citrix

Secure Hub

Contents

Citrix Secure Hub

September 29, 2020

O Citrix Secure Hub é a plataforma de lançamento dos aplicativos móveis de produtividade. Os usuários registram seus dispositivos no Secure Hub para obter acesso à loja de aplicativos. Na loja de aplicativos, eles podem adicionar aplicativos móveis de produtividade desenvolvidos pela Citrix e aplicativos de terceiros.

Você pode baixar o Secure Hub e outros componentes da Página de downloads do Citrix Endpoint Management.

Quanto aos requisitos do Secure Hub e de outros sistemas para aplicativos móveis de produtividade, consulte Requisitos do sistema.

Para obter as mais recentes informações sobre aplicativos móveis de produtividade, consulte o artigo Anúncios Recentes.

As seções a seguir listam os novos recursos nas versões atual e anteriores do Secure Hub.

O que há de novo na versão atual

Secure Hub 20.9.0

Secure Hub para iOS

O Secure Hub para iOS suporta o iOS 14 (pré-visualização).

Secure Hub para Android

Esta versão inclui correções de bugs.

O que há de novo em versões anteriores

Secure Hub 20.7.5

Secure Hub para Android

- O Secure Hub para Android suporta o Android 11.
- **Transição do Secure Hub 32 bits para 64 bits para aplicativos**. Na versão 20.7.5 do Secure Hub, o suporte se encerra para a arquitetura de 32 bits para aplicativos, e o Secure Hub foi atualizado para 64 bits. A Citrix recomenda que os clientes atualizem da versão 20.6.5 para a 20.7.5. Se os usuários ignorarem a atualização para o Secure Hub versão 20.6.5 e, em vez disso,

atualizarem diretamente da 20.1.5 para a 20.7.5, eles precisarão autenticar novamente. A reautenticação envolve inserir credenciais e redefinir o PIN do Secure Hub. O Secure Hub versão 20.6.5 está disponível na Google Play Store.

- **Instale atualizações a partir da App Store.** No Secure Hub para Android, se houver atualizações disponíveis para aplicativos, o aplicativo será realçado e o recurso **Atualizações disponíveis** aparecerá na tela da App Store.

  Ao tocar em **Atualizações disponíveis**, você navega até a loja que mostra a lista de aplicativos com atualizações pendentes. Toque em **Detalhes** no aplicativo para instalar as atualizações. Quando o aplicativo for atualizado, a seta para baixo em **Detalhes** mudará para uma marca de seleção.

Secure Hub 20.6.5

Secure Hub para Android

Transição de 32 bits para 64 bits para aplicativos. A versão 20.6.5 do Secure Hub é a versão final que suporta uma arquitetura de 32 bits para aplicativos móveis Android. Nas versões subsequentes, o Secure Hub oferece suporte à arquitetura de 64 bits. A Citrix recomenda que os usuários atualizem para o Secure Hub versão 20.6.5, para que assim os usuários possam atualizar para versões posteriores sem reautenticação. Se os usuários ignorarem a atualização para o Secure Hub versão 20.6.5 e, em vez disso, atualizarem diretamente para 20.7.5, eles precisarão autenticar novamente. A reautenticação envolve inserir credenciais e redefinir o PIN do Secure Hub.

> **Nota:**
>
> A versão 20.6.5 não bloqueia o registro de dispositivos que executam o Android 10 no modo de administrador do dispositivo.

Secure Hub para iOS

Ativar um proxy configurado em dispositivos iOS. O Secure Hub para iOS requer que você habilite uma nova propriedade de cliente, `ALLOW_CLIENTSIDE_PROXY`, se quiser permitir que os usuários usem servidores proxy configurados em **Ajustes > Wi-Fi**. Para obter mais informações, consulte `ALLOW_CLIENTSIDE_PROXY` em Referência da propriedade de cliente.

Secure Hub 20.3.0

> **Nota:**
>
> O suporte para as versões Android 6.x e iOS 11.x do Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace termina em junho de 2020.

Secure Hub para iOS

- **Extensão de rede desativada.** Devido a alterações recentes nas Diretrizes de Revisão da App Store, a partir da versão 20.3.0, o Secure Hub não dará suporte à Extensão de Rede (NE) em dispositivos com iOS. A NE não tem impacto nos aplicativos móveis de produtividade desenvolvidos pela Citrix. No entanto, a remoção da NE tem um certo impacto em aplicativos MDX preparados empresarialmente e implantados. Os usuários finais podem experimentar mudanças extras no Secure Hub durante a sincronização de componentes, como tokens de autorização, timers e tentativas de PIN. Para obter mais informações, consulte https://support.citrix.com/article/CTX270296.

> **Nota:**
>
> Novos usuários não são solicitados a instalar a VPN.

- **Suporte para perfis de registro aprimorado.** O Secure Hub oferece suporte aos recursos de perfil de registro aprimorado anunciados para o Citrix Endpoint Management no Suporte para perfil de registro aprimorado.

Secure Hub 20.2.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub 20.1.5

Esta versão inclui:

- Atualização à formatação e exibição da política de privacidade do usuário. Esta atualização de recurso altera o fluxo de registro do Secure Hub.
- Correções de bugs.

Secure Hub 19.12.5

Esta versão inclui correções de bugs.

Secure Hub 19.11.5

Esta versão inclui correções de bugs.

Secure Hub 19.10.5

Secure Hub para Android

Registrar o Secure Hub no modo COPE. Em dispositivos Android Enterprise, registre o Secure Hub no modo COPE (Propriedade da empresa, habilitado pessoalmente) quando o Citrix Endpoint Management estiver configurado no perfil de registro COPE.

Secure Hub 19.10.0

Esta versão inclui correções de bugs.

