



Aplicativos de produtividade móvel

Contents

Linha do tempo de lançamento de aplicativos de produtividade móvel	21
Sobre o processo de lançamento faseado do Secure Mail e Secure Web	21
Pré-requisitos para o gerenciamento de feature flags	21
Suporte para aplicativos de produtividade móvel	23
Sistemas operacionais suportados	24
Outras considerações e limitações	24
Secure Mail	25
Secure Web	25
QuickEdit	25
Citrix Content Collaboration™ para Endpoint Management	25
ShareConnect	25
Citrix Secure Notes e Citrix Secure Tasks	26
Tarefas e considerações do administrador	27
Gerenciamento de sinalizadores de recursos	27
Habilitar tráfego para as seguintes URLs	27
Criar uma lista de permissões por domínio	27
Listar endereços IP em uma lista de permissões	28
Requisitos de sistema do LaunchDarkly	28
Lojas de aplicativos compatíveis	28
Habilitando a distribuição de aplicativos da loja pública	29
Notificações push da Apple	30
FAQ da App Store pública	30
Android	30
iOS	31
Políticas MDX para aplicativos de produtividade móvel	34
Modo duplo no Secure Mail para Android	34

Pré-requisitos	35
Limitações	35
Conexões de usuário à rede interna	36
Restrições de acesso à rede	37
Propriedades do cliente do Endpoint Management	37
Cache de senha do usuário	37
Temporizador de inatividade	38
Autenticação por PIN Citrix	38
Autenticação por impressão digital ou Touch ID	38
Requisitos de autenticação por impressão digital	39
Para configurar a autenticação por impressão digital	39
Google Analytics	40
Desativar o Google Analytics	40
Políticas MDX para aplicativos de produtividade móvel em um relance	40
Autenticação	40
Senha do dispositivo	40
Senha do aplicativo	41
Período de carência de sessão online obrigatória (minutos)	41
Período offline máximo	41
Citrix Gateway alternativo	41
Segurança do dispositivo	42
Bloquear dispositivos com jailbreak ou root	42
Exigir bloqueio do dispositivo	42
Requisitos de rede	42
Exigir Wi-Fi	42
Redes Wi-Fi Permitidas	42
Acesso diverso	42
Período de carência para atualização do aplicativo (horas)	42

Desativar atualização obrigatória	43
Apagar dados do aplicativo ao bloquear	43
Período de sondagem ativa (minutos)	43
Criptografia	43
Tipo de criptografia	43
Comportamento de dispositivo não compatível	44
Habilitar criptografia MDX	44
Chaves de criptografia	44
Criptografia de arquivo privado	44
Exclusões de criptografia de arquivo privado	45
Limites de acesso para arquivos públicos	45
Criptografia de arquivo público	45
Exclusões de criptografia de arquivo público	45
Migração de arquivo público	45
Habilitar criptografia	46
Exclusões de criptografia de banco de dados	46
Exclusões de criptografia de arquivo	46
Interação do aplicativo	46
Grupo de Segurança	46
Recortar e copiar	47
Colar	47
Troca de documentos (Abrir em)	47
Domínios de URL excluídos da filtragem	47
Domínios da Web Segura permitidos	47
Nível de segurança da conexão	47
Troca de documentos de entrada (Abrir em)	48
Lista de exceção de Abertura Restrita	48
Esquemas de URL de aplicativo	48

URLs permitidas	48
Notificações de logoff explícito	48
Interação do aplicativo (URL de saída)	49
Domínios excluídos da filtragem de URL	49
URLs permitidas	49
Domínios Web Seguros Permitidos	49
Restrições de aplicativo	49
Bloquear câmera	49
Bloquear galeria	49
Bloquear Biblioteca de Fotos	49
Bloquear gravação de microfone	50
Bloquear ditado	50
Bloquear serviços de localização	50
Bloquear composição de SMS	50
Bloquear captura de tela	50
Bloquear sensor do dispositivo	50
Bloquear NFC	51
Bloquear iCloud	51
Bloquear Pesquisa	51
Bloquear backup de arquivo	51
Bloquear AirPrint	51
Bloquear Impressão	51
Bloquear AirDrop	51
Bloquear anexos de arquivo	52
Bloquear composição de e-mail	52
Bloquear APIs do Facebook e Twitter	52
Obscurecer conteúdo da tela	52
Bloquear teclados de terceiros	52

Bloquear logs de aplicativos	52
Habilitar ShareFile	53
Habilitar Anexar de Arquivos	53
Acesso à rede do aplicativo	53
Acesso à rede	53
Sessão micro VPN necessária	53
Período de carência da sessão micro VPN necessária (minutos)	53
Lista de Exclusão	54
Bloquear conexões localhost	54
Rótulo do certificado	54
Logs do aplicativo	54
Saída de log padrão	54
Nível de log padrão	54
Número máximo de arquivos de log	54
Tamanho máximo do arquivo de log	55
Redirecionar logs do aplicativo	55
Criptografar logs	55
Geocerca do aplicativo	55
Longitude do ponto central	55
Latitude do ponto central	55
Raio	55
Configurações do aplicativo	56
Servidor Exchange do Secure Mail	56
Domínio de usuário do Secure Mail	56
Serviços de rede em segundo plano	56
Expiração do tíquete de serviços em segundo plano	57
Gateway de serviço de rede em segundo plano	57
Exportar contatos	57

Campos de contato para exportar	57
Aceitar todos os certificados SSL	57
Controlar notificações da tela bloqueada	58
Usar Conexão Segura	58
Notificação de e-mail padrão	58
Intervalo de sincronização padrão	58
Limite de pesquisa de e-mail	58
Intervalo máximo de sincronização	59
Habilitar número da semana	59
Habilitar downloads de anexos via Wi-Fi	59
Permitir documentos offline	59
Gerenciamento de Direitos de Informação	59
Classificação de e-mail	59
Marcações de classificação de e-mail	59
Namespace de classificação de e-mail	60
Versão da classificação de e-mail	60
Classificação de e-mail padrão	60
Habilitar salvamento automático de rascunhos de e-mail	60
Habilitar proteção de dados do iOS	60
Nome do Host EWS para Notificações Push	60
Notificações push	61
Região de notificações push	61
Habilitar S/MIME durante a primeira inicialização do Secure Mail	61
Mecanismo de autenticação inicial	61
Credenciais de autenticação inicial	61
Habilitar número da semana	61
Opções de Web e Áudio do Calendário	61
Origem do certificado público S/MIME	62

Endereço do servidor LDAP	62
DN Base do LDAP	62
Acessar LDAP anonimamente	62
Domínios de e-mail permitidos	62
Tentar Migração de Nome de Usuário na Falha de Autenticação	62
Relatar Endereços de E-mail de Phishing	63
Mecanismo de Relatório de Phishing	63
Domínios de Reunião do Skype for Business	63
Exportar calendário	63
Habilitar Slack	63
Nome do espaço de trabalho do Slack	63
Identificação de chamadas	64
Análise	64
Habilitar Google Analytics	64
Nível de detalhe do Google Analytics	64
Relatórios	64
Relatórios Citrix	64
Token de upload	65
Enviar relatórios somente por Wi-Fi	65
Máximo de cache de arquivo de relatório	65
Suporte OAuth para Office 365	65
Usar autenticação moderna para Office 365	65
Mecanismo de autenticação do Office 365	65
Nomes de host confiáveis do Exchange Online	65
Nomes de host AD FS confiáveis	66
Agente de usuário personalizado para autenticação moderna	66
Redirecionamento de e-mail	66
Redirecionamento de e-mail	66

Integração com o Slack	66
Habilitar Slack	66
Nome do espaço de trabalho do Slack	66
Políticas MDX para aplicativos de produtividade móvel para Android	67
Autenticação	67
Senha do aplicativo	67
Período máximo offline (horas)	67
Citrix Gateway Alternativo	68
Segurança do Dispositivo	68
Bloquear dispositivos com jailbreak ou root	68
Exigir criptografia do dispositivo	68
Exigir bloqueio do dispositivo	68
Requisitos de Rede	69
Exigir Wi-Fi	69
Redes Wi-Fi Permitidas	69
Acesso Diverso	69
Período de carência para atualização do aplicativo (horas)	69
Desabilitar atualização obrigatória	70
Apagar dados do aplicativo ao bloquear	70
Período de sondagem ativa (minutos)	70
Criptografia	71
Tipo de criptografia	71
Comportamento de dispositivo não compatível	71
Chaves de criptografia	71
Criptografia de arquivo privado	71
Exclusões de criptografia de arquivo privado	71
Limites de acesso para arquivos públicos	72
Criptografia de arquivo público	73

Exclusões de criptografia de arquivo público	73
Migração de arquivo público	73
Interação do Aplicativo	74
Grupo de Segurança	74
Recortar e Copiar	74
Colar	74
Troca de documentos (Abrir em)	74
Domínios de URL excluídos da filtragem	75
Domínios da Web Segura Permitidos	75
Lista de exceções de Abrir em Restrito	75
Troca de documentos de entrada (Abrir em)	76
Lista de permissões de troca de documentos de entrada	76
Nível de segurança da conexão	76
Restrições de Aplicativo	77
Bloquear câmera	77
Bloquear Galeria	77
Bloquear gravação de microfone	77
Bloquear serviços de localização	77
Bloquear composição de SMS	78
Bloquear captura de tela	78
Bloquear sensor do dispositivo	78
Bloquear NFC	78
Bloquear logs de aplicativos	78
Bloquear impressão	78
Habilitar ShareFile	78
Acesso à Rede do Aplicativo	79
Acesso à rede	79
Sessão Micro VPN necessária	79

Lista de Exclusão	80
Bloquear conexões localhost	80
Rótulo do certificado	80
Logs do aplicativo	80
Saída de log padrão	80
Nível de log padrão	80
Número máximo de arquivos de log	81
Tamanho máximo do arquivo de log	81
Redirecionar logs do aplicativo	81
Criptografar logs	81
Cerca Geográfica do Aplicativo	82
Longitude do ponto central	82
Latitude do ponto central	82
Raio	82
Análises	82
Detalhe do Google Analytics	82
Configurações do Aplicativo	82
Servidor Exchange do Secure Mail	82
Domínio de usuário do Secure Mail	83
Serviços de rede em segundo plano	83
Expiração do tíquete de serviços em segundo plano	83
Gateway de serviço de rede em segundo plano	83
Exportar contatos	84
Campos de contato para exportar	84
Aceitar todos os certificados SSL	84
Usar conexão segura	84
Gerenciamento de Direitos de Informação	84
Controlar notificações da tela bloqueada	84

Intervalo de sincronização padrão	85
Habilitar download de anexos por Wi-Fi	85
Permitir documentos offline	85
Habilitar salvamento automático de rascunhos de e-mail	85
Mecanismo de autenticação inicial	85
Credenciais de autenticação iniciais	86
Habilitar número da semana	86
Classificação de e-mail	86
Marcações de classificação de e-mail	86
Namespace de classificação de e-mail	86
Versão de classificação de e-mail	86
Classificação de e-mail padrão	86
Limite de Pesquisa de E-mail	87
Intervalo máximo de sincronização	87
Opções de Web e Áudio do Calendário	87
Origem do Certificado Público S/MIME	87
Endereço do Servidor LDAP	88
DN Base do LDAP	88
Acessar LDAP Anonimamente	88
Domínios de E-mail Permitidos	88
Notificações push	88
Nome do host EWS para notificações push	88
Região das notificações push	88
Tentar migração de nome de usuário na falha de autenticação	88
Relatar Endereços de E-mail de Phishing	89
Mecanismo de Relato de Phishing	89
Domínios de Reunião do Skype for Business	89
Exportar Calendário	90

Suporte OAuth para Office 365	90
Usar autenticação moderna para O365	90
Nomes de host confiáveis do Exchange Online	90
Nomes de host confiáveis do AD FS	90
Agente de usuário personalizado para autenticação moderna	91
Integração com o Slack	91
Habilitar Slack	91
Nome do espaço de trabalho do Slack	91
Políticas MDX para aplicativos de produtividade móvel para iOS	91
Autenticação	91
Senha do dispositivo	91
Senha do aplicativo	92
Período máximo offline (horas)	92
Citrix Gateway alternativo	92
Segurança do dispositivo	93
Bloquear dispositivos com jailbreak ou root	93
Requisitos de rede	93
Exigir Wi-Fi	93
Redes Wi-Fi permitidas	93
Acesso diverso	93
Desativar atualização obrigatória	93
Período de carência para atualização do aplicativo (horas)	93
Apagar dados do aplicativo ao bloquear	94
Período de sondagem ativa (minutos)	94
Criptografia	95
Tipo de criptografia	95
Comportamento de dispositivo não compatível	95
Habilitar criptografia MDX	95

Exclusões de criptografia de banco de dados	95
Exclusões de criptografia de arquivo	96
Interação do aplicativo	96
Recortar e copiar	96
Colar	96
Troca de documentos (Abrir em)	97
Lista de exceções de Abrir em restrito	97
Nível de segurança da conexão	97
Troca de documentos de entrada (Abrir em)	97
Esquemas de URL do aplicativo	98
Interação do aplicativo (URL de saída)	99
Domínios excluídos da filtragem de URL	99
URLs Permitidas	99
Domínios permitidos do Secure Web	102
Restrições de Aplicativos	102
Bloquear câmera	102
Bloquear Biblioteca de Fotos	102
Bloquear gravação de microfone	102
Bloquear ditado	102
Bloquear serviços de localização	103
Bloquear composição de SMS	103
Bloquear composição de e-mail	103
Bloquear iCloud	103
Bloquear pesquisa	103
Bloquear backup de arquivo	103
Bloquear AirPrint	103
Bloquear AirDrop	104
Bloquear anexos de arquivo	104

Bloquear APIs do Facebook e Twitter	104
Obscurecer conteúdo da tela	104
Bloquear teclados de terceiros (somente iOS 11 e posterior)	104
Bloquear logs de aplicativos	104
Habilitar ShareFile	104
Habilitar Anexar de Arquivos	104
Acesso à rede do aplicativo	105
Acesso à rede	105
Sessão Micro VPN necessária	105
Período de carência da sessão Micro VPN necessária (minutos)	106
Rótulo do certificado	106
Lista de Exclusão	106
Logs do aplicativo	106
Saída de log padrão	106
Nível de log padrão	106
Máximo de arquivos de log	107
Tamanho máximo do arquivo de log	107
Cerca geográfica do aplicativo	107
Longitude do ponto central	107
Latitude do ponto central	107
Raio	107
Habilitar Google Analytics	108
Análises	108
Nível de detalhe do Google Analytics	108
Relatórios	108
Relatórios da Citrix	108
Token de upload	108
Enviar relatórios somente por Wi-Fi	108

Máximo de cache de arquivo de relatório	109
Interação do aplicativo	109
Notificação de logoff explícito	109
Configurações do aplicativo	109
Servidor Exchange do Secure Mail	109
Domínio de usuário do Secure Mail	109
Serviços de rede em segundo plano	109
Expiração do tíquete de serviços em segundo plano	110
Gateway de serviço de rede em segundo plano	110
Exportar Contatos	110
Campos de contato para exportar	110
Aceitar todos os certificados SSL	111
Controlar notificações da tela bloqueada	111
Notificação de e-mail padrão	111
Intervalo de sincronização padrão	111
Limite de pesquisa de e-mail	111
Intervalo máximo de sincronização	112
Habilitar número da semana	112
Habilitar download de anexos via Wi-Fi	112
Permitir documentos offline	112
Gerenciamento de Direitos de Informação	112
Classificação de e-mail	112
Marcações de classificação de e-mail	113
Namespace de classificação de e-mail	113
Versão de classificação de e-mail	113
Classificação de e-mail padrão	113
Habilitar salvamento automático de rascunhos de e-mail	113
Mecanismo de autenticação inicial	113

Credenciais de autenticação iniciais	114
Habilitar preenchimento automático do nome de usuário	114
Habilitar proteção de dados do iOS	114
Nome do host EWS de Notificações por Push	114
Notificações por push	114
Região das notificações por push	114
Origem do certificado público S/MIME	115
Habilitar S/MIME durante a primeira inicialização do Secure Mail	115
Opções de Web e Áudio do Calendário	115
Origem do certificado público S/MIME	115
Endereço do servidor LDAP	116
DN Base do LDAP	116
Acessar LDAP Anonimamente	116
Domínios de E-mail Permitidos	116
Tentar migração de nome de usuário na falha de autenticação	116
Endereço de e-mail para relatar phishing	116
Mecanismo de relatório de phishing	116
Domínios de reunião do Skype for Business	117
Exportar Calendário	117
Identificação do Chamador	118
Suporte OAuth para Office 365	118
Mecanismo de autenticação do Office 365	118
Nomes de host confiáveis do Exchange Online	118
Nomes de host AD FS confiáveis	118
Redirecionamento de E-mail	119
Redirecionamento de E-mail	119
Integração com Slack	119
Habilitar Slack	119

Nome do espaço de trabalho do Slack	119
Recursos por plataforma	120
Citrix Secure Hub™	120
Citrix Secure Mail	121
Citrix Secure Web™	134
Gerenciamento de feature flags	137
Endereços IP	137
Requisitos do sistema	137
Citrix Secure Hub™	139
Administrando o Secure Hub	139
PIN Citrix	139
Fixação de certificado	140
Configurando autenticação de certificado + senha de uso único para o Secure Hub	141
Requisito de porta para conectividade ADS para dispositivos Android	147
Recursos do Secure Hub	149
Visão geral do Secure Mail	155
Citrix Secure Web™	158
Integrando e entregando o Secure Web	158
Configurando conexões de usuário	159
Políticas do Secure Web	160
Sites permitidos ou bloqueados	161
Bloquear pop-ups	161
Favoritos pré-carregados	161
URL da página inicial	162
Interface do usuário do navegador	162
Opções	162
Habilitar cache de senha da web	162
Servidores proxy	163

Sufixos DNS	163
Preparando sites de intranet para o Secure Web	163
Solução de problemas de sites de intranet	164
Para criar um arquivo de arquivo da web	165
Recursos do Secure Web	166
Citrix Content Collaboration™ para Endpoint Management	169
Como os clientes do Citrix Content Collaboration para Endpoint Management diferem dos clientes móveis do Citrix Files	170
Acesso do usuário	170
SSO	170
Micro VPN	171
Autenticação de dois fatores	171
Permissões de pasta	171
Proteção de acesso a documentos	171
Acesso à conta do Citrix Files	172
Políticas de dispositivo	172
Políticas MDX	172
Criptografia de dados	173
Disponibilidade	173
Integrando e entregando o Citrix Content Collaboration para clientes do Endpoint Management	173
Para configurar as informações da conta do Citrix Files no Endpoint Management para SSO	175
Para adicionar clientes do Citrix Content Collaboration para Endpoint Management ao Endpoint Management	175
Pré-requisitos	175
Para validar clientes Citrix Content Collaboration for Endpoint Management	177
Aplicativos EOL e descontinuados	178
Permitindo interação segura com aplicativos do Office 365	180
Habilitando o Office 365 no iOS	180

Habilitando o Office 365 no Android	181
Formatos de arquivo suportados	182
Histórico de documentos de aplicativos móveis de produtividade	183

Linha do tempo de lançamento de aplicativos de produtividade móvel

O lançamento dos aplicativos de produtividade móvel Citrix® tem uma cadência de duas semanas. Embora as datas exatas possam mudar, conhecer essa cadência pode ajudar você a planejar com antecedência. Também queremos facilitar o gerenciamento das implantações e atualizações de aplicativos.

Sobre o processo de lançamento faseado do Secure Mail e Secure Web

Quando novas versões do Secure Mail e Secure Web estão disponíveis, os lançamentos são implementados em uma abordagem faseada, da seguinte forma:

- Para usuários de iOS e Android, as atualizações do Secure Mail e Secure Web estão disponíveis na App Store e na Google Play Store para uma porcentagem crescente de usuários ao longo de uma semana (sete dias).
- Novos downloads do Secure Mail e Secure Web para iOS obtêm a nova versão dentro desta semana. Novos downloads do Secure Mail e Secure Web para Android executarão a versão anterior durante a semana, até que a implementação do novo lançamento atinja 100% de todos os usuários.
- Para os usuários, alguns recursos são lançados em fases graduais.

Pré-requisitos para o gerenciamento de feature flags

Se ocorrer um problema com o Secure Hub ou Secure Mail em produção, podemos desabilitar um recurso afetado dentro do código do aplicativo. Para isso, usamos feature flags e um serviço de terceiros chamado LaunchDarkly. Você não precisa fazer nenhuma configuração para habilitar o tráfego para o LaunchDarkly, exceto quando tiver um firewall ou proxy bloqueando o tráfego de saída. Nesse caso, você habilita o tráfego para o LaunchDarkly por meio de URLs ou endereços IP específicos, dependendo dos requisitos da sua política. Para obter detalhes sobre o suporte no MDX desde os aplicativos de produtividade móvel 10.6.15 para a exclusão de domínios do

tunelamento, consulte a [documentação do MDX Toolkit](#). Para um FAQ sobre feature flags e LaunchDarkly, consulte este [artigo da Central de Conhecimento de Suporte](#)

Nota: Para aviso prévio sobre os recursos do Citrix Endpoint Management que estão sendo descontinuados, consulte [Descontinuação](#).

Suporte para aplicativos de produtividade móvel

Usuários que têm atualizações automáticas ativadas recebem a versão mais recente da loja de aplicativos. A versão mais recente dos aplicativos de produtividade móvel é a seguinte:

- 23.10.0 (Secure Web para Android)
- 23.9.0 (Secure Mail e Secure Web para iOS)
- 23.8.2 (Secure Mail para Android)

A Citrix® oferece suporte a atualizações das duas últimas versões dos aplicativos de produtividade móvel. As duas últimas versões dos aplicativos de produtividade móvel são as seguintes:

- 23.8.1 (Secure Mail para Android)
- 23.8.0 (Secure Web para Android)
- 23.7.0 (Secure Mail para Android e Secure Mail para iOS)
- 23.5.0 (Secure Mail para iOS e Secure Web para Android)
- 23.2.0 (Secure Web para iOS)
- 22.9.1 (Secure Web para iOS)

IMPORTANTE:

A criptografia MDX atingiu o fim da vida útil (EOL) em September 1, 2020. Para dispositivos registrados na administração de dispositivos legados (DA):

- Se você não usa a criptografia MDX, nenhuma ação é necessária.
- Se você usa criptografia MDX, migre seus dispositivos Android para o Android Enterprise. Dispositivos com Android 10 devem se registrar ou se registrar novamente usando o Android Enterprise. Isso inclui dispositivos Android no modo somente MAM. Consulte [Migrar a administração de dispositivos para o Android Enterprise](#) para obter detalhes.

Sistemas operacionais suportados

Os aplicativos de produtividade móvel suportam os seguintes sistemas operacionais:

NOME DO PRODUTO	SISTEMA OPERACIONAL	VERSÃO MÍNIMA DE IMPLANTAÇÃO	VERSÃO MAIS RECENTE DISPONÍVEL
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x
Secure Mail	Android	8.x	14.x
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

As versões mais recentes dos aplicativos de produtividade móvel são compatíveis com a versão mais recente e as duas versões anteriores do Citrix Endpoint Management. Para obter mais informações sobre os sistemas operacionais compatíveis com o Citrix Endpoint Management, consulte [Sistemas operacionais de dispositivos compatíveis](#).

A versão mais recente dos aplicativos de produtividade móvel requer a versão mais recente do Secure Hub. Certifique-se de manter o Secure Hub atualizado.

NOTA:

A qualquer momento, a Citrix oferece suporte apenas às versões mais recente e às duas anteriores (N, N-1 e N-2) dos sistemas operacionais Android e iOS.

Outras considerações e limitações

Para aviso prévio sobre os recursos do Citrix Endpoint Management que estão sendo descontinuados, consulte [Descontinuação](#).

Secure Mail

- O Endpoint Management atualmente não oferece suporte ao NetScaler 12.0.41.16 devido a um problema com o Secure Ticket Authority (STA) e o Secure Mail. O problema foi corrigido no NetScaler 12.0 build 41.22.
- O suporte no Secure Mail para Exchange 2007 e Lotus Notes 8.5.3 atingiu o Fim da Vida Útil (EOL) em September 30, 2017.
- Para o melhor desempenho ao enviar anexos do Citrix Files, as versões mais recentes do Citrix Files são recomendadas. O Citrix Files não é compatível com Windows.
- Em ambientes IBM Notes, você deve configurar o servidor IBM Domino Traveler, versão 9.0. Para obter detalhes, consulte Integração do Exchange Server ou IBM Notes Traveler Server.

NOTA:

- O Citrix Files para XenMobile atingiu o EOL em July 1, 2023. Para obter mais informações, consulte [Aplicativos EOL e descontinuados](#)

Secure Web

Instale a versão mais recente do Android WebView nos dispositivos. Os usuários podem baixar o Android WebView na Google Play Store.

QuickEdit

O QuickEdit permanece disponível como um aplicativo de produtividade móvel. O status de Fim de Vida (EOL) não foi aplicado em September 1, 2018, conforme comunicado anteriormente.

Citrix Content Collaboration™ para Endpoint Management

Os usuários acessam o Citrix Content Collaboration para Endpoint Management nas lojas de aplicativos públicas após a versão 6.5.

ShareConnect

O ShareConnect atingiu o Fim de Vida (EOL) em June 30, 2020. Para obter detalhes, consulte [Aplicativos EOL e descontinuados](#).

Citrix Secure Notes e Citrix Secure Tasks

O Citrix Secure Notes e o Citrix Secure Tasks atingiram o status de Fim de Vida (EOL) em December 31, 2018. Para obter detalhes, consulte [Aplicativos EOL e descontinuados](#).

Tarefas e considerações do administrador

Este artigo discute as tarefas e considerações relevantes para administradores de aplicativos de produtividade móvel.

Gerenciamento de sinalizadores de recursos

Se ocorrer um problema com um aplicativo de produtividade móvel em produção, podemos desabilitar um recurso afetado dentro do código do aplicativo. Podemos desabilitar o recurso para Secure Hub, Secure Mail e Secure Web para iOS e Android. Para fazer isso, usamos sinalizadores de recursos e um serviço de terceiros chamado LaunchDarkly. Você não precisa fazer nenhuma configuração para habilitar o tráfego para o LaunchDarkly, exceto quando tiver um firewall ou proxy bloqueando o tráfego de saída. Nesse caso, você habilita o tráfego para o LaunchDarkly por meio de URLs ou endereços IP específicos, dependendo dos requisitos da sua política. Para obter detalhes sobre o suporte para a exclusão de domínios do tunelamento, consulte a [documentação do MAM SDK](#).

Você pode habilitar o tráfego e a comunicação para o LaunchDarkly das seguintes maneiras:

Habilitar tráfego para as seguintes URLs

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

Criar uma lista de permissões por domínio

Anteriormente, oferecíamos uma lista de endereços IP para usar quando suas políticas internas exigiam que apenas endereços IP fossem listados. Agora, como a Citrix® fez melhorias na infraestrutura, estamos eliminando gradualmente os endereços IP públicos a partir de July 16, 2018. Recomendamos que você crie uma lista de permissões por domínio, se possível.

