



Secure Hub

Contents

Citrix Secure Hub™	19
Administrando o Secure Hub	19
PIN Citrix	19
Fixação de certificado	20
Configurando autenticação de certificado + senha de uso único para o Secure Hub	21
Requisito de porta para conectividade ADS para dispositivos Android	27
Recursos do Secure Hub	29
Citrix Secure Hub™	35
Novidades na versão atual	35
Secure Hub para iOS 26.8.1	35
Secure Hub para Android 26.8.0	36
Defina um aplicativo de inicialização automática na política de Configuração do Launcher no modo COSU	36
Detecção e renovação automáticas do certificado de dispositivo MDM	36
Novidades em versões anteriores	36
Secure Hub para iOS 26.8.0	36
Suporte para iOS/iPadOS 27	36
Secure Hub para Android 26.5.0	36
Suporte para Android 17	36
Secure Hub para Android 26.2.0	37
Aprimoramento da solução de problemas do certificado do dispositivo	37
Secure Hub para iOS 25.8.0	38
Suporte para iOS 26	38
Secure Hub para Android 25.10.0	38
Suporte para tamanho de página de memória de 16 KB	38
Secure Hub para Android 25.7.0	38

Secure Hub para iOS 25.6.0	38
Secure Hub para Android 25.4.0	39
Suporte para Android 16	39
Suporte para o protocolo TLS 1.3	39
Secure Hub para Android 25.1.0	39
Secure Hub para iOS 25.1.0	39
Secure Hub para iOS 24.11.0	39
Secure Hub para Android 24.10.0	40
Suporte para Android 15	40
Secure Hub para iOS 24.9.0	40
Exibe Termos e Condições no Programa de Registro de Dispositivos	40
Secure Hub para Android 24.8.0	40
Verificação de conformidade em dispositivos Android (Technical Preview)	40
Secure Hub para Android 24.6.0	41
Coleta e relatório de logs aprimorados	41
Secure Hub para iOS 24.5.0	42
Suporta Retorno ao Serviço do iOS 17	42
Secure Hub para Android 24.3.0	42
Suporta Samsung Knox Enhanced Attestation v3	42
Secure Hub para Android 23.12.0	43
Segurança Aprimorada com Samsung Knox	43
Acessar o Secure Mail do perfil pessoal do usuário	43
Secure Hub para iOS 24.1.0	44
Secure Hub para Android 23.12.0	44
Adicionar uma dica sobre o PIN de autenticação na página de login	44
A autenticação nFactor oferece suporte ao recurso de logon único	45
Suporte a limpeza completa no modo de inicialização direta	45
Velocidade de carregamento otimizada da App Store do Secure Hub	45

Secure Hub para iOS 23.11.0	45
Adicionar uma dica sobre o PIN de autenticação na página de login	45
A autenticação nFactor oferece suporte ao recurso de logon único	45
Secure Hub 23.10.0	46
Secure Hub para Android	46
Secure Hub 23.9.0	46
Secure Hub para Android	46
Secure Hub 23.8.1	46
Secure Hub para iOS	46
Secure Hub 23.8.0	46
Secure Hub para iOS	46
Secure Hub 23.7.0	46
Secure Hub para Android	46
Secure Hub 23.4.0	47
Secure Hub para iOS	47
Secure Hub 23.4.1	48
Secure Hub para Android	48
Secure Hub 23.4.0	48
Secure Hub para Android	48
Secure Hub 23.2.0	48
Secure Hub para Android	48
Secure Hub 22.11.0	49
Secure Hub para Android	49
Secure Hub 22.9.0	49
Secure Hub para Android	49
Secure Hub 22.7.0	51
Secure Hub para Android	51
Secure Hub 22.6.0	51

Secure Hub para Android	51
Secure Hub 22.5.0	51
Secure Hub para iOS	51
Secure Hub 22.4.0	51
Secure Hub para Android	51
Secure Hub 22.2.0	51
Secure Hub para iOS	51
Secure Hub para Android	52
Secure Hub 21.11.0	52
Secure Hub para Android	52
Secure Hub 21.10.0	52
Secure Hub para iOS	52
Secure Hub para Android	52
Secure Hub 21.8.0	52
Secure Hub para iOS	52
Secure Hub 21.7.1	52
Secure Hub para Android	52
Secure Hub 21.7.0	53
Secure Hub para iOS	53
Secure Hub para Android	53
Secure Hub 21.6.0	53
Secure Hub para iOS	53
Secure Hub para Android	53
Secure Hub 21.5.1	53
Secure Hub para iOS	53
Secure Hub para Android	53
Secure Hub 21.5.0	54
Secure Hub para iOS	54

Secure Hub 21.4.0	54
Secure Hub 21.3.2	54
Secure Hub para iOS	54
Secure Hub 21.3.0	54
Secure Hub 21.2.0	54
Secure Hub para Android	54
Secure Hub 21.1.0	54
Secure Hub para iOS	54
Secure Hub para Android	54
Secure Hub 20.12.0	54
Secure Hub para iOS	54
Secure Hub para Android	55
Secure Hub 20.11.0	55
Secure Hub para Android	55
Secure Hub 20.10.5	55
Secure Hub 20.9.0	55
Secure Hub para iOS	55
Secure Hub para Android	55
Secure Hub 20.7.5	55
Secure Hub para Android	55
Secure Hub 20.6.5	56
Secure Hub para Android	56
Secure Hub para iOS	56
Secure Hub 20.3.0	56
Secure Hub para iOS	57
Secure Hub 20.2.0	57
Secure Hub para iOS	57
Secure Hub 20.1.5	57

Secure Hub 19.12.5	57
Secure Hub 19.11.5	57
Secure Hub 19.10.5	58
Secure Hub para Android	58
Secure Hub 19.10.0	58
Secure Hub 19.9.5	58
Secure Hub para iOS	58
Secure Hub para Android	58
Secure Hub 19.9.0	58
Secure Hub para iOS	58
Secure Hub para Android	58
Secure Hub para Android 19.8.5	59
Secure Hub 19.8.0	59
Secure Hub para iOS	59
Secure Hub para Android	59
Secure Hub 19.7.5	59
Secure Hub para iOS	59
Secure Hub para Android	59
Secure Hub 19.3.5 a 19.6.6	59
Secure Hub 19.3.0	60
Secure Hub 19.2.0	60
Secure Hub 19.1.5	60
Secure Hub 19.1.0	60
Secure Hub 18.12.0	60
Secure Hub 18.11.5	60
Secure Hub 18.10.0	61
Secure Hub 10.8.60 a 18.9.0	61
Secure Hub 10.8.60	61

Secure Hub 10.8.55	63
Administrando o Secure Hub	63
PIN do Citrix	64
Fixação de certificado	64
Autenticação por certificado + senha de uso único	66
Requisito de porta para conectividade ADS para dispositivos Android	71
Desabilitando a opção Excluir Conta	73
Usando o Secure Hub	74
Registro automático no Secure Mail	76
Loja Personalizada	77
Opções de Ajuda Configuradas	78
Políticas de localização	79
Coleta e análise de falhas	79
Gerar logs do lado do dispositivo para o Secure Hub	80
Problemas conhecidos e corrigidos	81
Secure Hub para iOS 26.8.1	81
Problemas corrigidos	81
Problemas conhecidos	81
Secure Hub para Android 26.8.0	81
Problemas corrigidos	81
Problemas conhecidos	82
Secure Hub para iOS 26.8.0	82
Problemas corrigidos	82
Problemas conhecidos	82
Secure Hub para Android 26.5.0	82
Problemas corrigidos	82
Problemas conhecidos	83
Secure Hub para Android 26.2.0	83

Problemas corrigidos	83
Problemas conhecidos	83
Secure Hub para Android 25.10.0	83
Problemas corrigidos	83
Problemas conhecidos	83
Secure Hub para iOS 25.8.0	83
Problemas corrigidos	83
Problemas conhecidos	83
Secure Hub para Android 25.7.0	84
Problemas corrigidos	84
Problemas conhecidos	84
Secure Hub para iOS 25.6.0	84
Problemas corrigidos	84
Problemas conhecidos	84
Secure Hub para Android 25.4.0	84
Problemas corrigidos	84
Problemas conhecidos	84
Secure Hub para iOS 25.1.0	85
Problemas corrigidos	85
Problemas conhecidos	85
Secure Hub para Android 25.1.0	85
Problemas corrigidos	85
Problemas conhecidos	85
Secure Hub para iOS 24.11.0	85
Problemas corrigidos	85
Problemas conhecidos	85
Secure Hub para Android 24.10.0	85
Problemas corrigidos	85

Problemas conhecidos	85
Secure Hub para iOS 24.9.0	86
Problemas corrigidos	86
Problemas conhecidos	86
Secure Hub para Android 24.8.0	86
Problemas corrigidos	86
Problemas conhecidos	86
Secure Hub para Android 24.6.0	86
Problemas corrigidos	86
Problemas conhecidos	86
Secure Hub para iOS 24.5.0	86
Problemas corrigidos	86
Problemas conhecidos	86
Secure Hub para Android 24.3.0	87
Problemas corrigidos	87
Problemas conhecidos	87
Secure Hub para iOS 24.1.0	87
Problemas corrigidos	87
Secure Hub para Android 23.12.0	88
Problemas corrigidos	88
Secure Hub para iOS 23.11.0	88
Problemas corrigidos	88
Secure Hub para Android 23.10.0	88
Problemas corrigidos	88
Problemas conhecidos	88
Secure Hub para Android 23.9.0	89
Problemas corrigidos	89
Problemas conhecidos	89

Secure Hub para iOS 23.8.1	89
Problemas corrigidos	89
Problemas conhecidos	89
Secure Hub para iOS 23.8.0	89
Problemas corrigidos	89
Problemas conhecidos	89
Problemas conhecidos e corrigidos em versões anteriores	89
Histórico de problemas conhecidos e corrigidos do Secure Hub	90
Secure Hub para Android 23.7.0	90
Problemas corrigidos	90
Problemas conhecidos	90
Secure Hub para iOS 23.4.0	91
Problemas corrigidos	91
Problemas conhecidos	91
Secure Hub para Android 23.4.1	91
Problemas corrigidos	91
Problemas conhecidos	91
Secure Hub para Android 23.4.0	91
Problemas corrigidos	91
Problemas conhecidos	91
Secure Hub para Android 23.2.0	92
Problemas corrigidos	92
Secure Hub 22.11.0	92
Secure Hub 22.9.0	92
Secure Hub 22.7.0	93
Problemas corrigidos	93
Secure Hub 22.6.0	93
Secure Hub 22.5.0	93

Secure Hub 22.4.0	93
Secure Hub 22.2.0	93
Problemas conhecidos no Secure Hub 22.2.0	93
Problemas corrigidos no Secure Hub 22.2.0	93
Secure Hub para iOS	93
Secure Hub para Android	94
Secure Hub 21.11.0	94
Problemas conhecidos no Secure Hub 21.11.0	94
Problemas corrigidos no Secure Hub 21.11.0	94
Secure Hub para Android	94
Secure Hub 21.10.0	95
Problemas conhecidos no Secure Hub 21.10.0	95
Problemas corrigidos no Secure Hub 21.10.0	95
Secure Hub para iOS	95
Secure Hub para Android	95
Secure Hub 21.8.0	95
Secure Hub para iOS	95
Problemas conhecidos no Secure Hub 21.8.0	95
Problemas corrigidos no Secure Hub 21.8.0	95
Secure Hub 21.7.1	96
Secure Hub para Android	96
Problemas conhecidos e corrigidos em versões anteriores	96
Secure Hub 21.7.1	96
Secure Hub para Android	96
Secure Hub 21.7.0	96
Secure Hub para iOS	96
Secure Hub para Android	96
Problemas conhecidos no Secure Hub 21.7.0	96

Problemas corrigidos no Secure Hub 21.7.0	96
Secure Hub 21.6.0	96
Secure Hub para iOS	96
Problemas conhecidos no Secure Hub 21.6.0	96
Problemas corrigidos no Secure Hub 21.6.0	97
Secure Hub para Android	97
Problemas conhecidos no Secure Hub 21.6.0	97
Problemas corrigidos no Secure Hub 21.6.0	97
Secure Hub 21.5.1	97
Secure Hub para iOS	97
Secure Hub para Android	97
Secure Hub 21.5.0	97
Problemas conhecidos no Secure Hub 21.5.0	97
Problema corrigido no Secure Hub 21.5.0	97
Secure Hub 21.4.0	97
Secure Hub 21.3.2	98
Secure Hub para iOS	98
Problemas conhecidos no Secure Hub 21.3.2	98
Problema corrigido no Secure Hub 21.3.2	98
Secure Hub 21.3.0	98
Problema conhecido no Secure Hub 21.3.0	98
Problemas corrigidos no Secure Hub 21.3.0	98
Secure Hub 21.2.0	98
Secure Hub para Android	98
Problemas conhecidos no Secure Hub 21.2.0	98
Problemas corrigidos no Secure Hub 21.2.0	99
Secure Hub 21.1.0	99
Problemas conhecidos no Secure Hub 21.1.0	99

Problemas corrigidos no Secure Hub 21.1.0	99
Secure Hub 20.12.0	99
Problemas conhecidos no Secure Hub 20.12.0	99
Problemas corrigidos no Secure Hub 20.12.0	99
Secure Hub 20.11.0	100
Secure Hub para Android	100
Problemas conhecidos no Secure Hub 20.11.0	100
Problemas corrigidos no Secure Hub 20.11.0	100
Secure Hub 20.10.5	100
Problemas conhecidos no Secure Hub 20.10.5	100
Problemas corrigidos no Secure Hub 20.10.5	100
Secure Hub 20.9.0	100
Problemas conhecidos no Secure Hub 20.9.0	100
Problemas corrigidos no Secure Hub 20.9.0	101
Secure Hub 20.7.5	101
Problemas conhecidos no Secure Hub 20.7.5	101
Problemas corrigidos no Secure Hub 20.7.5	101
Secure Hub 20.6.5	101
Secure Hub 20.3.0	101
Secure Hub para iOS	101
Secure Hub 20.2.0	101
Secure Hub para iOS	101
Problemas conhecidos no Secure Hub 20.2.0	102
Problemas corrigidos no Secure Hub 20.2.0	102
Secure Hub 20.1.5	102
Secure Hub 19.12.5	102
Problemas conhecidos no Secure Hub 19.12.5	102
Problemas corrigidos no Secure Hub 19.12.5	102

Secure Hub 19.11.5	102
Problemas conhecidos no Secure Hub 19.11.5	102
Problemas corrigidos no Secure Hub 19.11.5	102
Secure Hub 19.10.5	103
Secure Hub para Android	103
Problemas conhecidos no Secure Hub 19.10.5	103
Problemas corrigidos no Secure Hub 19.10.5	103
Secure Hub 19.10.0	103
Problemas conhecidos no Secure Hub 19.10.0	103
Problemas corrigidos no Secure Hub 19.10.0	103
Secure Hub 19.9.5	103
Secure Hub 19.9.0	103
Problemas conhecidos no Secure Hub 19.9.0	103
Problemas corrigidos no Secure Hub 19.9.0	104
Secure Hub 19.8.5	104
Secure Hub 19.8.0	104
Problemas conhecidos no Secure Hub 19.8.0	104
Problemas corrigidos no Secure Hub 19.8.0	104
Secure Hub 19.7.5	104
Problemas conhecidos no Secure Hub 19.7.5	104
Problemas corrigidos no Secure Hub 19.7.5	104
Secure Hub 19.6.5	105
Problemas conhecidos no Secure Hub 19.6.5	105
Problemas corrigidos no Secure Hub 19.6.5	105
Secure Hub 19.5.5	105
Problemas conhecidos no Secure Hub 19.5.5	105
Problemas corrigidos no Secure Hub 19.5.5	106
Secure Hub 19.5.0	106

Problemas conhecidos no Secure Hub 19.5.0	106
Problemas corrigidos no Secure Hub 19.5.0	106
Secure Hub 19.4.5	106
Problemas conhecidos no Secure Hub 19.4.5	106
Problemas corrigidos no Secure Hub 19.4.5	106
Secure Hub 19.3.5	107
Problemas conhecidos no Secure Hub 19.3.5	107
Problemas corrigidos no Secure Hub 19.3.5	107
Secure Hub 19.3.0	107
Problemas conhecidos no Secure Hub 19.3.0	107
Problemas corrigidos no Secure Hub 19.3.0	108
Secure Hub 19.2.0	108
Problemas conhecidos no Secure Hub 19.2.0	108
Problemas corrigidos no Secure Hub 19.2.0	108
Secure Hub 19.1.5	109
Problemas conhecidos no Secure Hub 19.1.5	109
Problemas corrigidos no Secure Hub 19.1.5	109
Secure Hub 19.1.0	109
Problemas conhecidos no Secure Hub 19.1.0	109
Problemas corrigidos no Secure Hub 18.12.0	109
Secure Hub 18.11.0	110
Problemas corrigidos no Secure Hub 18.11.0	110
Secure Hub 18.10.5	110
Problemas corrigidos no Secure Hub 18.10.5	110
Versões do Secure Hub de 10.8.25 a 18.10.6	110
Problemas corrigidos nas versões do Secure Hub de 10.8.25 a 18.10.6	110
Secure Hub 18.10.0	110
Problemas corrigidos no Secure Hub 18.10.0	110

Secure Hub 10.8.60	111
Problemas corrigidos no Secure Hub 10.8.60	111
Secure Hub 10.8.55	111
Problemas corrigidos no Secure Hub 10.8.55	111
Problemas corrigidos relacionados ao MDX na versão 10.8.55	111
Secure Hub 10.8.55	112
Problema conhecido no Secure Hub 10.8.55	112
Secure Hub 10.8.50	112
Problema conhecido no Secure Hub 10.8.50	112
Secure Hub 10.8.35	112
Problemas corrigidos no Secure Hub 10.8.35	112
Secure Hub 10.8.25	112
Problemas corrigidos no Secure Hub 10.8.25	112
Secure Hub 10.8.20	113
Problemas corrigidos no Secure Hub 10.8.20	113
Secure Hub 10.8.15	113
Problemas corrigidos no Secure Hub 10.8.15	113
Secure Hub 10.8.10	113
Problemas corrigidos no Secure Hub 10.8.10	113
Secure Hub para Android e iOS - Prévia	114
Gerenciamento de sinalizadores de recursos	115
Cenários de solicitação de autenticação	116
Tipos de credenciais	118
Sobre as inversões de tela do Secure Hub	120
Complexidade da senha para a senha do dispositivo (Android 12+)	121
Registrando dispositivos usando credenciais derivadas	123
Etapas de registro de dispositivo ao usar credenciais derivadas	123
Configurar dica através do console do Citrix Endpoint Management™	130

Configurar dica como texto	130
Configurar texto da dica com link de página da web	131
Verificação de conformidade em dispositivos Android (Prévia Técnica)	134

Citrix Secure Hub™

O Citrix Secure Hub é a plataforma de lançamento para a experiência do Citrix Endpoint Management™ (anteriormente, XenMobile). Os usuários registram seus dispositivos no Secure Hub para obter acesso à Loja. Na loja, eles podem adicionar aplicativos de produtividade móvel desenvolvidos pela Citrix e aplicativos de terceiros.

Para requisitos de sistema do Secure Hub e de outros aplicativos de produtividade móvel, consulte [Requisitos do sistema](#).

Administrando o Secure Hub

Você realiza a maioria das tarefas de administração relacionadas ao Secure Hub durante a configuração inicial do Endpoint Management. Para disponibilizar o Secure Hub aos usuários, para iOS e Android, carregue o Secure Hub na iOS App Store e na Google Play Store.

Além de fornecer um portal para aplicativos Citrix, o Secure Hub atualiza a maioria das políticas MDX armazenadas no Endpoint Management para os aplicativos instalados quando a sessão do Citrix Gateway de um usuário é renovada após a autenticação usando o Citrix Gateway.

Importante:

Alterações em qualquer uma das seguintes políticas exigem que um usuário exclua e reinstale o aplicativo para aplicar a política atualizada: Security Group, Enable encryption e Secure Mail Exchange Server.

PIN Citrix

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

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

Os usuários que fazem login no Secure Hub pela primeira vez devem inserir seu nome de usuário e senha do Active Directory. Durante o login, o Secure Hub salva as credenciais do Active Directory ou um certificado de cliente no dispositivo do usuário e, em seguida, solicita que o usuário insira um PIN. Quando os usuários fazem login novamente, eles inserem o PIN para acessar seus aplicativos Citrix e a Loja com segurança, até que o próximo período de tempo limite de inatividade termine para a sessão de usuário ativa. As propriedades de cliente relacionadas permitem criptografar segredos usando o PIN, especificar o tipo de senha para o PIN e especificar os requisitos de força e comprimento do PIN. Para obter detalhes, consulte [Propriedades do cliente](#).

Quando a autenticação por impressão digital está ativada, os usuários podem fazer login usando uma impressão digital quando a autenticação offline é necessária devido à inatividade do aplicativo. Os usuários ainda precisam inserir um PIN ao fazer login no Secure Hub pela primeira vez, ao reiniciar o dispositivo e após o término do temporizador de inatividade. Para obter informações sobre como ativar a autenticação por impressão digital, consulte [Autenticação por impressão digital ou Touch ID](#).

Fixação de certificado

O Secure Hub para iOS e Android suporta fixação de certificado SSL. Esse recurso garante que o certificado assinado pela sua empresa seja usado quando os clientes Citrix se comunicam com o Endpoint Management. A fixação de certificado impede conexões de clientes com o Endpoint Management quando a instalação de um certificado raiz no dispositivo compromete a sessão SSL. Quando o Secure Hub detecta quaisquer alterações na chave pública do servidor, o Secure Hub nega a conexão.

A partir do Android N, o sistema operacional não permite mais autoridades de certificação (CAs) adicionadas pelo usuário. A Citrix recomenda usar uma CA raiz pública em vez de uma CA adicionada pelo usuário.

Usuários que atualizam para o Android N podem ter problemas se usarem CAs privadas ou autoassinadas. As conexões em dispositivos Android N são interrompidas nos seguintes cenários:

- CAs privadas/autoassinadas e a opção CA Confiável Necessária para Endpoint Management no Serviço de Descoberta Automática estão definidas como **ATIVADAS**. Para obter detalhes, consulte [Serviço de Descoberta Automática do Endpoint Management](#).

- CAs privadas/autoassinadas e o Serviço de Descoberta Automática (ADS) não estão acessíveis. Devido a preocupações de segurança, quando o ADS não está acessível, a CA Confiável Necessária é ativada (**ON**), mesmo que tenha sido definida como **OFF** inicialmente.

Antes de registrar dispositivos ou atualizar o Secure Hub, considere habilitar o certificate pinning. A opção está **Desativada** por padrão e é gerenciada pelo Serviço de Descoberta Automática do Endpoint Management (ADS). Ao habilitar o certificate pinning, 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 falha se os usuários não aceitarem o certificado.

Para usar o certificate pinning, solicite que a Citrix faça o upload dos certificados para o servidor Citrix ADS. Abra um caso de suporte técnico usando o [portal de Suporte da Citrix](#). Em seguida, forneça as seguintes informações:

- O domínio que contém as contas com as quais os usuários se registrarão.
- 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 diferencia maiúsculas de minúsculas.
- Tipo de ID de Usuário, que pode ser UPN ou Email. Por padrão, o tipo é UPN.
- A porta usada para o registro de iOS, caso você tenha alterado o número da porta padrão 8443.
- A porta através da qual o Endpoint Management aceita conexões, caso você tenha alterado o número da porta padrão 443.
- A URL completa do seu Citrix Gateway.
- Opcionalmente, um endereço de e-mail para o seu administrador do Endpoint Management.
- Os certificados no formato PEM que você deseja adicionar ao domínio.

Configurando autenticação de certificado + senha de uso único para o Secure Hub

Você pode configurar o Citrix ADC para que o Secure Hub autentique usando um certificado mais um token de segurança que serve como uma senha de uso único. Essa configuração oferece uma opção de segurança forte que não deixa um rastro do Active Directory nos dispositivos.

Para permitir que o Secure Hub use esse tipo de autenticação, adicione uma ação de reescrita e uma política de reescrita no Citrix ADC que insere um cabeçalho de resposta personalizado no

formato **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar o tipo de logon do Citrix Gateway.

Normalmente, o Secure Hub usa o tipo de logon do Citrix Gateway configurado no console do Endpoint Management. No entanto, essa informação não está disponível para o Secure Hub até que ele conclua o logon pela primeira vez. Portanto, o cabeçalho personalizado é necessário para permitir que o Secure Hub faça isso.

Nota:

Se diferentes tipos de logon forem definidos no Endpoint Management e no Citrix ADC, a configuração do Citrix ADC substituirá a configuração. Para obter detalhes, consulte [Citrix Gateway e Endpoint Management](#).

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

A tela **Create Rewrite Action** é exibida.

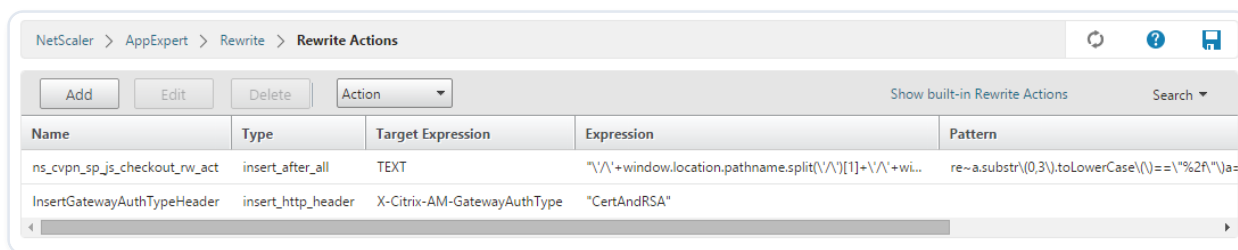
3. Preencha cada campo conforme mostrado na figura a seguir e clique em **Create**.