Secure Hub 19.9.5

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Suporte para gerenciar recursos do keyguard para o perfil de trabalho Android Enterprise e dispositivos totalmente gerenciados. O Android keyguard gerencia as telas de bloqueio de dispositivo e de Work Challenge. Use a política de dispositivo de Gerenciamento de Keyguard no Citrix Endpoint Management para controlar o gerenciamento de keyguard em dispositivos de perfil de trabalho e o gerenciamento de keyguard em dispositivos totalmente gerenciados e dedicados. Com o gerenciamento de keyguard, você pode especificar os recursos disponíveis para os usuários, como agentes de confiança e câmera segura, antes que eles desbloqueiem a tela de keyguard. Ou, você pode optar por desativar todos os recursos do keyguard.

Para obter mais informações sobre as configurações do recurso e como configurar a política de dispositivo, consulte Política de dispositivo de gerenciamento de keyguard.

Secure Hub 19.9.0

Secure Hub para iOS

O Secure Hub para iOS suporta iOS 13.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub para Android 19.8.5

Esta versão inclui correções de bugs.

Secure Hub 19.8.0

Secure Hub para iOS

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub para Android

Suporte para Android Q. Esta versão inclui suporte para Android Q. Antes de atualizar para a plataforma Android Q, consulte Migrar do Device Administration para o Android Enterprise para obter informações sobre como a substituição de APIs do Google Device Administration afeta os dispositivos que executam o Android Q. Consulte também o blog, Citrix Endpoint Management e Android Enterprise - uma temporada de mudanças.

Secure Hub 19.7.5

Secure Hub para iOS

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub para Android

Suporte para Samsung Knox SDK 3.x. O Secure Hub para Android dá suporte a Samsung Knox SDK 3.x. Para obter mais informações sobre como migrar para o Samsung Knox 3.x, consulte a documentação do desenvolvedor do Samsung Knox. Esta versão também inclui suporte para os novos espaços de nome Samsung Knox. Para obter mais informações sobre alterações aos espaços de nome antigos do Samsung Knox, consulte Alterações aos espaços de nome do Samsung Knox.

> **Nota:**
>
> O Secure Hub para Android não dá suporte ao Samsung Knox 3.x em dispositivos com Android 5.

Secure Hub 19.3.5 a 19.6.6

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Hub 19.3.0

Suporte para Samsung Knox Platform for Enterprise. O Secure Hub para Android suporta o Knox Platform for Enterprise (KPE) em dispositivos Android Enterprise.

Secure Hub 19.2.0

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub 19.1.5

O Secure Hub para Android Enterprise agora oferece suporte às seguintes políticas:

- **Política de dispositivo WiFi.** A política de dispositivo Wi-Fi agora suporta o Android Enterprise. Para obter mais informações sobre esta política, consulte Política de dispositivo Wi-Fi.
- **Política de dispositivo de XML personalizado.** A política de dispositivo XML personalizada agora suporta o Android Enterprise. Para obter mais informações sobre esta política, consulte Política de dispositivo de XML personalizado.
- **Política de dispositivo de arquivo.** Você pode adicionar arquivos de script no Citrix Endpoint Management para executar funções em dispositivos Android Enterprise. Para obter mais informações sobre esta política, consulte Política de dispositivo de arquivo.

Secure Hub 19.1.0

O Secure Hub oferece aprimoramento de fontes, cores e outras melhorias na interface do usuário. Esse aprimoramento fornece uma experiência melhor ao usuário, alinhando-se com a estética da marca Citrix utilizada em nosso conjunto completo de aplicativos móveis de produtividade.

Secure Hub 18.12.0

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub 18.11.5

- **Configurações de política do dispositivo de restrições para Android Enterprise.** As novas configurações da política de dispositivos Restrições permitem que os usuários acessem esses recursos em dispositivos Android Enterprise: barra de status, proteção de tela de bloqueio, gerenciamento de conta, compartilhamento de localização e manutenção da tela do dispositivo ativada em dispositivos Android Enterprise. Para obter informações, consulte Política de dispositivo de restrições.

O Secure Hub 18.10.5 a 18.11.0 inclui aprimoramentos de desempenho e correções de bugs.

Secure Hub 18.10.0

- **Suporte para o modo Samsung DeX:** o Samsung DeX permite que os usuários conectem dispositivos habilitados para KNOX a um monitor externo para usar aplicativos, revisar documentos e

assistir a vídeos em uma interface semelhante a um PC. Para obter informações sobre os requisitos do dispositivo Samsung DeX e a configuração do Samsung DeX, consulte Como funciona o Samsung DeX.

Para configurar os recursos do modo Samsung DeX no Citrix Endpoint Management, atualize a política de dispositivo Restrições para o Samsung Knox. Para obter informações, consulte **Configurações do Samsung KNOX** em Política de dispositivo de restrições.