Listar endereços IP em uma lista de permissões

Se você precisar listar endereços IP em uma lista de permissões, para uma lista de todos os intervalos de endereços IP atuais, consulte esta [lista pública de IPs do LaunchDarkly](#). Você pode usar esta lista para garantir que as configurações do seu firewall sejam atualizadas automaticamente, de acordo com as atualizações da infraestrutura. Para obter detalhes sobre o status das alterações na infraestrutura, consulte a [Página de Status do LaunchDarkly](#).

Nota:

Aplicativos da loja de aplicativos pública exigem uma nova instalação na primeira vez que você os implanta. Não é possível fazer upgrade da versão corporativa empacotada atual do aplicativo para a versão da loja pública.

Com a distribuição de aplicativos da loja pública, você não assina e empacota aplicativos desenvolvidos pela Citrix com o MDX Toolkit. Você pode usar o MDX Toolkit para empacotar aplicativos de terceiros ou corporativos.

Requisitos de sistema do LaunchDarkly

- Endpoint Management 10.7 ou posterior.
- Certifique-se de que os aplicativos possam se comunicar com os seguintes serviços se você tiver o tunelamento dividido no Citrix ADC definido como **OFF**:
 - Serviço LaunchDarkly
 - Serviço de escuta APNs

Lojas de aplicativos compatíveis

Os aplicativos de produtividade móvel estão disponíveis na Apple App Store e no Google Play.

Na China, onde o Google Play não está disponível, o Secure Hub para Android está disponível nas seguintes lojas de aplicativos:

- <<https://shouji.baidu.com>>
- <<http://apk.hiapk.com>>
- <<https://apk.91.com>>

Habilitando a distribuição de aplicativos da loja pública

1. Baixe os arquivos .mdx da loja pública para iOS e Android na [página de downloads do Endpoint Management](#).
2. Carregue os arquivos .mdx para o console do Endpoint Management. As versões da loja pública dos aplicativos de produtividade móvel ainda são carregadas como aplicativos MDX. Não carregue os aplicativos como aplicativos da loja pública no servidor. Para obter as etapas, consulte [Adicionar aplicativos](#).
3. Altere as políticas de seus padrões com base em suas políticas de segurança (opcional).
4. Envie os aplicativos como aplicativos obrigatórios (opcional). Esta etapa exige que seu ambiente esteja habilitado para gerenciamento de dispositivos móveis.
5. Instale aplicativos no dispositivo a partir da App Store, Google Play ou da loja de aplicativos do Endpoint Management.
 - No Android, o usuário é direcionado à Play Store para instalar o aplicativo. No iOS, em implantações com MDM, o aplicativo é instalado sem que o usuário seja levado à loja de aplicativos.
 - Quando o aplicativo é instalado da App Store ou Play Store, a seguinte ação ocorre. O aplicativo transita para um aplicativo gerenciado, desde que o arquivo .mdx correspondente tenha sido carregado para o servidor. Ao fazer a transição para um aplicativo gerenciado, o aplicativo solicita um PIN Citrix. Quando os usuários inserem o PIN Citrix, o Secure Mail exibe a tela de configuração da conta.
6. Os aplicativos são acessíveis somente se você estiver inscrito no Secure Hub e o arquivo .mdx correspondente estiver no servidor. Se qualquer uma das condições não for atendida, os usuários poderão instalar o aplicativo, mas o uso do aplicativo será bloqueado.

Se você usa atualmente aplicativos do Citrix Ready Marketplace™ que estão em lojas de aplicativos públicas, já está familiarizado com o processo de implantação. Os aplicativos de produtividade móvel adotam a mesma abordagem que muitos ISVs usam atualmente. Incorpore o MDX SDK no aplicativo para torná-lo pronto para a loja pública.

Nota:

As versões da loja pública do aplicativo Citrix Files para iOS e Android agora são universais. O aplicativo Citrix Files é o mesmo para telefones e tablets.

Notificações push da Apple

Para obter mais informações sobre como configurar notificações push, consulte [Configurando o Secure Mail para Notificações Push](#).

FAQ da App Store pública

- Posso implantar várias cópias do aplicativo da loja pública para diferentes grupos de usuários? Por exemplo, quero implantar políticas diferentes para diferentes grupos de usuários.

Carregue um arquivo .mdx diferente para cada grupo de usuários. No entanto, neste caso, um único usuário não pode pertencer a vários grupos. Se os usuários pertencessem a vários grupos, várias cópias do mesmo aplicativo seriam atribuídas a esse usuário. Várias cópias de um aplicativo da loja pública não podem ser implantadas no mesmo dispositivo, porque o ID do aplicativo não pode ser alterado.

- Posso enviar aplicativos da loja pública como aplicativos obrigatórios?

Sim. O envio de aplicativos para dispositivos requer MDM; não é suportado para implantações somente MAM.

- Devo atualizar alguma política de tráfego ou regras do Exchange Server que sejam baseadas no agente de usuário?

As strings para quaisquer políticas e regras baseadas em agente de usuário por plataforma são as seguintes.

Importante:

Secure Notes e Secure Tasks atingiram o status de Fim de Vida (EOL) em December 31, 2018. Para detalhes, consulte [Aplicativos EOL e descontinuados](#).

Android

APLICATIVO	SERVIDOR	STRING DE AGENTE DE USUÁRIO
Citrix Secure Mail™	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web™		WorxMail

APLICATIVO	SERVIDOR	STRING DE AGENTE DE USUÁRIO
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

APLICATIVO	SERVIDOR	STRING DE USER-AGENT
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- Posso impedir atualizações de aplicativos?

Não. Quando uma atualização é publicada na loja de aplicativos pública, todos os usuários que têm atualizações automáticas ativadas recebem a atualização.

- Posso forçar atualizações de aplicativos?

Sim, as atualizações são forçadas por meio da política de período de carência de atualização. Essa política é definida quando o novo arquivo .mdx correspondente à versão atualizada do aplicativo é carregado no Endpoint Management.

- Como faço para testar os aplicativos antes que a atualização chegue aos usuários se não consigo controlar os prazos de atualização?

Semelhante ao processo para o Secure Hub, os aplicativos estão disponíveis para teste no TestFlight para iOS durante o período EAR. Para Android, os aplicativos estão disponíveis por meio do programa beta do Google Play durante o período EAR. Você pode testar as atualizações de aplicativos durante esse período.

- O que acontece se eu não atualizar o novo arquivo .mdx antes que a atualização automática chegue aos dispositivos dos usuários?

O aplicativo atualizado permanece compatível com o arquivo .mdx mais antigo. Quaisquer novos recursos que dependam de uma nova política não são ativados.

- O aplicativo fará a transição para gerenciado se o Secure Hub estiver instalado ou o aplicativo precisa ser registrado?

Os usuários devem estar registrados no Secure Hub para que o aplicativo da loja pública seja ativado como um aplicativo gerenciado (protegido por MDX) e seja utilizável. Se o Secure Hub estiver instalado, mas não registrado, o usuário não poderá usar o aplicativo da loja pública.

- Preciso de uma conta de desenvolvedor Apple Enterprise para os aplicativos da loja pública?

Não. Como a Citrix agora mantém os certificados e perfis de provisionamento para aplicativos de produtividade móvel, uma conta de desenvolvedor Apple Enterprise não é necessária para implantar os aplicativos para os usuários.

- O fim da distribuição empresarial se aplica a qualquer aplicativo empacotado que eu tenha implantado?

Não, aplica-se apenas aos aplicativos de produtividade móvel: Secure Mail, Secure Web e Citrix Content Collaboration™ para Endpoint Management, QuickEdit e ShareConnect.

Quaisquer aplicativos empacotados empresariais que você implantou, desenvolvidos internamente ou por terceiros, podem continuar a usar o empacotamento empresarial. O MDX Toolkit continua a oferecer suporte ao empacotamento empresarial para desenvolvedores de aplicativos.

- Quando instalo um aplicativo do Google Play, recebo um erro do Android com o código de erro 505.

Nota:

O suporte para Android 5.x terminou em December 31, 2018.

Este é um problema conhecido com o Google Play e as versões do Android 5.x. Se esse erro ocorrer, você pode seguir estas etapas para limpar dados obsoletos no dispositivo que impedem a instalação do aplicativo:

1. Reinicie o dispositivo.
2. Limpe o cache e os dados do Google Play pelas configurações do dispositivo.

3. Como último recurso, remova e adicione novamente a conta do Google no seu dispositivo.

Para obter mais informações, pesquise neste [site](#) usando as seguintes palavras-chave "Corrigir erro 505 da Google Play Store no Android: Código de erro desconhecido"

- Embora o aplicativo no Google Play tenha sido lançado para produção e uma nova versão beta não esteja disponível, por que vejo Beta após o título do aplicativo no Google Play?

Se você faz parte do nosso programa de Lançamento de Acesso Antecipado (EAR), você sempre verá Beta ao lado do título do aplicativo. Este nome simplesmente notifica os usuários sobre seu nível de acesso para um aplicativo específico. O nome Beta indica que os usuários recebem a versão mais recente do aplicativo disponível. A versão mais recente pode ser a última versão publicada em um canal de produção ou em um canal beta.

- Após instalar e abrir o aplicativo, os usuários veem a mensagem Aplicativo Não Autorizado, mesmo que o arquivo .mdx esteja no console do Endpoint Management.

Esse problema pode ocorrer se os usuários instalarem o aplicativo diretamente da App Store ou do Google Play e se o Secure Hub não for atualizado. O Secure Hub deve ser atualizado quando o temporizador de inatividade expirar. As políticas são atualizadas quando os usuários abrem o Secure Hub e se reautenticam. O aplicativo é autorizado na próxima vez que os usuários o abrirem.

- Preciso de um código de acesso para usar o aplicativo? Vejo uma tela me pedindo para inserir um código de acesso ao instalar o aplicativo da App Store ou Play Store.

Se você vir uma tela solicitando um código de acesso, você não está inscrito no Endpoint Management através do Secure Hub. Inscreva-se com o Secure Hub e certifique-se de que o arquivo .mdx para o aplicativo esteja implantado no servidor. Certifique-se também de que o aplicativo possa ser usado. O código de acesso é limitado apenas ao uso interno da Citrix. Os aplicativos exigem uma implantação do Endpoint Management para serem ativados.

- Posso implantar aplicativos da loja pública do iOS via VPP ou DEP?

O Endpoint Management é otimizado para distribuição VPP de aplicativos de loja pública que não são habilitados para MDX. Embora você possa distribuir os aplicativos da loja pública do Endpoint Management com VPP, a implantação não é ideal, até que façamos mais aprimoramentos no Endpoint Management e na loja do Secure Hub para resolver as limitações. Para obter uma lista de problemas conhecidos com a implantação de aplicativos da loja pública do Endpoint Management via VPP, além de possíveis soluções alternativas, consulte este artigo no [centro de conhecimento da Citrix](#).

Políticas MDX para aplicativos de produtividade móvel

As políticas MDX permitem configurar as definições que o Endpoint Management impõe. As políticas abrangem autenticação, segurança do dispositivo, requisitos e acesso à rede, criptografia, interação de aplicativos, restrições de aplicativos e muito mais. Muitas políticas MDX se aplicam a todos os aplicativos de produtividade móvel. Algumas políticas são específicas de aplicativos.

Os arquivos de política são fornecidos como arquivos .mdx para as versões da loja pública dos aplicativos de produtividade móvel. Você também pode configurar políticas no console do Endpoint Management ao adicionar um aplicativo.

Para descrições completas das políticas MDX, consulte os seguintes artigos nesta seção:

- [Políticas MDX para aplicativos de produtividade móvel em resumo](#)
- [Políticas MDX para aplicativos de produtividade móvel para Android](#)
- [Políticas MDX para aplicativos de produtividade móvel para iOS](#)

As seções a seguir descrevem as políticas MDX relacionadas às conexões de usuário.

Modo duplo no Secure Mail para Android

Um SDK de gerenciamento de aplicativos móveis (MAM) está disponível para substituir áreas da funcionalidade MDX que não são cobertas pelas plataformas iOS e Android. A tecnologia de encapsulamento MDX está programada para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos corporativos, você deve incorporar o SDK MAM.

A partir da versão 20.8.0, os aplicativos Android são lançados com o MDX e o SDK MAM para preparar a estratégia de EOL do MDX mencionada anteriormente. O modo duplo MDX destina-se a fornecer uma maneira de fazer a transição para novos SDKs MAM a partir do atual MDX Toolkit. Usar o modo duplo permite que você:

- Continue gerenciando aplicativos usando o MDX Toolkit (agora chamado de Legacy MDX no console do Endpoint Management)
- Gerencie aplicativos que incorporam o novo SDK MAM.

NOTA:

Ao usar o SDK MAM, você não precisa encapsular aplicativos.

Não há etapas adicionais necessárias após a mudança para o SDK MAM.

Para obter mais detalhes sobre o MAM SDK, consulte os seguintes artigos:

- [Visão geral do MAM SDK](#)
- [Últimos lançamentos do MAM SDK](#)
- Seção Citrix Developer sobre [Gerenciamento de Dispositivos](#)
- [Postagem do blog da Citrix](#)

Pré-requisitos

Para uma implantação bem-sucedida do recurso de modo duplo, certifique-se do seguinte:

- Atualize seu Citrix Endpoint Management para as versões 10.12 RP2 e posteriores, ou 10.11 RP5 e posteriores.
- Atualize seus aplicativos móveis para a versão 20.8.0 ou posterior.
- Atualize o arquivo de políticas para a versão 20.8.0 ou posterior.
- Se sua organização usa aplicativos de terceiros, certifique-se de incorporar o MAM SDK em seus aplicativos de terceiros antes de mudar para a opção MAM SDK para seus aplicativos de produtividade móvel da Citrix. Todos os seus aplicativos gerenciados devem ser movidos para o MAM SDK de uma só vez.

NOTA:

O MAM SDK é compatível com todos os clientes baseados em nuvem.

Limitações

- O MAM SDK oferece suporte apenas a aplicativos publicados na plataforma Android Enterprise em sua implantação do Citrix Endpoint Management™. Para os aplicativos recém-publicados, a criptografia padrão é a criptografia baseada em plataforma.
- O MAM SDK suporta apenas criptografia baseada em plataforma, e não criptografia MDX.
- Se você não atualizar o Citrix Endpoint Management, e os arquivos de política estiverem executando a versão 20.8.0 ou posterior para os aplicativos móveis, então entradas duplicadas da política de Rede serão criadas para o Secure Mail.

Ao configurar o Secure Mail no Citrix Endpoint Management, o recurso de modo duplo permite que você continue gerenciando aplicativos usando o MDX Toolkit (agora Legacy MDX) ou mude para o

novo MAM SDK para gerenciamento de aplicativos. A Citrix recomenda que você mude para o MAM SDK, pois os MAM SDKs são mais modulares e pretendem permitir que você use apenas um subconjunto da funcionalidade MDX que sua organização utiliza.

Você obtém as seguintes opções para configurações de política no **contêiner de política MDX ou MAM SDK**:

- **MAM SDK**
- **Legacy MDX**

The screenshot displays the Citrix Cloud Endpoint Management interface. The top navigation bar includes 'Citrix Cloud' and 'Endpoint Management'. The main navigation tabs are 'Analyze', 'Manage', 'Configure', and 'Monitor'. Under 'Configure', there are sub-tabs: 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, showing a list of policy containers on the left. The 'MDX' container is selected, and its configuration details are shown on the right. The 'MDX or MAM SDK policy container' section is highlighted with a red box, showing 'MAM SDK' selected and 'Legacy MDX' as an option. The configuration details include fields for 'File name', 'App Description', 'App version', 'Minimum OS version', 'Maximum OS version', 'Excluded devices', and several toggle switches for 'Remove app if MDM profile is removed', 'Prevent app data backup', 'Force app to be managed', and 'App deployed via Volume purchase'.

Na política do **contêiner de política MDX ou MAM SDK**, você só pode alterar sua opção de **Legacy MDX** para **MAM SDK**. A opção de alternar de **MAM SDK** para **Legacy MDX** não é permitida, e você precisa republicar o aplicativo. O valor padrão é **Legacy MDX**. Certifique-se de definir o mesmo modo de política para o Secure Mail e o Secure Web executando no mesmo dispositivo. Você não pode ter dois modos diferentes executando no mesmo dispositivo.

Conexões de usuário à rede interna

As conexões que fazem túnel para a rede interna podem usar um túnel VPN completo ou uma variação de uma VPN sem cliente, conhecida como Tunneled – Web SSO. A política de modo VPN preferencial controla esse comportamento. Por padrão, as conexões usam Tunneled – Web SSO, que é recomendado para conexões que exigem SSO. A configuração de túnel VPN completo é recomendada para conexões que usam certificados de cliente ou SSL de ponta a

ponta para um recurso na rede interna. A configuração lida com qualquer protocolo sobre TCP e pode ser usada com computadores Windows e Mac, e com dispositivos iOS e Android.

A política Permitir troca de modo VPN permite a alternância automática entre o túnel VPN completo e os modos Tunneled – Web SSO conforme necessário. Por padrão, esta política está desativada. Quando esta política está ativada, uma solicitação de rede que falha devido a uma solicitação de autenticação que não pode ser tratada no modo VPN preferencial é repetida no modo alternativo. Por exemplo, os desafios do servidor para certificados de cliente podem ser acomodados pelo modo de túnel VPN completo, mas não pelo modo Tunneled – Web SSO. Da mesma forma, os desafios de autenticação HTTP são mais propensos a serem atendidos com SSO ao usar o modo Tunneled – Web SSO.

Restrições de acesso à rede

A política de acesso à rede especifica se restrições são impostas ao acesso à rede. Por padrão, o acesso ao Secure Mail é irrestrito, o que significa que nenhuma restrição é imposta ao acesso à rede. Os aplicativos têm acesso irrestrito às redes às quais o dispositivo está conectado. Por padrão, o acesso ao Secure Web é tunelado para a rede interna, o que significa que um túnel VPN por aplicativo de volta à rede interna é usado para todo o acesso à rede e as configurações de túnel dividido do Citrix ADC são usadas. Você também pode especificar acesso bloqueado para que o aplicativo opere como se o dispositivo não tivesse conexão de rede.

Não bloqueie a política de acesso à rede se quiser permitir recursos como AirPrint, iCloud e APIs do Facebook e Twitter.

A política de acesso à rede também interage com a política de serviços de rede em segundo plano. Para detalhes, consulte [Integrando o Exchange Server ou o IBM Notes Traveler Server](#).

Propriedades do cliente do Endpoint Management

As propriedades do cliente contêm informações que são fornecidas diretamente ao Secure Hub nos dispositivos do usuário. As propriedades do cliente estão localizadas no console do Endpoint Management em **Configurações > Cliente > Propriedades do Cliente**.

As propriedades do cliente são usadas para configurar definições como as seguintes:

Cache de senha do usuário

O cache de senha do usuário permite que a senha do Active Directory dos usuários seja armazenada em cache localmente no dispositivo móvel. Se você habilitar o cache de senha do usuário, os usuários serão solicitados a definir um PIN ou senha Citrix.

Temporizador de inatividade

O temporizador de inatividade define o tempo em minutos que os usuários podem deixar o dispositivo inativo e acessar um aplicativo sem serem solicitados a inserir um PIN ou senha Citrix. Para habilitar essa configuração para um aplicativo MDX, você deve definir a política de senha do aplicativo como **Ativada**. Se a política de senha do aplicativo estiver **Desativada**, os usuários são redirecionados para o Secure Hub para realizar uma autenticação completa. Ao alterar essa configuração, o valor entra em vigor na próxima vez que os usuários forem solicitados a autenticar.

Autenticação por PIN Citrix

O PIN Citrix simplifica a experiência de autenticação do usuário. O PIN é usado para proteger um certificado de cliente ou salvar credenciais do Active Directory localmente no dispositivo. Se você configurar as definições de PIN, a experiência de login do usuário será a seguinte:

1. Quando os usuários iniciam o Secure Hub pela primeira vez, eles recebem uma solicitação para inserir um PIN, que armazena as credenciais do Active Directory em cache.
2. Quando os usuários iniciam um aplicativo de produtividade móvel, como o Secure Mail, eles inserem o PIN e fazem login.

Você usa as propriedades do cliente para habilitar a autenticação por PIN, especificar o tipo de PIN e especificar os requisitos de força, comprimento e alteração do PIN.

Autenticação por impressão digital ou Touch ID

A autenticação por impressão digital, também conhecida como autenticação por Touch ID, para dispositivos iOS é uma alternativa ao PIN Citrix. O recurso é útil quando aplicativos empacotados, exceto o Secure Hub, precisam de autenticação offline, como quando o temporizador de inatividade expira. Você pode habilitar esse recurso nos seguintes cenários de autenticação:

- Configuração de PIN Citrix + certificado de cliente
- Configuração de PIN Citrix + senha AD em cache
- Configuração de PIN Citrix + certificado de cliente e configuração de senha AD em cache
- O PIN Citrix está desativado

Se a autenticação por impressão digital falhar ou se um usuário cancelar o prompt de autenticação por impressão digital, os aplicativos encapsulados retornarão à autenticação por PIN Citrix ou senha AD.

Requisitos de autenticação por impressão digital

- Dispositivos iOS (versão mínima 8.1) que suportam autenticação por impressão digital e têm pelo menos uma impressão digital configurada.
- A entropia do usuário deve estar desativada.

Para configurar a autenticação por impressão digital

Importante:

Se a entropia do usuário estiver ativada, a propriedade Enable Touch ID Authentication será ignorada. A entropia do usuário é ativada por meio da chave Encrypt secrets using the Passcode.

1. Na console do Endpoint Management, vá para **Configurações > Cliente > Propriedades do Cliente**.
2. Clique em **Adicionar**.

The screenshot shows the 'Add New Client Property' form within the Endpoint Management console. The breadcrumb trail is 'Settings > Client Properties > Add New Client Property'. The form has four fields: 'Key' (a dropdown menu with 'Select an option' and a help icon), 'Value' (a text input field with a red asterisk), 'Name' (a text input field with a red asterisk), and 'Description' (a larger text input field with a red asterisk). The 'Key' field is currently set to 'Select an option'.

3. Adicione a chave **ENABLE_TOUCH_ID_AUTH**, defina seu **Valor** como **True** e, em seguida, defina o nome da política como **Enable Fingerprint Authentication**.

Depois de configurar a autenticação por impressão digital, os usuários não precisam registrar novamente seus dispositivos.

Para mais informações sobre a chave Encrypt Secrets using Passcode e as propriedades do cliente em geral, consulte o artigo do Endpoint Management sobre [Propriedades do cliente](#).

Google Analytics

O Citrix Secure Mail usa o Google Analytics para coletar estatísticas de aplicativos e dados de análise de informações de uso para melhorar a qualidade do produto. A Citrix não coleta nem armazena nenhuma outra informação pessoal do usuário.

Desativar o Google Analytics

Os administradores podem desativar o Google Analytics configurando a propriedade de cliente personalizada **DISABLE_GA**. Para desativar o Google Analytics, faça o seguinte:

1. Faça login no console do Citrix Endpoint Management e navegar para **Configurações > Propriedades do Cliente > Adicionar Nova Propriedade do Cliente**.
2. Adicione o valor **DISABLE_GA** ao campo **Chave**.
3. Defina o valor da propriedade do cliente como **true**.

NOTA:

Se você não configurar o valor **DISABLE_GA** no console do Citrix Endpoint Management, os dados do Google Analytics estarão ativos.

Políticas MDX para aplicativos de produtividade móvel em um relance

Este artigo descreve as políticas de aplicativo MDX para aplicativos de produtividade móvel da Citrix para iOS e Android, juntamente com os valores padrão. Você altera as configurações de política no console do Citrix Endpoint Management. Para obter detalhes, consulte [Adicionar aplicativos](#).

NOTA:

O Secure Hub atualiza as políticas durante certas ações. Para obter detalhes, consulte [Administrar o Secure Hub](#).

Autenticação

Senha do dispositivo

- iOS: Sim

- Android: Não
- Configuração padrão: Desativado

NOTA:

Esta política se aplicava apenas a dispositivos iOS 9, que a Citrix® não oferece mais suporte.

Senha do aplicativo

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Período de carência de sessão online obrigatória (minutos)

- iOS: Sim
- Android: Não
- Configuração padrão: 0

Período offline máximo

- iOS: Sim
- Android: Sim
- Configuração padrão: 168 horas (7 dias)

Citrix Gateway alternativo

NOTA:

O nome desta política no console do Endpoint Management é Alternate NetScaler® Gateway.

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Segurança do dispositivo

Bloquear dispositivos com jailbreak ou root

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Exigir bloqueio do dispositivo

- iOS: Não
- Android: Sim
- Configuração padrão: Desativado

NOTA:

Em dispositivos Android M, as opções de bloqueio de tela PIN do dispositivo ou senha e padrão do dispositivo têm o mesmo efeito: Com qualquer uma dessas opções, o aplicativo é bloqueado se o dispositivo não tiver um PIN, senha ou bloqueio de tela padrão configurado.

Requisitos de rede

Exigir Wi-Fi

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Redes Wi-Fi Permitidas

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Acesso diverso

Período de carência para atualização do aplicativo (horas)

- iOS: Sim

- Android: Sim
- Configuração padrão: 168 horas (7 dias)

NOTA:

A Citrix recomenda usar um valor diferente de zero (0). Um valor zero impede imediatamente os usuários, sem aviso, de usar um aplicativo em execução até que baixem e instalem a atualização. Essa configuração pode levar a uma situação em que os usuários são forçados a sair do aplicativo e, potencialmente, perder o trabalho.

Desativar atualização obrigatória

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Apagar dados do aplicativo ao bloquear

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Período de sondagem ativa (minutos)

- iOS: Sim
- Android: Sim
- Configuração padrão: 60 minutos (1 hora)

NOTA:

Defina este valor abaixo do padrão apenas para aplicativos de alto risco, ou o desempenho pode ser afetado.

Criptografia

Tipo de criptografia

- iOS: Sim

- Android: Sim
- Configuração padrão: Criptografia MDX

CUIDADO:

Para aplicativos recém-adicionados, quando você muda de **Criptografia de plataforma com aplicação de conformidade** para **Criptografia MDX**, você é forçado a remover e reinstalar o aplicativo. A configuração padrão para aplicativos recém-adicionados é **Criptografia de plataforma com aplicação de conformidade**.

Comportamento de dispositivo não compatível

- iOS: Sim
- Android: Sim
- Configuração padrão: Permitir aplicativo após aviso

Habilitar criptografia MDX

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

CUIDADO:

Se você alterar esta política após implantar um aplicativo, os usuários devem reinstalar o aplicativo.

Chaves de criptografia

- iOS: Não
- Android: Sim
- Configuração padrão: Acesso offline permitido é a única opção disponível.

Criptografia de arquivo privado

- iOS: Não
- Android: Sim
- Configuração padrão: SecurityGroup

Exclusões de criptografia de arquivo privado

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

Limites de acesso para arquivos públicos

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

NOTA:

A ativação da política de criptografia de arquivo público impõe esta política (alterada da opção Desativar para a opção SecurityGroup ou Aplicativo). Esta política se aplica apenas a arquivos públicos existentes e não criptografados e especifica quando criptografar os arquivos.