The screenshot shows the 'Create Rewrite Action' dialog box. It has the following fields and values:

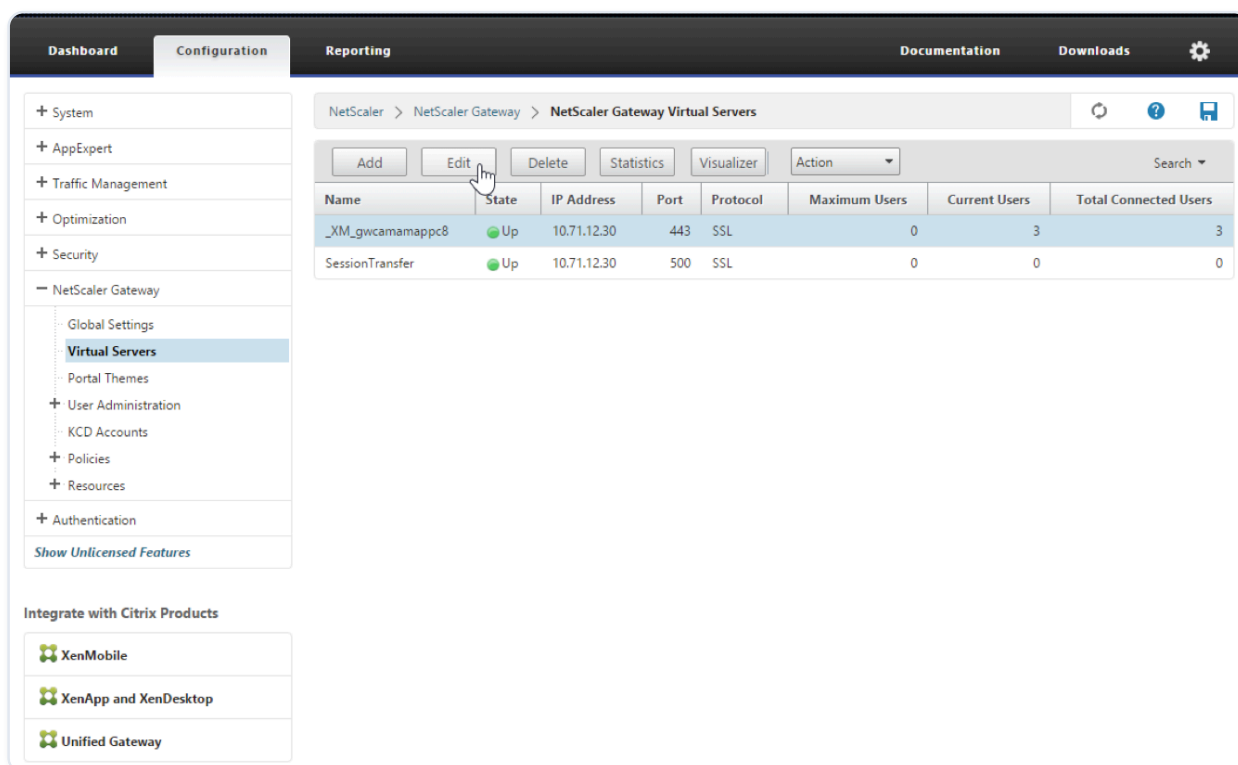
- Name***: InsertGatewayAuthTypeHeader
- Type***: INSERT_HTTP_HEADER
- Header Name***: X-Citrix-AM-GatewayAuthType
- Expression**: CertAndRSA

At the bottom, there are 'Create' and 'Close' buttons. A note at the bottom states: 'In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.'

O seguinte resultado aparece na tela principal **Rewrite Actions**.



4. Vincule a ação de reescrita ao servidor virtual como uma política de reescrita. Vá para **Configuration > NetScaler® Gateway > Virtual Servers** e selecione seu servidor virtual.



5. Clique em **Editar**.
6. Na tela de **configuração de Servidores Virtuais**, role para baixo até **Políticas**.
7. Clique em **+** para adicionar uma política.

8. No campo **Escolher Política**, escolha **Reescrever**.

9. No campo **Escolher Tipo**, escolha **Resposta**.

10. Clique em **Continuar**.

A seção **Associação de Política** se expande.

11. Clique em **Selecionar Política**.

Uma tela com as políticas disponíveis aparece.

12. Clique na linha da política que você acabou de criar e depois clique em **Selecionar**. A tela **Associação de Política** aparece novamente, com sua política selecionada preenchida.

Choose Type

Policies

Choose Policy: **Rewrite**

Choose Type: **Response**

Policy Binding

Select Policy*: InsertGatewayAuthTypePolicy

Binding Details

Priority*: 100

Goto Expression*: END

Bind **Close**

13. Clique em **Bind**.

Se o bind for bem-sucedido, a tela de configuração principal aparece com a política de reescrita concluída exibida.

Published Applications

- No Next HOP Server
- 1 STA Server
- No Url

Other Settings

ICMP Virtual Server Response: **Passive**

RHI State: **Passive**

Redirect to Home page: **true**

Policies

- Request Policies
- 3 Session Policies
- 2 ClientlessAccess Policies
- 4 Cache Policies
- Response Policies**
- 1 Rewrite Policy**

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

Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END

Requisito de porta para conectividade ADS para dispositivos Android

A configuração da 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 o ADS é importante ao baixar atualizações de segurança disponibilizadas por meio do ADS. As conexões ADS podem não ser compatíveis com seu servidor proxy. Nesse cenário, permita que a conexão 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 Endpoint Management. Observe que essa comunicação ocorre na porta de saída 443. É altamente provável que seu ambiente existente seja projetado para permitir esse acesso. Os clientes que não podem garantir essa comunicação são fortemente desencorajados a atualizar para o Secure Hub 10.2. Se tiver alguma dúvida, entre em contato com o suporte da Citrix.

Para habilitar o certificate pinning, você deve realizar os seguintes pré-requisitos:

- Colete os certificados do Endpoint Management e do Citrix ADC. Os certificados devem 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 habilitar o certificate pinning. Durante esse processo, seus certificados serão solicitados.

As novas melhorias de certificate pinning exigem que os dispositivos se conectem ao ADS antes que o dispositivo seja registrado. Isso garante que as informações de segurança mais recentes estejam disponíveis para o Secure Hub para o ambiente no qual o dispositivo está sendo registrado. Se os dispositivos não conseguirem acessar o ADS, o Secure Hub não permitirá o

registro do dispositivo. Portanto, abrir o acesso ao ADS dentro da rede interna é fundamental para permitir que os dispositivos sejam registrados.

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

FQDN	ENDEREÇO IP	PORTA	USO DE IP E PORTA
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - Comunicação ADS
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - Comunicação ADS
<code>ads.xm.cloud.com</code> : observe que a versão 10.6.15 e posterior do SecureHub usa <code>ads.xm.cloud.com</code> .	34.194.83.188	443	Secure Hub - Comunicação ADS
<code>ads.xm.cloud.com</code> : note que a versão 10.6.15 e posterior do SecureHub usa <code>ads.xm.cloud.com</code> .	34.193.202.23	443	Secure Hub - Comunicação ADS

Se a fixação de certificado estiver ativada:

- O Secure Hub fixa seu certificado corporativo durante o registro do dispositivo.
- Durante uma atualização, o Secure Hub descarta qualquer certificado atualmente fixado e então 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 se registrar novamente.

- A renovação do certificado não exige novo registro, desde que a chave pública do certificado não tenha sido alterada.

A fixação de certificado suporta certificados folha, não certificados intermediários ou de emissor. A fixação de certificado se aplica a servidores Citrix, como Endpoint Management e Citrix Gateway, e não a servidores de terceiros.

Recursos do Secure Hub

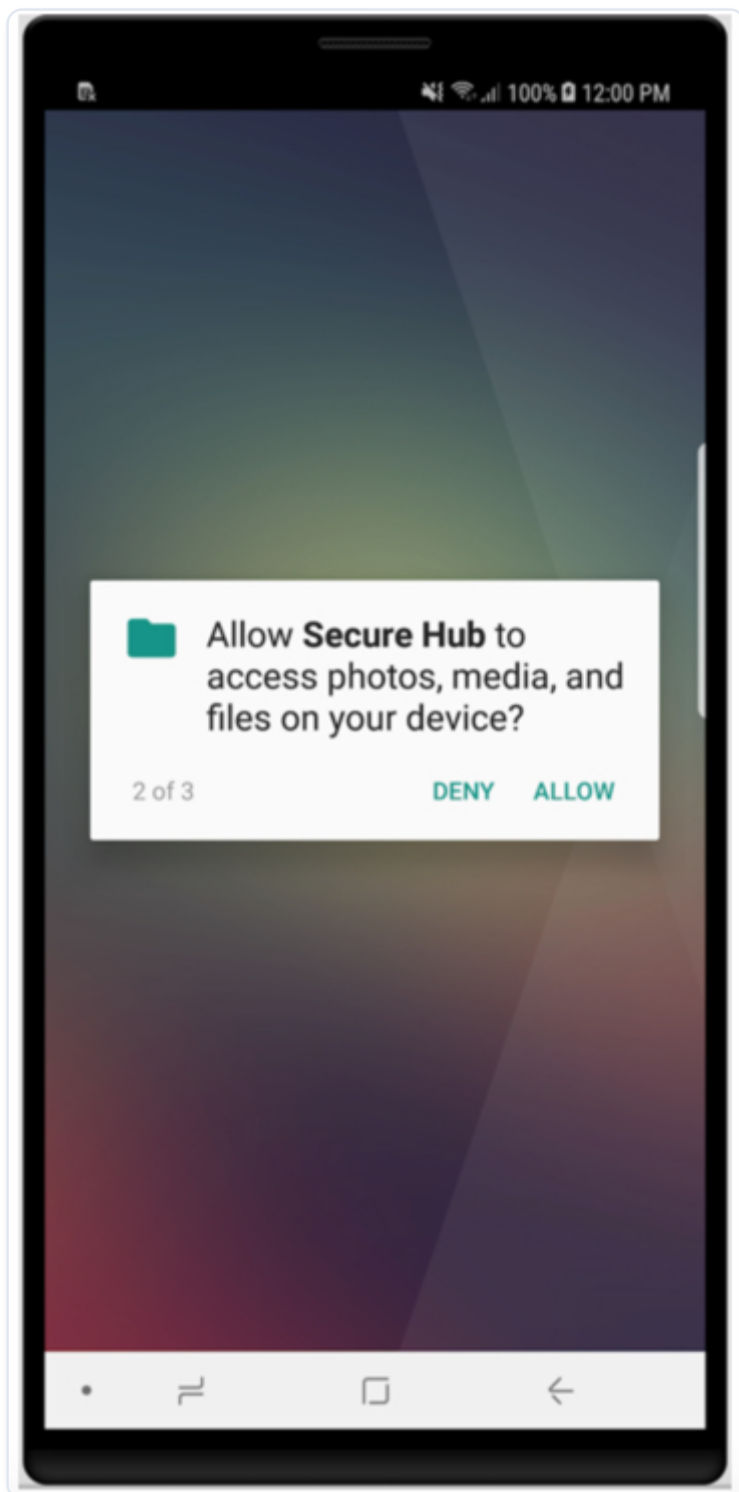
O Secure Hub permite que você monitore e imponha políticas móveis ao mesmo tempo em que fornece acesso à Loja e suporte ao vivo. Os usuários começam baixando o Secure Hub em seus dispositivos da loja de aplicativos da Apple, Android ou Windows.

Quando o Secure Hub é aberto, os usuários inserem as credenciais fornecidas por suas empresas para registrar seus dispositivos no Secure Hub. Para mais detalhes sobre o registro de dispositivos, consulte [Usuários, contas, funções e registro](#).

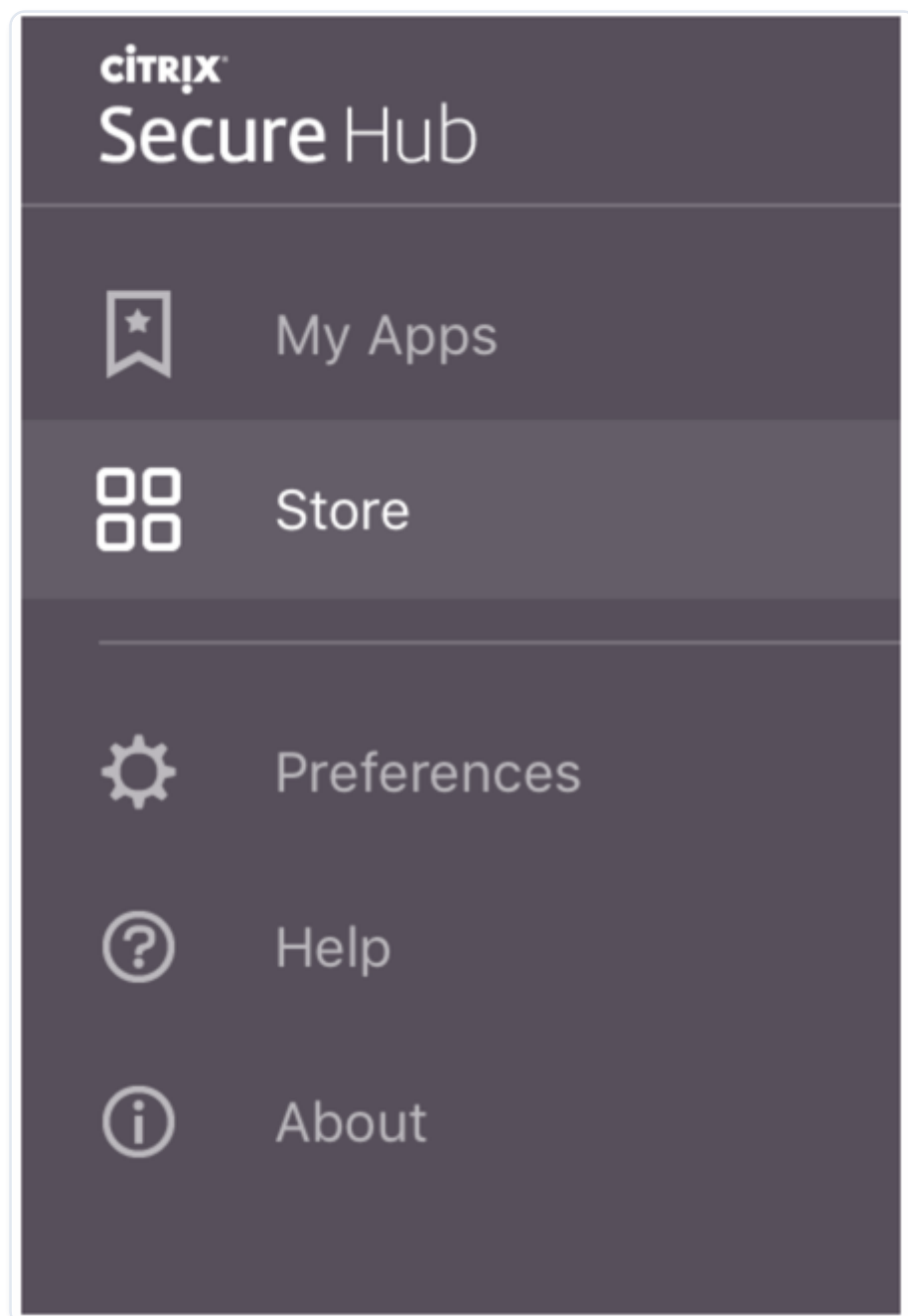
No Secure Hub para Android, durante a instalação inicial e o registro, a seguinte mensagem aparece: Permitir que o Secure Hub acesse fotos, mídias e arquivos em seu dispositivo?

Observe que esta mensagem vem do sistema operacional Android e não da Citrix. Ao tocar em **Permitir**, a Citrix e os administradores que gerenciam o Secure Hub não visualizam seus dados pessoais em nenhum momento. No entanto, se você conduzir uma sessão de suporte remoto com seu administrador, o administrador poderá visualizar seus arquivos pessoais dentro da sessão.

Uma vez inscritos, os usuários veem todos os aplicativos e desktops que você enviou na guia **Meus Aplicativos**. Os usuários podem adicionar mais aplicativos da Loja. Em telefones, o link da Loja está sob o ícone de hambúrguer de Configurações no canto superior esquerdo.



Em tablets, a Loja é uma guia separada.



Quando usuários de iPhones com iOS 9 ou posterior instalam aplicativos de produtividade móvel da loja de aplicativos do Endpoint Management, eles veem uma mensagem informando que o desenvolvedor corporativo, Citrix, não é confiável naquele iPhone e que o aplicativo não estará disponível para uso até que o desenvolvedor seja confiável. Quando esta mensagem aparece, o Secure Hub solicita aos usuários que visualizem um guia que os orienta no processo de confiar nos aplicativos corporativos da Citrix para seus iPhones.

Para implantações somente MAM, você pode configurar o Endpoint Management para que usuários com dispositivos Android ou iOS que se inscrevem no Secure Hub usando credenciais de e-mail sejam automaticamente inscritos no Secure Mail. Os usuários não precisam inserir mais informações ou seguir mais etapas para se inscrever no Secure Mail.

No primeiro uso do Secure Mail, o Secure Mail obtém o endereço de e-mail, domínio e ID de usuário do Secure Hub. O Secure Mail usa o endereço de e-mail para autodescoberta. O servidor Exchange é identificado usando o domínio e o ID de usuário, o que permite ao Secure Mail autenticar o usuário automaticamente. O usuário é solicitado a inserir uma senha se a política estiver configurada para não passar a senha, mas o usuário não é obrigado a inserir mais nenhuma informação.

Para habilitar este recurso, crie três propriedades:

- A propriedade de 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](#).

Se você quiser personalizar sua Loja, vá para **Configurações > Branding do Cliente** para alterar o nome, adicionar um logotipo e especificar como os aplicativos aparecem.

Client Branding
You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name

Default store view
☐ Category
☒ A-Z

Device
☒ Phone
☐ Tablet

Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
A .zip file should be created from the files, not a folder with the files inside of it.

Você pode editar descrições de aplicativos no console do Endpoint Management. Clique em **Configurar** e depois em **Aplicativos**. Selecione o aplicativo na tabela e clique em **Editar**. Selecione as plataformas para o aplicativo com a descrição que você está editando e digite o texto na caixa **Descrição**.

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under the 'Apps' section, the 'App Information' step is active. The configuration form includes:

- Name:** A text field containing 'Workmail'.
- Description:** An empty text field.
- App category:** A dropdown menu set to 'Workapps'.

On the left, a sidebar lists the configuration steps: 1 App Information (selected), 2 Platform, 3 Approvals (optional), and 4 Delivery Group Assignments (optional). The 'Platform' section shows checkboxes for 'iOS' and 'Android' (both checked), and 'Windows Phone' (unchecked).

Na Loja, os usuários podem navegar apenas pelos aplicativos e desktops que você configurou e protegeu no Endpoint Management. Para adicionar o aplicativo, os usuários tocam em **Detalhes** e depois em **Adicionar**.

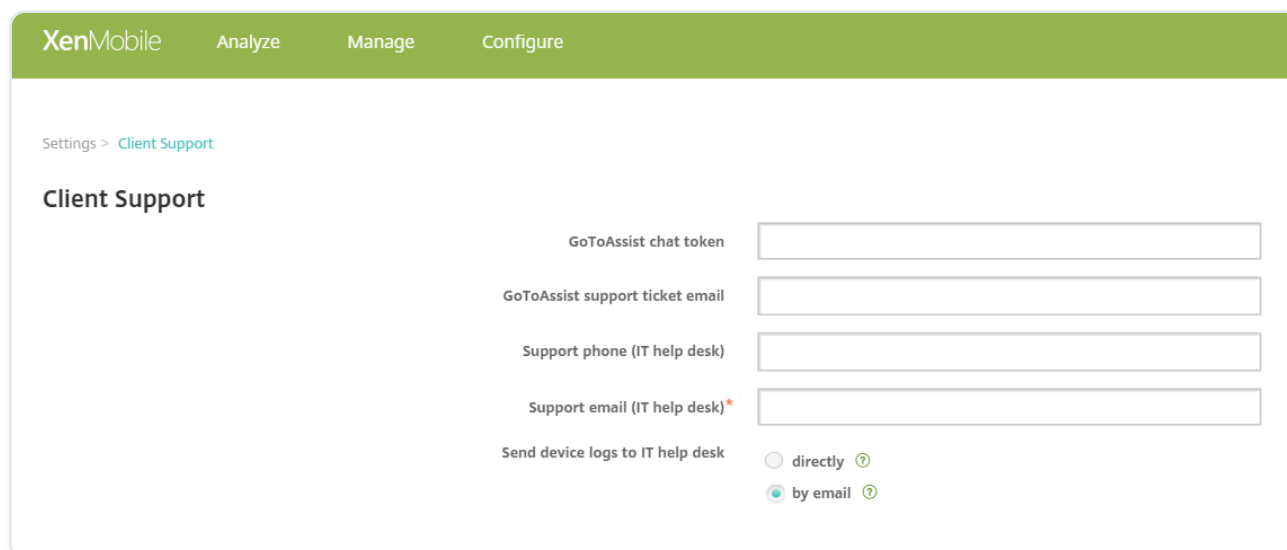
O Secure Hub também oferece aos usuários uma variedade de maneiras de obter ajuda. Em tablets, tocar no ponto de interrogação no canto superior direito abre as opções de ajuda. Em telefones, os usuários tocam no ícone do menu hambúrguer no canto superior esquerdo e depois tocam em **Ajuda**.

The screenshot shows a 'Help Desk' overlay with a 'Close' button in the top left. The overlay contains the following options:

- Your IT Department >
- Report Issue >
- Send Feedback to Citrix

At the bottom, there is a 'Citrix Support' link.

Seu Departamento de TI mostra o telefone e o e-mail do suporte técnico da sua empresa, que os usuários podem acessar diretamente do aplicativo. Você insere números de telefone e endereços de e-mail no console do Endpoint Management. Clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida. Clique em **Mais** e depois em **Suporte ao Cliente**. A tela onde você insere as informações é exibida.



Relatar Problema mostra uma lista de aplicativos. Os usuários selecionam o aplicativo que apresenta o problema. O Secure Hub gera logs automaticamente e, em seguida, abre uma mensagem no Secure Mail com os logs anexados como um arquivo zip. Os usuários adicionam linhas de assunto e descrições do problema. Eles também podem anexar uma captura de tela.

Enviar Feedback para a Citrix abre uma mensagem no Secure Mail com um endereço de suporte da Citrix preenchido. No corpo da mensagem, o usuário pode inserir sugestões para melhorar o Secure Mail. Se o Secure Mail não estiver instalado no dispositivo, o programa de e-mail nativo será aberto.

Os usuários também podem tocar em **Suporte Citrix**, que abre o [Citrix Knowledge Center](#). A partir daí, eles podem pesquisar artigos de suporte para todos os produtos Citrix.

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

O Secure Hub também fornece políticas de geolocalização e geomonitoramento se, por exemplo, você quiser garantir que um dispositivo corporativo não viole um determinado perímetro geográfico. Para obter detalhes, consulte [Política de dispositivo de localização](#). Além disso, o Secure Hub coleta e analisa automaticamente informações de falha para que você possa ver o que levou a uma falha específica. Essa função é suportada pelo software Crashlytics.

Citrix Secure Hub™

O Citrix Secure Hub é o ponto de partida para os aplicativos de produtividade móvel. Os usuários registram seus dispositivos no Secure Hub para obter acesso à loja de aplicativos. Na loja de aplicativos, eles podem adicionar aplicativos de produtividade móvel desenvolvidos pela Citrix e aplicativos de terceiros.

Você pode baixar o Secure Hub e outros componentes na [página de downloads do Citrix Endpoint Management](#).

Para o Secure Hub e outros requisitos de sistema para os aplicativos de produtividade móvel, consulte [Requisitos do sistema](#).

Para obter as informações mais recentes sobre aplicativos de produtividade móvel, consulte [Anúncios recentes](#).

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

NOTA:

O suporte para as versões Android 9.x e iOS 11.x do Secure Hub terminou em abril de 2025.

Novidades na versão atual

Secure Hub para iOS 26.8.1

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 26.8.0

Defina um aplicativo de inicialização automática na política de Configuração do Launcher no modo COSU

Em dispositivos Android Enterprise kiosk (COSU) que executam o Citrix Launcher, os administradores agora podem definir um aplicativo de inicialização automática na política de Configuração do Launcher para iniciar um aplicativo gerenciado automaticamente na inicialização do dispositivo. O Secure Hub encaminha a configuração para o Citrix Launcher, que executa a inicialização.

Deteção e renovação automáticas do certificado de dispositivo MDM

O Secure Hub para Android agora detecta automaticamente um certificado de dispositivo MDM inválido, ausente ou expirado e o renova em segundo plano. Isso restaura a conectividade do dispositivo sem que o usuário precise executar a solução de problemas manual do certificado ou registrar novamente o dispositivo.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Novidades em versões anteriores

Secure Hub para iOS 26.8.0

Suporte para iOS/iPadOS 27

A partir do lançamento do Secure Hub 26.8.0 para iOS, o aplicativo é compatível com iOS/iPadOS 27. Você pode atualizar seu dispositivo para iOS/iPadOS 27 e continuar usando a versão mais recente do Secure Hub.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 26.5.0

Suporte para Android 17

A partir do lançamento do Secure Hub 26.5.0 para Android, o aplicativo é compatível com Android 17. Você pode atualizar seu dispositivo para Android 17 e continuar usando a versão mais recente do Secure Hub.

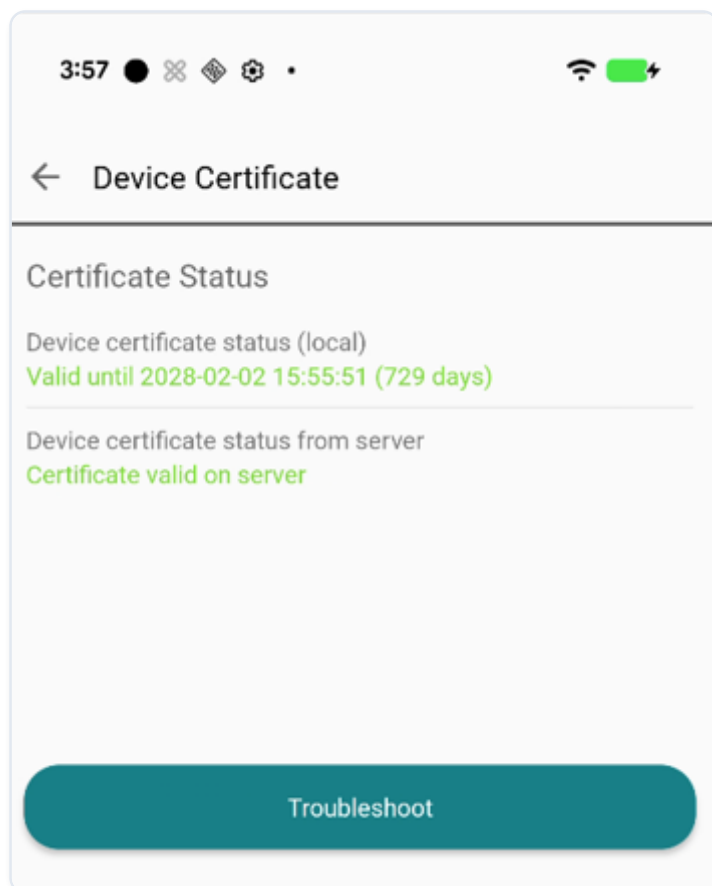
Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 26.2.0

Aprimoramento da solução de problemas do certificado do dispositivo

A partir do lançamento do Secure Hub 26.2.0 para Android, o Secure Hub inclui uma ferramenta de solução de problemas de certificado de dispositivo de autoatendimento que ajuda a diagnosticar e resolver problemas de conectividade do dispositivo causados por certificados de cliente revogados ou inválidos.