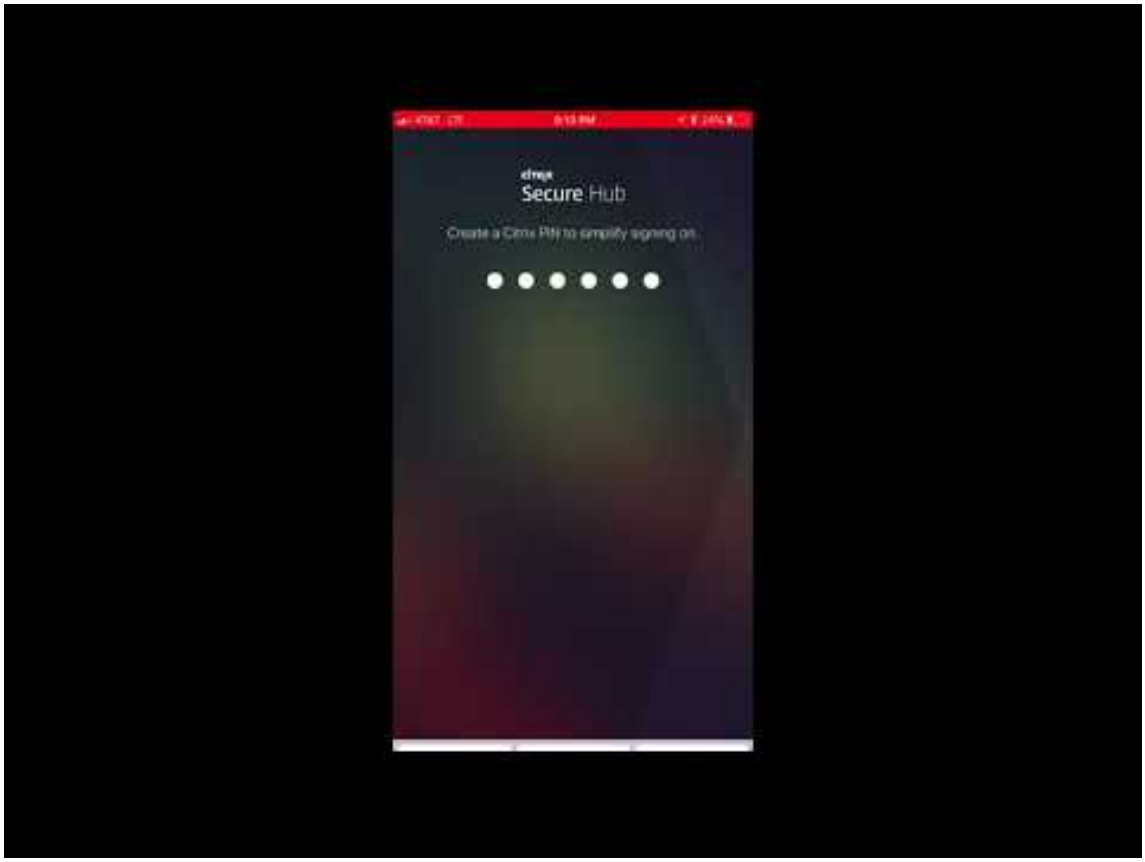
- **Suporte para Android SafetyNet:** você pode configurar o Endpoint Management para usar o recurso **Android SafetyNet** para avaliar a compatibilidade e a segurança de dispositivos Android que têm o Secure Hub instalado. Os resultados podem ser usados para acionar ações automatizadas nos dispositivos. Para obter informações, consulte Android SafetyNet.
- **Prevenir o uso da câmera em dispositivos Android Enterprise:** a nova configuração **Permitir o uso da câmera** da política de dispositivo Restrições permite impedir que os usuários usem a câmera em seus dispositivos Android Enterprise. Para obter informações, consulte Política de dispositivo de restrições.

Secure Hub 10.8.60 a 18.9.0

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Hub 10.8.60

- Suporte para o idioma polonês.
- Suporte para Android P.
- Suporte para o uso da loja de aplicativos do Workspace.
  Ao abrir o Secure Hub, os usuários não verão mais a loja de aplicativos do Secure Hub. O botão **Adicionar aplicativos** leva os usuários para a loja de aplicativos do Workspace. O vídeo a seguir mostra um dispositivo iOS executando uma inscrição no Citrix Endpoint Management usando o aplicativo Citrix Workspace.



> Importante:
>
> Este recurso está disponível apenas para novos clientes. Atualmente, não oferecemos suporte à migração para clientes existentes.

Para usar esse recurso, configure o seguinte:

- Ative as políticas de Senha em cache e Autenticação de senha. Para obter mais informações sobre como configurar políticas, consulte Resumo das políticas de MDX para aplicativos móveis de produtividade.
- Configurar a autenticação do Active Directory como AD ou AD+Cert. Damos suporte a esses dois modos. Para obter mais informações sobre como configurar a autenticação, consulte Configure autenticação de domínio ou de domínio de segurança.
- Habilite a integração do Workspace para o Endpoint Management. Para obter mais informações sobre a integração do espaço de trabalho, consulte Configurar espaços de trabalho.

> **Importante:**
>
> Depois que esse recurso é ativado, o SSO do Citrix Files ocorre por meio do Workspace e não pelo Endpoint Management (anteriormente, XenMobile). Recomendamos que você desative a integração de Citrix Files no console Endpoint Management antes de habilitar a

> integração do Workspace.

Secure Hub 10.8.55

- A capacidade de transmitir um nome de usuário e senha para o portal Google zero-touch e Samsung Knox Mobile Environment (KME) usando a configuração JSON. Para obter detalhes, consulte Registro em massa do Samsung Knox.
- Quando você ativa a fixação de certificado, os usuários não podem se registrar no Endpoint Management com um certificado autoassinado. Se os usuários tentarem se registrar ao Endpoint Management com um certificado autoassinado, eles serão avisados de que o certificado não é confiável.

Secure Hub 10.8.25: Secure Hub para Android inclui suporte para dispositivos Android P.

> **Nota:**
>
> 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 a documentação do desenvolvedor do Android.

Atualização do Secure Hub para iOS em 19 de março de 2018: O Secure Hub versão 10.8.6 para iOS está disponível para corrigir um problema com a política de aplicativo VPP. Para obter detalhes, consulte este artigo do Citrix Knowledge Center.

Secure Hub 10.8.5: suporte no Secure Hub para Android para o modo COSU para o Android Work (Android for Work). Para obter detalhes, consulte a Documentação do Citrix Endpoint Management.

Administração do Secure Hub

Você executa a maioria das tarefas administrativas relacionadas ao Secure Hub durante a configuração inicial do Endpoint Management. Para tornar o Secure Hub disponível para os usuários, para iOS e Android, carregue o Secure Hub no iOS App Store e no Google Play Store.

O Secure Hub também atualiza a maioria das políticas de MDX armazenadas no Endpoint Management para os aplicativos instalados quando uma sessão de usuário do Citrix Gateway se renova após autenticação usando o Citrix Gateway.

> **Importante:**
>
> Alterações a qualquer uma dessas políticas exigem que um usuário exclua e reinstale o aplicativo para aplicar a atualização de política: Grupo de Segurança, Ativar criptografia e o Exchange

> Server do Secure Mail.

