma senha ou PIN.

A ativação da entropia de usuário adiciona outra camada de autenticação a vários lugares. Isso significa que sempre que um aplicativo exigir acesso a dados compartilhados no cofre UserEntropy, que inclui senhas, PINs e certificados, os usuários precisarão digitar uma senha ou PIN.

Você pode saber mais sobre a entropia de usuário lendo Sobre o MDX Toolkit na documentação do XenMobile. Para ativar a entropia de usuário, você pode encontrar as configurações relacionadas nas Propriedades do cliente.

Políticas

As políticas MDX e MDM oferecem bastante flexibilidade às organizações, mas também podem restringir os usuários. Você pode precisar disso em algumas situações, mas as políticas também podem tornar um sistema inutilizável. Por exemplo, você pode querer bloquear o acesso a aplicativos em nuvem, como a Siri ou o iCloud, que têm o potencial de enviar dados confidenciais para onde você não quer. Você pode configurar uma política para bloquear o acesso a esses serviços, mas lembre-se de que tal política pode ter consequências indesejadas. O microfone para teclado do iOS também depende do acesso à nuvem, e você irá bloquear o acesso a esse recurso também.

Aplicativos

Gerenciamento de Mobilidade Empresarial (EMM) em Gerenciamento de Dispositivos Móveis (MDM) e Gerenciamento de Aplicativos Móveis (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 implementar uma solução MAM, como o XenMobile, para ajudar na entrega de aplicativos, no licenciamento de software, na configuração e no gerenciamento do ciclo de vida do aplicativo.

Com o XenMobile, você pode proteger esses aplicativos ainda mais, configurando políticas específicas de MAM e configurações de VPN para evitar o vazamento de dados e outras ameaças de segurança. O XenMobile fornece às organizações a flexibilidade de implantar sua solução como um ambiente somente MAM ou somente MDM, ou implementar o XenMobile como um ambiente XenMobile Enterprise unificado que fornece a funcionalidade MDM e MAM na mesma plataforma.

Além da capacidade de fornecer aplicativos para dispositivos móveis, o XenMobile oferece contêiner de aplicativos por meio da tecnologia MDX. O MDX protege os aplicativos por meio de criptografia separada da criptografia no nível do dispositivo; você pode apagar ou bloquear o aplicativo, e os aplica-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tivos estão sujeitos a controles baseados em políticas granulares. Os fornecedores independentes de software (ISVs) podem aplicar esses controles usando o SDK do aplicativo Worx.

Em um ambiente corporativo, os usuários usam uma variedade de aplicativos móveis para ajudar em suas funções. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente ou aplicativos nativos, em alguns casos. O XenMobile categoriza esses aplicativos da seguinte maneira:

Aplicativos públicos: estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como iTunes ou o Google Play. Fornecedores fora da organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Esta 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 os aplicativos GoToMeeting, Salesforce e EpicCare.

A Citrix não suporta o download de binários de aplicativos diretamente de lojas de aplicativos públicas para posterior preparação o MDX Toolkit para distribuição corporativa. Se você precisar preparar aplicativos de terceiros, fale com o fornecedor do aplicativo para obter os binários do aplicativo, que você pode preparar usando o MDX Toolkit.

Aplicativos internos: muitas organizações possuem desenvolvedores internos que criam aplicativos que fornecem funcionalidade específica e são desenvolvidos e distribuídos de maneira independente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos que os ISVs fornecem. Você pode implantar esses aplicativos como aplicativos nativos ou pode agrupar os aplicativos em contêineres usando uma solução MAM, como o XenMobile. Por exemplo, uma organização de medicina e saúde pode criar um aplicativo interno que permita que os médicos visualizem informações do paciente em dispositivos móveis. A organização pode então usar o MDX Toolkit para preparar o aplicativo, a fim de proteger as informações do paciente e permitir o acesso VPN ao servidor de banco de dados de pacientes de back-end.

Aplicativos Web e SaaS: esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). O XenMobile também permite que você crie aplicativos da Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) em aplicativos da Web existentes. Para obter detalhes, consulte Tipos de conector de aplicativo. Por exemplo, você pode usar o SAML do Google Apps para SSO com base no SAML (Security Assertion Markup Language) para o Google Apps.

Aplicativos móveis de produtividade: aplicativos desenvolvidos pela Citrix e incluídos na licença do XenMobile. Para obter detalhes, consulte Sobre aplicativos móveis de produtividade. A Citrix também oferece outros aplicativos prontos para negócios que os ISVs desenvolvem usando o Worx App SDK.

Aplicativos HDX: esses são aplicativos hospedados no Windows que você publica com o StoreFront. Se você tiver um ambiente Citrix XenApp e XenDesktop, poderá integrar os aplicativos ao XenMobile para disponibilizar os aplicativos para os usuários registrados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração e a arquitetura subjacentes serão diferentes. Por exemplo, se vários grupos de usuários com diferentes níveis de permissões consumirem um único aplicativo, talvez seja necessário criar grupos de entrega separados para implantar duas versões separadas do mesmo aplicativo. Além disso, você deve garantir que a associação do grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos dos usuários.

Você também pode querer gerenciar o licenciamento de aplicativos iOS usando o Volume Purchase Program (VPP) da Apple. Essa opção exigirá que você se registre no programa VPP e defina as configurações do XenMobile VPP no console XenMobile para distribuir os aplicativos com as licenças do VPP. Uma variedade de tais casos de uso torna importante avaliar e planejar sua estratégia MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia MAM definindo o seguinte:

Tipos de aplicativos: liste os diferentes tipos de aplicativos aos quais você planeja oferecer suporte e categorizar, como públicos, nativos, aplicativos móveis de produtividade, da Web, internos, de ISV e assim por diante. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajudará no alinhamento de diferentes configurações do XenMobile necessárias para cada tipo de aplicativo. Por exemplo, determinados aplicativos podem não se qualificar para o agrupamento ou alguns aplicativos podem exigir o uso do SDK do aplicativo Worx para ativar APIs especiais para interação com outros aplicativos.

Requisitos de rede: você precisa configurar 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 VPN; alguns aplicativos podem exigir acesso à Internet para rotear o acesso por meio da DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você precisa definir várias configurações de acordo. A definição de requisitos de rede por aplicativo ajuda a finalizar suas decisões de arquitetura desde o início, o que simplificará o processo geral de implementação.

Requisitos de segurança: a definição dos requisitos de segurança que se aplicam a aplicativos individuais ou a todos os aplicativos é fundamental para garantir que você crie as configurações corretas ao instalar o XenMobile Server. Embora as configurações, como as políticas MDX, se apliquem a aplicativos individuais, as configurações de sessão e autenticação se aplicam a todos os aplicativos e alguns aplicativos podem ter requisitos específicos de criptografia, contêiner, preparação, criptografia, autenticação, geocerca, senha ou compartilhamento de dados precisa delinear com antecedência para simplificar sua implantação.

Requisitos de implantação: convém usar uma implantação baseada em políticas para permitir que apenas usuários em conformidade baixem os aplicativos publicados. Por exemplo, você pode querer que determinados aplicativos exijam que a criptografia do dispositivo esteja ativada ou que o dispositivo seja gerenciado ou que o dispositivo atenda a uma versão mínima do sistema operacional. Você também pode querer que determinados aplicativos estejam disponíveis apenas para usuários corpo-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

rativos. Você precisa descrever esses requisitos com antecedência para poder configurar as regras ou ações de implantação apropriadas.

Requisitos de licenciamento: você deve registrar os requisitos de licenciamento relacionados ao aplicativo. Essas notas ajudarão você a gerenciar o uso da licença com eficiência e a decidir se você precisa configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo para iOS, independentemente de ser um aplicativo gratuito ou pago, a Apple aplicará os requisitos de licenciamento ao aplicativo, fazendo com que os usuários entrem em sua conta do iTunes. Você pode se registrar no Apple VPP para distribuir e gerenciar esses aplicativos via XenMobile. O VPP permite que os usuários baixem os aplicativos sem precisar entrar em suas contas do iTunes. Além disso, ferramentas como o Samsung SAFE e o Samsung KNOX têm requisitos especiais de licenciamento, que você precisa concluir antes de implantar esses recursos.

Requisitos da lista negra/lista branca: haverá aplicativos que você não deseja que os usuários instalem ou usem. A criação de uma lista negra definirá um evento fora de conformidade. Você pode configurar políticas para acionar no caso de tal coisa acontecer. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode se enquadrar na lista negra por um motivo ou outro. Se esse for o 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. Isso pode entrar em conflito com sua estratégia de lista negra.

Caso de uso de aplicativos

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

- **Aplicativos móveis de produtividade:** Aplicativos para iOS e Android fornecidos pela Citrix.
- **Secure Mail:** email, calendário e aplicativo de contato.
- **Secure Web:** navegador seguro que fornece acesso aos sites da Internet e da intranet.
- **Secure Notes:** aplicativo de anotações seguro com integração de email e calendário.
- **ShareFile:** 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 parâmetros de segurança, configurações e aplicativos móveis para dispositivos móveis via cliente do Secure Hub. Dispositivos Android e iOS se registram no XenMobile através do Secure Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Citrix Receiver:** aplicativo móvel que permite aos usuários abrir aplicativos host do XenApp em dispositivos móveis.
- **GoToMeeting:** um cliente de reunião on-line, compartilhamento de área de trabalho e videoconferência que permite que os usuários se encontrem com outros usuários de computador, clientes, consumidores ou colegas pela Internet em tempo real.
- **SalesForce1:** o Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúnam todos os aplicativos Chatter, CRM, personalizados e 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, listas de pacientes, agendamentos e mensagens.
  - **Haiku:** aplicativo móvel para telefones iPhone e Android.
  - **Canto:** aplicativo móvel para o iPad
  - **Rover:** aplicativos móveis para iPhone e iPad.

HDX: esses aplicativos são entregues via Citrix XenApp.

- **Epic Hyperspace:** aplicativo cliente Epic para gerenciamento eletrônico de prontuários médicos.

ISV

- **Vocera:** aplicativo móvel de mensagens e IP de voz compatível com HIPAA que amplia os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, através de 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 da web internos

- **PatientRounding:** aplicativo da Web usado para registrar informações médicas do paciente por diferentes departamentos.
- **Outlook Web Access:** permite o acesso de email por meio de um navegador da 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome do aplicativo	Tipo de aplicativo	Preparação de MDX	iOS	Android
Secure Mail	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Web	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Notes	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
ShareFile	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo público	N/D	Sim	Sim
Citrix Receiver	Aplicativo público	N/D	Sim	Sim
GoToMeeting	Aplicativo público	N/D	Sim	Sim
SalesForce1	Aplicativo público	N/D	Sim	Sim
RSA SecurID	Aplicativo público	N/D	Sim	Sim
Epic Haiku	Aplicativo público	N/D	Sim	Sim
Epic Canto	Aplicativo público	N/D	Sim	Não
Epic Rover	Aplicativo público	N/D	Sim	Não
Epic Hyperspace	Aplicativo HDX	N/D	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo interno	Sim	Sim	Sim

© 1999-2019 Citrix Systems, Inc. All rights reserved.

PatientRounding	Aplicativo Web	N/D	Sim	Sim
Outlook Web Access	Aplicativo Web	N/D	Sim	Sim
SharePoint	Aplicativo Web	N/D	Sim	Sim

As tabelas a seguir listam os requisitos específicos que você pode consultar ao configurar as políticas do MAM no XenMobile.

Nome do aplicativo	**VPN necessária**	**Interação**	**Interação**	**Criptografia de dispositivo**
		(com aplicativos fora do contêiner)	**(de aplicativos fora do contêiner)**	
——————–	——————	——————————————————–	——————————————————–	——————–
Secure Mail	S	Permitido seletivamente	Permitido	Desnecessário
Secure Web	S	Permitido	Permitido	Desnecessário
Secure Notes	S	Permitido	Permitido	Desnecessário
ShareFile	S	Permitido	Permitido	Desnecessário
Secure Hub	S	N/D	N/D	N/D
Citrix Receiver	S	N/D	N/D	N/D
GoToMeeting	N	N/D	N/D	N/D
SalesForce1	N	N/D	N/D	N/D
RSA SecurID	N	N/D	N/D	N/D
Epic Haiku	S	N/D	N/D	N/D
Epic Canto	S	N/D	N/D	N/D
Epic Rover	S	N/D	N/D	N/D
Epic Hyperspace	S	N/D	N/D	N/D
Vocera	S	Não permitido	Não permitido	Desnecessário
HCMail	S	Não permitido	Não permitido	Obrigatório
PatientRounding	S	N/D	N/D	Obrigatório
Outlook Web Access	S	N/D	N/D	Desnecessário
SharePoint	S	N/D	N/D	Desnecessário

Nome do aplicativo	**Filtragem Proxy**	**Licenciamento**	**Cerca geográfica**	**Worx App SDK**	**Versão mínima do sistema operacional**
Secure Mail	Obrigatório	N/D	Seletivamente Obrigatório	N/D	Imposto

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome do aplicativo	Filtragem Proxy	Licenciamento	Cerca geográfica	Worx App SDK	Versão mínima do sistema operacional
Secure Web	Obrigatório	N/D	Desnecessário	N/D	Imposto
Secure Notes	Obrigatório	N/D	Desnecessário	N/D	Imposto
ShareFile	Obrigatório	N/D	Desnecessário	N/D	Imposto
Secure Hub	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
Citrix Receiver	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
GoToMeeting	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
SalesForce1	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
RSA SecurID	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
Epic Haiku	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
Epic Canto	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
Epic Rover	Desnecessário	VPP	Desnecessário	N/D	Não aplicado
Epic Hyperspace	Desnecessário	N/D	Desnecessário	N/D	Não aplicado
Vocera	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto
HCMail	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto
PatientRound-ing	Obrigatório	N/D	Desnecessário	N/D	Não aplicado
Outlook Web Access	Obrigatório	N/D	Desnecessário	N/D	Não aplicado
SharePoint	Obrigatório	N/D	Desnecessário	N/D	Não aplicado

Comunidades do usuário

Cada organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários executam tarefas e funções de escritório diferentes usando vários recursos fornecidos por meio dos dispositivos móveis dos usuários. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis fornecidos por você ou usando dispositivos móveis deles próprios, o que permite que acessem ferramentas que estão sujeitas a determinadas regras de conformidade de segurança.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

À medida que mais e mais comunidades de usuários começam a usar dispositivos móveis para simplificar ou ajudar em suas funções, o gerenciamento de mobilidade empresarial (EMM) se torna crítico para evitar o vazamento de dados e impor restrições de segurança de uma organização. Para um gerenciamento eficiente e sofisticado de dispositivos móveis, 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 assistência médica são classificadas para o EMM.

Cado de uso de comunidades de usuários

Neste exemplo, esta organização de assistência médica fornece recursos de tecnologia e acesso a vários usuários, incluindo funcionários e voluntários da rede e afiliados. A organização optou por implantar a solução EMM apenas para usuários não executivos.

Os cargos e funções dos usuários dessa organização podem ser divididos em subgrupos, incluindo: clínico, não clínico e contratados. Um grupo 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 correto de restrições de segurança e impedir o vazamento de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado, corporativo e BYOD (traga seu próprio dispositivo). Além disso, os usuários só podem registrar um único dispositivo.

A seção a seguir fornece uma visão geral dos cargos e funções de cada subgrupo:

Clínico

- Enfermeiros
- Médicos (doutores, cirurgiões e outros)
- Especialistas (nutricionistas, flebotomistas, anestesistas, radiologistas, cardiologistas, oncologistas e outros)
- Médicos externos (médicos não empregados e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (trabalhadores de escritório e móveis realizando serviços médicos em visitas domiciliares ao paciente)
- Especialista em pesquisa (trabalhadores do conhecimento e usuários avançados em seis institutos de pesquisa que realizam pesquisas clínicas para encontrar respostas para problemas clínicos)
- Educação e Formação (enfermeiros, médicos e especialistas em educação e formação)

Não clínico

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Serviços compartilhados (funcionários de escritório executando várias funções de back-office, incluindo: RH, folha de pagamento, contas a pagar, serviço de cadeia de fornecimento e outros)
- Serviços Médicos (funcionários do escritório realizando uma variedade de soluções de gestão de saúde, serviços administrativos e processos de negócios para fornecedores, incluindo: Serviços Administrativos, Analytics e Business Intelligence, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e outros)
- Serviços de Suporte (trabalhadores de escritório realizando uma variedade de funções não clínicas, incluindo Administração de Benefícios, Integração Clínica, Comunicações, Gerenciamento de Compensação e Desempenho, Serviços de Instalações e Propriedade, Sistemas de Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos e outros)
- Programas filantrópicos (funcionários de escritório e móveis que realizam várias funções de apoio a programas filantrópicos)

Contratados

- Parceiros fabricantes e fornecedores (conectados no local e remotamente via VPN site-to-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.

Grupos e Unidades Organizacionais (OUs) 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 Formação
- OU = Não clínico; Grupos =
  - XM-Serviços Compartilhados
  - XM-Serviços Médicos
  - XM-Serviços de Suporte
  - XM-Programas Filantrópicos

Usuários locais e grupos do XenMobile

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ForGroup= Contratados, Usuários =

- Vendor1
- Vendor2
- Vendor3
- … Vendor10

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 Formação
- Não clínicos-Serviços Compartilhados
- Não clínicos-Serviços Médicos
- Não clínicos-Serviços de Suporte
- Não clínicos-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 Formação	Clínico-Educação e Formação
XM-Serviços Compartilhados	Não clínicos-Serviços Compartilhados
XM-Serviços Médicos	Não clínicos-Serviços Médicos
XM-Serviços de Suporte	Não clínicos-Serviços de Suporte
XM-Programas Filantrópicos	Não clínicos-Programas Filantrópicos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 o aplicativo público, os aplicativos HDX e os 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 Formação		X	X
Não clínicos-Serviços Compartilhados		X	X
Não clínicos-Serviços Médicos		X	X
Não clínicos-Serviços de Suporte	X	X	X
Não clínicos-Programas Filantrópicos	X	X	X
Contratados	X	X	X

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Grupos de entrega do XenMobile	Aplicativo público: RSA SecurID	Aplicativo público: EpicCare Haiku	Aplicativo HDX: Epic Hyperspace	Política de código secreto	Restrições de dispositivos	Ações automatizadas	Política de WiFi
Clínico-Enfermeiros							X
Clínico-Médicos					X		
Clínico-Especialistas							
Clínico-Médicos Externos							
Clínico-Serviços de Saúde Domiciliar							
Clínico-Especialista em Pesquisa							
Clínico-Educação e Formação		X	X				
Não clínicos-Serviços Compartilhados		X	X				

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Não clínicos-Serviços Médicos	X	X	
Não clínicos-Serviços de Suporte	X	X	

Notas e considerações

- O XenMobile cria um grupo de entrega padrão chamado Todos os Usuários durante a configuração inicial. Se você não desabilitar esse grupo de entrega, todos os usuários do Active Directory terão direitos para 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 esteja 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 no MDM obrigatório, você deve definir a opção de Registro Obrigatório como True em Propriedades do Servidor no console 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 de 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 da empresa e dispositivos de propriedade do usuário, também conhecidos como BYOD (traga o seu próprio dispositivo). Você pode controlar como os dispositivos BYOD se conectam à sua rede em dois locais no console XenMobile: nas Regras de implantação e nas propriedades do XenMobile Server na página Configurações. Para obter detalhes sobre regras de implantação, consulte Configuração de regras de implantação na documentação do XenMobile. Para obter detalhes sobre as propriedades do servidor, consulte Propriedades do servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ao definir as propriedades do servidor, você pode exigir que todos os usuários de BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que eles possam acessar os aplicativos, ou você pode conceder aos usuários acesso a aplicativos corporativos sem precisar 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 o registro não terá acesso aos aplicativos. Sugerimos configurar **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança em conjunto com uma experiência de usuário positiva, o que tem muito a ver com o registro do dispositivo dos usuários no XenMobile.

Se você deixar o **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários poderão recusar o registro, mas ainda poderão acessar os aplicativos em seus dispositivos através da XenMobile Store. Você pode considerar a configuração de **wsapi.mdm.required.flag** como **false** em ambientes nos quais as restrições de privacidade, legais ou regulamentares não exigem gerenciamento de dispositivos, 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 apagamento seletivo ou completo, você controla o acesso aos aplicativos por meio de políticas de aplicativos. As políticas, dependendo dos valores definidos, exigem que o dispositivo verifique o XenMobile Server rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Requisitos de segurança

A quantidade de considerações de segurança ao implantar um ambiente XenMobile pode se acumular rapidamente. Há muitas definições e configurações interligadas, que você pode acabar por não saber por onde começar ou o que escolher para garantir que um nível aceitável de proteção esteja disponível. Para tornar essas escolhas mais simples, a Citrix fornece recomendações para Alta, Maior e Altíssima Segurança, conforme descrito na tabela a seguir.

Observe que as preocupações de segurança sozinhas não devem ditar sua opção de modo de implementação. É importante também revisar os requisitos do caso de uso e decidir se você pode atenuar as considerações com a 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.

Maior: essas configurações atingem um equilíbrio mais acirrado entre segurança e usabilidade.

Altíssima: seguir essas recomendações fornecerá um nível bastante alto de segurança em troca de usabilidade e adoção do usuário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Considerações sobre segurança no modo de implantação

A tabela a seguir especifica os modos de implantação para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
MAM e/ou MDM	MDM+MAM	MDM+MAM; mais FIPS

Notas:

- Dependendo do caso de uso, uma implantação somente MDM ou somente MAM pode atender aos requisitos de segurança e fornecer uma boa experiência ao usuário.
- Se não houver necessidade de conteinerização de aplicativo, micro VPN ou políticas específicas de aplicativo, o MDM deve ser suficiente para gerenciar e proteger dispositivos.
- Para casos de uso como BYOD e nos quais todos os requisitos comerciais e de segurança podem ser satisfeitos apenas com conteinerização de aplicativos, a Citrix recomenda o modo somente MAM.
- Para ambientes de alta segurança (e dispositivos corporativos), a Citrix recomenda o MDM+MAM para aproveitar todos os recursos de segurança disponíveis. Você deve impor o registro MDM por meio de uma propriedade do servidor no console XenMobile.
- Opções FIPS para ambientes com as mais altas necessidades de segurança, como o governo federal.

Se você habilitar o modo FIPS, deverá configurar o SQL Server para criptografar o tráfego do SQL.

Considerações de segurança do NetScaler e do NetScaler Gateway

A tabela a seguir especifica as recomendações do NetScaler e do NetScaler Gateway para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O NetScaler é recomendado. O NetScaler Gateway é necessário para MAM e ENT; recomendado para MDM	Configuração do assistente para Standard NestScale for XenMobile com ponte SSL se o XenMobile estiver na DMZ; ou descarga de SSL se necessário para atender aos padrões de segurança quando o XenMobile Server estiver na rede interna.	Descarga de SSL com criptografia de ponta a ponta

Notas:

- Expor o XenMobile Server à Internet via NAT ou proxies/balanceadores de carga existentes de terceiros pode ser uma opção para o MDM, desde que o tráfego SSL termine no XenMobile Server, mas essa escolha representa um risco potencial à segurança.
- Para ambientes de alta segurança, o NetScaler com a configuração padrão do XenMobile deve atender ou exceder os requisitos de segurança.
- Para ambientes de MDM com as mais altas necessidades de segurança, a terminação SSL no NetScaler fornece a capacidade de inspecionar o tráfego no perímetro, enquanto mantém a criptografia SSL de ponta a ponta.
- Opções para definir criptografias SSL/TLS.
- O hardware SSL FIPS NetScaler também está disponível.
- Para obter mais informações, consulte Integração com o NetScaler Gateway e NetScaler.

Considerações sobre segurança de registro

A tabela a seguir especifica as recomendações do NetScaler e do NetScaler Gateway para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado.	Modo de registro apenas por convite. Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado	Modo de registro vinculado ao ID do dispositivo. Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Notas:

- A Citrix geralmente recomenda que você restrinja o registro somente aos usuários em grupos predefinidos do Active Directory. Isso requer a desativação do grupo de entrega interno Todos os Usuários.
- Você pode usar convites de registro para restringir o registro para os usuários com apenas um convite.
- Você pode usar os convites de registro de PIN de uso único (OTP) como uma solução de dois fatores e controlar o número de dispositivos que um usuário pode registrar.
- Para ambientes com requisitos de segurança, você pode associar convites de registro a um dispositivo por UDID/SN/EMEI. Uma opção de dois fatores também está disponível para exigir senha do Active Directory e OTP. (No momento, o OTP não é uma opção disponível para dispositivos Windows.)

Considerações sobre segurança do PIN do dispositivo

A tabela a seguir especifica as recomendações de PIN do dispositivo para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
Recomendado Alta segurança é necessária para criptografia no nível do dispositivo. Pode ser aplicado com o MDM. Pode ser definido conforme necessário para somente MAM usando uma política MDX.	Aplicado usando a política do MDM e/ou MDX.	Aplicado usando a política MDM e MDX. Política de código secreto Complexo do MDM.

Notas:

- A Citrix recomenda o uso de um PIN de dispositivo.
- Você pode impor um PIN de dispositivo por meio de uma política de MDM.
- Você pode usar uma política de MDX para tornar um PIN de dispositivo um requisito para o uso de aplicativos gerenciados como, por exemplo, para casos de uso de 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 complexas de código secreto e aplicá-las com o MDM. Você pode configurar ações automáticas para

© 1999-2019 Citrix Systems, Inc. All rights reserved.

notificar os administradores ou iniciar o apagamento seletivo/completo de dispositivos quando um dispositivo não obedecer a uma política de código secreto.

Aplicativos

April 15, 2019

Gerenciamento de Mobilidade Empresarial (EMM) em Gerenciamento de Dispositivos Móveis (MDM) e Gerenciamento de Aplicativos Móveis (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 implementar uma solução MAM, como o XenMobile, para ajudar na entrega de aplicativos, no licenciamento de software, na configuração e no gerenciamento do ciclo de vida do aplicativo.

Com o XenMobile, você pode proteger esses aplicativos ainda mais, configurando políticas específicas de MAM e configurações de VPN para evitar o vazamento de dados e outras ameaças de segurança. O XenMobile fornece às organizações a flexibilidade de implantar sua solução como um ambiente somente MAM ou somente MDM, ou implementar o XenMobile como um ambiente XenMobile Enterprise unificado que fornece a funcionalidade MDM e MAM na mesma plataforma.

Além da capacidade de fornecer aplicativos para dispositivos móveis, o XenMobile oferece contêiner de aplicativos por meio da tecnologia MDX. O MDX protege os aplicativos por meio de criptografia separada da criptografia no nível do dispositivo; você pode apagar ou bloquear o aplicativo, e os aplicativos estão sujeitos a controles baseados em políticas granulares. Os fornecedores independentes de software (ISVs) podem aplicar esses controles usando o SDK do aplicativo Worx.

Em um ambiente corporativo, os usuários usam uma variedade de aplicativos móveis para ajudar em suas funções. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente ou aplicativos nativos, em alguns casos. O XenMobile categoriza esses aplicativos da seguinte maneira:

- **Aplicativos públicos:** estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como iTunes ou o Google Play. Fornecedores fora da organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Esta 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 os aplicativos GoToMeeting, Salesforce e EpicCare.

  A Citrix não suporta o download de binários de aplicativos diretamente de lojas de aplicativos públicas para posterior preparação o MDX Toolkit para distribuição corporativa. Se você precisar preparar aplicativos de terceiros, fale com o fornecedor do aplicativo para obter os binários do aplicativo, que você pode preparar usando o MDX Toolkit.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Aplicativos internos:** muitas organizações possuem desenvolvedores internos que criam aplicativos que fornecem funcionalidade específica e são desenvolvidos e distribuídos de maneira independente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos que os ISVs fornecem. Você pode implantar esses aplicativos como aplicativos nativos ou pode agrupar os aplicativos em contêineres usando uma solução MAM, como o XenMobile. Por exemplo, uma organização de medicina e saúde pode criar um aplicativo interno que permita que os médicos visualizem informações do paciente em dispositivos móveis. A organização pode então usar o MDX Toolkit para preparar o aplicativo, a fim de proteger as informações do paciente e permitir o acesso VPN ao servidor de banco de dados de pacientes de back-end.
- **Aplicativos Web e SaaS:** esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). O XenMobile também permite que você crie aplicativos da Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) em aplicativos da Web existentes. Para obter detalhes, consulte Tipos de conector de aplicativo. Por exemplo, você pode usar o SAML do Google Apps para SSO com base no SAML (Security Assertion Markup Language) para o Google Apps.
- **Aplicativos móveis de produtividade Citrix:** aplicativos desenvolvidos pela Citrix e incluídos na licença do XenMobile. Para obter detalhes, consulte Sobre aplicativos móveis de produtividade. A Citrix também oferece outros aplicativos prontos para negócios que os ISVs desenvolvem usando o Worx App SDK.
- **Aplicativos HDX:** esses são aplicativos hospedados no Windows que você publica com o StoreFront. Se você tiver um ambiente Citrix XenApp e XenDesktop, poderá integrar os aplicativos ao XenMobile para disponibilizar os aplicativos para os usuários registrados.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração e a arquitetura subjacentes serão diferentes. Por exemplo, se vários grupos de usuários com diferentes níveis de permissões consumirem um único aplicativo, talvez seja necessário criar grupos de entrega separados para implantar duas versões separadas do mesmo aplicativo. Além disso, você deve garantir que a associação do grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos dos usuários.

Você também pode querer gerenciar o licenciamento de aplicativos iOS usando o Volume Purchase Program (VPP) da Apple. Essa opção exigirá que você se registre no programa VPP e defina as configurações do XenMobile VPP no console XenMobile para distribuir os aplicativos com as licenças do VPP. Uma variedade de tais casos de uso torna importante avaliar e planejar sua estratégia MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia MAM definindo o seguinte:

- **Tipos de aplicativos** - Liste os diferentes tipos de aplicativos aos quais você planeja oferecer suporte e categorizar, como aplicativos públicos, nativos, do Worx, da Web, internos, de ISV e

© 1999-2019 Citrix Systems, Inc. All rights reserved.

assim por diante. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajudará no alinhamento de diferentes configurações do XenMobile necessárias para cada tipo de aplicativo. Por exemplo, determinados aplicativos podem não se qualificar para o agrupamento ou alguns aplicativos podem exigir o uso do SDK do aplicativo Worx para ativar APIs especiais para interação com outros aplicativos.

- **Requisitos de rede** - você precisa configurar 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 VPN; alguns aplicativos podem exigir acesso à Internet para rotear o acesso por meio da DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você precisa definir várias configurações de acordo. A definição de requisitos de rede por aplicativo ajuda a finalizar suas decisões de arquitetura desde o início, o que simplificará o processo geral de implementação.
- **Requisitos de segurança** - a definição dos requisitos de segurança que se aplicam a aplicativos individuais ou a todos os aplicativos é fundamental para garantir que você crie as configurações corretas ao instalar o XenMobile Server. Embora as configurações, como as políticas MDX, se apliquem a aplicativos individuais, as configurações de sessão e autenticação se aplicam a todos os aplicativos e alguns aplicativos podem ter requisitos específicos de criptografia, contêiner, preparação, criptografia, autenticação, geocerca, senha ou compartilhamento de dados precisa delinear com antecedência para simplificar sua implantação. Para obter detalhes sobre segurança no XenMobile, consulte Segurança e experiência do usuário.
- **Requisitos de implantação** - convém usar uma implantação baseada em políticas para permitir que apenas usuários em conformidade baixem os aplicativos publicados. Por exemplo, você pode querer que determinados aplicativos exijam que a criptografia do dispositivo esteja ativada ou que o dispositivo seja gerenciado ou que o dispositivo atenda a uma versão mínima do sistema operacional. Você também pode querer que determinados aplicativos estejam disponíveis apenas para usuários corporativos. Você precisa descrever esses requisitos com antecedência para poder configurar as regras ou ações de implantação apropriadas.
- **Requisitos de licenciamento** - você deve registrar os requisitos de licenciamento relacionados ao aplicativo. Essas notas ajudarão você a gerenciar o uso da licença com eficiência e a decidir se você precisa configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo para iOS, independentemente de ser um aplicativo gratuito ou pago, a Apple aplicará os requisitos de licenciamento ao aplicativo, fazendo com que os usuários entrem em sua conta do iTunes. Você pode se registrar no Apple VPP para distribuir e gerenciar esses aplicativos via XenMobile. O VPP permite que os usuários baixem os aplicativos sem precisar entrar em suas contas do iTunes. Além disso, ferramentas como o Samsung SAFE e o Samsung KNOX têm requisitos especiais de licenciamento, que você precisa concluir antes de implantar esses recursos.
- **Requisitos da lista negra/lista branca** - Haverá aplicativos que você não deseja que os usuários instalem ou usem. A criação de uma lista negra definirá um evento fora de conformidade. Você

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pode configurar políticas para acionar no caso de tal coisa acontecer. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode se enquadrar na lista negra por um motivo ou outro. Se esse for o 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. Isso pode entrar em conflito com sua estratégia de lista negra.

Caso de uso

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

Aplicativos móveis de produtividade: Aplicativos para iOS e Android fornecidos pela Citrix. Para obter detalhes, consulte aplicativos móveis de produtividade.

Citrix Secure Hub: cliente usado por todos os dispositivos móveis para se comunicar com o XenMobile. A TI envia parâmetros de segurança, configurações e aplicativos móveis para dispositivos móveis via Secure Hub. Dispositivos Android e iOS se registram no XenMobile através do Secure Hub.

Citrix Receiver: aplicativo móvel que permite aos usuários abrir aplicativos host do XenApp em dispositivos móveis.

GoToMeeting: um cliente de reunião on-line, compartilhamento de área de trabalho e videoconferência que permite que os usuários se encontrem com outros usuários de computador, clientes, consumidores ou colegas pela Internet em tempo real.

SalesForce1: o Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúnam todos os aplicativos Chatter, CRM, personalizados e 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, listas de pacientes, agendamentos e mensagens.

Haiku: aplicativo móvel para telefones iPhone e Android.

Canto: aplicativo móvel para o iPad

Rover: aplicativos móveis para iPhone e iPad.

HDX: esses aplicativos são entregues via Citrix XenApp.

- **Epic Hyperspace:** aplicativo cliente Epic para gerenciamento eletrônico de prontuários médicos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ISV:

- **Vocera:** aplicativo móvel de mensagens e IP de voz compatível com HIPAA que amplia os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, através de smartphones iPhone e Android.

Apps 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 da web internos:

- **PatientRounding:** aplicativo da Web usado para registrar informações médicas do paciente por diferentes departamentos.
- **Outlook Web Access:** permite o acesso de email por meio de um navegador da 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	Preparação de MDX	iOS	Android
Secure Mail	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Web	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Notes	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
ShareFile	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo público	N/D	Sim	Sim
Citrix Receiver	Aplicativo público	N/D	Sim	Sim
GoToMeeting	Aplicativo público	N/D	Sim	Sim

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SalesForce1	Aplicativo público	N/D	Sim	Sim
RSA SecurID	Aplicativo público	N/D	Sim	Sim
Epic Haiku	Aplicativo público	N/D	Sim	Sim
Epic Canto	Aplicativo público	N/D	Sim	Não
Epic Rover	Aplicativo público	N/D	Sim	Não
Epic Hyperspace	Aplicativo HDX	N/D	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo interno	Sim	Sim	Sim
PatientRounding	Aplicativo Web	N/D	Sim	Sim
Outlook Web Access	Aplicativo Web	N/D	Sim	Sim
SharePoint	Aplicativo Web	N/D	Sim	Sim

A tabela a seguir lista os requisitos específicos que você pode consultar para configurar as políticas do MAM no XenMobile.

Nome do aplicativo	**VPN necessária**	**Interação (com aplicativos fora do contêiner)**	**Interação (de aplicativos fora do contêiner)**	**Criptografia de dispositivo**	**Filtragem Proxy**	**Licenciamento**	**Cerca geográfica**	**Worx App SDK**	**Versão mínima do sistema operacional**
Secure Mail	S	Permitid seleti-va-mente	Permitid	Desnece	Obrigatć	N/D	Seletivar Obri-gatório	N/D	Imposto

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome do aplicativo	VPN necessária	Interação (com aplicativos fora do contêiner)	Interação (de aplicativos fora do contêiner)	Criptografia de dispositivo	Filtragem	Proxy	Licenciamento	Cerca geográfica	Worx App SDK	Versão mínima do sistema operacional
Secure Web	S	Permitido	Permitido	Desnecessário	Obrigatório	N/D	Desnecessário	N/D		Imposto
Secure Notes	S	Permitid	Permitid	Desnece	Obrigatć	N/D	Desnece	N/D		Imposto
ShareFile	S	Permitido	Permitido	Desnecessário	Obrigatório	N/D	Desnecessário	N/D		Imposto
Secure Hub	S	N/D	N/D	N/D	Desnece	VPP	Desnece	N/D		Não aplicado
Citrix Receiver	S	N/D	N/D	N/D	Desnecessário	VPP	Desnecessário	N/D		Não aplicado
GoToMe	N	N/D	N/D	N/D	Desnece	VPP	Desnece	N/D		Não aplicado
SalesForce	N	N/D	N/D	N/D	Desnecessário	VPP	Desnecessário	N/D		Não aplicado
RSA SecurID	N	N/D	N/D	N/D	Desnece	VPP	Desnece	N/D		Não aplicado
Epic Haiku	S	N/D	N/D	N/D	Desnecessário	VPP	Desnecessário	N/D		Não aplicado
Epic Canto	S	N/D	N/D	N/D	Desnece	VPP	Desnece	N/D		Não aplicado
Epic Rover	S	N/D	N/D	N/D	Desnecessário	VPP	Desnecessário	N/D		Não aplicado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nome do aplicativo	VPN necessária	Interação (com aplicativos fora do contêiner)	Interação (de aplicativos fora do contêiner)	Criptografia de dispositivo	Filtragem Proxy	Licenciamento	Cerca geográfica	Worx App SDK	Versão mínima do sistema operacional
Epic Hyperspace	S	N/D	N/D	N/D	Desnece	N/D	Desnece	N/D	Não aplicado
Vocera	S	Não permitido	Não permitido	Desnecessário	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto
HCMail	S	Não permitido	Não permitido	Obrigatć	Obrigatć	N/D	Obrigatć	Obrigatć	Imposto
PatientRoutending	S	N/D	N/D	Obrigatório	Obrigatório	N/D	Desnecessário	N/D	Não aplicado
Outlook Web Access	S	N/D	N/D	Desnece	Obrigatć	N/D	Desnece	N/D	Não aplicado
SharePoint	S	N/D	N/D	Desnecessário	Obrigatório	N/D	Desnecessário	N/D	Não aplicado

Comunidades do usuário

August 31, 2018

Cada organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários executam tarefas e funções de escritório diferentes usando vários recursos fornecidos por meio dos dispositivos móveis dos usuários. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis fornecidos por você. Ou, os usuários podem usar dispositivos móveis pessoais, o que permite que eles acessem ferramentas que estão sujeitas a determinadas regras de conformidade de segurança.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Com mais comunidades de usuários usando dispositivos móveis, o gerenciamento de mobilidade empresarial (EMM) se torna crítico para evitar o vazamento de dados e impor restrições de segurança organizacional. Para um gerenciamento eficiente e sofisticado de dispositivos móveis, 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.