Quando um problema de certificado é detectado, a ferramenta tenta automaticamente renovar o certificado para restaurar a conectividade. Para acessar esta ferramenta, vá para **Ajuda > Solução de problemas > Certificado do dispositivo** e toque em **Solução de problemas**.



Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para iOS 25.8.0

Suporte para iOS 26

A partir do lançamento do Secure Hub 25.8.0 para iOS, o aplicativo oferece suporte a dispositivos que executam o iOS 26. A atualização para o Secure Hub versão 25.8.0 garante suporte e compatibilidade contínuos para os dispositivos que são atualizados para o iOS 26.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 25.10.0

Suporte para tamanho de página de memória de 16 KB

A partir do lançamento do Secure Hub 25.10.0 para Android, o aplicativo oferece suporte a um tamanho de página de memória de 16 KB para otimizar o desempenho e cumprir os requisitos do Google Play.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 25.7.0

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade geral.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para iOS 25.6.0

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 25.4.0

Suporte para Android 16

A partir do lançamento do Secure Hub 25.4.0 para Android, o aplicativo é compatível com o Android 16. Você pode atualizar seu dispositivo para o Android 16 e continuar usando a versão mais recente do Secure Hub.

Suporte para o protocolo TLS 1.3

A partir do lançamento do Secure Hub 25.4.0 para Android, o aplicativo oferece suporte ao protocolo TLS 1.3 em dispositivos Android. O TLS 1.3 é a versão mais recente do protocolo TLS e oferece desempenho mais rápido, segurança aprimorada e maior resiliência contra ataques cibernéticos em comparação com o TLS 1.2. O TLS 1.3 também reduz a latência da rede, resultando em conexões HTTPS mais rápidas e uma melhor experiência do usuário.

Para saber mais sobre o TLS 1.3, consulte [O Protocolo Transport Layer Security \(TLS\) Versão 1.3](#).

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 25.1.0

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para iOS 25.1.0

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para iOS 24.11.0

Esta versão aborda algumas questões que ajudam a melhorar o desempenho e a estabilidade gerais.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para Android 24.10.0

Suporte para Android 15

A atualização da versão do Secure Hub para 24.10.0 garante suporte contínuo para dispositivos que são atualizados para o Android 15.

Para obter mais informações sobre correções de bugs, consulte [Problemas conhecidos e corrigidos](#).

Secure Hub para iOS 24.9.0

Exibe Termos e Condições no Programa de Registro de Dispositivos

A partir do Secure Hub 24.9.0 para iOS, os administradores podem configurar a política de dispositivo de Termos e Condições através do Citrix Endpoint Management (CEM). Uma vez configurada, a página de **Termos e Condições** será exibida durante o processo de registro para dispositivos registrados via Programa de Registro de Dispositivos (DEP) da Apple. Isso garante que os usuários revisem e reconheçam os termos e condições antes de concluir seu registro, aprimorando a conformidade e as medidas de segurança durante a integração do dispositivo.

Secure Hub para Android 24.8.0

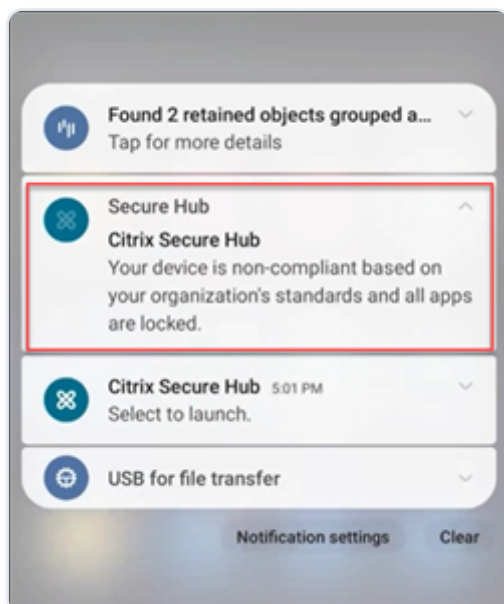
Verificação de conformidade em dispositivos Android (Technical Preview)

NOTA:

Este recurso é aplicável a dispositivos Android registrados no modo *Proprietário do Dispositivo*.

A partir desta versão, o Secure Hub verifica a conformidade dos dispositivos Android em relação às políticas configuradas pelo administrador através do Citrix Endpoint Management. Esta verificação de conformidade inclui garantir a força da senha do dispositivo, verificar a instalação de aplicativos obrigatórios e confirmar a remoção de aplicativos proibidos.

Se um dispositivo for considerado não compatível com as políticas definidas pelo administrador, o Secure Hub bloqueia todos os seus aplicativos e solicita que os usuários resolvam os problemas de conformidade para desbloqueá-los. A seguinte notificação aparece nos dispositivos dos usuários quando o dispositivo não está em conformidade.

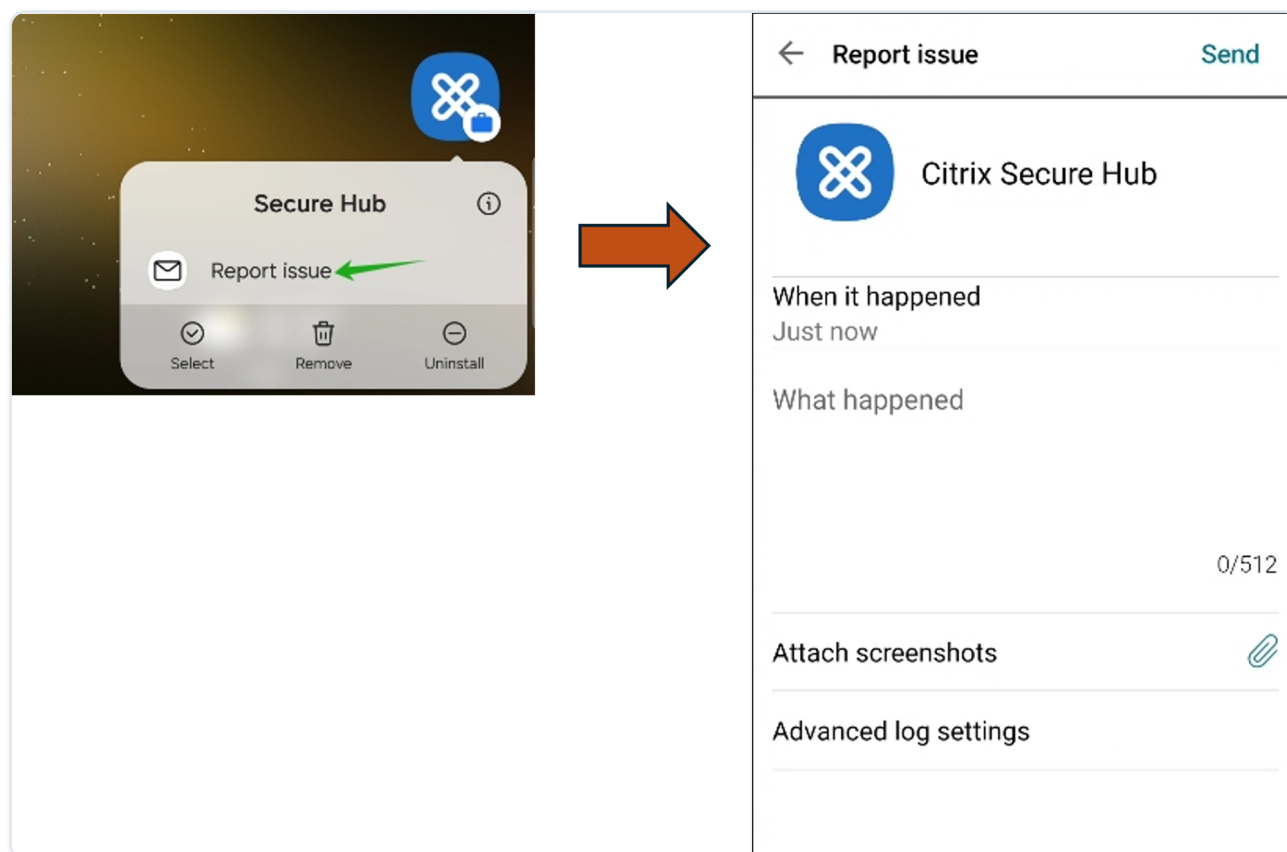


Para obter mais informações, consulte [Verificação de conformidade em dispositivos Android](#).

Secure Hub para Android 24.6.0

Coleta e relatório de logs aprimorados

O Secure Hub apresenta uma capacidade aprimorada de relatar problemas e enviar logs de forma contínua, sem abrir o Secure Hub. Com esta versão, os usuários podem acessar a opção **Relatar Problema** pressionando e segurando o ícone do aplicativo Secure Hub. Ao clicar na opção **Relatar Problema**, o Secure Hub abre diretamente a página **Relatar Problema**.



Secure Hub para iOS 24.5.0

Suporta Retorno ao Serviço do iOS 17

O Secure Hub oferece suporte ao recurso Retorno ao Serviço no iOS 17, que proporciona uma experiência de Gerenciamento de Dispositivos Móveis (MDM) mais eficiente e segura.

Anteriormente, era necessária uma configuração manual para configurá-lo para um novo usuário após apagar o dispositivo. Agora, o recurso Retorno ao Serviço automatiza esse processo, seja para reutilizar um dispositivo da empresa ou integrar um dispositivo pessoal (BYOD) com as políticas de segurança corretas.

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

Secure Hub para Android 24.3.0

Suporta Samsung Knox Enhanced Attestation v3

O Secure Hub agora oferece suporte ao Samsung Enhanced Attestation v3, aproveitando a atestação Knox para fortalecer as medidas de segurança para dispositivos Samsung gerenciados

por meio do Citrix Endpoint Management. Este protocolo de atestação avançado verifica a integridade e o status de segurança dos dispositivos, garantindo que eles não estejam roteados e estejam executando firmware autorizado. O recurso fornece uma camada essencial de proteção contra ameaças de segurança e garante a adesão às políticas de segurança corporativas.

Secure Hub para Android 23.12.0

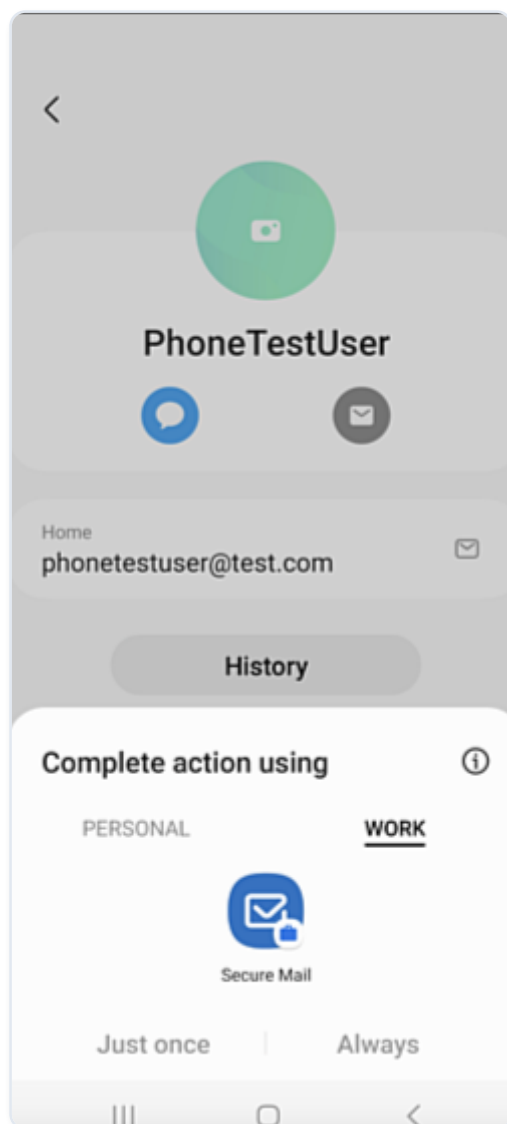
Segurança Aprimorada com Samsung Knox

A adição da política de dispositivo Chave da Plataforma Knox para Empresas no Citrix Endpoint Management aprimora significativamente os recursos de segurança do Secure Hub em dispositivos Samsung. Essa política permite que você forneça as informações de licença necessárias da Plataforma Knox para Empresas (KPE) da Samsung e use as licenças KPE para aprimorar a segurança do seu dispositivo Samsung. O Samsung Knox garante que os dados corporativos permaneçam protegidos, ao mesmo tempo em que mantém a facilidade de gerenciamento e uma experiência de usuário tranquila.

Para obter mais informações, consulte [Política de dispositivo Chave da Plataforma Knox para Empresas](#).

Acessar o Secure Mail do perfil pessoal do usuário

Os usuários agora podem acessar e usar o Secure Mail em seu perfil de trabalho a partir de seu perfil pessoal. Quando os usuários clicam em um endereço de e-mail em sua lista de endereços do perfil pessoal, eles recebem uma opção para usar o Secure Mail em seu perfil de trabalho. Esse recurso oferece conveniência, permitindo que os usuários enviem um e-mail de seu perfil pessoal. Esse recurso é aplicável em dispositivos BYOD ou WPCOD.



Secure Hub para iOS 24.1.0

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Secure Hub para Android 23.12.0

Adicionar uma dica sobre o PIN de autenticação na página de login

A partir da versão 23.12.0, você pode adicionar uma dica sobre o PIN de autenticação na página de login. Esse recurso é opcional e se aplica a dispositivos registrados para autenticação de dois fatores. A dica informa como acessar o PIN.

Você pode configurar uma dica como texto ou link. O texto da dica oferece informações concisas sobre o PIN, enquanto o link fornece informações detalhadas sobre como acessar o PIN. Para obter mais informações sobre como configurar uma dica, consulte [Configurar dica por meio do console do Citrix Endpoint Management](#).

A autenticação nFactor oferece suporte ao recurso de logon único

A partir do Secure Hub para Android versão 23.12.0, o nFactor para registro ou login do Mobile Application Management (MAM) oferece suporte ao recurso de logon único (SSO). Esse recurso permite que as credenciais de login inseridas anteriormente passem pelo processo de registro ou login do MAM, eliminando a necessidade de os usuários as inserirem manualmente novamente. Para obter mais informações sobre a propriedade nFactor SSO, consulte a [Referência de propriedade do cliente](#) na documentação do Citrix Endpoint Management.

Suporte a limpeza completa no modo de inicialização direta

Anteriormente, era necessário desbloquear o dispositivo para executar um comando de limpeza completa em um dispositivo reiniciado. Agora, você pode executar um comando de limpeza completa no modo de inicialização direta, mesmo que o dispositivo esteja bloqueado. Esse recurso é útil do ponto de vista da segurança, especialmente quando o dispositivo está na posse de um indivíduo não autorizado. Para obter mais informações sobre o comando de limpeza completa, consulte as [Ações de segurança](#) na documentação do Citrix Endpoint Management.

Velocidade de carregamento otimizada da App Store do Secure Hub

A App Store no Secure Hub agora carrega mais rápido do que antes, permitindo que os usuários a acessem mais rapidamente.

Secure Hub para iOS 23.11.0

Adicionar uma dica sobre o PIN de autenticação na página de login

A partir da versão 23.11.0, você pode adicionar uma dica sobre o PIN de autenticação na página de login. Esse recurso é opcional e se aplica a dispositivos registrados para autenticação de dois fatores. A dica informa como acessar o PIN.

Você pode configurar uma dica como texto ou um link. O texto da dica oferece informações concisas sobre o PIN, enquanto o link fornece informações detalhadas sobre como acessar o PIN. Para obter mais informações sobre como configurar uma dica, consulte o artigo [Configurar dica através do console do Citrix Endpoint Management](#).

A autenticação nFactor oferece suporte ao recurso de logon único

A partir do Secure Hub para iOS versão 23.11.0, o nFactor para registro ou login do Mobile Application Management (MAM) oferece suporte ao recurso de logon único (SSO). Esse recurso permite que as credenciais de login inseridas anteriormente passem pelo processo de registro ou login do MAM, eliminando a necessidade de os usuários as inserirem manualmente novamente.

Para obter mais informações sobre a propriedade nFactor SSO, consulte a [Referência de propriedades do cliente](#) na documentação do Citrix Endpoint Management.

Secure Hub 23.10.0

Secure Hub para Android

O Secure Hub para Android 23.10.0 oferece suporte ao Android 14. A atualização da versão do Secure Hub para 23.10.0 garante suporte contínuo para dispositivos que são atualizados para o Android 14.

Secure Hub 23.9.0

Secure Hub para Android

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Secure Hub 23.8.1

Secure Hub para iOS

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Secure Hub 23.8.0

Secure Hub para iOS

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Secure Hub 23.7.0

Secure Hub para Android

Play Integrity API

A API SafetyNet Attestation será descontinuada em breve pelo Google, conforme o cronograma de descontinuação, e migrada para a API Play Integrity sugerida.

Para obter mais informações, consulte [API Play Integrity](#) no documento do Citrix Endpoint Management.

Para obter detalhes sobre a descontinuação, consulte [Descontinuações e remoções](#) no documento do Citrix Endpoint Management.

Para ler sobre o recurso SafetyNet do Android, consulte [SafetyNet](#)

Secure Hub 23.4.0

Secure Hub para iOS

Experiência do usuário aprimorada

A partir da versão 23.4.0, o Secure Hub para iOS aprimora as seguintes experiências do usuário:

- Experiência da Loja:
 - ◆ Anteriormente, a página Meus Aplicativos aparecia primeiro. Com a versão 23.4.0, a página da Loja aparece primeiro.
 - ◆ Anteriormente, a loja do Secure Hub realizava a ação de recarregar toda vez que o usuário clicava na opção Loja.
- Com a versão 23.4.0, a experiência do usuário é aprimorada. Agora, o aplicativo recarrega quando o usuário o inicia pela primeira vez, o reinicia ou desliza a tela para baixo.
- Interface do usuário: Anteriormente, a opção Sair estava localizada no canto inferior esquerdo da tela. Com a versão 23.4.0, a opção Sair faz parte do menu principal e está acima da opção Sobre.
- Hiperlinks: Anteriormente, os hiperlinks na página de detalhes do aplicativo apareciam como texto simples. Com a versão 23.4.0, os hiperlinks são clicáveis e possuem formatação de sublinhado para indicar links.

Experiência de transição de MDX para MAM SDK

A partir da versão 23.4.0, a experiência de transição do MDX legado para o MAM SDK é aprimorada para aplicativos iOS de modo duplo. Esse recurso melhora a experiência do usuário ao usar aplicativos de produtividade móvel, reduzindo as mensagens de alerta e alternando para o Secure Hub.

Use o PIN do Citrix para desbloquear aplicativos

Anteriormente, o usuário final inseria a senha do dispositivo para desbloquear aplicativos baseados em Mobile App Management (MAM).

A partir da versão 23.4.0, o usuário final pode inserir o PIN do Citrix como senha para desbloquear aplicativos baseados em MAM. Os administradores podem configurar a complexidade da senha usando as propriedades do cliente no servidor CEM.

Sempre que o aplicativo estiver inativo por mais tempo do que o permitido, os usuários finais podem inserir o PIN do Citrix para desbloquear o aplicativo, dependendo da configuração definida pelos administradores.

Para o Secure Hub para Android, existe uma propriedade de cliente separada para configurar como manipular com o temporizador de inatividade em aplicativos MAM. Para obter mais informações, consulte [Temporizador de Inatividade Separado para Android](#).

Secure Hub 23.4.1

Secure Hub para Android

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Secure Hub 23.4.0

Secure Hub para Android

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Secure Hub 23.2.0

Secure Hub para Android

NOTA:

- Nenhum dado analítico é coletado para os usuários na União Europeia (UE), Espaço Econômico Europeu (EEE), Suíça e Reino Unido (RU).

VPN MDX em modo de túnel completo

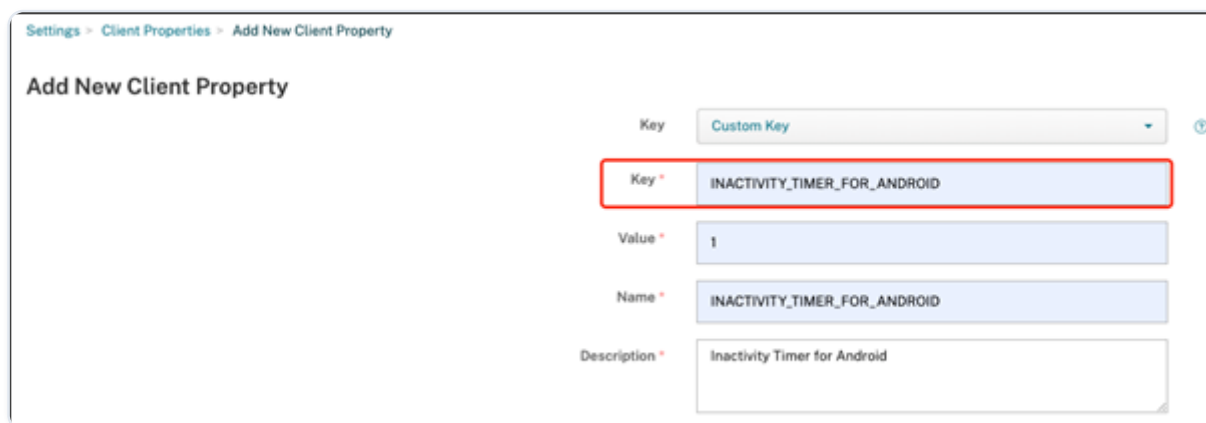
A Micro VPN MDX (modo de túnel completo) foi descontinuada.

Para obter mais informações, consulte [Descontinuação](#) na documentação do Citrix Endpoint Management.

Temporizador de Inatividade Separado para Android

Anteriormente, a propriedade de cliente **Inactivity Timer** era comum para o Secure Hub para Android e iOS.

A partir da versão 23.2.0, um administrador de TI pode usar a nova propriedade de cliente **Inactivity_Timer_For_Android** para separar o temporizador de inatividade do iOS. Um administrador de TI pode definir o **Value** de **Inactivity_Timer_For_Android** como 0 para desativar o temporizador de inatividade do Android de forma independente. Dessa forma, todos os aplicativos no perfil de trabalho, incluindo o Secure Hub, solicitam apenas o PIN de trabalho.



The screenshot shows the 'Add New Client Property' form in the XenMobile console. The form has the following fields:

- Key:** A dropdown menu with 'Custom Key' selected. The field is highlighted with a red box.
- Value:** A text input field containing the number '1'.
- Name:** A text input field containing the text 'INACTIVITY_TIMER_FOR_ANDROID'.
- Description:** A text input field containing the text 'Inactivity Timer for Android'.

Para obter mais informações sobre como adicionar e modificar uma propriedade de cliente, consulte [Propriedades do cliente](#) na documentação do XenMobile.

Secure Hub 22.11.0

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 22.9.0

Secure Hub para Android

Esta versão inclui:

- Complexidade de senha para a senha do dispositivo (Android 12+)
- Suporte para SDK 31
- Correções de bugs

Complexidade de senha para a senha do dispositivo (Android 12+)

A complexidade da senha é preferível a um requisito de senha personalizado. O nível de complexidade da senha é um dos níveis predefinidos. Assim, o usuário final não consegue definir uma senha com um nível de complexidade inferior.

A complexidade do código de acesso para dispositivos no Android 12+ é a seguinte:

- **Aplicar complexidade do código de acesso:** Requer uma senha com um nível de complexidade definido pela plataforma, em vez de um requisito de senha personalizado. Apenas para dispositivos no Android 12+ e usando o Secure Hub 22.9 ou posterior.
- **Nível de complexidade:** Níveis predefinidos de complexidade de senha.
 - **Nenhum:** Nenhuma senha é necessária.
 - **Baixo:** As senhas podem ser:
 - Um padrão
 - Um PIN com um mínimo de quatro números
 - **Médio:** As senhas podem ser:
 - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234), e um mínimo de quatro números
 - Alfabético com um mínimo de quatro caracteres
 - Alfanumérico com um mínimo de quatro caracteres
 - **Alto:** As senhas podem ser:
 - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234), e um mínimo de oito números
 - Alfabético com um mínimo de seis caracteres
 - Alfanumérico com um mínimo de seis caracteres

OBSERVAÇÕES:

- Para dispositivos BYOD, as configurações de senha, como Comprimento mínimo, Caracteres obrigatórios, Reconhecimento biométrico e Regras avançadas, não são aplicáveis no Android 12+. Em vez disso, use a complexidade da senha.
- Se a complexidade da senha para o perfil de trabalho estiver ativada, então a complexidade da senha para o lado do dispositivo também deve ser ativada.

Para obter mais informações, consulte [Configurações do Android Enterprise](#) na documentação do Citrix Endpoint Management.

Secure Hub 22.7.0

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 22.6.0

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 22.5.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub 22.4.0

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 22.2.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 21.11.0

Secure Hub para Android

Suporte para perfil de trabalho para dispositivos de propriedade da empresa

Em dispositivos Android Enterprise, agora você pode registrar o Secure Hub no modo de perfil de trabalho para dispositivos de propriedade da empresa. Este recurso está disponível em dispositivos que executam Android 11 ou posterior. Dispositivos anteriormente registrados no modo COPE (Corporate Owned Personally Enabled) migram automaticamente para o modo de perfil de trabalho para dispositivos de propriedade da empresa, quando o dispositivo é atualizado do Android 10 para o Android 11 ou posterior.

Secure Hub 21.10.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Suporte para Android 12. A partir desta versão, o Secure Hub é compatível com dispositivos que executam Android 12.