PIN da Citrix

Você pode configurar o Secure Hub para usar o PIN da Citrix, um recurso de segurança ativado no console Endpoint Management em **Configurações** > **Propriedades do Cliente**. A configuração requer que os usuários de dispositivos móveis registrados façam logon no Secure Hub e ativem os aplicativos MDX incluídos usando um número de identificação pessoal (PIN).

O recurso de PIN da Citrix simplifica a experiência de autenticação do usuário ao fazer logon nos aplicativos seguros preparados. Os usuários não precisam inserir outra credencial repetidamente, como o nome de usuário e a senha do Active Directory.

Os usuários que fazem logon no Secure Hub pela primeira vez precisam inserir seu nome de usuário e senha do Active Directory. Durante o logon, o Secure Hub salva as credenciais do Active Directory ou um certificado de cliente no dispositivo do usuário e, em seguida, solicita ao usuário para inserir um PIN. Quando o usuário faz logon novamente, ele digita o PIN para acessar seus aplicativos Citrix e o Store com segurança, até que o próximo período de tempo limite de ociosidade termine para a sessão de usuário ativa. Propriedades de cliente correlatas permitem criptografar segredos usando o PIN, especificar o tipo de código secreto para PIN e especificar os requisitos de força e comprimento do PIN. Para obter detalhes, consulte Propriedades do cliente.

Quando a autenticação da impressão digital (Touch ID) está ativada, os usuários podem fazer logon usando impressão digital quando for necessária a autenticação offline devido à inatividade de aplicativo. Os usuários ainda têm que inserir um PIN quando fizerem logon ao Secure Hub pela primeira vez ou ao reiniciar o dispositivo, e depois que o tempo limite de inatividade expirar. Para obter informações sobre como habilitar a autenticação de impressão digital, consulte Autenticação por impressão digital ou por Touch ID.

Fixação de certificado

O Secure Hub para iOS e Android oferecem suporte a fixação de certificado SSL. Esse recurso garante que o certificado assinado por sua empresa seja usado quando clientes Citrix se comunicam com o Endpoint Management, evitando conexões de clientes com o Endpoint Management quando a instalação de um certificado raiz no dispositivo comprometer a sessão SSL. Quando o Secure Hub detecta alterações no servidor chave pública, o Secure Hub nega a conexão.

A partir do Android N, o sistema operacional não permite mais autoridades de certificação (AC) adicionadas pelo usuário. A Citrix recomenda o uso de uma Autoridade de Certificação raiz pública no lugar de uma autoridade de certificação adicionada pelo usuário.

Os usuários que fizerem a atualização para Android N podem ter problemas se usarem autoridades de certificação privadas ou autoassinadas. As conexões em dispositivos Android N são interrompidas

nos seguintes cenários:

- Autoridades de certificação privadas/autoassinadas e a opção Required Trusted CA for Endpoint Management está definida como **ON.** Para obter detalhes, consulte Gerenciamento de dispositivos.
- Autoridades de certificação privadas/autoassinadas e o Endpoint Management AutoDiscovery Service (ADS) não estão acessíveis. Devido a questões de segurança, quando ADS não está acessível, a opção Required Trusted CA é **ativada** mesmo que tenha sido definida como **desativada** inicialmente.

Antes de registrar dispositivos ou atualizar o Secure Hub, considere ativar a fixação de certificados. A opção está **desativada** por padrão e é gerenciada pelo ADS. Quando você ativa a fixação de certificado, os usuários não podem se registrar no Endpoint Management com um certificado autoassinado. Se os usuários tentarem se registrar com um certificado autoassinado, eles serão avisados de que o certificado não é confiável. O registro falhará se os usuários não aceitarem o certificado.

Para usar fixação de certificado, solicite que a Citrix carregue certificados no seu servidor Citrix ADS. Abra um caso de suporte técnico usando o Portal de suporte Citrix. Em seguida, forneça as seguintes informações:

- O domínio que contém as contas com que os usuários se registram.
- O nome de domínio totalmente qualificado (FQDN) do Endpoint Management.
- O nome da instância do Endpoint Management. Por padrão, o nome da instância é zdm e ela diferencia maiúsculas de minúsculas.
- Tipo de ID de usuário, que pode ser UPN ou Email. Como padrão, o tipo é UPN.
- A porta usada para registro de iOS se você tiver alterado o número de porta da porta padrão 8443.
- A porta através da qual o Endpoint Management aceita conexões se você tiver alterado o valor do número de porta padrão 443.
- O URL completo do seu Citrix Gateway.
- Optionalmente, um endereço de email para o seu administrador.
- Os certificados formatados com PEM que você deseja adicionar ao domínio.
- Como lidar com os certificados de servidor existentes: remover o certificado de servidor antigo imediatamente (porque está comprometido) ou continuar a dar suporte ao certificado de servidor antigo até que expire.

O caso do suporte técnico caso é atualizado quando seus detalhes e o certificado tiverem sido adicionados aos servidores Citrix.

Certificado + autenticação de senha de uso único

Você pode configurar o Citrix ADC para que o Secure Hub autentique usando um certificado além de um token de segurança que atua como uma senha de uso único. Esta opção fornece uma configuração

de alta segurança que não deixa rastros do Active Directory nos dispositivos.

Para ativar o Secure Hub para usar o tipo de autenticação Certificado + Senha de uso único, faça o seguinte: adicione uma ação de regravação e uma política de regravação no Citrix ADC que insira um cabeçalho de resposta personalizado do formulário **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar o tipo de logon Citrix Gateway.

Em geral, o Secure Hub usa o tipo de logon do Citrix Gateway configurado no console Endpoint Management. No entanto, essas informações não estão disponíveis para o Secure Hub até que o Secure Hub conclua o logon pela primeira vez. Portanto, o cabeçalho personalizado é obrigatório.