A categorização de comunidades de usuários pode incluir o uso dos seguintes componentes:

- Grupos e Unidades Organizacionais (OUs) do Active Directory

  Os 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 a recursos do XenMobile permitidos anteriormente.

- Usuários locais e grupos do XenMobile

  Para usuários que não possuem uma conta no Active Directory, você pode criá-los como usuários locais do XenMobile. Você pode adicionar usuários locais a grupos de entrega e provisionar recursos a eles da mesma maneira que aos usuários do Active Directory.

- Grupos de entrega do XenMobile

  Se vários grupos de usuários com diferentes níveis de permissão consumirem um único aplicativo, seria indicado 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

  O grupo de entrega para mapeamentos de grupos do Active Directory pode ser um para um ou um para muitos. Atribuir políticas e aplicativos de base a um mapeamento de grupo de entrega de um para muitos. Atribuir políticas e aplicativos específicos a função a mapeamentos de grupo de entrega um para um.

- Mapeamento de Grupo de entrega e Recursos dos aplicativos

  Atribuir aplicativos específicos a cada grupo de entrega.

- Mapeamento de Grupo de entrega e Recursos do MDM

  Atribua aplicativos e recursos de gerenciamento de dispositivos específicos a cada grupo de entrega. Por exemplo, configure um grupo de entrega com qualquer destas combinações: tipos de aplicativos (públicos, HDX e assim por diante), aplicativos específicos por tipo de aplicativo, e recursos, como políticas de dispositivos e ações automatizadas.

O exemplo a seguir ilustra como as comunidades de usuários de uma organização de assistência médica são classificadas para o EMM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Caso de uso

Neste exemplo, esta organização de assistência médica fornece recursos de tecnologia e acesso a vários usuários, incluindo funcionários e voluntários da rede e afiliados. A organização optou por implantar a solução EMM apenas para usuários não executivos.

Você pode dividir os cargos e funções dos usuários dessa organização em subgrupos, incluindo: clínico, não clínico e contratados. Um grupo selecionado de usuários recebe dispositivos móveis corporativos, enquanto outros podem acessar recursos limitados da empresa a partir de seus dispositivos pessoais (BYOD, traga seu próprio dispositivo). Para impor o nível apropriado de restrições de segurança e impedir o vazamento de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado. Além disso, os usuários só podem registrar um único dispositivo.

Aa seções a seguir fornecem uma visão geral dos cargos e funções de cada subgrupo:

Clínico

- Enfermeiros
- Médicos (doutores, cirurgiões e outros)
- Especialistas (nutricionistas, flebotomistas, anestesistas, radiologistas, cardiologistas, oncologistas e outros)
- Médicos externos (médicos não empregados e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (trabalhadores de escritório e móveis realizando serviços médicos em visitas domiciliares ao paciente)
- Especialista em pesquisa (trabalhadores do conhecimento e usuários avançados em seis institutos de pesquisa que realizam pesquisas clínicas para encontrar respostas para problemas clínicos)
- Educação e Formação (enfermeiros, médicos e especialistas em educação e formação)

Não clínico

- Serviços compartilhados (funcionários de escritório executando várias funções de back-office, incluindo: RH, folha de pagamento, contas a pagar, serviço de cadeia de fornecimento e outros)
- Serviços Médicos (funcionários do escritório realizando várias soluções de gestão de saúde, serviços administrativos e processos de negócios para fornecedores, incluindo: Serviços Administrativos, Analytics e Business Intelligence, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e outros)
- Serviços de Suporte (trabalhadores de escritório realizando várias funções não clínicas, incluindo Administração de Benefícios, Integração Clínica, Comunicações, Gerenciamento de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Compensação e Desempenho, Serviços de Instalações e Propriedade, Sistemas de Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos e outros)
- Programas filantrópicos (funcionários de escritório e móveis que realizam várias funções de apoio a programas filantrópicos)

Contratados

- Parceiros fabricantes e fornecedores (conectados no local e remotamente via VPN site-to-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.

Grupos e Unidades Organizacionais (OUs) 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 Formação
- OU = Não clínico; Grupos =
  - XM-Serviços Compartilhados
  - XM-Serviços Médicos
  - XM-Serviços de Suporte
  - XM-Programas Filantrópicos

Usuários locais e grupos do XenMobile

ForGroup= Contratados, Usuários =

- Vendor1
- Vendor2
- Vendor3
- … Vendor10

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Formação
- Não clínicos-Serviços Compartilhados
- Não clínicos-Serviços Médicos
- Não clínicos-Serviços de Suporte
- Não clínicos-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 Formação	Clínico-Educação e Formação
XM-Serviços Compartilhados	Não clínicos-Serviços Compartilhados
XM-Serviços Médicos	Não clínicos-Serviços Médicos
XM-Serviços de Suporte	Não clínicos-Serviços de Suporte
XM-Programas Filantrópicos	Não clínicos-Programas Filantrópicos

Mapeamento de Grupo de entrega e Recursos dos aplicativos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Secure Mail	Secure Web	Secure Notes	ShareFil	Citrix Re-ceiver	SalesFo	RSA Se-curID	EpicCar Haiku	Epic Hy-per-space
Clínico-Enfermeiros	X	X	X	X					
Clínico-Médicos									
Clínico-Especialistas									
Clínico-Médicos Exter-nos	X		X	X					
Clínico-Serviços de Saúde Domi-ciliar	X		X	X					
Clínico-Especial em Pesquisa	X		X	X					
Clínico-Educação e For-mação								X	X
Não clínicos-Serviços Com-partil-hados								X	X

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Não clínicos-Serviços Médicos							X	X
Não clínicos-Serviços de Suporte	X		X	X			X	X
Não clínicos-Programas Filantrópicos	X		X	X			X	X
Contrata	X		X	X	X	X	X	X

Mapeamento de Grupo de entrega e Recursos do MDM

	MDM: Política de código secreto	MDM: Restrições de dispositivos	MDM: Ações automatizadas	MDM: Política de WiFi
Clínico-Enfermeiros				X
Clínico-Médicos		X		
Clínico-Especialistas				
Clínico-Médicos Externos				
Clínico-Serviços de Saúde Domiciliar				

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Clínico-Especialista em Pesquisa	
Clínico-Educação e Formação	
Não clínicos-Serviços Compartilhados	
Não clínicos-Serviços Médicos	
Não clínicos-Serviços de Suporte	
Não clínicos-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 desabilitar esse grupo de entrega, todos os usuários do Active Directory terão direitos para 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 esteja mapeado no XenMobile, esse usuário não poderá se registrar. Da mesma forma, se um usuário for membro de vários grupos, o XenMobile categoriza o usuário apenas como estando nos grupos mapeados para o XenMobile.
- Para tornar o registro no MDM obrigatório, defina a opção de **Registro Obrigatório** como **True** em **Propriedades do Servidor** no console 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Cuidado:**
>
> Antes de executar esta ação, crie um backup do XenMobile e do banco de dados.

Sobre a Propriedade de 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 da empresa e dispositivos de propriedade do usuário, também conhecidos como BYOD (traga o seu próprio dispositivo). Você pode controlar como os dispositivos BYOD se conectam à sua rede em dois locais no console XenMobile: nas Regras de implantação e nas propriedades do XenMobile Server na página **Configurações**. Para obter detalhes sobre 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 de BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que eles possam acessar os aplicativos. Ou você pode conceder aos usuários acesso a aplicativos corporativos sem precisar 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 não terá acesso aos aplicativos. Considere configurar o **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança, além de uma experiência de usuário positiva durante o registro.

Se você deixar o **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários poderão recusar o registro. No entanto, eles podem acessar aplicativos em seus dispositivos através da XenMobile Store. Considere configurar **wsapi.mdm.required.flag** como **false** em ambientes nos quais as restrições de privacidade, legais ou regulamentares não exigem gerenciamento de dispositivos, 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 apagamento seletivo ou completo, você controla o acesso aos aplicativos por meio de políticas de aplicativos. Algumas configurações de políticas exigem que o dispositivo verifique o XenMobile Server rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Estratégia de email

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O acesso seguro ao email de dispositivos móveis é um dos principais impulsionadores da iniciativa de gerenciamento de mobilidade de qualquer organização. Decidir sobre a estratégia de e-mail adequada é muitas vezes um componente-chave de qualquer design do XenMobile. O XenMobile oferece várias opções para acomodar diferentes casos de uso, com base na segurança, na experiência do usuário e nos requisitos de 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 correio.

Escolhendo seus clientes de e-mail

A seleção de clientes geralmente está no topo da lista do design geral da estratégia de email. Você pode escolher entre vários clientes: o Citrix Secure Mail, o correio nativo incluído em um determinado sistema operacional de plataforma móvel ou outros clientes de terceiros disponíveis nas lojas de aplicativos públicas. Dependendo de suas necessidades, você pode possivelmente oferecer suporte às comunidades de usuários com um único cliente (padrão) ou talvez seja necessário usar uma combinação de clientes.

A tabela a seguir descreve as considerações de design para as diferentes opções de cliente disponíveis:

Tópico	Secure Mail	Nativo (por exemplo, o iOS Mail)	Email de terceiros (por exemplo, TouchDown)
XenMobile Edition mínimo	Advanced	MDM	MDM
Configuração	Perfis de conta do Exchange configurados por meio de uma política do MDX.	Perfis de conta do Exchange configurados por meio de uma política do MDM. O suporte para Android está limitado a: SAFE/KNOX, HTC e Android for Work. Todos os outros clientes são considerados clientes de terceiros.	Geralmente requer configuração manual pelo usuário. Configuração de perfis de conta do Exchange por meio de uma política de MDM somente para TouchDown.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Segurança	Seguro por design, proporcionando a mais alta segurança. Usa políticas de MDX com níveis de criptografia de dados adicionais. O Secure Mail é um aplicativo totalmente gerenciado por meio de uma política de MDX. Camada adicional de autenticação com o Citrix PIN.	Com base no conjunto de recursos do fornecedor/aplicativo. Fornece maior segurança. Usa configurações de criptografia de dispositivo (sem segurança por meio de políticas de MDX). Depende da autenticação no nível do dispositivo para acesso ao aplicativo.	Com base no conjunto de recursos do fornecedor/aplicativo. Fornece alta segurança.
Integração	Permite a interação com aplicativos gerenciados (MDX) por padrão. Abra URLs da Web com o Citrix Secure Web. Salve arquivos no e anexe arquivos do ShareFile. Entrar e digitar diretamente no GoToMeeting.	Só é possível interagir com outros aplicativos não gerenciados (não MDX) por padrão.	Só é possível interagir com outros aplicativos não gerenciados (não MDX) por padrão.
Implantação/licenciamento	Você pode enviar o Secure Mail pelo MDM diretamente de lojas de aplicativos públicas. Incluído no licenciamento XenMobile Advanced e Enterprise.	Aplicativo cliente incluído no sistema operacional da plataforma. Nenhum requisito de licenciamento adicional.	Pode enviar por meio do MDM, como um aplicativo corporativo ou diretamente de lojas de aplicativos públicas. Modelo de licenciamento associado/custos com base no fornecedor do aplicativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Suporte	Único suporte de fornecedor para o cliente e solução de EMM (Citrix). Informações de contato do suporte incorporado nos recursos de registro de depuração do Secure Hub/aplicativo. Um cliente para suporte.	Suporte definido pelo fornecedor (Apple/Google). Pode ser necessário oferecer suporte a diferentes clientes com base na plataforma do dispositivo.	Suporte definido pelo fornecedor. Um cliente para suportar, pressupondo-se que o cliente de terceiros é suportado em todas as plataformas de dispositivos gerenciados.

Fluxo de tráfego de email e considerações de filtragem

Esta seção discute os três principais cenários e considerações de design relacionadas ao fluxo de tráfego de email (ActiveSync) no contexto do XenMobile.

Cenário 1: Exchange exposto

Ambientes que suportam clientes externos geralmente possuem serviços do Exchange ActiveSync expostos à Internet. Os clientes do Mobile ActiveSync se conectam por meio desse caminho externo por meio de um proxy reverso (por exemplo, NetScaler) ou por meio de um servidor de borda. Essa opção é necessária para o uso de clientes de email nativos ou de terceiros, tornando esses clientes a escolha popular para esse cenário. Embora não seja uma prática comum, você também pode usar o cliente do Secure Mail nesse cenário. Ao fazer isso, você se beneficia dos recursos de segurança oferecidos pelo uso de políticas de MDX e pelo gerenciamento do aplicativo.

Cenário 2: Encapsulado via NetScaler (micro VPN e STA)

Esse cenário é o padrão ao usar o cliente do Secure Mail, devido aos seus recursos de micro VPN. Nesse caso, o cliente do Secure Mail estabelece uma conexão segura com o ActiveSync via NetScaler Gateway. Em essência, você pode considerar o Secure Mail como o cliente que se conecta diretamente ao ActiveSync pela rede interna. Os clientes da Citrix costumam padronizar o Secure Mail como o cliente móvel do ActiveSync preferido. Essa decisão é parte de uma iniciativa para evitar a exposição

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dos serviços do ActiveSync à Internet em um Exchange Server exposto, conforme descrito no primeiro cenário.

Somente aplicativos gerenciados (MDX preparado) podem usar a função micro VPN. Portanto, esse cenário não se aplica a clientes nativos. Mesmo que seja possível preparar clientes de terceiros com o MDX Toolkit, essa prática não é comum. O uso de clientes VPN em nível de dispositivo para permitir acesso com túnel para clientes nativos ou de terceiros provou ser uma solução incômoda e não viável.

Cenário 3: Serviços do Hosted Exchange na nuvem

Serviços do Hosted Exchange na nuvem, como o Microsoft Office 365, estão se tornando mais populares. No contexto do XenMobile, esse cenário pode ser tratado da mesma maneira que o primeiro cenário, porque o serviço ActiveSync também é exposto à Internet. Nesse caso, os requisitos do provedor de serviços de nuvem determinam as escolhas do cliente. As opções geralmente incluem suporte para a maioria dos clientes do ActiveSync, como o Secure Mail e outros clientes nativos ou de terceiros.

O XenMobile pode agregar valor em três áreas neste cenário:

- Preparação do cliente com políticas de MDX e gerenciamento de aplicativos com o Secure Mail
- Configuração do cliente com o uso de uma política do MDM em clientes suportados (nativos, como o TouchDown)
- Opções de filtragem do ActiveSync com o uso do conector de Endpoint Management para Exchange ActiveSync

Considerações sobre filtragem de tráfego de email

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: conector Citrix Gateway para Exchange ActiveSync e conector de Endpoint Management para Exchange ActiveSync.

Conector Citrix Gateway para Exchange ActiveSync

O uso do conector Citrix Gateway para Exchange ActiveSync fornece filtragem do ActiveSync no perímetro, usando o NetScaler como um proxy para o tráfego do ActiveSync. Como resultado, o componente de filtragem fica no caminho do fluxo de tráfego de mensagens, interceptando mensagens à medida que elas entram ou saem do ambiente. O conector Citrix Gateway para Exchange ActiveSync atua como intermediário entre o NetScaler e o XenMobile Server. Quando um dispositivo se comunica com o Exchange através do servidor virtual ActiveSync no NetScaler, o NetScaler executa uma chamada HTTP para o serviço do conector para Exchange ActiveSync. Esse serviço verifica o status do dispositivo com o XenMobile. Com base no status do dispositivo, o conector para Exchange

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ActiveSync responde ao NetScaler para permitir ou negar a conexão. Você também pode configurar regras estáticas para filtrar o acesso com base no usuário, agente e tipo de dispositivo ou ID.

Essa configuração permite que os serviços do Exchange ActiveSync sejam expostos à Internet com uma camada adicional de segurança para impedir o acesso não autorizado. Considerações de design incluem o seguinte:

- Windows Server: o componente conector para Exchange ActiveSync requer um Windows Server.
- Conjunto de regras de filtragem: o conector do Exchange ActiveSync foi projetado para filtragem com base no estado e nas informações do dispositivo, em vez de se basear nas informações do usuário. Embora você possa configurar regras estáticas para filtrar por ID do usuário, não há opções para filtragem com base na associação do grupo do Active Directory, por exemplo. Se houver um requisito para a filtragem de grupos do Active Directory, você poderá usar o conector Endpoint Management para Exchange ActiveSync.
- Escalabilidade do NetScaler: dado o requisito de fazer o proxy do tráfego do ActiveSync via NetScaler: o dimensionamento adequado da instância do NetScaler é crítico para suportar a carga de trabalho adicional de todas as conexões SSL do ActiveSync.
- Cache Integrado do NetScaler: a configuração do conector para Exchange ActiveSync no NetScaler usa a função Cache Integrado para armazenar em cache as respostas do conector para Exchange ActiveSync. Como resultado dessa configuração, o NetScaler não precisa emitir uma solicitação ao conector Citrix Gateway para Exchange ActiveSync para cada transação do ActiveSync em uma determinada sessão. Essa configuração também é crítica para um desempenho e escala adequados. O Cache Integrado está disponível com o NetScaler Platinum Edition, ou você pode licenciar o recurso separadamente para Enterprise Editions.
- Políticas de filtragem personalizadas: pode ser necessário criar políticas personalizadas do NetScaler para restringir determinados clientes do ActiveSync fora dos clientes móveis nativos padrão. Essa configuração requer conhecimento sobre solicitações HTTP do ActiveSync e criação de políticas de resposta do NetScaler.
- 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 NetScaler Gateway. Se for necessário suporte para clientes nativos e de terceiros (com o conector para Exchange ActiveSync) e Secure Mail, a Citrix recomenda que o tráfego do Secure Mail não flua pelo servidor virtual NetScaler usado para o conector para Exchange ActiveSync. Você pode realizar esse fluxo de tráfego via DNS e evitar que a política do Exchange ActiveSync afete os clientes Secure Mail.

Para obter um diagrama do conector Citrix Gateway para Exchange ActiveSync em uma implantação do XenMobile, consulte Arquitetura de referência para implantações locais.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conector de Endpoint Management para Exchange ActiveSync

O conector de Endpoint Management para Exchange ActiveSync é um componente do XenMobile que fornece filtragem do ActiveSync no nível de serviço do Exchange. Como resultado, a filtragem só ocorre quando o email chega ao serviço do Exchange, e não quando entra no ambiente do XenMobile. O Mail Manager usa o PowerShell para consultar o Exchange ActiveSync em busca de informações sobre parceria de dispositivos e controle de acesso por meio de ações de quarentena de dispositivos. Essas ações colocam e retiram os dispositivos da quarentena com base nos critérios de regra do conector de Endpoint Management para Exchange ActiveSync. Semelhante ao conector Citrix Gateway para Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync verifica o status do dispositivo no 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, na versão do agente e na associação do grupo do Active Directory.

Esta solução não requer o uso do NetScaler. Você pode implantar o conector de Endpoint Management para Exchange ActiveSync sem alterar o roteamento do tráfego do ActiveSync existente. Considerações de design incluem:

- Windows Server: o componente conector de Endpoint Management ára Exchange ActiveSync requer a implantação do Windows Server.
- Conjunto de regras de filtragem: assim como o conector Citrix Gateway para Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync inclui regras de filtragem para avaliar o estado do dispositivo. Além disso, o conector de Endpoint Management para Exchange ActiveSync também oferece suporte a regras estáticas para filtrar com base na associação do grupo do Active Directory.
- Integração com o Exchange: o conector de Endpoint Management para Exchange ActiveSync requer acesso direto ao servidor de acesso para cliente (CAS) do Exchange que hospeda a função do ActiveSync e controla as ações de quarentena do dispositivo. Esse requisito pode representar um desafio, dependendo da arquitetura do ambiente e da postura de segurança. É fundamental que você avalie essa exigência técnica antecipadamente.
- Outros clientes do ActiveSync: como o conector de Endpoint Management para Exchange ActiveSync está sendo filtrado no nível de serviço do ActiveSync, considere outros clientes do ActiveSync fora do ambiente do XenMobile. Você pode configurar as regras estáticas do conector de Endpoint Management para Exchange ActiveSync para evitar impacto não intencional em outros clientes do ActiveSync.
- Funções estendidas do Exchange: por meio da integração direta com o Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync permite que o XenMobile execute um apagamento do Exchange ActiveSync em um dispositivo móvel. O conector de Endpoint Management para Exchange ActiveSync também permite que o XenMobile acesse informações sobre dispositivos Blackberry e realize outras operações de controle.

Para obter um diagrama do conector de Endpoint Management para Exchange ActiveSync em uma

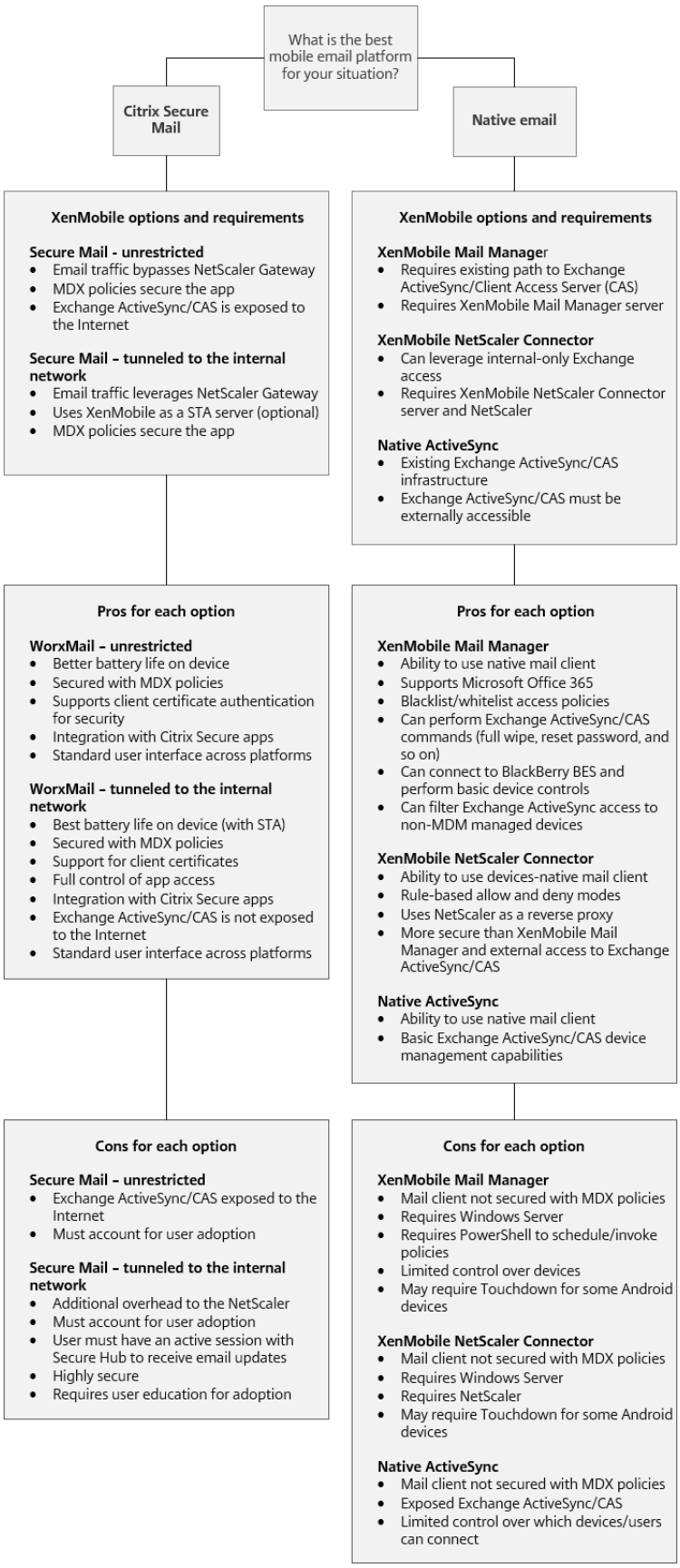
© 1999-2019 Citrix Systems, Inc. All rights reserved.

implantação do XenMobile, consulte Arquitetura de referência para implantações locais.

Árvore de decisão da plataforma de e-mail

A figura a seguir ajuda a distinguir os prós e contras entre o uso de soluções de email nativo ou Secure Mail na sua implantação do XenMobile. Cada escolha permite opções e requisitos associados ao XenMobile para habilitar o acesso ao servidor, rede e banco de dados. Os prós e contras incluem detalhes sobre considerações de segurança, política e interface do usuário.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Integração do XenMobile

April 15, 2019

Este artigo aborda o que considerar ao planejar como o XenMobile deve se integrar à sua rede e soluções existentes. Por exemplo, se você já estiver usando o NetScaler para XenApp e XenDesktop:

- Você deve usar a instância existente do NetScaler ou uma nova instância dedicada?
- Você deseja integrar com o XenMobile os aplicativos HDX que são publicados usando o StoreFront?
- Você planeja usar o ShareFile com o XenMobile?
- Você tem uma solução de controle de acesso da rede que deseja integrar ao XenMobile?
- Você implementa proxies da web para todo o tráfego de saída da sua rede?

NetScaler e NetScaler Gateway

O NetScaler Gateway é obrigatório nos modos XenMobile ENT e MAM. O NetScaler Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator. O balanceamento de carga do NetScaler 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 rede DMZ ou interna (e, portanto, o tráfego flui dos dispositivos para o NetScaler para o XenMobile).

Você pode usar instâncias existentes do NetScaler ou configurar instâncias novas para o XenMobile. As seções a seguir observam as vantagens e desvantagens de usar instâncias NetScaler dedicadas novas ou existentes.

NetScaler MPX compartilhado com um VIP NetScaler Gateway criado para o XenMobile

Vantagens:

- Usa uma instância comum do NetScaler para todas as conexões remotas do Citrix: XenApp, VPN completa e VPN sem cliente.
- Usa as configurações existentes do NetScaler, como para autenticação de certificado e para acessar serviços como DNS, LDAP e NTP.
- Usa uma única licença de plataforma NetScaler.

Desvantagens:

- É mais difícil planejar a escala quando você lida com dois casos de uso muito diferentes no mesmo NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Às vezes você precisa de uma versão específica do NetScaler para um caso de uso do XenApp. Essa mesma versão pode ter problemas conhecidos no XenMobile. Ou o XenMobile pode ter problemas conhecidos na versão do NetScaler.
- Se existir um NetScaler Gateway, não será possível executar o assistente NetScaler for XenMobile uma segunda vez para criar a configuração do NetScaler para o XenMobile.
- Exceto quando licenças Platinum são usadas para o NetScaler Gateway 11.1 ou posterior: as licenças de acesso de usuário instaladas no NetScaler e necessárias para conectividade VPN são agrupadas. Como essas licenças estão disponíveis para todos os servidores virtuais NetScaler, outros serviços além do XenMobile podem potencialmente consumi-las.

Instância do NetScaler VPX/MPX dedicada

Vantagens:

A Citrix recomenda o uso de uma instância dedicada do NetScaler.

- Mais fácil de planejar a escala e separa o tráfego do XenMobile de uma instância do NetScaler que pode já estar com restrição de recursos.
- Evita problemas quando o XenMobile e o XenApp precisam de versões diferentes do software NetScaler. A recomendação geralmente é usar a última versão e compilação compatíveis do NetScaler for XenMobile.
- Permite a configuração do XenMobile do NetScaler através do assistente interno do NetScaler for XenMobile.
- Separação virtual e física de serviços.
- Exceto quando as licenças Platinum são usadas para o NetScaler Gateway 11.1 ou posterior: as licenças de acesso de usuário necessárias para o XenMobile só estão disponíveis para os serviços XenMobile no NetScaler.

Desvantagens:

- Requer configuração de serviços extras no NetScaler para suportar a configuração do XenMobile.
- Requer outra licença de plataforma NetScaler. Licencie cada instância do NetScaler para o NetScaler Gateway.

Para obter informações sobre o que considerar ao integrar o NetScaler e o NetScaler Gateway com cada modo de XenMobile Server, consulte Integração com NetScaler e NetScaler Gateway.

StoreFront

Se você tiver um ambiente Citrix XenApp e XenDesktop, poderá integrar aplicativos HDX ao XenMobile usando o StoreFront. Quando você integra aplicativos HDX ao XenMobile:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Os aplicativos ficam disponíveis para usuários registrados no XenMobile.
- Os aplicativos são exibidos na XenMobile Store juntamente 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 começam a usar o Receiver.

StoreFront tem uma limitação de um site de serviços por instância de StoreFront. Suponha que você tenha várias lojas de aplicativos e queira segmentá-las de outro uso de produção. Nesse caso, a Citrix geralmente recomenda que você considere usar uma nova instância do StoreFront e site de serviço para o XenMobile.

As considerações incluem:

- Existem requisitos de autenticação diferentes para o StoreFront? O site de serviços StoreFront requer credenciais do Active Directory para logon. Os clientes que usam somente a autenticação baseada em certificado não podem enumerar aplicativos por meio do XenMobile usando o mesmo NetScaler 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 StoreFront separado ou combinado para Citrix Receiver e aplicativos móveis de produtividade.

Integrar sua instância StoreFront existente com o XenMobile Server

Vantagens:

- Mesma loja de aplicativos: nenhuma configuração adicional do StoreFront é necessária para o XenMobile, supondo que você use o mesmo NetScaler VIP para acesso HDX. Suponha que você decida usar a mesma loja e queira direcionar o acesso do Citrix Receiver a um novo VIP NetScaler. Nesse caso, adicione a configuração apropriada do NetScaler Gateway ao StoreFront.
- Mesmo servidor StoreFront: usa a instalação e configuração do StoreFront existente.

Desvantagens:

- Mesma loja de aplicativos: qualquer reconfiguração do StoreFront para suportar cargas de trabalho do XenApp e XenDesktop pode afetar adversamente o XenMobile também.
- Mesmo servidor StoreFront: em ambientes grandes, considere a carga adicional do uso do XenMobile do PNAgent para enumeração e inicialização do aplicativo.

Use uma nova instância dedicada do StoreFront para integração com o XenMobile Server

Vantagens:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Nova loja de aplicativos: as alterações na configuração da loja StoreFront para o XenMobile não devem afetar as cargas de trabalho de XenApp e XenDesktop existentes.
- Novo servidor StoreFront: as alterações na configuração do servidor não devem afetar o fluxo de trabalho do XenApp e XenDesktop. Além disso, a carga fora do uso do XenMobile do PNAgent para enumeração e inicialização de aplicativos não deve afetar a escalabilidade.

Desvantagens:

- Nova loja de aplicativos: configuração da loja StoreFront.
- Novo servidor StoreFront: requer nova instalação e configuração do StoreFront.

Para obter mais informações, consulte XenApp e XenDesktop através do Citrix Secure Hub na documentação do XenMobile.

ShareFile

O ShareFile permite que os usuários acessem e sincronizem todos os seus dados de qualquer dispositivo. Com o ShareFile, os usuários podem compartilhar dados com segurança com pessoas dentro e fora da organização. Se você integrar o ShareFile ao XenMobile Advanced Edition ou Enterprise Edition, o XenMobile poderá fornecer ao ShareFile:

- Autenticação de logon único para usuários do XenMobile App.
- Provisionamento de conta de usuário baseado no Active Directory.
- Políticas abrangentes de controle de acesso.

Os usuários móveis podem se beneficiar do conjunto completo de recursos do ShareFile Enterprise.

Como alternativa, você pode configurar o XenMobile para integração apenas com StorageZone Connectors. Através de StorageZone Connectors, o ShareFile fornece acesso a:

- Documentos e pastas
- Compartilhamentos de arquivos de rede
- Nos sites do SharePoint: conjuntos de sites e bibliotecas de documentos.

Os compartilhamentos de arquivos conectados podem incluir as mesmas unidades iniciais de rede usadas nos ambientes Citrix XenDesktop e XenApp. Você usa o console XenMobile para configurar a integração com ShareFile Enterprise ou StorageZones Connectors. Para obter mais informações, consulte Uso do ShareFile com o XenMobile.

As seções a seguir observam as perguntas a serem feitas ao tomar decisões de design para o ShareFile.

Integrar com ShareFile Enterprise ou somente com StorageZone Connectors

Perguntas a serem feitas:

- Você precisa armazenar dados em StorageZones gerenciados pela Citrix?

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Você deseja fornecer aos usuários recursos de compartilhamento e sincronização de arquivos?
- Deseja permitir que os usuários acessem arquivos no site do ShareFile? Ou acessar conteúdo do Office 365 e conectores de nuvem pessoal de dispositivos móveis?

Decisão de design:

- Se a resposta a qualquer uma dessas perguntas for “sim”, integre-se ao ShareFile Enterprise.
- Uma integração apenas com o StorageZone Connectors fornece aos usuários do iOS acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos em rede. Nessa configuração, você não configura um subdomínio do ShareFile, provisiona usuários ao ShareFile ou hospeda dados do ShareFile. O uso do StorageZones Connectors com XenMobile está em conformidade com as restrições de segurança contra o vazamento de informações do usuário fora da rede corporativa.

Localização do servidor do ShareFile StorageZones Controller

Perguntas a serem feitas:

- Você precisa de armazenamento ou recursos locais, como StorageZone Connectors?
- Se estiver usando recursos locais do ShareFile, onde os ShareFile StorageZones Controllers ficarão na rede?

Decisão de design:

- Determine se deseja localizar os servidores do StorageZones Controller na nuvem do ShareFile, em seu sistema de armazenamento de locatário único no local ou no armazenamento na nuvem de terceiros suportados.
- StorageZones Controllers exigem certo acesso à Internet para se comunicar com o Citrix ShareFile Control Plane. Você pode se conectar de várias maneiras, incluindo acesso direto, configurações NAT/PAT ou configurações de proxy.

Conectores StorageZone

Perguntas a serem feitas:

- Quais são os caminhos de compartilhamento CIFS?
- Quais são os URLs do SharePoint?

Decisão de design:

- Determine se StorageZones Controllers locais precisam acessar esses localizações.
- Devido à comunicação do StorageZone Connector com recursos internos, como repositórios de arquivos, compartilhamentos CIFS e SharePoint, a Citrix recomenda que os StorageZones Controllers residam na rede interna por trás dos firewalls DMZ e protegidos pelo NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Integração SAML com XenMobile Enterprise

Perguntas a serem feitas:

- A autenticação do Active Directory é necessária para o ShareFile?
- O primeiro uso do aplicativo ShareFile para XenMobile requer SSO?
- Existe um IdP padrão no seu ambiente atual?
- Quantos domínios são necessários para usar SAML?
- Existem vários aliases de email para usuários do Active Directory?
- Há alguma migração de domínio do Active Directory em andamento ou agendada para breve?

Decisão de design:

Os ambientes do XenMobile Enterprise podem optar por usar SAML como o mecanismo de autenticação do ShareFile. As opções de autenticação são:

- Usar o XenMobile Server como o provedor de identidade (IdP) para SAML

Essa opção pode fornecer excelente experiência do usuário e automatizar a criação de conta de ShareFile, bem como habilitar recursos SSO do aplicativo móvel.

- O servidor XenMobile é aprimorado para este processo: ele não exige a sincronização do Active Directory.
- Use a ShareFile User Management Tool para provisionamento de usuários.
- Use um fornecedor de terceiros suportado como o IdP para SAML

Se você tiver um IdP existente e compatível e não precisar de recursos de SSO de aplicativos móveis, essa é a melhor opção para você. Essa opção também requer o uso da ShareFile User Management Tool para provisionamento de contas.

O uso de soluções de IdP de terceiros, como ADFS, também pode fornecer recursos de SSO no lado do cliente do Windows. Não deixe de avaliar casos de uso antes de escolher seu IdP SAML do ShareFile.

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 serem feitas:

- Qual aplicativo ShareFile Mobile você planeja usar (público, MDM, MDX)?

Decisão de design:

- Você distribui aplicativos móveis de produtividade a partir da Apple App Store e da Google Play Store. Com essa distribuição de lojas de aplicativos públicas, você obtém aplicativos preparados da página de downloads da Citrix.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Se a segurança estiver baixa e você não precisar de conteinerização, o aplicativo ShareFile público pode não ser adequado. Em um ambiente somente MDM, você pode entregar a versão MDM do aplicativo ShareFile usando o XenMobile no modo MDM.
- Para obter mais informações, consulte Aplicativos e Citrix ShareFile para XenMobile.

Segurança, políticas e controle de acesso

Perguntas a serem feitas:

- Quais restrições você precisa para usuários de computadores, web e dispositivos móveis?
- Quais configurações de controle de acesso padrão você deseja para os usuários?
- Qual política de retenção de arquivo você planeja usar?

Decisão de design:

- O ShareFile 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 do dispositivo ShareFile e políticas MDX controlam os mesmos recursos. Nesses casos, as políticas do XenMobile têm precedência, seguidas pelas configurações de segurança do dispositivo ShareFile. Exemplos: se você desativar aplicativos externos no ShareFile, mas ativá-los no XenMobile, os aplicativos externos serão desativados no ShareFile. Você pode configurar os aplicativos para que o XenMobile não exija um PIN/código secreto, mas o aplicativo ShareFile exija um PIN/código secreto.