Criptografia de arquivo público

- iOS: Não
- Android: Sim
- Configuração padrão: SecurityGroup

Exclusões de criptografia de arquivo público

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

Migração de arquivo público

- iOS: Não
- Android: Sim
- Configuração padrão: Gravação (RO/RW)

NOTA:

Criptografar um arquivo público existente torna o arquivo indisponível para outros aplicativos que não possuem a mesma chave de criptografia.

Habilitar criptografia

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

NOTA:

Se você alterar esta política para um aplicativo existente, os usuários deverão remover e reinstalar o aplicativo para aplicar a alteração da política.

Exclusões de criptografia de banco de dados

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Exclusões de criptografia de arquivo

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Interação do aplicativo

Grupo de Segurança

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

NOTA:

Se você alterar esta política para um aplicativo existente, os usuários devem remover e reinstalar o aplicativo para aplicar a alteração da política.

Recortar e copiar

- iOS: Sim
- Android: Sim
- Configuração padrão: Restrito

Colar

- iOS: Sim
- Android: Sim
- Configuração padrão: Irrestrito

Troca de documentos (Abrir em)

- iOS: Sim
- Android: Sim
- Configuração padrão: Restrito

Domínios de URL excluídos da filtragem

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

Domínios da Web Segura permitidos

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

Nível de segurança da conexão

- iOS: Sim
- Android: Sim

- Configuração padrão: TLS

Troca de documentos de entrada (Abrir em)

- iOS: Sim
- Android: Sim
- Configuração padrão: Irrestrito

Lista de exceção de Abertura Restrita

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio (para Android); aplicativos do Office 365 (para iOS)

NOTA:

No Android, esta política era anteriormente chamada de exclusões de Abertura. No iOS, esta política está oculta. Para obter detalhes, consulte [Políticas MDX para aplicativos iOS](#).

Esquemas de URL de aplicativo

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio. Todos os esquemas de URL de aplicativo registrados são bloqueados.

URLs permitidas

- iOS: Sim
- Android: Não
- Configuração padrão: Para obter detalhes sobre as configurações padrão, consulte a seção Interação do aplicativo em políticas MDX para aplicativos iOS.

Notificações de logoff explícito

- iOS: Sim
- Android: Não
- Configuração padrão: Somente dispositivos compartilhados, para Secure Mail

Interação do aplicativo (URL de saída)

Domínios excluídos da filtragem de URL

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

URLs permitidas

- iOS: Sim
- Android: Não
- Configuração padrão: Para obter detalhes sobre as configurações padrão, consulte a seção Interação do aplicativo (URL de saída) em [políticas MDX para aplicativos iOS](#)

Domínios Web Seguros Permitidos

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Restrições de aplicativo

Bloquear câmera

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado para iOS; Ativado para Android

Bloquear galeria

- iOS: Não
- Android: Sim
- Configuração padrão: Desativado

Bloquear Biblioteca de Fotos

- iOS: Sim
- Android: Não

- Configuração padrão: Ativado

Bloquear gravação de microfone

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Bloquear ditado

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear serviços de localização

- iOS: Sim
- Android: Sim
- Configuração padrão: Para Android: O valor padrão é Desativado para o Secure Mail. O valor padrão é Ativado para outros aplicativos.

Bloquear composição de SMS

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Bloquear captura de tela

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Bloquear sensor do dispositivo

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Bloquear NFC

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Bloquear iCloud

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear Pesquisa

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear backup de arquivo

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear AirPrint

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear Impressão

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Bloquear AirDrop

- iOS: Sim
- Android: Não

- Configuração padrão: Ativado

Bloquear anexos de arquivo

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

Bloquear composição de e-mail

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear APIs do Facebook e Twitter

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Obscurecer conteúdo da tela

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Bloquear teclados de terceiros

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

OBSERVAÇÃO

iOS 11 e posterior

Bloquear logs de aplicativos

- iOS: Sim

- Android: Sim
- Configuração padrão: Desativado

Habilitar ShareFile

- iOS:
- Android: Sim
- Configuração padrão: Ativado

Habilitar Anexar de Arquivos

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Acesso à rede do aplicativo

Acesso à rede

- iOS: Sim
- Android: Sim
- Configuração padrão: Para aplicativos recém-carregados, o padrão é **Bloqueado** para todos os aplicativos, exceto o Secure Mail. Como o Intune não tem um estado bloqueado, o padrão para o Secure Mail é **Irrestrito**.

Sessão micro VPN necessária

- iOS: Sim
- Android: Sim
- Configuração padrão: Usar Configuração Anterior. Para aplicativos recém-carregados, o valor padrão é Não.

Período de carência da sessão micro VPN necessária (minutos)

- iOS: Sim
- Android: Sim
- Configuração padrão: 0 (sem período de carência)

Lista de Exclusão

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Bloquear conexões localhost

- iOS: Não
- Android: Sim
- Configuração padrão: Desativado

Rótulo do certificado

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Logs do aplicativo

Saída de log padrão

- iOS: Sim
- Android: Sim
- Configuração padrão: arquivo

Nível de log padrão

- iOS: Sim
- Android: Sim
- Configuração padrão: 4 (mensagens informativas)

Número máximo de arquivos de log

- iOS: Sim
- Android: Sim
- Configuração padrão: 2

Tamanho máximo do arquivo de log

- iOS: Sim
- Android: Sim
- Configuração padrão: 2 MB

Redirecionar logs do aplicativo

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Criptografar logs

- iOS: Não
- Android: Sim
- Configuração padrão: Desativado

Geocerca do aplicativo

Longitude do ponto central

- iOS: Sim
- Android: Sim
- Configuração padrão: 0

Latitude do ponto central

- iOS: Sim
- Android: Sim
- Configuração padrão: 0

Raio

- iOS: Sim
- Android: Sim
- Configuração padrão: 0 (desabilitado)

NOTA:

Defina o raio em metros. Quando definido como zero, a cerca geográfica é desabilitada.

Configurações do aplicativo

Servidor Exchange do Secure Mail

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

NOTA:

Se você alterar esta política para um aplicativo existente, os usuários deverão remover e reinstalar o aplicativo para aplicar a alteração da política.

Domínio de usuário do Secure Mail

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Serviços de rede em segundo plano

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

NOTA:

Se você configurar esta política, defina a política de Acesso à rede como Tunelado para a rede interna, após o que esta política entrará em vigor. Use esta política quando o Exchange Server estiver em sua rede interna e você quiser usar o Citrix Gateway para fazer proxy da conexão com o Exchange Server interno.

Expiração do tíquete de serviços em segundo plano

- iOS: Sim
- Android: Sim
- Configuração padrão: 168 horas (7 dias)

Gateway de serviço de rede em segundo plano

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

NOTA:

Se você configurar esta política, defina a política de acesso à rede como Tunelado para a rede interna, após o que esta política entrará em vigor. Use esta política quando o Exchange Server estiver em sua rede interna ou se você quiser usar o Citrix Gateway para fazer proxy da conexão com o Exchange Server interno. Esta política entra em vigor quando você configura a política de Acesso à rede.

Exportar contatos

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Campos de contato para exportar

- iOS: Sim
- Android: Sim
- Configuração padrão: Todos

Aceitar todos os certificados SSL

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Controlar notificações da tela bloqueada

- iOS: Sim
- Android: Sim
- Configuração padrão: Permitir

Usar Conexão Segura

- iOS: Não
- Android: Sim
- Configuração padrão: Ativado

Notificação de e-mail padrão

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Intervalo de sincronização padrão

- iOS: Sim
- Android: Sim
- Configuração padrão: 3 dias

NOTA:

A configuração da política de caixa de correio do Exchange ActiveSync, Filtro de idade máxima do e-mail, tem prioridade sobre esta política. O Secure Mail exibe apenas os valores de intervalo de sincronização que são menores que o Filtro de idade máxima do e-mail.

Limite de pesquisa de e-mail

- iOS: Sim
- Android: Sim
- Configuração padrão: Ilimitado

Intervalo máximo de sincronização

- iOS: Sim
- Android: Sim
- Configuração padrão: Todos

Habilitar número da semana

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Habilitar downloads de anexos via Wi-Fi

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Permitir documentos offline

- iOS: Sim
- Android: Sim
- Configuração padrão: Ilimitado

Gerenciamento de Direitos de Informação

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Classificação de e-mail

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

Marcações de classificação de e-mail

- iOS: Sim
- Android: Não

- Configuração padrão: Vazio

Namespace de classificação de e-mail

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Versão da classificação de e-mail

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Classificação de e-mail padrão

- iOS: Sim
- Android: Não
- Configuração padrão: NÃO OFICIAL

Habilitar salvamento automático de rascunhos de e-mail

- iOS: Sim
- Android: Sim
- Configuração padrão: Ativado

Habilitar proteção de dados do iOS

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

Nome do Host EWS para Notificações Push

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Notificações push

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

Região de notificações push

- iOS: Sim
- Android: Não
- Configuração padrão: Américas

Habilitar S/MIME durante a primeira inicialização do Secure Mail

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

Mecanismo de autenticação inicial

- iOS: Sim
- Android: Sim
- Configuração padrão: Usar endereço de servidor de e-mail fornecido pelo MDX

Credenciais de autenticação inicial

- iOS: Sim
- Android: Sim
- Configuração padrão: Nome de usuário de registro

Habilitar número da semana

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Opções de Web e Áudio do Calendário

- iOS: Sim
- Android: Sim

- Configuração padrão: GoToMeeting e Inserido pelo Usuário

Origem do certificado público S/MIME

- iOS: Sim
- Android: Sim
- Configuração padrão: Exchange

Endereço do servidor LDAP

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

DN Base do LDAP

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Acessar LDAP anonimamente

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Domínios de e-mail permitidos

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

NOTA

Se vazio, não restringe domínios.

Tentar Migração de Nome de Usuário na Falha de Autenticação

- iOS: Sim

- Android: Sim
- Configuração padrão: Desativado

Relatar Endereços de E-mail de Phishing

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Mecanismo de Relatório de Phishing

- iOS: Não
- Android: Sim
- Configuração padrão: Relatar via anexo (.eml)

Domínios de Reunião do Skype for Business

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Exportar calendário

- iOS: Sim
- Android: Sim
- Configuração padrão: Horário da reunião

Habilitar Slack

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Nome do espaço de trabalho do Slack

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Identificação de chamadas

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

NOTA:

Se Ativado, o Secure Mail fornece ao iOS nomes e números de telefone dos seus contatos salvos para identificação de chamadas.

Análise

Habilitar Google Analytics

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Nível de detalhe do Google Analytics

- iOS: Sim
- Android: Sim
- Configuração padrão: Completo

Relatórios

Relatórios Citrix

- iOS: Sim
- Android: Não
- Configuração padrão: Desativado

NOTA:

A Citrix também pode controlar este recurso com um sinalizador de recurso. Tanto o sinalizador de recurso quanto esta política devem estar ativados para que este recurso funcione.

Token de upload

- iOS: Sim
- Android: Não
- Configuração padrão: Vazio

Enviar relatórios somente por Wi-Fi

- iOS: Sim
- Android: Não
- Configuração padrão: Ativado

Máximo de cache de arquivo de relatório

- iOS: Sim
- Android: Não
- Configuração padrão: 2 MB

Suporte OAuth para Office 365

Usar autenticação moderna para Office 365

- iOS: Não
- Android: Sim
- Configuração padrão: Desativado

Mecanismo de autenticação do Office 365

- iOS: Sim
- Android: Não
- Configuração padrão: Não usar OAuth

Nomes de host confiáveis do Exchange Online

- iOS: Sim
- Android: Sim
- Configuração padrão: outlook.office365.com

Nomes de host AD FS confiáveis

- iOS: Sim
- Android: Sim
- Configuração padrão: `login.microsoftonline.com`

Agente de usuário personalizado para autenticação moderna

- iOS: Não
- Android: Sim
- Configuração padrão: Vazio

NOTA:

Se você não configurar esta política, o agente de usuário padrão do Secure Mail será usado durante a autenticação moderna.

Redirecionamento de e-mail

Redirecionamento de e-mail

- iOS: Sim
- Android: Não
- Configuração padrão: Secure Mail

Integração com o Slack

Habilitar Slack

- iOS: Sim
- Android: Sim
- Configuração padrão: Desativado

Nome do espaço de trabalho do Slack

- iOS: Sim
- Android: Sim
- Configuração padrão: Vazio

Políticas MDX para aplicativos de produtividade móvel para Android

Este artigo descreve as políticas MDX para aplicativos Android. Você altera as configurações da política no console do Citrix Endpoint Management. Para obter detalhes, consulte [Adicionar aplicativos](#).

A lista a seguir não inclui políticas MDX específicas para o Secure Web. Para obter detalhes sobre as políticas que aparecem para o Secure Web, consulte [Políticas do Secure Web](#).

Autenticação

Senha do aplicativo

Se **Ativado**, um PIN ou código de acesso é necessário para desbloquear o aplicativo quando ele inicia ou é retomado após um período de inatividade. O valor padrão é **Ativado**.

Para configurar o temporizador de inatividade para todos os aplicativos, defina o valor de INACTIVITY_TIMER em minutos em **Propriedades do Cliente** na guia **Configurações**. O valor padrão do temporizador de inatividade é de 60 minutos. Para desativar o temporizador de inatividade, de modo que um prompt de PIN ou código de acesso apareça apenas quando o aplicativo iniciar, defina o valor como zero.

NOTA:

Se você selecionar Offline seguro para a política de chaves de criptografia, esta política será habilitada automaticamente.

Período máximo offline (horas)

Define o período máximo que um aplicativo pode ser executado offline sem um logon de rede para reconfirmar o direito e atualizar as políticas. O valor padrão é **168 horas** (7 dias). O período mínimo é de 1 hora.

O usuário é lembrado de fazer logon 30, 15 e 5 minutos antes do período expirar. Após a expiração, o aplicativo permanece bloqueado até que o usuário conclua um logon de rede bem-sucedido.

Citrix Gateway Alternativo

NOTA:

O nome desta política no console do Endpoint Management é **Alternate NetScaler® Gateway**.

Endereço de um Citrix Gateway alternativo específico (anteriormente, NetScaler Gateway) que é usado para autenticação e para sessões de micro VPN com este aplicativo. **Alternate NetScaler Gateway** é uma política opcional que, quando usada com a política de sessão online obrigatória, força os aplicativos a se reautenticarem no gateway específico. Esses gateways normalmente teriam requisitos de autenticação e políticas de gerenciamento de tráfego diferentes (com maior garantia). Se deixado em branco, o padrão do servidor é sempre usado. O valor padrão é vazio.

Segurança do Dispositivo

Bloquear dispositivos com jailbreak ou root

Se **Ativado**, o aplicativo é bloqueado quando o dispositivo tem jailbreak ou root. Se **Desativado**, o aplicativo pode ser executado mesmo que o dispositivo tenha jailbreak ou root. O valor padrão é **Ativado**.

Exigir criptografia do dispositivo

Se **Ativado**, o aplicativo é bloqueado se o dispositivo não tiver criptografia configurada. Se **Desativado**, o aplicativo pode ser executado mesmo que o dispositivo não tenha criptografia configurada. O valor padrão é **Desativado**.

NOTA:

Esta política é compatível apenas com Android 3.0 (Honeycomb). Definir a política como **Ativado** impede que um aplicativo seja executado em versões mais antigas.

Exigir bloqueio do dispositivo

Se **PIN ou senha do dispositivo** for selecionado, o aplicativo será bloqueado se o dispositivo não tiver um PIN ou senha. Se **Bloqueio de tela por padrão do dispositivo** for selecionado, o aplicativo será bloqueado se o dispositivo não tiver um bloqueio de tela por padrão definido. Se **Desativado**, o aplicativo pode ser executado mesmo que o dispositivo não tenha um PIN, senha ou bloqueio de tela por padrão definido. O valor padrão é **Desativado**.

PIN ou senha do dispositivo exige uma versão mínima do Android 4.1 (Jelly Bean). Definir a política como **PIN ou senha do dispositivo** impede que um aplicativo seja executado em versões mais antigas.

Em dispositivos Android M, as opções **PIN ou senha do dispositivo** e **Bloqueio de tela por padrão do dispositivo** têm o mesmo efeito: Com qualquer uma dessas opções, o aplicativo é bloqueado se o dispositivo não tiver um PIN, senha ou bloqueio de tela por padrão definido.

Requisitos de Rede

Exigir Wi-Fi

Se **Ativado**, o aplicativo é bloqueado quando o dispositivo não está conectado a uma rede Wi-Fi. Se **Desativado**, o aplicativo pode ser executado se o dispositivo tiver uma conexão ativa, como 4G/3G, LAN ou Wi-Fi. O valor padrão é **Desativado**.

Redes Wi-Fi Permitidas

Lista de redes Wi-Fi permitidas, delimitada por vírgulas. Se o nome da rede contiver caracteres não alfanuméricos (incluindo vírgulas), o nome deverá ser colocado entre aspas duplas. O aplicativo só será executado se estiver conectado a uma das redes listadas. Se deixado em branco, todas as redes serão permitidas. Este valor não afeta as conexões a redes celulares. O valor padrão é em branco.

Acesso Diverso

Período de carência para atualização do aplicativo (horas)

Define o período de carência durante o qual um aplicativo pode ser usado depois que o sistema descobre que uma atualização do aplicativo está disponível. O valor padrão é **168 horas** (7 dias).

NOTA:

Não é recomendado usar zero, pois isso impede imediatamente que um aplicativo em execução seja usado até que a atualização seja baixada e instalada (sem qualquer aviso ao usuário). Esse valor pode levar a uma situação em que o usuário que executa o aplicativo é forçado a sair do aplicativo (potencialmente perdendo trabalho) para cumprir a atualização necessária.

Desabilitar atualização obrigatória

Desabilita a exigência de que os usuários atualizem para a versão mais recente do aplicativo na App Store. O valor padrão é **ATIVADO**.

Apagar dados do aplicativo ao bloquear

Apaga os dados e redefine o aplicativo quando ele é bloqueado. Se **Desativado**, os dados do aplicativo não são apagados quando o aplicativo é bloqueado. O valor padrão é **Desativado**.

Um aplicativo pode ser bloqueado por qualquer um dos seguintes motivos:

- Perda de direito de uso do aplicativo para o usuário
- Assinatura do aplicativo removida
- Conta removida
- Secure Hub desinstalado
- Muitas falhas de autenticação do aplicativo
- Dispositivo com jailbreak detectado (conforme configuração da política)
- Dispositivo colocado em estado bloqueado por outra ação administrativa

Período de sondagem ativa (minutos)

Quando um aplicativo é iniciado, a estrutura MDX consulta o Citrix Endpoint Management para determinar o status atual do aplicativo e do dispositivo. Supondo que o servidor que executa o Endpoint Management possa ser alcançado, a estrutura retorna informações sobre o status de bloqueio/limpeza do dispositivo e o status de ativação/desativação do aplicativo.

Independentemente de o servidor poder ser alcançado ou não, uma sondagem subsequente é agendada com base no intervalo do período de sondagem ativa. Após o término do período, uma nova sondagem é tentada novamente. O valor padrão é **60 minutos** (1 hora).

IMPORTANTE:

Defina este valor como menor apenas para aplicativos de alto risco, caso contrário, o desempenho poderá ser afetado.

Criptografia

Tipo de criptografia

Permite escolher se o MDX ou a plataforma do dispositivo lida com a criptografia de dados. Se você selecionar **Criptografia MDX**, o MDX criptografa os dados. Se você selecionar **Criptografia de plataforma com imposição de conformidade**, a plataforma do dispositivo criptografa os dados. O valor padrão é **Criptografia MDX**.

Comportamento de dispositivo não compatível

Permite escolher uma ação quando um dispositivo não adere aos requisitos mínimos de conformidade de criptografia. Selecione **Permitir aplicativo** para que o aplicativo seja executado normalmente. Selecione **Permitir aplicativo após aviso** para que o aplicativo seja executado após o aviso aparecer. Selecione **Bloquear** para impedir que o aplicativo seja executado. O valor padrão é **Permitir aplicativo após aviso**.

Chaves de criptografia

Permite que segredos usados para derivar chaves de criptografia sejam persistidos no dispositivo. A única opção disponível é o acesso offline permitido.

A Citrix recomenda que você defina a política de Autenticação para habilitar um logon de rede ou um desafio de senha offline para proteger o acesso ao conteúdo criptografado.

Criptografia de arquivo privado

Controla a criptografia de arquivos de dados privados nos seguintes locais: /data/data/<appname> e /mnt/sdcard/Android/data/<appname>.

A opção **Desabilitado** significa que os arquivos privados não são criptografados. A opção **SecurityGroup** criptografa arquivos privados usando uma chave compartilhada por todos os aplicativos MDX no mesmo grupo de segurança. A opção **Application** criptografa arquivos privados usando uma chave exclusiva para este aplicativo. O valor padrão é **SecurityGroup**.

Exclusões de criptografia de arquivo privado

Contém uma lista de caminhos de arquivo separados por vírgulas. Cada caminho é uma expressão regular que representa um ou mais arquivos que são criptografados. Os caminhos de arquivo são relativos aos sandboxes internos e externos. O valor padrão é vazio.

As exclusões se aplicam apenas às seguintes pastas:

- **Armazenamento Interno:**

```
/data/data/<your_package_name>
```

- **Cartão SD:**

```
/storage/emulated/\<SD Card Slot>/Android/data/<your_package_name>
```

```
/storage/emulated/legacy/Android/data/<your_package_name>
```

Exemplos

ARQUIVO A SER EXCLUÍDO	VALOR NA EXCLUSÃO DE CRIPTOGRAFIA DE ARQUIVO PRIVADO
/data/data/com.citrix.mail/files/a.txt	^files/a.txt
Todos os arquivos de texto em /storage/emulated/0/Android/data/com.citrix.mail/files	^files/(.)+.txt\$
Todos os arquivos em /data/data/com.citrix.mail/files	^arquivos/

Limites de acesso para arquivos públicos

Contém uma lista separada por vírgulas. Cada entrada é um caminho de expressão regular seguido por (NA), (RO) ou (RW). Os arquivos que correspondem ao caminho são limitados a acesso de **Sem Acesso**, **Somente Leitura** ou **Leitura e Gravação**. A lista é processada em ordem e o primeiro caminho correspondente é usado para definir o limite de acesso. O valor padrão é vazio.

Esta política é aplicada somente quando a **criptografia de arquivo público está ativada** (alterada da opção **Desativar** para a opção **SecurityGroup** ou **Aplicativo**). Esta política é aplicável apenas a arquivos públicos existentes e não criptografados e especifica quando esses arquivos são criptografados.

ARQUIVOS A SEREM EXCLUÍDOS	VALOR NA CRIPTOGRAFIA DE ARQUIVO PRIVADO
Pasta Downloads no armazenamento externo somente leitura	EXT:^Download/(RO)
Todos os arquivos MP3 na pasta Música no armazenamento virtual sem acesso	VS:^Music/(.)+.mp3\$(NA)

Criptografia de arquivo público

Controla a criptografia de arquivos públicos. Se **Desativado**, os arquivos públicos não são criptografados. Se **SecurityGroup**, criptografa arquivos públicos usando uma chave compartilhada por todos os aplicativos MDX no mesmo grupo de segurança. Se **Application**, criptografa arquivos públicos usando uma chave exclusiva para este aplicativo.

O valor padrão é **SecurityGroup**.

Exclusões de criptografia de arquivo público

Contém uma lista de caminhos de arquivo separados por vírgulas. Cada caminho é uma expressão regular que representa um ou mais arquivos que não são criptografados. Os caminhos de arquivo são relativos ao armazenamento externo padrão e a qualquer armazenamento externo específico do dispositivo.

As exclusões de criptografia de arquivo público incluem apenas locais de pastas externas.

Exemplos

ARQUIVO A SER EXCLUÍDO	VALOR NA EXCLUSÃO DE CRIPTOGRAFIA DE ARQUIVO PÚBLICO
Pasta Downloads no cartão SD	Download
Todos os arquivos MP3 na pasta Música	^Music/(.)+.mp3\$

Migração de arquivo público

Esta política é aplicada apenas quando você habilita a política de criptografia de arquivo público (alterada de **Desativado** para **SecurityGroup** ou **Application**). Esta política é aplicável apenas a arquivos públicos existentes e não criptografados e especifica quando esses arquivos são criptografados. O valor padrão é **Gravar (RO/RW)**.

A opção **Desativado** significa que os arquivos existentes não são criptografados. A opção **Gravar (Somente Leitura/Leitura e Gravação)** criptografa os arquivos existentes somente quando são abertos para acesso somente gravação ou leitura e gravação. A opção **Qualquer** criptografa os arquivos existentes quando são abertos em qualquer modo. Opções:

- **Desativado**. Não criptografa arquivos existentes.
- **Gravar (Somente Leitura/Leitura e Gravação)**. Criptografa os arquivos existentes somente quando são abertos para acesso somente gravação ou leitura e gravação.
- **Qualquer**. Criptografa os arquivos existentes quando são abertos em qualquer modo.

OBSERVAÇÕES:

-Novos arquivos ou arquivos existentes não criptografados que são sobrescritos criptografam os arquivos de substituição em todos os casos. -A criptografia de um arquivo público existente torna o arquivo indisponível para outros aplicativos que não possuem a mesma chave de criptografia.

Interação do Aplicativo

Grupo de Segurança

Deixe este campo em branco se quiser que todos os aplicativos móveis gerenciados pelo Citrix Endpoint Management™ troquem informações entre si. Defina um nome de grupo de segurança para gerenciar as configurações de segurança para conjuntos específicos de aplicativos (por exemplo, Finanças ou Recursos Humanos).

CUIDADO:

Se você alterar esta política para um aplicativo existente, os usuários deverão excluir e reinstalar o aplicativo para aplicar a alteração da política.

Recortar e Copiar

Bloqueia, permite ou restringe as operações de recortar e copiar da área de transferência para este aplicativo. Se **Restrito**, os dados copiados da Área de Transferência são colocados em uma Área de Transferência privada que está disponível apenas para aplicativos MDX. O valor padrão é **Restrito**.

Colar

Bloqueia, permite ou restringe as operações de colar da área de transferência para o aplicativo. Se **Restrito**, os dados colados da área de transferência são originados de uma Área de Transferência privada que está disponível apenas para aplicativos MDX. O valor padrão é **Não Restrito**.

Troca de documentos (Abrir em)

Bloqueia, permite ou restringe as operações de troca de documentos para o aplicativo. Se **Restrito**, os documentos podem ser trocados apenas com outros aplicativos MDX e as exceções de aplicativo especificadas na política de lista de exceções de Abrir em Restrito. Se **Não Restrito**,

defina as políticas de Criptografia de arquivo privado e Criptografia de arquivo público como **Desabilitado** para que os usuários possam abrir documentos em aplicativos não encapsulados. O valor padrão é **Restrito**.