> **Nota:**
>
> Se diferentes tipos de logon forem definidos no Endpoint Management e no Citrix ADC, a configuração do Citrix ADC substituirá. Para obter detalhes, consulte Citrix Gateway e Endpoint Management.

1. No Citrix ADC, navegue para **Configuration > AppExpert > Rewrite > Actions**.
2. Clique em **Adicionar**.

   É exibida a tela **Create Rewrite Action**.
3. Preencha cada campo conforme mostrado na figura a seguir e, em seguida, clique em **Create**.

   O resultado é exibido na tela principal **Rewrite Actions**.
4. Vincule a ação de regravar ao servidor virtual como uma política de regravação. Vá para **Configuration > NetScaler Gateway > Virtual Servers**e depois selecione seu servidor virtual.
5. Clique em **Edit**.
6. Na tela **Virtual Servers configuration**, role até **Policies**.
7. Clique em **+** para adicionar uma política.
8. No campo **Choose Policy**, selecione **Rewrite**.
9. No campo **Choose Type**, selecione **Response**.
10. Clique em **Continue**.

    A seção **Policy Binding** se expande.
11. Clique em **Select Policy**.

    É exibida uma tela com políticas disponíveis.
12. Clique na linha da política que você criou e clique em **Select**. A tela **Policy Binding** aparece novamente, com a sua política selecionada preenchida.
13. Clique em **Bind**.

Se a associação for bem-sucedida, é exibida a principal tela de configuração com a política de reescrever concluída exibida.

14. Para exibir os detalhes da política, clique em **Rewrite Policy**.

Requisito de porta para conectividade ADS para dispositivos Android

A configuração de porta garante que dispositivos Android que se conectam do Secure Hub possam acessar o Citrix ADS de dentro da rede corporativa. A capacidade de acessar ADS é importante ao baixar as atualizações de segurança disponibilizadas por meio do ADS. As conexões ADS podem não ser compatíveis com o servidor proxy. Nesse cenário, permita que a conexão do ADS ignore o servidor proxy.

> **Importante:**
>
> O Secure Hub para Android e iOS exige que você permita que dispositivos Android acessem o ADS. Para obter detalhes, consulte Requisitos de porta na documentação do Citrix Endpoint Management. Essa comunicação é na porta de saída 443. É altamente provável que o ambiente existente tenha sido criado para permitir isso. Recomenda-se aos clientes que não possam garantir essa comunicação que não atualizem para o Secure Hub 10.2. Se tiver alguma dúvida, entre em contato com o Atendimento ao Cliente Citrix.

Pré-requisitos:

- Colete os certificados do Endpoint Management e do Citrix ADC. Os certificados precisam estar no formato PEM e devem ser um certificado público e não a chave privada.
- Entre em contato com o suporte da Citrix e faça uma solicitação para permitir a fixação de certificado. Durante este processo, você será solicitado a fornecer seus certificados.

As melhorias do novo certificado de fixação exigem que os dispositivos se conectem ao ADS antes de o dispositivo se registrar. Esse pré-requisito garante que as informações de segurança mais recentes estejam disponíveis ao Secure Hub para o ambiente no qual o dispositivo está se registrando. Se os dispositivos não puderem alcançar o ADS, o Secure Hub não permitirá o registro do dispositivo. Portanto, a abertura de acesso a ADS na rede interna é crítica para possibilitar que os dispositivos se registrem.

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

FQDN	Endereço IP	Porta	Uso de IP e porta
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS Communication
`discovery.mdm.zenprise.com`	52.1.30.122	443	Secure Hub - ADS Communication

FQDN	Endereço IP	Porta	Uso de IP e porta
ads.xm.cloud.com: observe que o Secure Hub versão 10.6.15 e posterior usa ads.xm.cloud.com.	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com: observe que o Secure Hub versão 10.6.15 e posterior usa ads.xm.cloud.com.	34.193.202.23	443	Secure Hub - ADS Communication

Se a fixação de certificado estiver ativada:

- O Secure Hub fixa o certificado corporativo durante o registro do dispositivo.
- Durante uma atualização, o Secure Hub descarta os certificados fixados e, em seguida, fixa o certificado do servidor na primeira conexão para usuários registrados.

  > **Nota:**
  >
  > Se você ativar a fixação de certificado após uma atualização, os usuários devem fazer novo registro.

- A renovação do certificado não exige o processo de novo registro, se a chave pública de certificado não tiver sido alterada.

A fixação de certificado dá suporte a certificados de folha, mas não certificados intermediários ou certificados de emissor. A fixação de certificado se aplica a servidores Citrix, como, por exemplo, Endpoint Management e Citrix Gateway, e não a servidores de terceiros.

Usando o Secure Hub

Os usuários começam com o download do Secure Hub para seus dispositivos a partir das lojas de aplicativos Apple ou Android.

Quando o Secure Hub é aberto, os usuários digitam as credenciais fornecidas pela sua empresa para registrar seus dispositivos no Secure Hub. Para obter mais detalhes sobre o registro de dispositivos, consulte Contas de usuário, funções e registro.

No Secure Hub para Android, durante a instalação inicial e registro, aparece a seguinte mensagem: Permitir que o Secure Hub acesse fotos, mídia e arquivos em seu dispositivo?

Esta mensagem vem do sistema operacional Android e não da Citrix. Quando você toca em **Allow**, a Citrix e os administradores que administram o Secure Hub não veem seus dados pessoais em nenhum momento. Se, no entanto, você realizar uma sessão de suporte remoto com seu administrador, o administrador pode visualizar seus arquivos pessoais dentro da sessão.

Depois de inscritos, os usuários veem os aplicativos e áreas de trabalho que você enviou nas respectivas guias **My Apps**. Os usuários podem adicionar mais aplicativos do Store. Nos telefones o link do Store está sob o ícone de **configurações** tipo hambúrguer no canto superior esquerdo.