StorageZones Padrões e Restritos StorageZones Restritos

Perguntas a serem feitas:

- Você precisa de StorageZones Restritos?

Decisão de design:

- Um StorageZone padrão é destinado a dados não confidenciais 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.
- Um StorageZone restrito protege os dados confidenciais: somente os usuários do 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 tiver acesso à Internet para en-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dereços IP 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 Ativar servidores proxy.

A tabela a seguir descreve as vantagens e desvantagens do proxy mais comum usado com o XenMobile.

Opção	Vantagens	Desvantagens
Usar um proxy HTTP(S)/SOCKS com o XenMobile Server.	Nos casos em que as políticas não permitem conexões de saída da 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 do APNs (iOS) ou do Google Cloud Messaging (Android) será interrompida. Como resultado, as notificações do dispositivo falham em todos os dispositivos iOS e Android.
Use um Proxy HTTP(S) com 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 Secure Web Internet retorne para a rede corporativa antes de ser enviado de volta à Internet. Se a sua conexão com a Internet restringir a navegação: essa configuração pode afetar o desempenho da navegação na Internet.

Sua configuração de perfil da sessão do NetScaler para túnel dividido afeta o tráfego da seguinte maneira.

Quando o Túnel dividido do NetScale está **desativado**:

- Se a política de **acesso à rede** MDX for **Com túnel para a rede interna:** todo o tráfego é forçado a usar o túnel micro VPN ou VPN sem cliente (cVPN) de volta ao NetScaler Gateway.
- Configure os perfis/políticas de tráfego do NetScaler para o servidor proxy e vincule-os ao VIP NetScaler Gateway.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Importante:
>
> Certifique-se de excluir o tráfego cVPN Secure Hub do proxy.

- Para obter mais informações, consulte Tráfego do XenMobile Secure Hub através do servidor proxy no modo Secure Browse.

Quando o **Túnel dividido do NetScale** está **ativado**:

- Quando os aplicativos são configurados com a política de **acesso à rede** MDX configurada como **Com túnel para a rede interna**: primeiro, os aplicativos tentam obter o recurso da Web diretamente. Se o recurso da Web não estiver publicamente disponível, esses aplicativos retornarão ao NetScaler Gateway.
- Configure políticas e perfis de tráfego do NetScaler para o servidor proxy. Em seguida, associe essas políticas e perfis ao VIP NetScaler Gateway.

> Importante:
>
> Certifique-se de excluir o tráfego cVPN Secure Hub do proxy.

Sua configuração do perfil de sessão do NetScaler para o **DNS Dividido** (em **Experiência do Cliente**) funciona de forma semelhante ao Túnel Dividido.

Com o **DNS Dividido** ativado e definido como **Ambos**:

- Primeiro, o cliente tenta resolver o FQDN localmente e, em seguida, retorna para o NetScaler para a resolução de DNS durante a falha.

Com o **DNS Dividido** definido como **Remoto**:

- A resolução de DNS ocorre apenas no NetScaler.

Com o **DNS Dividido** definido como **Local**:

- O cliente tenta resolver o FQDN localmente. O NetScaler não é usado para resolução de DNS.

Controle de acesso

As empresas agora podem gerenciar dispositivos móveis dentro e fora das redes. As soluções de Gerenciamento de Mobilidade Empresarial, como o XenMobile, são ótimas para fornecer segurança e controles para dispositivos móveis, independentemente da localização. No entanto, quando acoplado a uma solução NAC (Network Access Control), você pode adicionar QoS e um controle mais refinado aos dispositivos internos da sua rede. Essa combinação permite estender a avaliação de segurança do dispositivo XenMobile através da sua solução NAC. Sua solução NAC pode então usar a avaliação de segurança do XenMobile para facilitar e m,anipular decisões de autenticação. A Citrix validou a integração do NAC com o XenMobile para o Cisco Identity Services Engine (ISE) ou o ForeScout. A Citrix não garante integração para outras soluções NAC.

As vantagens de uma integração de solução NAC com o XenMobile incluem o seguinte:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Melhor segurança, conformidade e controle para todos os endpoints em uma rede corporativa.
- Uma solução NAC pode:
  - Detectar dispositivos no instante em que eles tentarem se conectar à sua rede.
  - Consultar o XenMobile para atributos do dispositivo.
  - Em seguida, usar essas informações para determinar se deve permitir, bloquear, limitar ou redirecionar esses dispositivos. Essas decisões dependem das políticas de segurança que você decide impor.
- Uma solução NAC fornece aos administradores de TI uma visão de dispositivos não gerenciados e não compatíveis.

Para obter uma descrição dos filtros de conformidade com NAC suportados pelo XenMobile, consulte Controle de Acesso da Rede.

Requisitos para vários locais

March 6, 2019

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais para alta disponibilidade e recuperação de desastres. Este artigo fornece uma visão geral dos modelos de alta disponibilidade e recuperação de desastres usados nas implantações do XenMobile.

Alta disponibilidade

- Para nós de cluster do XenMobile, o NetScaler manipula o balanceamento de carga.
- Nós do XenMobile Server operam em uma configuração ativa/ativa.
- Nós adicionais do XenMobile Server são adicionados a um cluster de alta disponibilidade, pois a capacidade é necessária. Um nó pode manipular até aproximadamente 8.500 dispositivos de usuário (consulte Escalabilidade e desempenho para obter detalhes adicionais).
- A Citrix recomenda a configuração de “n+1” XenMobile Servers: um servidor para cada 8.500 dispositivos de usuários e um servidor extra para redundância.
- A Citrix recomenda alta disponibilidade para todas as instâncias do NetScaler, sempre que possível, para permitir que as configurações sejam sincronizadas com um segundo NetScaler.
- O par padrão de alta disponibilidade do NetScaler opera em uma configuração ativa/passiva.

Uma implantação típica do XenMobile de alta disponibilidade geralmente inclui:

- Duas instâncias do NetScaler (VPX ou MPX). Se a plataforma NetScaler SDX for usada, a alta disponibilidade também deve ser considerada.
- Dois ou mais XenMobile Servers configurados com as mesmas configurações de banco de dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Recuperação de desastres

Você pode configurar o XenMobile para recuperação de desastre em dois datacenters com um datacenter ativo e um datacenter passivo. O NetScaler e o Global Server Load Balancing (GSLB) são usados para criar um caminho de dados ativo/ativo para que a experiência do usuário seja a de uma configuração ativa/ativa.

Para recuperação de desastres, uma implantação do XenMobile inclui:

- Dois data centers: cada um contém uma ou mais instâncias do NetScaler, XenMobile Servers e bancos de dados do SQL Server.
- Um servidor GSLB para direcionar o tráfego para os datacenters. O servidor GSLB é configurado para a URL de registro do XenMobile e para a URL do NetScaler Gateway que manipulam o tráfego para o site.
- Quando você usa o Assistente NetScaler para XenMobile para configurar o NetScaler Gateway, por padrão, o GSLB não está habilitado para resolver o tráfego para o servidor de registro do XenMobile e o tráfego para o NetScaler Gateway, na rota para o servidor de balanceamento de carga do MAM; como resultado, etapas adicionais são necessárias. Para obter mais informações sobre como preparar e implementar essas etapas, consulte Recuperação de desastres.
- SQL Servers em cluster de grupos de disponibilidade Always On.
- A latência entre os XenMobile Servers e o SQL Server deve ser menor que 5 ms.

> Nota:
>
> Os métodos de recuperação de desastres descritos neste manual fornecem apenas recuperação automatizada de desastres para a camada de acesso. Você deve iniciar manualmente todos os nós do XenMobile Server e o banco de dados do SQL Server no failover do site antes que os dispositivos possam se conectar ao XenMobile Server.

Integração com o NetScaler Gateway e NetScaler

April 15, 2019

Quando integrado ao XenMobile, o NetScaler Gateway fornece um mecanismo de autenticação para o acesso de dispositivos remotos à rede interna para dispositivos MAM. A integração permite que os aplicativos móveis de produtividade se conectem a servidores corporativos na intranet através de uma micro VPN criada a partir dos aplicativos no dispositivo móvel para o NetScaler Gateway.

O balanceamento de carga NetScaler é necessário para todos os modos de dispositivos do XenMobile Server se você tiver vários XenMobile Servers ou se o XenMobile Server estiver dentro de sua rede DMZ ou interna (e, portanto, o tráfego fluir de dispositivos para NetScaler para XenMobile).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos de integração para os modos do XenMobile Server

Os requisitos de integração para o NetScaler Gateway e NetScaler diferem com base nos modos do XenMobile Server: MAM, MDM e ENT.

MAM

Com o XenMobile Server no modo MAM:

- O **NetScaler Gateway** é necessário. O NetScaler Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator.
- O **NetScaler** é recomendado para balanceamento de carga.

  A Citrix recomenda implantar 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 Legado.

MDM

Com o XenMobile Server no modo MDM:

- O NetScaler Gateway não é necessário. Para implantações de MDM, a Citrix recomenda o NetScaler Gateway para VPN de dispositivo móvel.
- O NetScaler é recomendado para segurança e balanceamento de carga.

  A Citrix recomenda que você implemente um dispositivo NetScaler na frente do XenMobile Server, para segurança e balanceamento de carga. Para implantações padrão com o XenMobile Server na DMZ, a Citrix recomenda o assistente do NetScaler para XenMobile juntamente com o balanceamento de carga do XenMobile Server no modo Ponte SSL. Você também pode considerar a descarga de SSL para implantações nas quais o XenMobile Server reside na rede interna em vez da DMZ e/ou onde a segurança exige tais configurações.

  Embora você possa considerar a exposição do XenMobile Server à Internet via NAT ou proxies de terceiros existentes ou balanceadores de carga para o MDM, desde que o tráfego SSL termine no XenMobile Server (ponte SSL), a Citrix não recomenda essa abordagem devido ao possível risco de segurança.

  Para ambientes de alta segurança, o NetScaler com a configuração padrão do XenMobile deve atender ou exceder os requisitos de segurança.

  Para ambientes de MDM com as mais altas necessidades de segurança, a terminação SSL no NetScaler fornece a capacidade de inspecionar o tráfego no perímetro, enquanto mantém a

© 1999-2019 Citrix Systems, Inc. All rights reserved.

criptografia SSL de ponta a ponta. Para obter mais informações, consulte Requisitos de segurança. O NetScaler oferece opções para definir criptografias SSL/TLS e hardware SSL FIPS NetScaler.

ENT (MAM+MDM)

Com o XenMobile Server no modo ENT:

- O NetScaler Gateway é necessário. O NetScaler Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator.

  Quando o modo do servidor XenMobile é ENT e um usuário opta pelo registro no MDM, o dispositivo opera no modo MAM Legado. No modo MAM legado, os dispositivos se registram usando o FQDN do NetScaler Gateway. Para obter detalhes, consulte Sobre os modos MAM e MAM Legado.

- O NetScaler é recomendado para balanceamento de carga. Para mais informações, consulte o ponto NetScaler acima em "MDM".

> Importante:
>
> Esteja ciente de que, para o registro inicial, o tráfego dos dispositivos do usuário é autenticado no servidor XenMobile, independentemente de você configurar servidores virtuais de balanceamento de carga para Descarga SSL ou Ponte SSL.

Decisões de design

As seções a seguir resumem as várias decisões de design a serem consideradas ao planejar uma integração do NetScaler Gateway com o XenMobile.

Licenciamento e edição

Detalhe da decisão:

- Qual edição do NetScaler você usará?
- Você já aplicou licenças de plataforma ao NetScaler?
- Caso precise da funcionalidade MAM, você aplicou as licenças de acesso universal do NetScaler?

Orientação de design:

Certifique-se de aplicar as licenças apropriadas ao NetScaler Gateway. Se você estiver usando o conector Citrix Gateway para Exchange ActiveSync, o armazenamento em cache integrado pode ser necessário; portanto, você deve garantir que o NetScaler Edition apropriado esteja em vigor.

Os requisitos de licença para ativar os recursos do NetScaler são os seguintes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- O balanceamento de carga do XenMobile MDM requer uma licença de plataforma padrão do NetScaler no mínimo.
- O balanceamento de carga do ShareFile com o StorageZones Controller requer uma licença de plataforma padrão do NetScaler no mínimo.
- A edição XenMobile Enterprise inclui as licenças universais necessárias do NetScaler Gateway para o MAM.
- O balanceamento de carga do Exchange requer uma licença de plataforma NetScaler Platinum ou uma licença de plataforma NetScaler Enterprise com a adição de uma licença de Cache Integrado.

Versão do NetScaler para o XenMobile

Detalhe da decisão:

- Qual versão o NetScaler está executando no ambiente XenMobile?
- Será necessária uma instância separada?

Orientação de design:

A Citrix recomenda o uso de uma instância dedicada do NetScaler para o seu servidor virtual NetScaler Gateway. Certifique-se de que a versão e a compilação mínimas do NetScaler estejam em uso no ambiente XenMobile. Geralmente, o melhor é usar a última versão e compilação compatíveis do NetScaler for XenMobile. Se a atualização do NetScaler Gateway afetar seus ambientes existentes, uma segunda instância dedicada para o XenMobile poderá ser apropriada.

Se você planeja compartilhar uma instância do NetScaler com XenMobile e outros aplicativos que usam conexões VPN, certifique-se de ter licenças de VPN suficientes para todos. Tenha em mente que os ambientes de teste e produção do XenMobile não podem compartilhar uma instância do NetScaler.

Certificados

Detalhe da decisão:

- Você exige um maior grau de segurança para registros e acesso ao ambiente XenMobile?
- O LDAP não é uma opção?

Orientação de design:

A configuração padrão para o XenMobile é autenticação de nome de usuário e senha. Para adicionar outra camada de segurança para registro e acesso ao ambiente do XenMobile, considere usar a autenticação baseada em certificado. Você pode usar certificados com LDAP para autenticação de dois fatores, fornecendo um maior grau de segurança sem precisar de um servidor RSA.

Se você não permitir LDAP e usar cartões inteligentes ou similar métodos, a configuração de certificados permite a você representar um cartão inteligente para o XenMobile. Em seguida, os usuários se

© 1999-2019 Citrix Systems, Inc. All rights reserved.

registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que o usuário pode acessar, o XenMobile cria e subsequentemente implanta o certificado usado para autenticar no ambiente XenMobile.

O XenMobile dá suporte a lista de certificados revogados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o NetScaler para gerenciar a revogação. Quando você configura a autenticação baseada em certificado de cliente, decida se você precisa configurar a opção lista de certificados revogados (CRL) **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 emite um novo certificado porque não impede que um usuário gere um certificado de usuário de um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

Topologia de rede

Detalhe da decisão:

- Qual topologia do NetScaler é necessária?

Orientação de design:

A Citrix recomenda o uso de uma instância do NetScaler para o XenMobile. No entanto, se não quiser que haja tráfego entre a rede interna e a DMZ externa, considere configurar uma instância adicional do NetScaler, de modo que você use uma instância do NetScaler para usuários internos e outra para usuários externos. Esteja ciente de que, quando os usuários alternam entre as redes interna e externa, o cache de registros DNS pode resultar em um aumento nas solicitações de logon no Secure Hub.

Observe que o XenMobile atualmente não suporta o salto duplo do NetScaler Gateway.

VIPs NetScaler Gateway dedicados ou compartilhados

Detalhe da decisão:

- Você usa atualmente o NetScaler Gateway para XenApp e XenDesktop?
- O XenMobile aproveitará o mesmo NetScaler Gateway que o XenApp e XenDesktop?
- Quais são os requisitos de autenticação para ambos os fluxos de tráfego?

Orientação de design:

Quando seu ambiente Citrix inclui o XenMobile, além do XenApp e XenDesktop, você pode usar a mesma instância NetScaler e o servidor virtual NetScaler Gateway para ambos. Devido a possíveis conflitos de versão e isolamento do ambiente, instâncias dedicadas do NetScaler e do NetScaler Gateway são recomendadas para cada ambiente XenMobile. No entanto, se uma instância dedicada do NetScaler não for uma opção, a Citrix recomenda o uso de um NetScaler Gateway vServer dedicado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

em vez de um vServer compartilhado entre o XenMobile e o XenApp e XenDesktop para separar os fluxos de tráfego do Secure Hub.

Se você usar a autenticação LDAP, o Citrix Receiver e o Secure Hub poderão se autenticar no mesmo NetScaler Gateway sem problemas. Se você usar a autenticação baseada em certificado, o XenMobile enviará um certificado no contêiner MDX e o Secure Hub usará o certificado para se autenticar no NetScaler Gateway. O Citrix Receiver é separado do Secure Hub e não pode usar o mesmo certificado do Secure Hub para se autenticar no mesmo NetScaler Gateway.

Considere esta alternativa, a qual permite que você use o mesmo FQDN para dois VIPs do NetScaler Gateway. Você pode criar dois VIPs do NetScaler Gateway com o mesmo endereço IP, mas o do Secure Hub usa a porta padrão 443 e o do XenApp e XenDesktop (que implanta o Citrix Receiver) usa a porta 444. Em seguida, um FQDN resolve para o mesmo endereço IP. Para essa alternativa, talvez seja necessário configurar o StoreFront para retornar um arquivo ICA para a porta 444, em vez da porta padrão 443. Esta solução alternativa não requer que os usuários insiram um número de porta.

Tempos limite do NetScaler Gateway

Detalhe da decisão:

- Como você deseja configurar os tempos limite do Gateway NetScaler para o tráfego do XenMobile?

Orientação de design:

O NetScaler Gateway inclui as configurações Tempo limite da sessão e Tempo limite forçado. Para obter detalhes, consulte Configurações recomendadas. Tenha em mente que existem diferentes valores de tempo limite para serviços em segundo plano, NetScaler e para acessar aplicativos enquanto estiver off-line.

Endereço IP do balanceador de carga XenMobile para MAM

Detalhe 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 NetScaler Gateway, atribuir o VIP e o endereço de balanceamento de carga do XenMobile dessa maneira causará falhas no registro.

Verifique se o VIP de balanceamento de carga usa um IP interno para evitar falhas de registro nesse cenário. Esse endereço IP virtual deve seguir o padrão RFC 1918 de endereços IP privados. Se você

© 1999-2019 Citrix Systems, Inc. All rights reserved.

usar um endereço IP não privado para esse servidor virtual, o NetScaler não poderá contatar o servidor XenMobile com êxito durante o processo de autenticação. Para obter detalhes, consulte https://support.citrix.com/article/CTX200430.

Mecanismo de balanceamento de carga do MDM

Detalhe da decisão:

- Como os servidores XenMobile terão a carga balanceada pelo NetScaler Gateway?

Orientação de design:

Use a Ponte SSL se o XenMobile estiver na DMZ. Use descarga de SSL se for necessário para atender aos padrões de segurança quando o XenMobile Server estiver na rede interna.

- Quando você faz o balanceamento de carga do XenMobile Server com VIPs do NetScaler no modo Ponte SSL, o tráfego da Internet flui diretamente para o XenMobile Server, onde as conexões terminam. O modo Ponte SSL é o modo mais simples de configurar e solucionar problemas.
- Quando você faz o balanceamento de carga do XenMobile Server com VIPs do NetScaler no modo Descarga de SSL, o tráfego da Internet flui diretamente para o NetScaler, onde as conexões terminam. O NetScaler estabelece novas sessões do NetScaler para o XenMobile Server. O modo de descarga SSL envolve complexidade adicional durante a configuração e a solução de problemas.

Porta de serviço para balanceamento de carga do MDM com a descarga de SSL

Detalhe da decisão:

- Se você usar o modo de descarga de SSL para o balanceamento de carga, qual porta o serviço de backend usará?

Orientação de design:

Para Descarga de SSL, escolha a porta 80 ou 8443 da seguinte maneira:

- Alavanque a porta 80 de volta ao XenMobile Server, para uma verdadeira descarga.
- A criptografia de ponta a ponta, ou seja, a uma nova criptografia do tráfego, não é suportada. Para obter detalhes, consulte o artigo do Suporte Citrix, Arquiteturas suportadas entre o NetScaler e o XenMobile Server.

FQDN de registro

Detalhe da decisão:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Qual será o FQDN para registro e o VIP para instância/balanceamento de carga do XenMobile?

Orientação de design:

A configuração inicial do primeiro XenMobile Server em um cluster requer que você insira o FQDN do XenMobile Server. Esse FQDN deve corresponder ao URL do VIP de MDM e ao URL do VIP do balanceador de carga de MAM interno. (Um registro de endereço interno do NetScaler resolve o VIP do balanceador de carga do MAM.) Para obter detalhes, consulte "FQDN de registro para cada tipo de implantação", posteriormente neste artigo.

Além disso, você deve usar o mesmo certificado que o certificado de ouvinte SSL do XenMobile, o certificado VIP interno do balanceador de carga do MAM e o certificado VIP do MDM (se estiver usando a descarga do SSL para o VIP do MDM).

> Importante:
>
> Depois de configurar o FQDN de registro, você não poderá alterá-lo. Um novo FQDN de registro exigirá uma nova compilação do banco de dados do SQL Server e do XenMobile Server.

Tráfego do Secure Web

Detalhe da decisão:

- Você restringirá o Secure Web à navegação interna apenas?
- Você habilitará o Secure Web para a navegação na Web interna e externa?

Orientação de design:

Se você usar a Secure Web apenas para a navegação interna, a configuração do NetScaler Gateway será simples e direta, supondo que a Secure Web possa acessar todos os sites internos por padrão; talvez seja necessário configurar firewalls e servidores proxy.

Se você usar o Secure Web para a navegação interna e externa, deverá ativar o SNIP para ter acesso de saída à Internet. Como a TI geralmente vê os dispositivos registrados (usando o contêiner MDX) como uma extensão da rede corporativa, a TI geralmente quer que as conexões do Secure Web retornem ao NetScaler, passem por um servidor proxy e então saiam para a Internet. Como padrão, o acesso ao Secure Web é com túnel para a rede interna, o que significa que o Secure Web utilizada um túnel de VPN por aplicativo de volta para rede interna para todo o acesso à rede e o NetScaler utilizada configurações de túnel dividido.

Para ver uma discussão sobre conexões do Secure Web, consulte Configurando conexões de usuário.

Notificações por Push para o Secure Mail

Detalhe da decisão:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Você vai usar notificações por push?

Orientação de design para iOS:

Caso a sua configuração do NetScaler Gateway inclua o Secure Ticket Authority (STA) e o túnel dividido está desativado, o NetScaler Gateway deve permitir o tráfego do Secure Mail para as URLs do serviço de ouvinte Citrix especificadas em Notificações por Push para o Secure Mail para iOS:

Orientação de design para o Android:

Como uma alternativa à política do MDX, Período de votação ativa, você pode usar o Google Cloud Messaging (GCM) para controlar como e quando os dispositivos Android precisam se conectar ao XenMobile. Com o GCM configurado, qualquer ação de segurança ou comando de implantação dispara uma notificação por push para o Secure Hub para solicitar ao usuário que se reconecte ao XenMobile Server.

STAs HDX

Detalhe da decisão:

- Quais STAs usar se você integrar o acesso ao aplicativo HDX?

Orientação de design:

As STAs HDX devem corresponder às STAs no StoreFront e devem ser válidas para o farm XenApp/XenDesktop.

ShareFile

Detalhe da decisão:

- Você usará os ShareFile StorageZone Controllers no ambiente?
- Qual URL de VIP do ShareFile você usará?

Orientação de design:

Se você incluir ShareFile StorageZone Controllers em seu ambiente, configure corretamente o seguinte: VIP do comutador de conteúdo do ShareFile (usado pelo Plano de Controle do ShareFile para se comunicar com os servidores do StorageZone Controller), VIPs de Balanceamento de Carga do ShareFile e todas as políticas e perfis necessários. Para obter informações, consulte a documentação do Citrix ShareFile StorageZones Controller.

IdP SAML

Detalhe da decisão:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Se o SAML for necessário para o ShareFile, você deseja usar o XenMobile como o IdP SAML?

Orientação de design:

A prática recomendada é integrar o ShareFile ao XenMobile Advanced Edition ou ao XenMobile Enterprise Edition, uma alternativa mais simples para configurar a federação baseada em SAML. Quando você usa o ShareFile com essas edições do XenMobile, o XenMobile fornece ao ShareFile a autenticação de logon único (SSO) de usuários de aplicativos móveis de produtividade, provisionamento de conta de usuário com base no Active Directory e políticas abrangentes de controle de acesso. O console XenMobile permite que você execute a configuração do ShareFile e monitore os níveis de serviço e o uso da licença.

Observe que há dois tipos de clientes do ShareFile: clientes do ShareFile para XenMobile (também chamados de ShareFile preparados) e clientes móveis do ShareFile (também chamados de ShareFile não preparados). Para entender as diferenças, consulte [Em que os clientes do ShareFile para XenMobile diferem dos clientes móveis do ShareFile](/pt-br/mobile-productivity-apps/sharefile.html#how-citrix-files-for-endpoint-management-clients-differ-from-citrix-files-mobile-clients.

Você pode configurar o XenMobile e o ShareFile para usar o SAML para fornecer acesso SSO aos aplicativos móveis do ShareFile que você prepara com o kit de ferramentas MDX, bem como os clientes do ShareFile não preparados, como site da Web, o plug-in Outlook ou clientes de sincronização.

Se você quiser usar o XenMobile como o IdP SAML para o ShareFile, verifique se as configurações adequadas foram definidas. Para obter detalhes, consulte SAML para SSO com o ShareFile.

Conexões diretas do ShareConnect

Detalhe da decisão:

- Os usuários acessarão um computador host a partir de um computador ou dispositivo móvel que esteja executando o ShareConnect usando conexões diretas?

Orientação de design:

O ShareConnect permite que os usuários se conectem com segurança com seus computadores através iPads, tablets Android e telefones Android para acessar seus arquivos e aplicativos. Para ligações diretas, o XenMobile usa o NetScaler Gateway para fornecer o acesso seguro a recursos de dados fora da rede local. Para ver detalhes de configuração, consulte ShareConnect.

FQDN de registro para cada tipo de implantação

Tipo de implantação	FQDN de registro

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Enterprise (MDM+MAM) com registro obrigatório no MDM	FQDN do XenMobile Server
Enterprise (MDM+MAM) com registro opcional no MDM	FQDN do XenMobile server ou FQDN do NetScaler Gateway
Apenas MDM	FQDN do XenMobile Server
Apenas MAM (legado)	FQDN do NetScaler Gateway
Apenas MAM	FQDN do XenMobile Server

Resumo de Implantação

A Citrix recomenda que você use o assistente NetScaler for XenMobile para garantir a configuração adequada. Esteja ciente de que você pode usar o assistente apenas uma vez. Se você tiver várias instâncias do XenMobile, como ambientes de teste, desenvolvimento e produção, deverá configurar o NetScaler para os ambientes adicionais manualmente. Quando você tiver um ambiente de trabalho, anote as configurações antes de tentar configurar o NetScaler manualmente para o XenMobile.

A sua principal decisão quando usa o assistente é se usará HTTPS ou HTTP para comunicação com o XenMobile Server. O HTTPS fornece comunicação de backend segura, já que o tráfego entre o NetScaler e o XenMobile é criptografado; a nova criptografia afeta o desempenho do XenMobile Server. O HTTP fornece melhor desempenho do XenMobile Server; o tráfego entre o NetScaler e o XenMobile não é criptografado. As tabelas a seguir mostram os requisitos de porta HTTP e HTTPS para o servidor NetScaler e XenMobile.

HTTPS

A Citrix normalmente recomenda a Ponte SSL para configurações do servidor virtual MDM do NetScaler. Para o uso da descarga de SSL do NetScaler com servidores virtuais MDM, o XenMobile suporta apenas a porta 80 como o serviço de backend.

Tipo de implantação	Método de balanceamento de carga do NetScaler	Nova criptografia SSL	Porta do XenMobile Server
MDM	Ponte SSL	N/D	443, 8443
MAM	Descarga de SSL	Ativado	8443

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Empresarial	MDM: Ponte SSL	N/D	443, 8443
Empresarial	MAM: Descarga de SSL	Ativado	8443

HTTP

Tipo de implantação	Método de balanceamento de carga do NetScaler	Nova criptografia SSL	Porta do XenMobile Server
MDM	Descarga de SSL	Sem suporte	80
MAM	Descarga de SSL	Ativado	8443
Empresarial	MAM: Descarga de SSL	Sem suporte	80
Empresarial	MAM: Descarga de SSL	Ativado	8443

Para obter diagramas do NetScaler Gateway em implantações XenMobile, consulte Arquitetura de referência para implantações locais.

Considerações sobre SSO e proxy para aplicativos MDX

April 15, 2019

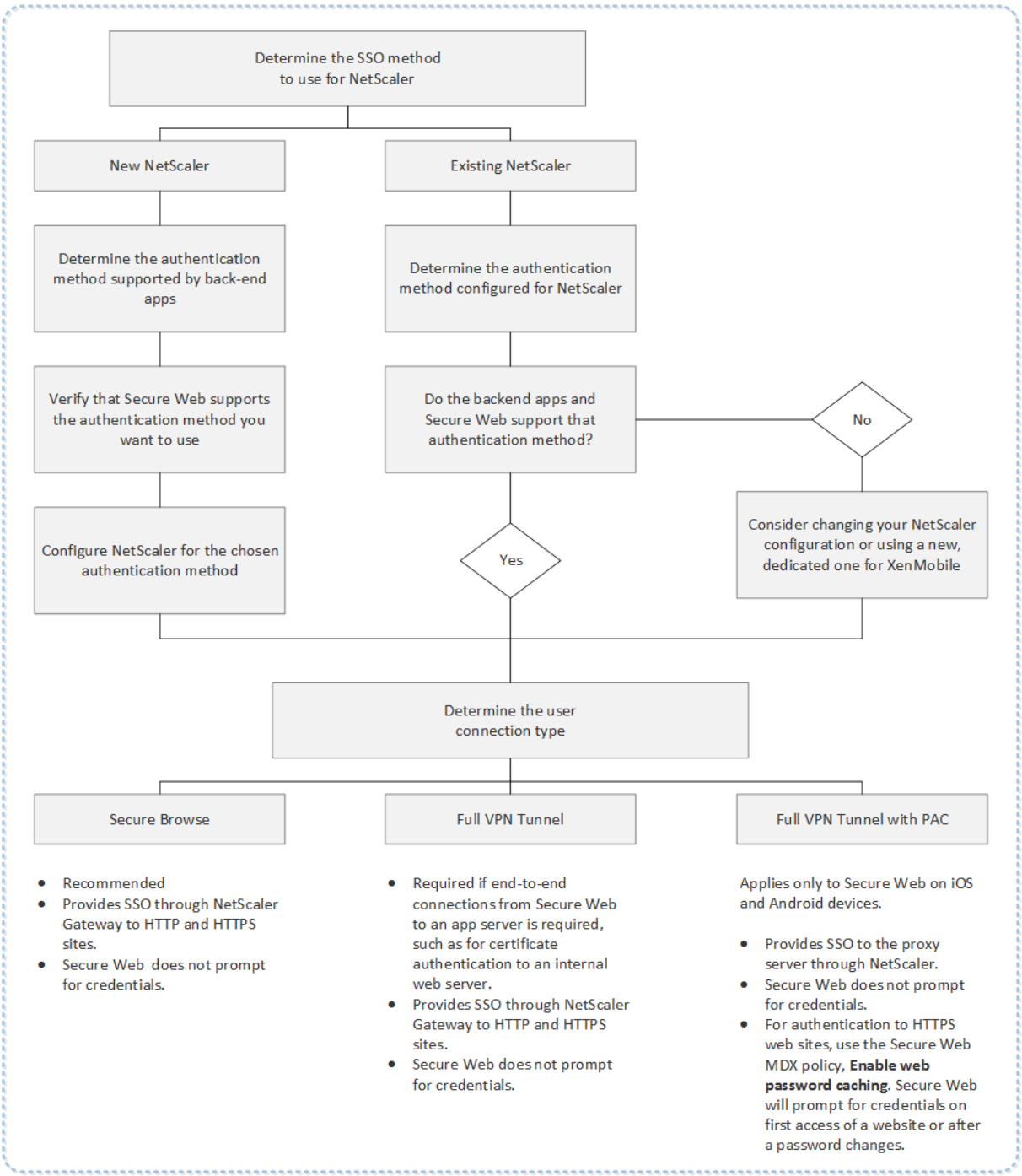
A integração do XenMobile com o NetScaler permite que você forneça aos usuários logon único (SSO) para todos os recursos HTTP/HTTPS de back-end. Dependendo dos seus requisitos de autenticação de SSO, você pode configurar conexões de usuário para um aplicativo MDX para usar uma das seguintes opções:

- Secure Browse, que é um tipo de VPN sem cliente
- Túnel Full VPN

Se o NetScaler não for a melhor maneira de fornecer o SSO em seu ambiente, você poderá configurar um aplicativo MDX com senhas locais em cache com base em políticas. Este artigo explora as diversas opções de SSO e proxy, com foco no Secure Web. Os conceitos se aplicam a outros aplicativos MDX.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O fluxograma a seguir resume o fluxo de decisão para conexões do usuário e SSO.



Métodos de Autenticação NetScaler

Esta seção fornece informações gerais sobre os métodos de autenticação suportados pelo NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Autenticação SAML

Quando você configura o NetScaler para SAML (Security Assertion Markup Language), os usuários podem se conectar a aplicativos da Web que suportam o protocolo SAML para conexões de logon único. O NetScaler Gateway suporta o logon único do provedor de identidade (IdP) para aplicativos da Web SAML.

Configuração necessária:

- Configure o SAML SSO no perfil do NetScaler Traffic.
- Configure o SAML iDP para o serviço solicitado.

Autenticação NTLM

Se o SSO para aplicativos da Web estiver ativado no perfil da sessão, o NetScaler executará a autenticação NTLM automaticamente.

Configuração necessária:

- Ative o SSO no perfil NetScaler Session ou NetScaler Traffic.

Representação de Kerberos

O XenMobile oferece suporte apenas ao Kerberos for Secure Web. Quando você configura o NetScaler for Kerberos SSO, o NetScaler usa a representação quando uma senha de usuário está disponível para o NetScaler. Representação significa que o NetScaler usa credenciais de usuário para obter o ticket necessário para obter acesso a serviços, como o Secure Web.

Configuração necessária:

- Configure a política de sessão “Worx” do NetScaler para permitir que identifique o realm Kerberos de sua conexão.
- Configure uma conta Kerberos Constrained Delegation (KCD) no NetScaler. 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 and Kerberos Impersonation SSO.

Kerberos Constrained Delegation

O XenMobile oferece suporte apenas ao Kerberos for Secure Web. Quando você configura o NetScaler for Kerberos SSO, o NetScaler usa a delegação restrita quando uma senha de usuário não está disponível para o NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Com a delegação restrita, o NetScaler 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 KDC no NetScaler.
- Ative o SSO no perfil NetScaler Traffic.
- Configure o site de backend para autenticação Kerberos.
- Para esses e outros detalhes de configuração, consulte o blog da Citrix, Configuring Kerberos Single Sign-on for WorxWeb.

Autenticação de preenchimento de formulário

Quando você configura o NetScaler para o logon único baseado em formulário, os usuários podem efetuar login uma única vez para acessar todos os aplicativos protegidos em sua rede. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Configure o SSO baseado em formulário no perfil NetScaler Traffic.

Autenticação HTTP Digest

Se você habilitar o SSO para aplicativos da Web no perfil da sessão, o NetScaler executará a autenticação HTTP resumida automaticamente. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Ative o SSO no perfil NetScaler Session ou NetScaler Traffic.

Autenticação HTTP Basic

Se você habilitar o SSO para aplicativos da Web no perfil da sessão, o NetScaler executará a autenticação HTTP básica automaticamente. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Ative o SSO no perfil NetScaler Session ou NetScaler Traffic.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Secure Browse, Túnel Full VPN ou Túnel Full VPN com PAC

As seções a seguir descrevem os tipos de conexão do usuário para o Secure Web. Para obter mais informações, consulte este artigo da Secure Web na documentação do Citrix, Configurando conexões de usuário.

Túnel Full VPN

Conexões que fazem túnel para a rede interna podem usar um túnel VPN completo. Use a política de modo Preferred VPN do Secure Web para configurara o túnel Full VPN. A Citrix recomenda o Túnel Full VPN para conexões que usam certificados de cliente ou SSL de ponta a ponta a um recurso na rede interna. O túnel Full VPN lida com qualquer protocolo sobre TCP. Você pode usar o túnel Full VPN com dispositivos Windows, Mac, iOS e Android.

No modo Túnel Full VPN, o NetScaler não tem visibilidade dentro de uma sessão HTTPS.

Navegação segura

Conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, chamado de Secure Browse. O Secure Browse é a configuração padrão especificada para a política do Secure Web **Modo VPN preferencial**. A Citrix recomenda o Secure Browse para conexões que exigem um logon único (SSO).

No modo Secure Browse, o NetScaler divide a sessão HTTPS em duas partes:

- Do cliente para o NetScaler
- Do NetScaler para o servidor de recursos de backend.

Dessa maneira, o NetScaler tem total visibilidade de todas as transações entre o cliente e o servidor, permitindo que ele forneça o SSO.

Você também pode configurar servidores proxy para o WorxWeb quando usado no modo navegação segura. Para obter detalhes, consulte o blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Túnel Full VPN com PAC

Você pode usar um arquivo PAC (Proxy Automatic Configuration) com uma implantação de túnel Full VPN para o Secure Web em dispositivos iOS e Android. O XenMobile é compatível com a autenticação de proxy fornecida pelo NetScaler. Um arquivo PAC contém regras que definem como os navegadores selecionam um proxy para acessar uma URL especificada. O arquivo de regras PAC pode especificar a manipulação tanto para sites internos quanto externos. O WorxWeb analisa o arquivo de regras

© 1999-2019 Citrix Systems, Inc. All rights reserved.

PAC e envia as informações do servidor proxy para o NetScaler Gateway. O NetScaler Gateway não reconhece o arquivo PAC nem o servidor proxy.