Domínios de URL excluídos da filtragem

Esta política é usada para excluir certas URLs de saída da filtragem MDX. A seguinte lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou sufixos DNS é excluída de qualquer filtragem MDX. Se esta política contiver alguma entrada, as URLs com campos de host que correspondem a pelo menos um item na lista (por meio de correspondência de sufixo DNS) são enviadas inalteradas para o navegador padrão. O valor padrão é vazio.

Domínios da Web Segura Permitidos

Esta política está em vigor apenas para os domínios não excluídos por uma política de filtragem de URL. Adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou sufixos DNS que são redirecionados para o aplicativo Secure Web quando a Troca de Documentos é Restrita.

Se esta política contiver alguma entrada, somente as URLs com campos de host que correspondem a pelo menos um item na lista (por meio de correspondência de sufixo DNS) são redirecionadas para o aplicativo Secure Web quando a Troca de Documentos é Restrita.

Todas as outras URLs são enviadas para o navegador da web Android padrão (ignorando a política de Troca de Documentos Restrita). O valor padrão é vazio.

Lista de exceções de Abrir em Restrito

Quando a política de troca de documentos (Abrir em) é **Restrita**, esta lista de intents do Android tem permissão para passar para aplicativos não gerenciados. É necessário ter familiaridade com os intents do Android para adicionar filtros à lista. Um filtro pode especificar ação, pacote, esquema ou qualquer combinação.

Exemplos

```
{action=android.intent.action.MAIN}

{package=com.sharefile.mobile}

{action=android.intent.action.DIAL scheme=tel}
```

```
{action=android.intent.action.VIEW scheme=msteams  
package=com.microsoft.teams}
```

Cuidado

Certifique-se de considerar as implicações de segurança desta política. A lista de exceções permite que o conteúdo transite entre aplicativos não gerenciados e o ambiente MDX.

Troca de documentos de entrada (Abrir em)

Bloqueia, restringe ou permite operações de troca de documentos de entrada para este aplicativo. Se **Restrito**, os documentos podem ser trocados apenas com outros aplicativos MDX. O valor padrão é **Não Restrito**.

Se **Bloqueado** ou **Restrito**, você pode usar a política de lista de permissões de troca de documentos de entrada para especificar aplicativos que podem enviar documentos para este aplicativo. Para obter informações sobre outras interações de política, consulte a política Bloquear Galeria.

Opções: **Não Restrito**, **Bloqueado** ou **Restrito**

Lista de permissões de troca de documentos de entrada

Quando a política de troca de documentos de entrada é restrita ou bloqueada, esta lista de IDs de aplicativos separada por vírgulas, incluindo aplicativos não-MDX, tem permissão para enviar documentos para o aplicativo. Esta política está oculta e não pode ser editada.

Nível de segurança da conexão

Determina a versão mínima de TLS/SSL usada para conexões. Se **TLS**, as conexões suportam todos os protocolos TLS. Se **SSLv3 e TLS**, as conexões suportam SSL 3.0 e TLS. O valor padrão é **TLS**.

Restrições de Aplicativo

IMPORTANTE:

Certifique-se de considerar as implicações de segurança das políticas que impedem que os aplicativos acessem ou usem os recursos do telefone. Quando essas políticas estão **Desativadas**, o conteúdo pode transitar entre aplicativos não gerenciados e o ambiente seguro.

Bloquear câmera

Se **Ativado**, impede que um aplicativo use diretamente o hardware da câmera. O valor padrão é **Ativado**.

Bloquear Galeria

Se **Ativado**, impede que um aplicativo acesse a Galeria no dispositivo. O valor padrão é **Desativado**. Esta política funciona em conjunto com a política de troca de documentos de entrada (Abrir em).

- Se a troca de documentos de entrada (Abrir em) estiver definida como **Restrito**, os usuários que trabalham no aplicativo gerenciado não poderão anexar imagens da Galeria, independentemente da configuração de Bloquear Galeria.
- Se a troca de documentos de entrada (Abrir em) estiver definida como **Não Restrito**, os usuários que trabalham no aplicativo gerenciado experimentarão o seguinte:
 - Os usuários podem anexar imagens se Bloquear Galeria estiver definido como **Desativado**.
 - Os usuários são impedidos de anexar imagens se Bloquear Galeria estiver **Ativado**.

Bloquear gravação de microfone

Se **Ativado**, impede que um aplicativo use diretamente o hardware do microfone. O valor padrão é **Ativado**.

Bloquear serviços de localização

Se **Ativado**, impede que um aplicativo use os componentes dos serviços de localização (GPS ou rede). O valor padrão é **Desativado** para o Secure Mail.

Bloquear composição de SMS

Se **Ativado**, impede que um aplicativo use o recurso de composição de SMS para enviar mensagens SMS/de texto do aplicativo. O valor padrão é **Ativado**.

Bloquear captura de tela

Se **Ativado**, impede que os usuários capturem a tela enquanto o aplicativo está em execução. Além disso, quando o usuário troca de aplicativo, a tela do aplicativo é obscurecida. O valor padrão é **Ativado**.

Ao usar o recurso Near Field Communication (NFC) do Android, alguns aplicativos tiram uma captura de tela de si mesmos antes de transmitir o conteúdo. Para habilitar esse recurso em um aplicativo encapsulado, altere a política **Bloquear captura de tela** para **Desativado**.

Bloquear sensor do dispositivo

Se **Ativado**, impede que um aplicativo use os sensores do dispositivo (como acelerômetro, sensor de movimento e giroscópio). O valor padrão é **Ativado**.

Bloquear NFC

Se **Ativado**, impede que um aplicativo use o Near Field Communications (NFC). O valor padrão é **Ativado**.

Bloquear logs de aplicativos

Se **Ativado**, proíbe um aplicativo de usar o recurso de registro de diagnóstico do aplicativo de produtividade móvel. Se **Desativado**, os logs do aplicativo são registrados e podem ser coletados usando o recurso de suporte por e-mail do Secure Hub. O valor padrão é **Desativado**.

Bloquear impressão

Se **Ativado**, impede que um aplicativo imprima dados. Se um aplicativo tiver um comando Compartilhar, você deve definir a Troca de Documentos (Abrir em) como **Restrito** ou **Bloqueado** para bloquear a impressão completamente. O valor padrão é **ATIVADO**.

Habilitar ShareFile

Permite que os usuários usem o ShareFile para transferir arquivos. O valor padrão é **ATIVADO**.

Acesso à Rede do Aplicativo

Acesso à rede

NOTA:

Tunneled - Web SSO é o nome para **Secure Browse** nas configurações. O comportamento é o mesmo.

As opções de configuração são as seguintes:

- **Usar Configurações Anteriores:** Retorna aos valores que você havia definido nas políticas anteriores. Se você alterar esta opção, não deve reverter para ela. Observe também que as alterações nas novas políticas não entram em vigor até que o usuário atualize o aplicativo para a versão 18.12.0 ou posterior.
- **Bloqueado:** As APIs de rede usadas pelo seu aplicativo falham. Conforme a diretriz anterior, você deve manipular tal falha de forma elegante.
- **Irrestrito:** Todas as chamadas de rede vão diretamente e não são tuneladas.
- **Tunelado - VPN Completa:** Todo o tráfego do aplicativo gerenciado é tunelado através do Citrix Gateway.
- **Tunneled - Web SSO:** A URL HTTP/HTTPS é reescrita. Esta opção permite apenas o tunelamento de tráfego HTTP e HTTPS. Uma vantagem significativa de **Tunneled - Web SSO** é o logon único (SSO) para tráfego HTTP e HTTPS e também a autenticação PKINIT. No Android, esta opção tem baixa sobrecarga de configuração e, portanto, é a opção preferida para operações de navegação na web.

Se um dos **modos Tunneled** for selecionado, um túnel VPN por aplicativo neste modo inicial é criado de volta para a rede corporativa. Aqui, as configurações de túnel dividido do Citrix Gateway são usadas. A Citrix recomenda **Tunneled Full VPN** para conexões que empregam certificados de cliente ou SSL de ponta a ponta para um recurso na rede corporativa. A Citrix recomenda **Tunneled - Web SSO** para conexões que exigem logon único (SSO).

Sessão Micro VPN necessária

Se **Sim**, o usuário deve ter uma conexão com a rede corporativa e uma sessão ativa. Se **Não**, uma sessão ativa não é necessária. O valor padrão é **Usar Configuração Anterior**. Para aplicativos recém-carregados, o valor padrão é **Não**. Qualquer configuração selecionada antes da

atualização para esta política permanece em vigor até que uma opção diferente de **Usar Configuração Anterior** seja selecionada.

Lista de Exclusão

Lista de FQDNs ou sufixos DNS separados por vírgulas a serem acessados diretamente em vez de por meio de uma conexão VPN. Esta política se aplica apenas ao modo **Tunneled - Web SSO** quando o Citrix Gateway está configurado com o modo reverso de túnel dividido.

Bloquear conexões localhost

Se **Ativado**, os aplicativos não têm permissão para fazer conexões localhost. Localhost é um endereço (como 127.0.0.1) para comunicações que ocorrem localmente no dispositivo. O localhost ignora o hardware da interface de rede local e acessa os serviços de rede em execução no host. Se **Desativado**, esta política substitui a política de Acesso à Rede, o que significa que os aplicativos podem se conectar fora do contêiner seguro se o dispositivo estiver executando um servidor proxy localmente. O padrão é **Desativado**.

Rótulo do certificado

Quando usado com o serviço de integração de certificado StoreFront™, este rótulo identifica o certificado específico necessário para este aplicativo. Se nenhum rótulo for fornecido, um certificado não será disponibilizado para uso com uma infraestrutura de chave pública (PKI). O valor padrão é vazio (nenhum certificado usado).

Logs do aplicativo

Saída de log padrão

Determina quais meios de saída são usados pelas instalações de registro de diagnóstico de aplicativos do Citrix Endpoint Management por padrão. As possibilidades são arquivo, console ou ambos. O valor padrão é arquivo.

Nível de log padrão

Controla a verbosidade padrão da instalação de registro de diagnóstico de aplicativos de produtividade móvel. Números de nível superior incluem registro mais detalhado.

- 0 - Nada registrado
- 1 - Erros críticos
- 2 - Erros
- 3 - Avisos

- 4 - Mensagens informativas
- 5 - Mensagens informativas detalhadas
- 6 a 15 - Níveis de depuração de 1 a 10

O valor padrão é o nível **4** (Mensagens informativas).

Número máximo de arquivos de log

Limita o número de arquivos de log retidos pelo recurso de registro de diagnóstico do aplicativo de produtividade móvel antes de serem substituídos. O mínimo é **2**. O máximo é **8**. O valor padrão é **2**.

Tamanho máximo do arquivo de log

Limita o tamanho em MB dos arquivos de log retidos pelo recurso de registro de diagnóstico do aplicativo de produtividade móvel antes de serem substituídos. O mínimo é **1** MB. O máximo é **5** MB. O valor padrão é **2** MB.

Redirecionar logs do aplicativo

Se **Ativado**, intercepta e redireciona logs do sistema ou do console de um aplicativo para o recurso de diagnóstico do aplicativo de produtividade móvel. Se esta configuração estiver **Desativada**, o uso de logs do sistema ou do console pelo aplicativo não é interceptado. O valor padrão é **Ativado**.

Criptografar logs

Se **Ativado**, o Citrix Endpoint Management criptografa os logs de diagnóstico à medida que os registra. Se **Desativado**, os logs de diagnóstico permanecem não criptografados na sandbox do aplicativo.

CUIDADO:

Dependendo dos níveis de log configurados, a criptografia de log pode ter um impacto notável no desempenho do aplicativo e na vida útil da bateria.

O valor padrão é **Desativado**.

Cerca Geográfica do Aplicativo

Longitude do ponto central

Longitude (coordenada X) do ponto central da cerca geográfica de ponto/raio na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado. O valor deve ser expresso no formato de graus com sinal (DDD.dddd), por exemplo "-31.9635". As longitudes oeste devem ser precedidas por um sinal de menos. O valor padrão é **0**.

Latitude do ponto central

Latitude (coordenada Y) do ponto central da cerca geográfica de ponto/raio na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado.

Os valores devem ser expressos no formato de graus com sinal (DDD.dddd), por exemplo "43.06581". As latitudes sul devem ser precedidas por um sinal de menos. O valor padrão é **0**.

Raio

O raio da cerca geográfica na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado. O valor deve ser expresso em metros. Quando definido como zero, a cerca geográfica é desativada. O padrão é 0 (desativado).

Análises

Detalhe do Google Analytics

A Citrix coleta dados de análise para melhorar a qualidade do produto. A seleção de Anônimo o exclui da inclusão de informações identificáveis da empresa.

Configurações do Aplicativo

Servidor Exchange do Secure Mail

O nome de domínio totalmente qualificado (FQDN) para o Exchange Server ou, somente para iOS, o servidor IBM Notes Traveler. O valor padrão é vazio. Se você fornecer um nome de domínio neste campo, os usuários não poderão editá-lo. Se você deixar o campo vazio, os usuários fornecerão suas próprias informações de servidor.

CUIDADO:

Se você alterar esta política para um aplicativo existente, os usuários deverão excluir e reinstalar o aplicativo para aplicar a alteração da política.

Domínio de usuário do Secure Mail

Nome de domínio padrão do Active Directory para usuários do Exchange ou, somente para iOS, usuários do Notes. O valor padrão é vazio.

Serviços de rede em segundo plano

O FQDN e a porta dos endereços de serviço permitidos para acesso à rede em segundo plano. Este valor pode ser um Exchange Server ou um servidor ActiveSync, seja em sua rede interna ou em outra rede à qual o Secure Mail se conecta, como mail.example.com:443.

Se você configurar esta política, defina a política de acesso à rede como **Tunelado para a rede interna**. Esta política entra em vigor quando você configura a política de acesso à rede. Use esta política quando o Exchange Server residir em sua rede interna e você quiser usar o NetScaler Gateway para fazer proxy da conexão com o Exchange Server interno.

O valor padrão é vazio, o que implica que os serviços de rede em segundo plano não estão disponíveis.

Expiração do tíquete de serviços em segundo plano

Período de tempo durante o qual um tíquete de serviço de rede em segundo plano permanece válido. Após a expiração, será necessário um logon corporativo para renovar o tíquete. O valor padrão é de **168 horas** (7 dias).

Gateway de serviço de rede em segundo plano

Endereço de gateway alternativo a ser usado para serviços de rede em segundo plano, no formato FQDN:porta. Este endereço é o FQDN e o número da porta do Citrix Gateway que o Secure Mail usa para se conectar ao Exchange Server interno. No utilitário de configuração do Citrix Gateway, você deve configurar a Secure Ticket Authority (STA) e vincular a política ao servidor virtual.

O valor padrão está vazio, o que implica que um gateway alternativo não existe.

Se você configurar esta política, defina a política de acesso à rede como **Tunneled to the internal network**. Esta política entra em vigor quando você configura a política de acesso à rede. Use esta

política quando o Exchange Server residir em sua rede interna e você quiser usar o Citrix Gateway para fazer proxy da conexão com o Exchange Server interno.

Exportar contatos

IMPORTANTE:

Não habilite este recurso se os usuários puderem acessar seu Exchange Server diretamente (ou seja, fora do Citrix Gateway). Caso contrário, os contatos serão duplicados no dispositivo e no Exchange.

Se **Off**, impede a sincronização unidirecional dos contatos do Secure Mail para o dispositivo e impede o compartilhamento de contatos do Secure Mail (como vCards). O valor padrão é **Off**.

Campos de contato para exportar

Controla os campos de contato a serem exportados para o catálogo de endereços. Se **All**, todos os campos de contato são exportados. Se **Name and Phone**, todos os campos de contato relacionados a nome e telefone são exportados. Se **Name, Phone and Email**, todos os campos de contato relacionados a nome, telefone e e-mail são exportados. O valor padrão é **All**.

Aceitar todos os certificados SSL

Se **On**, o Secure Mail aceita todos os certificados SSL (válidos ou não) e permite o acesso. Se **Off**, o Secure Mail bloqueia o acesso quando ocorre um erro de certificado e exibe um aviso. O valor padrão é **Off**.

Usar conexão segura

Se **On**, o Secure Mail usa uma Conexão Segura. Se **Off**, o Secure Mail não usa uma Conexão Segura. O padrão é **On**.

Gerenciamento de Direitos de Informação

Se **On**, o Secure Mail oferece suporte aos recursos de Gerenciamento de Direitos de Informação (IRM) do Exchange. O valor padrão é **Off**.

Controlar notificações da tela bloqueada

Controla se as notificações de e-mail e calendário aparecem na tela de um dispositivo bloqueado. Se **Permitir** for selecionado, todas as informações contidas na notificação aparecem. Se **Bloquear** for selecionado, as notificações não aparecem. Se **Remetente do e-mail ou título do evento** for selecionado, apenas o nome do remetente do e-mail ou o título do evento do

calendário aparece. Se **Somente contagem** for selecionado, apenas a contagem de e-mails e convites de reunião, mais a hora dos lembretes de calendário, aparecem. O valor padrão é **Permitir**.

Intervalo de sincronização padrão

Especifica o intervalo de sincronização padrão para o Secure Mail. Os usuários do Secure Mail podem alterar o padrão.

A configuração de política **Caixa de correio do Exchange ActiveSync Filtro de idade máxima do e-mail** tem prioridade sobre esta política. Se você especificar um Intervalo de sincronização padrão que seja maior do que o filtro de idade máxima do e-mail, a configuração do filtro **Idade máxima do e-mail** será usada em vez disso. O Secure Mail exibe apenas os valores de intervalo de sincronização que são menores do que a configuração do filtro **Idade máxima do e-mail do Active Sync**.

O valor padrão é **3 dias**.

Habilitar download de anexos por Wi-Fi

Se **Ativado**, a opção Baixar anexos do Secure Mail é habilitada para que os usuários possam, por padrão, baixar anexos por redes Wi-Fi internas. Se **Desativado**, a opção Baixar anexos do Secure Mail é desabilitada para que, por padrão, os usuários não possam baixar anexos por Wi-Fi. O valor padrão é **Desativado**.

Permitir documentos offline

Especifica se, e por quanto tempo, os usuários podem armazenar documentos offline em dispositivos. O valor padrão é **Ilimitado**.

Habilitar salvamento automático de rascunhos de e-mail

Se **Ativado**, o Secure Mail oferece suporte ao salvamento automático de mensagens na pasta **Rascunhos**. O valor padrão é **Ativado**.

Mecanismo de autenticação inicial

Esta política indica se o endereço do servidor de e-mail fornecido pelo MDX é usado para preencher o campo **Endereço** na tela de provisionamento de primeiro uso ou se o endereço de e-mail do usuário é usado. O valor padrão é **Endereço do servidor de e-mail**.

Credenciais de autenticação iniciais

Esta política define o valor que deve ser escolhido como nome de usuário para preencher a tela de provisionamento inicial de primeiro uso. O valor padrão é **Nome de usuário de inscrição**.

Habilitar número da semana

Se **Ativado**, as visualizações do calendário incluem o número da semana. O valor padrão é **Desativado**.

Classificação de e-mail

Se **Ativado**, o Secure Mail oferece suporte a marcações de classificação de e-mail para SEC (segurança) e DLM (marcadores de limitação de disseminação). As marcações de classificação aparecem nos cabeçalhos de e-mail como **valores X-Protective-Marking**. Certifique-se de configurar as políticas de classificação de e-mail relacionadas. O valor padrão é **Desativado**.

Marcações de classificação de e-mail

Especifica as marcações de classificação a serem disponibilizadas aos usuários finais. Se a lista estiver vazia, o Secure Mail não incluirá uma lista de marcações de proteção. A lista de marcações contém pares de valores separados por ponto e vírgula. Cada par inclui o valor que aparece no Secure Mail e o valor da marcação que é o texto anexado ao assunto e cabeçalho do e-mail no Secure Mail. Por exemplo, no par de marcação `"UNOFFICIAL, SEC=UNOFFICIAL;"`, o valor da lista é **"UNOFFICIAL"** e o valor da marcação é **"SEC=UNOFFICIAL"**.

Namespace de classificação de e-mail

Especifica o namespace de classificação que é exigido no cabeçalho do e-mail pelo padrão de classificação usado. Por exemplo, o namespace "gov.au" aparece no cabeçalho como "NS=gov.au". O valor padrão é vazio.

Versão de classificação de e-mail

Especifica a versão de classificação que é exigida no cabeçalho do e-mail pelo padrão de classificação usado. Por exemplo, a versão "2012.3" aparece no cabeçalho como "VER=2012.3". O valor padrão é vazio.

Classificação de e-mail padrão

Especifica a marcação de proteção que o Secure Mail aplica a um e-mail se um usuário não escolher uma marcação. Este valor deve estar na lista da política de marcações de classificação de e-mail. O valor padrão é **UNOFFICIAL**.

Limite de Pesquisa de E-mail

Restringe a quantidade de histórico de e-mail acessível a partir de dispositivos móveis, limitando o número de dias incluídos nas pesquisas do servidor de e-mail. Para restringir a quantidade de e-mail sincronizada com um dispositivo móvel, configure a política de intervalo máximo de sincronização. O valor padrão é **Ilimitado**.

Intervalo máximo de sincronização

Controla a quantidade de e-mails armazenados localmente em um dispositivo móvel, limitando o período de sincronização.

Para restringir o período em que um dispositivo pode pesquisar no servidor de e-mail, configure a política de limite de pesquisa do servidor de e-mail.

Os valores são:

- 3 dias
- 1 semana
- 2 semanas
- 1 mês
- Todos

O valor padrão é **Todos**.

Opções de Web e Áudio do Calendário

- **GoToMeeting e Inserido pelo Usuário** - Quando esta opção é escolhida, os usuários podem selecionar o tipo de conferência que desejam configurar. As opções incluem GoToMeeting, que abre uma página do GoToMeeting, e Outra Conferência, que permite aos usuários inserir informações da reunião manualmente.
- **Somente Inserido pelo Usuário** - Quando esta opção é escolhida, os usuários são direcionados diretamente para a página Outra Conferência, onde podem inserir informações da reunião manualmente.

Origem do Certificado Público S/MIME

Especifica a origem dos certificados públicos S/MIME. Se **Exchange**, o Secure Mail busca certificados do Exchange Server. Se **LDAP**, o Secure Mail busca certificados do servidor LDAP. O valor padrão é **Exchange**.

Endereço do Servidor LDAP

Endereço do servidor LDAP incluindo o número da porta. O valor padrão está vazio.

DN Base do LDAP

Nome distinto da Base LDAP. O valor padrão está vazio.

Acessar LDAP Anonimamente

Se esta política estiver **Ativada**, o Secure Mail pode pesquisar no LDAP sem autenticação prévia. O padrão é **Desativado**.

Domínios de E-mail Permitidos

Defina uma lista de domínios de e-mail permitidos em um formato separado por vírgulas, como server.company.com,server.company.co.uk. O valor padrão está vazio, o que implica que o Secure Mail não filtra domínios de e-mail e suporta todos os domínios de e-mail. O Secure Mail compara os domínios listados com o nome de domínio no endereço de e-mail.

Por exemplo, quando server.company.com é um nome de domínio listado e o endereço de e-mail é user@internal.server.company.com, o Secure Mail suporta o endereço de e-mail.

Notificações push

Ativa notificações baseadas em FCM sobre a atividade da caixa de correio. Se **Ativada**, o Secure Mail suporta notificações push. O valor padrão é **Desativado**.

Nome do host EWS para notificações push

O servidor que hospeda os Serviços Web do Exchange (EWS) para e-mail. O valor deve ser a URL do EWS, juntamente com o número da porta. O valor padrão está vazio.

Região das notificações push

A região onde o host FCM está localizado para seus usuários do Secure Mail. As opções são Américas, EMEA e PAC. O valor padrão é Américas.

Tentar migração de nome de usuário na falha de autenticação

Esta política tenta migrar o nome de usuário do Exchange para um UPN para autenticação. O valor padrão é **Desativado**.

Relatar Endereços de E-mail de Phishing

Se configurado, você pode relatar e-mails de phishing suspeitos para um endereço de e-mail fornecido ou uma lista de endereços de e-mail separados por vírgulas. O valor padrão é vazio. Se você não configurar esta política, não poderá relatar mensagens de phishing.

Mecanismo de Relato de Phishing

Esta política indica o mecanismo usado para relatar e-mails de phishing suspeitos.

- Relatar via anexo (.eml) – Relate e-mails de phishing como um anexo. O anexo é enviado para um endereço de e-mail ou uma lista de endereços de e-mail separados por vírgulas configurados na política Relatar Endereços de E-mail de Phishing.
- Relatar via encaminhamento – Relate e-mails de phishing como um encaminhamento. O e-mail é encaminhado para um endereço de e-mail ou uma lista de endereços de e-mail separados por vírgulas configurados na política Relatar Endereços de E-mail de Phishing.

NOTA:

Esta política está disponível apenas para o servidor Microsoft Exchange.

O padrão é Relatar via anexo (.eml).

Domínios de Reunião do Skype for Business

Esta política contém uma lista de domínios separados por vírgulas usados para reuniões do Skype for Business. O Secure Mail já lida com reuniões com prefixo de URL da seguinte forma:

- `https://join`
- `https://meet`
- `https://lync`

Com esta política, outros domínios do Skype for Business podem ser adicionados no formato `https://*domain*`. O domínio pode ser uma sequência de caracteres alfanuméricos e não pode conter caracteres especiais. Não insira o `https://` precedente ou o ponto seguinte.

Exemplo

Se o valor da política for `customDomain1,customDomain2`, os prefixos de URL suportados para o Skype for Business seriam: `https://customDomain1` `http://customDomain1` `https://customDomain2` `http://customDomain2`

O valor padrão está vazio.

Exportar Calendário

Esta política permite que os eventos do calendário do Secure Mail sejam exportados para o seu dispositivo ou calendário pessoal. Você pode visualizar seus eventos no seu calendário pessoal. Você pode editar os eventos usando o Secure Mail. O valor padrão é **Hora da Reunião**.

Os seguintes valores de política MDX estão disponíveis para os campos de evento do calendário que aparecem no seu calendário pessoal:

- Nenhum (Não Exportar)
- Hora da Reunião
- Hora da Reunião, Local
- Hora da Reunião, Assunto, Local
- Hora da Reunião, Disponibilidade, Participantes, Assunto, Local, Notas

Suporte OAuth para Office 365

Usar autenticação moderna para O365

Se esta política estiver **Ativada**, o Secure Mail usa o protocolo OAuth para autenticação ao configurar uma conta no Office 365. Se **Desativada**, o Secure Mail usa autenticação Básica. O padrão é **Desativada**.

Nomes de host confiáveis do Exchange Online

Defina uma lista de nomes de host confiáveis do Exchange Online que usam o mecanismo OAuth para autenticação ao configurar uma conta. Este valor é um formato separado por vírgulas, como server.company.com, server.company.co.uk. Se a lista estiver vazia, o Secure Mail usará a autenticação Básica para a configuração da conta. O valor padrão é outlook.office365.com.