Em tablets, o Store é uma guia separada.

Quando usuários com iPhones com iOS 9 ou posterior instalam aplicativos móveis de produtividade da loja, eles veem uma mensagem. A mensagem afirma que o desenvolvedor corporativo, Citrix, não é confiável nesse iPhone. A mensagem observa que o aplicativo não está disponível para uso até que o desenvolvedor seja confiável. Quando esta mensagem é exibida, o Secure Hub avisa aos usuários para exibir um guia que os orienta pelo processo de confiar nos aplicativos empresariais Citrix para seu iPhone.

Registro automático no Secure Mail

Para as implantações somente MAM, você pode configurar o Endpoint Management para que os usuários com dispositivos Android ou iOS que se registrarem no Secure Hub com credenciais de email sejam automaticamente registrados no Secure Mail. Os usuários não têm que digitar mais informações nem executar mais etapas para se registrarem no Secure Mail.

Ao ser usado pela primeira vez, o Secure Mail obtém do Secure Hub o endereço de email do usuário, o domínio e a identificação de usuário. O Secure Mail usa o endereço de email no AutoDiscovery. O Exchange Server é identificado com o uso do domínio e ID de usuário, o que permite que o Secure Mail autentique o usuário automaticamente. O usuário é solicitado a inserir uma senha se a política estiver configurada para não passar pela senha. O usuário não é, no entanto, obrigado a inserir mais informações.

Para ativar esse recurso, crie três propriedades:

- A propriedade do servidor MAM_MACRO_SUPPORT. Para obter instruções, consulte Propriedades do servidor.
- As propriedades de cliente ENABLE_CREDENTIAL_STORE e SEND_LDAP_ATTRIBUTES. Para obter instruções, consulte Propriedades do cliente.

Loja personalizada

Se você deseja personalizar sua Store, vá para **Settings > Client Branding** para alterar o nome, adicionar um logotipo e especificar como os aplicativos serão exibidos.

Você pode editar as descrições do aplicativo no console Endpoint Management. Clique em **Configure** e em **Apps**. Selecione o aplicativo na tabela e clique em **Edit**. Selecione as plataformas para o aplicativo com a descrição que você está editando e digite o texto na caixa **Description**.

No Store, os usuários poderão procurar somente os aplicativos e áreas de trabalho que você tiver configurado e protegido no Endpoint Management. Para adicionar o aplicativo, os usuários devem tocar em **Details** e depois em **Add**.

Opções configuradas de Help

O Secure Hub também oferece aos usuários várias formas de obter ajuda. Em tablets, tocar o ponto de interrogação no canto superior direito abre as opções de ajuda. Em telefones, os usuários devem tocar no ícone de hambúrguer no canto superior esquerdo e depois tocar em **Help**.

Your IT Department mostra o telefone e o email do suporte técnico de sua empresa, que os usuários podem acessar diretamente do aplicativo. Você pode inserir números de telefone e endereços de email no console Endpoint Management. Clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida. Clique em **More** e em **Client Support**. É exibida a tela em que você insere as informações.

Report Issue mostra uma lista de aplicativos. Os usuários devem selecionar o aplicativo que apresenta o problema. O Secure Hub gera automaticamente os logs e abre uma mensagem em Secure Mail com os logs anexados como um arquivo zip. Os usuários podem adicionar linhas de assunto e descrição do problema. Eles também podem anexar uma captura de tela.

Send Feedback to Citrix abre uma mensagem no Secure Mail com um endereço de suporte da Citrix preenchido. No corpo da mensagem, o usuário pode fornecer sugestões para melhorar o Secure Mail. Se o Secure Mail não estiver instalado no dispositivo, o programa de email nativo será aberto.

Os usuários também podem tocar em **Suporte Citrix,** que abre o Citrix Knowledge Center. Ali eles podem pesquisar artigos de suporte para todos os produtos da Citrix.

Em **Preferences**, os usuários podem encontrar informações sobre suas contas e dispositivos.

Políticas de localização

O Secure Hub também fornece políticas de localização geográfica e rastreio geográfico se, por exemplo, você desejar garantir que um dispositivo pertencente à empresa não invade um determinado perímetro geográfico. Para obter detalhes, consulte Política de dispositivo de localização.

Coleta e a análise de panes

O Secure Hub coleta automaticamente e analisa informações de falhas para que você possa ver o que levou a uma determinada falha. O software Crashlytics suporta essa função.

Para obter mais recursos disponíveis para iOS e Android, consulte a matriz Recursos por plataforma para o Citrix Secure Hub.

Problemas conhecidos e resolvidos

September 10, 2020

A Citrix oferece suporte a atualizações das duas últimas versões dos aplicativos móveis de produtividade.

Secure Hub 20.9.0

Secure Hub para iOS

Problemas conhecidos no Secure Hub 20.9.0

Não há problemas conhecidos nesta versão.

Problemas resolvidos no Secure Hub 20.9.0

- No Secure Hub para iOS, quando a fixação de certificados está ativada, as conexões são estabelecidas entre servidores, mesmo que o certificado fixado de um dos servidores esteja incorreto. [CXM-84028]
- No Secure Hub para iOS, você não recebe notificações. Você recebe o seguinte erro: **Não há dispositivos com um token válido do Secure Hub**. [CXM-84228]

Secure Hub 20.7.5

Problemas conhecidos no Secure Hub 20.7.5

Em dispositivos corporativos para uso único (COSU) que executam o Android 11, você não pode definir o Secure Hub como o Launcher padrão. [CXM-80244]

Problemas resolvidos no Secure Hub 20.7.5

- No Secure Hub para Android, o registro de dispositivos Android falha quando a fixação de certificado está habilitada. [CXM-74371]
- No Secure Hub para Android, o recurso **Alteração de data e hora** na política de Restrições não funciona em dispositivos Samsung. [CXM-79757]
- No Secure Hub para Android, a política de firewall não funciona em dispositivos Samsung que executam as versões 19.12.5 e posteriores. [CXM-79785]

- No Secure Hub para Android, não é possível desinstalar aplicativos em **Meus aplicativos**. [CXM-80668]

Secure Hub 20.6.5

Não há problemas conhecidos nem resolvidos nesta versão.