Para autenticação de sites HTTPS, a política MDX do Secure Web, **Ativar armazenamento em cache de senha da web**, permite ao Secure Web autenticar e fornecer SSO para o servidor proxy por meio de MDX.

Túnel dividido do NetScale

Ao planejar sua configuração de SSO e proxy, você também deve decidir se deseja usar o túnel dividido do NetScaler. A Citrix recomenda que você use o túnel dividido do NetScaler somente se necessário. Esta seção fornece uma visão de alto nível de como funciona o túnel dividido: o NetScaler determina o caminho de tráfego com base em sua tabela de roteamento. Quando o túnel dividido do NetScaler está ativado, o Secure Hub distingue o tráfego de rede interno (protegido) do tráfego da Internet. O Secure Hub faz essa determinação com base nos aplicativos de sufixo DNS e intranet. O Secure Hub então encapsula apenas o tráfego da rede interna através do túnel VPN. Quando o túnel dividido do NetScaler está desativado, todo o tráfego passa pelo túnel VPN.

- Se você preferir monitorar todo o tráfego devido a considerações de segurança, desative o túnel dividido do NetScaler. Como resultado, todo o tráfego passa pelo túnel VPN.
- Se você usar o túnel Full VPN com PAC, deve desativar o túnel dividido do NetScaler Gateway. Se o túnel dividido estiver ativado e você tiver configurado um arquivo PAC, as regras do arquivo PAC substituem as regras de túnel dividido NetScaler. Um servidor proxy configurado em uma política de tráfego não substitui as regras de túnel dividido do NetScaler.

O padrão da política **Acesso à rede** no Secure Web é ser configurada como **Com túnel para a rede interna**. Com essa configuração, os aplicativos MDX usam as configurações do túnel dividido do NetScaler. O padrão da política **Acesso à rede** é diferente para alguns outros aplicativos móveis de produtividade.

O NetScaler Gateway também possui um modo de túnel dividido Micro VPN reverse. Essa configuração suporta uma lista de exclusão de endereços IP que não são encapsulados no NetScaler. Em vez disso, esses endereços são enviados usando a conexão de internet do dispositivo. Para obter mais informações sobre o túnel dividido reverse, consulte a documentação do NetScaler Gateway.

O XenMobile inclui a **Lista de exclusão de reverse split tunnel**. Para impedir que determinados sites se encapsulem em um túnel por meio do NetScaler Gateway, adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou de sufixos DNS que se conectam usando a rede local (LAN). Esta lista se aplica apenas ao modo Secure Browse com o NetScaler Gateway configurado para o túnel dividido reverse.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Autenticação

April 15, 2019

Em uma implantação do XenMobile, várias considerações entram em ação ao decidir como configurar a autenticação. Esta seção ajudará você a entender os vários fatores que afetam a autenticação e falará sobre:

- As principais políticas de MDX, as propriedades do cliente XenMobile e as configurações do NetScaler 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 aumentar o grau de segurança.

Em termos gerais, uma segurança mais forte resulta em uma experiência de usuário não tão ideal, porque os usuários precisam se autenticar com mais frequência. Como você equilibra essas preocupações depende das necessidades e prioridades de sua organização. Após examinar as três configurações recomendadas, você entenderá melhor a interação das medidas de autenticação disponíveis para você e como melhor implantar seu próprio ambiente XenMobile.

Modos de Autenticação

Autenticação on-line: permite que os usuários entrem na rede do XenMobile. Requer uma conexão com a Internet.

Autenticação offline: acontece no dispositivo. Os usuários desbloqueiam o cofre seguro e têm acesso offline a itens, como emails baixados, sites em cache e anotações.

Métodos de Autenticação

Fator Único

LDAP: você pode configurar uma conexão no XenMobile a um ou mais diretórios, como o Active Directory, que sejam compatíveis com o protocolo LDAP. Esse é um método comumente usado para fornecer logon único (SSO) para ambientes da empresa. Você pode optar pelo Citrix PIN com senha em cache do Active Directory para melhorar a experiência do usuário com o LDAP e, ao mesmo tempo, fornecer a segurança de senhas complexas no registro, expiração de senha e bloqueio de conta.

Para obter mais detalhes, consulte Domínio ou domínio mais autenticação de ticket de segurança.

Certificado de cliente: o XenMobile pode integrar-se a autoridades de certificação padrão do setor para usar certificados como o único método de autenticação on-line. O XenMobile fornece esse certificado após o registro do usuário, o que requer uma senha de uso único, URL de convite ou credenciais

© 1999-2019 Citrix Systems, Inc. All rights reserved.

LDAP. Ao usar um certificado de cliente como o principal método de autenticação, um Citrix PIN é necessário em ambientes cliente somente certificado para proteger o certificado no dispositivo.

O XenMobile dá suporte a lista de certificados revogados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o NetScaler para gerenciar a revogação. Quando você configurar a autenticação baseada em certificado de cliente, decida se precisa definir a configuração de CRL (Lista de revogação de certificados do NetScaler), Ativar atualização automática da 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 emite um novo certificado porque não impede que um usuário gere um certificado de usuário de um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

Para obter um diagrama que mostre a implantação necessária, se você planeja usar a autenticação baseada em certificado para os usuários ou se precisar usar sua autoridade de certificação corporativa para emitir certificados de dispositivo, consulte Arquitetura de referência para implantações locais.

Dois Fatores

LDAP + Certificado cliente: No ambiente do XenMobile, essa configuração é a melhor combinação para a segurança e experiência do usuário, com as melhores possibilidades de SSO combinadas com a segurança fornecidas pela autenticação de dois fatores no NetScaler. O uso de LDAP e certificado cliente fornece segurança com algo que os usuários sabem (suas senhas do Active Directory) e algo que eles têm (certificados cliente em seus dispositivos). O Secure Mail (e alguns outros aplicativos móveis de produtividade) pode configurar automaticamente e fornecer uma experiência aos usuários iniciais sem interrupções com autenticação de certificado cliente, com um ambiente de servidor de acesso cliente Exchange corretamente configurado. Para melhor usabilidade, você pode combinar essa opção com o Citrix PIN e armazenamento em 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 melhor usabilidade, você pode combinar essa opção com o Citrix PIN e armazenamento em cache de senha do Active Directory.

Políticas Importantes, Configurações e Propriedades do Cliente Envolvidas na Autenticação

As seguintes políticas, configurações e propriedades do cliente entram em ação com as três configurações recomendadas a seguir:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Políticas de MDX

Código secreto de aplicativo: se o valor for **Ativado**, será necessário um Citrix PIN ou código secreto para desbloquear o aplicativo quando ele for iniciado ou reiniciado após um período de inatividade. O padrão é **Ativado**.

Para configurar o timer de inatividade de todos os aplicativos, defina o valor de INACTIVITY_TIMER em minutos no console XenMobile nas **Propriedades do cliente** da guia **Configurações**. O padrão é 15 minutos. Para desativar o timer de inatividade de forma que um aviso de PIN ou código secreto seja exibido somente quando o aplicativo for iniciado, defina o valor como zero.

> Nota:
>
> Se você selecionar Seguro offline para a política Chaves de criptografia, a política será ativada automaticamente.

Sessão online obrigatória de o valor for **Ativado**, o usuário deverá ter uma conexão com a rede corporativa e uma sessão ativa para poder acessar o aplicativo no dispositivo. Se **Desativado**, não será necessária uma sessão ativa para acessar o aplicativo no dispositivo. O padrão é **Desativado**.

Período máximo offline (horas): define o período máximo durante o qual um aplicativo pode ser executado sem reconfirmar o direito de aplicativo e atualizar as políticas do XenMobile. Quando você define o Período máximo offline, se o Secure Hub para iOS tiver um token válido do NetScaler Gateway, o aplicativo recuperará novas políticas para aplicativos MDX do XenMobile sem interrupção para os usuários. Se o Secure Hub não tiver um token válido do NetScaler, os usuários deverão se autenticar por meio do Secure Hub para que as políticas de aplicativo sejam atualizadas. O token do NetScaler pode se tornar inválido devido a uma inatividade de sessão do NetScaler Gateway ou a uma política de tempo limite de sessão forçada. Quando os usuários fazem logon no Secure Hub novamente, eles podem continuar a executar o aplicativo.

Os usuários são lembrados para fazer logon em 30, 15 e 5 minutos antes da expiração do período. Após a expiração, o aplicativo será bloqueado até que usuários façam logon. O valor 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 de tíquete de serviços em segundo plano: O período de tempo que um serviço de rede em segundo plano continua válido. Quando o Secure Mail se conecta por meio do NetScaler Gateway a um Exchange Server com ActiveSync, XenMobile emite um token que o Secure Mail usa para se conectar ao Exchange Server interno. Essa definição de configuração determina a duração que o Secure Mail pode usar o token sem exigir um novo token de autenticação e a conexão ao Exchange Server. Quando o limite de tempo expirar, os usuários devem fazer logon novamente para gerar um

© 1999-2019 Citrix Systems, Inc. All rights reserved.

novo token. O padrão é **168 horas (7 dias)**. Quando esse tempo limite expirar, as notificações por email serão interrompidas.

Período de tolerância para sessão online obrigatória: determina por quantos minutos um usuário pode usar o aplicativo offline antes de a política Sessão online obrigatória impedir o uso do aplicativo (até que a sessão online seja validada). O padrão é 0 (sem período de tolerância).

Para obter mais informações sobre políticas de autenticação MDX Toolkit, consulte Políticas do XenMobile MDX para iOS e Políticas do XenMobile MDX para Android.

Propriedades do cliente XenMobile

> Nota:
>
> Propriedades do cliente são uma configuração global que se aplica a todos os dispositivos que se conectam ao XenMobile.

Citrix PIN: para uma experiência de login simplificada, você pode optar por ativar o Citrix PIN. Com o PIN, os usuários não precisam inserir outras credenciais repetidamente, como o nome de usuário e senha do Active Directory. Você pode configurar o PIN Citrix somente como uma autenticação offline autônoma ou combinar o PIN com o armazenamento de senha em cache do Active Directory para agilizar a autenticação e otimizar a usabilidade. Você configura o Citrix PIN em **Configurações > Cliente > Propriedades do Cliente** no console XenMobile.

Veja a seguir um resumo de algumas propriedades importantes. Para obter mais informações, consulte Propriedades do cliente.

ENABLE_PASSCODE_AUTH

Nome de exibição: ativar Autenticação do Citrix PIN

Essa chave permite que você ative a funcionalidade do PIN da Citrix. Com o PIN ou código secreto da Citrix, os usuários são solicitados a definir um PIN a ser usado em vez da senha do Active Directory. Você deve ativar essa configuração se **ENABLE_PASSWORD_CACHING** estiver ativado ou se o XenMobile estiver usando a autenticação de certificado.

Valores possíveis: true ou **false**

Valor padrão: false

ENABLE_PASSWORD_CACHING

Nome de exibição: ativar Armazenamento em Cache de Senha do Usuário

Essa chave permite que a senha do Active Directory de usuários seja armazenada em cache localmente no dispositivo móvel. Quando você define essa chave como true, os usuários são solicitados a definir um PIN ou código secreto da Citrix. A chave ENABLE_PASSCODE_AUTH deve ser definida como true quando você define essa chave como **true**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Valores possíveis: true ou **false**

Valor padrão: false

PASSCODE_STRENGTH

Nome de exibição: requisito de Força do PIN

Essa chave define a força do Citrix PIN ou do código secreto. Quando você alterar essa configuração, os usuários serão solicitados a definir um novo PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.

Valores possíveis: Baixa, **Média** ou **Forte**

Valor padrão: Média

INACTIVITY_TIMER

Nome de exibição: Timer de Inatividade

Essa chave define o tempo, em minutos, durante o qual os usuários podem deixar seus dispositivos inativos para depois poder acessar um aplicativo sem que lhes seja solicitado um Citrix PIN ou código secreto. Para ativar essa configuração em um aplicativo MDX, você deve definir a configuração Código Secreto do Aplicativo como **Ativado**. Se a configuração de código secreto de aplicativo estiver definida como **Desativado**, os usuários serão redirecionados para o Secure Hub para efetuar uma autenticação completa. Quando você altera essa configuração, o valor entra em vigor na próxima vez em que houver solicitação para que os usuários se autentiquem. O padrão é 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nome de exibição: Ativar Autenticação de Touch ID

Permite o uso do leitor de impressão digital (somente no iOS) para autenticação offline. A autenticação online ainda exigirá o método de autenticação principal.

ENCRYPT_SECRETS_USING_PASSCODE

Nome de exibição: Criptografar segredos usando o Código Secreto

Essa chave permite que dados confidenciais sejam armazenados no dispositivo móvel em um cofre secreto em vez de em um armazenamento nativo baseada na plataforma, como as chaves do iOS. Essa chave de configuração ativa a 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: true ou **false**

Valor padrão: false

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurações do NetScaler

Tempo limite da sessão: se você habilitar essa configuração, o NetScaler Gateway desconectará a sessão se o NetScaler não detectar atividade de rede para o intervalo especificado. Essa configuração é imposta aos usuários que se conectam com o plug-in do NetScaler 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 desativada.

Tempo limite forçado: se você habilitar essa configuração, o NetScaler Gateway desconectará a sessão após o intervalo de tempo limite, independentemente de o que o usuário esteja fazendo. Quando o intervalo de tempo limite termina, não há nada que o usuário possa fazer para evitar a desconexão. Essa configuração é imposta aos usuários que se conectam com o plug-in do NetScaler Gateway, Citrix Receiver, Secure Hub ou por meio de um navegador da Web. Se o Secure Mail estiver usando STA, um modo especial do NetScaler, a configuração Tempo Limite Forçado não se aplicará às sessões do Secure Mail. O padrão é **1440** minutos. Se você deixar esse valor em branco, a configuração será desativada.

Para obter mais informações sobre configurações de tempo limite no NetScaler Gateway, consulte a documentação do NetScaler.

Para obter mais informações sobre os cenários que solicitam que os usuários se autentiquem no XenMobile inserindo as credenciais em seus dispositivos, consulte Aviso de autenticação de cenários.

Definições da configuração padrão

Essas configurações são os padrões fornecidos pelo assistente NetScaler for XenMobile, pelo MDX Toolkit e no console XenMobile.

Configuração	Onde encontrar a configuração	Configuração padrão
Tempo limite de sessão	NetScaler Gateway	1440 minutos
Forçar tempo limite	NetScaler Gateway	1440 minutos
Período máximo offline	Políticas de MDX	72 horas
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	168 horas (7 dias)
Sessão online obrigatória	Políticas de MDX	Desativado
Período de tolerância para sessão online obrigatória	Políticas de MDX	0
Código secreto do aplicativo	Políticas de MDX	Ativado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração	Onde encontrar a configuração	Configuração padrão
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	false
Requisito de força do PIN	Propriedades do cliente XenMobile	Média
Tipo de PIN	Propriedades do cliente XenMobile	Numérico
Ativar armazenamento em cache de senha	Propriedades do cliente XenMobile	false
Timer de inatividade	Propriedades do cliente XenMobile	15
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	false

Configurações recomendadas

Esta seção fornece exemplos de três configurações do XenMobile que abrangem desde a mais baixa segurança, com a experiência ideal do usuário, até a mais alta segurança, com a experiência do usuário mais intrusiva. Esses exemplos fornecem pontos de referência úteis para determinar onde, na escala, você deseja colocar sua própria configuração. Esteja ciente de que modificar essas configurações pode exigir que você altere outras configurações também. Por exemplo, o período máximo offline deve ser sempre menor que o tempo limite da sessão.

Maior segurança

Essa configuração oferece o mais alto nível de segurança, mas contém desvantagens de usabilidade significativas.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tempo limite de sessão	NetScaler Gateway	1440	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 24 horas.
Forçar tempo limite	NetScaler Gateway	1440	A autenticação on-line será estritamente necessária a cada 24 horas. A atividade não prolonga a vida da sessão.
Período máximo offline	Políticas de MDX	23	Requer atualização da política todos os dias.
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	72 horas	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do NetScaler Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do NetScaler Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).
Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	true	Uma chave derivada da entropia do usuário protege o cofre.
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Forte	Requisitos de senha de alta complexidade.
Tipo de PIN	Propriedades do cliente XenMobile	Alfanumérico	O PIN é uma sequência alfanumérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	false	A senha do Active Directory não é armazenada em cache e o Citrix PIN será usado para autenticações offline.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Timer de inatividade	Propriedades do cliente XenMobile	15	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	false	Desativa o Touch ID para casos de uso de autenticação off-line no iOS.

Maior segurança

Uma abordagem mais intermediária, essa configuração exige que os usuários se autentiquem com mais frequência: a cada três dias, no máximo, em vez de sete, e reforcem a segurança. O aumento do número de autenticações bloqueia o contêiner com mais freqüência, garantindo a segurança dos dados quando os dispositivos não estão em uso.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Tempo limite de sessão	NetScaler Gateway	4320	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 3 dias.
Forçar tempo limite	NetScaler Gateway	Sem valor	As sessões serão estendidas se houver alguma atividade.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Período máximo offline	Políticas de MDX	71	Requer atualização da política a cada 3 dias. A diferença de horário serve para permitir a atualização antes do tempo limite da sessão.
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	168 horas	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do NetScaler Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.
Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do NetScaler Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false	Não exija entropia de usuário para criptografar o cofre.
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Média	Aplica regras de complexidade de senha média.
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	PIN é uma sequência numérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	true	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Timer de inatividade	Propriedades do cliente XenMobile	30	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	true	Ativa o Touch ID para casos de uso de autenticação off-line no iOS.

Alta Segurança

Essa configuração, a mais conveniente para os usuários, oferece segurança básica.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Tempo limite de sessão	NetScaler Gateway	10080	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 7 dias
Forçar tempo limite	NetScaler Gateway	Sem valor	As sessões serão estendidas se houver alguma atividade.
Período máximo offline	Políticas de MDX	167	Requer atualização da política toda semana (a cada 7 dias). A diferença de horário serve para permitir a atualização antes do tempo limite da sessão.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Expiração de tíquete de serviços em segundo plano	Políticas de MDX	240	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do NetScaler Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.
Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do NetScaler Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).
Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false	Não exija entropia de usuário para criptografar o cofre.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Baixo	Nenhum requisito de complexidade de senha
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	PIN é uma sequência numérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	true	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Timer de inatividade	Propriedades do cliente XenMobile	90	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	true	Ativa o Touch ID para casos de uso de autenticação off-line no iOS.

Usando a autenticação aumentada

Alguns aplicativos podem exigir autenticação avançada (por exemplo, um fator de autenticação secundário, como um token ou tempos limites de sessão rígidos). 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 dispositivos NetScaler separados).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
NetScaler Gateway alternativo	Políticas de MDX	Requer o FQDN e a porta do dispositivo NetScaler secundário.	Permite a autenticação avançada controlada pelas políticas de sessão e autenticação do dispositivo do NetScaler secundário.

Se um usuário abrir um aplicativo que efetua logon na instância alternativa do NetScaler Gateway, todos os outros aplicativos usarão essa instância do NetScaler Gateway para se comunicar com a rede interna. A sessão só voltará para a instância do NetScaler Gateway de segurança inferior quando a sessão expirar na instância do NetScaler Gateway com segurança avançada.

Usando a sessão online obrigatória

Para determinados aplicativos, como o Secure Web, uma sugestão seria você garantir que os usuários executem um aplicativo somente quando tiverem uma sessão autenticada e enquanto o dispositivo estiver conectado a uma rede. Essa política aplica essa opção e permite um período de tolerância para que os usuários possam concluir seu trabalho.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Sessão online obrigatória	Políticas de MDX	Ativado	Garante que o dispositivo esteja on-line e tenha um token de autenticação válido.
Período de tolerância para sessão online obrigatória	Políticas de MDX	15	Permite um período de tolerância de 15 minutos antes que o usuário não possa mais usar aplicativos

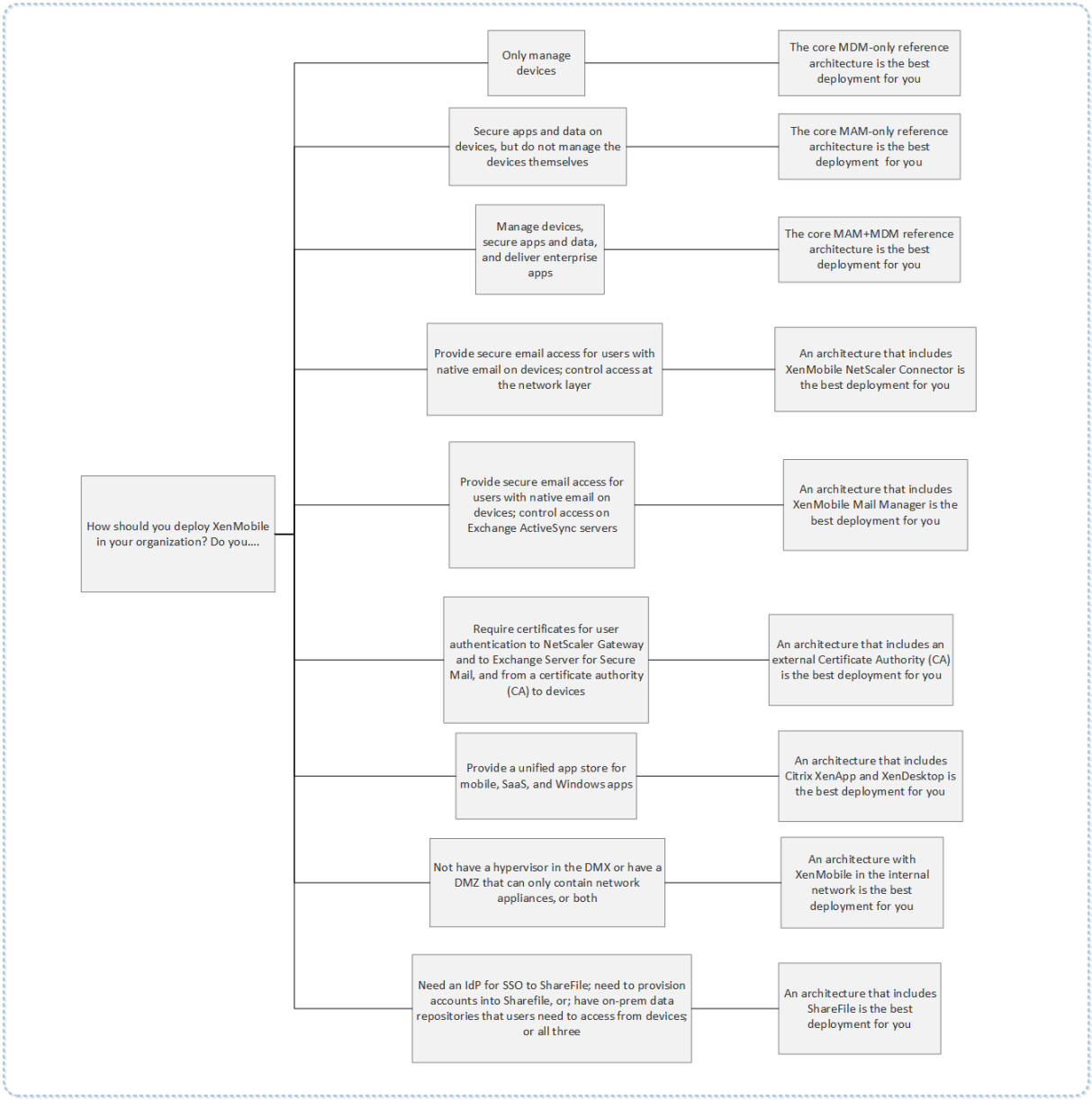
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Arquitetura de referência para implantações locais

April 15, 2019

As figuras neste artigo ilustram as arquiteturas de referência para a implantação do XenMobile nas instalações locais. Os cenários de implantação incluem somente MDM, somente MAM e MDM+MAM como as principais arquiteturas, bem como aquelas que incluem componentes, como o SNMP Manager, conector Citrix Gateway para Exchange ActiveSync, conector de Endpoint Management para Exchange ActiveSync e XenApp e XenDesktop. As figuras mostram os componentes mínimos necessários para o XenMobile.

Use este gráfico como um guia geral para suas decisões de implantação.

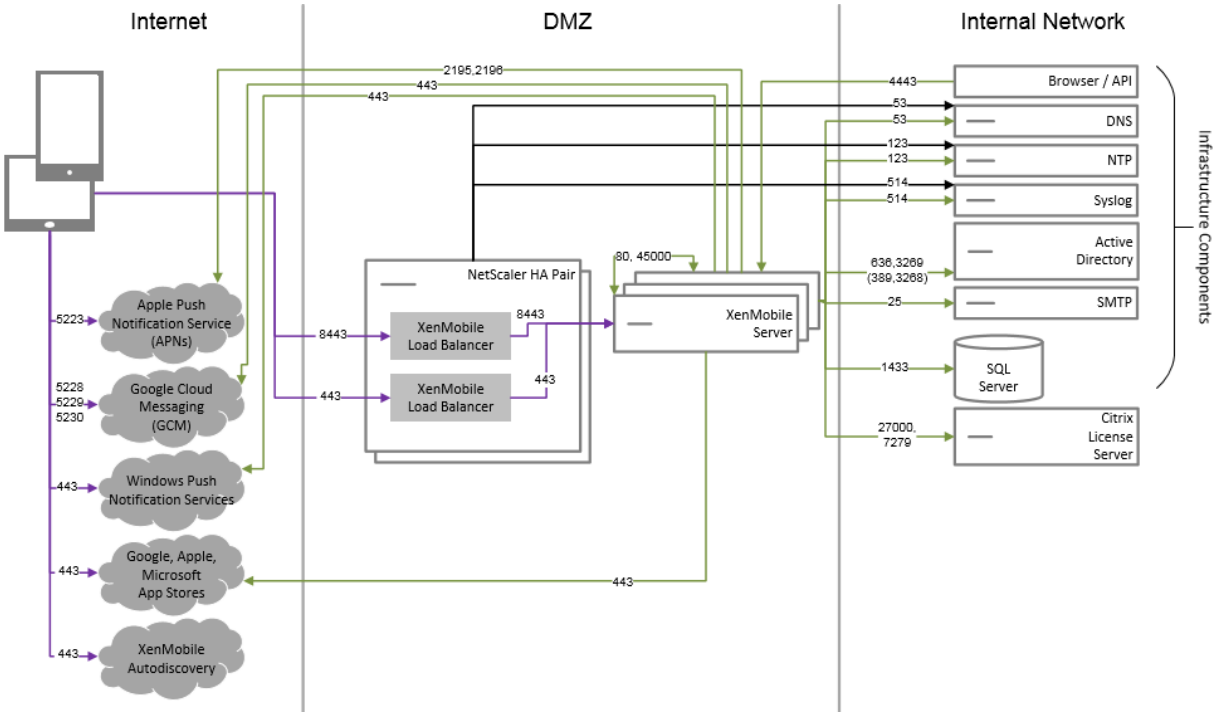


© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nas figuras, os números dos conectores representam portas que você deve abrir para permitir as conexões entre os componentes. Para obter uma lista completa de portas, consulte Requisitos de porta na documentação do XenMobile.

Arquitetura de referência somente MDM principal

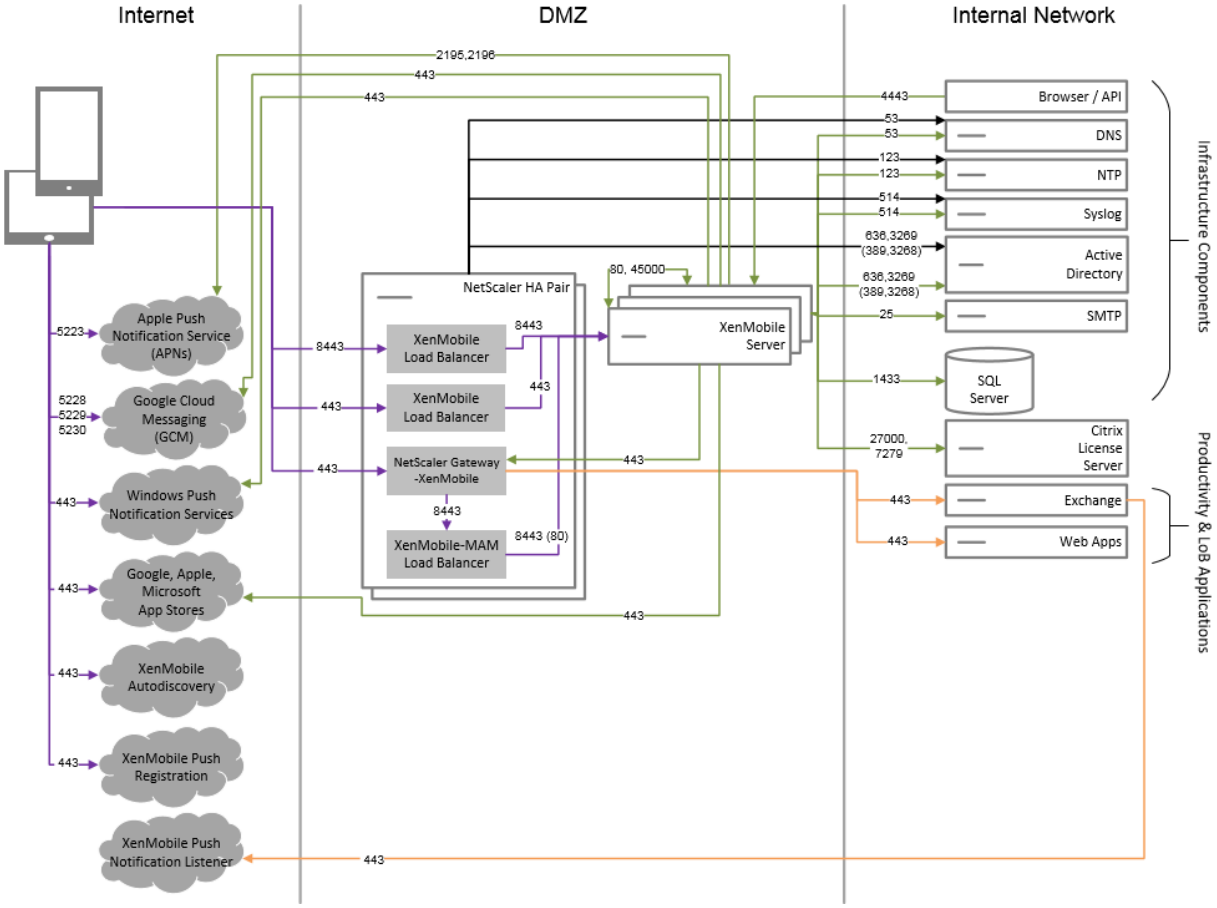
Implante essa arquitetura se você planeja usar somente os recursos MDM do XenMobile. Por exemplo, você precisa gerenciar um dispositivo emitido pela empresa por meio do MDM para implantar políticas de dispositivo e aplicativos, além de recuperar os inventários de ativos e ser capaz de realizar ações em dispositivos, como um apagamento de dispositivo.



Arquitetura de referência somente MAM principal

Implante essa arquitetura se você planeja usar somente os recursos MAM do XenMobile sem precisar registrar dispositivos para MDM. Por exemplo, você deseja proteger aplicativos e dados em dispositivos móveis BYO; você deseja entregar aplicativos móveis empresariais e ser capaz de bloquear aplicativos e apagar os respectivos dados. Os dispositivos não podem registrados no MDM.

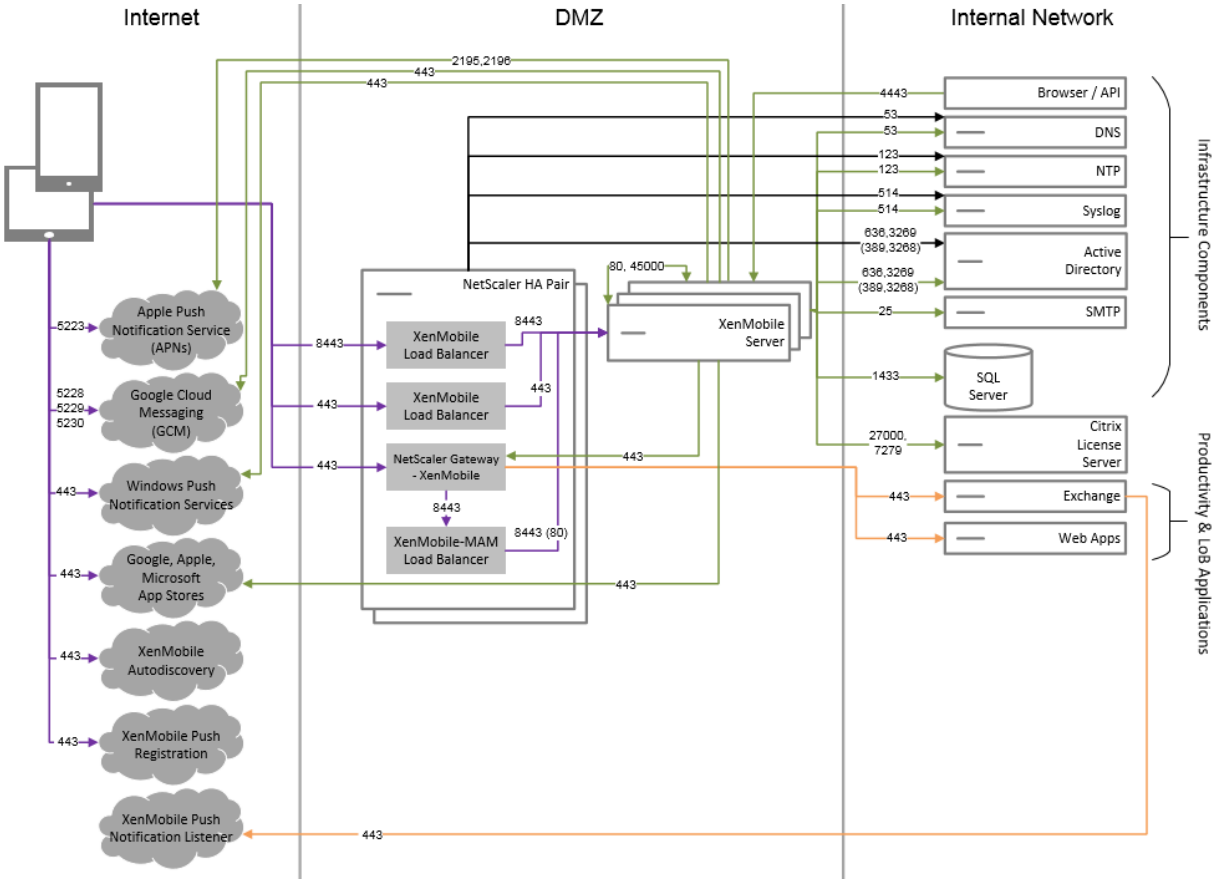
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência MAM+ MDM principal

Implante essa arquitetura se você planeja usar os recursos do MDM+MAM do XenMobile. Por exemplo, você precisa gerenciar um dispositivo emitido pela empresa por meio do MDM; você deseja implantar políticas de dispositivo e aplicativos, recuperar um inventário de ativos e poder apagar dispositivos. Você também deseja entregar aplicativos móveis empresariais e ser capaz de bloquear aplicativos e apagar os respectivos dados.

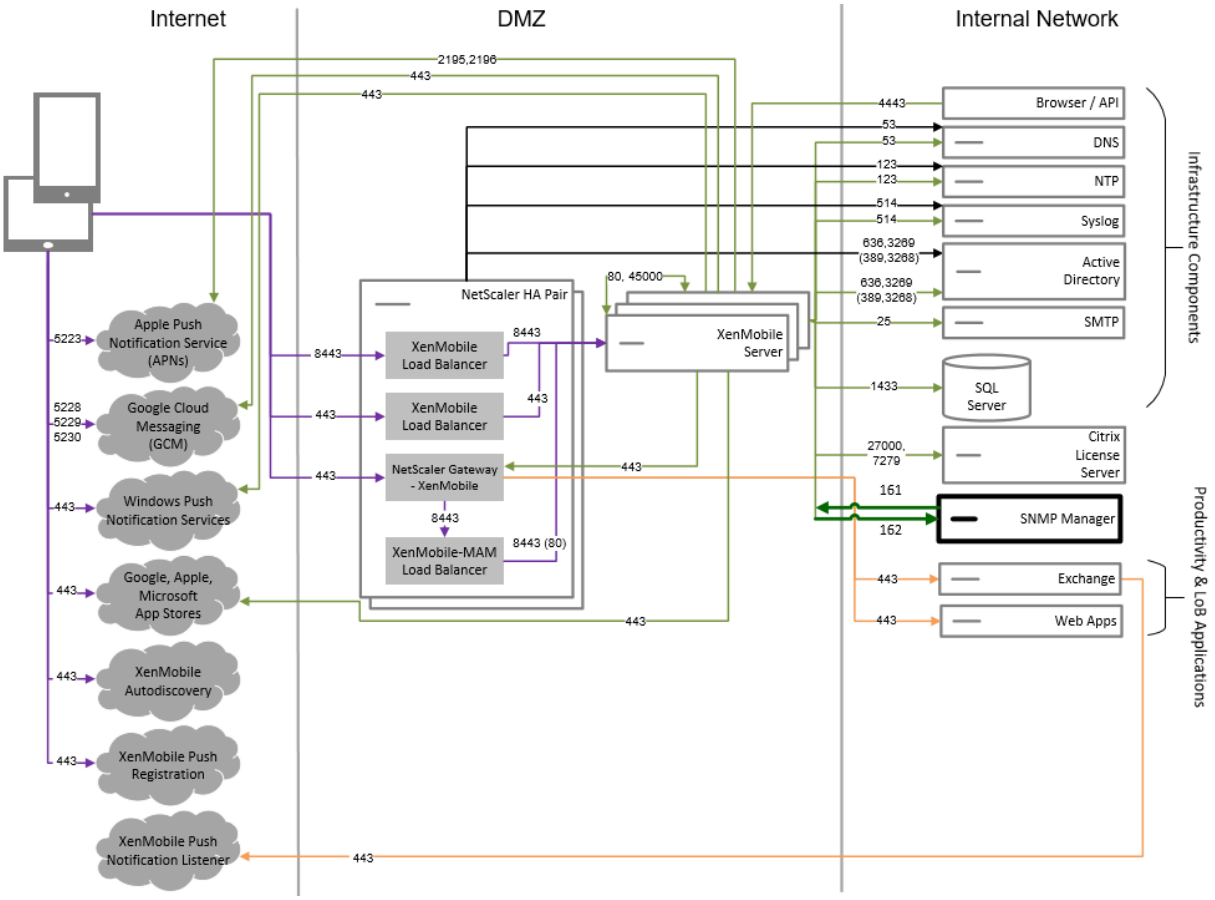
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência com SNMP

Implemente esta arquitetura se você planeja ativar o monitoramento SNMP com o XenMobile. Por exemplo, se você quiser permitir que os sistemas de monitoramento consultem e obtenham informações nos nós do XenMobile. Para obter detalhes, consulte SNMP monitoring.