Nomes de host confiáveis do AD FS

Defina uma lista de nomes de host confiáveis do AD FS para páginas da web onde a senha é preenchida durante a autenticação OAuth do Office 365. Este valor é um formato separado por vírgulas, como sts.companyname.com, sts.company.co.uk. Se a lista estiver vazia, o Secure Mail não preencherá automaticamente as senhas. O Secure Mail compara os nomes de host listados com o nome de host da página da web encontrada durante a autenticação do Office 365 e verifica se a página usa o protocolo HTTPS.

Por exemplo, quando sts.company.com é um nome de host listado e se o usuário navega para `https://sts.company.com`, o Secure Mail preenche a senha se a página tiver um campo de senha. O valor padrão é `login.microsoftonline.com`.

Agente de usuário personalizado para autenticação moderna

Esta política permite alterar a string de agente de usuário padrão para autenticação moderna. Se configurada, esta string de agente de usuário é usada para autenticação com o Microsoft AD FS. Se você não configurar esta política, o agente de usuário padrão do Secure Mail será usado durante a autenticação moderna.

Integração com o Slack

Habilitar Slack

Bloqueia ou permite a integração com o Slack. Se **Ativado**, a interface do Secure Mail inclui recursos do Slack. Se **Desativado**, a interface do Secure Mail não inclui recursos do Slack.

Nome do espaço de trabalho do Slack

O nome do espaço de trabalho do Slack para sua empresa. Se você fornecer um nome, o Secure Mail preencherá o nome do espaço de trabalho durante o login. Se você não fornecer um nome, os usuários deverão digitar o nome do espaço de trabalho (name.slack.com).

Políticas MDX para aplicativos de produtividade móvel para iOS

Este artigo descreve as políticas MDX para aplicativos iOS. Você altera as configurações de política no console do Citrix Endpoint Management. Para obter detalhes, consulte [Adicionar aplicativos](#).

A lista a seguir não inclui políticas MDX específicas do Secure Web. Para obter detalhes sobre as políticas que aparecem para o Secure Web, consulte [Políticas do Secure Web](#).

Autenticação

Senha do dispositivo

Se **Ativado**, um PIN ou senha é necessário para desbloquear o dispositivo quando ele inicia ou é retomado após um período de inatividade. Uma senha de dispositivo é necessária para criptografar dados de aplicativos usando a criptografia de arquivos da Apple. Os dados de todos os aplicativos no dispositivo são criptografados. O valor padrão é **Desativado**.

Senha do aplicativo

Se **Ativado**, um PIN ou senha é necessário para desbloquear o aplicativo quando ele inicia ou é retomado após um período de inatividade. O valor padrão é **Ativado**.

Para configurar o temporizador de inatividade para todos os aplicativos, defina o valor de **INACTIVITY_TIMER** em minutos em **Propriedades do Cliente** na guia **Configurações**. O valor padrão do temporizador de inatividade é **60** minutos. Para desativar o temporizador de inatividade, de modo que um prompt de PIN ou senha apareça apenas quando o aplicativo iniciar, defina o valor como zero.

NOTA:

Se você selecionar **Seguro offline** para a política de chaves de criptografia, esta política será habilitada automaticamente.

Período máximo offline (horas)

Define o período máximo que um aplicativo pode ser executado sem reconfirmar o direito do aplicativo e atualizar as políticas do Citrix Endpoint Management. Ao expirar, o login no servidor pode ser acionado, se necessário. O valor padrão é **168** horas (7 dias). O período mínimo é de **1** hora.

Citrix Gateway alternativo

NOTA:

Este nome de política no console do Endpoint Management é **Alternate NetScaler® Gateway**.

Endereço de um Citrix Gateway alternativo específico que deve ser usado para autenticação e para sessões de micro VPN com este aplicativo. Esta política é opcional. Quando usada com a política de sessão online obrigatória, a política força os aplicativos a se reautenticarem no gateway específico. Tais gateways normalmente teriam requisitos de autenticação e políticas de gerenciamento de tráfego diferentes (de maior garantia). Se deixado em branco, o gateway padrão do servidor é sempre usado. O valor padrão é vazio.

Segurança do dispositivo

Bloquear dispositivos com jailbreak ou root

Se **Ativado**, o aplicativo é bloqueado quando o dispositivo tem jailbreak ou root. Se **Desativado**, o aplicativo pode ser executado mesmo que o dispositivo tenha jailbreak ou root. O valor padrão é **Ativado**.

Requisitos de rede

Exigir Wi-Fi

Se **Ativado**, o aplicativo é bloqueado quando o dispositivo não está conectado a uma rede Wi-Fi.

Se **Desativado**, o aplicativo pode ser executado se o dispositivo tiver uma conexão ativa, como uma conexão 4G/3G, LAN ou Wi-Fi. O valor padrão é **Desativado**.

Redes Wi-Fi permitidas

Lista de redes Wi-Fi separadas por vírgulas. Se o nome da rede contiver caracteres não alfanuméricos (incluindo vírgulas), o nome deve ser colocado entre aspas duplas. O aplicativo é executado somente se conectado a uma das redes listadas. Se em branco, todas as redes são permitidas. Este valor não afeta as conexões com redes celulares. O valor padrão é em branco.

Acesso diverso

Desativar atualização obrigatória

Desativa a exigência de que os usuários atualizem para a versão mais recente do aplicativo na App Store. O valor padrão é **Ativado**.

Período de carência para atualização do aplicativo (horas)

Define o período de carência durante o qual um aplicativo pode continuar a ser usado depois que o sistema descobriu que uma atualização do aplicativo está disponível. O valor padrão é **168 horas (7 dias)**.

NOTA:

Recomendamos que você não use um valor de zero. Um valor zero impede imediatamente que um aplicativo em execução seja usado até que a atualização seja baixada e instalada (sem qualquer aviso ao usuário). Usar este valor pode levar a uma situação em que o usuário é forçado a sair do aplicativo (potencialmente perdendo trabalho) para cumprir a atualização necessária.

Apagar dados do aplicativo ao bloquear

Apaga os dados e redefine o aplicativo quando ele é bloqueado. Se **Desativado**, os dados do aplicativo não são apagados quando o aplicativo é bloqueado. O valor padrão é **Desativado**.

Um aplicativo pode ser bloqueado por qualquer um dos seguintes motivos:

- Perda de direito de uso do aplicativo para o usuário
- Assinatura do aplicativo removida
- Conta removida
- Secure Hub desinstalado
- Muitas falhas de autenticação do aplicativo
- Dispositivo com jailbreak detectado (conforme configuração da política)
- Dispositivo colocado em estado bloqueado por outra ação administrativa

Período de sondagem ativa (minutos)

Quando um aplicativo é iniciado, o MDX Framework consulta o Citrix Endpoint Management para determinar o status atual do aplicativo e do dispositivo. Assumindo que o servidor que executa o Endpoint Management possa ser alcançado, o framework retorna informações sobre o status de bloqueio/apagamento do dispositivo e o status de ativação/desativação do aplicativo.

Independentemente de o servidor poder ser alcançado ou não, uma sondagem subsequente é agendada com base no intervalo do período de sondagem ativa. Após o término do período, uma nova sondagem é novamente tentada. O valor padrão é **60 minutos** (1 hora).

IMPORTANTE:

Defina este valor mais baixo apenas para aplicativos de alto risco, ou o desempenho pode ser afetado.

Criptografia

Tipo de criptografia

Permite escolher se o MDX ou a plataforma do dispositivo lida com a criptografia dos dados. Se você selecionar **Criptografia MDX**, o MDX criptografa os dados. Se você selecionar **Criptografia de plataforma com aplicação de conformidade**, a plataforma do dispositivo criptografa os dados. O valor padrão é **Criptografia MDX**.

Comportamento de dispositivo não compatível

Permite escolher uma ação quando um dispositivo não adere aos requisitos mínimos de conformidade de criptografia. Selecione **Permitir aplicativo** para que o aplicativo seja executado normalmente. Selecione **Permitir aplicativo após aviso** para que o aplicativo seja executado após o aviso aparecer. Selecione **Bloquear** para impedir que o aplicativo seja executado. O valor padrão é **Permitir aplicativo após aviso**.

Habilitar criptografia MDX

Se **Desativado**, os dados armazenados no dispositivo não são criptografados. Se **Ativado**, os dados armazenados no dispositivo são criptografados. O valor padrão é **Ativado**.

CUIDADO:

Se você alterar esta política após implantar um aplicativo, os usuários deverão reinstalar o aplicativo.

Exclusões de criptografia de banco de dados

Lista de exclusão de bancos de dados que não são criptografados automaticamente. Para evitar a criptografia de um banco de dados específico, adicione uma entrada a esta lista de expressões regulares separadas por vírgulas. Se um nome de caminho de banco de dados corresponder a qualquer uma das expressões regulares, o banco de dados será excluído da criptografia. Os padrões de exclusão suportam a sintaxe de Expressões Regulares Estendidas Posix 1003.2. A correspondência de padrões não diferencia maiúsculas de minúsculas.

Exemplos

`\\.db$,\\.sqlite$` exclui qualquer nome de caminho de banco de dados que termine com `.db` ou `.sqlite`.

`\\Database\\unencrypteddb\\.db` corresponde ao banco de dados unencrypteddb.db na subpasta Database.

\\Database corresponde a todos os bancos de dados que contêm **/Database/** em seu caminho.

O valor padrão é vazio.

Exclusões de criptografia de arquivo

Lista de exclusão de arquivos que não são criptografados automaticamente. Para evitar a criptografia de um conjunto específico de arquivos, adicione uma entrada a esta lista de expressões regulares separadas por vírgulas. Se um nome de caminho de arquivo corresponder a qualquer uma das expressões regulares, esse arquivo será excluído da criptografia. Os padrões de exclusão suportam a sintaxe de Expressões Regulares Estendidas Posix 1003.2. A correspondência de padrões não diferencia maiúsculas de minúsculas.

Exemplos

`\\.log$,\\.dat$` exclui qualquer nome de caminho de arquivo que termine com `.log` ou `.dat`.

\\Documents\\unencrypteddoc.txt corresponde ao conteúdo do arquivo unencrypteddoc.txt na subpasta Documents.

\\Documents\\UnencryptedDocs\\.*.txt corresponde a arquivos ".txt" no subcaminho / Documents/UnencryptedDocs/.

O valor padrão é vazio.

Interação do aplicativo

Recortar e copiar

Bloqueia, permite ou restringe as operações de recortar e copiar da Área de Transferência para este aplicativo. Se **Restricted**, os dados copiados da Área de Transferência são colocados em uma Área de Transferência privada que está disponível apenas para aplicativos MDX. O valor padrão é **Restricted**.

Colar

Bloqueia, permite ou restringe as operações de colar da Área de Transferência para este aplicativo. Se **Restricted**, os dados colados da Área de Transferência são originados de uma Área de Transferência privada que está disponível apenas para aplicativos MDX. O valor padrão é **Unrestricted**.

Troca de documentos (Abrir em)

Bloqueia, permite ou restringe as operações de troca de documentos para este aplicativo. Se **Restrito**, os documentos podem ser trocados apenas com outros aplicativos MDX.

Se **Irrestrito**, defina a política Habilitar criptografia como **Ativado** para que os usuários possam abrir documentos em aplicativos não encapsulados. Se o aplicativo receptor não for encapsulado ou tiver a criptografia desabilitada, o Citrix Endpoint Management descriptografa o documento. O valor padrão é **Restrito**.

Lista de exceções de Abrir em restrito

Quando a política Troca de documentos (Abrir em) é **Restrita**, um aplicativo MDX pode compartilhar documentos com esta lista de IDs de aplicativos não gerenciados, separada por vírgulas. Isso é verdade mesmo que a política Troca de documentos (Abrir em) seja **Restrita** e Habilitar criptografia esteja **Ativada**. A lista de exceções padrão permite aplicativos do Office 365:

com.microsoft.Office.Word,com.microsoft.Office.Excel,com.microsoft.Office.Powerpoint,
com.microsoft.onenote,com.microsoft.onenoteiPad,com.microsoft.Office.Outlook

Somente aplicativos do Office 365 são suportados para esta política.

CUIDADO:

Certifique-se de considerar as implicações de segurança desta política. A lista de exceções permite que o conteúdo transite entre aplicativos não gerenciados e o ambiente MDX.

Nível de segurança da conexão

Determina a versão mínima de TLS/SSL usada para conexões. Se **TLS**, as conexões suportam todos os protocolos TLS. Se **SSLv3 e TLS**, as conexões suportam SSL 3.0 e TLS. O valor padrão é **TLS**.

Troca de documentos de entrada (Abrir em)

Bloqueia, restringe ou permite operações de troca de documentos de entrada para este aplicativo. Se **Restrito**, os documentos podem ser trocados apenas com outros aplicativos MDX. O valor padrão é **Irrestrito**.

Se **Bloqueado** ou **Restrito**, você pode usar a política de lista de permissões de troca de documentos de entrada para especificar aplicativos que podem enviar documentos para este aplicativo.

Opções: **Irrestrito**, **Bloqueado** ou **Restrito**

Esquemas de URL do aplicativo

Aplicativos iOS podem despachar solicitações de URL para outros aplicativos que foram registrados para manipular esquemas específicos (como "`http://`"). Este recurso fornece um mecanismo para um aplicativo passar solicitações de ajuda para outro aplicativo. Esta política serve para filtrar os esquemas que são passados para este aplicativo para tratamento (ou seja, URLs de entrada). O valor padrão é vazio, o que significa que todos os esquemas de URL de aplicativos registrados são bloqueados.

A política deve ser formatada como uma lista de padrões separados por vírgulas, onde um sinal de mais "+" ou menos "-" precede cada padrão. As URLs de entrada são comparadas com os padrões na ordem listada até que uma correspondência seja encontrada. Uma vez correspondido, o prefixo dita a ação a ser tomada.

- Um prefixo de menos "-" bloqueia a URL de ser passada para este aplicativo.
- Um prefixo de mais "+" permite que a URL seja passada para o aplicativo para tratamento.
- Se nem "+" nem "-" for fornecido com o padrão, "+" (permitir) é assumido.
- Se uma URL de entrada não corresponder a nenhum padrão na lista, a URL será bloqueada.

A tabela a seguir contém exemplos de esquemas de URL de aplicativos:

ESQUEMA	APLICATIVO QUE REQUER O ESQUEMA DE URL	FINALIDADE
<code>ctxmobilebrowser</code>	Secure Web-	Permitir que o Secure Web manipular URLs HTTP: de outros aplicativos.-
<code>ctxmobilebrowsers</code>	Secure Web-	Permitir que o Secure Web manipular URLs HTTPS: de outros aplicativos.
<code>ctxmail</code>	Secure Mail-	Permitir que o Secure Mail manipular URLs <code>mailto:</code> de outros aplicativos.
COL-G2M	GoToMeeting-	Permitir que um aplicativo GoToMeeting empacotado

ESQUEMA	APLICATIVO QUE REQUER O ESQUEMA DE URL	FINALIDADE
		manipular solicitações de reunião.
<code>ctxsalesforce</code>	Citrix para Salesforce -	Permitir que o Citrix for Salesforce manipular solicitações do Salesforce.
<code>wbx</code>	WebEx	Permitir que um aplicativo WebEx empacotado manipular solicitações de reunião.

Interação do aplicativo (URL de saída)

Domínios excluídos da filtragem de URL

Esta política exclui URLs de saída de qualquer filtragem de "URLs Permitidas". Adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou sufixos DNS a serem excluídos da filtragem de "URLs Permitidas". Se esta política estiver vazia (o padrão), a filtragem de "URLs Permitidas" definida processa as URLs. Se esta política contiver alguma entrada, as URLs com campos de host que correspondam a pelo menos um item na lista (por meio de correspondência de sufixo DNS) são enviadas inalteradas para o iOS. Esta comunicação ignora a lógica de filtragem de "URLs Permitidas". O valor padrão é vazio.

URLs Permitidas

Aplicativos iOS podem despachar solicitações de URL para outros aplicativos que foram registrados para manipular esquemas específicos (como `"http://"`). Este recurso fornece um mecanismo para um aplicativo passar solicitações de ajuda para outro aplicativo. Esta política serve para filtrar as URLs que são passadas deste aplicativo para outros aplicativos para tratamento (ou seja, URLs de saída).

A política deve ser formatada como uma lista de padrões separados por vírgulas, na qual cada padrão pode ser precedido por um sinal de mais "+" ou menos "-". As URLs de saída são comparadas com os padrões na ordem listada até que uma correspondência seja encontrada. Uma vez correspondido, o prefixo decide a ação a ser tomada. Um prefixo de menos "-" bloqueia a URL de ser passada para outro aplicativo. Um prefixo de mais "+" permite que a URL seja passada para outro aplicativo para tratamento. Se nem "+" nem "-" for fornecido com o padrão, "+" (permitir) é assumido. Um par de valores separados por "=" indica uma substituição

onde as ocorrências da primeira string são substituídas pela segunda. Você pode usar o prefixo de expressão regular "\^" para pesquisar a string e ancorá-la ao início da URL. Se uma URL de saída não corresponder a nenhum padrão na lista, ela será bloqueada.

Padrão

+maps.apple.com

+itunes.apple.com

\^http:=ctxmobilebrowser::

\^https:=ctxmobilebrowsers::

\^mailto:=ctxmail::

+\\^citrixreceiver::

+\\^telprompt::

+\\^tel::

+\\^lmi-g2m::

+\\^maps:ios_addr

+\\^mapitem::

+\\^sms::

+\\^facetime::

+\\^ctxnotes::

+\\^ctxnotesex::

+\\^ctxtasks::

+\\^facetime-audio::

+\\^itms-apps::

+\\^ctx-sf::

+\\^sharefile::

+\\^lync::

`+\\^slack:`

`+\\^msteams:`

Se a configuração estiver em branco, todas as URLs são bloqueadas, exceto pelas seguintes:

- `http:`
- `https:`
- `+citrixreceiver: +tel:`

A tabela a seguir contém exemplos de URLs permitidas:

FORMATO DA URL	DESCRIÇÃO
<code>\\^mailto:=ctxmail:</code>	Todas as URLs <code>mailto:</code> são abertas no Secure Mail.
<code>\\^http:</code>	Todas as URLs HTTP são abertas no Secure Web.
<code>\\^https:</code>	Todas as URLs HTTPS são abertas no Secure Web.
<code>\\^tel:</code>	Permite ao usuário fazer chamadas.
<code>-//www.dropbox.com</code>	Bloqueia URLs do Dropbox despachadas de aplicativos gerenciados.
<code>+\\^COL-G2M:</code>	Permite que aplicativos gerenciados abram o aplicativo cliente GoToMeeting.
<code>-\\^SMS:</code>	Bloqueia o uso de um cliente de chat de mensagens.
<code>-\\^wbx:</code>	Bloqueia que aplicativos gerenciados abram o aplicativo cliente WebEx.
<code>+\\^ctxsalesforce:</code>	Permite que o Citrix for Salesforce se comunique com seu servidor Salesforce.

Domínios permitidos do Secure Web

Esta política afeta apenas as entradas da política "URLs Permitidas" que redirecionariam uma URL para o aplicativo Secure Web (`\^ http://ctxmobilebrowser:` e `\^https://ctxmobilebrowsers:`). Adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou sufixos DNS permitidos para redirecionar para o aplicativo Secure Web. Se esta política estiver vazia (o padrão), todos os domínios podem redirecionar para o aplicativo Secure Web. Se esta política contiver alguma entrada, então apenas as URLs com campos de host que correspondam a pelo menos um item na lista (via correspondência de sufixo DNS) redirecionarão para o aplicativo Secure Web. Todas as outras URLs são enviadas inalteradas para o iOS, ignorando o aplicativo Secure Web. O valor padrão é vazio.

Restrições de Aplicativos

Importante:

Certifique-se de considerar as implicações de segurança das políticas que impedem que os aplicativos acessem ou usem os recursos do telefone. Quando essas políticas estão **Desativadas**, o conteúdo pode transitar entre aplicativos não gerenciados e o ambiente Seguro.

Bloquear câmera

Se **Ativado**, impede que um aplicativo use diretamente o hardware da câmera. O valor padrão é **DESATIVADO**.

Bloquear Biblioteca de Fotos

Se **Ativado**, impede que um aplicativo acesse a Biblioteca de Fotos no dispositivo. O valor padrão é **Ativado**.

Bloquear gravação de microfone

Se **Ativado**, impede que um aplicativo use diretamente o hardware do microfone. O valor padrão é **Ativado**.

Bloquear ditado

Se **Ativado**, impede que um aplicativo use diretamente os serviços de ditado. O valor padrão é **Ativado**.

Bloquear serviços de localização

Se **Ativado**, impede que um aplicativo use os componentes dos serviços de localização (GPS ou rede). O valor padrão é **Desativado** para o Secure Mail.

Bloquear composição de SMS

Se **Ativado**, impede que um aplicativo use o recurso de composição de SMS para enviar mensagens SMS/de texto do aplicativo. O valor padrão é **Ativado**.

Bloquear composição de e-mail

Se **Ativado**, impede que um aplicativo use o recurso de composição de e-mail para enviar mensagens de e-mail do aplicativo. O valor padrão é **Ativado**.

Bloquear iCloud

Se **Ativado**, impede que um aplicativo use o iCloud para armazenar e compartilhar configurações e dados.

NOTA

O arquivo de dados do iCloud é controlado pela política Bloquear backup de arquivo.

O valor padrão é **Ativado**.

Bloquear pesquisa

Se **Ativado**, impede que um aplicativo use o recurso Pesquisar, que busca texto destacado no Dicionário, iTunes, App Store, horários de filmes, locais próximos e muito mais. O valor padrão é **Ativado**.

Bloquear backup de arquivo

Se **Ativado**, impede que o iCloud ou o iTunes façam backup de arquivos de dados. O valor padrão é **Ativado**.

Bloquear AirPrint

Se **Ativado**, impede que um aplicativo use os recursos do AirPrint para imprimir dados em impressoras habilitadas para AirPrint. O valor padrão é **Ativado**.

Bloquear AirDrop

Se **Ativado**, impede que um aplicativo use o AirDrop. O valor padrão é **Ativado**.

Bloquear anexos de arquivo

NOTA

Esta política é aplicada no iOS 11 ou posterior.

Se **Ativado**, o tratamento de anexos é desativado. O valor padrão é **Desativado**.

Bloquear APIs do Facebook e Twitter

Se **Ativado**, impede que um aplicativo use as APIs do Facebook e Twitter do iOS. O valor padrão é **Ativado**.

Obscurecer conteúdo da tela

Se **Ativado**, quando os usuários trocam de aplicativo, a tela é obscurecida. Esta política impede que o iOS grave o conteúdo da tela e exiba miniaturas. O valor padrão é **Ativado**.

Bloquear teclados de terceiros (somente iOS 11 e posterior)

Se **Ativado**, impede que um aplicativo use extensões de teclado de terceiros no iOS 8+. O valor padrão é **Ativado**.

Bloquear logs de aplicativos

Se **Ativado**, proíbe que um aplicativo use o recurso de registro de diagnóstico do aplicativo de produtividade móvel. Se **Desativado**, os logs do aplicativo são registrados e podem ser coletados usando o recurso de suporte por e-mail do Secure Hub. O valor padrão é **Desativado**.

Habilitar ShareFile

Permite que os usuários usem o ShareFile para transferir arquivos. O valor padrão é **Ativado**.

Habilitar Anexar de Arquivos

Permite que os usuários adicionem anexos do aplicativo Arquivos do iOS. O valor padrão é **Ativado**.

Acesso à rede do aplicativo

Acesso à rede

NOTA:

Tunneled - Web SSO é o nome para **Secure Browse** nas configurações. O comportamento é o mesmo.

As opções de configuração são as seguintes:

- **Bloqueado:** Todo o acesso à rede é bloqueado. As APIs de rede usadas pelo seu aplicativo falham. Conforme a diretriz anterior, você deve manipular essa falha de forma elegante.
- **Irrestrito:** Todas as chamadas de rede vão diretamente e não são tuneladas.
- **Tunelado - Web SSO:** A URL HTTP/HTTPS é reescrita. Esta opção permite apenas o tunelamento de tráfego HTTP e HTTPS. Uma vantagem significativa de **Tunelado - Web SSO** é o logon único (SSO) para tráfego HTTP e HTTPS e também a autenticação PKINIT. No Android, esta opção tem baixa sobrecarga de configuração e, portanto, é a opção preferida para operações de navegação na web.

Se você estiver usando as políticas **Tunelado - VPN Completa** ou **Tunelado - VPN Completa e Web SSO**, então você deve mudar para a política **Tunelado - Web SSO**. Seus e-mails não serão sincronizados se você continuar a usar as políticas obsoletas.

NOTA:

Se você estiver usando **Tunelado - VPN Completa** e a Secure Ticket Authority (STA) estiver configurada, a tela de autenticação moderna não será carregada.

Sessão Micro VPN necessária

Se **Sim**, o usuário deve ter uma conexão com a rede corporativa e uma sessão ativa. Se **Não**, uma sessão ativa não é necessária. O valor padrão é **Usar Configuração Anterior**. Para aplicativos recém-carregados, o valor padrão é **Não**. Qualquer configuração selecionada antes da atualização para esta nova política permanece em vigor até que uma opção diferente de **Usar Configuração Anterior** seja selecionada.

Período de carência da sessão Micro VPN necessária (minutos)

Este valor determina quantos minutos os usuários podem usar o aplicativo antes que a política Sessão Online Necessária os impeça de continuar o uso (até que a sessão online seja validada). O valor padrão é **0** (sem período de carência). Esta política não é aplicável para integração com Microsoft Intune/EMS.

Rótulo do certificado

Quando usado com o serviço de integração de certificados StoreFront™, este rótulo identifica o certificado específico necessário para este aplicativo. Se nenhum rótulo for fornecido, um certificado não será disponibilizado para uso com uma infraestrutura de chave pública (PKI). O valor padrão é vazio (nenhum certificado usado).

Lista de Exclusão

Lista de FQDNs ou sufixos DNS separados por vírgulas a serem acessados diretamente em vez de por meio de uma conexão VPN. Este valor se aplica apenas ao modo **Tunelado - Web SSO** quando o Citrix Gateway está configurado com o modo de túnel dividido reverso.

Logs do aplicativo

Saída de log padrão

Determina qual mídia de saída é usada pelas facilidades de registro de diagnóstico do aplicativo de produtividade móvel por padrão. As possibilidades são arquivo, console ou ambos. O valor padrão é **arquivo**.

Nível de log padrão

Controla a verbosidade padrão da facilidade de registro de diagnóstico do aplicativo de produtividade móvel. Cada nível inclui níveis de valores menores. O intervalo de níveis possíveis inclui:

- 0 - Nada registrado
- 1 - Erros críticos
- 2 - Erros
- 3 - Avisos
- 4 - Mensagens informativas
- 5 - Mensagens informativas detalhadas
- 6 a 15 - Níveis de depuração de 1 a 10

O valor padrão é o nível 4 (Mensagens informativas).