Secure Hub 21.8.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub 21.7.1

Secure Hub para Android

Suporte para Android 12 em dispositivos já registrados. Se você estiver considerando atualizar para o Android 12, certifique-se de atualizar o Secure Hub para a versão 21.7.1 primeiro. O Secure Hub 21.7.1 é a versão mínima necessária para atualizar para o Android 12. Esta versão garante uma atualização perfeita do Android 11 para o Android 12 para usuários já registrados.

NOTA:

Se o Secure Hub não for atualizado para a versão 21.7.1 antes de você atualizar para o Android 12, seu dispositivo pode exigir um novo registro ou uma redefinição de fábrica para recuperar a funcionalidade anterior.

A Citrix está comprometida em fornecer suporte no Dia 1 para o Android 12 e adicionará mais atualizações às versões subsequentes do Secure Hub para dar suporte total ao Android 12.

Secure Hub 21.7.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 21.6.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 21.5.1

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 21.5.0

Secure Hub para iOS

Com esta versão, os aplicativos empacotados com o MDX Toolkit versão 19.8.0 ou anterior não funcionarão mais. Certifique-se de empacotar seus aplicativos com o MDX Toolkit mais recente para retomar a funcionalidade adequada.

Secure Hub 21.4.0

Renovação de cores para o Secure Hub. O Secure Hub está em conformidade com as atualizações de cores da marca Citrix.

Secure Hub 21.3.2

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub 21.3.0

Esta versão inclui correções de bugs.

Secure Hub 21.2.0

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 21.1.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 20.12.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub para Android

O Secure Hub para Android oferece suporte ao modo Direct Boot. Para obter mais informações sobre o modo Direct Boot, consulte a documentação do Android em *Developer.android.com*.

Secure Hub 20.11.0

Secure Hub para Android

O Secure Hub oferece suporte aos requisitos atuais da API de destino do Google Play para Android 10.

Secure Hub 20.10.5

Esta versão inclui correções de bugs.

Secure Hub 20.9.0

Secure Hub para iOS

O Secure Hub para iOS oferece suporte ao iOS 14.

Secure Hub para Android

Esta versão inclui correções de bugs.

Secure Hub 20.7.5

Secure Hub para Android

- O Secure Hub para Android oferece suporte ao Android 11.
- **Transição do Secure Hub de 32 bits para 64 bits para aplicativos.** Na versão 20.7.5 do Secure Hub, o suporte para arquitetura de 32 bits para aplicativos termina, e o Secure Hub foi atualizado para 64 bits. A Citrix recomenda que os clientes atualizem para a versão 20.7.5 a partir da 20.6.5. Se os usuários pularem a atualização para a versão 20.6.5 do Secure Hub e, em vez disso, atualizarem diretamente da 20.1.5 para a 20.7.5, eles deverão se reautenticar. A reautenticação envolve a inserção de credenciais e a redefinição do PIN do Secure Hub. A versão 20.6.5 do Secure Hub está disponível na Google Play Store.
- **Instalar atualizações da App Store.** No Secure Hub para Android, se houver atualizações disponíveis para aplicativos, o aplicativo é destacado e o recurso **Atualizações disponíveis** aparece na tela da App Store.

Ao tocar em **Atualizações disponíveis**, você navegar para a loja que mostra a lista de aplicativos com atualizações pendentes. Toque em **Detalhes** ao lado do aplicativo para instalar as atualizações. Quando o aplicativo é atualizado, a seta para baixo em **Detalhes** muda 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 oferece suporte à 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 a versão 20.6.5 do Secure Hub, para que possam atualizar para versões posteriores sem reautenticação. Se os usuários pularem a atualização para a versão 20.6.5 do Secure Hub e, em vez disso, atualizarem diretamente para a 20.7.5, eles precisarão se reautenticar. A reautenticação envolve a inserção de credenciais e a redefinição do 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

Habilitar um proxy configurado em dispositivos iOS. O Secure Hub para iOS exige que você habilite uma nova propriedade de cliente, `ALLOW_CLIENTSIDE_PROXY`, se quiser permitir que os usuários usem servidores proxy que eles configuram em **Ajustes > Wi-Fi**. Para obter mais informações, consulte `ALLOW_CLIENTSIDE_PROXY` em [Referência de propriedades do 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 Citrix Workspace app terminará em junho de 2020.

Secure Hub para iOS

- **Extensão de Rede desabilitada.** Devido a mudanças recentes nas Diretrizes de Revisão da App Store, a partir da versão 20.3.0, o Secure Hub não oferece suporte à Extensão de Rede (NE) em dispositivos iOS. A NE não tem impacto nos aplicativos de produtividade móvel desenvolvidos pela Citrix. No entanto, a remoção da NE tem algum impacto nos aplicativos MDX empacotados implantados na empresa. Os usuários finais podem experimentar alternâncias extras para o Secure Hub ao sincronizar componentes como tokens de autorização, temporizadores e tentativas de PIN.

NOTA:

Novos usuários não são solicitados a instalar a VPN.

- **Suporte para perfis de registro aprimorados.** O Secure Hub oferece suporte aos recursos de perfil de registro aprimorados anunciados para o Citrix Endpoint Management em [Suporte a perfil de registro](#).

Secure Hub 20.2.0

Secure Hub para iOS

Esta versão inclui correções de bugs.

Secure Hub 20.1.5

Esta versão inclui:

- Atualização na 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

Registre o Secure Hub no modo COPE. Em dispositivos Android Enterprise, registre o Secure Hub no modo COPE (Corporate Owned Personally Enabled) 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 de keyguard para perfil de trabalho do Android Enterprise e dispositivos totalmente gerenciados. O keyguard do Android gerencia as telas de bloqueio do dispositivo e do desafio de trabalho. 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 desabilitar todos os recursos de keyguard.

Para obter mais informações sobre as configurações de recursos 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 oferece suporte ao 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 da administração de dispositivos para o Android Enterprise](#) para obter informações sobre como a descontinuação das APIs de Administração de Dispositivos do Google 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 oferece suporte ao Samsung Knox SDK 3.x. Para obter mais informações sobre a migração para o Samsung Knox 3.x, consulte a documentação do desenvolvedor do Samsung Knox. Esta versão também inclui suporte para os novos namespaces do Samsung Knox. Para obter mais informações sobre as alterações nos antigos namespaces do Samsung Knox, consulte [Alterações nos antigos namespaces do Samsung Knox](#).

NOTA:

O Secure Hub para Android não oferece suporte ao Samsung Knox 3.x em dispositivos que executam o 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 oferece suporte ao 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 oferece suporte ao Android Enterprise. Para obter mais informações sobre esta política, consulte [Política de dispositivo Wi-Fi](#).
- **Política de dispositivo XML personalizada.** A política de dispositivo XML personalizada agora oferece suporte ao Android Enterprise. Para obter mais informações sobre esta política, consulte [Política de dispositivo XML personalizada](#).
- **Política de dispositivo de arquivos.** 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 arquivos](#).

Secure Hub 19.1.0

O Secure Hub reformulou fontes, cores e outras melhorias na interface do usuário. Essa reformulação oferece uma experiência de usuário aprimorada, alinhando-se de perto com a estética da marca Citrix em todo o nosso conjunto completo de aplicativos de produtividade móvel.

Secure Hub 18.12.0

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub 18.11.5

- **Configurações da política de dispositivo de restrições para Android Enterprise.** Novas configurações para a política de dispositivo de Restrições permitem que os usuários acessem estes recursos em dispositivos Android Enterprise: barra de status, bloqueio de tela, gerenciamento de contas, compartilhamento de localização e manter a tela do dispositivo ligada para dispositivos Android Enterprise. Para obter informações, consulte [Política de dispositivo de restrições](#).

O Secure Hub 18.10.5 a 18.11.0 inclui melhorias 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 de dispositivo do Samsung DeX e como configurar o Samsung DeX, consulte [Como o Samsung DeX funciona](#).

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

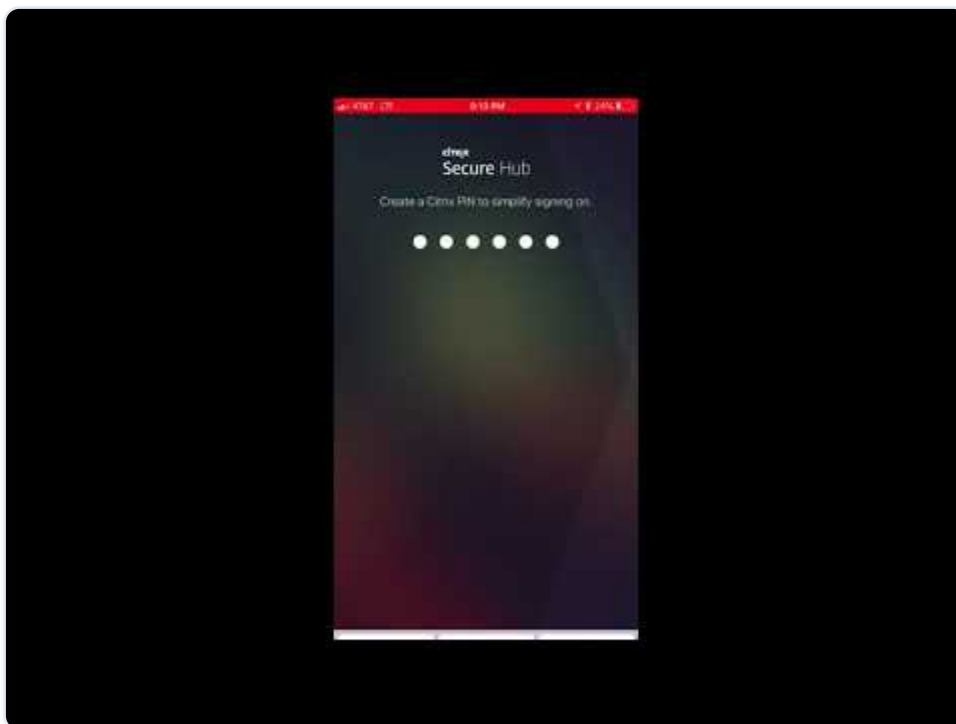
- **Suporte para Android SafetyNet:** Você pode configurar o Endpoint Management para usar o recurso **Android SafetyNet** para avaliar a compatibilidade e a segurança de dispositivos Android que têm o Secure Hub instalado. Os resultados podem ser usados para acionar ações automatizadas nos dispositivos. Para obter informações, consulte [Android SafetyNet](#).
- **Impedir o uso da câmera para dispositivos Android Enterprise:** A nova configuração **Permitir uso da câmera** para a política de dispositivo de 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

Esses lançamentos 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 veem mais a loja do Secure Hub. Um botão **Adicionar aplicativos** leva os usuários à loja de aplicativos do Workspace. O vídeo a seguir mostra um dispositivo iOS realizando um registro 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 este recurso, configure o seguinte:

- Habilite as políticas de Cache de Senha e Autenticação de Senha. Para obter mais informações sobre como configurar políticas, consulte [Políticas MDX para aplicativos de produtividade móvel em um relance](#).
- Configure a autenticação do Active Directory como AD ou AD+Cert. Oferecemos suporte a esses dois modos. Para obter mais informações sobre como configurar a autenticação, consulte [Autenticação de domínio ou domínio mais token de segurança](#).
- Habilite a integração do Workspace para o Endpoint Management. Para obter mais informações sobre a integração do workspace, consulte [Configurar workspaces](#).

IMPORTANTE:

Depois que este recurso é habilitado, o SSO do Citrix Files ocorre através do Workspace e não através do Endpoint Management (anteriormente, XenMobile®). Recomendamos que você desabilite a integração do Citrix Files no console do Endpoint Management antes de habilitar a integração do Workspace.

Secure Hub 10.8.55

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

Secure Hub 10.8.25: O 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 esteja em conformidade com certificados de segurança que tenham um nome de host correspondente na extensão subjectAltName (SAN). Para verificar um nome de host, o servidor deve apresentar um certificado com um SAN correspondente. Certificados que não contêm um SAN correspondente ao nome do host não são mais confiáveis. Para obter detalhes, consulte a documentação do Desenvolvedor Android.

Atualização do Secure Hub para iOS em March 19, 2018: A versão 10.8.6 do Secure Hub para iOS está disponível para corrigir um problema com a política de aplicativo VPP.

Secure Hub 10.8.5: Suporte no Secure Hub para Android para o modo COSU para Android Work (Android for Work). Para obter detalhes, consulte a [documentação do Citrix Endpoint Management](#).

Administrando o Secure Hub

A maioria das tarefas de administração relacionadas ao Secure Hub é realizada durante a configuração inicial do Endpoint Management. Para disponibilizar o Secure Hub aos usuários, para iOS e Android, carregue o Secure Hub na iOS App Store e na Google Play Store.

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

IMPORTANTE:

Alterações em qualquer uma dessas políticas exigem que o usuário exclua e reinstale o aplicativo para aplicar a política atualizada: Grupo de Segurança, Habilitar criptografia e Servidor Exchange do Secure Mail.

PIN do Citrix

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

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

Os usuários que fazem login no Secure Hub pela primeira vez devem inserir seu nome de usuário e senha do Active Directory. Durante o login, o Secure Hub salva as credenciais do Active Directory ou um certificado de cliente no dispositivo do usuário e, em seguida, solicita que o usuário insira um PIN. Quando os usuários fazem login novamente, eles inserem o PIN para acessar seus aplicativos Citrix e a Store com segurança, até que o próximo período de tempo limite de inatividade termine para a sessão de usuário ativa. As propriedades de cliente relacionadas permitem criptografar segredos usando o PIN, especificar o tipo de senha para o PIN e especificar os requisitos de força e comprimento do PIN. Para obter detalhes, consulte [Propriedades do cliente](#).

Quando a autenticação por impressão digital (Touch ID) está habilitada, os usuários podem fazer login usando uma impressão digital quando a autenticação offline é necessária devido à inatividade do aplicativo. Os usuários ainda precisam inserir um PIN ao fazer login no Secure Hub pela primeira vez, reiniciar o dispositivo e após o término do temporizador de inatividade. Para obter informações sobre como habilitar a autenticação por impressão digital, consulte [Autenticação por impressão digital ou Touch ID](#).

Fixação de certificado

O Secure Hub para iOS e Android oferece suporte à fixação de certificado SSL. Esse recurso garante que o certificado assinado por sua empresa seja usado quando os clientes Citrix se

comunicam com o Endpoint Management, evitando assim conexões de clientes com o Endpoint Management quando a instalação de um certificado raiz no dispositivo compromete a sessão SSL. Quando o Secure Hub detecta quaisquer alterações na chave pública do servidor, o Secure Hub nega a conexão.

A partir do Android N, o sistema operacional não permite mais autoridades de certificação (CAs) adicionadas pelo usuário. A Citrix recomenda o uso de uma CA raiz pública em vez de uma CA adicionada pelo usuário.

Os usuários que atualizam para o Android N podem ter problemas se usarem CAs privadas ou autoassinadas. As conexões em dispositivos Android N são interrompidas nos seguintes cenários:

- CAs privadas/autoassinadas e a opção CA Confiável Necessária para Endpoint Management está definida como **ATIVADA**. Para obter detalhes, consulte [Gerenciamento de dispositivos](#).
- CAs privadas/autoassinadas e o Serviço de Descoberta Automática (ADS) do Endpoint Management não estão acessíveis. Devido a preocupações de segurança, quando o ADS não está acessível, a CA Confiável Necessária é ativada (**ON**), mesmo que tenha sido definida como desativada (**OFF**) inicialmente.

Antes de registrar dispositivos ou atualizar o Secure Hub, considere habilitar a fixação de certificado. A opção está **Desativada** por padrão e é gerenciada pelo ADS. Quando você habilita 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 são avisados de que o certificado não é confiável. O registro falha se os usuários não aceitarem o certificado.

Para usar a fixação de certificado, solicite que a Citrix carregue certificados para o servidor ADS da Citrix. Abra um caso de suporte técnico usando o [portal de Suporte da Citrix](#). Certifique-se de não enviar a chave privada para a Citrix. Em seguida, forneça as seguintes informações:

- O domínio que contém as contas com as quais 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 diferencia maiúsculas de minúsculas.
- Tipo de ID de Usuário, que pode ser UPN ou Email. Por padrão, o tipo é UPN.
- A porta usada para o registro de iOS se você alterou o número da porta da porta padrão 8443.
- A porta através da qual o Endpoint Management aceita conexões se você alterou o número da porta da porta padrão 443.

- A URL completa do seu Citrix Gateway.
- Opcionalmente, um endereço de e-mail para o seu administrador.
- Os certificados no formato PEM que você deseja adicionar ao domínio, que devem ser certificados públicos e não a chave privada.
- Como manipular quaisquer certificados de servidor existentes: Se deve remover o certificado de servidor antigo imediatamente (porque foi comprometido) ou continuar a dar suporte ao certificado de servidor antigo até que ele expire.

Seu caso de suporte técnico é atualizado quando seus detalhes e certificado forem adicionados aos servidores Citrix.

Autenticação por certificado + senha de uso único

Você pode configurar o Citrix ADC para que o Secure Hub autentique usando um certificado mais um token de segurança que serve como uma senha de uso único. Essa configuração oferece uma opção de segurança forte que não deixa um rastro do Active Directory nos dispositivos.

Para permitir que o Secure Hub use o tipo de autenticação de certificado + senha de uso único, faça o seguinte: Adicione uma ação de reescrita e uma política de reescrita no Citrix ADC que insira um cabeçalho de resposta personalizado no formato **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar o tipo de logon do Citrix Gateway.

Normalmente, o Secure Hub usa o tipo de logon do Citrix Gateway configurado no console do Endpoint Management. No entanto, essa informação não está disponível para o Secure Hub até que o Secure Hub conclua o logon pela primeira vez. Portanto, o cabeçalho personalizado é necessário.

NOTA:

Se diferentes tipos de logon forem definidos para o Endpoint Management e o Citrix ADC, a configuração do Citrix ADC prevalecerá. Para obter detalhes, consulte [Citrix Gateway e Endpoint Management](#).

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

A tela **Create Rewrite Action** é exibida.

3. Preencha cada campo conforme mostrado na figura a seguir e, em seguida, clique em **Create**.

Create Rewrite Action

Name*

Type*

Use this action type to insert a header.

Header Name*

Expression Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

"CertAndRSA"

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

Create Close

O seguinte resultado aparece na tela principal **Rewrite Actions**.

NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action Show built-in Rewrite Actions Search

Name	Type	Target Expression	Expression	Pattern
ns_cvprn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\\\' + window.location.pathname.split("\\\'")[1] + \\' + wi...	re~a.substr(0,3).toLowerCase() =~ "%2f" a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

- Vincule a ação de reescrita ao servidor virtual como uma política de reescrita. Vá para **Configuration > NetScaler® Gateway > Virtual Servers** e, em seguida, selecione seu servidor virtual.

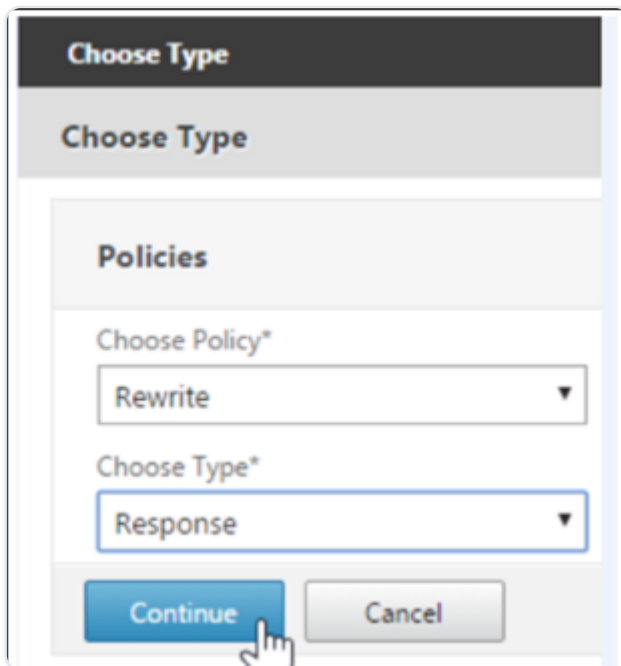
The screenshot shows the NetScaler Configuration page. The left sidebar contains a tree view with categories like System, AppExpert, Traffic Management, Optimization, Security, and NetScaler Gateway. Under NetScaler Gateway, 'Virtual Servers' is selected. The main area displays a table of Virtual Servers with columns: Name, State, IP Address, Port, Protocol, Maximum Users, Current Users, and Total Connected Users. Two servers are listed: '_XM_gwcamamappc8' and 'SessionTransfer', both in 'Up' state. Above the table are buttons for 'Add', 'Edit', 'Delete', 'Statistics', 'Visualizer', and an 'Action' dropdown. A mouse cursor is pointing at the 'Edit' button.

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

5. Clique em **Edit**.
6. Na tela de **configuração de Servidores Virtuais**, role para baixo até **Políticas**.
7. Clique em **+** para adicionar uma política.

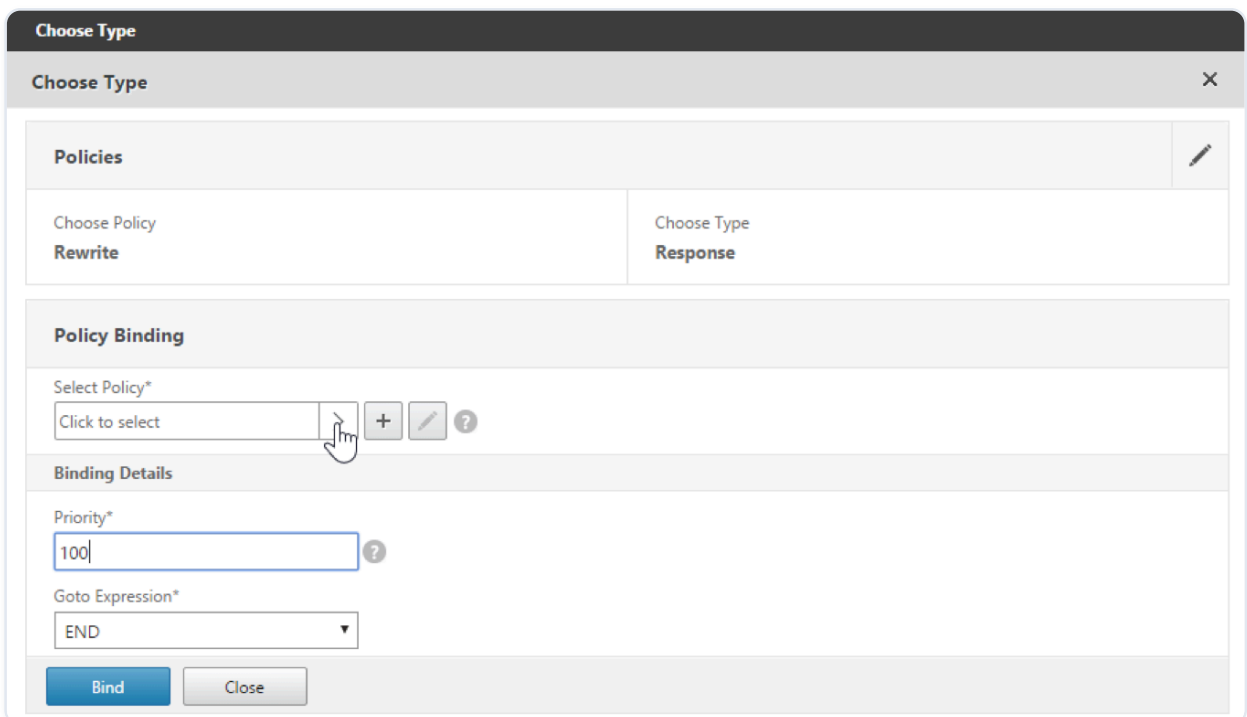
The screenshot shows the NetScaler Profiles configuration page. It has several sections: 'Profiles' (showing Net, TCP, and HTTP profiles), 'Published Applications' (showing Next Hop Server, STA Server, and Url), 'Other Settings' (showing ICMP, RHI, Redirect, Listen Priority, Listen Policy Expression, ShareFile, AppController, and L2 Connection), and 'Policies' (showing Request Policies, Session Policies, ClientlessAccess Policies, and Cache Policies). A mouse cursor is pointing at the '+' button in the 'Policies' section header.

8. No campo **Escolher Política**, selecione **Reescrever**.
9. No campo **Escolher Tipo**, selecione **Resposta**.



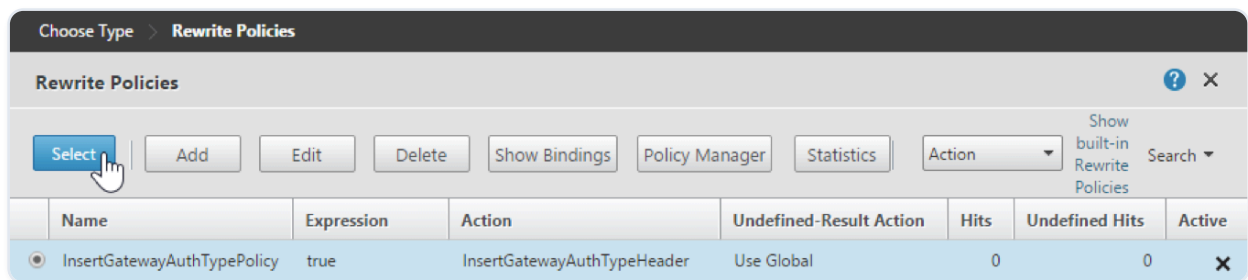
10. Clique em **Continuar**.

A seção **Associação de Política** se expande.