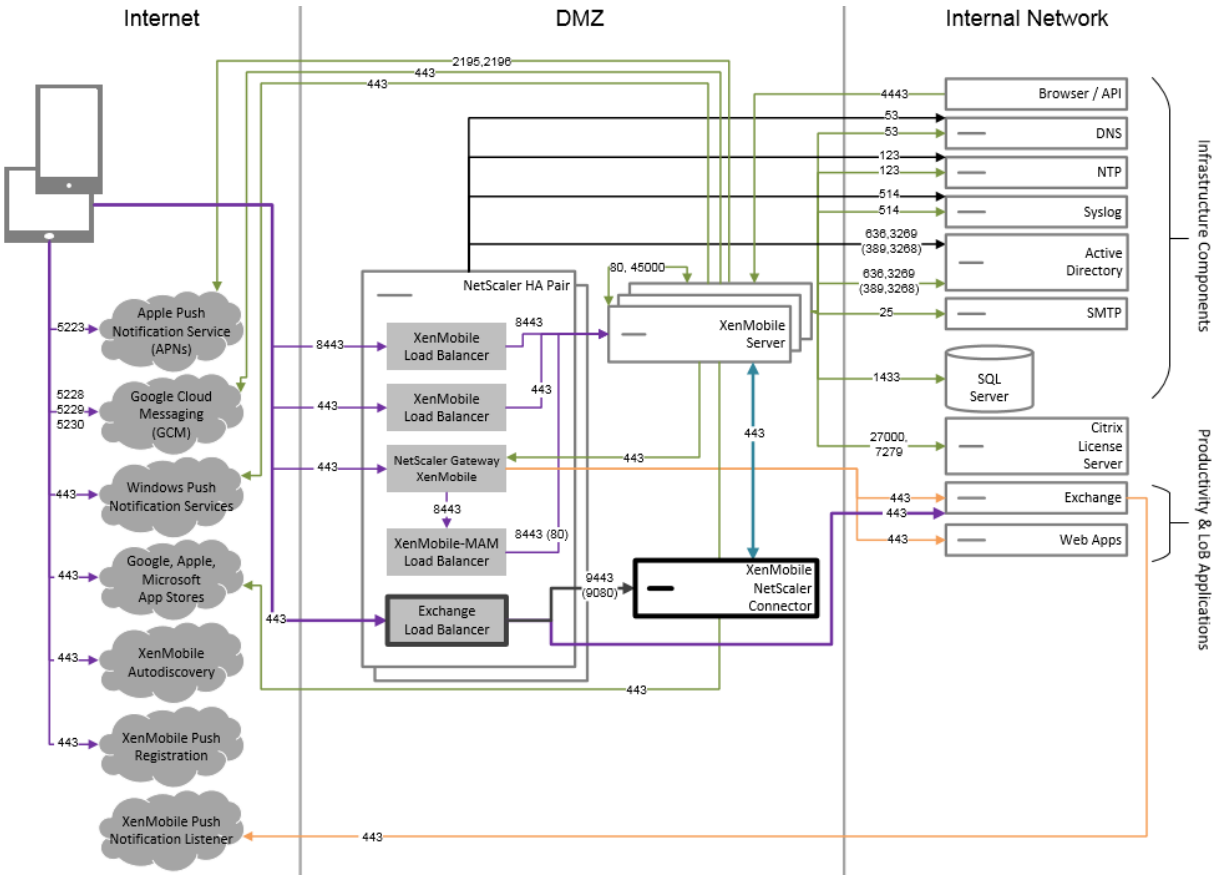
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência com o conector Citrix Gateway para Exchange ActiveSync

Implemente esta arquitetura se você planeja usar o conector Citrix Gateway para Exchange ActiveSync com o XenMobile. Por exemplo, se você precisar fornecer acesso seguro a e-mail aos usuários que usam aplicativos de e-mail móveis nativos. Esses usuários continuarão acessando o e-mail por meio de um aplicativo nativo, ou, se quiser, você poderá fazer a transição gradual deles para o Citrix Secure Mail. O controle de acesso precisa ocorrer na camada de rede antes que o tráfego atinja os servidores do Exchange Active Sync. Embora o diagrama mostre o conector do Exchange ActiveSync implantado em uma arquitetura MDM e MAM, você também pode implantar o conector de Exchange ActiveSync da mesma maneira como parte de uma arquitetura somente MDM.

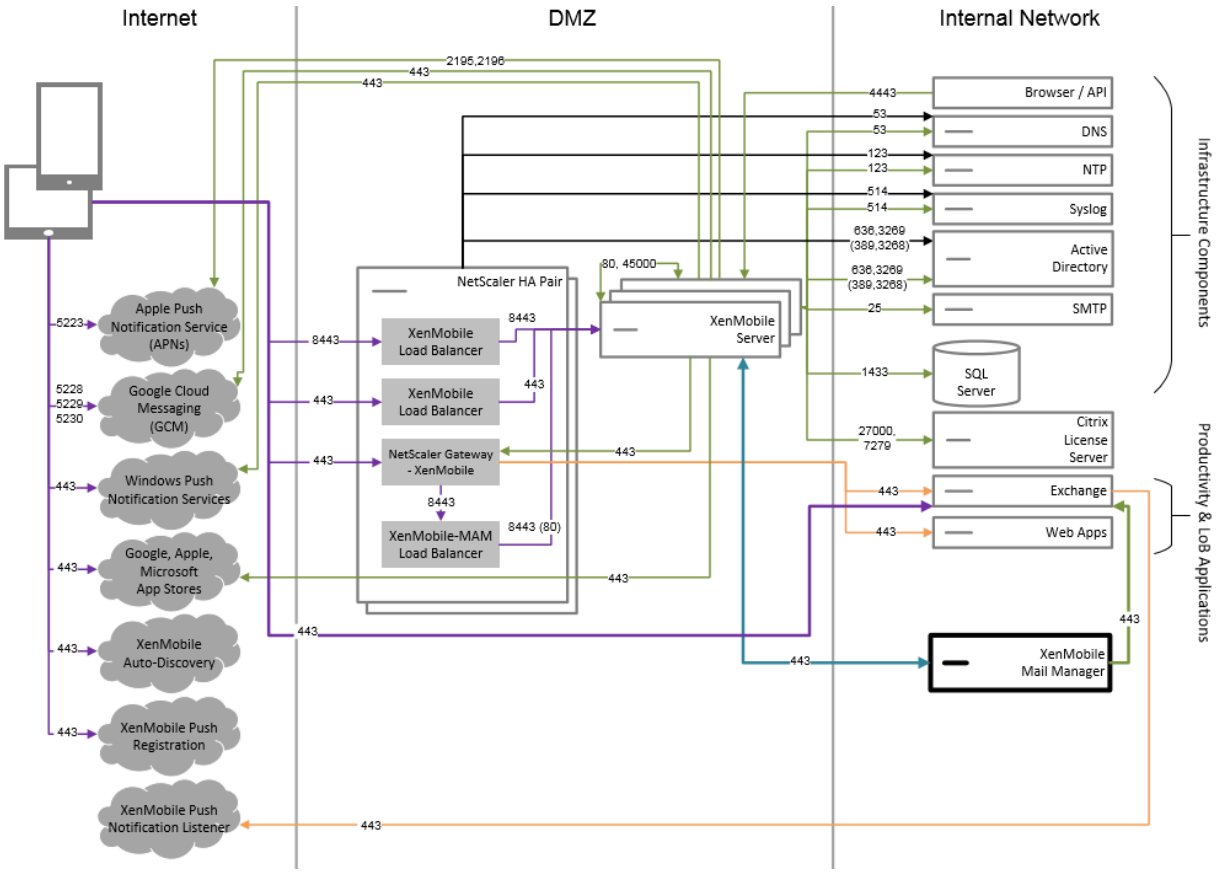
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência com conector de Endpoint Management para Exchange ActiveSync

Implemente esta arquitetura se você planeja usar o conector de Endpoint Management para Exchange ActiveSync com o XenMobile. Por exemplo, se você quiser fornecer acesso seguro a e-mail aos usuários que usam aplicativos de e-mail móveis nativos. Esses usuários continuarão acessando o e-mail por meio de um aplicativo nativo, ou, se quiser, você poderá fazer a transição gradual deles para o Secure Mail. Você pode obter o controle de acesso nos servidores Exchange ActiveSync. Embora o diagrama mostre o conector de Endpoint Management para Exchange ActiveSync implantado em uma arquitetura MDM e MAM, você também pode implantar o conector de Endpoint Management para o Exchange ActiveSync da mesma maneira como parte de uma arquitetura somente MDM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



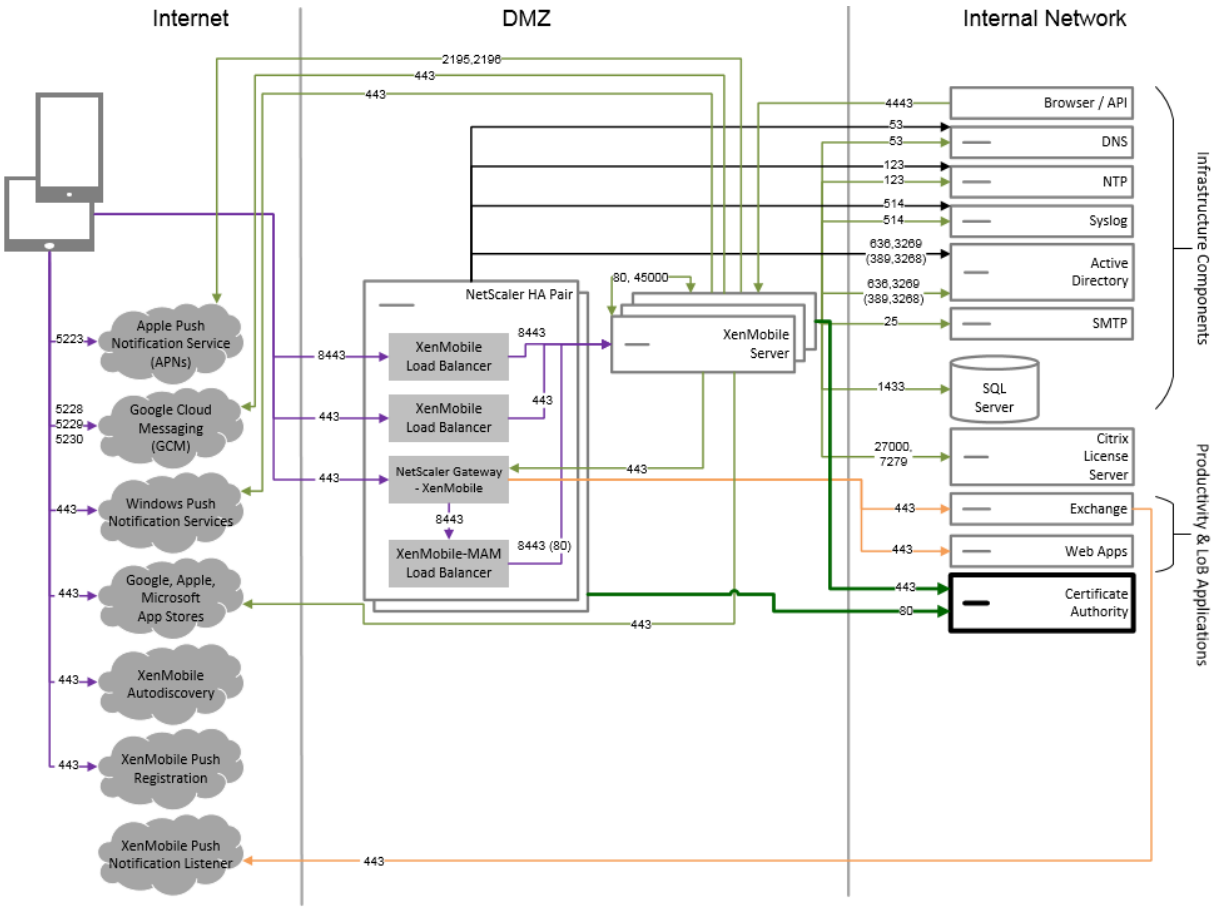
Arquitetura de referência com autoridade de certificação externa

Recomenda-se uma implantação que inclua uma autoridade de certificação externa para atender a um ou mais dos seguintes requisitos:

- Você precisa de certificados de usuário para autenticação do usuário no NetScaler Gateway (para acesso à intranet).
- Você precisa que os usuários do Secure Mail sejam autenticados no Exchange Server usando um certificado de usuário.
- Você precisa enviar certificados emitidos pela Autoridade de Certificação corporativa para dispositivos móveis para acesso Wi-Fi, por exemplo.

Embora o diagrama mostre uma autoridade de certificação externa implantada em uma arquitetura MDM+MAM, você também pode implantar uma Autoridade de Certificação externa da mesma maneira como parte de uma arquitetura somente MDM ou somente MAM.

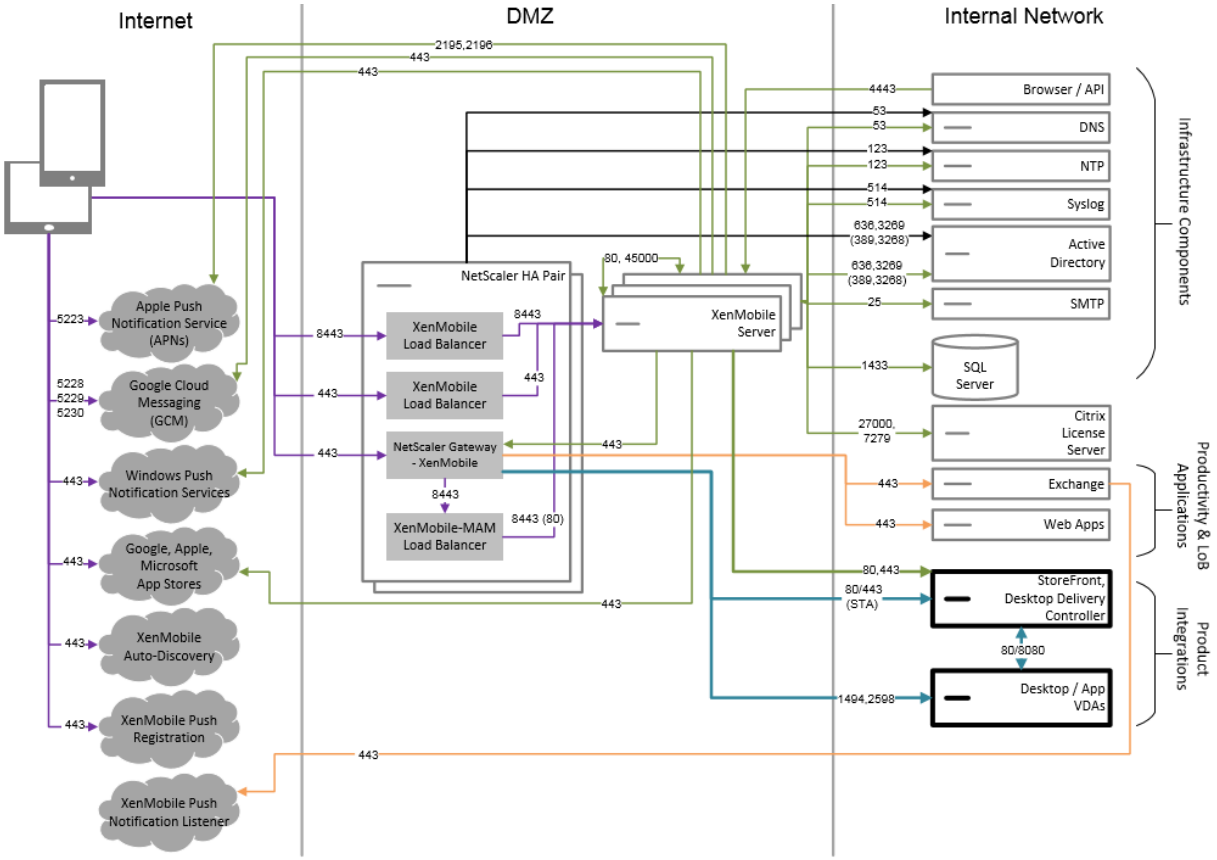
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência com o XenApp e o XenDesktop

Implemente esta arquitetura se você planeja integrar o XenApp e o XenDesktop 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 XenDesktop implementado em uma arquitetura MDM e MAM, você também pode implantar o XenDesktop da mesma maneira como parte de uma arquitetura somente MAM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

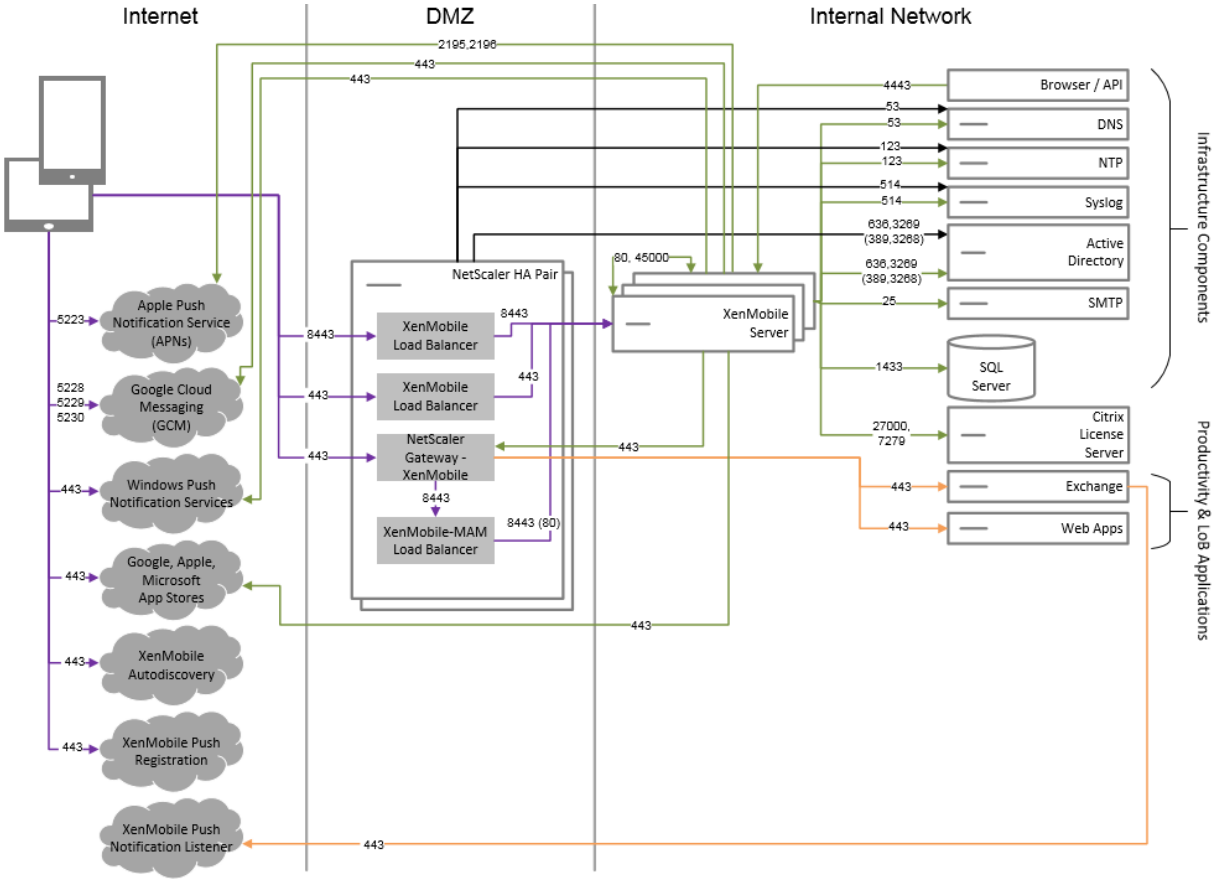


Arquitetura de referência com o XenMobile na rede interna

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 hipervisor na DMZ.
- Sua DMZ pode conter apenas dispositivos de rede.
- Seus requisitos de segurança requerem o uso do SSL Offload.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Arquitetura de referência com ShareFile

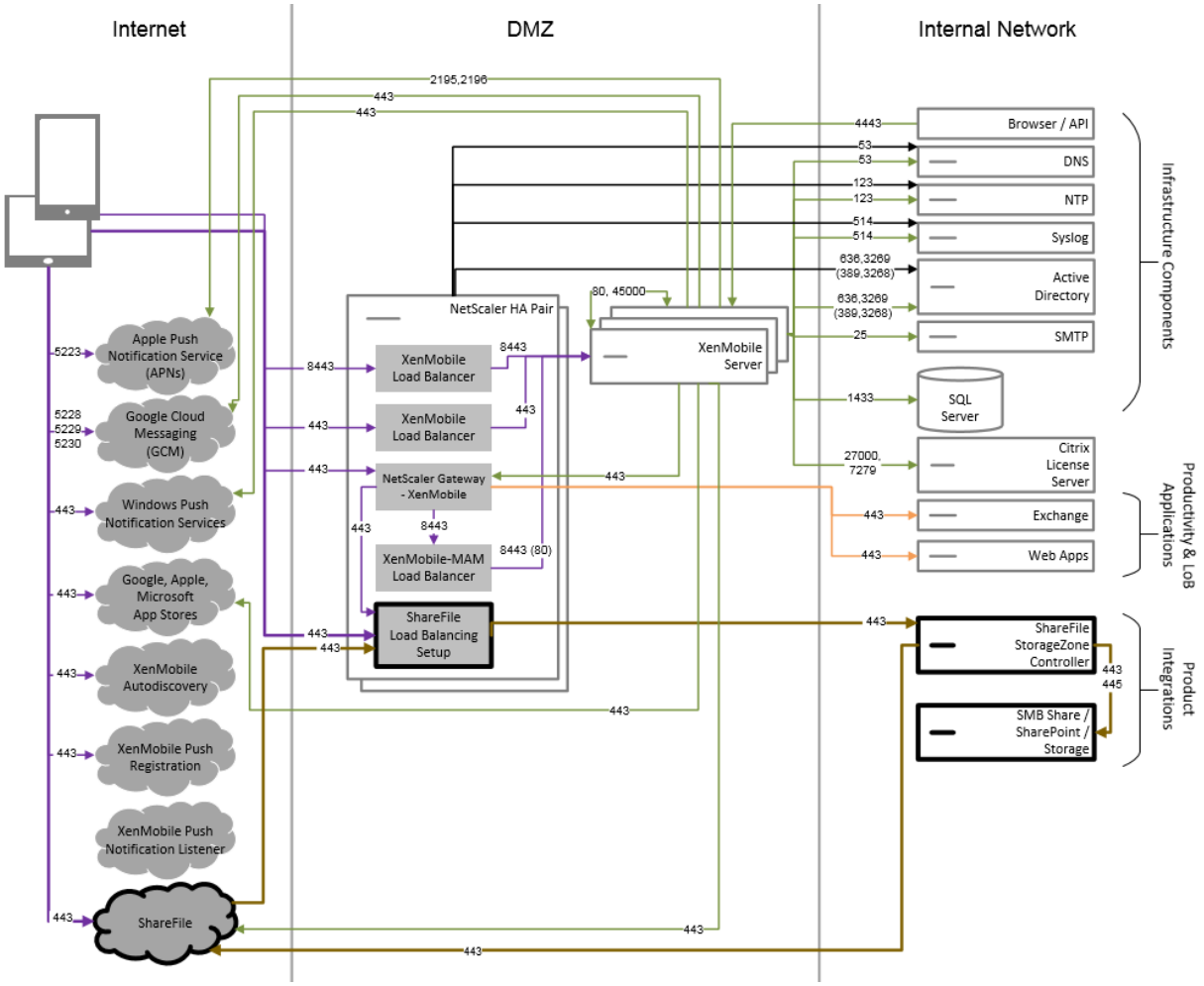
Implemente esta arquitetura se você quiser integrar o ShareFile Enterprise ou apenas os StorageZone Connectors com o XenMobile. A integração do ShareFile Enterprise permite atender a um ou mais dos seguintes requisitos:

- Você precisa de um IDP para fornecer aos usuários logon único (SSO) para o ShareFile.com.
- Você precisa de uma maneira de provisionar contas no ShareFile.com.
- Você tem repositórios de dados no local que precisam ser acessados a partir de dispositivos móveis.

Uma integração apenas com o StorageZone Connectors fornece aos usuários acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos em rede. Nessa configuração, você não precisa configurar um subdomínio do ShareFile, provisionar usuários ao ShareFile ou hospedar dados do ShareFile.

Embora o diagrama mostre o ShareFile implementado em uma arquitetura MDM+MAM, você também pode implantar o ShareFile da mesma maneira como parte de uma arquitetura somente MAM.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Propriedades do servidor

April 15, 2019

Propriedades do servidor são propriedades globais que se aplicam a operações, usuários e dispositivos em uma instância inteira do XenMobile. A Citrix recomenda que você avalie para o seu ambiente as propriedades do servidor abordadas neste artigo. Não deixe de consultar a Citrix antes de alterar outras propriedades do servidor.

Esteja ciente de que uma alteração em algumas propriedades do servidor requer uma reinicialização de cada nó do XenMobile Sever. O XenMobile avisa quando uma reinicialização é necessária.

Algumas propriedades do servidor ajudam a melhorar o desempenho e a estabilidade. Para obter detalhes, consulte Ajuste das operações do XenMobile.

Bloquear registro de dispositivos Android com root e iOS com jailbreak: quando essa propriedade é **True**, o XenMobile bloqueia o registro de dispositivos Android com root e dispositivos iOS com jail-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

break. O padrão é **True**. A configuração recomendada é **True** para todos os níveis de segurança.

Registro obrigatório: esta propriedade, que se aplica somente quando o Modo do XenMobile Server é ENT, especifica se você exige que os usuários se registrem no MDM. A propriedade se aplica a todos os usuários e dispositivos da instância do XenMobile. Exigir o registro proporciona 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 essa propriedade é **False**, os usuários podem recusar o registro, mas ainda podem acessar os aplicativos em seus dispositivos através da XenMobile Store. Quando essa propriedade for **True**, qualquer usuário que recusar o registro terá acesso negado aos aplicativos.

Se você alterar essa propriedade depois que os usuários se registrarem, os usuários deverão se registrar novamente.

Para ver um debate sobre a necessidade de exigir o registro no MDM, consulte Gerenciamento de dispositivos e registro do MDM.

Intervalo máximo de inatividade para o console do portal de autoatendimento do XenMobile MDM (em minutos): esse nome de propriedade reflete as versões antigas do XenMobile. A propriedade controla o intervalo máximo de inatividade do console XenMobile. Esse intervalo é o número de minutos após os quais o XenMobile faz logoff de um usuário inativo do console XenMobile. Um tempo limite de 0 significa que um usuário inativo permanece conectado. O padrão é **30**.

Tempo limite de inatividade em minutos: o número de minutos após os quais o XenMobile faz o logout de um usuário inativo que usou a API pública do XenMobile Server para acessar o console XenMobile ou algum aplicativo de terceiros. Um tempo limite de **0** significa que um usuário inativo permanece conectado. Para aplicativos de terceiros que acessam a API, normalmente é necessário permanecer conectado. O padrão é **5**.

Registro no gerenciamento de dispositivo iOS: instalar CA raiz se necessário: o fluxo de trabalho de registro mais recente da Apple requer que os usuários instalem manualmente os perfis MDM. Esse fluxo de trabalho não se aplica ao registro do 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 receberão somente a solicitação do certificado de dispositivo MDM durante o registro.

Para proporcionar uma melhor experiência de usuário durante o registro manual, a Citrix recomenda alterar a propriedade do servidor de `ios.mdm.enrollment.installRootCaIfRequired` para **`false`**. O valor padrão é **`true`** . Com essa alteração, uma janela do Safari é aberta durante o registro no MDM para simplificar a instalação do perfil para os usuários.

Intervalo de linha de base do VPP: o **intervalo de linha de base do VPP** define o intervalo mínimo em que o XenMobile reimporta licenças do VPP da Apple. A atualização de informações de licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado do VPP. Por padrão, o XenMobile atualiza a linha de base da licença do VPP no mínimo a cada **720** minutos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Se você tem um grande número de licenças do VPP 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 de importação de licenças. Se você espera mudanças frequentes de licenças do VPP da Apple, a Citrix recomenda reduzir o valor para manter o XenMobile atualizado com essas mudanças. O intervalo mínimo entre duas linhas de base é de 60 minutos. Como o trabalho cron é executado em segundo plano a cada 60 minutos, se o intervalo de linha de base do VPP for de 60 minutos, o intervalo entre linhas de base poderá ser atrasado até 119 minutos.

Políticas de dispositivos e aplicativos

April 15, 2019

As políticas de dispositivos e aplicativos do XenMobile permitem otimizar o equilíbrio entre fatores, como:

- Segurança da empresa
- Dados corporativos e proteção de ativos
- 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 outros setores, como educação e varejo, nos quais a produtividade do usuário é uma consideração primordial.

Você pode controlar e configurar as políticas de modo centralizado com base na identidade, no dispositivo, no local e no tipo de conectividade dos usuários para restringir o uso mal-intencionado de conteúdo corporativo. No caso de um dispositivo ser perdido ou roubado, você poderá desabilitar, bloquear ou apagar remotamente aplicativos e dados comerciais. O resultado geral é uma solução que aumenta a satisfação e a produtividade dos funcionários, garantindo segurança e controle administrativo.

O foco principal deste artigo são as várias políticas de dispositivos e aplicativos relacionadas à segurança.

Políticas que abordam riscos de segurança

As políticas de dispositivos e aplicativos do XenMobile abordam muitas situações que podem representar um risco de segurança, como:

- Quando os usuários tentam acessar aplicativos e dados de dispositivos não confiáveis e locais imprevisíveis.
- Quando os usuários passam dados de um dispositivo para outro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Quando um usuário não autorizado tenta acessar dados.
- Quando um usuário que saiu da empresa usou seu próprio dispositivo (BYOD).
- Quando um usuário perde um dispositivo.
- Quando os usuários precisam acessar a rede com segurança todo o tempo.
- Quando os usuários têm seu próprio dispositivo gerenciado e você precisa separar os dados de trabalho dos dados pessoais.
- Quando um dispositivo está inativo e requer verificação de credenciais do usuário novamente.
- Quando os usuários copiam e colam conteúdo confidencial em sistemas de e-mail desprotegidos.
- Quando os usuários recebem anexos de e-mail ou links da Web com dados confidenciais em um dispositivo que contém contas pessoais e corporativas.

Essas situações referem-se a duas áreas principais de preocupação ao proteger os dados da empresa, que ocorrem quando os dados estão:

- Em repouso
- Em trânsito

Como o XenMobile protege os dados em repouso

Dados armazenados em dispositivos móveis são vistos como dados em repouso. Os recursos de gerenciamento de aplicativos móveis (MAM) do XenMobile permitem gerenciamento, proteção e controle total de aplicativos móveis de produtividade, aplicativos habilitados para MDX e seus dados associados. O Worx App SDK, que habilita aplicativos para a implantação do XenMobile, aproveita a tecnologia de contêiner do aplicativo Citrix MDX para separar aplicativos e dados corporativos de aplicativos e dados pessoais no dispositivo móvel do usuário. Isso permite que você proteja qualquer aplicativo personalizado desenvolvido, de terceiros ou BYO com controles abrangentes baseados em políticas.

Além de uma extensa biblioteca de políticas MDX, o XenMobile também inclui criptografia em nível de aplicativo. O XenMobile criptografa separadamente os dados armazenados em qualquer aplicativo habilitado para MDX sem exigir um código PIN do dispositivo e sem exigir que você gerencie o dispositivo para impor a política.

Políticas e o SDK do Worx App permitem que você:

- Separe aplicativos e dados comerciais e pessoais em um contêiner móvel seguro.
- Proteja aplicativos com criptografia e outras tecnologias móveis de prevenção contra perda de dados (DLP).

As políticas MDX fornecem muitos controles operacionais, para que você possa ativar a integração perfeita entre aplicativos preparados com MDX e, ao mesmo tempo, controlar toda a comunicação.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dessa forma, você pode impor políticas, de modo a garantir que os dados sejam acessíveis somente por aplicativos habilitados para MDX.

Além do controle de políticas de dispositivos e aplicativos, a melhor maneira de proteger os dados em repouso é a criptografia. O XenMobile adiciona uma camada de criptografia a todos os dados armazenados em um aplicativo habilitado para MDX, oferecendo a você controle de políticas de recursos como criptografia de arquivos públicos, criptografia de arquivos privados e exclusões de criptografia. O SDK do Worx App usa criptografia FIPS 140-2 de compatibildiade AES 256 bits com chaves armazenadas em um Citrix Secret Vault protegido.

Como o XenMobile protege os dados em trânsito

Os dados que se movem entre os dispositivos móveis de seus usuários e sua rede interna são chamados de dados em trânsito. A tecnologia de contêiner de aplicativo MDX fornece acesso VPN específico ao aplicativo para sua rede interna por meio do NetScaler Gateway.

Considere a situação em que um funcionário deseja acessar os seguintes recursos residentes na rede corporativa segura a partir de um dispositivo móvel: o servidor de e-mail corporativo, um aplicativo da Web habilitado para SSL hospedado na intranet corporativa e documentos armazenados em um servidor de arquivos ou no Microsoft SharePoint. O MDX permite o acesso a todos esses recursos corporativos a partir de dispositivos móveis por meio de uma micro VPN específica ao aplicativo. Cada dispositivo tem seu próprio túnel micro VPN dedicado.

A funcionalidade Micro VPN não requer uma VPN de dispositivo, o que pode comprometer a segurança em dispositivos móveis não confiáveis. Como resultado, a rede interna não fica exposta a malwares 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 Gateway NetScaler alternativo, usada para autenticação e para sessões de micro VPN com um aplicativo. Você pode usar um Gateway NetScaler Alternativo com a política necessária para a sessão On-line para forçar os aplicativos a se autenticarem novamente no gateway específico. Esses gateways normalmente têm requisitos de autenticação (maior garantia) e políticas de gerenciamento de tráfego diferentes.

Além dos recursos de segurança, o micro VPN também oferece técnicas de otimização de dados, incluindo algoritmos de compressão para garantir que apenas dados mínimos sejam transferidos e que a transferência seja feita no menor tempo possível, melhorando assim a experiência do usuário, que é um importante fator para o sucesso do projeto.

Você deve reavaliar suas políticas de dispositivo periodicamente, como nessas situações:

- Quando uma nova versão do XenMobile inclui políticas novas ou atualizadas devido ao lançamento de atualizações do sistema operacional do dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Quando você adiciona um novo tipo de dispositivo. Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. Como resultado, você pode encontrar diferenças entre dispositivos iOS, Android e Windows, e até mesmo entre diferentes fabricantes de dispositivos que executam o Android.
- Manter a operação do XenMobile em sincronia com as mudanças na empresa ou do setor, como novas políticas de segurança corporativa ou regulamentos de conformidade.
- Quando uma nova versão do MDX Toolkit inclui políticas novas ou atualizadas.
- Quando você adiciona ou atualiza um aplicativo.
- Quando você precisa integrar novos fluxos de trabalho para seus usuários como resultado de novos aplicativos ou novos requisitos.

Políticas de aplicativos e cenários de casos de uso

Embora você possa escolher quais aplicativos estão disponíveis por meio do Secure Hub, convém também definir como esses aplicativos interagem com o XenMobile. Se você quiser que os usuários se autentiquem após um determinado período de tempo ou se você quiser fornecer aos usuários acesso offline às informações deles, faça isso por meio das políticas do aplicativo. A lista a seguir inclui algumas das políticas e discute como você pode usá-las. Para obter uma lista de todas as políticas de MDX por plataforma, consulte Resumo das políticas do MDX.

Políticas de autenticação

- **Código secreto do dispositivo**

  Por que usar esta política: ative a política de código secreto do dispositivo para garantir que um usuário possa acessar um aplicativo MDX somente se o dispositivo tiver um PIN de dispositivo ativado. Esse recurso, para dispositivos iOS 9, garante o uso de criptografia iOS no nível do dispositivo e para o contêiner MDX.

  Exemplo de usuário: ativar essa política significa que o usuário deve definir um código PIN no dispositivo iOS antes de poder acessar o aplicativo MDX.

- **Código secreto do aplicativo**

  Por que usar esta política: ative a política de senha do aplicativo para que o Secure Hub solicite que um usuário se autentique no aplicativo gerenciado antes que ele possa abrir o aplicativo e acessar os dados. O usuário pode se autenticar com sua senha do Active Directory, PIN da 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 nas Propriedades do Cliente para que, com o uso continuado, o Secure Hub não solicite que o usuário se autentique no aplicativo gerenciado novamente até que o timer expire.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O código secreto do aplicativo difere de um código secreto de dispositivo no sentido que, com uma política de código secreto de dispositivo enviada para um dispositivo, o Secure Hub solicita aos usuários que configurem um código secreto ou PIN, que eles devem desbloquear antes que possam acessar o dispositivo quando ligarem o dispositivo ou quando o timer 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 Citrix PIN antes de poder navegar nos sites se o período de inatividade expirar.

- **Sessão online obrigatória**

  Por que usar esta política: se um aplicativo exigir acesso a um aplicativo da web (serviço da web), ative essa política para que o XenMobile solicite que o usuário se conecte à rede da empresa ou tenha uma sessão ativa antes de usar o aplicativo.