Máximo de arquivos de log

Limita o número de arquivos de log retidos pela facilidade de registro de diagnóstico do aplicativo de produtividade móvel antes de serem substituídos. O mínimo é 2. O máximo é 8. O valor padrão é 2.

Tamanho máximo do arquivo de log

Limita o tamanho em MB dos arquivos de log retidos pelo recurso de registro de diagnóstico do aplicativo de produtividade móvel antes de serem substituídos. O mínimo é 1 MB. O máximo é 5 MB. O valor padrão é 2 MB.

Cerca geográfica do aplicativo

Longitude do ponto central

Longitude (coordenada X) do ponto central da cerca geográfica de ponto/raio na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado.

O valor deve ser expresso no formato de graus com sinal (DDD.dddd), por exemplo "-31.9635". Longitudes oeste devem ser precedidas por um sinal de menos. O valor padrão é **0**.

Latitude do ponto central

Latitude (coordenada Y) do ponto central da cerca geográfica de ponto/raio na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado.

O valor deve ser expresso no formato de graus com sinal (DDD.dddd), por exemplo "43.06581". Latitudes sul devem ser precedidas por um sinal de menos. O valor padrão é **0**.

Raio

O raio da cerca geográfica na qual o aplicativo é restrito a operar. Quando operado fora da cerca geográfica configurada, o aplicativo permanece bloqueado.

O valor deve ser expresso em metros. Quando definido como zero, a cerca geográfica é desabilitada. Quando a política de Bloquear serviço de localização está habilitada, o geofencing não funciona corretamente. O padrão é **0** (desabilitado).

Habilitar Google Analytics

Se **Ativado**, a Citrix coleta dados anônimos para melhorar a qualidade do produto. Se **Desativado**, nenhum dado é coletado. O valor padrão é **Ativado**.

Análises

Nível de detalhe do Google Analytics

A Citrix coleta dados de análise para melhorar a qualidade do produto. A seleção de **Anônimo** impede que os usuários incluam informações de identificação da empresa. O padrão é Completo.

Relatórios

Relatórios da Citrix

Se **Ativado**, a Citrix coleta relatórios de falhas e diagnósticos para ajudar a solucionar problemas. Se **Desativado**, a Citrix não coleta dados.

NOTA

A Citrix também pode controlar esse recurso com um sinalizador de recurso. Tanto o sinalizador de recurso quanto esta política devem estar habilitados para que esse recurso funcione.

O valor padrão é **Desativado**.

Token de upload

Você pode obter um token de upload da sua conta do Citrix Insight Services (CIS). Se você especificar este token opcional, o CIS lhe dará acesso a relatórios de falhas e diagnósticos carregados de seus dispositivos. A Citrix tem acesso a essas mesmas informações. O valor padrão é vazio.

Enviar relatórios somente por Wi-Fi

Se **Ativado**, a Citrix envia relatórios de falhas e diagnósticos somente quando você está conectado a uma rede Wi-Fi. O valor padrão é **Ativado**.

Máximo de cache de arquivo de relatório

Limita o tamanho dos pacotes de relatórios de falhas e diagnósticos retidos antes de limpar o cache. O mínimo é 1 MB. O máximo é 5 MB. O valor padrão é 2 MB.

Interação do aplicativo

Notificação de logoff explícito

Se **Desativado**, o aplicativo não é ativado durante o logoff do usuário. Se **Somente dispositivos compartilhados**, o aplicativo é ativado durante o logoff do usuário, somente se o dispositivo estiver configurado como um dispositivo compartilhado. O padrão é **Somente dispositivos compartilhados** para o Secure Mail.

Configurações do aplicativo

Servidor Exchange do Secure Mail

O nome de domínio totalmente qualificado (FQDN) para o Exchange Server ou, somente para iOS, o servidor IBM Notes Traveler. O valor padrão é vazio. Se você fornecer um nome de domínio neste campo, os usuários não poderão editá-lo. Se você deixar o campo vazio, os usuários fornecerão suas próprias informações de servidor.

CUIDADO

Se você alterar esta política para um aplicativo existente, os usuários deverão excluir e reinstalar o aplicativo para aplicar a alteração da política.

Domínio de usuário do Secure Mail

Nome de domínio padrão do Active Directory para usuários do Exchange ou, somente para iOS, usuários do Notes. O valor padrão é vazio.

Serviços de rede em segundo plano

O FQDN e a porta dos endereços de serviço permitidos para acesso à rede em segundo plano. Este valor pode ser um Exchange Server ou um servidor ActiveSync, seja em sua rede interna ou em outra rede à qual o Secure Mail se conecta, como mail.example.com:443.

Se você configurar esta política, defina a política de acesso à rede como **Tunelado para a rede interna**. Esta política entra em vigor quando você configura a política de acesso à rede. Use esta

política quando o Exchange Server residir em sua rede interna e você quiser usar o Citrix Gateway (anteriormente, NetScaler Gateway) para fazer proxy da conexão com o Exchange Server interno.

O valor padrão é vazio, o que implica que os serviços de rede em segundo plano não estão disponíveis.

Expiração do tíquete de serviços em segundo plano

Período de tempo durante o qual um tíquete de serviço de rede em segundo plano será válido. Após a expiração, será necessário um logon corporativo para renovar o tíquete. O valor padrão é **168 horas** (7 dias).

Gateway de serviço de rede em segundo plano

Endereço de gateway alternativo a ser usado para serviços de rede em segundo plano, no formato `fqdn:port`. Este valor é o FQDN e o número da porta do Citrix Gateway que o Secure Mail usa para se conectar ao servidor Exchange interno. No utilitário de configuração do Citrix Gateway, você deve configurar a Autoridade de Tíquetes Seguros (STA) e vincular a política ao servidor virtual. O valor padrão é vazio, o que implica que um gateway alternativo não existe.

Se você configurar esta política, defina a política de acesso à rede como **Tunelado para a rede interna**. Esta política entra em vigor quando você configura a política de acesso à rede. Use esta política quando o Exchange Server residir em sua rede interna e você quiser usar o Citrix Gateway para fazer proxy da conexão com o Exchange Server interno.

Exportar Contatos

Importante:

Não ative este recurso se os usuários puderem acessar seu Exchange Server diretamente (ou seja, fora do Citrix Gateway). Caso contrário, contatos duplicados serão criados no dispositivo e no Exchange.

Se **Desativado**, impede a sincronização unidirecional de contatos do Secure Mail para o dispositivo e o compartilhamento de contatos do Secure Mail (como vCards). O valor padrão é **Desativado**.

Campos de contato para exportar

Controla os campos de contato a serem exportados para o catálogo de endereços. Se **Todos**, todos os campos de contato são exportados. Se **Nome e Telefone**, todos os campos de contato

relacionados a nome e telefone são exportados. Se **Nome, Telefone e E-mail**, todos os campos de contato relacionados a nome, telefone e e-mail são exportados.

O valor padrão é **Todos**.

Aceitar todos os certificados SSL

Se **Ativado**, o Secure Mail aceita todos os certificados SSL (válidos ou não) e permite o acesso.

Se **Desativado**, o Secure Mail bloqueia o acesso quando ocorre um erro de certificado e exibe um aviso.

O valor padrão é **Desativado**.

Controlar notificações da tela bloqueada

Controla se as notificações de e-mail e calendário aparecem em uma tela de dispositivo bloqueada. Se **Permitir**, todas as informações contidas na notificação aparecem. Se **Bloquear**, as notificações não aparecem. Se **Remetente do e-mail ou título do evento**, apenas o nome do remetente do e-mail ou o título do evento do calendário aparece. Se **Somente contagem**, a contagem de e-mails e convites de reunião, além do horário dos lembretes de calendário, aparece. O valor padrão é **Permitir**.

Notificação de e-mail padrão

Se **Ativado**, o Secure Mail mostra a notificação da tela de bloqueio para e-mails. O valor padrão é **Ativado**.

Intervalo de sincronização padrão

Especifica o intervalo de sincronização padrão para o Secure Mail. Os usuários do Secure Mail podem alterar o padrão. A configuração da política **Caixa de correio do Exchange ActiveSync Filtro de idade máxima do e-mail** tem prioridade sobre esta política. Se você especificar um Intervalo de sincronização padrão que seja maior do que o Filtro de idade máxima do e-mail, a configuração **Filtro de idade máxima do e-mail** será usada em vez disso.

O Secure Mail exibe apenas os valores de intervalo de sincronização que são menores que a configuração **Filtro de idade máxima do e-mail do Active Sync**.

O valor padrão é **3 dias**.

Limite de pesquisa de e-mail

Restringe a quantidade de histórico de e-mail acessível a partir de dispositivos móveis, limitando o número de dias incluídos nas pesquisas do servidor de e-mail. O valor padrão é **Ilimitado**.

Para restringir a quantidade de e-mails sincronizados com um dispositivo móvel, configure a política Período máximo de sincronização do cliente.

Intervalo máximo de sincronização

Controla a quantidade de e-mails armazenados localmente em um dispositivo móvel, limitando o período de sincronização. O valor padrão é **Todos**. Para restringir o período de tempo que um dispositivo pode pesquisar no servidor de e-mail, configure a política Limite de pesquisa do servidor de e-mail.

Habilitar número da semana

Se **Ativado**, as visualizações do calendário incluem o número da semana. O valor padrão é **Desativado**.

Habilitar download de anexos via Wi-Fi

Se **Ativado**, a opção Baixar anexos do Secure Mail é habilitada para que os usuários possam, por padrão, baixar anexos por redes Wi-Fi internas permitidas. Se **Desativado**, a opção Baixar anexos do Secure Mail é desabilitada para que, por padrão, os usuários não possam baixar anexos por Wi-Fi.

O valor padrão é **Desativado**.

Permitir documentos offline

Especifica se, e por quanto tempo, os usuários podem armazenar documentos offline em dispositivos. O valor padrão é **Ilimitado**.

Gerenciamento de Direitos de Informação

Se **Ativado**, o Secure Mail oferece suporte aos recursos de Gerenciamento de Direitos de Informação (IRM) do Exchange. O valor padrão é **Desativado**.

Classificação de e-mail

Se **Ativado**, o Secure Mail oferece suporte a marcações de classificação de e-mail para SEC (segurança) e DLM (marcadores de limitação de disseminação). As marcações de classificação aparecem nos cabeçalhos de e-mail como valores "X-Protective-Marking". Certifique-se de configurar as políticas de classificação de e-mail relacionadas.

O valor padrão é **Desativado**.

Marcações de classificação de e-mail

Especifica as marcações de classificação a serem disponibilizadas aos usuários. Se a lista estiver vazia, o Secure Mail não incluirá uma lista de marcações de proteção. A lista de marcações contém pares de valores separados por ponto e vírgula. Cada par inclui o valor que aparece no Secure Mail e o valor da marcação que é o texto anexado ao assunto e ao cabeçalho do e-mail no Secure Mail. Por exemplo, no par de marcação "UNOFFICIAL,SEC=UNOFFICIAL;", o valor da lista é "UNOFFICIAL" e o valor da marcação é "SEC=UNOFFICIAL".

Namespace de classificação de e-mail

Especifica o namespace de classificação que é exigido no cabeçalho do e-mail pelo padrão de classificação usado. Por exemplo, o namespace "gov.au" aparece no cabeçalho como "NS=gov.au".

O valor padrão é vazio.

Versão de classificação de e-mail

Especifica a versão de classificação que é exigida no cabeçalho do e-mail pelo padrão de classificação usado. Por exemplo, a versão "2012.3" aparece no cabeçalho como "VER=2012.3".

O valor padrão está vazio.

Classificação de e-mail padrão

Especifica a marcação de proteção que o Secure Mail aplica a um e-mail se um usuário não escolher uma marcação. Este valor deve estar na lista da política de marcações de classificação de e-mail.

O valor padrão é **NÃO OFICIAL**.

Habilitar salvamento automático de rascunhos de e-mail

Se **Ativado**, o Secure Mail oferece suporte ao salvamento automático de mensagens na pasta **Rascunhos**.

O valor padrão é **Ativado**.

Mecanismo de autenticação inicial

Esta política indica se o endereço do servidor de e-mail fornecido pelo MDX ou o endereço de e-mail do usuário deve ser usado para preencher o campo "endereço" na tela de provisionamento de primeiro uso.

O valor padrão é **"Endereço do servidor de e-mail"**.

Credenciais de autenticação iniciais

Esta política define o valor que deve ser escolhido como nome de usuário para preencher a tela de provisionamento inicial de primeiro uso.

O valor padrão é **"Nome de usuário de inscrição"**.

Habilitar preenchimento automático do nome de usuário

Se ativado, o nome de usuário é preenchido automaticamente na interface do usuário de provisionamento de conta. O valor padrão é **ATIVADO**.

Habilitar proteção de dados do iOS

NOTA:

Esta política destina-se a empresas que devem atender aos requisitos de segurança de computador da Australian Signals Directorate (ASD).

Habilita a proteção de dados do iOS ao trabalhar com arquivos. Se **Ativado**, especifica o nível de proteção de arquivo ao criar e abrir arquivos na sandbox do aplicativo. O valor padrão é **Desativado**.

Nome do host EWS de Notificações por Push

O servidor que hospeda os Exchange Web Services (EWS) para e-mail. O valor deve ser a URL do EWS, juntamente com o número da porta. O valor padrão é vazio.

Notificações por push

Habilita notificações baseadas em APNs sobre a atividade da caixa de correio. Se **Ativado**, o Secure Mail oferece suporte a notificações por push.

O valor padrão é **Desativado**.

Região das notificações por push

A região onde o host APNs está localizado para usuários do Secure Mail. As opções são **Américas**, **EMEA** e **APAC**. O valor padrão é **Américas**.

Origem do certificado público S/MIME

Especifica a origem dos certificados S/MIME. Se **E-mail**, você deve enviar os certificados do usuário por e-mail aos usuários, que então abrem o e-mail no Secure Mail e importam os certificados anexados.

Se **Cofre compartilhado**, um provedor de identidade digital compatível fornece certificados para o cofre compartilhado do Secure App. A integração com o provedor de terceiros exige que você publique um aplicativo relacionado para os usuários. Consulte a descrição da política Habilitar S/MIME durante a primeira inicialização do Secure Mail para obter detalhes sobre a experiência do usuário.

O valor padrão é **E-mail**.

Habilitar S/MIME durante a primeira inicialização do Secure Mail

Determina se o Secure Mail habilita o S/MIME durante a primeira inicialização do Secure Mail, se a política de origem do certificado S/MIME for **Cofre compartilhado**. Se **Ativado**, o Secure Mail habilita o S/MIME se houver certificados para o usuário no cofre compartilhado. Se não houver certificados no cofre compartilhado, o usuário será solicitado a importar os certificados. Em ambos os cenários, os usuários devem configurar certificados de um aplicativo de provedor de identidade digital compatível antes de criar uma conta no Secure Mail.

Se **Desativado**, o Secure Mail não habilita o S/MIME e o usuário pode habilitá-lo nas configurações do Secure Mail. O valor padrão é **Desativado**.

Opções de Web e Áudio do Calendário

- **GoToMeeting e Inserido pelo Usuário:** Os usuários podem escolher o tipo de conferência que desejam configurar. As opções incluem **GoToMeeting**, que abre uma página do GoToMeeting, e **Outra Conferência**, que permite aos usuários inserir informações da reunião manualmente.
- **Somente Inserido pelo Usuário:** Os usuários são levados diretamente para a página Outra Conferência, onde podem inserir informações da reunião manualmente.

Origem do certificado público S/MIME

Especifica a origem dos certificados públicos S/MIME. Se **Exchange**, o Secure Mail busca certificados do Exchange Server. Se **LDAP**, o Secure Mail busca certificados do servidor LDAP. O valor padrão é **Exchange**.

Endereço do servidor LDAP

Endereço do servidor LDAP, incluindo o número da porta. O valor padrão é vazio.

DN Base do LDAP

Nome distinto base do LDAP. O valor padrão é vazio.

Acessar LDAP Anonimamente

Se esta política estiver **Ativada**, o Secure Mail pode pesquisar no LDAP sem autenticação prévia. O padrão é **Desativado**.

Domínios de E-mail Permitidos

Define uma lista de domínios de e-mail permitidos em um formato separado por vírgulas, como server.company.com,server.company.co.uk. O valor padrão é vazio, o que implica que o Secure Mail não filtra domínios de e-mail e suporta todos os domínios de e-mail. O Secure Mail compara os domínios listados com o nome de domínio no endereço de e-mail. Por exemplo, quando server.company.com é um nome de domínio listado e o endereço de e-mail é user@internal.server.company.com, o Secure Mail suporta o endereço de e-mail.

Tentar migração de nome de usuário na falha de autenticação

Tenta migrar o nome de usuário do Exchange para um UPN para autenticação. O valor padrão é **Desativado**.

Endereço de e-mail para relatar phishing

Se configurado, você pode relatar e-mails suspeitos de phishing para um determinado endereço de e-mail ou uma lista de endereços de e-mail separados por vírgulas. O valor padrão é vazio. Se você não configurar esta política, não poderá relatar mensagens de phishing.

Mecanismo de relatório de phishing

Esta política indica o mecanismo usado para relatar e-mails suspeitos de phishing.

- **Relatar via anexo:** Relate e-mails de phishing como um anexo. O anexo é enviado para um endereço de e-mail ou uma lista de endereços de e-mail separados por vírgulas configurados na política de Endereços de E-mail para Relatar Phishing.
- **Relatar via encaminhamento:** Relate e-mails de phishing como um encaminhamento. O e-mail é encaminhado para um endereço de e-mail ou uma lista de endereços de e-mail separados por vírgulas configurados na política de Endereços de E-mail para Relatar Phishing.

NOTA:

Esta política está disponível apenas para o Microsoft Exchange Server.

O padrão é **Relatar via anexo**.

Domínios de reunião do Skype for Business

Esta política contém uma lista de domínios separados por vírgulas usados para reuniões do Skype for Business.

O Secure Mail já lida com reuniões com prefixo de URL como o seguinte:

- `https://join`
- `https://meet`
- `https://lync`

Com esta política, outros domínios do Skype for Business podem ser adicionados no formato `https://*domain*`. O domínio pode ser uma sequência de caracteres alfanuméricos e não pode conter caracteres especiais. Não insira o `https://` precedente ou o ponto seguinte.

Exemplo:

Se o valor da política for **customDomain1,customDomain2**, os prefixos de URL suportados para o Skype for Business seriam:

- `https://customDomain1`
- `http://customDomain1`
- `https://customDomain2`
- `http://customDomain2`

O valor padrão está vazio.

Exportar Calendário

Esta política permite que os eventos do calendário do Secure Mail sejam exportados para o seu dispositivo ou calendário pessoal. Você pode visualizar seus eventos no seu calendário pessoal. Você pode editar os eventos usando o Secure Mail. O valor padrão é **Meeting Time**.

Os seguintes valores de política MDX estão disponíveis para os campos de evento do calendário que aparecem no seu calendário pessoal:

- Nenhum (Não Exportar)
- Hora da Reunião
- Hora da Reunião, Local
- Hora da Reunião, Assunto, Local
- Hora da Reunião, Assunto, Local, Notas

Identificação do Chamador

Se **Ativado**, o Secure Mail fornece o nome e o número de contato dos seus contatos salvos para o iOS para fins de identificação do chamador. Esses dados são usados apenas para identificar e exibir detalhes de chamadas recebidas da sua lista de contatos salvos do Secure Mail. O valor padrão é **Ativado**.

Suporte OAuth para Office 365

Mecanismo de autenticação do Office 365

Esta política indica o mecanismo OAuth usado para autenticação ao configurar uma conta no Office 365.

- **Não usar OAuth:** O OAuth não é usado e o Secure Mail usa autenticação Básica para a configuração da conta.
- **Usar OAuth com Nome de Usuário e Senha:** O usuário deve fornecer seu nome de usuário e senha e, opcionalmente, um código MFA para o fluxo OAuth.
- **Usar OAuth com Certificado de Cliente:** O usuário autentica o fluxo OAuth usando um certificado de cliente.

O padrão é "**Não usar OAuth**".

Nomes de host confiáveis do Exchange Online

Define uma lista de nomes de host confiáveis do Exchange Online que usam o mecanismo OAuth para autenticação ao configurar uma conta. Este valor é um formato separado por vírgulas, como server.company.com, server.company.co.uk. Se a lista estiver vazia, o Secure Mail usa autenticação Básica para a configuração da conta. O valor padrão é **outlook.office365.com**.

Nomes de host AD FS confiáveis

Defina uma lista de nomes de host AD FS confiáveis para páginas da web onde a senha é preenchida durante a autenticação OAuth do Office 365. Este valor está em formato separado por vírgulas, como sts.companyname.com, sts.company.co.uk. Se a lista estiver vazia, o Secure Mail

não preenche automaticamente as senhas. O Secure Mail compara os nomes de host listados com o nome de host da página da web encontrada durante a autenticação do Office 365 e verifica se a página usa o protocolo HTTPS. Por exemplo, quando sts.company.com é um nome de host listado e se o usuário navega para `https://sts.company.com`, o Secure Mail preenche a senha se a página tiver um campo de senha. O valor padrão é **login.microsoftonline.com**.

Redirecionamento de E-mail

Redirecionamento de E-mail

Bloqueia ou restringe qualquer composição de e-mail. O Secure Mail redireciona a composição de e-mail para o Secure Mail. O e-mail nativo redireciona a composição de e-mail para o e-mail nativo se uma conta estiver configurada. O valor padrão é **Secure Mail**.

Integração com Slack

Habilitar Slack

Bloqueia ou permite a integração com o Slack. Se **ON**, a interface do Secure Mail inclui recursos do Slack. Se **OFF**, a interface do Secure Mail não inclui recursos do Slack. O valor padrão é **OFF**.

Nome do espaço de trabalho do Slack

O nome do espaço de trabalho do Slack para sua empresa. Se você fornecer um nome, o Secure Mail preencherá o nome do espaço de trabalho durante o login. Se você não fornecer um nome, os usuários deverão digitar o nome do espaço de trabalho (name.slack.com). O valor padrão é vazio.

Recursos por plataforma

As tabelas a seguir resumem os recursos dos aplicativos de produtividade móvel da Citrix. **X** indica que o recurso está disponível para essa plataforma. Para recursos no QuickEdit, consulte o [Citrix QuickEdit](#).

Citrix Secure Hub™

RECURSO	IOS	ANDROID
Fazer logon para autenticar	X	X
Monitorar a conformidade da política	X	X
Acessar aplicativos e desktops	X	X
Aplicativos e desktops HDX™	X	X
Criar e enviar logs de problemas	X	X
Anexar capturas de tela aos logs	X	X
Entrar em contato com o suporte técnico dentro do aplicativo	X	X
Entrar em contato com o suporte da Citrix® dentro do aplicativo	X	X
Coleta e análise de falhas	X	X
Autenticação offline	X	X

RECURSO	IOS	ANDROID
Enviar logs com Citrix Secure Mail™	X	X
Google Analytics	X	X
Modo retrato e paisagem	X	X
Guia no aplicativo para confiar em aplicativos	X	X
Quando inscrito com e-mail, inscrição automática no Secure Mail (somente MAM)	X	X
Autenticação offline do Touch ID	X	X
Inscriver-se com credenciais derivadas	X	
Autenticação biométrica		X
Uso da loja de aplicativos do Workspace	X	X

Citrix Secure Mail

RECURSO	IOS	ANDROID
Produtividade de E-mail		
Minimizar rascunhos	X	X
Desfazer e-mails enviados		X
Gerenciamento de criptografia	X	X
Widget para agenda do Calendário		X

RECURSO	IOS	ANDROID
Imagem de contato no Secure Mail	X	X
Suporte para e-mails responsivos	X	X
Sincronização automática da pasta Rascunhos	X	X
Sincronização de anexos na pasta Rascunhos		X
Enviar, receber, responder, responder a todos, encaminhar e-mail	X	X
Criar, editar, excluir rascunhos	X	X
Marcar e-mail	X	X
Marcar como não lido	X	X
Visualizar todas as pastas e subpastas	X	X
Salvar rascunhos automaticamente quando o aplicativo é colocado em segundo plano	X	X
Email para nota com Citrix Secure Notes. Importante: O Secure Notes atingiu o status de Fim de Vida (EOL) em December 31, 2018. Para obter detalhes, consulte Aplicativos EOL e descontinuados .	X	X

RECURSO	IOS	ANDROID
Pesquisar e-mail (local e servidor)	X	X
Selecionar período de sincronização de e-mail (até 1 mês ou Todos os e-mails)	X	X
Visualizar e-mail não lido	X	X
Visualização/reprodução segura de anexos de imagens, vídeo e áudio	X	X
Vários anexos	X	X
Responder e encaminhar anexos	X	X
Anexar arquivos do Citrix Files	X	X
Anexar arquivos de Zonas Restritas e conectores do Citrix Files	X	X
Repositório de anexos	X	X
Edição de rich text	X	X
Notificação de e-mail com assunto, pré-visualização na tela de bloqueio	X	X
Responder e excluir e-mails e convites da tela de notificação	X	
Anexar ou tirar foto	X	X
Selecionar várias mensagens	X	X
Baixar anexos	X	X

RECURSO	IOS	ANDROID
Carregar imagens em linha	X	X
Classificação rápida	X	X
Enviar, receber, abrir e salvar anexos de arquivo .zip	X	X
Modos retrato e paisagem	X; Em listas de e-mail, leitura de e-mail, composição, calendário e visualizações de contatos	X: Apenas para visualizações de leitura e composição de e-mail
Texto colado mantém a formatação	X	X
SMS de contatos	X	X
FaceTime de contatos	X	
Mensagens não enviadas devido a problemas de conectividade ou caixa de correio cheia armazenadas na Caixa de Saída	X	X
Pastas recentes em destaque		X
Atualização de e-mail por arrastar para baixo	X	X
Carimbo de data/hora da última atualização	X	X
Deslizar para a esquerda para ações de mensagem	X	X
Suporte para Microsoft Exchange e IBM Notes Traveler	X	X
Toque para atualizar e-mail, calendário e contatos	X	X

RECURSO	IOS	ANDROID
Respeitar as configurações de acessibilidade/tamanho da fonte do dispositivo nas visualizações de e-mail	X	X
Assinatura e criptografia S/MIME	X	X
Importação de certificado S/MIME por e-mail	X	X
S/MIME, integração com Intercede	X	
S/MIME, integração com Entrust	X	
Proteção IRM da Microsoft para o corpo da mensagem	X	X
Notificações push	X	X
As notificações push para a Caixa de Entrada atualizam automaticamente todas as pastas, incluindo o calendário	X	
Abrir documentos do Office 365	X	X
Ações 3D Touch	X	
Ícones contextuais na tela de bloqueio	X	X
Pesquisar pastas	X	X
Pasta de e-mail VIP	X	X
Suporte a Tipo Dinâmico	X	X
Manter pastas expandidas	X	X