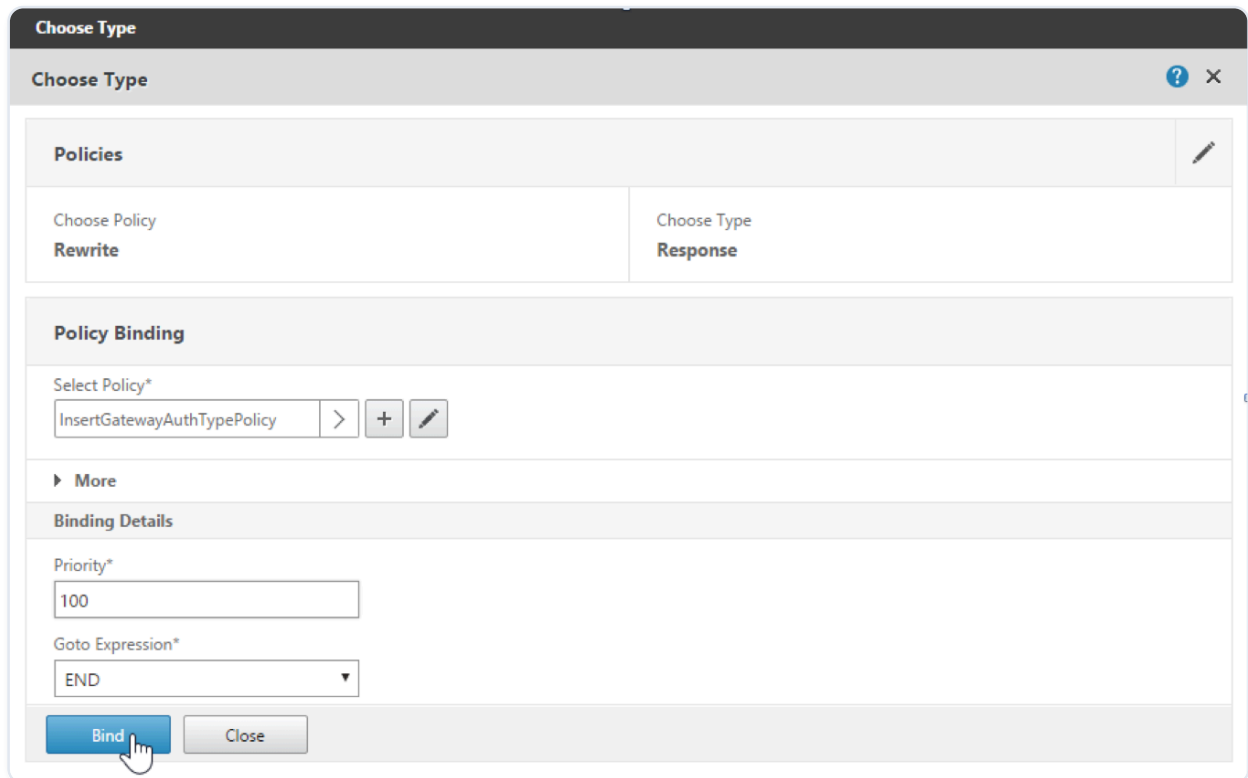


11. Clique em **Selecionar Política**.

Uma tela com as políticas disponíveis é exibida.



12. Clique na linha da política que você criou e, em seguida, clique em **Selecionar**. A tela **Associação de Política** é exibida novamente, com a política selecionada preenchida.



13. Clique em **Vincular**.

Se a vinculação for bem-sucedida, a tela de configuração principal aparecerá com a política de reescrita concluída exibida.

The screenshot shows the configuration interface for a VPN Virtual Server. It includes sections for 'Published Applications' and 'Other Settings'. The 'Policies' section is highlighted with a green border and contains a list of policies: Request Policies, Session Policies (3), ClientlessAccess Policies (2), Cache Policies (4), Response Policies (1), and Rewrite Policy (1). The 'Rewrite Policy' is highlighted with a red border.

Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED
Refresh Count	0	Client Authentication	ENABLED	SSLv3	ENABLED
Enable Session Reuse	ENABLED	Client Certificate	Mandatory	TLSv1	ENABLED
Time-out	120	Send Close-Notify	YES	TLSv1.1	ENABLED
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLSv1.2	ENABLED
		SNI Enable	DISABLED		

Published Applications

- No Next HOP Server
- 1 STA Server
- No Uri

Other Settings

ICMP Virtual Server Response	Passive	Listen Priority	
RHI State	Passive	Listen Policy Expression	None
Redirect to Home page	true	ShareFile	
		AppController	https://xms3.dm.com:8443
		L2 Connection	false

Policies

- Request Policies
- 3 Session Policies
- 2 ClientlessAccess Policies
- 4 Cache Policies
- Response Policies
- 1 Rewrite Policy

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

The screenshot shows the 'VPN Virtual Server Rewrite Policy Binding' configuration window. It includes a table with columns: Priority, Policy Name, Expression, Action, and Goto Expression. The table contains one row with the following values: Priority 100, Policy Name InsertGatewayAuthTypeHeaderPolicy, Expression true, Action InsertGatewayAuthTypeHeader, and Goto Expression END.

Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END

Requisito de porta para conectividade ADS para dispositivos Android

A configuração da porta garante que os dispositivos Android que se conectam do Secure Hub possam acessar o Citrix ADS de dentro da rede corporativa. A capacidade de acessar o ADS é importante ao baixar atualizações de segurança disponibilizadas por meio do ADS. As conexões ADS podem não ser compatíveis com seu servidor proxy. Nesse cenário, permita que a conexão 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 ocorre na porta de saída 443. É altamente provável que seu ambiente existente seja projetado para permitir esse acesso. Clientes que não podem garantir essa comunicação são desencorajados a atualizar para o Secure Hub 10.2. Se tiver alguma dúvida, entre em contato com o suporte da Citrix.

Pré-requisitos:

- Colete os certificados do Endpoint Management e do Citrix ADC. Os certificados devem estar no formato PEM e devem ser um certificado público, não a chave privada.
- Entre em contato com o suporte da Citrix e faça uma solicitação para habilitar o certificate pinning. Durante esse processo, seus certificados serão solicitados.

As novas melhorias de certificate pinning exigem que os dispositivos se conectem ao ADS antes que o dispositivo seja registrado. Esse pré-requisito garante que as informações de segurança mais recentes estejam disponíveis para o Secure Hub para o ambiente no qual o dispositivo está sendo registrado. Se os dispositivos não conseguirem alcançar o ADS, o Secure Hub não permitirá o registro do dispositivo. Portanto, abrir o acesso ao ADS dentro da rede interna é fundamental para permitir que os dispositivos sejam registrados.

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

FQDN	ENDEREÇO IP	PORTA	USO DE IP E PORTA
<code>discovery.mdm.zenprise.com</code>	52.5.138.94	443	Secure Hub - Comunicação ADS
<code>discovery.mdm.zenprise.com</code>	52.1.30.122	443	Secure Hub - Comunicação ADS
<code>ads.xm.cloud.com</code> : observe que o Secure Hub versão 10.6.15 e posterior usa	34.194.83.188	443	Secure Hub - Comunicação ADS

FQDN	ENDEREÇO IP	PORTA	USO DE IP E PORTA
ads.xml.cloud.com			
ads.xml.cloud.com : observe que o Secure Hub versão 10.6.15 e posterior usa ads.xml.cloud.com	34.193.202.23	443	Secure Hub - Comunicação ADS

Se o fixamento de certificado estiver habilitado:

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

NOTA:

Se você habilitar o fixamento de certificado após uma atualização, os usuários deverão se registrar novamente.

- A renovação do certificado não exige novo registro, se a chave pública do certificado não for alterada.

O fixamento de certificado suporta certificados folha, não certificados intermediários ou de emissor. O fixamento de certificado se aplica a servidores Citrix, como Endpoint Management e Citrix Gateway, e não a servidores de terceiros.

Desabilitando a opção Excluir Conta

Você pode desabilitar a opção **Excluir Conta** no Secure Hub em ambientes onde o Auto Discovery Services (ADS) está habilitado.

Execute as seguintes etapas para desabilitar a opção **Excluir Conta**:

1. Configure o ADS para seu domínio.
2. Abra as **Informações do Serviço de Descoberta Automática** no Citrix Endpoint Management e defina o valor para `displayReenrollLink` como **False**. Por padrão, esse valor é **True**.

3. Se o seu dispositivo estiver registrado no modo MDM+MAM (ENT), saia e faça login novamente para que as alterações entrem em vigor. Se o seu dispositivo estiver registrado em outros modos, você deve registrá-lo novamente.

Usando o Secure Hub

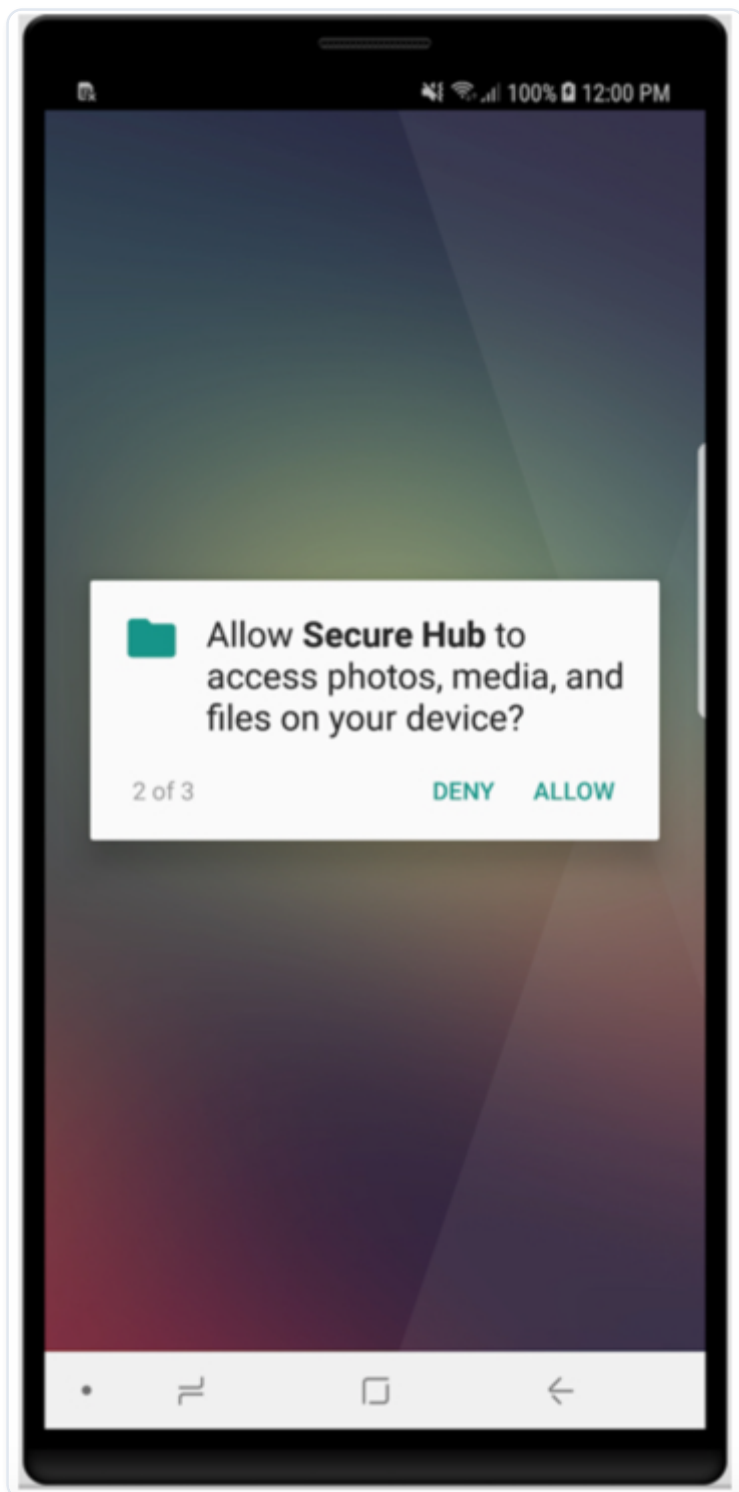
Os usuários começam baixando o Secure Hub em seus dispositivos na loja da Apple ou Android.

Quando o Secure Hub é aberto, os usuários inserem as credenciais fornecidas por suas empresas para registrar seus dispositivos no Secure Hub. Para mais detalhes sobre o registro de dispositivos, consulte [Contas de usuário, funções e registro](#).

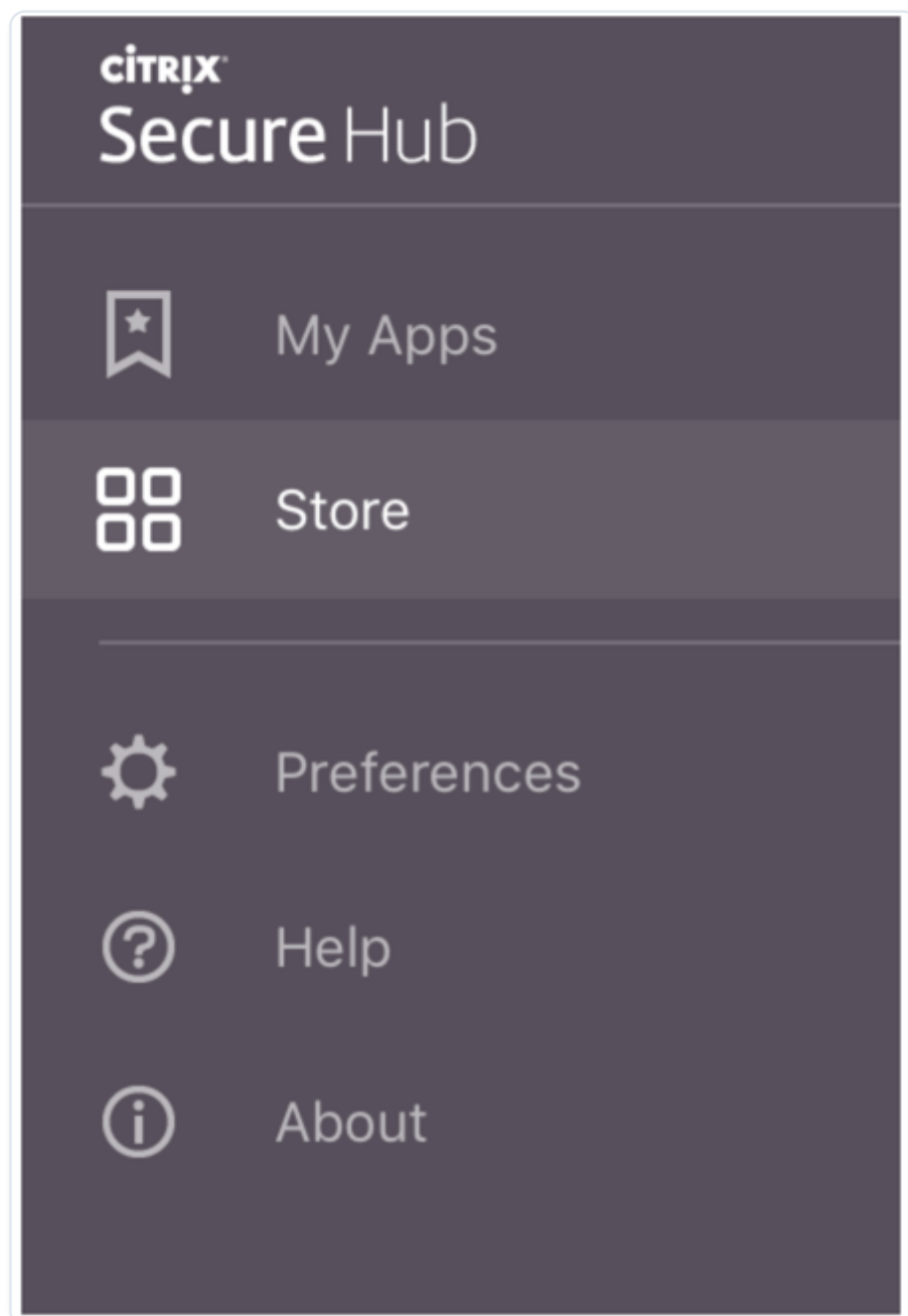
No Secure Hub para Android, durante a instalação e o registro iniciais, a seguinte mensagem aparece: Permitir que o Secure Hub acesse fotos, mídias e arquivos em seu dispositivo?

Esta mensagem vem do sistema operacional Android e não da Citrix. Ao tocar em **Permitir**, a Citrix e os administradores que gerenciam o Secure Hub não visualizam seus dados pessoais a qualquer momento. No entanto, se você realizar uma sessão de suporte remoto com seu administrador, o administrador poderá visualizar seus arquivos pessoais dentro da sessão.

Uma vez registrados, os usuários veem todos os aplicativos e desktops que você enviou na guia **Meus Aplicativos**. Os usuários podem adicionar mais aplicativos da Loja. Em telefones, o link da Loja está sob o ícone de hambúrguer **Configurações** no canto superior esquerdo.



Em tablets, a Loja é uma guia separada.



Quando usuários de iPhones com iOS 9 ou posterior instalam aplicativos de produtividade móvel da loja, eles veem uma mensagem. A mensagem indica que o desenvolvedor corporativo, Citrix, não é confiável naquele iPhone. A mensagem observa que o aplicativo não está disponível para uso até que o desenvolvedor seja confiável. Quando esta mensagem aparece, o Secure Hub solicita aos usuários que visualizem um guia que os orienta no processo de confiar nos aplicativos corporativos da Citrix para seus iPhones.

Registro automático no Secure Mail

Para implantações somente MAM, você pode configurar o Endpoint Management para que usuários com dispositivos Android ou iOS que se registram no Secure Hub usando credenciais de

e-mail sejam automaticamente registrados no Secure Mail. Os usuários não precisam inserir mais informações ou seguir mais etapas para se registrar no Secure Mail.

No primeiro uso do Secure Mail, o Secure Mail obtém o endereço de e-mail, domínio e ID de usuário do Secure Hub. O Secure Mail usa o endereço de e-mail para AutoDiscovery. O Exchange Server é identificado usando o domínio e o ID de usuário, o que permite que o Secure Mail autenticar o usuário automaticamente. O usuário é solicitado a inserir uma senha se a política estiver configurada para não passar a senha. No entanto, o usuário não é obrigado a inserir mais informações.

Para habilitar este recurso, crie três propriedades:

- A propriedade do servidor MAM_MACRO_SUPPORT. Para obter instruções, consulte [Propriedades do servidor](#).
- As propriedades do cliente ENABLE_CREDENTIAL_STORE e SEND_LDAP_ATTRIBUTES. Para obter instruções, consulte [Propriedades do cliente](#).

Loja Personalizada

Se você quiser personalizar sua Loja, vá para **Configurações > Marca do Cliente** para alterar o nome, adicionar um logotipo e especificar como os aplicativos aparecem.

The screenshot shows the 'Client Branding' configuration page in the XenMobile console. The page has a green header with 'XenMobile' and navigation tabs: 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'administrator'. The breadcrumb trail is 'Settings > Client Branding'. The main heading is 'Client Branding' with a subtext: 'You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.' The configuration options include: 'Store name' (text input with 'Store' and a help icon), 'Default store view' (radio buttons for 'Category' and 'A-Z', with 'A-Z' selected), 'Device' (radio buttons for 'Phone' and 'Tablet', with 'Phone' selected), and 'Branding file' (text input with a 'Browse' button). A 'Note' section at the bottom provides guidelines for the branding file: it must be in .png format, have a white logo/text on a transparent background at 72 dpi, not exceed 170px x 25px (1x) + 340px x 50px (2x), and be named 'Header.png' and 'Header@2x.png'. A .zip file should be created from these files, not a folder containing them. At the bottom right are 'Cancel' and 'Save' buttons.

Você pode editar descrições de aplicativos no console do Endpoint Management. Clique em **Configurar** e depois em **Aplicativos**. Selecione o aplicativo na tabela e clique em **Editar**.

Selecione as plataformas para o aplicativo com a descrição que você está editando e digite o texto na caixa **Descrição**.

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is selected, and the 'App Information' section is active. On the left, there is a sidebar with a list of steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. Under '2 Platform', 'iOS' and 'Android' are checked, while 'Windows Phone' is unchecked. The main area contains fields for 'Name' (set to 'Workmail'), 'Description' (empty), and 'App category' (set to 'Workapps').

Na Loja, os usuários podem navegar apenas pelos aplicativos e desktops que você configurou e protegeu no Endpoint Management. Para adicionar o aplicativo, os usuários tocam em **Detalhes** e depois em **Adicionar**.

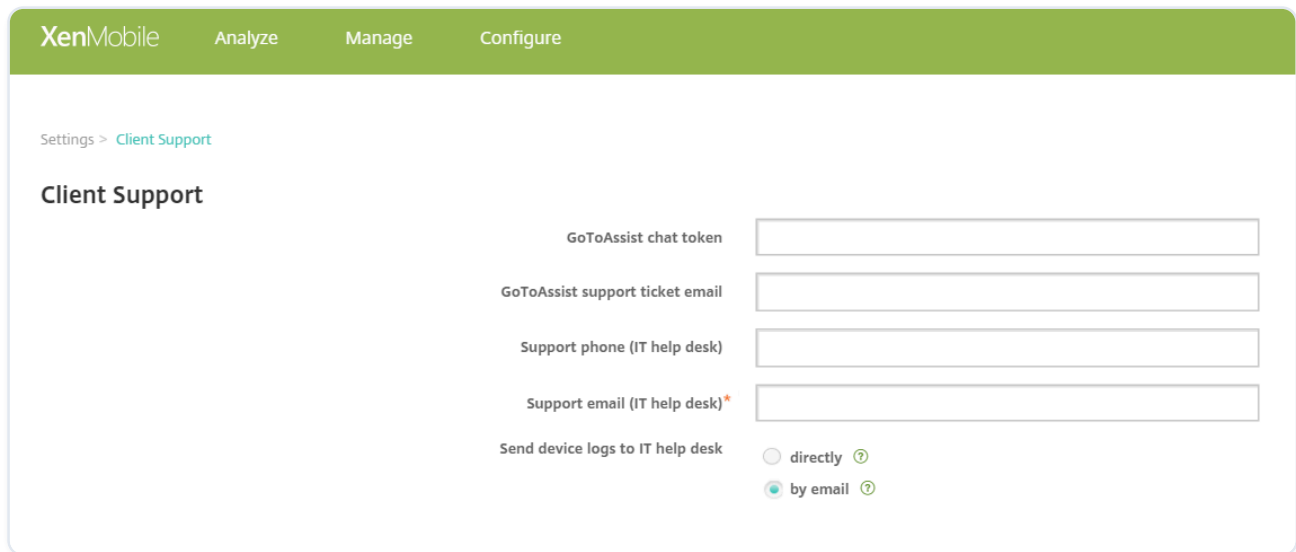
Opções de Ajuda Configuradas

O Secure Hub também oferece aos usuários várias maneiras de obter ajuda. Em tablets, tocar no ponto de interrogação no canto superior direito abre as opções de ajuda. Em telefones, os usuários tocam no ícone do menu hambúrguer no canto superior esquerdo e depois tocam em **Ajuda**.

The screenshot shows a 'Help Desk' modal with a 'Close' button in the top left. The modal contains three main options: 'Your IT Department' with a right arrow, 'Report Issue' with a right arrow, and 'Send Feedback to Citrix'. At the bottom, there is a 'Citrix Support' link.

Seu Departamento de TI mostra o telefone e o e-mail do suporte técnico da sua empresa, que os usuários podem acessar diretamente do aplicativo. Você insere números de telefone e endereços de e-mail no console do Endpoint Management. Clique no ícone de engrenagem no canto superior

direito. A página **Configurações** é exibida. Clique em **Mais** e depois em **Suporte ao Cliente**. A tela onde você insere as informações é exibida.



The screenshot shows the 'Client Support' configuration page in the XenMobile interface. The top navigation bar is green with the XenMobile logo and tabs for 'Analyze', 'Manage', and 'Configure'. The breadcrumb trail is 'Settings > Client Support'. The page title is 'Client Support'. There are four text input fields for: 'GoToAssist chat token', 'GoToAssist support ticket email', 'Support phone (IT help desk)', and 'Support email (IT help desk)*'. Below these fields is a section 'Send device logs to IT help desk' with two radio button options: 'directly' (unselected) and 'by email' (selected). Each radio button has a help icon (question mark in a circle).

Relatar Problema mostra uma lista de aplicativos. Os usuários selecionam o aplicativo que apresenta o problema. O Secure Hub gera logs automaticamente e, em seguida, abre uma mensagem no Secure Mail com os logs anexados como um arquivo zip. Os usuários adicionam linhas de assunto e descrições do problema. Eles também podem anexar uma captura de tela.

Enviar Feedback para a Citrix abre uma mensagem no Secure Mail com um endereço de suporte da Citrix preenchido. No corpo da mensagem, o usuário pode inserir sugestões para melhorar o Secure Mail. Se o Secure Mail não estiver instalado no dispositivo, o programa de e-mail nativo será aberto.

Os usuários também podem tocar em **Suporte Citrix**, que abre o [Citrix Knowledge Center](#). A partir daí, eles podem pesquisar artigos de suporte para todos os produtos Citrix.

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

Políticas de localização

O Secure Hub também oferece políticas de geolocalização e geomonitoramento se, por exemplo, você quiser garantir que um dispositivo corporativo não viole um determinado perímetro geográfico. Para obter detalhes, consulte [Política de dispositivo de localização](#).

Coleta e análise de falhas

O Secure Hub coleta e analisa automaticamente as informações de falha para que você possa ver o que levou a uma falha específica. O software Crashlytics oferece suporte a essa função.

Para mais recursos disponíveis para iOS e Android, consulte a matriz de recursos por plataforma para [Citrix Secure Hub](#).

Gerar logs do lado do dispositivo para o Secure Hub

Esta seção explica como gerar os logs do lado do dispositivo do Secure Hub e como configurar o nível de depuração correto neles.

Para obter os logs do Secure Mail, faça o seguinte:

1. Vá para **Secure Hub > Ajuda > Relatar Problema**. Selecione Secure Mail na lista de aplicativos. Um e-mail endereçado ao suporte técnico da sua organização é aberto.
2. Altere as configurações de log somente se sua equipe de suporte o tiver instruído a fazê-lo. Sempre confirme se as configurações estão definidas corretamente.
3. Retorne ao Secure Mail e reproduza o problema. Anote a hora em que o problema começou a ser reproduzido e a hora em que o problema ocorre ou a mensagem de erro é exibida.
4. Retorne a **Secure Hub > Ajuda > Relatar Problema**. Selecione Secure Mail na lista de aplicativos. Um e-mail endereçado ao suporte técnico da sua organização é aberto.
5. Preencha a linha de assunto e o corpo com algumas palavras descrevendo seu problema. Inclua os carimbos de data e hora coletados na etapa 3 e clique em **Enviar**. A mensagem concluída é aberta com arquivos de log compactados anexados.
6. Clique em **Enviar** novamente.

Os arquivos zip enviados incluem os seguintes logs:

- CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt e WH_logx.txt (Windows Phone)

Os logs de informações do aplicativo incluem informações sobre o dispositivo e o aplicativo.