  Exemplo de usuário: quando um usuário tenta abrir um aplicativo MDX com a política necessária para sessão online ativada, 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 as políticas de direito e atualização de aplicativos do XenMobile.

  Exemplo de usuário: se você configurar um aplicativo MDX com um período offline Máximo, o usuário poderá abrir e usar o aplicativo offline até que o período do timer offline expire. Nesse ponto, o usuário deve se conectar novamente à rede por meio do serviço de celular ou Wi-Fi e se autenticar novamente, se solicitado.

Outras Políticas de Acesso

- **Período de tolerância de atualização de aplicativo (horas)**

  Por que usar esta política: o período de tolerância da atualização do aplicativo é o tempo disponível para o usuário antes que ele precise atualizar um aplicativo que tenha uma versão mais recente liberada na XenMobile Store. No momento da expiração, o usuário deve atualizar o aplicativo antes que possa obter acesso aos dados no aplicativo. Ao definir esse valor, lembre-se das necessidades de sua força de trabalho móvel, especialmente daqueles que podem passar longos períodos offline quando viajando internacionalmente.

  Exemplo de usuário: você carrega uma nova versão do Secure Mail na XenMobile Store e, em seguida, define um período de tolerância de atualização do aplicativo de 6 horas. Todos os usuários do Secure Mail verão uma mensagem solicitando a atualização do aplicativo Secure Mail, até que as 6 horas expirem. Quando as 6 horas expirarem, o Secure Hub encaminhará os usuários para a XenMobile Store.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Intervalo ativo de sondagem (minutos)**

  Por que usar esta política: o intervalo ativo de sondagem é o período no qual o XenMobile verifica aplicativos para executar ações de segurança, como o Bloqueio de aplicativos e o Apagamento de aplicativos.

  Exemplo de usuário: se você definir a política Intervalo ativo de sondagem para 60 minutos, quando você enviar o comando de bloqueio de aplicativo do XenMobile para o dispositivo, o bloqueio ocorrerá dentro de 60 minutos a contar de quando a última pesquisa foi realizada.

Políticas de criptografia

Por que usar estas políticas: o XenMobile inclui um cofre secreto com uma camada de criptografia forte que o Secure Hub e outros aplicativos móveis de produtividade usam para manter seus dados confidenciais, como senhas e chaves de criptografia, no dispositivo sem depender de keystores nativos da plataforma. Como resultado, se o dispositivo ficar comprometido de alguma forma, os dados corporativos permanecerão criptografados no contêiner MDX e o XenMobile ofuscará os dados antes de transferi-los para fora do contêiner.

Exemplo de usuário: se o proprietário do dispositivo não definiu um PIN do dispositivo ou o PIN do dispositivo foi comprometido, os dados corporativos dentro do contêiner do Secure Hub permanecem seguros.

Políticas de interação de aplicativos

Por que usar essas políticas: use 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 nos aplicativos em contêineres.

Exemplo de usuário: você define uma política de interação de aplicativos como Restrito, o que significa que um usuário pode copiar texto do Secure Mail para o Secure Web, mas não pode copiar esses dados para o navegador pessoal Safari ou Chrome que está fora do contêiner. Além disso, um usuário pode abrir um documento anexado do Secure Mail no ShareFile ou no Quick Edit, mas não pode abrir o documento anexado em seus próprios aplicativos de visualização de arquivo pessoal 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 a partir de um aplicativo MDX enquanto ele estiver aberto. Isso ajuda

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a garantir que nenhuma atividade maliciosa ocorra enquanto o aplicativo estiver em execução. As políticas de restrição de aplicativos variam ligeiramente entre o iOS e o 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 estiver em execução.

Exemplo de usuário: se você ativar a política de restrição de aplicativos para bloquear o ditado no iOS em um aplicativo MDX, o usuário não poderá usar a função ditar no teclado do iOS enquanto o aplicativo MDX estiver em execução. Assim, o ditado dos usuários de dados não é passado para o serviço de ditado de nuvem de terceiros desprotegido. 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 do aplicativo

Por que usar essas políticas: use as políticas de acesso à rede do aplicativo para fornecer acesso a partir de um aplicativo MDX no contêiner do dispositivo a dados localizados dentro de sua rede corporativa. Para a política de acesso à rede, defina a opção **Com túnel para a rede interna** para automatizar uma micro VPN a partir do aplicativo MDX por meio do NetScaler para um serviço da web de backend ou armazenamento de dados.

Exemplo de usuário: quando um usuário abre um aplicativo MDX, como o Secure Web, que tem o encapsulamento ativado, o navegador abre e inicia um site de intranet sem que o usuário precise iniciar uma VPN. O aplicativo Secure Web acessa automaticamente o site interno usando a tecnologia micro VPN.

Políticas de geolocalização e geocerca do aplicativo

Por que usar essas políticas: as políticas que controlam a geolocalização e a delimitação geográfica de aplicativos incluem a longitude do ponto central, a latitude do ponto central e o raio. Essas políticas contêm acesso aos dados nos aplicativos MDX para 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 fusão e aquisição enquanto está na localidade do escritório. Quando sai a localidade do escritório, esses dados confidenciais ficam inacessíveis.

Políticas do Aplicativo Secure Mail

- **Serviços de rede em segundo plano**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por que usar esta política: os serviços de rede em segundo plano no Secure Mail utilizam STA (Secure Ticket Authority), que é efetivamente um proxy SOCKS5 para conexão através do NetScaler Gateway. O STA suporta conexões de longa duração e oferece melhor duração da bateria em comparação com a micro VPN. Assim, o STA é ideal para correios que se conectam constantemente. A Citrix recomenda que você defina essas configurações para o Secure Mail. O assistente NetScaler for XenMobile configura automaticamente o STA para Secure Mail.

Exemplo de usuário: quando a STA não está habilitada e um usuário do Android abre o Secure Mail, ele é solicitado a abrir uma VPN, que permanece aberta no dispositivo. Quando o STA está habilitado e o usuário do Android abre o Secure Mail, o Secure Mail conecta-se sem precisar de VPN.

- **Intervalo de sincronização padrão**

  Por que usar esta política: essa configuração especifica os dias padrão de email que são sincronizados com o Secure Mail quando o usuário acessa o Secure Mail pela primeira vez. Esteja ciente de que duas semanas de e-mail demoram mais para sincronizar do que três dias e prolongam o processo de configuração do usuário.

  Exemplo de usuário: se o intervalo de sincronização padrão for definido como 3 dias quando o usuário configurar pela primeira vez o Secure Mail, ele poderá ver todos os e-mails na Caixa de entrada que recebeu da data presente até três dias anteriores. Se um usuário quiser ver e-mails de mais de três dias atrás, ele poderá fazer uma busca. O Secure Mail mostra os e-mails mais antigos armazenados no servidor. Depois de instalar o Secure Mail, cada usuário pode alterar essa configuração para melhor atender às suas necessidades.

Políticas de dispositivo e comportamento do caso de uso

As políticas de dispositivo, às vezes chamadas de políticas de MDM, determinam como o XenMobile funciona com dispositivos. Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. A lista a seguir inclui algumas das políticas do dispositivo e discute como você pode usá-las. Para obter uma lista de todas as políticas de dispositivos, 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 os aplicativos instalados pessoalmente. Você deve usar esta política se quiser colocar na lista negra determinados aplicativos em execução em dispositivos corporativos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exemplo de usuário: um usuário com um dispositivo gerenciado pelo MDM não pode desativar essa funcionalidade. Os aplicativos instalados pelo usuário ficam visíveis para os administradores do XenMobile.

- **Política de bloqueio de aplicativo**

  Por que usar essa política: a política de Bloqueio de aplicativos, para Android, permite que você coloque aplicativos na lista negra ou na lista branca. Por exemplo, ao colocar aplicativos na lista branca, você pode configurar um dispositivo de quiosque. Normalmente, você implanta a política de bloqueio de aplicativos somente em dispositivos de propriedade corporativa, pois limita os aplicativos que os usuários podem instalar. Você pode definir uma senha de substituição para fornecer acesso de usuário a aplicativos bloqueados.

  Exemplo de usuário: suponha que você implemente uma política de bloqueio de aplicativo que bloqueie o aplicativo Angry Birds. O usuário pode instalar o aplicativo Angry Birds no Google Play, mas quando ele abre o aplicativo, uma mensagem avisa 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 dispositivos Android e Windows Mobile possam se conectar de volta ao XenMobile para gerenciamento de MDM, envio de aplicativo e implantação de políticas. Se você não implantar essa política e não tiver ativado o FCM (Firebase Cloud Messaging) do Google, os dispositivos não se conectarão novamente ao XenMobile. É importante implantar essa política no pacote base para registrar dispositivos. As opções de agendamento são as seguintes:

  - **Sempre:** mantém a conexão ativa de forma permanente. A Citrix recomenda esta opção para segurança otimizada. Quando você escolher **Sempre**, use também a política de timer de conexão para garantir que a conexão não esteja esgotando a bateria. Ao manter a conexão ativa, você pode enviar comandos de segurança por push, como apagar ou bloquear o dispositivo sob demanda. Você também deve selecionar a opção do Cronograma de implantação **Implantar para conexão permanente** em cada política implantada no dispositivo.
  - **Nunca:** conecta-se manualmente. A Citrix não recomenda essa opção para implantações de produção, pois a opção **Nunca** impede que você implante políticas de segurança nos dispositivos; portanto, os usuários nunca recebem novos aplicativos ou políticas.
  - **A cada:** conecta-se no intervalo designado. Quando essa opção está em vigor e você envia uma política de segurança, como um bloqueio ou um apagamento, o XenMobile processa a política no dispositivo na próxima vez em que ele se conectar.
  - **Definir programação:** quando ativada, o XenMobile tenta se reconectar o dispositivo do usuário ao XenMobile Server após uma perda de conexão de rede e monitora a conexão

© 1999-2019 Citrix Systems, Inc. All rights reserved.

mediante a transmissão de pacotes de controle em intervalos regulares no período de tempo que você definir.

Exemplo de usuário: você deseja implantar uma política de código secreto para dispositivos registrados. A política de agendamento garante que os dispositivos se conectem novamente ao servidor em um intervalo regular para coletar a nova política.

- **Política de credenciais**

  Por que usar esta política: geralmente usada em conjunto com uma política WiFi, a política de Credenciais permite que você implante certificados para autenticação em recursos internos que exigem autenticação de 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 implementa um certificado que é armazenado no keystore do sistema operacional. O usuário pode então selecionar o certificado quando conectado ao recurso interno.

  - **Política do Exchange**

  Por que usar esta política: com o XenMobile, você tem duas opções para entregar e-mails do Microsoft Exchange ActiveSync.

  - **Aplicativo Secure Mail:** entregue e-mails usando o aplicativo Secure Mail que você distribui da loja de aplicativos pública ou da XenMobile Store.
  - **Aplicativo de e-mal nativo:** use a política do Exchange para habilitar e-mail do 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 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: quando você envia a política do Exchange, envia detalhes do Exchange Server para o dispositivo. O Secure Hub, em seguida, solicita que o usuário se autentique e o e-mail começa a ser sincronizado.

- **Política de localização**

  Por que usar esta política: a política de localização permite localizar geograficamente dispositivos em um mapa, se o dispositivo tiver o GPS ativado para o Secure Hub. Depois de implantar essa política e enviar um comando locate do XenMobile Server, o dispositivo responde com as coordenadas de localização.

  Exemplo de usuário: quando você implanta a política de localização e o GPS está habilitado no dispositivo, se os usuários perderem o dispositivo, eles poderão fazer logon no Portal de Autoatendimento do XenMobile e escolher a opção locate para ver a localização do dispositivo em um mapa. Observe que o usuário opta por permitir que o Secure Hub use os serviços de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

localização. Você não pode impor o uso de serviços de localização quando os usuários registram um dispositivo. Outra consideração para usar esta política é o efeito na duração da bateria.

- **Política de código secreto**

  Por que usar esta política: a política de código secreto permite que você imponha um código PIN ou senha em um dispositivo gerenciado. Essa política permite definir a complexidade e os tempos limite do código secreto no dispositivo.

  Exemplo de usuário: quando você implementa uma política de código secreto para um dispositivo gerenciado, o Secure Hub solicita aos usuários que configurem um código secreto ou PIN, que eles devem desbloquear antes que possam acessar o dispositivo quando ligarem o dispositivo ou quando o timer de inatividade expirar.

- **Política de remoção de perfil**

  Por que usar esta política: suponha que você implemente uma política para um grupo de usuários e, posteriormente, precise remover essa política de um subconjunto de usuários. Você pode remover a política dos usuários selecionados criando uma política de remoção de perfil e usando regras de implantação para implementar a política de remoção de perfil apenas a nomes de usuário especificados.

  Exemplo de usuário: quando você implanta 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 desativou a câmera do dispositivo, o usuário não saberá que o uso da câmera agora é permitido. Considere informar os usuários quando as alterações afetarem a experiência do usuário.

- **Política de restrições**

  Por que usar esta política: a política de restrição dá a você muitas opções para bloquear e controlar os recursos e as funcionalidades no dispositivo gerenciado. Você pode habilitar centenas de opções de restrição para permitir que os dispositivos compatíveis desativem a câmera ou o microfone em um dispositivo para aplicar as regras de roaming e o 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 loja do iTunes.

- **Política de termos e condições**

  Por que usar esta política: você talvez precise informar os usuários sobre as implicações legais de terem seus dispositivos gerenciados. Além disso, convém garantir que os usuários estejam cientes dos riscos de segurança quando os dados corporativos são enviados para o dispositivo. O documento Termos e Condições personalizado permite publicar regras e avisos antes de o usuário se registrar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exemplo de usuário: um usuário vê as informações dos Termos e Condições durante o processo de registro. Caso se recuse a aceitar as condições declaradas, o processo de registro terminará e o usuário 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 a tecnologia de gateway de VPN mais antiga. A política suporta um número de provedores de VPN, incluindo Cisco AnyConnect, Juniper, bem como Citrix VPN. Também é possível vincular essa política a uma CA e à VPN ativada sob demanda (se o gateway VPN oferecer suporte a essa opção).

  Exemplo de usuário: com a política de VPN ativada, o dispositivo de um usuário abre uma conexão VPN quando o usuário acessa um domínio interno.

- **Política de clip web**

  Por que usar esta política: use a política de clip Web se você quiser enviar para os dispositivos um ícone que seja aberto diretamente para um site. Um clip web contém um link para um site e pode incluir um ícone personalizado. Em um dispositivo, um clip web parece um ícone de aplicativo.

  Exemplo de usuário: um usuário pode clicar em um ícone de clip web para abrir um site da Internet que fornece serviços que precisa 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 WiFi**

  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: quando você implanta 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 se proteger contra o possível vazamento de dados corporativos. Você pode especificar os aplicativos que requerem Proteção de informações do Windows no nível de execução que você definir. Por exemplo, você pode bloquear compartilhamentos de dados inadequados ou avisar sobre um compartilhamento de dados adequado e permitir que os usuários substituam a política. Você pode executar o WIP silenciosamente enquanto registra o log e permite o compartilhamento de dados inadequado.

  Exemplo de usuário: suponha que você configure a política de WIP para bloquear o compartilhamento de dados inadequado. Se um usuário copiar ou salvar um arquivo protegido em um

© 1999-2019 Citrix Systems, Inc. All rights reserved.

local não protegido, será exibida uma mensagem semelhante à seguinte: Não é possível colocar conteúdo protegido de trabalho neste local.

- **Política XenMobile Store**

  Por que usar esta política: a XenMobile Store é uma loja de aplicativos unificada, na qual os administradores podem publicar todos os aplicativos corporativos e recursos de dados necessários para seus usuários. Um administrador pode adicionar aplicativos Web, aplicativos SaaS, aplicativos preparados MDX, aplicativos de produtividade Citrix, aplicativos móveis nativos, como arquivos .ipa ou .apk, aplicativos de reprodução iTunes e Google, links da Web e aplicativos XenApp e XenDesktop publicados usando o Citrix StoreFront.

  Exemplo de usuário: depois que um usuário registra seu dispositivo no XenMobile, ele acessa a XenMobile Store por meio do aplicativo Citrix Secure Hub. O usuário pode 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, além de baixar as atualizações de aplicativos da XenMobile Store.

Opções de registro do usuário

April 15, 2019

Você pode fazer com que os usuários registrem seus dispositivos no XenMobile de várias maneiras. Antes de considerar os detalhes, você deve decidir se os dispositivos em seu ambiente serão registrados no modo Empresarial (MDM+MAM), no modo MDM ou no modo MAM (também conhecido como modo somente MAM). Para obter mais informações sobre os 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 um link de convite aos usuários.
- **Portal de autoajuda:** configure um portal que os usuários possam visitar para fazer o download do Secure Hub e registrar seus dispositivos ou enviar um convite de registro a eles mesmos.
- **Registro manual:** envie um e-mail, manual ou alguma outra comunicação informando aos usuários que o sistema está ativo e que eles podem se registrar. Os usuários então baixam o Secure Hub e registram seus dispositivos manualmente.
- **Empresarial:** outra opção para o registro de dispositivos é por meio do Programa de Registro de Dispositivos da Apple (DEP) e do Google Android for Work. Por meio de cada um desses programas, você pode comprar dispositivos pré-configurados e prontos para o uso pelos funcionários. Para obter mais informações, consulte Device Enrollment Program (DEP) da Apple e Google Android for Work.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Convite para registro

Você pode enviar um convite para registro por e-mail para usuários com dispositivos iOS, macOS ou Android. Você também pode enviar um link de instalação por SMTP ou SMS aos usuários com dispositivos iOS, macOS, Android, ou Windows. Para obter mais informações, consulte Registrar dispositivos.

Se você optar por usar o método de convite para registro, poderá escolher entre sete modos de registro (dependendo da plataforma) e poderá usar qualquer combinação dos modos. Você pode ativar ou desativar os modos na página Configurações do XenMobile e selecionar um padrão, entre Nome de usuário + Senha, Dois fatores e Nome de usuário + PIN. Para obter informações sobre cada modo de registro, consulte Para configurar modos de registro.

Se você escolher baseado em certificado, considere a exclusão da autenticação convencional Nome de usuário + Senha das opções permitidas, pois esse modo pode expor um vetor de integração fraco em seu ambiente e possivelmente anular a qualidade de segurança obrigatória.

Convites servem a muitos propósitos. O uso mais comum de convites é notificar os usuários de que o sistema está disponível e que eles podem se registrar. URLs de convite são exclusivas: quando um usuário usa uma URL de convite, a URL não pode ser usada novamente. Você pode usar essa propriedade para limitar o registro de usuários ou dispositivos em seu sistema.

Você pode configurar o XenMobile para que os usuários do iOS forneçam credenciais durante o registro de uma das seguintes maneiras:

- Os usuários digitam suas credenciais durante o registro.
- Os usuários inserem um cartão inteligente de um provedor de credenciais derivadas em um leitor conectado à área de trabalho. Para obter informações sobre credenciais derivadas, consulte Credenciais derivadas.

No console XenMobile, você também pode escolher a opção para Perfis de Rergistro, através da qual você pode controlar o número de dispositivos que os usuários específicos podem registrar, com base nos grupos do Active Directory. Por exemplo, se você quiser permitir à sua divisão de Finanças apenas um dispositivo por usuário, poderá configurar esse cenário por meio de perfis de registro.

Esteja ciente dos custos extras e dos imprevistos de certas opções de registro. Se você quiser enviar convites usando o SMS, precisará configurar uma infraestrutura adicional. Para obter mais informações sobre essa opção, consulte Notificações.

Além disso, se você planeja enviar convites por e-mail, verifique se os usuários têm uma maneira de acessar e-mails fora do Secure Hub. Você pode usar os modos de registro de senha única (OTP) como uma alternativa às senhas do Active Directory para registro no MDM. Observe que o OTP está disponível apenas em dispositivos iOS e Android e não está disponível atualmente em dispositivos Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Portal de Autoajuda

Os usuários podem solicitar um convite de registro através do Portal de Autoajuda. O modo padrão é Nome de usuário + Senha, mas você também pode alterar esse requisito para Dois fatores ou Nome de usuário + PIN. Para obter informações sobre como configurar o Portal de Autoajuda, consulte Para configurar modos de registro.

Registro manual

Com o registro manual, os usuários se conectam ao XenMobile por meio da descoberta automática ou inserindo as informações do servidor. Com a descoberta automática, os usuários fazem login no servidor apenas com o endereço de email ou com as credenciais do Active Directory no formato Nome Principal do Usuário. Sem a descoberta automática, eles devem inserir o endereço do servidor e suas credenciais do Active Directory. Para obter mais informações sobre como configurar a descoberta automática, consulte XenMobile Autodiscovery Service.

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. O seu departamento de TI pode registrar os grupos de usuários manualmente em determinados intervalos de tempo. Você pode usar qualquer método semelhante no qual os usuários devem inserir suas credenciais e/ou informações do servidor.

Integração de usuários

Depois de configurar seu ambiente, você precisa decidir como colocar os usuários nesse ambiente. Uma seção anterior deste artigo discute as especificidades dos modos de registro do usuário. Esta seção discute como você chega aos usuários.

Registro aberto versus Convite seletivo

Ao integrar os usuários, você pode permitir o registro por meio de dois métodos básicos: o registro aberto, no qual, por padrão, qualquer usuário com credenciais LDAP e as informações do ambiente XenMobile pode se registrar. Ou você pode limitar o número de usuários permitindo apenas que os usuários com convites se registrem. Você também pode limitar o registro aberto pelo 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 serem consideradas:

- Se você estiver implantado um ambiente MAM, poderá limitar facilmente o registro por meio da associação ao grupo do Active Directory.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Em um ambiente MDM, a única maneira de limitar o registro é limitar o número de dispositivos que podem se registrar com base na associação do grupo do Active Directory. Se você permitir apenas dispositivos corporativos em seu ambiente, isso não será um problema. Contudo, você pode considerar esse método em um local de trabalho BYOD em que deseje limitar o número de dispositivos em seu ambiente.
- Você também deve considerar se terá licenças de usuário ou dispositivo. Com licenças de usuário, cada usuário pode ter vários dispositivos e apenas uma licença é consumida. Com licenças de dispositivo, cada dispositivo registrado consome uma licença.

Geralmente, o convite seletivo é realizado com menos frequência porque requer 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 convite para registro.

Você precisará enviar um convite para cada usuário ou grupo que desejar registrar em seu ambiente, o que pode levar muito tempo, dependendo do tamanho da sua organização. É possível usar grupos do Active Directory para criar convites em lotes, mas você deve executar essa abordagem de forma incremental.

Primeiro contato com os usuários

Depois de decidir se deseja usar registro aberto ou convite seletivo e configurar esses ambientes, você precisará informar os usuários sobre as opções de registro.

Se você usar o método de convite seletivo, as mensagens de e-mail e SMS farão parte do processo. Você também pode enviar e-mails através do console XenMobile para registro aberto. Para obter detalhes, consulte Envio de convite para registro.

Em ambos os casos, lembre-se de que, para email, você precisa de um servidor SMTP. Para mensagens de texto, você precisa de um servidor SMS. Esses podem incorrer em custos extras a serem considerados ao tomar sua decisão. Além disso, antes de selecionar um método, considere como você espera que novos usuários acessem informações, como email. Se você quiser que todos os usuários acessem seus emails através do XenMobile, enviar um convite por e-mail seria problemático.

Você também pode enviar uma comunicação por outro meio fora do XenMobile para um ambiente de registro aberto, desde que inclua todas as informações relevantes, como onde os usuários podem obter o aplicativo do Secure Hub e qual método eles devem usar para se registrar. Se você tiver a descoberta automática desativada, precisará informar também o endereço do XenMobile Server. Para saber mais sobre a descoberta automática, consulte XenMobile Autodiscovery Service.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ajuste das operações do XenMobile

April 15, 2019

O desempenho e a estabilidade das operações do XenMobile envolvem muitas configurações no XenMobile e dependem da configuração do banco de dados do NetScaler e do SQL Server. Este artigo enfoca nas configurações mais frequentemente definidas pelos administradores, relacionadas ao ajuste e à otimização do XenMobile. A Citrix recomenda que você avalie cada uma das configurações deste artigo antes de implantar o XenMobile.

> Importante:
>
> Essas diretrizes pressupõem que a CPU e a RAM do XenMobile Server são adequadas para o número de dispositivos. Para obter mais informações sobre escalabilidade, consulte Escalabilidade e desempenho.

As seguintes propriedades do servidor se aplicam globalmente a operações, usuários e dispositivos a uma instância inteira do XenMobile. A alteração em algumas propriedades do servidor requer uma reinicialização de cada nó do XenMobile Sever. O XenMobile avisa quando uma reinicialização é necessária.

Essas diretrizes de ajuste se aplicam a ambientes em cluster e não-cluster.

hibernate.c3p0.idle_test_period

Essa propriedade do XenMobile Server, uma chave personalizada, determina o tempo ocioso em segundos antes de uma conexão ser validada automaticamente. Configure a chave da seguinte maneira. O padrão é **30**.

- Chave: **chave personalizada**
- Chave: **hibernate.c3p0. idle_test_period**
- Valor: **30**
- Nome de exibição: **hibernate.c3p0. idle_test_period**
- Descrição: **período de teste de inatividade de hibernação**

hibernate.c3p0.max_size

Essa chave personalizada determina o número máximo de conexões que o XenMobile pode abrir no banco de dados do SQL Server. O XenMobile usa o valor especificado para esta chave personalizada como um limite superior. As conexões abrem somente se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Observe a seguinte equação em uma configuração em cluster. Sua conexão c3p0 multiplicada pelo número de nós é igual ao número máximo real de conexões que o XenMobile pode abrir para o banco de dados do SQL Server.

Na configuração em cluster e não-cluster, definir um valor muito alto com um SQL Server subdimensionado pode causar problemas de recursos no lado do SQL durante o pico de carga. Configurar um valor muito baixo poderá afetar o bom-aproveitamento dos recursos SQL disponíveis.

Configure a chave da seguinte maneira. O padrão é **1000**.

- Chave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nome de exibição: **hibernate.c3p0.max_size**
- Descrição: conexões de banco de dados com o SQL

hibernate.c3p0.min_size

Essa chave personalizada determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. Configure a chave da seguinte maneira. O padrão é **100**.

- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de exibição: **hibernate.c3p0.min_size**
- Descrição: conexões de banco de dados com o SQL

hibernate.c3p0.timeout

Essa chave personalizada determina o tempo limite de ociosidade. Se você usar o failover de cluster do banco de dados, a Citrix recomenda que você adicione essa chave personalizada e defina-a para reduzir o tempo limite de inatividade. 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

Intervalo de pulsação de serviços push

Esta configuração determina com que frequência um dispositivo iOS verifica se uma notificação de APNs não foi entregue nesse ínterim. Aumentar a freqüência de pulsação dos APNs pode otimizar as

© 1999-2019 Citrix Systems, Inc. All rights reserved.

comunicações do banco de dados. Um valor muito grande pode adicionar carga desnecessária. Essa configuração se aplica apenas ao iOS. O padrão é **20** horas.

Se você tiver vários dispositivos iOS em seu ambiente, o intervalo de pulsação pode levar a uma carga maior do que a necessária. As ações de segurança, como apagamento seletivo, bloqueio e apagamento completo, não dependem dessa pulsação. O motivo é que uma notificação de APNs é enviada ao dispositivo quando essas ações são executadas. Esse valor determina a rapidez com que uma política é atualizada depois que a associação ao Grupo do Active Directory é alterada. Como tal, muitas vezes é adequado aumentar esse valor para algo entre 12 e 20 horas para reduzir a carga.

Tamanho do pool de conexões APNS de iOS MDM

Um pool de conexões APNs muito pequeno pode afetar negativamente o desempenho das atividades de APNs quando você tem mais de 100 dispositivos. Os problemas de desempenho incluem a implantação mais lenta de aplicativos e políticas em dispositivos e o registro mais lento de dispositivos. A configuração recomendada é **10** ou até o número máximo de servidores APNs para sua localização geográfica. O padrão é **10**.

auth.ldap.connect.timeout

Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do 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 da conexão LDAP**

auth.ldap.read.timeout

Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do servidor para as seguintes chaves personalizadas.

- Chave: **chave personalizada**
- Chave: **auth.ldap.read.timeout**
- Valor: **60000**
- Nome de exibição: **auth.ldap.read.timeout**
- Descrição: **tempo limite de leitura do LDAP**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Outras otimizações de servidores

Propriedade do servidor	Configuração padrão	Por que mudar essa configuração?
Implementação em segundo plano	1.440 minutos	A frequência de implantações de políticas em segundo plano, em minutos. Aplica-se apenas a conexões permanentes de dispositivos Android. Aumentar a frequência de 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 do inventário de hardware em segundo plano, em minutos. Aplica-se apenas a conexões permanentes de dispositivos Android. Aumentar a frequência do inventário de hardware reduz a carga do servidor. A configuração recomendada é **1440** (24 horas).
Intervalo para verificação de usuário do Active Directory excluído	15 minutos	O tempo de sincronização padrão do Active Directory é de **15** minutos. O valor **0** impede que o XenMobile verifique usuários do Active Directory excluídos. A configuração recomendada é de **15** minutos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

MaxNumberOfWorker	3	O número de threads utilizados ao importar um várias licenças VPP. O padrão é **3**. Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, lembre-se de que com um número maior de threads, como 6, uma importação VPP resulta em uso de CPU alto.

Otimizar o Agendamento de Implantação para dispositivos Android

Você pode programar implantações para dispositivos Android usando as configurações do Google Firebase Cloud Messaging (FCM, anteriormente chamado Google Cloud Messaging).

A ativação do FCM para seu ambiente XenMobile permite notificações quase em tempo real a dispositivos Android, semelhante a de APNs a dispositivos iOS. Com o FCM configurado, quando o XenMobile precisa se conectar a um dispositivo para uma atualização de política, apagamento seletivo e assim por diante, o XenMobile Server envia uma mensagem de notificação ao servidor FCM para encaminhar a solicitação ao dispositivo cliente. Depois que o dispositivo recebe a notificação do FCM, o dispositivo se conecta de volta ao XenMobile para obter mais instruções. Lembre-se de que esse método depende de servidores de terceiros (Google) e, portanto, está sujeito a interrupções de serviço fora do controle de seu departamento de TI ou do Suporte Citrix.

Para obter informações sobre como se registrar no serviço FCM, consulte Configuração do XenMobile e Firebase Cloud Messaging (FCM).

Se estiver usando o FCM para Android, esteja ciente das seguintes propriedades do XenMobile Server. As propriedades ainda usam o acrônimo anterior para o Google Cloud Messaging, GCM.

- **GCM API Key:** a chave criada no Google Developers Console.
- **GCM Sender ID:** o número do projeto no Google Developers Console.
- **GCM Registration ID TTL:** o atraso, em dias, antes da renovação da ID de registro do FCM do dispositivo. O padrão é **10**.
- **GCM Heartbeat Interval:** o padrão é **6** horas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Como verificar deadlocks em um banco de dados SQL e excluir dados históricos

Quando você vir deadlocks, execute a consulta a seguir para ver os deadlocks. Depois, 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
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
34
35 GO
```

Para limpar o banco de dados

> Importante:
>
> Faça backup do banco de dados antes de fazer alterações nas tabelas.

1. Execute a consulta a seguir para verificar os dados históricos.

```
1 select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
2 select COUNT(\*) as total_record from dbo.EWSESS;
3 select COUNT(*) as total_record from dbo.EWAUDIT;
```

2. Exclua os dados das três tabelas anteriores.

> Nota:
>
> Você talvez não possa ver dados históricos em uma tabela. Em caso afirmativo, ignore a execução da consulta truncada dessa tabela específica.

```
1 truncate TABLE dbo.EWDEPLOY_HISTO;
2 truncate TABLE dbo.EWSESS;
3 truncate TABLE dbo.EWAUDIT;
```

3. Desbloquear as consultas SELECT que foram bloqueadas devido a deadlocks. Essa etapa cuida de mais deadlocks.

```
1 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 os dados de retenção de sessão e os dados de 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:

```
1 zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
2 zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
3 zdm.dbcleanup.auditRetentionTimeInDays=1 day
```

Provisionamento e desprovisionamento de aplicativos

April 15, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

O provisionamento de aplicativos gira em torno do gerenciamento do ciclo de vida de aplicativos móveis, que consiste principalmente em agrupar, configurar, entregar e gerenciar aplicativos móveis em um ambiente XenMobile. Em alguns casos, desenvolver ou modificar o código do aplicativo também pode fazer parte do processo de provisionamento. O XenMobile está equipado com várias ferramentas e processos que você pode usar para provisionamento de aplicativos.

Antes de ler este artigo sobre o provisionamento de aplicativos, é recomendável ler os artigos sobre Aplicativos e Comunidades do usuário. Depois de finalizar o tipo de aplicativos que sua organização planeja fornecer aos usuários, você pode descrever o processo de gerenciamento dos aplicativos em todo o ciclo de vida.

Considere os seguintes pontos ao definir seu processo de provisionamento de aplicativo:

- **Perfil de aplicativo:** sua organização pode começar com um número limitado de aplicativos. No entanto, o número de aplicativos gerenciados pode aumentar rapidamente conforme as taxas de adoção dos usuários aumentam e o ambiente se expande. Você deve definir perfis de aplicativos específicos desde o início para facilitar o gerenciamento do provisionamento de aplicativos. O perfil do aplicativo ajuda você a categorizar aplicativos em grupos lógicos de uma perspectiva não técnica. Por exemplo, você pode criar perfis de aplicativos com base nos seguintes fatores:
  - Versão: versão do aplicativo para acompanhamento
  - Instâncias: várias instâncias implantadas para diferentes conjuntos de usuários, por exemplo, com diferentes níveis de acesso
  - Plataforma: iOS, Android ou Windows
  - Público-alvo: usuários padrão, departamentos, executivos de nível C
  - Propriedade: departamento que possui o aplicativo
  - Tipo: MDX, Público, Web e SaaS ou links da Web
  - Ciclo de atualização: com que frequência o aplicativo é atualizado
  - Licenciamento: requisitos de licenciamento e propriedade
  - Políticas MDX: preparadas ou não preparadas com políticas de segurança MDX
  - Acesso à rede: tipo de acesso, como Secure Browse ou VPN completa

    > Nota:
    > Com túnel - SSO de Web é o nome do Secure Browse nas configurações de MDX. O comportamento é o mesmo.

Exemplo:

Fator	Secure Mail	Email	In-House	Epic Rover
Versão	10.1	10.1	X.x	X.x
Instância	VIP	Médicos	Clínico	Clínico
Plataforma	iOS	iOS	iOS	iOS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Fator	Secure Mail	Email	In-House	Epic Rover
Usuários-alvo	Usuários VIP	Médicos	Usuários Clínicos	Usuários Clínicos
Propriedade	IT	IT	IT	IT
Digite	MDX	MDX	Nativo	Público
Ciclo de Atualização	Trimestral	Trimestral	Anual	N/D
Licenciamento	N/D	N/D	N/D	VPP
Políticas de MDX	Sim	Sim	Sim	Não
Acesso à rede	VPN	VPN	VPN	Público

- **Versão de aplicativos:** manter e acompanhar versões de aplicativos é uma parte crítica do processo de provisionamento. O controle de versão é geralmente transparente para os usuários. Eles só recebem notificações quando uma nova versão do aplicativo está disponível para download. Do seu ponto de vista, revisar e testar cada versão do aplicativo na condição de não produção também é fundamental para evitar o impacto na produção.

  Também é importante avaliar se uma atualização específica é realmente necessária. As atualizações de aplicativos geralmente são de dois tipos: o primeiro tipo é uma atualização secundária, como a correção de um bug específico; o segundo tipo é uma atualização principal, que introduz mudanças significativas e melhorias no aplicativo. Em ambos os casos, você deve revisar cuidadosamente as notas de versão do aplicativo para avaliar se a atualização é necessária.

- **Assinatura e preparação de aplicativos:** com o XenMobile, você pode usar políticas de MDX com aplicativos gerenciados para proteger os dados corporativos por meio da preparação de aplicativos. Para obter mais informações sobre o MDX Toolkit para a preparação de aplicativo, consulte MDX Toolkit na documentação do XenMobile. O processo de provisionamento de aplicativo para um aplicativo preparado é significativamente diferente do processo de provisionamento de um aplicativo padrão não preparado.

- **Segurança do aplicativo:** você define os requisitos de segurança de aplicativos individuais ou perfis de aplicativos como parte do processo de provisionamento. Você pode mapear os requisitos de segurança para políticas MDM ou MAM específicas antes de implantar os aplicativos, o que simplifica e acelera bastante a implantação de aplicativos. Você pode implantar determinados aplicativos de maneira diferente ou talvez precise fazer alterações de arquitetura em seu ambiente XenMobile dependendo do tipo de conformidade de segurança exigida pelos aplicativos. Por exemplo, você pode querer que o dispositivo seja criptografado para permitir o uso de um aplicativo crítico de business intelligence, ou um determinado aplicativo pode exigir criptografia SSL de ponta a ponta ou geocerca.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Entrega de aplicativos:** o XenMobile permite entregar aplicativos como aplicativos MDM ou como aplicativos MAM. Os aplicativos MDM aparecem na XenMobile Store. Essa loja permite entregar aplicativos públicos ou nativos aos usuários sem o controle do aplicativo, exceto impor restrições no nível do dispositivo. Por outro lado, o modo MAM de entregar aplicativos permite controle total sobre a entrega de aplicativos e sobre o próprio aplicativo. Entregar os aplicativos no modo MAM é mais adequado na maioria dos casos em que você tem uma implantação local do XenMobile com requisitos de gerenciamento de aplicativos juntamente com o MDM. Quando você entrega aplicativos no modo MAM, o dispositivo móvel deve ser registrado no modo XME (MDM+MAM) ou somente MAM.
- **Manutenção de aplicativos:**
  - Realize uma auditoria inicial: você deve acompanhar a versão do aplicativo que está presente em seu ambiente de produção, bem como o último ciclo de atualização. Anote os recursos específicos ou as correções de bugs que exigiram a atualização.
  - Estabelecer linhas de base: você deve manter uma lista da versão estável mais recente de cada aplicativo. Essa versão do aplicativo deve ser reativada no caso de ocorrerem problemas inesperados após a atualização. Você também deve desenvolver um plano de reversão. Você deve testar atualizações de aplicativos em um ambiente de teste antes de sua implantação em produção: se possível, você deve primeiro implantar a atualização a um subconjunto de usuários em produção e depois a toda a base de usuários.
  - Inscreva-se para receber as notificações de atualização de software da Citrix e as notificações dos fornecedores de softwares de terceiros: isso é essencial para manter-se atualizado com a versão mais recente dos aplicativos. Em alguns casos, uma compilação de versão de acesso antecipado (EAR) também pode estar disponível para testar antecipadamente.
  - Conceba uma estratégia para notificar usuários: você deve definir uma estratégia para notificar os usuários quando as atualizações de aplicativos estiverem disponíveis. Prepare os usuários com treinamento antes da implantação. Você pode enviar várias notificações antes de atualizar os aplicativos. Dependendo do aplicativo, o melhor método de notificação será notificações por email ou sites.