Problemas conhecidos e resolvidos em versões anteriores

Para ver os problemas conhecidos e resolvidos em versões anteriores do Secure Hub, consulte Histórico de problemas conhecidos e resolvidos do Secure Hub.

Aviso de autenticação de cenários

April 16, 2019

Vários cenários avisam aos usuários para autentiquem com o Secure Hub digitando suas credenciais nos respectivos dispositivos.

Os cenários se alteram dependendo destes fatores:

- Sua política de aplicativo MDX e a configuração da Propriedade do Cliente nas configurações do console Endpoint Management.
- Se a autenticação ocorrer offline ou precisar ser uma autenticação online (o dispositivo precisa de uma conexão de rede com o Endpoint Management).

Além disso, o tipo das credenciais que os usuários digitam, como senha do Active Directory, o PIN da Citrix ou código secreto, senha de uso único, autenticação por impressão digital (conhecida como Touch ID no iOS), também muda com base no tipo de autenticação e na frequência de autenticação de que você precisa.

Vamos começar com os cenários que resultam em um aviso para autenticação.

- **Reinicialização do dispositivo:** Quando os usuários reiniciam seus dispositivos, eles devem se autenticar novamente com o Secure Hub.
- **Inatividade offline (tempo limite):** Com a política de MDX Código secreto de aplicativo ativada, que é ativada por padrão, a propriedade cliente do Endpoint Management chamada Timer de Inatividade entra em ação. O Timer de Inatividade limita o período em que pode não haver nenhuma atividade dos aplicativos que usam o contêiner seguro.

Quando o tempo do Timer de Inatividade se esgota, os usuários devem reautenticar ao contêiner seguro no dispositivo. Se, por exemplo, os usuários pousarem seus dispositivos e se afastarem, se o

tempo do Timer de Inatividade expirar, nenhuma outra pessoa poderá pegar o dispositivo e ter acesso a dados confidenciais presentes no contêiner. A propriedade do Timer de Inatividade pode ser configurada no console Endpoint Management. O padrão é 15 minutos. A combinação do código secreto do aplicativo definido como **ON** e a propriedade cliente do Timer de Inatividade é responsável por provavelmente o cenário mais comum de aviso para autenticação.

- **Logoff do Secure Hub**. Quando os usuários fazem logoff do Secure Hub, eles precisam autenticar novamente na próxima vez que acessam o Secure Hub ou qualquer aplicativo MDX, quando o aplicativo requer um código secreto, conforme determinado pela política de Código secreto do aplicativo de MDX e o status do Timer de Inatividade.
- **Período máximo offline**. Este cenário é específico para aplicativos porque é controlado por uma política de MDX por aplicativo. A política Período máximo offline de MDX tem uma configuração padrão de 3 dias. Se o período de tempo para que um aplicativo seja executado sem autenticação online com o Secure Hub se esgotar, é necessário um check-in com o Endpoint Management para confirmar o direito do aplicativo e para atualizar as políticas. Quando esse check-in ocorre, o aplicativo faz com que o Secure Hub exija uma autenticação online. Os usuários devem reautenticar para que possam ter acesso ao aplicativo MDX.

Observe que a relação entre o período máximo offline e a política de período de sondagem ativa de MDX:

- O período de sondagem ativa é o período durante o qual os aplicativos fazem check-in com o Endpoint Management para realizar ações de segurança, como bloqueio de aplicativo e apagamento de aplicativo. Além disso, o aplicativo também verifica se há atualizações de políticas de aplicativo.
- Depois que uma verificação bem-sucedida de políticas por meio da política Active poll period, o timer do Maximum offline period é zerado e começa a fazer uma nova contagem regressiva.

Os dois check-ins com o Endpoint Management, relativo a Active poll period e Maximum offline period expiry, requerem um token válido de do Citrix Gateway no dispositivo. Se o dispositivo tiver um token válido do Citrix Gateway, o aplicativo recupera novas políticas do Endpoint Management sem interrupções para os usuários. Se o aplicativo precisar de um Citrix Gateway, ocorre uma passagem para o Secure Hub e os usuários veem um aviso para autenticar no Secure Hub.

Em dispositivos Android, as telas de atividade do Secure Hub se abrem diretamente sobre a tela do aplicativo atual. Em dispositivos iOS, no entanto, o Secure Hub deve vir para o primeiro plano, o que temporariamente muda a posição do aplicativo atual.

Após os usuários inserirem suas credenciais, o Secure Hub passa para o aplicativo original. Se, nesse caso, você permitir credenciais em cache do Active Directory ou tiver um certificado de cliente configurado, os usuários podem inserir um PIN, senha ou autenticação de impressões digitais. Caso contrário, os usuários devem fornecer suas credenciais do Active Directory completas.

O token do Citrix ADC pode tornar-se inválido por causa de inatividade na sessão do Citrix Gateway

ou a imposição de um tempo limite de sessão, como comentado na seguinte lista de políticas do Citrix Gateway. Quando os usuários fazem logon no Secure Hub novamente, eles podem continuar a executar o aplicativo.

- **Políticas de sessão do Citrix Gateway:** duas políticas do Citrix Gateway também têm influência quando os usuários são avisados para autenticar. Nesses casos, eles autenticam para criar uma sessão online com o Citrix ADC para conexão com o Endpoint Management.
  - **Tempo limite da sessão:** A sessão do Citrix ADC para o Endpoint Management é desconectada se não ocorrer nenhuma atividade de rede por um determinado período de tempo. O padrão é 30 minutos. No entanto, se você usar o Assistente do Citrix Gateway para configurar a política, o padrão é 1440 minutos. Os usuários versão um aviso para autenticação para reconectar à sua rede corporativa.
  - **Tempo limite forçado:** Se o valor for **Ativado**, a sessão do Citrix ADC para o Endpoint Management é desconectada depois que o período de tempo limite tiver se esgotado. O tempo limite imposto torna obrigatória a reautenticação depois de um determinado período de tempo. Os usuários versão um aviso para autenticação para reconectar à sua rede corporativa no próximo uso. O padrão é **Off**. No entanto, se você usar o Assistente do Citrix Gateway para configurar a política, o padrão é 1440 minutos.