Problemas conhecidos e corrigidos

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

Secure Hub para iOS 26.8.1

Problemas corrigidos

- Ao iniciar aplicativos HDX do Secure Hub para iOS por meio do aplicativo Citrix Workspace, os aplicativos podem falhar ao iniciar.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 26.8.0

Problemas corrigidos

- Na política de Restrições do Android Enterprise, configurar uma lista de permissões de aplicativos de sistema específica pode substituir a configuração **All#** e ocultar novamente os aplicativos de sistema já permitidos.
- Em dispositivos Android Enterprise em modo quiosque (COSU), o PIN de bloqueio do dispositivo que o Secure Hub aplicou quando um dispositivo saiu de um perímetro de cerca geográfica pode não ser removido depois que o dispositivo retorna à área permitida. Como resultado, o dispositivo continua solicitando o PIN, e um administrador precisa recuperá-lo do console e desbloquear o dispositivo manualmente.
- Em dispositivos com Android 16 e Android 17, incluindo dispositivos Samsung com One UI 8.5, o dispositivo pode permanecer no modo de tarefa bloqueada (quiosque) após a conclusão do registro de dispositivo totalmente gerenciado ou dispositivo dedicado. Como resultado, os usuários não podem sair da tela do Secure Hub, o registro parece estar incompleto e o dispositivo precisa ser reiniciado.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 26.8.0

Problemas corrigidos

- Ao chamar o logout da Microsoft Authentication Library (MSAL), o Secure Hub pode falhar devido a uma condição de corrida ou deadlock.
- O Secure Mail e o Secure Web podem falhar no primeiro uso quando o sinalizador de recurso `mam-app-data-sharing` estiver ativado.
- Em dispositivos DEP, o perfil MDM pode não ser excluído durante uma limpeza seletiva acionada por aplicativos seguros.
- Quando os usuários enviam feedback do Secure Hub, o feedback pode ser enviado para um endereço de e-mail de suporte desatualizado.
- O pop-up do PIN pode persistir mesmo após a exclusão da conta.
- O botão **Enviar Log** pode não responder ao ser tocado.
- O Secure Hub pode incluir a permissão `NSAppleMusicUsageDescription` desnecessária.
- Para locatários com mais de 2100 licenças, a instalação de um aplicativo do Programa de Compra por Volume (VPP) pode redirecionar os usuários para a App Store em vez de instalar o aplicativo.
- O Secure Hub pode falhar com um erro SIGABRT ao carregar o cofre de chaves compartilhado.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 26.5.0

Problemas corrigidos

A descoberta automática do Secure Hub pode falhar quando as URLs do servidor ADS incluem um valor de porta inválido.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 26.2.0

Problemas corrigidos

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 25.10.0

Problemas corrigidos

O Secure Hub relata falha de implantação ao servidor CEM quando o aplicativo necessário não está instalado para desbloquear a implantação da política.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 25.8.0

Problemas corrigidos

- Ao ativar e desativar o sinalizador de recurso de compartilhamento de dados de aplicativos do Mobile Application Management (MAM), alguns aplicativos MAM podem exibir um alerta pop-up informando "O aplicativo foi removido".
- Ao cancelar o registro do Secure Hub, alguns aplicativos MAM podem permanecer disponíveis para uso.
- ao alterar as configurações de log para aplicativos MAM do Secure Hub, as alterações podem não ser efetivas.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 25.7.0

Problemas corrigidos

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 25.6.0

Problemas corrigidos

- Ao usar o aplicativo Secure Hub, você pode ter falhas ocasionais ou receber a seguinte mensagem de erro ao acessar a loja, mesmo após várias tentativas: “Não foi possível carregar a loja. Tente novamente.”
- Ao usar o Programa de Registro de Dispositivos (DEP) ou Retorno ao Serviço (RTS) no modo somente Gerenciamento de Dispositivos Móveis (MDM), o processo pode não ser suportado.
- Você pode encontrar falhas durante o registro do Azure Active Directory (AAD) para dispositivos registrados pelo Active Directory local.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 25.4.0

Problemas corrigidos

Quando um usuário reinscreve o mesmo dispositivo sem primeiro limpá-lo e excluí-lo do console CEM, ele não consegue atualizar manualmente a política se o serviço estiver desativado.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 25.1.0

Problemas corrigidos

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 25.1.0

Problemas corrigidos

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 24.11.0

Problemas corrigidos

Os dispositivos iOS estão solicitando aos usuários que insiram seu Nome Principal de Usuário (UPN) ao abrir o Secure Hub, apesar de os dispositivos já estarem registrados no Programa de Registro de Dispositivos (DEP).

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 24.10.0

Problemas corrigidos

Não há problemas corrigidos nesta versão.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 24.9.0

Problemas corrigidos

Não há problemas corrigidos nesta versão.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 24.8.0

Problemas corrigidos

Não há problemas corrigidos nesta versão.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 24.6.0

Problemas corrigidos

Não há problemas corrigidos nesta versão.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 24.5.0

Problemas corrigidos

Não há problemas corrigidos nesta versão.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 24.3.0

Problemas corrigidos

Os usuários podem realizar uma redefinição de fábrica em dispositivos Android Enterprise de propriedade da empresa, mesmo quando a política de restrição para redefinição de fábrica está definida como NÃO. Esse problema ocorre quando um usuário reinicia o Secure Hub.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 24.1.0

Problemas corrigidos

- Quando você faz o jailbreak de um dispositivo iOS com o aplicativo Palera1n, o servidor Citrix Endpoint Management™ não detecta o dispositivo como jailbroken. Como resultado, o servidor Endpoint Management não consegue redefinir o dispositivo jailbroken para as configurações de fábrica. Além disso, o servidor Endpoint Management não consegue limpar as entradas do dispositivo jailbroken do console do servidor.
- Ao usar o SDK MAM para gerenciar seus aplicativos iOS, a loja do Secure Hub encontra um dos seguintes problemas:
 - Não notifica quando uma atualização está disponível para os aplicativos.
 - Notifica continuamente sobre atualizações mesmo depois que os aplicativos são atualizados.
- Ao usar o SDK MAM para gerenciar seus aplicativos iOS, o seguinte alerta de conformidade pode aparecer:

"Este aplicativo foi removido da sua conta. Você pode removê-lo do seu dispositivo."

O problema ocorre quando você instala o MAM SDK e o MDX toolkit no mesmo dispositivo iOS.

Secure Hub para Android 23.12.0

Problemas corrigidos

Quando a credencial do Citrix Gateway expira, o Secure Hub pode não gerar um novo certificado para se conectar ao servidor Citrix Gateway. Como resultado, o Secure Hub falha ao iniciar com a seguinte mensagem de erro.

"Ocorreu um erro na sua conexão. Tente conectar novamente"

Secure Hub para iOS 23.11.0

Problemas corrigidos

- A autenticação do Secure Hub falha em dispositivos iOS, pois o certificado de cliente do Citrix Gateway não é renovado automaticamente quando expira. O problema ocorre quando o Citrix Gateway usa o protocolo TLSv1.3.
- Ao fazer login no Secure Hub através do Citrix Gateway, você pode receber a seguinte mensagem de erro:

"Não foi possível fazer login. Credenciais incorretas. Encerrando a sessão"

O problema ocorre quando você registra seu dispositivo iOS no Citrix Endpoint Management (CEM) com nFactor.

Secure Hub para Android 23.10.0

Problemas corrigidos

No Android versão 11 e posterior, a política de Wi-Fi em dispositivos Android Enterprise pode não ser implantada. Esse problema ocorre quando o valor do domínio não é especificado no campo Anônimo na política de Wi-Fi.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 23.9.0

Problemas corrigidos

Esta versão aborda áreas que melhoram o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 23.8.1

Problemas corrigidos

- Quando um usuário tenta registrar os dispositivos usando o Secure Hub 23.8.0, e o nome de usuário está no formato `sAMAccount`, o processo pode falhar com a seguinte mensagem de erro:

"Falha no registro, o usuário logado no MAM não corresponde ao usuário registrado, tente registrar novamente."

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 23.8.0

Problemas corrigidos

- Ao registrar seu dispositivo iOS no Citrix Endpoint Management (CEM) com nFactor, você pode ter problemas para estabelecer um túnel micro VPN.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Problemas conhecidos e corrigidos em versões anteriores

Para problemas conhecidos e corrigidos em versões anteriores do Secure Hub, consulte [Histórico de problemas conhecidos e corrigidos do Secure Hub](#).

Histórico de problemas conhecidos e corrigidos do Secure Hub

Este artigo lista problemas corrigidos e conhecidos do Secure Hub para versões anteriores às versões suportadas mais recentes. Para a documentação mais recente, consulte [Citrix Secure Hub](#).

Secure Hub para Android 23.7.0

Problemas corrigidos

- Na plataforma Android Enterprise, a política de Configurações Gerenciadas pode não ser aplicada ao dispositivo após o registro.
- Na plataforma Android Enterprise, o aplicativo da Loja de Aplicativos Pública necessário pode não ser instalado automaticamente no dispositivo após o registro.
- Ao reiniciar seu dispositivo e não desbloqueá-lo, talvez você não consiga redefinir a senha do dispositivo por meio do comando de bloqueio emitido pelo administrador de TI.

Este método é útil caso o usuário final perca a senha do dispositivo ou perca o dispositivo, ele pode pedir ao administrador para redefinir a senha do dispositivo ou bloquear o dispositivo por meio do comando de bloqueio.

- Quando os usuários finais abrem o Secure Hub em determinados dispositivos Android para registro, o aplicativo Secure Hub para de responder

O problema ocorre quando o registro MDM falha devido a uma licença expirada. Consequentemente, o aplicativo Secure Mail fica indisponível.

- Quando você configura o Citrix Gateway como provedor de identidade (IdP) para fins de autenticação, e a conexão de rede com o gateway está instável, a autenticação falha e os usuários finais não conseguem fazer login no Secure Hub.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para iOS 23.4.0

Problemas corrigidos

Esta versão aborda alguns problemas que ajudam a melhorar o desempenho e a estabilidade gerais.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 23.4.1

Problemas corrigidos

- Uma interface de usuário com um spinner de carregamento aparece ao iniciar o aplicativo Secure Hub. Este problema ocorre devido a uma condição de deadlock.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 23.4.0

Problemas corrigidos

- Depois de atualizar um dispositivo do Android 11 para o Android 12 e depois para o Android 13, o aplicativo Secure Hub falha ao iniciar.
- Depois de se registrar em um dispositivo de uso único de propriedade corporativa (COSU), o aplicativo Secure Hub solicita uma senha do Active Directory (AD) em vez do PIN do Citrix. O problema pode ocorrer devido à perda de credenciais em cache na versão 23.2.0 e anteriores do Secure Hub.
- O aplicativo Secure Hub para de responder porque o PIN não é aceito devido a uma exceção no código.

Problemas conhecidos

Não há problemas conhecidos nesta versão.

Secure Hub para Android 23.2.0

Problemas corrigidos

- Depois de se registrar em um dispositivo de uso único de propriedade corporativa (COSU) e a política de restrições permitir o uso de cartões SD, você ainda poderá não conseguir acessar o cartão SD externo nesses dispositivos. O problema é que se trata de um dispositivo dedicado.
- As configurações da política de senha para expiração de senha em dispositivos Android Enterprise não funcionam como esperado. O prompt de alteração de senha não aparece. Em vez disso, você precisa alterar a senha manualmente.
- Ocasionalmente, depois de atualizar um dispositivo do Android 11 para o Android 13, o aplicativo Secure Hub para de responder.
- Cada vez que você faz login no Secure Hub, o aplicativo solicita a senha do Active Directory (AD) em vez do PIN do Citrix. O problema ocorre depois que você alterou a senha do AD.
- Depois de alterar a senha do Active Directory (AD), as tentativas de login no Secure Hub falham com a seguinte mensagem de erro:

Credenciais incorretas.

Secure Hub 22.11.0

- Quando uma mensagem push é enviada do console CEM para o canal **Enrollment App**, a mensagem chega ao dispositivo, mas não aciona o alerta sonoro.
- Ao configurar a **Política de Credenciais** e definir o alias do certificado, o aplicativo Citrix SSO falha ao se conectar à VPN com um erro de autenticação ao usar o alias de certificado personalizado. A seguinte mensagem de erro aparece:

Erro de conexão: Não é possível conectar-se ao *ID do certificado*. Verifique sua conexão com a internet e as configurações para *ID do certificado*.

O problema ocorre quando você permite que os aplicativos usem os certificados para o aplicativo Citrix SSO.

Secure Hub 22.9.0

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 22.7.0

Problemas corrigidos

- Depois de mudar do Mobile Device Experience (MDX) para o Citrix Mobile Application Management (MAM) SDK e atualizar o XenMobile Server para 10.13 RP4, talvez você não consiga acessar sites da intranet através do Secure Hub/Secure Web.

A seguinte mensagem de erro aparece: "Err_Name_not_resolved".

- As configurações da política de configuração gerenciada não são aplicadas em perfis de trabalho que têm a configuração de registro como Perfil de Trabalho para Dispositivos de Propriedade da Empresa (WPCOD). O problema ocorre quando a autenticação é feita através do Provedor de Identidade (IdP) e o Perfil de Trabalho não está marcado como provisionado.

Secure Hub 22.6.0

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 22.5.0

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 22.4.0

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 22.2.0

Problemas conhecidos no Secure Hub 22.2.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 22.2.0

Secure Hub para iOS

- No Secure Hub para iOS, você é solicitado a se registrar usando um PIN em dispositivos registrados através do Programa de Implantação da Apple.
- Ao fazer login no Secure Mail depois que seu dispositivo ficou ocioso, o Secure Hub para iOS é aberto com a seguinte mensagem de erro:

"O Secure Hub precisa autorizar este aplicativo."

Depois de clicar em autorizar e fornecer suas credenciais, a autenticação entra em um loop. Você não consegue reautenticar ou fazer login mesmo após uma reinicialização.

- O Secure Hub para iOS para de responder em dispositivos com iOS 15.1 ao relatar um erro.
- No Secure Hub para iOS, a contagem do selo aparece como 1 ou 2, apesar de não haver novas notificações.
- No Secure Hub para iOS, o registro pode falhar em alguns dispositivos.
- Se você configurar o valor da política de tempo limite da sessão do Citrix Gateway para 30 dias, o Secure Hub para iOS solicitará que os usuários se reautentiquem a cada 24 a 72 horas.

Secure Hub para Android

- No modo Samsung DeX, o Secure Hub para de responder ao inserir o PIN.
- Ao registrar dispositivos Samsung S20, no modo totalmente gerenciado, no Android Enterprise, o seguinte erro aparece: "Certificado de servidor inválido"
- O registro de dispositivos com Android 10 ou 11 falha e a seguinte mensagem de erro aparece: "A política de segurança não permite que você se conecte".
- Ao se registrar no Secure Hub para Android, suas credenciais são substituídas por números aleatórios se você alternar do modo retrato para o modo paisagem.

Secure Hub 21.11.0

Problemas conhecidos no Secure Hub 21.11.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.11.0

Secure Hub para Android

- Durante o registro no Secure Hub para Android, a mensagem de erro **Nenhum certificado encontrado** é exibida. Ao clicar em **Instalar certificado**, um link vazio, sem nenhum certificado, aparece. Se você clicar em **Cancelar**, a tela de autenticação é exibida. Esse problema também ocorre quando você sai e entra no Secure Hub.

Secure Hub 21.10.0

Problemas conhecidos no Secure Hub 21.10.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.10.0

Secure Hub para iOS

- No Secure Hub para iOS, você é solicitado a se registrar usando um PIN em dispositivos registrados através do Programa de Implantação da Apple.

Secure Hub para Android

- Ao criar um perfil de registro para dispositivos Android para registrar no modo de perfil de trabalho em dispositivos de propriedade corporativa, você deve habilitar a configuração **Perfil de trabalho BYOD**. Se você não habilitar essa configuração, os dispositivos falharão ao registrar.
- Ao fazer login no Secure Hub para Android, o ID de e-mail é preenchido automaticamente.

Secure Hub 21.8.0

Secure Hub para iOS

Problemas conhecidos no Secure Hub 21.8.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.8.0

- Ao fazer login no Secure Mail depois que seu dispositivo ficou ocioso, o Secure Hub para iOS é aberto e tenta fazer login, mas a solicitação de login falha. O Secure Mail continua solicitando o login e cria um loop de login.
- Usuários com certos caracteres especiais em seu nome de usuário ou senha não conseguem se registrar.

Secure Hub 21.7.1

Secure Hub para Android

Não há problemas conhecidos ou corrigidos nesta versão.

Problemas conhecidos e corrigidos em versões anteriores

Para problemas conhecidos e corrigidos em versões anteriores do Secure Hub, consulte [Histórico de problemas conhecidos e corrigidos do Secure Hub](#).

Secure Hub 21.7.1

Secure Hub para Android

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 21.7.0

Secure Hub para iOS

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub para Android

Problemas conhecidos no Secure Hub 21.7.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.7.0

- No Secure Hub para Android, os logs do Secure Mail e do Secure Web estão ausentes quando você navegar para **Ajuda > Relatar Problema** depois de reiniciar seu dispositivo.

Secure Hub 21.6.0

Secure Hub para iOS

Problemas conhecidos no Secure Hub 21.6.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.6.0

No Secure Hub para iOS, ao registrar um dispositivo usando o Nome Principal do Usuário (UPN), o nome de usuário não é preenchido automaticamente. Esse problema ocorre quando o Serviço de Descoberta Automática está ativado.

Secure Hub para Android

Problemas conhecidos no Secure Hub 21.6.0

No Secure Hub para Android, não é possível registrar um dispositivo no modo MDM+MAM se o FQDN fornecido contiver letras maiúsculas. Em vez disso, o dispositivo é registrado no modo MAM.

Problemas corrigidos no Secure Hub 21.6.0

No Secure Hub para Android, não é possível registrar dispositivos redefinidos de fábrica que executam o Samsung Knox no modo Administrador do Dispositivo.

Secure Hub 21.5.1

Secure Hub para iOS

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub para Android

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 21.5.0

Problemas conhecidos no Secure Hub 21.5.0

Não há problemas conhecidos nesta versão.

Problema corrigido no Secure Hub 21.5.0

No Secure Hub para Android, não é possível implantar a política de dispositivo Wi-Fi em dispositivos Android Enterprise. A política permanece no estado Pendente.

Secure Hub 21.4.0

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 21.3.2

Secure Hub para iOS

Problemas conhecidos no Secure Hub 21.3.2

Não há problemas conhecidos nesta versão.

Problema corrigido no Secure Hub 21.3.2

Não é possível registrar um dispositivo no Citrix Endpoint Management™, após inserir o PIN do Citrix. O Secure Hub não exibe a mensagem correta para o requisito de PIN.

Secure Hub 21.3.0

Problema conhecido no Secure Hub 21.3.0

No Secure Hub para Android versão 20.9.0 e posterior, não é possível conectar no modo VPN em dispositivos Google Pixel 2.

Problemas corrigidos no Secure Hub 21.3.0

- No Secure Hub para Android, o ID do Cartão de Circuito Integrado (ICCID) é exibido para dispositivos que não têm um cartão SIM inserido.
- No Secure Hub para Android, os aplicativos de produtividade móvel instalados não são exibidos na tela **Meus Aplicativos** ao reiniciar o dispositivo.
- No Secure Hub para Android, não é possível desbloquear dispositivos Android Enterprise se você inseriu a senha errada várias vezes e tentou reiniciar o dispositivo. A seguinte mensagem de erro aparece: **Telefone desligado, entre em contato com o administrador de TI.**

Secure Hub 21.2.0

Secure Hub para Android

Problemas conhecidos no Secure Hub 21.2.0

No Secure Hub para Android, os aplicativos de produtividade móvel instalados não aparecem na tela **Meus Aplicativos** ao reiniciar o dispositivo.

Problemas corrigidos no Secure Hub 21.2.0

- O Secure Hub para Android trava durante o registro de dispositivos.
- Em certas versões do Secure Hub para Android, os botões **Início** e **Voltar** não ficam visíveis após a conclusão do registro em dispositivos Samsung Knox.

Secure Hub 21.1.0

Problemas conhecidos no Secure Hub 21.1.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 21.1.0

- Em dispositivos Android, o Secure Hub falha ao se conectar ao Citrix Endpoint Management quando a política de dispositivo de agendamento de conexão está ativada.
- Em certos dispositivos Samsung registrados, o número de série incorreto é relatado no console do Citrix Endpoint Management.

Secure Hub 20.12.0

Problemas conhecidos no Secure Hub 20.12.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 20.12.0

- No Secure Hub para iOS, você não consegue registrar seus dispositivos. Você recebe o seguinte erro: **Seu dispositivo não está registrado.**
- No Secure Hub para iOS, a string do agente do usuário não inclui a versão do SO para dispositivos registrados no MAM+MDM.
- Em dispositivos Android Enterprise, o Secure Hub trava durante o registro.
- O Secure Hub para Android versão 20.11.0 trava em certos dispositivos Samsung.

Secure Hub 20.11.0

Secure Hub para Android

Problemas conhecidos no Secure Hub 20.11.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 20.11.0

Em alguns dispositivos Samsung, o Secure Hub para Android trava, e você recebe o seguinte erro: **O Secure Hub continua parando.**

Secure Hub 20.10.5

Problemas conhecidos no Secure Hub 20.10.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 20.10.5

- Em dispositivos de uso único de propriedade corporativa (COSU) executando Android 11, você não pode definir o Secure Hub como o iniciador padrão.
- Em dispositivos Android, a criação de um perfil de trabalho falha em certos dispositivos Samsung. Você recebe o seguinte erro: **Não é possível configurar o perfil de trabalho.**
- O registro de gerenciamento de aplicativos móveis (MAM) de dispositivos Android falha através do Serviço de Descoberta Automática do Citrix Endpoint Management.
- Em dispositivos iOS, você não consegue iniciar certos aplicativos. Você recebe o erro **Atualize o Secure Hub para usar este aplicativo** mesmo quando não há atualização disponível para o Secure Hub.
- Em dispositivos iOS, o Secure Mail solicita autorização após o período offline máximo expirar. O Secure Mail então muda para o Secure Hub, impedindo que você o use.

Secure Hub 20.9.0

Problemas conhecidos no Secure Hub 20.9.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 20.9.0

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

Secure Hub 20.7.5

Problemas conhecidos no Secure Hub 20.7.5

Em dispositivos de uso único de propriedade corporativa (COSU) executando Android 11, você não pode definir o Secure Hub como o iniciador padrão.

Problemas corrigidos no Secure Hub 20.7.5

- No Secure Hub para Android, o registro de dispositivos Android falha quando a fixação de certificado está ativada.
- No Secure Hub para Android, o recurso **Date Time Change** na política de Restrições não funciona em dispositivos Samsung.
- No Secure Hub para Android, a política de firewall não funciona em dispositivos Samsung que executam as versões 19.12.5 e posteriores.
- No Secure Hub para Android, você não consegue desinstalar aplicativos de **Meus aplicativos**.

Secure Hub 20.6.5

Não há problemas conhecidos ou corrigidos nesta versão

Secure Hub 20.3.0

Secure Hub para iOS

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 20.2.0

Secure Hub para iOS

Problemas conhecidos no Secure Hub 20.2.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 20.2.0

- No Secure Hub para iOS, o registro do Mobile Application Management (MAM) falha em alguns dispositivos iOS.
- No Secure Hub para iOS, os aplicativos estão sendo removidos aleatoriamente dos dispositivos.

Secure Hub 20.1.5

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 19.12.5

Problemas conhecidos no Secure Hub 19.12.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.12.5

Em dispositivos com iOS 13, os certificados de usuário para o XenMobile® Server são verificados e renovados na data de expiração real, em vez de depender do código de erro SSL para verificar a expiração do certificado de usuário.

Secure Hub 19.11.5

Problemas conhecidos no Secure Hub 19.11.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.11.5

No Secure Hub para iOS, o registro falha para aplicativos empacotados em MDX após desativar a entropia do usuário.

Secure Hub 19.10.5

Secure Hub para Android

Problemas conhecidos no Secure Hub 19.10.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.10.5

No Secure Hub para Android, não é possível instalar aplicativos corporativos em dispositivos que executam o Secure Hub versão 19.10.5 quando a política de Credenciais está configurada.

Secure Hub 19.10.0

Problemas conhecidos no Secure Hub 19.10.0

- No Secure Hub para Android, o registro de dispositivos Google Pixel 2 executando a versão 10 do Android no modo Proprietário do Dispositivo falha devido a uma falha de permissão.
- No Secure Hub para Android, em dispositivos Google Pixel executando a versão 10 do Android, o registro de dispositivos no modo Proprietário do Dispositivo falha devido a uma falha na validação da permissão de localização.

Problemas corrigidos no Secure Hub 19.10.0

Não há problemas corrigidos nesta versão.

Secure Hub 19.9.5

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 19.9.0

Problemas conhecidos no Secure Hub 19.9.0

No Secure Hub para Android 19.9.0 com Android Enterprise ativado, o seguinte problema ocorre em dispositivos Pixel 2: A política de Credenciais não é implantada com sucesso. Como resultado, os usuários não são solicitados a fornecer um certificado junto com uma senha e um certificado não é instalado. Como solução alternativa, os usuários podem atualizar manualmente suas políticas no aplicativo em **Preferências > Informações do Dispositivo**. A partir daí, eles pressionam **Atualizar política**, inserem suas credenciais e confirmam a mensagem de sucesso.

Problemas corrigidos no Secure Hub 19.9.0

Não há problemas corrigidos nesta versão.

Secure Hub 19.8.5

Não há problemas conhecidos ou corrigidos nesta versão.

Secure Hub 19.8.0

Problemas conhecidos no Secure Hub 19.8.0

No Secure Hub para iOS, quando você insere uma senha incorreta em um dispositivo compartilhado e toca em **Trocar usuário** para fazer login novamente, a mensagem **Aguarde** aparece indefinidamente.

Problemas corrigidos no Secure Hub 19.8.0

A rede de Gerenciamento de Dispositivos Móveis é roteada incorretamente quando conectada através da VPN completa.