O gerenciamento do ciclo de vida do aplicativo representa o ciclo de vida completo de um aplicativo desde sua implantação inicial até a desativação do aplicativo. O ciclo de vida de um aplicativo pode ser dividido nestas cinco fases:

1. Requisitos para especificações: comece com o caso de negócios e os requisitos do usuário.
2. Desenvolvimento: valide se o aplicativo atende às necessidades de negócios.
3. Teste: identifique usuários de teste, problemas e bugs.
4. Implantação: implante o aplicativo para usuários em produção.
5. Manutenção: atualize a versão do aplicativo. Implante o aplicativo em um ambiente de teste antes de atualizar o aplicativo em um ambiente de produção.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Exemplo de ciclo de vida do aplicativo usando o Secure Mail

1. Requisitos para especificações: como um requisito de segurança, você precisa de um aplicativo de email que esteja em contêiner e ofereça suporte às políticas de segurança de MDX.
2. Desenvolvimento: valide se o aplicativo atende às necessidades de negócios. Você deve poder aplicar controles de política de MDX ao aplicativo.
3. Teste: atribua o Secure Mail a um grupo de usuários de teste e implante o arquivo MDX correspondente do XenMobile Server. Os usuários de teste validam que eles podem enviar e receber emails com sucesso e têm acesso a calendário e contatos. Os usuários de teste também relatam problemas e identificam bugs. Com base no feedback dos usuários de teste, você otimiza a configuração do Secure Mail para uso em produção.
4. Implantação: quando a fase de teste é concluída, você atribui o Secure Mail aos usuários de produção e implanta o arquivo MDX correspondente do XenMobile Server.
5. Manutenção: uma nova atualização para o Secure Mail está disponível. Você baixa o novo arquivo MDX dos downloads do Citrix e substitui o arquivo MDX existente no XenMobile Server. Instrua os usuários a realizar a atualização. Nota: a Citrix recomenda que você conclua e teste esse processo em um ambiente de teste antes de carregar o aplicativo para um ambiente de produção XenMobile e implantar o aplicativo para os usuários.

Para obter mais informações, consulte Preparação de aplicativos móveis iOS e Preparação de aplicativos móveis Android.

Operações baseadas em painel

March 6, 2019

Você pode exibir informações de forma abrangente acessando o painel de controle do console XenMobile. Com essas informações, você pode ver problemas e operações bem-sucedidas rapidamente usando widgets.

O painel é geralmente a tela exibida primeiramente quando você faz logon no console 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 editar os widgets exibidos.

- **Meus painéis:** você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e exibir cada um selecionando o painel salvo.
- **Estilo de layout:** nessa linha você pode selecionar quantos widgets são exibidos no painel e a sua disposição.
- **Seleção de widgets:** você pode escolher as informações que aparecem no 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 disposi-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tivos 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 não gerenciados e gerenciados por operadora. Clique em cada barra para ver um demonstrativo 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 são exibidos neste gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.
- **Dispositivos por Status do Gateway do ActiveSync:** exibe o número de dispositivos agrupados por status do ActiveSync Gateway. As informações mostram o status Desconhecido, Permitido ou Bloqueado. Você pode clicar em cada barra exibir os dados por plataforma.
- **Dispositivos por propriedade:** exibe o número de dispositivos agrupados por status de propriedade. As informações de mostram o status de propriedade de propriedade da empresa, propriedade do funcionário ou desconhecido.
- **Status de licença do android TouchDown:** exibe o número de dispositivos que têm uma licença do TouchDown.
- **Implantações de grupo de entrega com falha:** exibe o número total de falhas de implantação por pacote. Apenas os pacotes que têm falhas de implementação.
- **Dispositivos por motivo de bloqueio:** exibe o número de dispositivos bloqueados pelo ActiveSync
- **Aplicativos instalados:** usando este widget, você pode digitar um nome de aplicativo, e um gráfico exibe as informações sobre esse aplicativo.
- **Uso de licenças de aplicativos de VPP:** exibe as estatísticas de uso para aplicativos do Apple Volume Purchase Program.

Casos de uso

Veja abaixo alguns exemplos de diferentes maneiras de usar widgets do painel para monitorar seu ambiente.

- Você implantou aplicativos móveis de produtividade e está recebendo tíquetes de suporte referentes à falha de instalação de aplicativos móveis de produtividade nos dispositivos. Use os widgets **Dispositivos Fora de Conformidade** e **Aplicativos Instalados** para ver os dispositivos que não têm aplicativos móveis de produtividade instalados.
- Você gostaria de monitorar dispositivos inativos para poder remover os dispositivos de seu ambiente e recuperar as licenças. Use o widget **Dispositivos Inativos** para acompanhar esta estatística.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Você está recebendo tickets de suporte referentes a dados que não estão sendo sincronizados corretamente. Você pode querer usar os widgets **Dispositivos pelo Status do ActiveSync Gateway** e **Dispositivos pelo Motivo de bloqueio** para determinar se o problema está relacionado ao ActiveSync.

Criação de relatórios

Depois que seu ambiente for configurado e os usuários registrados, você poderá gerar relatórios para saber mais sobre sua implantação. O XenMobile vem com vários relatórios internos para ajudá-lo a ter uma melhor ideia sobre os dispositivos em execução no seu ambiente. Para obter detalhes, consulte Relatórios.

> Importante:
>
> Embora seja possível usar o SQL Server para criar relatórios personalizados, Citrix não recomenda esse método. Usar o banco de dados do SQL Server dessa maneira pode ter consequências inesperadas na sua implantação do XenMobile. Se você decidir tomar esse método de emissão de relatórios, certifique-se de que as consultas do SQL são executadas usando uma conta de somente leitura.

Controle de Acesso Baseado em Função e Suporte XenMobile

April 15, 2019

O XenMobile usa o controle de acesso baseado em função (RBAC) para restringir o acesso de usuários e grupos às funções do sistema XenMobile, como o Console XenMobile, o Portal de Autoajuda, o Remote Support e a API pública. Este artigo descreve as funções incorporadas ao XenMobile e inclui considerações para decidir sobre o modelo de suporte para o XenMobile que se integre com o RBAC.

Funções incorporadas

Você pode alterar o acesso concedido às seguintes funções internas e adicionar funções. Para obter o conjunto completo de permissões de acesso e recursos associados a cada função e suas configurações padrão, baixe os Padrões de Controle de Acesso Baseado em Funções da documentação do XenMobile. Para obter uma definição de cada recurso, consulte Configurar funções com RBAC na documentação do XenMobile.

Função de Administrador

Acesso padrão concedido:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Acesso total ao sistema, exceto ao Portal de Autoajuda e Remote Support.
- Por padrão, os administradores podem executar algumas tarefas de suporte, como verificar conectividade e criar pacotes de suporte.

Considerações:

- Alguns ou todos os seus administradores precisam acessar o Portal de Autoajuda ou o Remote Support? Nesse caso, você pode editar a função de administrador ou adicionar funções de administrador.
- Para restringir ainda mais o acesso a alguns administradores ou grupos de administradores, adicione funções com base no modelo de administrador e edite as permissões.

Provisionamento de dispositivo

Acesso padrão concedido:

- Acesso ao console XenMobile para executar administração básica em dispositivos Windows CE: adicionar, alterar e remover dispositivos; usar a página Configurações.

Considerações:

- Aplica-se apenas a dispositivos Windows CE.

Suporte

Acesso padrão concedido:

- Acesso ao Remote Support.

Considerações:

- Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível com somente dispositivos Samsung KNOX.
- O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

Usuário

Acesso padrão concedido:

- Acesso ao Portal de Autoajuda, que permite que usuários autenticados gerem links de registro. Os links permitem que eles registrem seus dispositivos ou enviem para si mesmos um convite de registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Acesso restrito ao console XenMobile: recursos do dispositivo (como apagar, bloquear/desbloquear dispositivo; bloquear/desbloquear contêiner; ver local 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 habilite os usuários a se ajudarem.
- Para suportar dispositivos compartilhados, crie uma função de usuário para o registro de dispositivos compartilhados.

Considerações para um modelo de suporte XenMobile

Os modelos de suporte que você pode adotar podem variar muito e podem envolver terceiros que lidam com suporte de nível 1 e 2, enquanto os funcionários lidam com suporte de nível 3 e 4. Independentemente de como você distribui a carga de suporte, tenha em mente as considerações nesta seção específicas à sua implantação e base de usuários do XenMobile.

Os usuários possuem dispositivos corporativos ou BYO?
A principal questão que influencia o suporte é quem possui os dispositivos do usuário em seu ambiente XenMobile. Se seus usuários tiverem dispositivos de propriedade da empresa, você poderá oferecer um nível de suporte mais baixo, como forma de bloquear os dispositivos. Nesse caso, você pode fornecer um suporte técnico que ajude os usuários com problemas de dispositivos e como usar os dispositivos. Dependendo dos tipos de dispositivos que você precisa dar suporte, pense em como você pode usar as funções de provisionamento e suporte de dispositivos RBAC para a sua central de ajuda.

Se seus usuários tiverem dispositivos BYO, sua organização provavelmente espera que os usuários encontrem suas próprias fontes para suporte ao dispositivo. Nesse caso, o suporte fornecido pela sua organização é mais uma função administrativa focada em problemas específicos do XenMobile.

Qual é o seu modelo de suporte para computadores desktop?
Considere se o seu modelo de suporte para desktops é apropriado para outros dispositivos de propriedade da empresa. Você pode usar a mesma organização de suporte? Que treinamento adicional eles precisam?

Deseja dar aos usuários acesso ao Portal de Autoajuda do XenMobile?
Embora algumas organizações prefiram não conceder aos usuários acesso ao XenMobile, dar aos usuários alguns recursos de autossuporte pode aliviar a carga em sua organização de suporte. Se a função de usuário padrão do RBAC incluir permissões que você não deseja conceder, considere a criação de uma nova função com apenas as permissões que você deseja incluir. Você pode criar quantas funções forem necessárias para atender aos seus requisitos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Monitoramento de sistemas

April 15, 2019

Para garantir o tempo de atividade ideal para o acesso e a conectividade do aplicativo, você deve monitorar os seguintes componentes principais no ambiente do XenMobile.

XenMobile server

O XenMobile Server gera e armazena logs no repositório local que você também pode exportar para um servidor de log de sistemas (syslogs). Você pode definir configurações de log para especificar restrições de tamanho, nível de log ou criar agentes de log personalizados para filtrar eventos específicos. Você pode consultar os logs do XenMobile Server no console XenMobile a qualquer momento. Você também pode exportar informações nos logs por meio do servidor syslog para seus servidores de log de produção do Splunk.

A lista a seguir descreve os diferentes tipos de arquivos de log disponíveis no XenMobile:

Arquivo de log de depuração: contém informações sobre o nível de depuração dos principais serviços da 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: contêm informações de auditoria sobre as atividades no console XenMobile.

> Nota:
>
> O mesmo formato é usado para os logs de auditoria do administrador e de auditoria do usuário.

Formato da mensagem:

Com exceção dos valores obrigatórios de Date e Timestamp, todos os outros atributos são opcionais. 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensagens de log de auditoria do administrador para eventos	Status
Login	sucesso/falha
Logout	sucesso/falha
Get admin	sucesso/falha
Update admin	sucesso/falha
Get application	sucesso/falha
Add application	sucesso/falha
Update application	sucesso/falha
Delete application	sucesso/falha
Bind application	sucesso/falha
Unbind application	sucesso/falha
Disable application	sucesso/falha
Enable application	sucesso/falha
Get category	sucesso/falha
Add category	sucesso/falha
Update category	sucesso/falha
Delete category	sucesso/falha
Add certificate	sucesso/falha
Delete certificate	sucesso/falha
Active certificate	sucesso/falha
Self-sign certificate	sucesso/falha
CSR certificate	sucesso/falha
Export certificate	sucesso/falha
Delete certificate chain	sucesso/falha
Add certificate chain	sucesso/falha
Get connector	sucesso/falha
Add connector	sucesso/falha
Delete connector	sucesso/falha
Update connector	sucesso/falha

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensagens de log de auditoria do administrador para eventos	Status
Get device	sucesso/falha
Lock device	sucesso/falha
Unlock device	sucesso/falha
Wipe device	sucesso/falha
Unwipe device	sucesso/falha
Delete device	sucesso/falha
Get role	sucesso/falha
Add role	sucesso/falha
Update role	sucesso/falha
Delete role	sucesso/falha
Bind role	sucesso/falha
Unbind role	sucesso/falha
Update config settings	sucesso/falha
Update workflow email	sucesso/falha
Add workflow	sucesso/falha
Delete workflow	sucesso/falha
Add Active Directory	sucesso/falha
Update Active Directory	sucesso/falha
Add masteruserlist	sucesso/falha
Update masteruserlist	sucesso/falha
Update DNS	sucesso/falha
Update Network	sucesso/falha
Update log server	sucesso/falha
Transfer log from log server	sucesso/falha
Update syslog	sucesso/falha
Update receiver updates	sucesso/falha
Update time server	sucesso/falha
Update trust	sucesso/falha

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensagens de log de auditoria do administrador para eventos	Status
Add service record	sucesso/falha
Update service record	sucesso/falha
Update receiver email	sucesso/falha
Upload patch	sucesso/falha
Import snapshot	sucesso/falha
Fetch app store app details	sucesso/falha
Update MDM	sucesso/falha
Delete MDM	sucesso/falha
Add HDX	sucesso/falha
Update HDX	sucesso/falha
Delete HDX	sucesso/falha
Add Branding	sucesso/falha
Delete Branding	sucesso/falha
Update SSL offload	sucesso/falha
Add account property	sucesso/falha
Delete account property	sucesso/falha
Update account property	sucesso/falha
Add 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 os logs de auditoria do usuário e de auditoria do administrador.

Formato da mensagem:

Com exceção dos valores obrigatórios de Date e Timestamp, todos os outros atributos são opcionais. 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>”
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A tabela a seguir lista os eventos do log de auditoria do usuário disponíveis:

Mensagens de log de auditoria do usuário para eventos	Status
Login	sucesso/falha
Session time-out	sucesso/falha
Subscribe	sucesso/falha
Unsubscribe	sucesso/falha
Pre-launch	sucesso/falha
AGEE SSO	sucesso/falha
SAML Token for ShareFile	sucesso/falha
Device registration	sucesso/falha
Device check	lock/wipe
Device update	sucesso/falha
Token refresh	sucesso/falha
Secret saved	sucesso/falha
Secret retrieved	sucesso/falha
User initiated change password	sucesso/falha
Mobile client download	sucesso/falha
Logout	sucesso/falha
Discovery Service	sucesso/falha
Endpoint Service	sucesso/falha

Funções do MDM	Status
REGHIVE	sucesso/falha
Cab inventory	sucesso/falha
Cab	sucesso/falha
Cab auto install	sucesso/falha
Cab shell install	sucesso/falha
Cab create folder	sucesso/falha
Cab file get	sucesso/falha

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Funções do MDM	Status
File create folder	sucesso/falha
File get	sucesso/falha
File sent	sucesso/falha
Script create folder	sucesso/falha
Script get	sucesso/falha
Script sent	sucesso/falha
Script shell execution	sucesso/falha
Script auto execution	sucesso/falha
APK inventory	sucesso/falha
APK	sucesso/falha
APK shell install	sucesso/falha
APK auto install	sucesso/falha
APK create folder	sucesso/falha
APK file get	sucesso/falha
APK App	sucesso/falha
EXT App	sucesso/falha
List get	sucesso/falha
List sent	sucesso/falha
Locate device	sucesso/falha
CFG	sucesso/falha
Unlock	sucesso/falha
SharePoint wipe	sucesso/falha
SharePoint Configuration	sucesso/falha
Remove profile	sucesso/falha
Remove application	sucesso/falha
Remove unmanaged application	sucesso/falha
Remove unmanaged profile	sucesso/falha
IPA App	sucesso/falha
EXT App	sucesso/falha

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Funções do MDM	Status
Apply redemption code	sucesso/falha
Apply settings	sucesso/falha
Enable tracking device	sucesso/falha
App management policy	sucesso/falha
SD card wipe	sucesso/falha
Encrypted email attachment	sucesso/falha
Branding	sucesso/falha
Secure browser	sucesso/falha
Container browser	sucesso/falha
Container unlock	sucesso/falha
Container password reset	sucesso/falha
AG client auth creds	sucesso/falha

O NetScaler também monitora o estado do serviço da Web do XenMobile, que é configurado com probes de monitoramento inteligente para simular solicitações HTTP para cada nó do cluster do XenMobile Server. Os probes determinam se o serviço está online e, em seguida, respondem com base na resposta recebida. No caso de um nó não responder como esperado, o NetScaler marca o servidor como inativo. Além disso, o NetScaler retira o nó do pool de balanceamento de carga e faz o log do evento para uso na geração de alertas por meio da solução de monitoramento NetScaler.

Você também pode usar ferramentas padrão de monitoramento de hipervisor para monitorar as máquinas virtuais do XenMobile e fornecer alertas relevantes em relação às 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 XenMobile Services. A instância do XenMobile requer acesso ao banco de dados em todos os momentos e fica offline (por exemplo, para de responder) no caso de uma interrupção na infraestrutura do SQL. O console XenMobile pode continuar a funcionar por um tempo após problemas de espaço em disco com o SQL Server. Para garantir o tempo de atividade máximo do banco de dados e o desempenho adequado da carga de trabalho do XenMobile, você deve monitorar proativamente o estado de seus SQL Servers seguindo as Recomendações da Microsoft. Além disso, você deve ajustar a alocação de recursos para CPU,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

memória e armazenamento para garantir acordos de nível de serviço à medida que seu ambiente XenMobile continua a crescer.

NetScaler

O NetScaler fornece a capacidade de registrar métricas no armazenamento interno ou enviar logs para um servidor de registro externo. Você pode configurar o servidor syslog para exportar logs do NetScaler para seus servidores de log de produção do Splunk. Os seguintes níveis de registro estão disponíveis no NetScaler:

- Emergência
- Alerta
- Crítico
- Erro
- Aviso
- Informativo

Os arquivos de log também são armazenados no repositório do NetScaler no diretório /var/log/ns.log e nomeados newnslog. O NetScaler reúne e comprime os arquivos usando o algoritmo GZIP. O nome dos arquivos de log é newnslog.xx.gz, em que xx representa um número de execução.

O NetScaler também suporta interceptações e alertas de SNMP como opção de monitoramento. Para obter uma lista de interceptações de SNMP, consulte o SNMP monitoring.

Recuperação de desastres

March 6, 2019

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais de 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 datacenter de uma localização geográfica atendendo a todos os usuários da empresa globalmente, conhecido como o site principal.
- Um segundo site XenMobile no datacenter de um segundo local geográfico, conhecido como site de recuperação de desastre. Este site de recuperação de desastre fornece failover de site ativo-passivo em caso de falha de um datacenter em todo o site principal. O site principal inclui o XenMobile, o banco de dados SQL, a infraestrutura do NetScaler para facilitar o failover e fornecer aos usuários acesso ao XenMobile por meio do evento de falha de conectividade no site principal.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Os servidores XenMobile no site de recuperação de desastre permanecem off-line durante as operações normais e são colocados on-line apenas em cenários de recuperação de desastre, onde é necessário um failover completo do site principal para o site de recuperação de desastre. Os SQL Servers no site de recuperação de desastre devem estar ativos e prontos para atender às conexões antes de iniciar os servidores XenMobile no site de recuperação de desastre.

Essa estratégia de recuperação de desastre depende do failover manual da camada de acesso do NetScaler por meio de alterações de DNS para rotear conexões do MDM e do MAM para o site de recuperação de desastre no caso de uma indisponibilidade.

> Nota:
>
> Para usar essa arquitetura, você deve ter um processo para backups assíncronos dos bancos de dados e alguma maneira 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 desastre, encerre os servidores XenMobile no site principal para simular a falha do site.
2. Altere os registros DNS públicos dos servidores XenMobile para apontar para os endereços IP externos do site de recuperação de desastre.
3. Altere o registro DNS interno do SQL Server para apontar para o endereço IP do SQL Server do site de recuperação de desastre.
4. Coloque os bancos de dados XenMobile SQL on-line no site de recuperação de desastre. 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. Ative os servidores XenMobile no site de recuperação de desastre.

Processo de atualização do servidor XenMobile

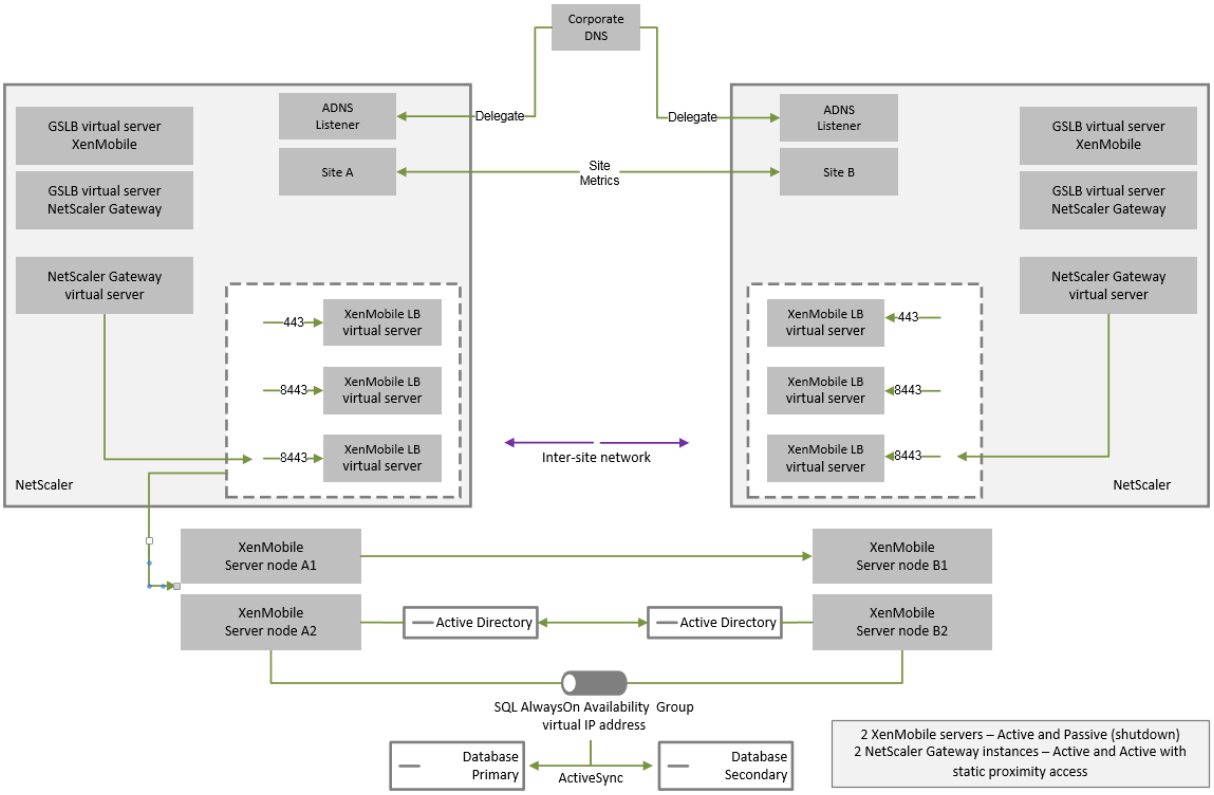
Siga estas etapas sempre que você atualizar o XenMobile com patches e novas versões, para manter o código dos servidores principal e de recuperação de desastres uniformes.

1. Certifique-se de que os servidores XenMobile no site principal foram corrigidos ou atualizados.
2. Verifique se o registro DNS do SQL Server está resolvendo o banco de dados ativo do SQL Server no site principal.
3. Coloque os servidores XenMobile do site de recuperação de desastre online. Os servidores se conectam ao banco de dados do site principal pela WAN somente durante o processo de atualização.
4. Aplique patches e atualizações necessárias a todos os servidores XenMobile do site de recuperação de desastre.
5. Reinicie os servidores XenMobile e confirme se o patch ou atualização foi bem-sucedido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Diagrama da Arquitetura de Referência de Recuperação de Desastres

O diagrama a seguir mostra a arquitetura de alto nível para uma implantação de recuperação de desastre do XenMobile.



GSLB para recuperação de desastres

Um elemento-chave dessa arquitetura é o uso do Global Server Load Balancing (GSLB) para direcionar o tráfego para o data center correto.

Por padrão, o Assistente NetScaler para XenMobile configura o NetScaler Gateway de uma maneira que não permite o uso do GSLB para recuperação de desastres. Portanto, você deve executar etapas adicionais.

Como funciona o GSLB

O GSLB é, no seu núcleo, uma forma de DNS. Os dispositivos NetScaler participantes atuam como servidores DNS autoritativos e resolvem os registros DNS para o endereço IP correto (geralmente o VIP que deve receber tráfego). O dispositivo NetScaler verifica a integridade do sistema antes de responder a uma consulta DNS direcionando o tráfego para esse sistema.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Quando um registro é resolvido, a função do GSLB na resolução do tráfego é concluída. O cliente se comunica diretamente com o endereço de 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 em grande parte fora dos limites do sistema NetScaler. Como tal, o GSLB está sujeito às mesmas limitações que a resolução de nomes DNS. Respostas de clientes em cache; entretanto, o balanceamento de carga dessa maneira não é tão em tempo real quanto o balanceamento de carga tradicional.

A configuração do GSLB no NetScaler, incluindo sites, serviços e monitores, existe para fornecer a resolução de nomes DNS correta.

A configuração real dos servidores de publicação (nesse cenário, a configuração criada pelo assistente do NetScaler para XenMobile) não é afetada pelo GSLB. O GSLB é um serviço separado no NetScaler.

Desafios com a delegação de domínio ao usar o GSLB com o XenMobile

O assistente NetScaler para XenMobile configura o NetScaler Gateway para XenMobile. Esse assistente gera três servidores virtuais de balanceamento de carga e um servidor virtual NetScaler Gateway.

Dois dos servidores virtuais de balanceamento de carga lidam com o tráfego do MDM, nas portas 443 e 8443. O NetScaler Gateway recebe o tráfego do MAM e o encaminha para o terceiro servidor, o servidor virtual de balanceamento de carga do MAM, na porta 8443. Todo o tráfego para o servidor virtual de balanceamento de carga do MAM passa pelo NetScaler Gateway.

O servidor virtual de balanceamento de carga do MAM requer o mesmo certificado SSL dos servidores XenMobile e usa o mesmo FQDN usado para registrar dispositivos. O servidor de balanceamento de carga do MAM também usa a mesma porta (8443) que um dos servidores de balanceamento de carga do MDM. Para permitir que o tráfego seja resolvido, o Assistente NetScaler para XenMobile cria um registro DNS local no NetScaler Gateway. O registro DNS corresponde ao FQDN usado para registrar dispositivos.

Essa configuração é efetiva quando o URL do servidor XenMobile não é uma URL de domínio do GSLB. Se uma URL de domínio do GSLB for usada como a URL do XenMobile Server, conforme exigido para recuperação de desastre, o registro DNS local impedirá que o NetScaler Gateway resolva o tráfego para os servidores de balanceamento de carga do MDM.

Usando o Método CNAME para Recuperação de Desastres GSLB

Para resolver os desafios apresentados pela configuração padrão criada pelo Assistente NetScaler para XenMobile, você pode criar um registro CNAME para o FQDN do XenMobile Server no domínio pai (`company.com`) e apontar um registro na subzona delegada (`gslb.company.com`) para a qual o NetScaler é autoritativo. Isso permite a criação do registro DNS A estático para o endereço VIP de balanceamento de carga do MAM, necessário para resolver o tráfego.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. No DNS externo, crie um CNAME para o FQDN do XenMobile Server que aponta para o FQDN do domínio GSLB no NetScaler GSLB. Você precisa de dois domínios GSLB: um para o tráfego do MDM e outro para o tráfego do MAM (NetScaler Gateway).

   Exemplo:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. Na instância do NetScaler Gateway de cada site, crie um servidor virtual GSLB com um FQDN, para o qual o registro CNAME está apontando.

   Exemplo:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   Ao usar o Assistente NetScaler para XenMobile para implantar o NetScaler Gateway, use a URL do XenMobile Server ao configurar o servidor de balanceamento de carga do MAM. Isso cria um registro DNS A estático para a URL do XenMobile Server.

3. Teste com clientes registrados 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 do MDM e é usada pelo registro de dispositivos, que é configurado neste exemplo usando o Assistente NetScaler para XenMobile.
   - `xms.gslb.company.com` é o FQDN do domínio GSLB para o XenMobile Server.

Processo de Suporte Citrix

April 15, 2019

Você pode ativar os Serviços de Suporte Técnico da Citrix para ajudar nos problemas relacionados aos produtos Citrix. O grupo oferece soluções alternativas e trabalha de mãos dadas com as equipes de desenvolvimento para oferecer soluções.

Citrix Consulting Services ou Citrix Education Services oferecem ajuda relacionada ao treinamento de produtos, conselhos sobre uso, configuração, instalação ou arquitetura e design do ambiente do produto.

A Citrix Consulting ajuda com os projetos relacionados ao produto Citrix, incluindo provas de conceitos, avaliação de impacto econômico, verificações de integridade de infraestrutura, análise de requisitos de projeto, verificação de projeto de arquitetura, integração e desenvolvimento de processos operacionais.

A Citrix Education oferece o melhor treinamento e certificação de TI da Citrix em virtualização, nuvem e tecnologias de rede.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

A Citrix recomenda que você aproveite ao máximo os recursos e recomendações do Citrix Self-Help antes de criar um caso de suporte. Por exemplo, existem vários lugares onde você pode acessar artigos e boletins escritos por especialistas técnicos da Citrix, ver a documentação do produto para conhecer as soluções e tecnologias da Citrix ou ler materiais diretamente dos executivos da Citrix, equipes de produtos e especialistas técnicos. Consulte as páginas Knowledge Center, Documentação de produtos e Blogs, respectivamente.

Para obter assistência mais interativa, você pode participar de fóruns de discussão nos quais pode fazer perguntas e obter respostas reais de outros clientes, compartilhar ideias, opiniões, informações técnicas e práticas recomendadas em grupos de usuários e grupos de interesse ou interagir com engenheiros do Citrix Support. que monitoram sites de redes sociais do Citrix Support. Consulte as páginas Fóruns de suporte, Comunidade Citrix e Suporte Citrix no Twitter, respectivamente.

Você também tem acesso a cursos de treinamento e certificação para desenvolver suas habilidades. Veja Citrix Education.

O Citrix Insight Services fornece uma plataforma simples para solução de problemas on-line e um verificador de integridade para seu ambiente Citrix. Disponível para XenMobile, XenDesktop, XenServer, XenApp e NetScaler. Veja Analysis Tool.

Para buscar suporte técnico, você pode criar um caso de suporte por telefone ou pela Web. Você pode usar a Web para resolver problemas de baixa e média gravidade e usar a opção de telefone para problemas de alta gravidade. Para obter informações sobre como entrar em contato com o suporte para solucionar problemas do XenMobile, consulte Como entrar em contato com o suporte.

Se você procura um único ponto de contato altamente treinado com ampla experiência na entrega de soluções Citrix, a Citrix Services oferece um Gerente de Relacionamento Técnico. Para obter mais informações sobre ofertas e benefícios de serviços da Citrix, consulte Citrix Worldwide Services.

Enviar convites para registro em grupo no XenMobile

April 15, 2019

Contribuição de John Bartel III

Você pode enviar convites de registro para grupos no XenMobile. Você também pode enviar convites para seus grupos aninhados. Ao configurar o convite de grupo, você pode especificar uma ou várias plataformas de dispositivos. Você também pode marcar dispositivos para, por exemplo, distinguir dispositivos de propriedade da empresa dos dispositivos de propriedade dos funcionários. Em seguida, você define o tipo de autenticação para dispositivos do usuário.

> Nota:
>
> Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> antes de você configurar os modos de registro. Para obter mais informações sobre modelos de notificação, consulte Criar e atualizar modelos de notificação.

Para obter mais informações sobre configurações básicas em contas de usuário, funções e modos de registro e convites, consulte Contas de usuário, funções e registro.

Etapas gerais

1. No console XenMobile, clique em **Gerenciar > Convites para registro**.
2. Clique em **Adicionar** no canto superior esquerdo da tela e clique em **Adicionar convite**.
3. Clique em **Grupo** no menu **Destinatário**.

   Esta etapa permite escolher uma ou várias plataformas. Se você tiver um misto de diferentes plataformas de sistema operacional em sua empresa, escolha todas as plataformas. Limpe a seleção da plataforma apenas se você tiver certeza de que nenhum usuário está usando a plataforma específica.
4. Você pode marcar dispositivos durante o processo de convite. Escolha **Corporativo** ou **Funcionário**.

   A marcação facilita a separação de dispositivos corporativos e dispositivos de propriedade dos funcionários.
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 registro** permite que você defina o tipo de autenticação que preferir 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
8. Para os modelos **Download do Agente**, **URL de registro**, **PIN de registro** e **Confirmação de registro**, escolha o modelo de notificação personalizado que você criou no passado. Ou escolha o padrão listado.

   Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de você configurar os modos de registro. Para obter mais informações sobre modelos de notificação, consulte Notificações.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para esses modelos de notificação, use a configuração do servidor SMTP configurado no XenMobile. Defina suas informações SMTP primeiro antes de prosseguir.

> Nota:
>
> As opções **Expira após** e **Máximo de tentativas** são alteradas com base na opção do **modo de registro** que você escolher. Você não pode alterar essas opções.

9. Selecione ON para **Enviar convite** e clique em **Salvar e Enviar** para concluir o processo.

Suporte a grupo aninhado

Você pode usar grupos aninhados para enviar convites. Normalmente, os grupos aninhados são usados em ambientes de grande porte, onde grupos com permissões semelhantes são vinculados uns aos outros.

Navegue para **Configurações > LDAP** e ative a opção **Proteger grupos aninhados**.

Resolução de problemas e limitações conhecidas

Problema: os convites estão sendo enviados aos usuários, mesmo que tenham sido removidos de um grupo do Active Directory.

Solução: dependendo do tamanho do seu ambiente do Active Directory, pode levar até seis horas para que as alterações se propaguem para todos os servidores. Se um usuário ou grupo aninhado foi removido recentemente, o XenMobile ainda poderá considerar esses usuários como parte do grupo.

Portanto, é melhor aguardar até seis horas antes de enviar outro convite em grupo para o seu grupo.

Configurar um servidor de atestado de integridade de dispositivo no local

April 15, 2019

Contribuição de Sanket Mishra

Você pode ativar o Atestado de Integridade de Dispositivo (DHA, Device Health Attestation) para dispositivos móveis Windows 10 por meio de um Windows Server no local. Para habilitar o DHA no local, você primeiro 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 essa política, consulte Política de dispositivo de Atestado de Integridade de Dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pré-requisitos para um servidor DHA

- Um servidor executando o Windows Server Technical Preview 5 ou posterior, instalado usando a opção de instalação do Desktop Experience.
- Um ou mais dispositivos clientes do Windows 10. Esses dispositivos devem ter o TPM 1.2 ou 2.0 executando a versão mais recente do Windows.
- Esses certificados:
  - **Certificado SSL DHA.** Um certificado SSL x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. Este certificado protege as comunicações de dados DHA em trânsito, incluindo as comunicações servidor a servidor (serviço DHA e servidor MDM) e servidor a cliente (serviço DHA e dispositivo Windows 10).
  - **Certificado de assinatura do DHA.** Um certificado x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA usa esse certificado para assinatura digital.
  - **Certificado de criptografia DHA.** Um certificado x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA também usa esse 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. Os dispositivos que se conectam a um serviço DHA em execução 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. Os dispositivos que se conectam a um serviço DHA em execução no modo de validação AIKCert devem ter acesso direto à Internet e estar habilitados a obter um certificado AIK da Microsoft.