RECURSO	IOS	ANDROID
Marcadores de classificação de mensagens	X	X
Verificação ortográfica	X	
Anexar última foto tirada	X	X
Visualização de URL	X	X
Abrir links do Citrix Files no Citrix Files	X	X
Suporte para arquivos <code>.pass</code>	X	
Selecionar vários e-mails no modo de pesquisa	X	X
Inserir imagens em linha	X	X
Atualizar para a versão 16 do Exchange ActiveSync (EAS)	X	X
Restringir usuários de usar domínios desconhecidos ou pessoais	X	
Suporte para telas de dispositivos super-largas		X
Configurar várias contas do Exchange	X	X
Deslizar para a esquerda ou direita para mais ações	X	X
Criptografar respostas ou encaminhamentos de e-mails criptografados	X	
Imprimir e-mails e imagens incorporadas	X	

RECURSO	IOS	ANDROID
Use Linhas de Visualização em Configurações para configurar quantas linhas do corpo de um e-mail aparecem como visualização na caixa de entrada	X	
Suporte para e-mails responsivos	X	X
Visualização de anexos no aplicativo (MS Office ou imagens).	X	X
Grupos de contatos pessoais	X	X
Migrar nomes de usuário para endereços de e-mail (UPN)	X	X
Denunciar e-mails de phishing	X	X
Autenticação moderna (OAuth)	X	X
Imprimir anexos	X	
Android Enterprise (Android para Trabalho)	X	
Assinaturas de rich text	X	
Notificações push ricas	X	
Feeds	X	X
Melhorias no anexo de fotos	X	X
Notificações de grupo	X	

RECURSO	IOS	ANDROID
Integração com Slack (Prévia)	X	X
Gerenciar feeds	X	
Domínios internos	X	X
Gerenciar seus feeds	X	X
Integração com o MS Teams	X	X
Opção de autodiagnóstico (Solução de problemas)		X
Modo duplo (MAM SDK)	X	X
Ferramenta de autodiagnóstico		X
Calendário		
Visualizar e importar arquivos ICS como Eventos de calendário		X
Arrastar e soltar eventos do Calendário	X	X
Visualizações de dia, semana, mês e agenda	X	X
Lembretes detalhados na tela de bloqueio	X	X
Sincronizar por seis meses	X	X
Definir eventos como privados	X	X
Rolar para a hora antes do primeiro evento	X	

RECURSO	IOS	ANDROID
Opções de atualização manual	X	X
Definir lembretes	X	X
Tocar para mapear endereço	X	X
Números da semana	X	X
Suporte a Dynamic Type	X	X
Marcadores de classificação de segurança	X	X
Toques longos em endereços	X	
Definir o dia de início da semana de trabalho	X	X
Visualização focada na semana da data selecionada	X	
Data atual sempre destacada	X	X
Anexos de calendário do repositório de anexos	X	X
Suporte a calendário pessoal	X	X
Exibir conflitos com eventos do calendário pessoal		X
Imprimir eventos do calendário	X	
Tocar em números de telefone e endereços da web em uma linha de assunto do calendário	X	
Pesquisar calendário	X	

RECURSO	IOS	ANDROID
Reuniões		
Responder, responder a todos, encaminhar reuniões	X	X
Visualização do organizador das respostas ao convite	X	X
Visualização do organizador da disponibilidade dos convidados com disponibilidade sugerida	X	X
Toque para participar de reuniões online. Observação: Para WebEx e Lync, você deve configurar políticas no Citrix Endpoint Management™ para habilitar esses aplicativos.	X	X
Toque para participar de conferências de áudio	X	X
Agendar reunião online, áudio, conferência em novo convite	X	X
Adicionar links do ShareFile a novos convites	X	X
Encaminhar convites com anexos	X	X
Tocar para enviar e-mail "estou atrasado"	X	X
Tocar para responder ao organizador da reunião	X	X

RECURSO	IOS	ANDROID
Toque para responder a todos os convites de reunião	X	X
Toque para responder a todos os convidados da reunião	X	X
Toque para responder a todos os convidados da reunião com anexos	X	X
Discar para o GoToMeeting	X	X
Responder ao convite da tela de bloqueio ou tela de notificação	X	X
Discar para reuniões do WebEx ou Lync	X	X
Ocultar eventos recusados	X	X
Exibir mais de 3 eventos simultâneos	X	X
Visualização rápida do status do convidado	X	X
Excluir, responder, responder a todos, adicionar comentários em eventos cancelados	X	X
Mostrar nome do organizador em convites encaminhados	X	X
Dispositivos compartilhados	X	X
Participar de reuniões do Skype for Business	X	X

RECURSO	IOS	ANDROID
Responder a notificações de reunião, como Aceitar, Recusar e Provisório.	X	X
Responder a notificações de mensagem com Responder e Excluir	X	
Contatos		
Criar pastas em Contatos		X
Sincronização de contato bidirecional	X	X
Informações detalhadas de contato Pesquisa GAL	X	X
Exportar e sincronizar contatos do Secure Mail para contatos locais	X	X
Contatos: Favoritos e Categoria		X
Controlar quais campos de contato são exportados	X	X
Detalhes de contato de e-mail não seguro	X	X
Suporte a Tipo Dinâmico	X	X
Marcar contatos como VIPs	X	X
Compartilhar contatos com .vcards	X	X
Visualizar contatos com toque longo		X

RECURSO	IOS	ANDROID
Exportar contatos mesmo que a conta de e-mail nativa exista	X	X
Visualizar pastas e subpastas	X	
Configurações configuradas no dispositivo		
Suporte a iMessage	X	
Opções avançadas para controlar notificações	X	X
Controle de notificações na tela de bloqueio	X	X
Sons de notificações de e-mail e calendário	X	X
Atualização automática de pastas	X	X
Definir notificações internas e externas de ausência do escritório	X	X
Perguntar antes de excluir	X	X
Visualizações de conversas encadeadas ou cronológicas	X	X
Carregar anexos via Wi-Fi	X	X
Tornar o carregamento de anexos via Wi-Fi padrão	X	X
Definir período de sincronização de e-mail	X	X

RECURSO	IOS	ANDROID
Sincronização ilimitada/ sincronizar todos os e-mails		X
Definir assinatura de e-mail	X	X
Listar contatos por primeiro nome ou sobrenome	X	X
Avanço automático	X	X
Usar fuso horário residencial		X
Modelos de resposta rápida		X
Frequência de configuração de push de e-mail		X
Exportar/importar configurações	X	X
Toque no botão Voltar no dispositivo para dispensar as opções do botão de ação flutuante		X
Microsoft Teams	X	X

Citrix Secure Web™

RECURSO	IOS	ANDROID
Use dois aplicativos simultaneamente com Multitarefa	X	
Baixar arquivos	X	X
Adicionar favoritos	X	X
Limpar nomes de usuário e senhas salvos	X	X

RECURSO	IOS	ANDROID
Excluir cache/histórico/cookies	X	X
Bloquear pop-ups	X	X
Salvar páginas offline	X	X
Pesquisar na barra de endereços	X	X
Abrir itens baixados das notificações	X	X
Senhas salvas automaticamente	X	X
Suporte a proxy		
Proxies corporativos	X	X
Listas de bloqueio e permissão de URL	X	X
Histórico	X	X
Página inicial padrão	X	X
Abas	X	X
Enviar favoritos	X	X
Bloqueio de captura de tela		X
Pesquisar na página atual	X	X
Ações 3D Touch	X	
Dispositivos compartilhados	X	X
Proteção contra adulteração de arquivos com dispositivos compartilhados	X	

RECURSO	IOS	ANDROID
Exportar/importar configurações	X	X
Modo retrato e paisagem	X	X
Android Enterprise (Android para Trabalho)		X
Puxar para atualizar o conteúdo na tela	X	X
Secure Web como navegador padrão		X

Gerenciamento de feature flags

Para garantir o funcionamento ideal dos recursos que estão sob feature flags, você precisa habilitar o tráfego para a URL `features.netscalergateway.net`.

Feature flags são usadas para habilitar ou desabilitar recursos dinamicamente. Se ocorrer um problema com os Aplicativos de Produtividade Móvel em produção, o recurso afetado pode ser desabilitado dinamicamente, mesmo após o recurso ser lançado. Para isso, usamos feature flags gerenciadas pela Citrix.

Nenhuma configuração manual é necessária para habilitar o tráfego para o gerenciamento de recursos, exceto quando você tem um firewall ou proxy que está bloqueando o tráfego de saída. Nesse caso, você precisa habilitar o tráfego usando URLs ou endereços IP específicos, dependendo dos requisitos da sua política.

Endereços IP

Se você precisar listar endereços IP em uma lista de permissões, inclua o seguinte endereço IP para permitir o tráfego para `features.netscalergateway.net`:

- 57.153.121.183 (para a região Europa Ocidental)
- 172.202.161.151 (para a região Centro-Sul dos EUA)
- 48.218.128.128 (para a região Leste do Japão)

Você pode adicionar esses endereços IP para garantir que as configurações do seu firewall sejam atualizadas automaticamente de acordo com as atualizações de infraestrutura.

Requisitos do sistema

Se estiver usando o NetScaler Gateway com o tunelamento dividido definido como **DESATIVADO**, certifique-se de que o NetScaler possa resolver e se conectar a `features.netscalergateway.net` pela porta 443.

A tabela a seguir lista a versão mínima dos aplicativos de produtividade móvel que suportam o gerenciamento de feature flags.

APLICATIVOS DE PRODUTIVIDADE MÓVEL	SISTEMA OPERACIONAL	VERSÃO MÍNIMA SUPORTADA
Secure Hub	Android	24.8.0 e posterior
Secure Hub	iOS	24.9.0 e posterior
MAM SDK	Android	24.9.0 e posterior
MAM SDK	iOS	24.7.1 e posterior
Secure Mail	Android, iOS	24.9.0 e posterior
Secure Web	Android	24.8.0 e posterior
Secure Web	iOS	24.9.0 e posterior

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**.

Create Rewrite Action

Name*
InsertGatewayAuthTypeHeader ?

Type*
INSERT_HTTP_HEADER ▼

Use this action type to insert a header.

Header Name*
X-Citrix-AM-GatewayAuthType

Expression Expression Editor

Operators ▼ Saved Policy Expressions ▼ Frequently Used Expressions ▼ Clear

"CertAndRSA"

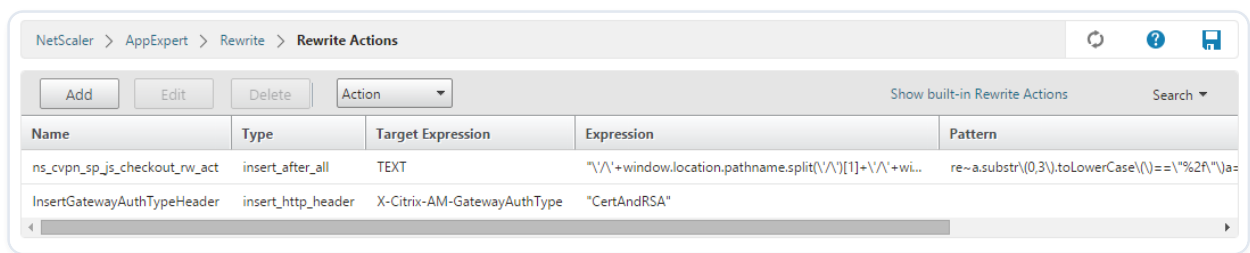
Evaluate

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

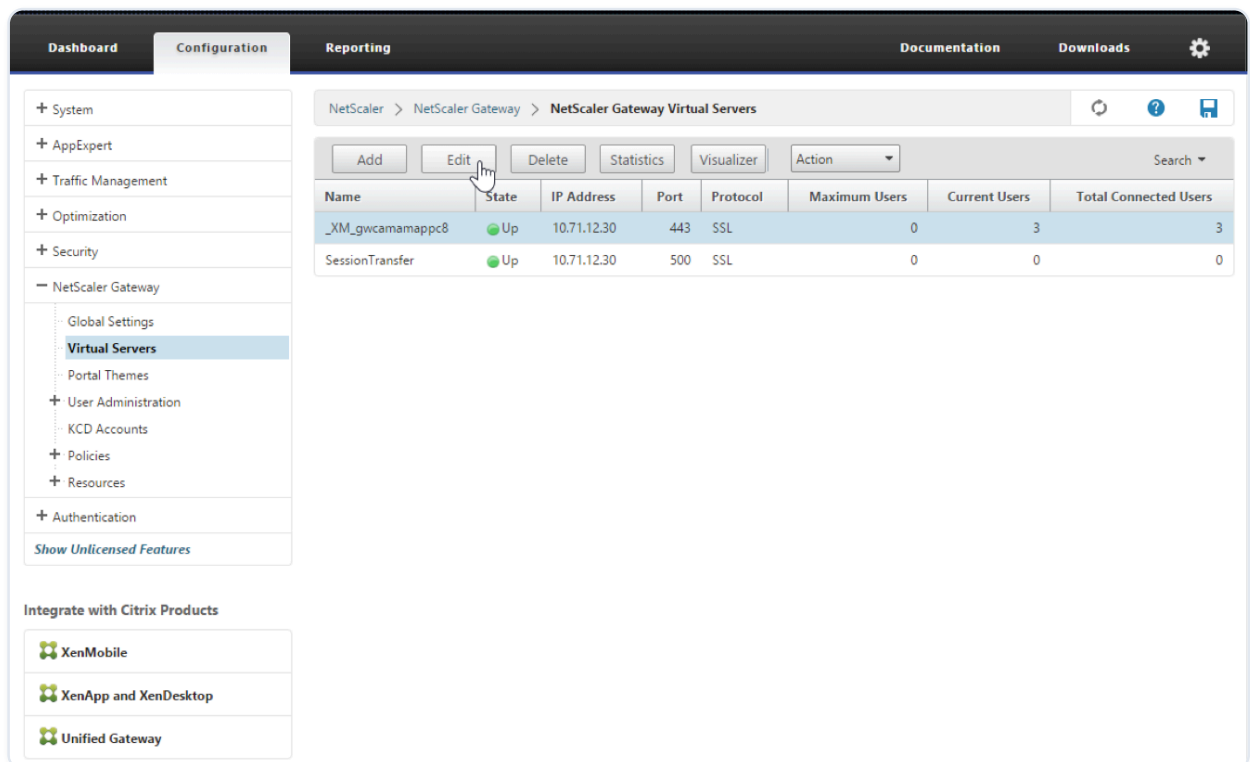
Comments

Create **Close**

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



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.

The screenshot shows the Citrix NetScaler configuration interface. The 'Profiles' section is expanded, showing the following settings:

- Net Profile: -
- TCP Profile: -
- HTTP Profile: nshttp_default_strict_validation

The 'Published Applications' section is also expanded, showing:

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

The 'Other Settings' section is expanded, showing the following settings:

ICMP Virtual Server Response	Passive	Listen Priority	
RHI State	Passive	Listen Policy Expression	NONE
Redirect to Home page	true	ShareFile	
		AppController	https://camamappc8.camam.net:8443
		L2 Connection	false

The 'Policies' section is expanded, showing:

- Request Policies
- 3 Session Policies
- 2 ClientlessAccess Policies
- 5 Cache Policies

A hand icon is pointing to the '+' button in the 'Policies' section header. The 'Done' button is at the bottom left.

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

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

The screenshot shows the 'Choose Type' dialog box. It has a title bar 'Choose Type' and a subtitle 'Choose Type'. The 'Policies' section is expanded, showing the following settings:

- Choose Policy*: Rewrite
- Choose Type*: Response

At the bottom, there are two buttons: 'Continue' and 'Cancel'. A hand icon is pointing to the 'Continue' button.

10. Clique em **Continuar**.

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

Choose Type

Choose Type

Policies

Choose Policy Rewrite	Choose Type Response
---------------------------------	--------------------------------

Policy Binding

Select Policy*

Click to select

Binding Details

Priority*

100

Goto Expression*

END

Bind **Close**

11. Clique em **Selecionar Política**.

Uma tela com as políticas disponíveis aparece.

Choose Type > Rewrite Policies

Rewrite Policies

Select **Add** **Edit** **Delete** **Show Bindings** **Policy Manager** **Statistics** **Action**

Show built-in Rewrite Policies Search

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	X

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

Choose Type

Policies

Choose Policy
Rewrite

Choose Type
Response

Policy Binding

Select Policy*
InsertGatewayAuthTypePolicy

► More

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.

Enable DH Param **DISABLED**
Enable Ephemeral RSA **ENABLED**
Refresh Count **0**
Enable Session Reuse **ENABLED**
Time-out **120**
SSL Redirect **DISABLED**

Clear Text Port **0**
Enable Cipher Redirect **DISABLED**
Client Authentication **ENABLED**
Client Certificate **Mandatory**
Send Close-Notify **YES**
PUSH Encryption Trigger **Always**
SNI Enable **DISABLED**

SSLv2 Redirect **DISABLED**
SSLv2 **DISABLED**
SSLv3 **ENABLED**
TLSv1 **ENABLED**
TLSv1.1 **ENABLED**
TLSv1.2 **ENABLED**

SSL Ciphers
SSL Policies
Profiles
Intranet IP Addresses
Intranet Applications

Published Applications

No Next HOP Server
1 STA Server
No Url

Other Settings

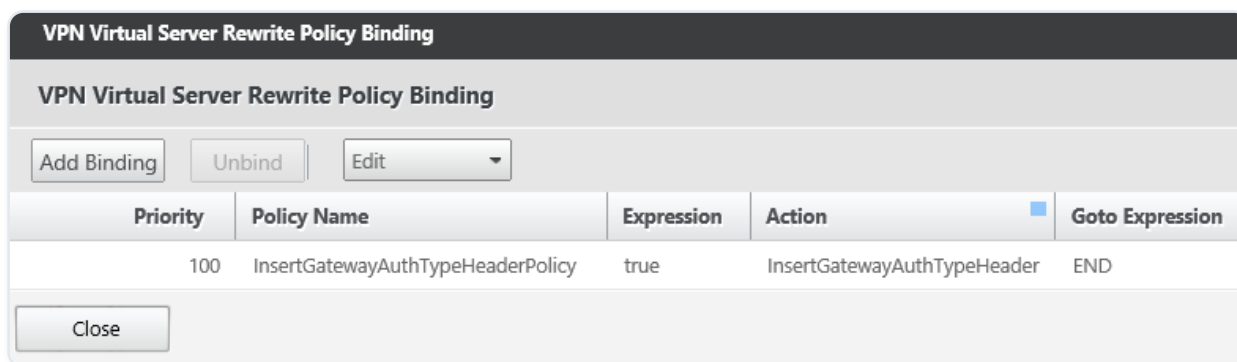
ICMP Virtual Server Response **Passive**
RHI State **Passive**
Redirect to Home page **true**

Listen Priority
Listen Policy Expression **None**
ShareFile
AppController **https://xms3.dm.com:8443**
L2 Connection **false**

Policies

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

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



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

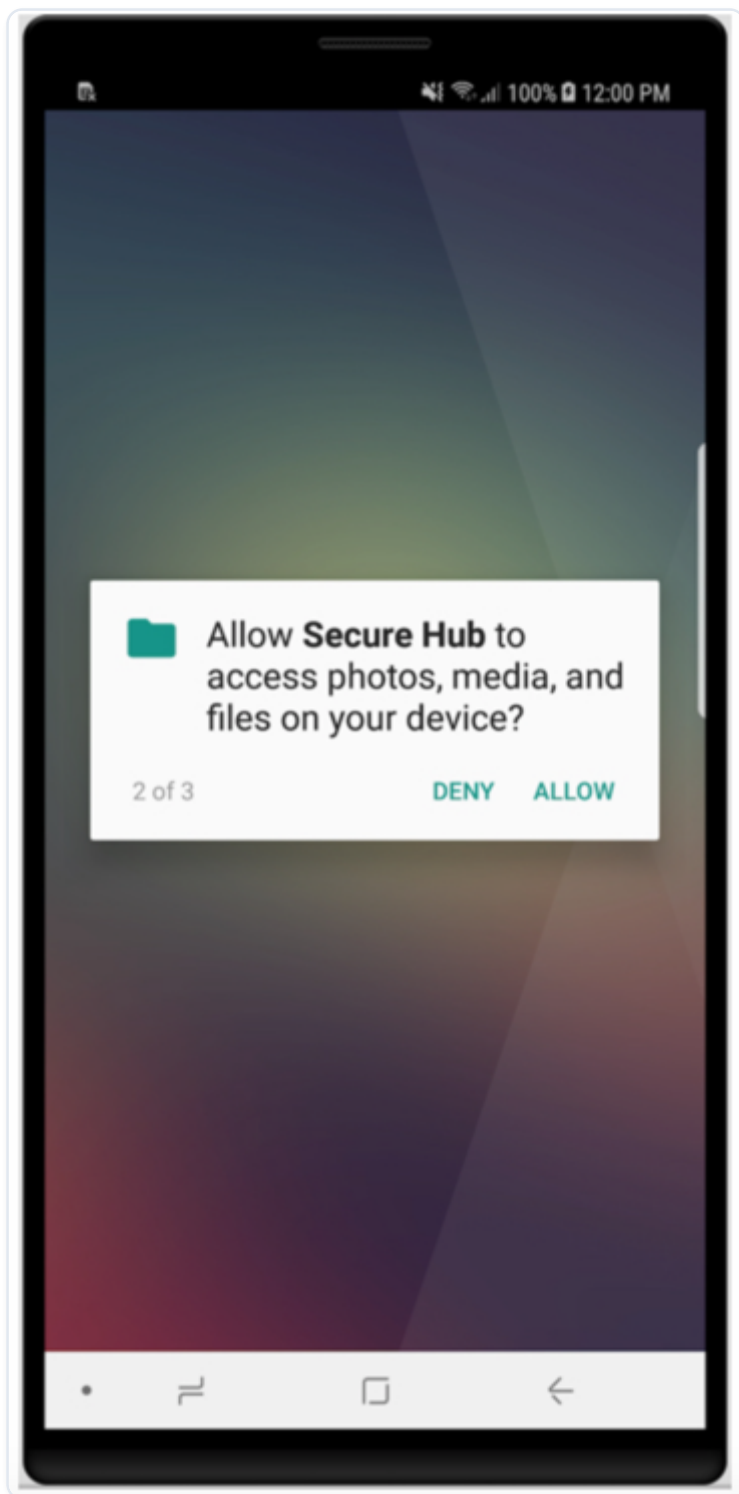
O Secure Hub permite que você monitore e imponha políticas móveis ao mesmo tempo em que fornece acesso à Loja e suporte ao vivo. Os usuários começam baixando o Secure Hub em seus dispositivos da loja de aplicativos da Apple, Android ou Windows.

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](#).

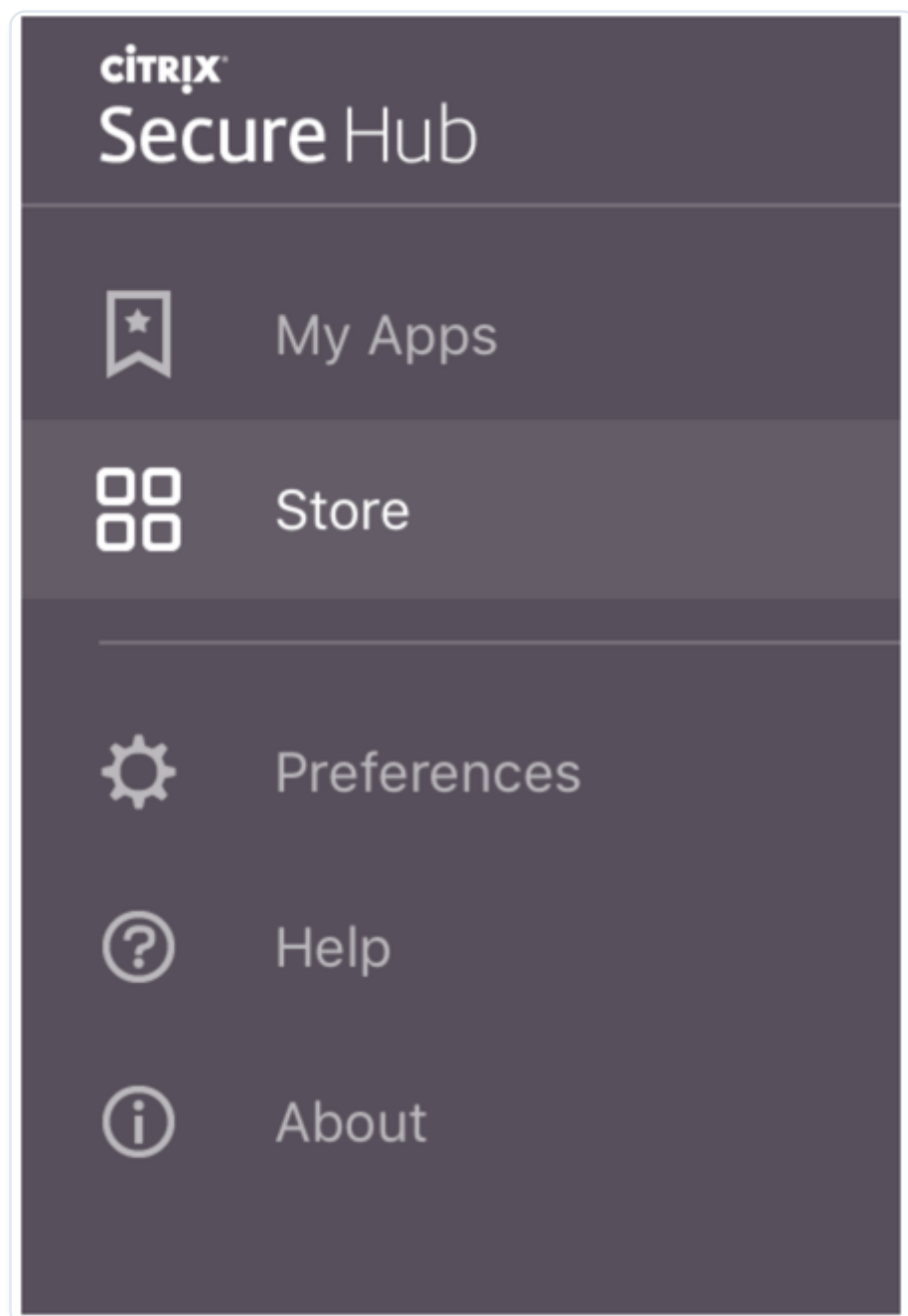
No Secure Hub para Android, durante a instalação inicial e o registro, a seguinte mensagem aparece: Permitir que o Secure Hub acesse fotos, mídias e arquivos em seu dispositivo?

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 'Configure' page. 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)'. The 'App Information' form contains the following fields: '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**.

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 the 'Help Desk' screen. At the top, there is a 'Close' button and the title 'Help Desk'. Below the title, there are three main options: 'Your IT Department', 'Report Issue', and 'Send Feedback to Citrix'. Each option has a right-pointing arrow. At the bottom of the screen, there is a 'Citrix Support' button.

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.

XenMobile Analyze Manage Configure

Settings > Client Support

Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)*

Send device logs to IT help desk ☐ directly ☐ by email

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.

Visão geral do Secure Mail

O Citrix Secure Mail™ permite que os usuários gerenciem seus e-mails, calendários e contatos em seus telefones celulares e tablets. Para manter a continuidade das contas do Microsoft Outlook ou IBM Notes, o Secure Mail sincroniza com o Microsoft Exchange Server e o IBM Notes Traveler Server.