Tipos de Credenciais

A seção anterior tratou de quando os usuários são solicitados a autenticar. Esta seção trata dos tipos de credenciais que eles devem inserir. É necessário efetuar autenticação por meio de vários métodos para obter acesso a dados criptografados no dispositivo. Para desbloquear inicialmente o dispositivo, você deve desbloquear o *contêiner primário*. Após isso ocorrer. e o contêiner estar protegido, para obter acesso, você deve desbloquear um *contêiner secundário*.

> Nota:
>
> Quando o artigo se refere a um *aplicativo gerenciado*, o termo se refere a um aplicativo preparado com o MDX Toolkit, no qual você deixou a política de senha de aplicativo MDX habilitada por padrão e aproveita a propriedade de Timer de Inatividade do cliente.

As circunstâncias que determinam o tipo de credencial são os seguintes:

- **Desbloqueio de contêiner primário:** Uma senha do Active Directory, PIN da Citrix ou código secreto, senha de uso único, Touch ID ou impressão digital são necessárias para desbloquear o contêiner primário.
  - No iOS, quando os usuários abrem o Secure Hub ou um aplicativo gerenciado pela primeira vez após o aplicativo estar instalado no dispositivo.
  - No iOS, quando os usuários reiniciam um dispositivo e, em seguida, abrem o Secure Hub.
  - No Android, quando os usuários abrem um aplicativo gerenciado se o Secure Hub não estiver em execução.

  - No Android, quando os usuários reiniciam o Secure Hub por qualquer motivo, incluindo uma reinicialização do dispositivo.
- **Desbloqueio de contêiner secundário:** Autenticação com impressão digital (se configurada), ou um PIN da Citrix ou código secreto ou credenciais do Active Directory para desbloquear o contêiner secundário.
  - Quando os usuários abrem um aplicativo depois que o timer de inatividade expira.
  - Quando os usuários fazem logoff do Secure Hub e subsequentemente abrem um aplicativo gerenciado.

São necessárias credenciais do Active Directory para a circunstância DE desbloquear o contêiner quando as seguintes condições são verdadeiras:

- Quando os usuários alteram a senha associada à sua conta corporativa.
- Quando você não tiver definido propriedades de cliente no console Endpoint Management para ativar o PIN da Citrix: ENABLE_PASSCODE_AUTH e ENABLE_PASSWORD_CACHING.
- Quando a sessão do NetScaler Gateway termina, o que ocorre sob as seguintes circunstâncias: quando se esgota o tempo limite da sessão ou se esgota o timer imposto da política de tempo limite, se o dispositivo não armazenar em cache as credenciais ou não tiver um certificado cliente.

Quando a autenticação da impressão digital está ativada, os usuários agora podem fazer logon usando uma impressão digital quando for necessária a autenticação offline devido à inatividade de aplicativo. Os usuários ainda têm que inserir um PIN quando fizerem logon ao Secure Hub pela primeira vez ou ao reiniciar o dispositivo. Para obter informações sobre como habilitar a autenticação de impressão digital, consulte Autenticação por impressão digital ou por Touch ID.

O fluxograma a seguir resume o fluxo de decisão que determina que credenciais um usuário deve fornecer quando é solicitado a se autenticar.

Sobre as alternâncias de tela do Secure Hub

Outra situação que deve ser notada é quando é necessária a alternância de um aplicativo para o Secure Hub e depois de volta a um aplicativo. A alternância exibe uma notificação que deve ser confirmada pelos usuários. Não é necessária a autenticação quando isso ocorre. A situação ocorre após ser efetuado um check-in com o Endpoint Management, conforme especificado pelas políticas Maximum offline period e Active poll period e o Endpoint Management detectar políticas atualizadas que precisam ser enviadas para o dispositivo através do Secure Hub.

Registro de dispositivos usando credenciais derivadas

June 12, 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 Personal Identity Verification (PIV) ou um Common Access Card (CAC).

As credenciais derivadas são um certificado de registro que contém o identificador de usuário, como UPN. O Endpoint Management armazena as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

O Endpoint Management pode usar credenciais derivadas para registro de dispositivo iOS. Se configurado para credenciais derivadas, o Endpoint Management não dá suporte a convites de registro ou outros modos de registro para dispositivos iOS. No entanto, você pode usar o mesmo Endpoint Management para registrar os dispositivos Android por meio de convites de registro e outros modos de registro.

Etapas de registro do dispositivo ao usar derivados de credenciais

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. Nesse exemplo, o aplicativo do provedor de identidade é o Intercede MyID Identity Agent.
2. O usuário inicia o Secure Hub. Quando solicitado, o usuário digita o nome de domínio totalmente qualificado (FQDN) do Endpoint Management e clica em **Avançar**. O registro no Secure Hub é iniciado. Se o Endpoint Management oferecer suporte a credenciais derivadas, o Secure Hub solicita ao usuário que crie um PIN da Citrix.
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.
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.

   O usuário insere seu PIN do Secure Hub quando solicitado.

Depois de autenticar o PIN, o Secure Hub baixa os certificados. O usuário segue os prompts para concluir o registro.

Para exibir informações sobre o dispositivo no console Endpoint Management, siga um destes procedimentos:

- Vá para **Gerenciar > Dispositivos** e selecione um dispositivo para exibir uma caixa de comando. Clique em **Mostrar mais.**
- Vá para **Analisar > Painel**.

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