Adicione a função de servidor DHA ao Windows Server

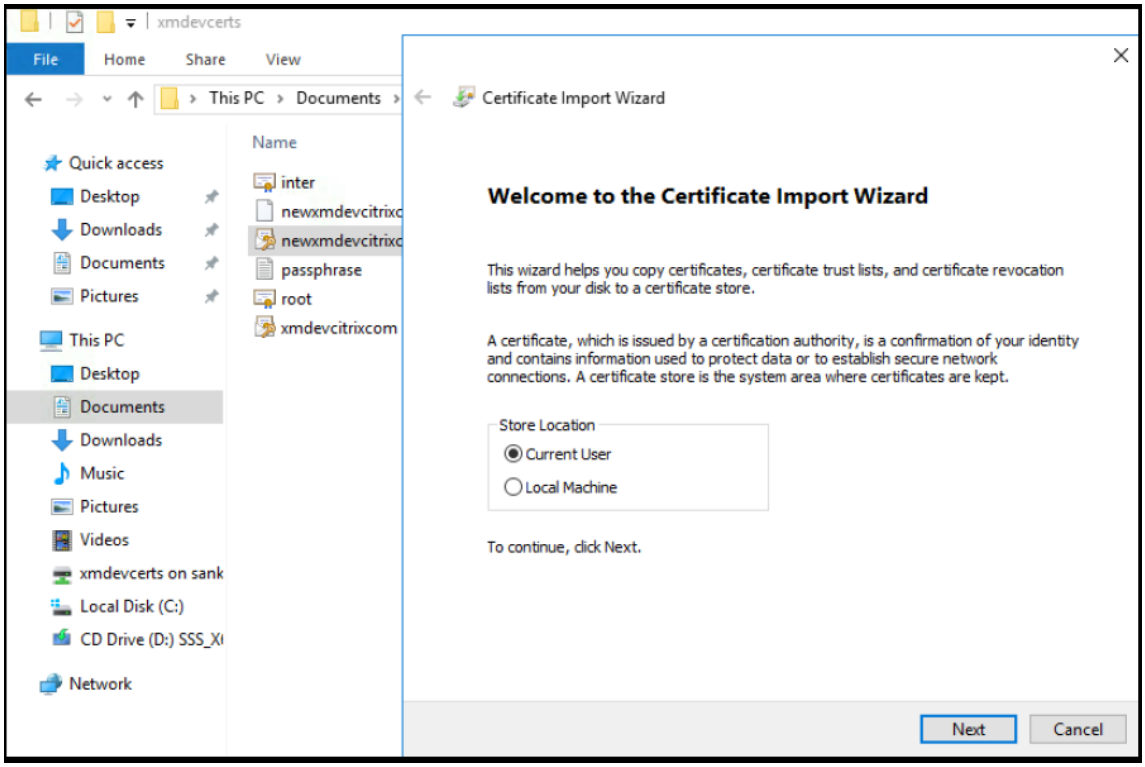
1. No Windows Server, se o Gerenciador de Servidores ainda não estiver aberto, clique em **Iniciar** e, em seguida, clique em **Gerenciador de Servidores**.
2. Clique em **Adicionar funções e recursos**.
3. Na página **Antes de começar**, clique em **Avançar**.
4. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e clique em **Avançar**.
5. Na página **Selecionar servidor de destino**, clique em **Selecionar um servidor no pool de servidor**, selecione o servidor e clique em **Avançar**.
6. Na página **Selecionar funções de servidor**, marque a caixa de seleção Atestado de Integridade de Dispositivo.
7. Opcional: clique em **Adicionar recursos** para instalar outros serviços e recursos de função necessários.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

8. Clique em **Avançar**.
9. Na página **Selecionar recursos**, clique em **Avançar**.
10. Na página **Função 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 estiver concluída, clique em **Fechar**.

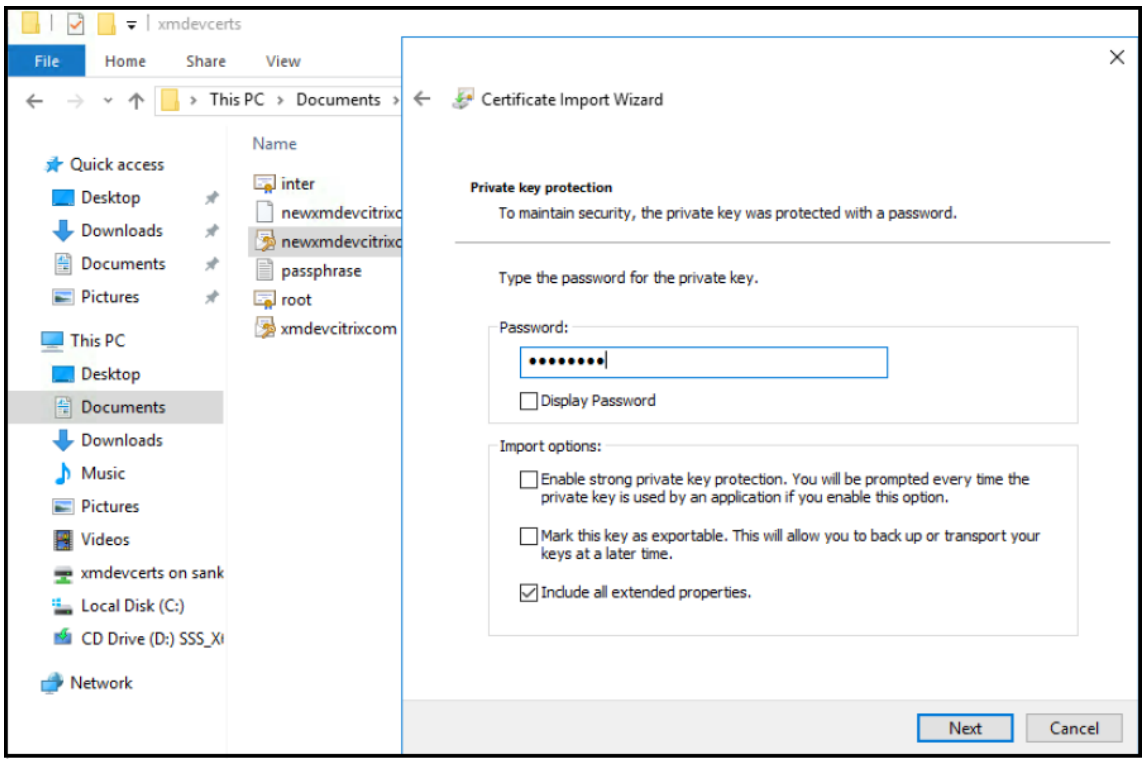
Adicione o certificado SSL ao repositório de certificados do servidor

1. Vá até o arquivo de certificado SSL e selecione-o.
2. Selecione **Usuário atual** como o local do repositório e clique em **Avançar**.



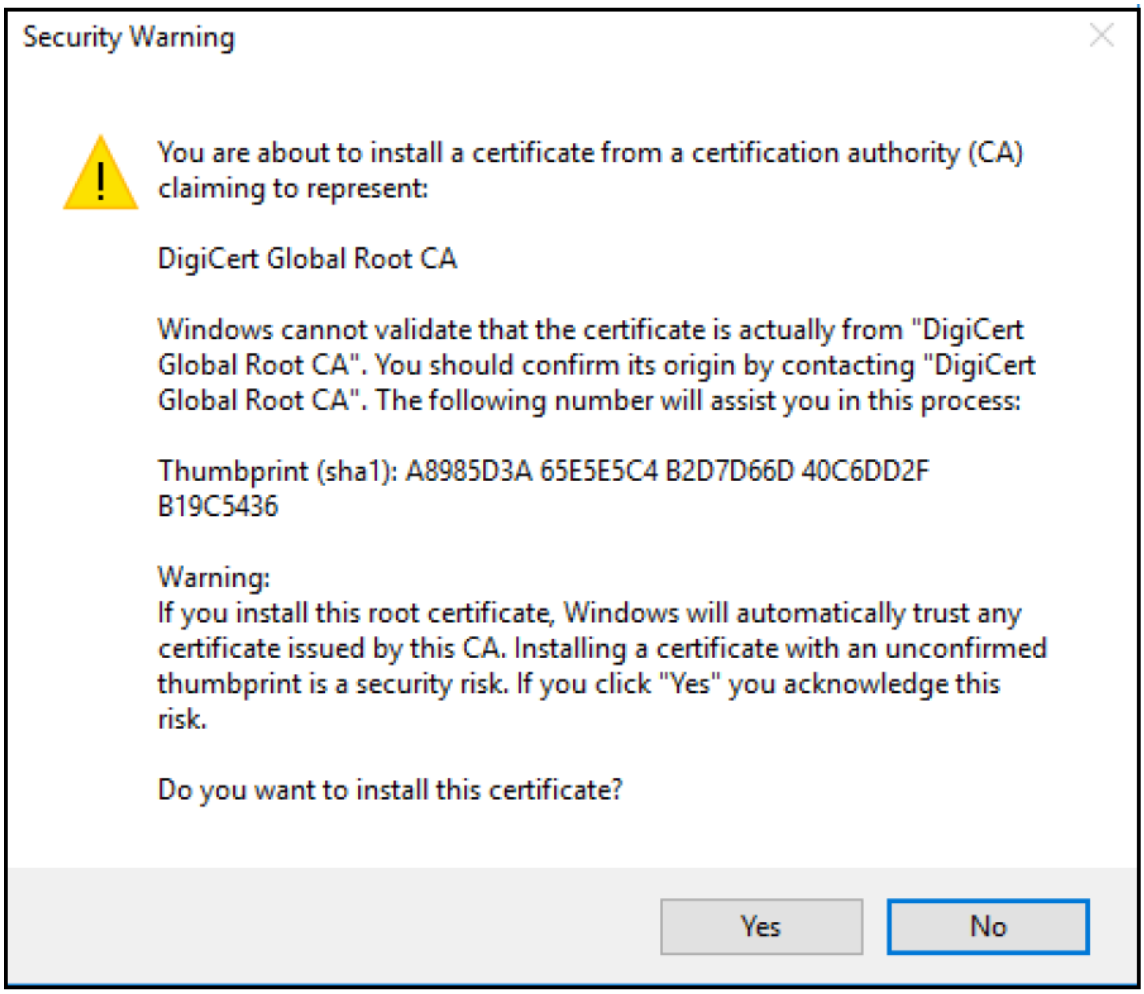
3. Digite a senha para a chave privada.
4. Assegure-se de que a opção de importação **Incluir todas as propriedades estendidas** esteja selecionada. Clique em **Avançar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



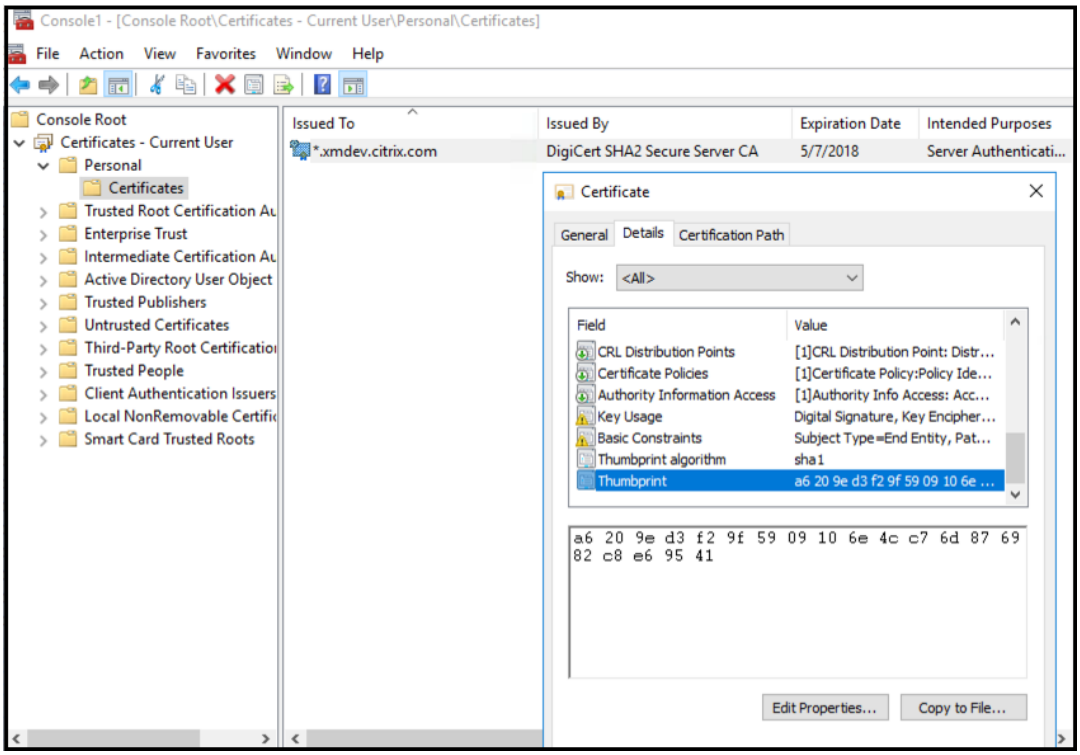
5. Quando esta janela aparecer, clique em **Sim**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

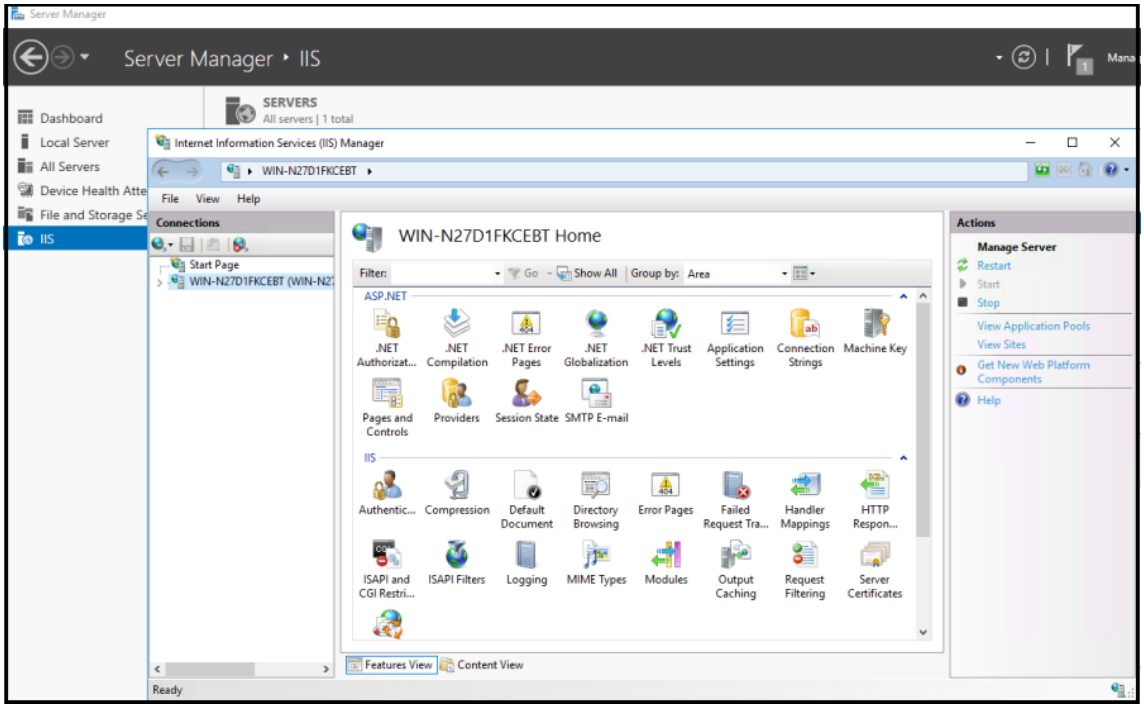


6. Confirme se o certificado está instalado:
    a) Abra uma janela do prompt de comando.
    b) Digite **mmc** e pressione a tecla Enter. Para exibir certificados no repositório do computador local, você deve estar na função Administrador.
    c) No menu Arquivo, clique em **Adicionar/Remover Snap-In**.
    d) Clique em **Adicionar**.
    e) Na caixa de diálogo Adicionar snap-in autônomo, selecione **Certificados**.
    f) Clique em **Adicionar**.
    g) Na caixa de diálogo Snap-in de Certificados, selecione **Minha conta de usuário.** (Se você estiver conectado como titular da conta de serviço, selecione **Conta de serviço**.)
    h) Na caixa de diálogo Selecionar Computador, clique em **Concluir**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

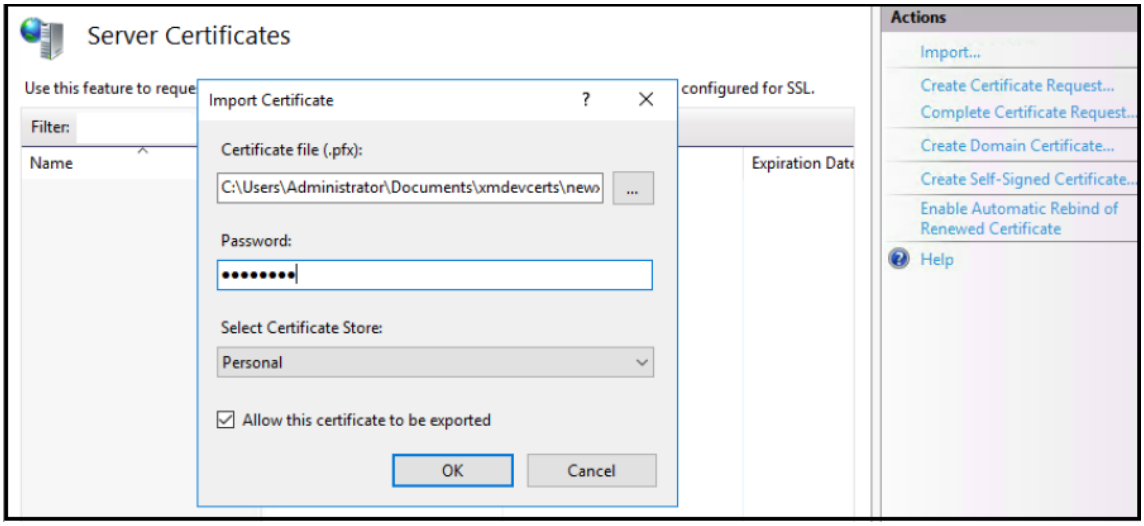


7. Vá para **Gerenciador do Servidor > IIS** e selecione **Certificados do Servidor** na lista de ícones.



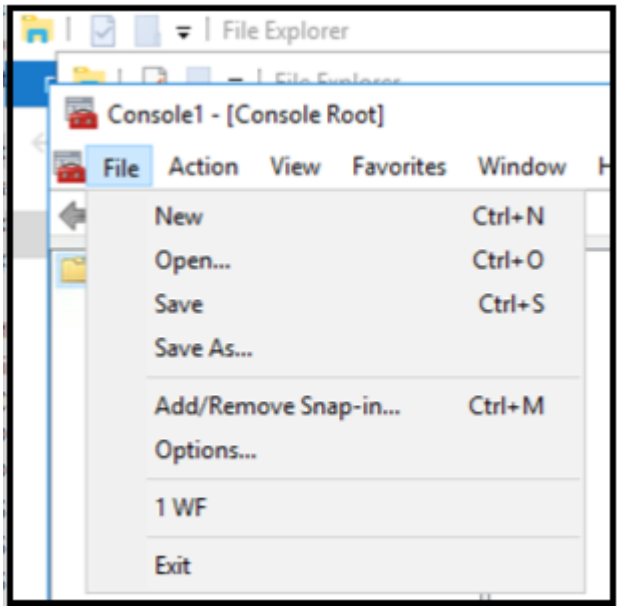
8. No menu Ação, selecione **Importar...** para importar o certificado SSL.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



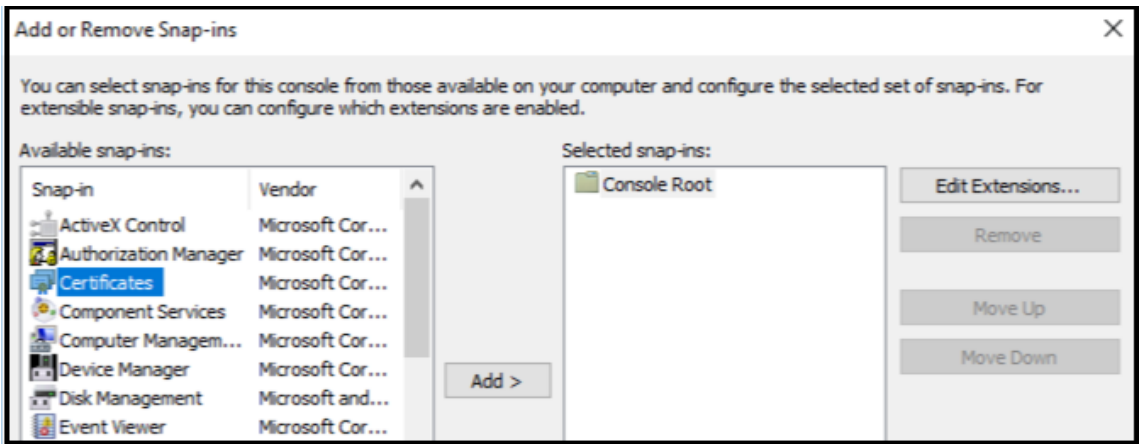
Recupere e salve a impressão digital do certificado

1. Na barra de pesquisa do Explorador de Arquivos, digite **mmc**.
2. Na janela Raiz do Console, clique em **Arquivo > Adicionar/Remover Snap-in…**.

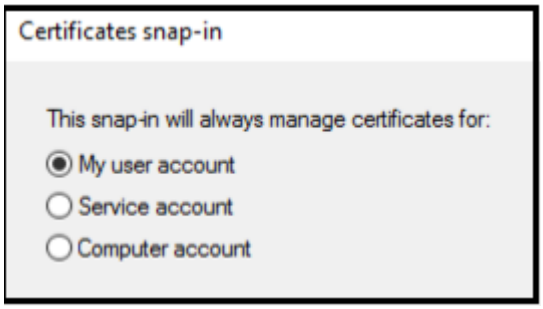


3. Selecione o certificado do snap-in disponível e adicione-o aos snap-ins selecionados.

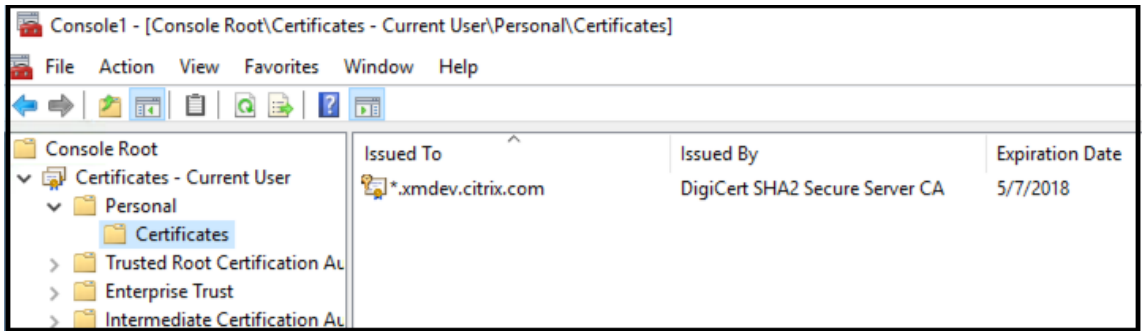
© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Selecione **Minha conta de usuário**.

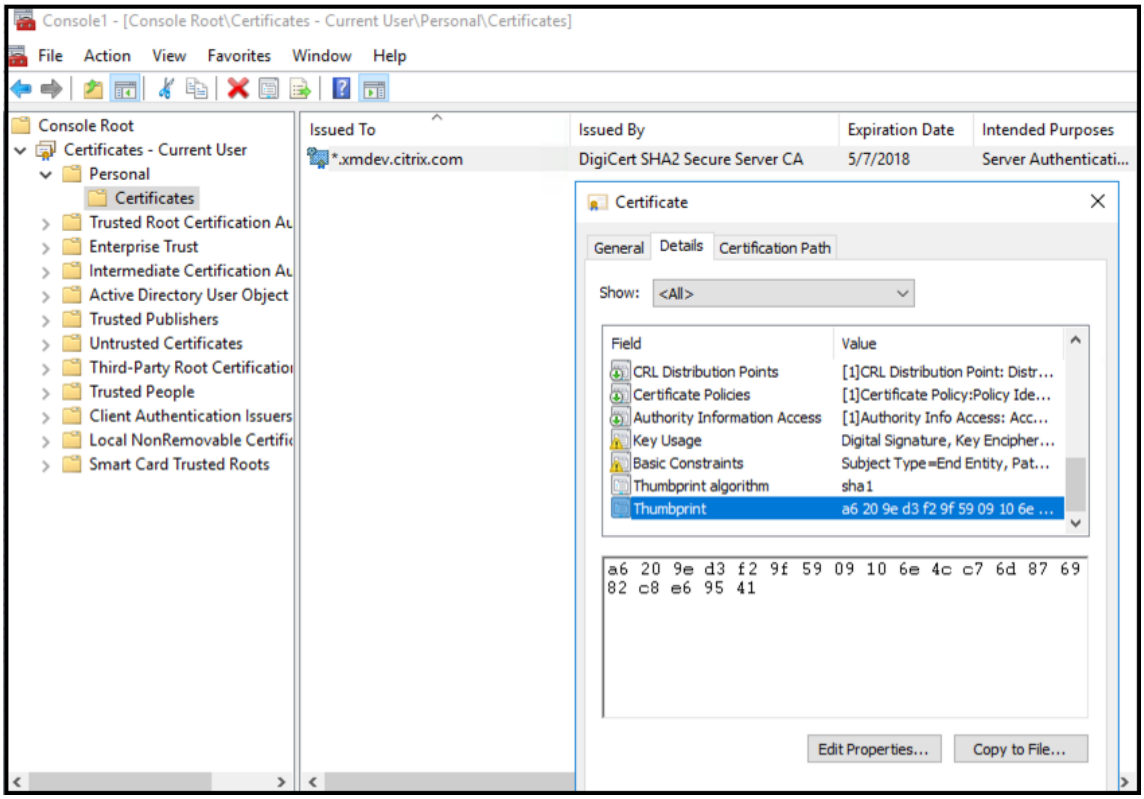


5. Selecione o certificado e clique em **OK**.



6. Clique duas vezes no certificado e selecione a guia **Detalhes**. Role para baixo para ver a impressão digital do certificado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



7. Copie a impressão digital para um arquivo. Remova os espaços ao usar a impressão digital nos comandos do PowerShell.

Instalar os certificados de assinatura e criptografia

Execute esses comandos do PowerShell no Windows Server 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
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Extraia o certificado raiz do TPM e instale o pacote de certificado confiável

Execute estes comandos no Windows Server:

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
```

Configurar o serviço DHA

Execute este comando no Windows Server para configurar o serviço DHA.

Substitua o espaço reservado ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
```

Execute esses comandos no Windows Server 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 maneira:

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on
       target "WIN-N27D1FKCEBT".
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
6
7       [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
           Help (default is "Y"): A
8
9       Adding SSL binding to website 'Default Web Site'.
10
11      Add SSL binding?
12
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
           Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
           inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
           .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 a impressão digital serão exibidos.

Para verificar se o DHASActiveSigningCertificate está ativo, execute estes comandod no servidor

Substitua o espaço reservado ReplaceWithThumbprint e coloque-o entre aspas duplas, conforme mostrado.

```
1 Set-DHASActiveEncryptionCertificate -Thumbprint ”ReplaceWithThumbprint”
      -Force
2
3 Get-DHASActiveEncryptionCertificate
```

Se o certificado estiver ativo, a impressão digital será exibida.

Para realizar uma verificação final, acesse esta URL:

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

Se o serviço DHA estiver sendo executado, será exibido “Método não permitido”.



Configurar a autenticação baseada em certificado com o EWS para notificações por push do Secure Mail

April 15, 2019

Contribuição de Vijay Kumar Kunchakuri

Para garantir que as notificações por push do Secure Mail funcionem, você deve configurar o Exchange Server para autenticação baseada em certificado. Esse requisito é especialmente 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

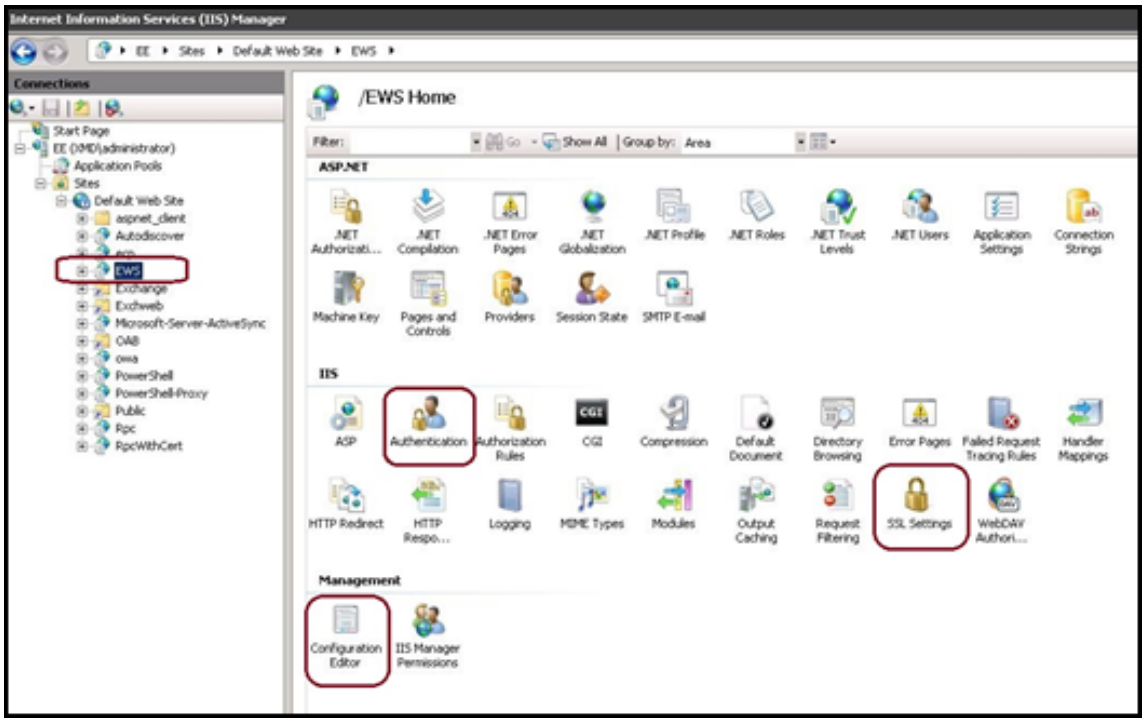
A menos que você conclua essas configurações, a assinatura das notificações por push do Secure Mail falhará e nenhuma atualização de selo ocorrerá no Secure Mail.

Este artigo descreve as etapas para configurar a autenticação baseada em certificado. As configurações são especificamente contra o diretório virtual do EWS no Exchange Server.

Para começar a usar a configuração, faça o seguinte:

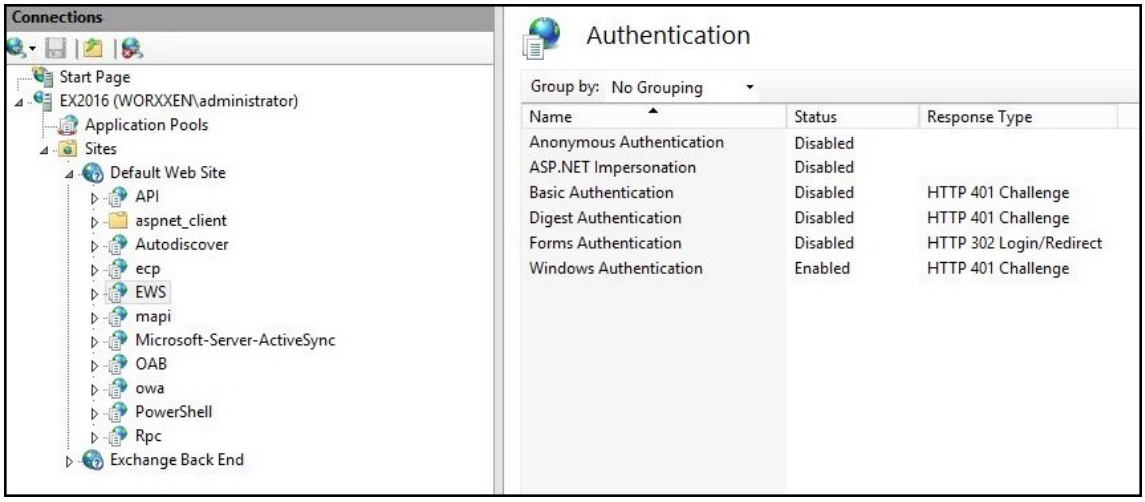
1. Faça logon no servidor ou servidores em que o diretório virtual do EWS está instalado.
2. Abra o console do gerenciador do IIS.
3. No **Site padrão**, clique no diretório virtual do EWS.

   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 o EWS estejam configuradas conforme mostrado na figura a seguir.

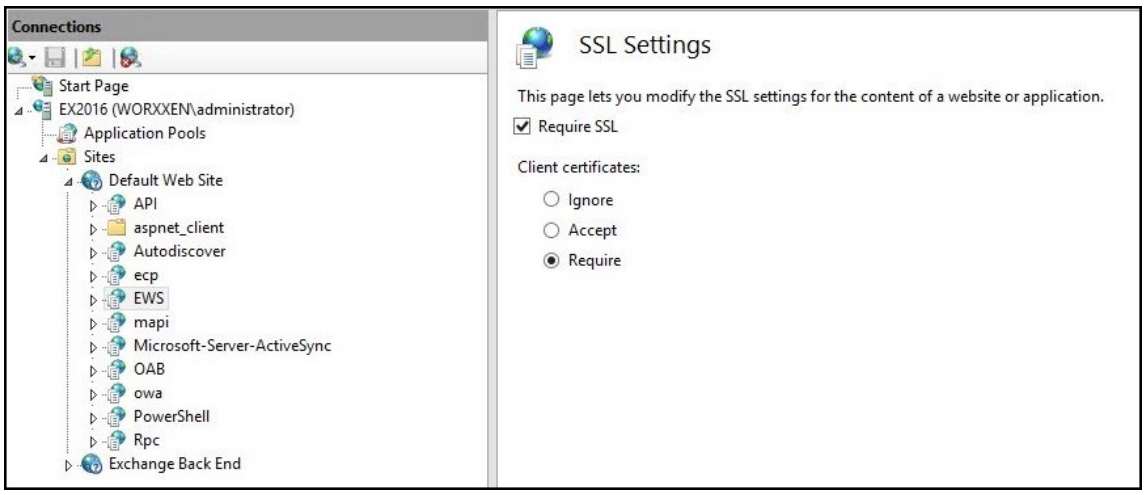
© 1999-2019 Citrix Systems, Inc. All rights reserved.



5. Defina as **Configurações de SSL** para o diretório virtual do EWS.

   a) Marque a caixa de seleção **Exigir SSL**.

   b) Em **Certificados do Cliente**, clique em **Exigir**. Você pode definir essa opção como **Aceitar** se outros clientes de e-mail do EWS se conectarem com nome de usuário e senha como credenciais para autenticar e se conectar ao Exchange Server.

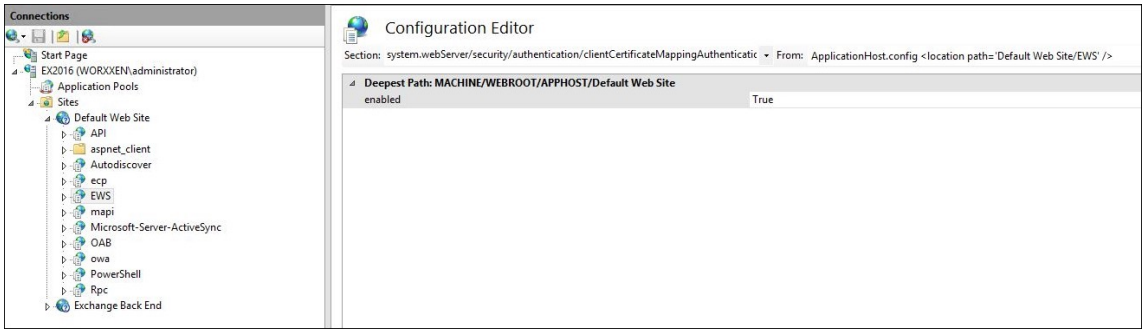


6. Clique em **Editor de configuração** e, na lista suspensa **Seção**, navegue até a seguinte seção:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Defina o valor **enabled** como **True**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

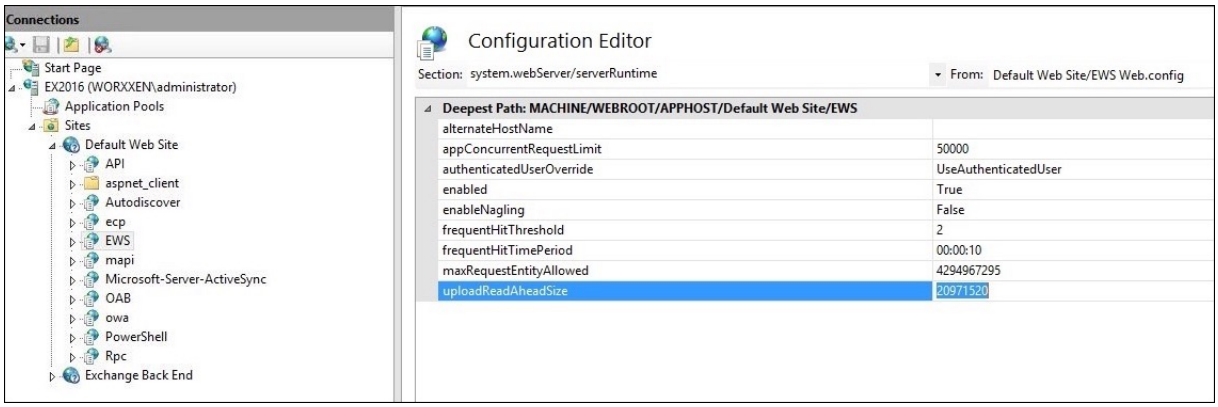


8. Clique em **Editor de configuração** e, na lista suspensa **Seção**, navegue até a seguinte seção:
   - **system.webServer/serverRuntime**
9. Defina o valor de **uploadReadAheadSize** para **10485760** (10 MB) ou **20971520** (20 MB) ou para um valor conforme exigido pela sua organização.

   > Importante:
   >
   > Se você não definir esse valor corretamente, a autenticação baseada em certificado durante o registro nas notificações push do EWS poderá falhar com um código de erro 413.
   >
   > Não defina esse valor como **0.**

Para mais informações, consulte os seguintes recursos de terceiros:

- Tempo de execução do servidor Microsoft IIS
- Blog de Gerenciamento de Cliente Butsch



Para obter mais informações sobre como solucionar problemas do Secure Mail com notificações por push do iOS, consulte este artigo do Citrix Support Knowledge Center.

Informações correlatas

Notificações por Push para o Secure Mail para iOS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).