Secure Hub 19.7.5

Problemas conhecidos no Secure Hub 19.7.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.7.5

- No Secure Hub para Android, os avisos para instalar clipes da web aparecem rapidamente, interferindo na configuração do PIN do Secure Hub.
- Em dispositivos Samsung Knox versão 3 e superiores, quando você registra o Secure Hub no modo Proprietário do Perfil e envia a política de **chave de licença MDM da Samsung** para a plataforma Android Enterprise, o comando **Redefinir Senha do Contêiner do Dispositivo** falha.
- O seguinte erro aparece no Secure Hub para iOS quando você tenta configurar um Aplicativo Público no modo MAM usando o novo URL do aplicativo da Apple Store: **Não foi possível carregar a Loja. Tente novamente.** Consulte a solução alternativa em <https://support.citrix.com/article/CTX256704>.

- No Secure Hub para Android, você não consegue instalar aplicativos MDX quando um túnel VPN completo é estabelecido.
- Quando ocorre um tempo limite de sessão em dispositivos Point Mobile PM80 executando o Secure Hub para Android no modo Dispositivos Compartilhados, você não consegue fazer login novamente.
- No Secure Hub para Android, você recebe o seguinte erro após instalar e iniciar aplicativos empacotados internamente: **A forma como seus dados são criptografados neste aplicativo mudou. Exclua este aplicativo e reinstale-o.**

Secure Hub 19.6.5

Problemas conhecidos no Secure Hub 19.6.5

Não há problemas conhecidos nesta versão

Problemas corrigidos no Secure Hub 19.6.5

- Em dispositivos iOS, o Secure Hub não carrega a loja quando há um failover de Global Server Load Balancing.
- No Secure Hub para Android, a política de Atualização falha. Como resultado, você não consegue implantar novas políticas de dispositivo.
- No Secure Hub para Android, as ações de registro ou política de Atualização em dispositivos Samsung S10 demoram muito.
- Em dispositivos Android, aplicativos não gerenciados perdem a conectividade quando o Secure Hub estabelece uma conexão VPN completa.

Secure Hub 19.5.5

Problemas conhecidos no Secure Hub 19.5.5

- No Secure Hub para Android, dispositivos no modo Corporate Owned Single Use (COSU) perdem a conectividade após alguns minutos de registro e não recebem notificações mesmo com o GCM ativado.
- Ao implantar a política de Localização em dispositivos, de uma só vez, para os modos Proprietário do Perfil e Proprietário do Dispositivo, a conta de usuário no modo Proprietário do Dispositivo é excluída. Esse problema ocorre durante o registro por NFC bump e quando o Endpoint Management está configurado no modo MDM.

Problemas corrigidos no Secure Hub 19.5.5

- A partir desta versão, o Secure Hub suporta apenas dispositivos com Android 5.0 e posterior.
- No Secure Hub para Android, registre um dispositivo no modo de proprietário do dispositivo e defina uma nova senha. O dispositivo não é bloqueado na primeira tentativa.

Secure Hub 19.5.0

Problemas conhecidos no Secure Hub 19.5.0

- Após o registro, os dispositivos OnePlus Android versão 7.1.1 e OnePlus 5T Android versão 9.0.3 exigem reinício manual do Secure Hub para que seja solicitado o PIN do Citrix.
- No Secure Hub para Android, os aplicativos necessários não são implantados em dispositivos Android, a menos que você atualize a política ou atualize a loja.

Problemas corrigidos no Secure Hub 19.5.0

- A partir desta versão, o Secure Hub suporta apenas dispositivos com Android 5.0 e posterior.
- No Secure Hub para Android, dispositivos Android 6.0 falham ao registrar se vários nomes alternativos de assunto estiverem presentes no certificado do servidor.
- No Secure Hub para Android, os aplicativos gerenciados não são desinstalados após o cancelamento do registro dos dispositivos.
- Em dispositivos Samsung S9, após os usuários atualizarem para o Android P, ocorre o seguinte problema: Ao alterar a senha do dispositivo via Endpoint Management, a senha no dispositivo não é alterada. Em vez disso, a tela fica preta e o console do Endpoint Management mostra um status de dispositivo bloqueado.

Secure Hub 19.4.5

Problemas conhecidos no Secure Hub 19.4.5

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.4.5

Em dispositivos iOS, ao clicar no link de registro do dispositivo, o nome da instância FQDN do Endpoint Management não é preenchido automaticamente no Secure Hub. A solicitação de registro do dispositivo falha.

Secure Hub 19.3.5

Problemas conhecidos no Secure Hub 19.3.5

Quando as notificações são enviadas do Secure Hub para iOS, a contagem do selo de notificação não é atualizada para o Secure Hub.

Problemas corrigidos no Secure Hub 19.3.5

- No Secure Hub para Android, ao registrar dispositivos compartilhados, implantar a política **Webclip** e adicionar aplicativos web e SaaS, a implantação é bem-sucedida. No entanto, essa implantação aparece como falha na tela **Inventário de aplicativos** no console do Citrix Endpoint Management.
- No Secure Hub para Android, quando os usuários fazem login com PIN seguro, um túnel VPN é estabelecido, mas o Secure Web não carrega nenhum site. No entanto, o site carrega conforme o esperado quando o Secure Web é fechado e reaberto.
- O Secure Mail para Android configurado com políticas do Microsoft Intune retorna uma tela em branco após a autenticação.
- No Secure Hub para Android, aplicativos que desativaram a criptografia estão tentando obter chaves de criptografia do Secure Hub.
- O Secure Mail para Android trava na inicialização quando a versão 5.0.4324.0 do Intune Company Portal está instalada.
- No Secure Hub para Android, você não consegue usar os aplicativos do sistema em dispositivos Android Enterprise de uso único de propriedade corporativa (COSU) executando o Android 7.1.1.
- No Secure Hub para Android, ao configurar vários aplicativos do Google Play como aplicativos obrigatórios e tentar registrar, você é solicitado a instalar o primeiro aplicativo. O prompt inicial é imediatamente seguido por outro prompt para instalar o segundo aplicativo e assim por diante.

Secure Hub 19.3.0

Problemas conhecidos no Secure Hub 19.3.0

- Em Secure Hub para Android, ao registrar dispositivos compartilhados, implantar a política **Webclip** e adicionar aplicativos web e SaaS, a implantação é bem-sucedida. No entanto, essa implantação aparece como falha na tela **Inventário de aplicativos** no console do Citrix Endpoint Management.

- Em dispositivos Android Enterprise, quando uma ação de bloqueio é definida para violação de cerca geográfica na política de Localização, o dispositivo solicita que você defina uma nova senha em vez de usar a senha gerada pelo sistema.

Problemas corrigidos no Secure Hub 19.3.0

O bloqueio remoto de dispositivos Android Enterprise totalmente gerenciados usando a ação de segurança Bloquear com senha pode falhar sem notificá-lo da falha. Para garantir que um dispositivo esteja bloqueado, defina Bloquear com senha duas vezes. O dispositivo é bloqueado com a segunda senha que você definir.

Secure Hub 19.2.0

Problemas conhecidos no Secure Hub 19.2.0

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Hub 19.2.0

- No Secure Hub para iOS, a seguinte mensagem de falha de handshake SSL aparece repetidamente quando os usuários saem da loja do Secure Hub: A solicitação de rede para buscar aplicativos expirou do Servidor.
- A política de dispositivo de Arquivos para Android Enterprise não é implantada em dispositivos Android no modo de perfil de trabalho.
- No Secure Hub para Android, a autorização de login para um novo usuário leva muito tempo em dispositivos compartilhados. Ao sair como um usuário registrado e tentar fazer login como um novo usuário, o Secure Hub continua carregando até que você reinicie o dispositivo.
- No Secure Hub para Android, os clientes da nuvem não conseguem registrar dispositivos Android Enterprise com um provedor de identidade externo.
- No Secure Hub para Android, quando você está no modo Corporate Owned Single Use (COSU), os ícones dos aplicativos ficam sobrepostos no Secure Hub.
- No Secure Hub para Android, quando o certificate pinning está ativado para sua configuração existente, a autenticação falha e retorna à tela do usuário iniciante quando o certificado possui vários Nomes Alternativos de Assunto.

Secure Hub 19.1.5

Problemas conhecidos no Secure Hub 19.1.5

- No Secure Hub para Android, ao atualizar a senha devido a uma alteração na política de senha, os aplicativos com selo não aparecem em dispositivos Samsung Galaxy S8.
- No Secure Hub para Android, a política de dispositivo de Arquivos do Android Enterprise não é implantada em dispositivos no modo de perfil de trabalho.

Problemas corrigidos no Secure Hub 19.1.5

- No Secure Hub para Android, quando os usuários fazem login com o PIN Seguro, um túnel VPN é estabelecido, mas o Secure Web não carrega nenhum site. No entanto, o site carrega conforme o esperado quando o Secure Web é fechado e reaberto.
- No Secure Hub para Android, ao fazer login com o PIN Seguro, um túnel VPN é estabelecido, mas o Secure Web não carrega nenhum site. No entanto, o site carrega conforme o esperado quando o Secure Web é fechado e reaberto.
- No Secure Hub para Android, ao tentar capturar logs do aplicativo interno chamado TechXpert, o Secure Hub reinicia e solicita que você se reautentique.

Secure Hub 19.1.0

Problemas conhecidos no Secure Hub 19.1.0

No Secure Hub para iOS, ao implantar aplicativos MDX e web ou SaaS, eles aparecem na tela **Meus Aplicativos**. Ao tocar em **Mais**, um pop-up aparece com as opções **Excluir** e **Cancelar** que têm o formato da antiga identidade visual da interface do usuário.

Problemas corrigidos no Secure Hub 18.12.0

- Em dispositivos Samsung Knox registrados para Android For Work, quando a política de senha é configurada para expirar em um ou dois dias, a mensagem **Senha Expirada** aparece repetidamente.
- Não é possível registrar dispositivos OnePlus 5T para Android Enterprise usando o método de registro por código QR.

Secure Hub 18.11.0

Problemas corrigidos no Secure Hub 18.11.0

- Você não consegue realizar o logon único em dispositivos Android registrados no modo Dispositivo Compartilhado. O seguinte erro aparece: **Suas credenciais corporativas não podem ser recuperadas neste momento. O login manual no ShareFile está bloqueado devido à política do administrador.**
- Você não pode editar os níveis de volume do Android em dispositivos de propriedade corporativa e de uso único (COSU).

Secure Hub 18.10.5

Problemas corrigidos no Secure Hub 18.10.5

- Se você tiver o modo FIPS ativado no XenMobile Server, depois que os usuários atualizarem o Secure Hub para iOS para a versão 18.10.5, uma mensagem de erro relacionada à criptografia aparecerá quando os usuários abrirem os aplicativos.

Versões do Secure Hub de 10.8.25 a 18.10.6

Problemas corrigidos nas versões do Secure Hub de 10.8.25 a 18.10.6

- As versões do Secure Hub de 10.8.25 a 18.10.6 (Android) não incluem problemas conhecidos. Os seguintes problemas foram corrigidos no Secure Hub. A lista inclui problemas com o MDX que afetam o Secure Hub.

Secure Hub 18.10.0

Problemas corrigidos no Secure Hub 18.10.0

- Se a política MVPN estiver desativada no console EMS, o Secure Hub exibirá uma tela em branco ao tentar abrir aplicativos gerenciados pelo Intune.

Secure Hub 10.8.60

Problemas corrigidos no Secure Hub 10.8.60

- Em dispositivos Samsung Galaxy Tab Active 2 SM-T395, a ação de segurança Limpeza Completa falha para o Secure Hub para Android quando os administradores definem uma restrição de Desativar Redefinição de Fábrica no XenMobile.
- O Secure Hub para Android deixa de responder durante o registro de dispositivos quando a política de VPN está configurada e o aplicativo Citrix SSO não está instalado no dispositivo. Ele volta a responder se você tocar no botão **Voltar** ou reiniciar o aplicativo.
- O Secure Hub para Android falha durante o registro no modo Proprietário do Dispositivo em um ambiente Android Enterprise.
- Depois que os usuários inserem um PIN válido para o Secure Hub para iOS, o Secure Hub solicita o PIN repetidamente.
- O Secure Hub para Android falha durante o registro no modo Proprietário do Perfil em um ambiente Android Enterprise.
- O uso do Android Enterprise no Secure Hub para Android instala o Google Chrome por padrão.
- A atualização do Secure Hub para iOS para a versão 10.8.55 não permite registros de dispositivos iOS existentes ou novos.

Secure Hub 10.8.55

Problemas corrigidos no Secure Hub 10.8.55

- Os usuários não conseguem fazer login no Secure Hub para se registrar em contas do Android for Work quando as credenciais do G Suite diferem das credenciais no Endpoint Management.

Problemas corrigidos relacionados ao MDX na versão 10.8.55

- Os aplicativos corporativos podem apresentar problemas de conectividade com recursos internos quando o modo VPN preferencial está definido como SecureBrowse.
- Aplicativos que especificam `android.support.multidex.MultiDexApplication` ou `android.app.Application` como sua classe de aplicativo não conseguem se conectar a redes internas no modo Tunneled – Web SSO.
- Em dispositivos Android, vários certificados estão sendo gerados e os certificados estão sendo revogados antes da data de expiração.

Secure Hub 10.8.55

Problema conhecido no Secure Hub 10.8.55

- Após remover sua conta do Secure Hub do seu dispositivo, o novo registro MDM falha.

Secure Hub 10.8.50

Problema conhecido no Secure Hub 10.8.50

- No Secure Hub para Android, os usuários não conseguem adicionar um atalho de link da web.

Secure Hub 10.8.35

Problemas corrigidos no Secure Hub 10.8.35

- No Android O, os atalhos criados por políticas não aparecem na tela inicial do dispositivo. Esse comportamento é intencional no Android O.
- No Android, o Secure Hub não abre em tablets Samsung após um período de inatividade.
- No Secure Hub para Android, não é possível implantar a política de push em dispositivos Samsung Knox.
- No Secure Hub para iOS, ocasionalmente ocorre o seguinte problema: Depois que os usuários alteram a senha do Active Directory, eles precisam continuar inserindo o PIN em um loop.

Secure Hub 10.8.25

Problemas corrigidos no Secure Hub 10.8.25

- Para aplicativos Cordova iOS de terceiros empacotados com o MDX Toolkit versão 10.7.20, uma tela preta aparece em vez de uma tela de PIN depois que você habilita a política **Obscure screen contents**.
- Em dispositivos Zebra T51 executando Android 7, os usuários não conseguem instalar o aplicativo Citrix Launcher.

Secure Hub 10.8.20

Problemas corrigidos no Secure Hub 10.8.20

- Depois que os usuários atualizam seus dispositivos Android para a versão 8 (Oreo): Eles não conseguem instalar aplicativos corporativos ou .apk da loja de aplicativos que você implanta do Endpoint Management. Mesmo quando eles ativam a instalação de aplicativos de terceiros, o problema persiste. O problema não se limita a dispositivos Samsung.

Secure Hub 10.8.15

Problemas corrigidos no Secure Hub 10.8.15

- O Secure Hub para Android trava ao buscar detalhes de localização em dispositivos que executam o Android O.

Secure Hub 10.8.10

Problemas corrigidos no Secure Hub 10.8.10

- Em dispositivos Android, quando vários aplicativos não são instalados automaticamente ou os usuários não clicam em **Instalar** por conta própria, os aplicativos continuam sendo baixados. Como resultado, ocorre alto uso de dados.
- Em dispositivos com Android 7 ou posterior: Ao enviar uma ação de segurança de bloqueio com uma senha para o dispositivo a partir do XenMobile Server, o dispositivo é bloqueado. No entanto, a senha do dispositivo não muda se os usuários tiverem uma senha de tela de bloqueio existente. Os usuários podem usar a senha original para desbloquear o dispositivo.

Atualização do Secure Hub para iOS em March 19, 2018: A versão 10.8.6 do Secure Hub para iOS está disponível para corrigir um problema com a política de aplicativos VPP.

Secure Hub para Android e iOS - Prévia

Aguarde os novos recursos e problemas resolvidos na próxima versão.

Para obter mais informações sobre a versão atual, consulte [O que há de novo no Secure Hub](#).

Gerenciamento de sinalizadores de recursos

Os administradores podem gerenciar sinalizadores de recursos para acessar recursos de visualização e controlar dinamicamente os recursos em produção. Para garantir o funcionamento ideal dos recursos que estão sob sinalizadores de recursos, você precisa habilitar o tráfego para a URL `features.netscalergateway.net`. Para obter mais informações, consulte [Gerenciamento de sinalizadores de recursos](#).

Cenários de solicitação de autenticação

Vários cenários solicitam que os usuários autenticar com o Secure Hub inserindo suas credenciais em seus dispositivos.

Os cenários mudam dependendo destes fatores:

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

Além disso, o tipo de credenciais que os usuários inserem, como a senha do Active Directory, PIN ou senha Citrix, senha de uso único, autenticação por impressão digital (conhecida como Touch ID no iOS), que também mudam com base no tipo de autenticação e na frequência da autenticação.

Vamos começar com os cenários que resultam em uma solicitação de autenticação.

- **Reinicialização do dispositivo:** Quando os usuários reiniciam seus dispositivos, eles devem se reautenticar com o Secure Hub.
- **Inatividade offline (tempo limite):** Com a política MDX de Senha do Aplicativo habilitada (por padrão), a propriedade de cliente do Endpoint Management chamada Temporizador de Inatividade entra em ação. O Temporizador de Inatividade limita o tempo que pode passar sem atividade do usuário em qualquer um dos aplicativos que usam o contêiner seguro.

Quando o Temporizador de Inatividade expira, os usuários devem se reautenticar no contêiner seguro no dispositivo. Por exemplo, quando os usuários largam seus dispositivos e se afastam, e o Temporizador de Inatividade expirou, outra pessoa não pode pegar o dispositivo e acessar dados confidenciais dentro do contêiner. Você define a propriedade de cliente **Temporizador de Inatividade** no console do Endpoint Management. O padrão é 15 minutos. A combinação da Senha do Aplicativo definida como **ATIVADA** e a propriedade de cliente Temporizador de Inatividade é responsável pelos cenários de solicitação de autenticação provavelmente mais comuns.

- **Sair do Secure Hub:** Quando os usuários saem do Secure Hub, eles precisam se reautenticar na próxima vez que acessarem o Secure Hub ou qualquer aplicativo MDX,

quando o aplicativo exigir uma senha, conforme determinado pela política MDX de Senha do Aplicativo e pelo status do Temporizador de Inatividade.

- **Período máximo offline:** Este cenário é específico para aplicativos individuais porque é impulsionado por uma política MDX por aplicativo. A política MDX de Período máximo offline tem uma configuração padrão de 3 dias. Se o período de tempo para um aplicativo ser executado sem autenticação online com o Secure Hub expirar, é necessário um check-in com o Endpoint Management para confirmar o direito ao aplicativo e atualizar as políticas. Quando este check-in ocorre, o aplicativo aciona o Secure Hub para uma autenticação online. Os usuários devem se reautenticar antes de poderem acessar o aplicativo MDX.

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

- O Período de sondagem ativa é o intervalo durante o qual os aplicativos proteger com o Endpoint Management para realizar ações de segurança, como bloqueio e limpeza de aplicativos. Além disso, o aplicativo também verifica se há políticas de aplicativo atualizadas.
- Após uma verificação bem-sucedida de políticas por meio da política de Período de sondagem ativa, o temporizador de Período máximo offline é redefinido e começa a contagem regressiva novamente.

Ambos os check-ins com o Endpoint Management, para o período de pesquisa ativa e o vencimento do período offline máximo, exigem um token Citrix Gateway válido no dispositivo. Se o dispositivo tiver um token Citrix Gateway válido, o aplicativo recupera novas políticas do Endpoint Management sem qualquer interrupção para os usuários. Se o aplicativo precisar de um token Citrix Gateway, ocorre uma alternância para o Secure Hub, e os usuários veem um prompt de autenticação no Secure Hub.

Em dispositivos Android, as telas de atividade do Secure Hub 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 desloca o aplicativo atual.

Depois que os usuários inserem suas credenciais, o Secure Hub retorna ao aplicativo original. Se, neste caso, você permitir credenciais de Active Directory em cache ou tiver um certificado de cliente configurado, os usuários podem inserir um PIN, senha ou autenticação por impressão digital. Caso contrário, os usuários devem inserir suas credenciais completas do Active Directory.

O token do Citrix ADC pode se tornar inválido devido à inatividade da sessão do Citrix Gateway ou a uma política de tempo limite de sessão forçada, conforme discutido na lista a seguir de políticas do Citrix Gateway. Quando os usuários fazem login no Secure Hub novamente, eles podem continuar executando o aplicativo.

- **Políticas de sessão do Citrix Gateway:** Duas políticas do Citrix Gateway também afetam quando os usuários são solicitados a autenticar. Nesses casos, eles autenticar para criar uma sessão online com o Citrix ADC para se conectar ao Endpoint Management.
 - **Tempo limite da sessão:** A sessão do Citrix ADC para o Endpoint Management é desconectada se nenhuma atividade de rede ocorrer durante o período definido. O padrão é 30 minutos. No entanto, se você usar o assistente do Citrix Gateway para configurar a política, o padrão será 1440 minutos. Os usuários veem um prompt de autenticação para se reconectar à sua rede corporativa.
 - **Tempo limite forçado:** Se **Ativado**, a sessão do Citrix ADC para o Endpoint Management é desconectada após o período de tempo limite forçado expirar. O tempo limite forçado torna a reautenticação obrigatória após um período definido. Os usuários verão então um prompt de autenticação para se reconectar à sua rede corporativa no próximo uso. O padrão é **Desativado**. No entanto, se você usar o assistente do Citrix Gateway para configurar a política, o padrão será 1440 minutos.

Tipos de credenciais

A seção anterior discutiu quando os usuários são solicitados a autenticar. Esta seção discute os tipos de credenciais que eles devem inserir. A autenticação é necessária por meio de vários métodos de autenticação para obter acesso a dados criptografados no dispositivo. Para desbloquear inicialmente o dispositivo, você desbloqueia o *contêiner primário*. Depois que isso ocorre e o contêiner é novamente protegido, para obter acesso novamente, você desbloqueia um *contêiner secundário*.

Nota:

O termo *aplicativo gerenciado* refere-se a um aplicativo empacotado pelo MDX Toolkit, no qual você deixou a política MDX de Código de Acesso do Aplicativo habilitada por padrão e está usando a propriedade de cliente Inactivity Timer.

As circunstâncias que determinam os tipos de credenciais são as seguintes:

- **Desbloqueio do contêiner primário:** Uma senha do Active Directory, PIN ou código de acesso Citrix, senha de uso único, Touch ID ou ID de impressão digital são necessários para desbloquear o contêiner primário.
 - No iOS, quando os usuários abrem o Secure Hub ou um aplicativo gerenciado pela primeira vez após a instalação do aplicativo no dispositivo.

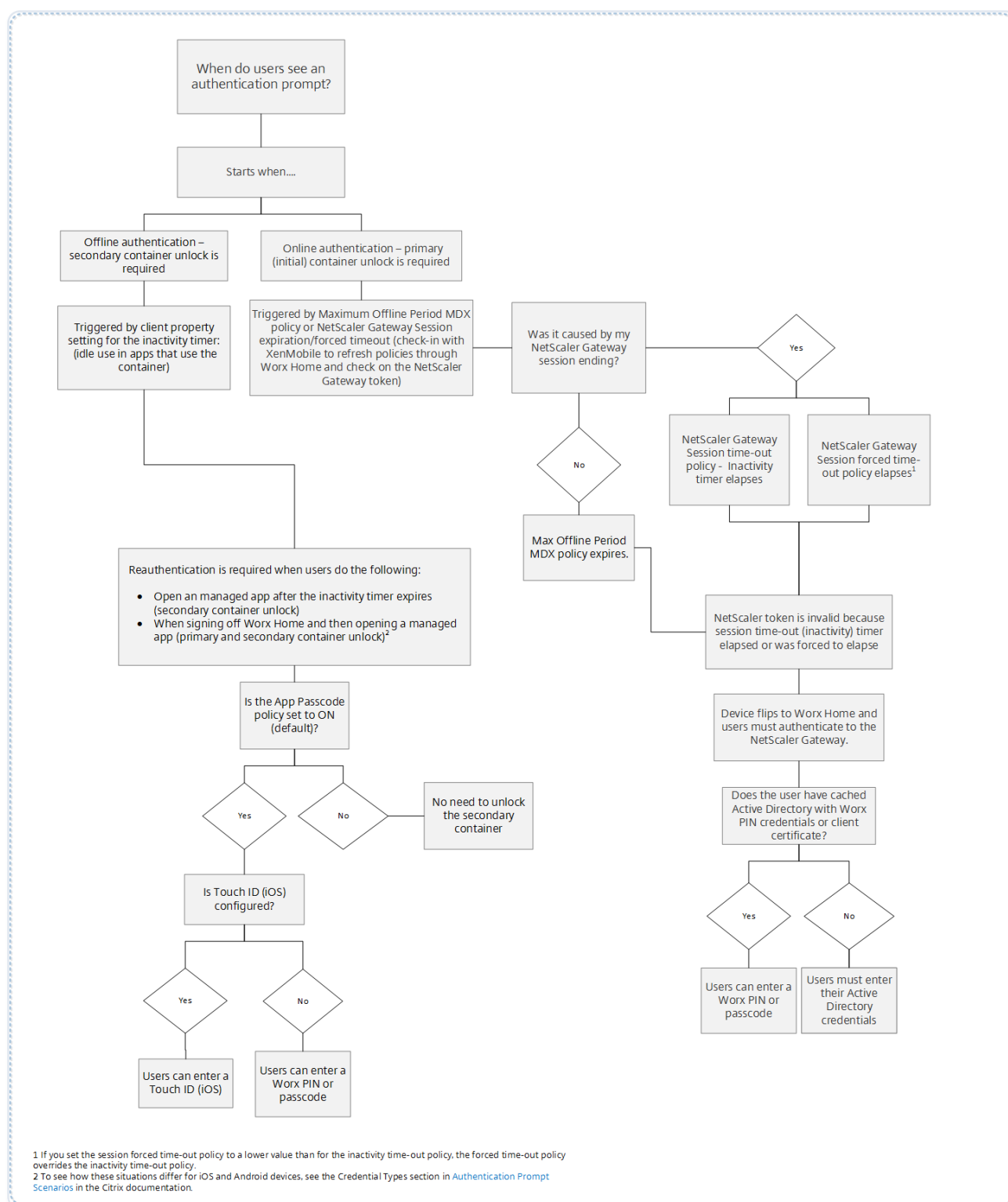
- No iOS, quando os usuários reiniciam um dispositivo e, em seguida, abrem o Secure Hub.
 - No Android, quando os usuários abrem um aplicativo gerenciado se o Secure Hub não estiver em execução.
 - No Android, quando os usuários reiniciam o Secure Hub por qualquer motivo, incluindo a reinicialização do dispositivo.
- **Desbloqueio do contêiner secundário:** Autenticação por impressão digital (se configurada), um PIN ou senha Citrix, ou credenciais do Active Directory, para desbloquear o contêiner secundário.
 - Quando os usuários abrem um aplicativo gerenciado após o tempo limite de inatividade expirar.
 - Quando os usuários saem do Secure Hub e depois abrem um aplicativo gerenciado.

As credenciais do Active Directory são necessárias para qualquer uma das circunstâncias de desbloqueio do contêiner quando as seguintes condições são verdadeiras:

- Quando os usuários alteram a senha associada à sua conta corporativa.
- Quando você não definiu as propriedades do cliente no console do Endpoint Management para habilitar o PIN Citrix: `ENABLE_PASSCODE_AUTH` e `ENABLE_PASSWORD_CACHING`.
- Quando a sessão do NetScaler® Gateway termina, o que ocorre nas seguintes circunstâncias: quando o tempo limite da sessão ou o temporizador da política de tempo limite forçado expira, se o dispositivo não armazena as credenciais em cache ou não possui um certificado de cliente.

Quando a autenticação por impressão digital está habilitada, os usuários podem fazer login usando uma impressão digital quando a autenticação offline é necessária devido à inatividade do aplicativo. Os usuários ainda precisam inserir um PIN ao fazer login no Secure Hub pela primeira vez e ao reiniciar o dispositivo. Para obter informações sobre como habilitar a autenticação por impressão digital, consulte [Autenticação por impressão digital ou Touch ID](#).

O fluxograma a seguir resume o fluxo de decisão que determina quais credenciais um usuário deve inserir quando solicitado a autenticar.



Sobre as inversões de tela do Secure Hub

Outra situação a ser observada é quando é necessária uma inversão de um aplicativo para o Secure Hub e depois de volta para um aplicativo. A inversão exibe uma notificação que os usuários devem reconhecer. A autenticação não é necessária quando isso ocorre. A situação ocorre após um check-in com o Endpoint Management, conforme especificado pelas políticas

MDX de Período máximo offline e Período de sondagem ativa, e o Endpoint Management detecta políticas atualizadas que precisam ser enviadas ao dispositivo através do Secure Hub.

Complexidade da senha para a senha do dispositivo (Android 12+)

A complexidade do código de acesso é preferível a um requisito de senha personalizado. O nível de complexidade do código de acesso é um dos níveis predefinidos. Assim, o usuário final não consegue definir uma senha com um nível de complexidade inferior.

A complexidade do código de acesso para dispositivos no Android 12+ é a seguinte:

- **Aplicar complexidade do código de acesso:** Requer uma senha com um nível de complexidade definido pela plataforma, em vez de um requisito de senha personalizado. Somente para dispositivos no Android 12+ e usando o Secure Hub 22.9 ou posterior.
- **Nível de complexidade:** Níveis predefinidos de complexidade de senha.
 - **Nenhum:** Nenhuma senha é necessária.
 - **Baixo:** As senhas podem ser:
 - Um padrão
 - Um PIN com um mínimo de quatro números
 - **Médio:** As senhas podem ser:
 - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234) e um mínimo de quatro números
 - Alfabético com um mínimo de quatro caracteres
 - Alfanumérico com um mínimo de quatro caracteres
 - **Alto:** As senhas podem ser:
 - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234) e um mínimo de oito números
 - Alfabético com um mínimo de seis caracteres
 - Alfanumérico com um mínimo de seis caracteres

OBSERVAÇÕES:

- Para dispositivos BYOD, as configurações de senha, como Comprimento mínimo, Caracteres obrigatórios, Reconhecimento biométrico e Regras avançadas, não são aplicáveis no Android 12+. Use a complexidade da senha em vez disso.
- Se a complexidade da senha para o perfil de trabalho estiver ativada, a complexidade da senha para o lado do dispositivo também deverá ser ativada.

Para obter mais informações, consulte [Configurações do Android Enterprise](#) na documentação do Citrix Endpoint Management.

Registrando dispositivos usando credenciais derivadas

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 (PIV) ou um Cartão de Acesso Comum (CAC).

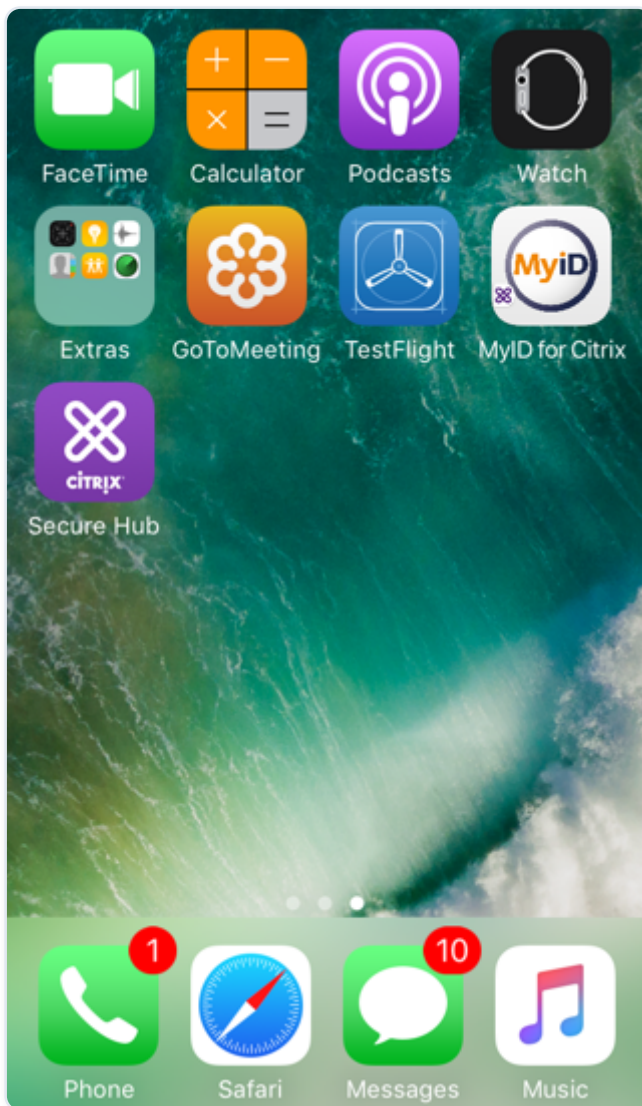
As credenciais derivadas são um certificado de registro que contém o identificador do usuário, como UPN. O Endpoint Management armazena as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

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

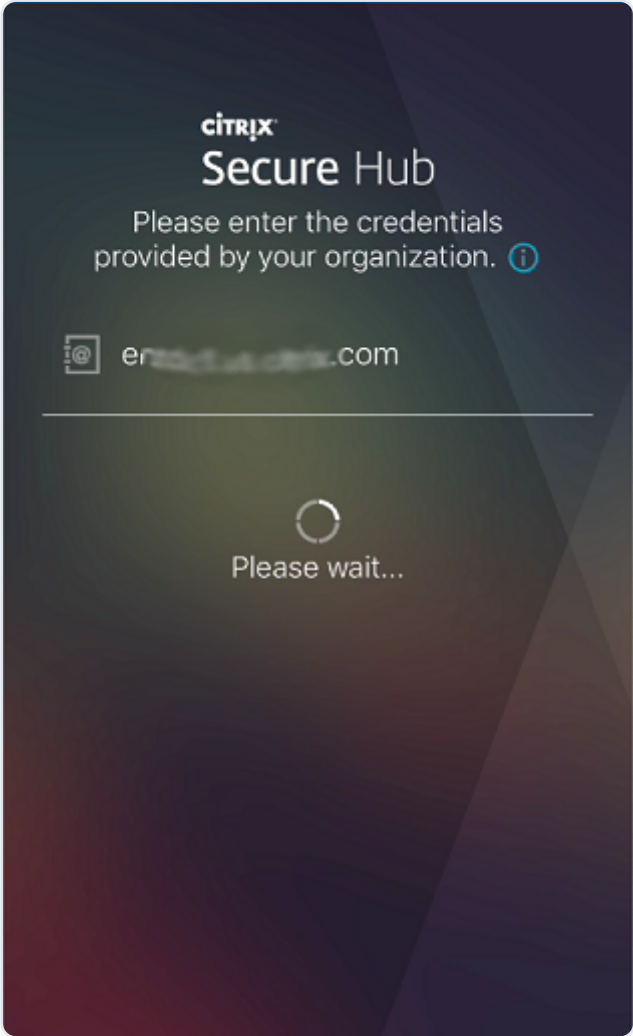
Etapas de registro de dispositivo ao usar credenciais derivadas

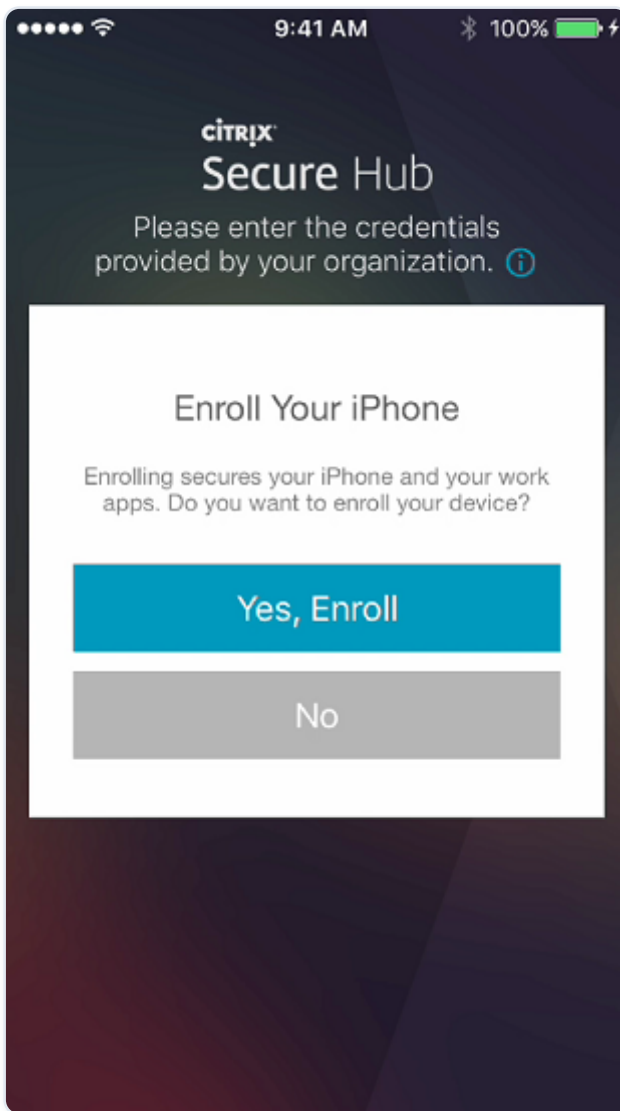
O registro exige que os usuários insiram seu cartão inteligente em um leitor conectado ao seu desktop.

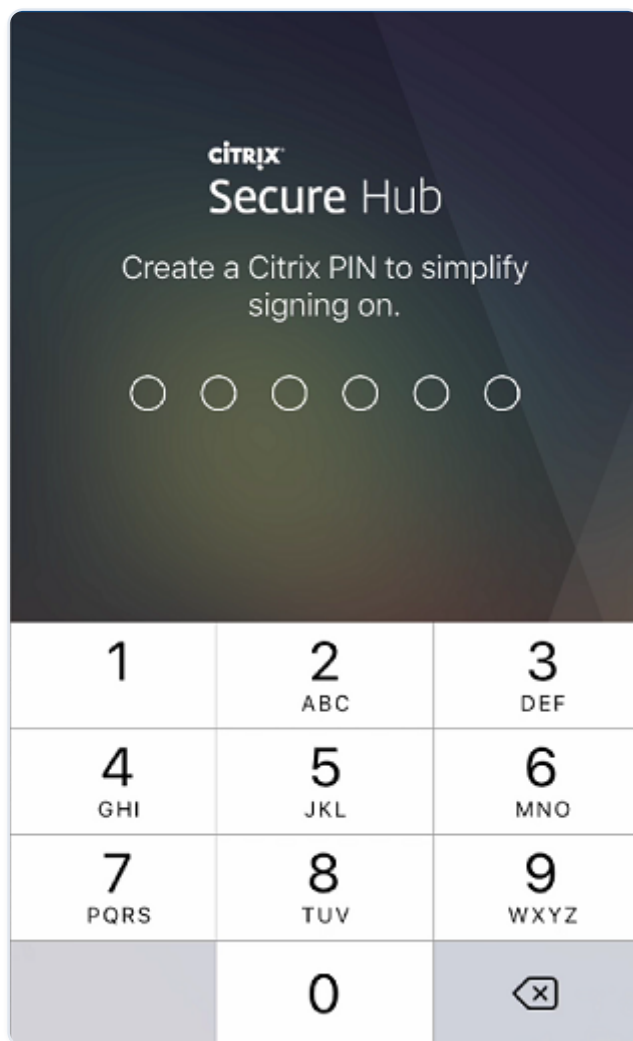
1. O usuário instala o Secure Hub e o aplicativo do seu provedor de credenciais derivadas. Neste exemplo, o aplicativo do provedor de identidade é o Intercede MyID Identity Agent.



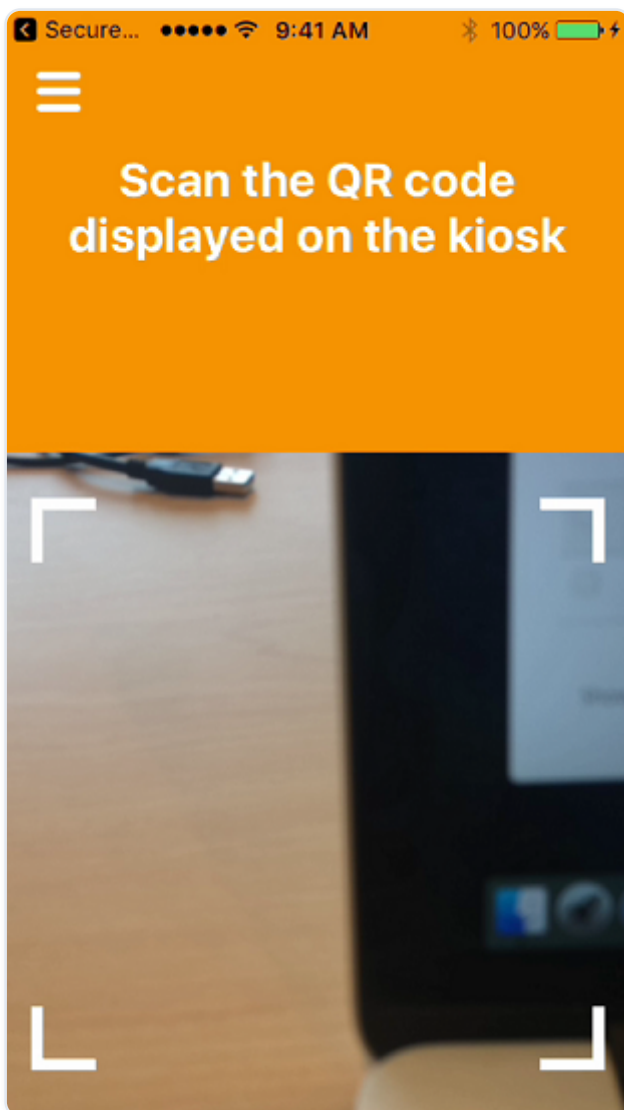
2. O usuário inicia o Secure Hub. Quando solicitado, o usuário digita o nome de domínio totalmente qualificado (FQDN) do Endpoint Management e clica em **Avançar**. O registro no Secure Hub é iniciado. Se o Endpoint Management oferecer suporte a credenciais derivadas, o Secure Hub solicitará que o usuário crie um PIN Citrix.







3. O usuário segue as instruções para ativar sua credencial inteligente. Uma tela inicial aparece, seguida por um prompt para escanear um código QR.



4. O usuário insere seu cartão no leitor de cartão inteligente conectado ao seu desktop. O aplicativo de desktop então exibe um código QR e solicita que o usuário escaneie o código usando seu dispositivo móvel.

Imagem do prompt de digitalização(/en-us/mobile-productivity-apps/media/derived-credentials-kiosk2.png)

O usuário insere o PIN do Secure Hub quando solicitado.

Imagem do prompt de PIN(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-pin.png)

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

Para visualizar informações do dispositivo no console do Endpoint Management, faça um dos seguintes:

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

Configurar dica através do console do Citrix Endpoint Management™

Um administrador pode configurar uma dica na página de login do Secure Hub para dispositivos com o modo de registro definido como **Dois Fatores**. Você pode configurar uma dica de uma das seguintes maneiras:

- Configurar dica como texto
- Configurar texto da dica com link de página da web

Configurar dica como texto

Para configurar um texto de dica, execute as seguintes etapas:

1. Faça login no console do Citrix Endpoint Management usando credenciais de administrador.
2. navegar para **Configurações > Propriedades do Cliente**, e clique em **Adicionar Nova Propriedade do Cliente**.
3. Na lista suspensa **Chave**, selecione **Chave Personalizada**.
4. No campo **Chave**, insira **enrollment.twofactor.token.hint**.
5. No campo **Valor**, você pode fornecer um texto que será exibido como uma dica na página de login. A dica orienta os usuários a localizar o PIN para autenticação de dois fatores.
6. No campo **Nome**, insira **enrollment.twofactor.token.hint**.
7. No campo **Descrição**, você pode fornecer observações sobre a dica que configurou, o que será útil para sua referência futura.

Settings > Client Properties > Add New Client Property

Add New Client Property

Key	Custom Key
Key *	enrollment.twofactor.token.hint
Value *	Please check your mail for security token/PIN
Name *	enrollment.twofactor.token.hint
Description *	Please check your mail for security token/PIN. This is where to get your security token/PIN.

8. Clique em **Salvar**.

O texto da dica aparece na página de login assim que você conclui a configuração.

Configurar texto da dica com link de página da web

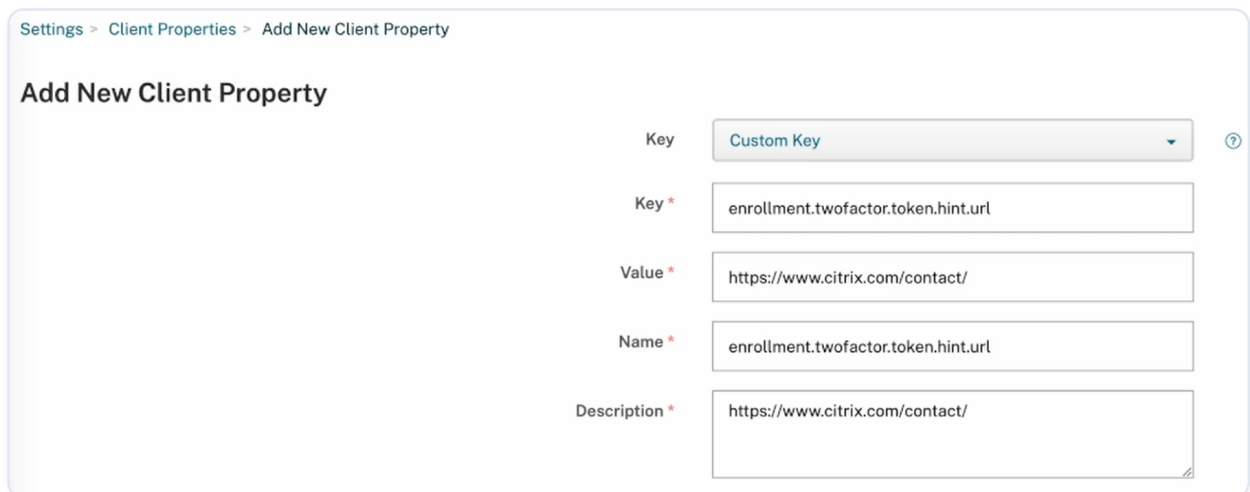
Você pode configurar uma página da web com informações detalhadas sobre como acessar o PIN. Posteriormente, forneça o link da página da web como um hiperlink no texto da dica. Quando um usuário clica na dica na página de login, o Secure Hub abre um navegador incorporado e navega para a página da web que você já configurou.

Para configurar o texto da dica com um link de página da web, primeiro, você precisa configurar o texto da dica conforme explicado no artigo [Configurar dica como texto](#). Uma vez concluído, continue com as seguintes etapas:

1. Faça login no console do Citrix Endpoint Management usando credenciais de administrador.
2. navegar para **Settings > Client Properties** e clique em **Add New Client Property**.
3. Na lista suspensa **Key**, selecione **Custom Key**.
4. No campo **Key**, insira **enrollment.twofactor.token.hint.url**.
5. No campo **Value**, insira o URL da página da web que você configurou.
6. No campo **Name**, insira **enrollment.twofactor.token.hint.url**.
7. No campo **Description**, você pode fornecer observações sobre a dica que configurou, o que será útil para sua referência futura.

NOTA:

Quando um usuário clica no link da dica, uma página da web aparece em um navegador incorporado.



Settings > Client Properties > Add New Client Property

Add New Client Property

Key	Custom Key
Key *	enrollment.twofactor.token.hint.url
Value *	https://www.citrix.com/contact/
Name *	enrollment.twofactor.token.hint.url
Description *	https://www.citrix.com/contact/

8. Clique em **Salvar**.

Após concluir a configuração, o texto de dica com o link da página da web aparece na página de login.

citrix | Secure Hub

Please enter the credentials provided by your organization.

 Username Password Pin[Where to get your enrollment token?](#)

Back

Next

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

Verificação de conformidade em dispositivos Android (Prévia Técnica)

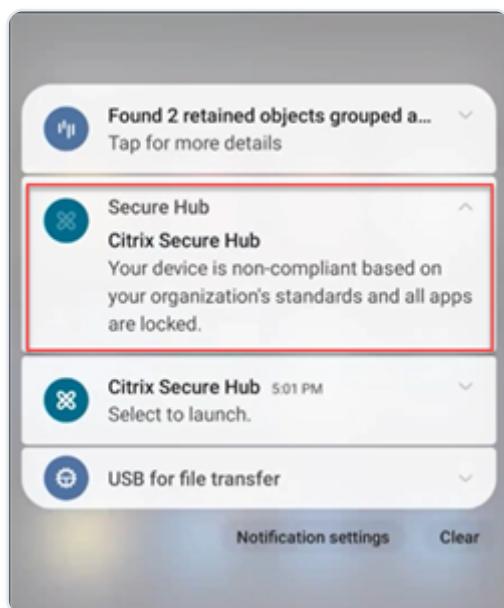
NOTA:

Este recurso é aplicável a dispositivos Android registrados no modo *Proprietário do Dispositivo*.

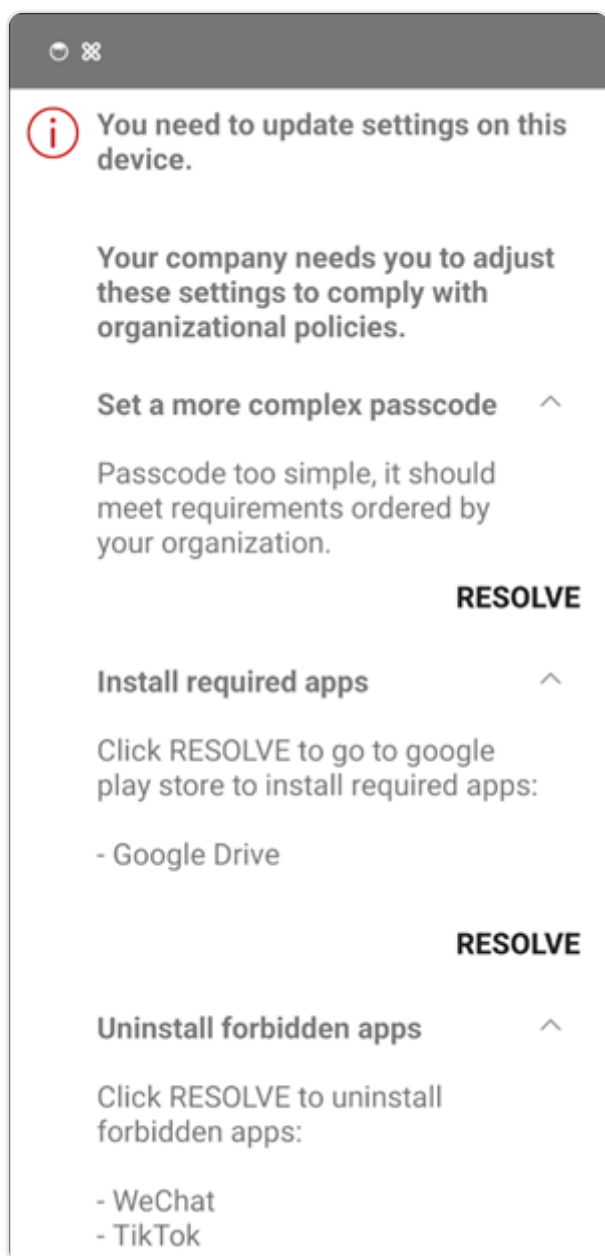
A partir do lançamento do Secure Hub para Android 24.8.0, o Secure Hub verifica a conformidade dos dispositivos Android com as políticas configuradas pelo administrador através do Citrix Endpoint Management. Esta verificação de conformidade inclui:

- Garantir a força da senha do dispositivo
- Verificar a instalação de aplicativos obrigatórios
- Confirmar a remoção de aplicativos proibidos

Quando um dispositivo não está em conformidade, a seguinte notificação aparece no dispositivo do usuário.



Quando um dispositivo não está em conformidade, os usuários veem a seguinte mensagem ao abrir o Secure Hub.



Os usuários podem clicar no botão **RESOLVER** para resolver os respectivos problemas.

NOTA:

- Os aplicativos permanecem bloqueados até que a conformidade seja atendida.
- Você tem a opção de desbloquear aplicativos específicos adicionando-os à lista de aplicativos a serem desbloqueados. Para obter mais informações, consulte [Aplicação de Conformidade para Dispositivos Android \(Prévia Técnica\)](#).

Para obter mais informações sobre como configurar políticas e verificações de conformidade, consulte [Aplicação de Conformidade para Dispositivos Android \(Technical Preview\)](#) na documentação do produto Citrix Endpoint Management.