Como parte do conjunto de aplicativos Citrix, o Secure Mail se beneficia da compatibilidade de logon único (SSO) com o Citrix Secure Hub. Depois que os usuários fazem logon no Secure Hub, eles podem passar facilmente para o Secure Mail sem precisar reinserir seus nomes de usuário e senhas. Você pode configurar o Secure Mail para ser enviado automaticamente para os dispositivos dos usuários quando os dispositivos se registrarem no Secure Hub, ou os usuários podem adicionar o aplicativo da Loja.

NOTA:

- O suporte para o Exchange Server 2010 terminou em October 13, 2020.
- O suporte para o Exchange Server 2013 terminou em April 11, 2023.

O Secure Mail é compatível com:

- Exchange Server SE RTM
- Exchange Server 2019 Atualização Cumulativa 15
- Exchange Server 2019 Atualização Cumulativa 14
- Exchange Server 2019 Atualização Cumulativa 13
- Exchange Server 2019 Atualização Cumulativa 12
- Exchange Server 2019 Atualização Cumulativa 11
- Exchange Server 2019 Atualização Cumulativa 10
- Exchange Server 2019 Atualização Cumulativa 9
- Exchange Server 2019 Atualização Cumulativa 8
- Exchange Server 2019 Atualização Cumulativa 7

- Exchange Server 2019 Atualização Cumulativa 6
- Exchange Server 2016 Atualização Cumulativa 23
- Exchange Server 2016 Atualização Cumulativa 22
- Exchange Server 2016 Atualização Cumulativa 21
- Exchange Server 2016 Atualização Cumulativa 20
- Exchange Server 2016 Atualização Cumulativa 19
- Exchange Server 2016 Atualização Cumulativa 18
- Exchange Server 2016 Atualização Cumulativa 17
- HCL Domino versão 14.0 FP1
- HCL Domino versão 12.0.2 FP2
- HCL Traveler versão 12.0.2.1 Build 202302010413_30
- HCL Domino 11 (anteriormente Lotus Notes)
- HCL Domino 10.0.1 (anteriormente Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (anteriormente Lotus Notes)
- HCL Domino 10.0.1.0 build 201811191126_20 (anteriormente Lotus Notes)
- HCL Domino 9.0.1.21 (anteriormente Lotus Notes)
- Microsoft Office 365 (Exchange Online)

Para começar, baixe o Secure Mail e outros componentes do Endpoint Management em [Citrix Endpoint Management Downloads](#).

Para os requisitos de sistema do Secure Mail e de outros aplicativos de mobilidade, consulte [System requirements](#).

Para obter informações sobre notificações no Secure Mail para iOS e Android quando o aplicativo está sendo executado em segundo plano ou fechado, consulte [Push notifications for Secure Mail](#).

Para recursos do iOS compatíveis com o Secure Mail, consulte [iOS features for Secure Mail](#).

Para recursos do Android compatíveis com o Secure Mail, consulte [Android features for Secure Mail](#).

Para recursos do iOS e Android compatíveis com o Secure Mail, consulte [iOS and Android features for Secure Mail](#).

Para a documentação de ajuda do usuário, consulte a página [Citrix Secure Mail](#) no Centro de Ajuda do Usuário da Citrix.

Citrix Secure Web™

O Citrix Secure Web é um navegador da web móvel compatível com HTML5 que fornece acesso seguro a sites internos e externos. Você pode configurar o Secure Web para ser enviado automaticamente para os dispositivos dos usuários quando os dispositivos são registrados no Secure Hub. Alternativamente, você pode adicionar o aplicativo da loja de aplicativos do Endpoint Management.

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

Integrando e entregando o Secure Web

NOTA:

O MDX Toolkit 10.7.10 é a versão final que oferece suporte ao empacotamento de aplicativos de produtividade móvel. Os usuários acessam as versões 10.7.5 e posteriores dos aplicativos de produtividade móvel nas lojas de aplicativos públicas.

Para integrar e entregar o Secure Web, siga estas etapas gerais:

1. Para habilitar o Single sign-on (SSO) para a rede interna, configure o Citrix Gateway.

Para tráfego HTTP, o Citrix ADC pode fornecer SSO para todos os tipos de autenticação de proxy suportados pelo Citrix ADC. Para tráfego HTTPS, a política de cache de senha da Web permite que o Secure Web autentique e forneça SSO ao servidor proxy por meio do MDX. O MDX suporta apenas autenticação de proxy básica, digest e NTLM. A senha é armazenada em cache usando MDX e armazenada no cofre compartilhado do Endpoint Management, uma área de armazenamento segura para dados de aplicativos confidenciais. Para obter detalhes sobre a configuração do Citrix Gateway, consulte [Citrix Gateway](#).

2. Baixe o Secure Web.
3. Determine como você deseja configurar as conexões do usuário com a rede interna.
4. Adicione o Secure Web ao Endpoint Management, usando as mesmas etapas que para outros aplicativos MDX e, em seguida, configure as políticas MDX. Para obter detalhes sobre políticas

específicas do Secure Web, consulte "Sobre as políticas do Secure Web" posteriormente neste artigo.

Configurando conexões de usuário

O Secure Web suporta as seguintes configurações para conexões de usuário:

- **Tunneled – Web SSO:** As conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, conhecida como Tunneled – Web SSO. Esta é a configuração padrão especificada para a política **Preferred VPN mode**. O Tunneled – Web SSO é recomendado para conexões que exigem single sign-on (SSO).
- **Túnel VPN completo:** As conexões que fazem túnel para a rede interna podem usar um túnel VPN completo, configurado pela política de modo **Preferred VPN**. O túnel VPN completo é recomendado para conexões que usam certificados de cliente ou SSL de ponta a ponta para um recurso na rede interna. O Secure Web, no entanto, não é um aplicativo que pode ler certificados de cliente armazenados em um dispositivo móvel. Alguns aplicativos empresariais de terceiros, empacotados, podem ser instalados e oferecer essa capacidade. O túnel VPN completo lida com qualquer protocolo sobre TCP e pode ser usado com computadores Windows e Mac, além de dispositivos iOS e Android.
- A política **Permit VPN mode switching** permite a alternância automática entre os modos de túnel VPN completo e Tunneled – Web SSO conforme necessário. Por padrão, esta política está desativada. Quando esta política está ativada, uma solicitação de rede que falha devido a uma solicitação de autenticação que não pode ser tratada no modo VPN preferencial é repetida no modo alternativo. Por exemplo, o modo de túnel VPN completo acomoda desafios de servidor para certificados de cliente, mas não o modo Tunneled – Web SSO. Da mesma forma, os desafios de autenticação HTTP são mais propensos a serem atendidos com SSO ao usar o modo Tunneled – Web SSO.

A tabela a seguir indica se o Secure Web solicita credenciais a um usuário, com base na configuração e no tipo de site:

MODO DE CONEXÃO	TIPO DE SITE	CACHE DE SENHA	SSO CONFIGURADO PARA CITRIX GATEWAY	O SECURE WEB SOLICITA CREDENCIAIS NO PRIMEIRO ACESSO A UM SITE	O SECURE WEB SOLICITA CREDENCIAIS EM ACESSOS SUBSEQUENTES AO SITE	O SECURE WEB SOLICITA CREDENCIAIS APÓS A ALTERAÇÃO DA SENHA
Tunneled – Web SSO	HTTP	Não	Sim	Não	Não	Não
Tunelado – Web SSO	HTTPS	Não	Sim	Não	Não	Não
VPN Completa	HTTP	Não	Sim	Não	Não	Não
VPN Completa	HTTPS	Sim; Se a política MDX do Secure Web 'Habilitar cache de senha da web' estiver ativada.	Não	Sim; Necessário para armazenar a credencial em cache no Secure Web.	Não	Sim

Políticas do Secure Web

Ao adicionar o Secure Web, esteja ciente destas políticas MDX específicas do Secure Web. Para todos os dispositivos móveis suportados:

Sites permitidos ou bloqueados

O Secure Web normalmente não filtra links da web. Você pode usar esta política para configurar uma lista específica de sites permitidos ou bloqueados. Você configura padrões de URL para restringir os sites que o navegador pode abrir, formatados como uma lista separada por vírgulas. Um sinal de mais (+) ou menos (-) precede cada padrão na lista. O navegador compara uma URL com os padrões na ordem listada até que uma correspondência seja encontrada. Quando uma correspondência é encontrada, o prefixo decide a ação a ser tomada, da seguinte forma:

- Um prefixo de menos (-) instrui o navegador a bloquear a URL. Neste caso, a URL é tratada como se o endereço do servidor web não pudesse ser resolvido.
- Um prefixo de mais (+) permite que a URL seja processada normalmente.
- Se nem + nem - for fornecido com o padrão, + (permitir) é assumido.
- Se a URL não corresponder a nenhum padrão na lista, a URL será permitida

Para bloquear todas as outras URLs, termine a lista com um sinal de menos seguido por um asterisco (*). Por exemplo:

- O valor da política `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permite URLs HTTP dentro do domínio `mycorp.com`, mas as bloqueia em outros lugares, permite URLs HTTPS e FTP em qualquer lugar e bloqueia todas as outras URLs.
- O valor da política `+http://*.training.lab/*,+https://*.training.lab/*,-*` permite que os usuários abram quaisquer sites no domínio Training.lab (intranet) via HTTP ou HTTPS. No entanto, você não pode abrir URLs públicas como Facebook, Google e Hotmail, independentemente do protocolo.

O valor padrão está vazio (todas as URLs permitidas).

Bloquear pop-ups

Pop-ups são novas abas que os sites abrem sem sua permissão. Esta política determina se o Secure Web permite pop-ups. Se Ativado, o Secure Web impede que os sites abram pop-ups. O valor padrão é Desativado.

Favoritos pré-carregados

Define um conjunto pré-carregado de favoritos para o navegador Secure Web. A política é uma lista de tuplas separadas por vírgulas que incluem um nome de pasta, nome amigável e endereço da web. Cada trio deve ter a forma pasta, nome, url, onde pasta e nome podem opcionalmente ser incluídos entre aspas duplas (").

Por exemplo, os valores da política `"Mycorp, Inc. home page",https://www.mycorp.com,"MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx` definem três favoritos. O primeiro é um link principal (sem nome de pasta) intitulado "Mycorp, Inc. home page". O segundo link é colocado em uma pasta intitulada "MyCorp Links" e rotulado como "Account logon". O terceiro é colocado na subpasta "Investor Relations" da pasta "MyCorp Links" e exibido como "Contact us".

O valor padrão está vazio.

URL da página inicial

Define o site que o Secure Web carrega ao ser iniciado. O valor padrão está vazio (página inicial padrão).

Apenas para dispositivos Android e iOS compatíveis:

Interface do usuário do navegador

Ditado o comportamento e a visibilidade dos controles da interface do usuário do navegador para o Secure Web. Normalmente, todos os controles de navegação estão disponíveis. Isso inclui avançar, voltar, barra de endereço e os controles de atualização/parada. Você pode configurar esta política para restringir o uso e a visibilidade de alguns desses controles. O valor padrão é Todos os controles visíveis.

Opções

- Todos os controles visíveis. Todos os controles estão visíveis e os usuários não são impedidos de usá-los.
- Barra de endereço somente leitura. Todos os controles estão visíveis, mas os usuários não podem editar o campo de endereço do navegador.
- Ocultar barra de endereço. Oculta a barra de endereço, mas não outros controles.
- Ocultar todos os controles. Suprime toda a barra de ferramentas para fornecer uma experiência de navegação sem moldura.

Habilitar cache de senha da web

Quando os usuários do Secure Web inserem credenciais ao acessar ou solicitar um recurso da web, esta política determina se o Secure Web armazena silenciosamente a senha em cache no

dispositivo. Esta política se aplica a senhas inseridas em diálogos de autenticação e não a senhas inseridas em formulários da web.

Se **Ativado**, o Secure Web armazena em cache todas as senhas que os usuários inserem ao solicitar um recurso da web. Se **Desativado**, o Secure Web não armazena senhas em cache e remove as senhas em cache existentes. O valor padrão é **Desativado**.

Esta política é habilitada somente quando você também define a política de VPN Preferencial como Túnel VPN completo para este aplicativo.

Servidores proxy

Você também pode configurar servidores proxy para o Secure Web quando usado no modo Tunneled – Web SSO. Para obter detalhes, consulte esta [publicação do blog](#).

Sufixos DNS

No Android, se os sufixos DNS não estiverem configurados, a VPN pode falhar. Para obter detalhes sobre como configurar sufixos DNS, consulte [Suporte a consultas DNS usando sufixos DNS para dispositivos Android](#).

Preparando sites de intranet para o Secure Web

Esta seção é para desenvolvedores de sites que precisam preparar um site de intranet para uso com o Secure Web para Android e iOS. Sites de intranet projetados para navegadores de desktop exigem alterações para funcionar corretamente em dispositivos Android e iOS.

O Secure Web depende do Android WebView e do iOS WKWebView para fornecer suporte à tecnologia web. Algumas das tecnologias web suportadas pelo Secure Web são:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets

Algumas das tecnologias web não suportadas pelo Secure Web são:

- Flash

- Java

A tabela a seguir mostra os recursos e tecnologias de renderização HTML suportados pelo Secure Web. X indica que o recurso está disponível para uma combinação de plataforma, navegador e componente.

TECNOLOGIA	SECURE WEB PARA IOS	SECURE WEB PARA ANDROID 6.X/7.X
Mecanismo JavaScript	JavaScriptCore	V8
Armazenamento Local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
fonte	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

As tecnologias funcionam da mesma forma em todos os dispositivos; no entanto, o Secure Web retorna diferentes strings de agente de usuário para diferentes dispositivos. Para determinar a versão do navegador usada para o Secure Web, você pode visualizar sua string de agente de usuário. No Secure Web, navegar para `<https://whatsmyuseragent.com/>`.

Solução de problemas de sites de intranet

Para solucionar problemas de renderização quando seu site de intranet é visualizado no Secure Web, compare como o site é renderizado no Secure Web e em um navegador de terceiros compatível.

Para iOS, os navegadores de terceiros compatíveis para teste são Chrome e Dolphin.

Para Android, o navegador de terceiros compatível para testes é o Dolphin.

NOTA:

O Chrome é um navegador nativo no Android. Não o use para a comparação.

No iOS, certifique-se de que os navegadores tenham suporte a VPN no nível do dispositivo. Você pode configurar a VPN no dispositivo navegando até **Ajustes > VPN > Adicionar Configuração de VPN**.

Você também pode usar aplicativos cliente VPN disponíveis na App Store, como [Citrix VPN](#), [Cisco AnyConnect](#) ou [Pulse Secure](#).

- Se uma página da web é renderizada da mesma forma nos dois navegadores, o problema está no seu site. Atualize seu site e certifique-se de que ele funcione bem para o SO.
- Se o problema em uma página da web aparecer apenas no Secure Web, entre em contato com o Suporte Citrix para abrir um tíquete de suporte. Forneça suas etapas de solução de problemas, incluindo o navegador testado e os tipos de SO. Se o Secure Web para iOS tiver problemas de renderização, inclua um arquivo de arquivo da web da página, conforme descrito nas etapas a seguir. Isso ajuda a Citrix a resolver o problema mais rapidamente.

Para criar um arquivo de arquivo da web

Usando o Safari no macOS 10.9 ou posterior, você pode salvar uma página da web como um arquivo de arquivo da web (referido como uma lista de leitura). O arquivo de arquivo da web inclui todos os arquivos vinculados, como imagens, CSS e JavaScript.

1. No Safari, esvazie a pasta Lista de Leitura: No **Finder**, clique no menu **Ir** na barra de **Menu**, escolha **Ir para a Pasta**, digite o nome do caminho ~/Library/Safari/ReadingListArchives/ e, em seguida, exclua todas as pastas nesse local.
2. Na barra de **Menu**, vá para **Safari > Preferências > Avançado** e ative **Mostrar menu Desenvolvedor** na barra de menu.
3. Na barra de **Menu**, vá para **Desenvolver > Agente do Usuário** e insira o agente do usuário do Secure Web: (Mozilla/5.0 (iPad; CPU OS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. No Safari, abra o site que você deseja salvar como uma lista de leitura (arquivo de arquivo da web).

5. Na barra de **Menu**, vá para **Favoritos > Adicionar à Lista de Leitura**. O arquivamento ocorre em segundo plano e pode levar alguns minutos.
6. Localize a lista de leitura arquivada: Na barra de **Menu**, vá para **Visualizar > Mostrar Barra Lateral da Lista de Leitura**.
7. Verificar o arquivo morto:
 - Desative a conectividade de rede do seu Mac.
 - Abra o site da lista de leitura.

O site é renderizado completamente.
8. Comprima o arquivo morto: No **Finder**, clique no menu **Ir** na barra de **Menu**, escolha **Ir para Pasta**, digite o nome do caminho ~/Library/Safari/ReadingListArchives/. Agora, comprima a pasta que tem uma string hexadecimal aleatória como nome de arquivo. Você pode enviar este arquivo para o suporte da Citrix ao abrir um tíquete de suporte.

Recursos do Secure Web

O Secure Web usa tecnologias de troca de dados móveis para criar um túnel VPN dedicado para que os usuários acessem sites internos e externos e todos os outros sites. Isso inclui sites com informações confidenciais, em um ambiente protegido pelas políticas da sua organização.

A integração do Secure Web com o Secure Mail e o Citrix Files oferece uma experiência de usuário perfeita dentro do contêiner seguro do Endpoint Management. Aqui estão alguns exemplos de recursos de integração:

- Quando os usuários tocam em links **Mailto**, uma nova mensagem de e-mail é aberta no Citrix Secure Mail™ sem necessidade de autenticação adicional.
- No iOS, os usuários podem abrir um link no Secure Web a partir de um aplicativo de e-mail nativo inserindo **ctxmobilebrowser://** na frente da URL. Por exemplo, para abrir `example.com` de um aplicativo de e-mail nativo, use a URL `ctxmobilebrowser://example.com`.
- Quando os usuários clicam em um link de intranet em uma mensagem de e-mail, o Secure Web acessa esse site sem necessidade de autenticação adicional.
- Os usuários podem carregar arquivos para o Citrix Files que eles baixam da web no Secure Web.

Os usuários do Secure Web também podem realizar as seguintes ações:

- Bloquear pop-ups.

NOTA:

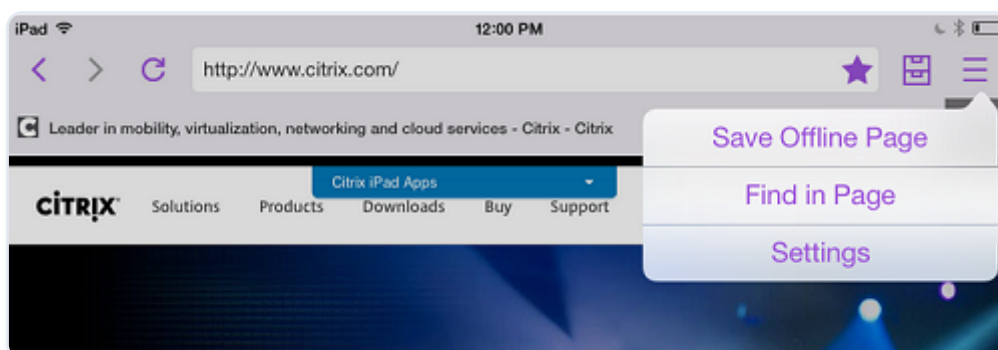
Grande parte da memória do Secure Web é usada para renderizar pop-ups, então o desempenho geralmente é melhorado bloqueando pop-ups em Configurações.

- Adicionar aos favoritos seus sites preferidos.
- Baixar arquivos.
- Salvar páginas offline.
- Salvar senhas automaticamente.
- Limpar cache/histórico/cookies.
- Desabilitar cookies e armazenamento local HTML5.
- Compartilhar dispositivos com segurança com outros usuários.
- Pesquisar na barra de endereços.
- Permitir que aplicativos web executados com o Secure Web acessem sua localização.
- Exportar e importar configurações.
- Abrir arquivos diretamente no Citrix Files sem precisar baixá-los. Para habilitar este recurso, adicione **ctx-sf** à política de URLs Permitidas no Endpoint Management.
- No iOS, use as ações 3D Touch para abrir uma nova guia e acessar páginas offline, sites favoritos e downloads diretamente da tela inicial.
- No iOS, baixe arquivos de qualquer tamanho e abra-os no Citrix Files ou em outros aplicativos.

NOTA:

Colocar o Secure Web em segundo plano faz com que o download pare.

- Pesquise um termo na exibição da página atual usando **Localizar na Página**.



O Secure Web também oferece suporte a texto dinâmico. O aplicativo exibe a fonte que os usuários definem em seus dispositivos.

NOTA:

- O Citrix Files para XenMobile atingiu o EOL em July 1, 2023. Para obter mais informações, consulte [Aplicativos EOL e descontinuados](#)

Citrix Content Collaboration™ para Endpoint Management

Os clientes do Citrix Content Collaboration para Endpoint Management são versões compatíveis com MDX dos clientes móveis do Citrix Files. Esses clientes fornecem acesso seguro e integrado a dados em outros aplicativos empacotados em MDX. Os clientes do Citrix Content Collaboration para Endpoint Management também se beneficiam dos recursos MDX, como micro VPN, logon único (SSO) com Secure Hub e autenticação de dois fatores.

O Citrix Files é um serviço de sincronização e compartilhamento de arquivos corporativos que permite aos usuários trocar documentos de forma fácil e segura. O Citrix Files oferece aos usuários várias opções de acesso, incluindo clientes móveis do Citrix Files, como Citrix Files para Android Phone e Citrix Files para iPad.

Você pode integrar o Citrix Files ao Endpoint Management para fornecer o conjunto completo de recursos do Citrix Files ou para fornecer acesso apenas aos conectores de zonas de armazenamento. Por padrão, o console do Citrix Endpoint Management permite a configuração apenas do Citrix Files. Para configurar o Endpoint Management para uso com conectores de zonas de armazenamento, consulte [Usar o Citrix Content Collaboration com o Endpoint Management](#) na documentação do Citrix Endpoint Management.

Você usa o Endpoint Management, Citrix Files, controlador de zonas de armazenamento e Citrix ADC da seguinte forma para implantar e gerenciar clientes do Citrix Content Collaboration para Endpoint Management:

- Quando o Endpoint Management é configurado com o Citrix Files, o Endpoint Management atua como um provedor de identidade SAML (IdP) e implanta clientes do Citrix Content Collaboration para Endpoint Management. O Citrix Files gerencia os dados do Citrix Files. Nenhum dado do Citrix Files trafega pelo Endpoint Management.
- Quando o Endpoint Management é configurado com o Citrix Files ou com conectores de zonas de armazenamento, o controlador de zonas de armazenamento fornece conectividade a dados em compartilhamentos de rede e SharePoint. Os usuários acessam seus dados armazenados por meio dos aplicativos de produtividade móvel do Citrix Files. Os usuários podem editar documentos do Microsoft Office, visualizar e anotar arquivos PDF da Adobe a partir de dispositivos móveis.

- O Citrix ADC gerencia solicitações de usuários externos, protegendo suas conexões, balanceando a carga das solicitações e lidando com a troca de conteúdo para conectores de zonas de armazenamento.

Para os requisitos de sistema do Citrix Content Collaboration para Endpoint Management e outros aplicativos de produtividade móvel, consulte [Suporte para aplicativos de produtividade móvel](#).

Como os clientes do Citrix Content Collaboration para Endpoint Management diferem dos clientes móveis do Citrix Files

O seguinte descreve as diferenças entre os clientes do Citrix Content Collaboration para Endpoint Management e os clientes móveis do Citrix Files.

Acesso do usuário

Clientes do Citrix Content Collaboration para Endpoint Management:

Os usuários obtêm e abrem clientes do Citrix Content Collaboration para Endpoint Management do Secure Hub.

Clientes móveis do Citrix Files:

Os usuários obtêm clientes móveis do Citrix Files em lojas de aplicativos.

SSO

Clientes do Citrix Content Collaboration para Endpoint Management:

Para integração do Endpoint Management com o Citrix Files: Você pode configurar o Endpoint Management como um IdP SAML para o Citrix Files. Nesta configuração, o Secure Hub obtém um token SAML para o cliente Citrix Content Collaboration para Endpoint Management, usando o Endpoint Management como o IdP SAML. Um usuário que inicia o cliente Citrix Content Collaboration para Endpoint Management, mas não está conectado ao Secure Hub, é solicitado a fazer login no Secure Hub. O usuário não precisa saber seu domínio ou informações de conta do Citrix Files.

Clientes móveis do Citrix Files:

Você pode configurar o Endpoint Management e o Citrix Gateway como um IdP SAML para o Citrix Files. Nesta configuração, um usuário que faz login no Citrix Files usando um navegador da web ou outros clientes do Citrix Files é redirecionado para o ambiente do Endpoint Management

para autenticação do usuário. Após a autenticação bem-sucedida pelo Endpoint Management, o usuário recebe um token SAML válido para fazer login em sua conta do Citrix Files.

Micro VPN

Clientes do Citrix Content Collaboration para Endpoint Management:

Usuários remotos podem se conectar usando uma conexão VPN ou micro VPN através do Citrix Gateway para acessar aplicativos e desktops na rede interna. Este recurso, disponível através da integração do Citrix ADC com o Endpoint Management, é transparente para os usuários.

Clientes móveis do Citrix Files:

Não aplicável.

Autenticação de dois fatores

Clientes do Citrix Content Collaboration para Endpoint Management:

A integração do Citrix ADC com o Endpoint Management também suporta autenticação usando uma combinação de autenticação por certificado de cliente e outro tipo de autenticação, como LDAP ou RADIUS.

Clientes móveis do Citrix Files:

Não aplicável.

Permissões de pasta

Clientes do Citrix Content Collaboration para Endpoint Management e clientes móveis do Citrix Files:

Para integração do Endpoint Management com o Citrix Files: Determinado pelo Citrix Files.

Proteção de acesso a documentos

Clientes do Citrix Content Collaboration para Endpoint Management:

Os usuários podem abrir anexos recebidos no Secure Mail ou baixados por qualquer aplicativo empacotado com MDX. Somente aplicativos empacotados com MDX aparecem quando o usuário executa uma ação Abrir em. Dados de um aplicativo não empacotado não estão disponíveis para um cliente do Citrix Content Collaboration para Endpoint Management. Os usuários do Secure Mail podem anexar arquivos de seu repositório do Citrix Files sem precisar baixar o arquivo para o

dispositivo. Se um usuário tiver o Citrix Files empacotado e não empacotado em um dispositivo, o cliente Citrix Files empacotado não poderá acessar arquivos na conta pessoal do Citrix Files do usuário. O cliente Citrix Files empacotado pode acessar apenas o subdomínio do Citrix Files configurado no Endpoint Management.

Clientes móveis do Citrix Files:

Os usuários podem abrir anexos de qualquer aplicativo.

Acesso à conta do Citrix Files

Clientes do Citrix Content Collaboration para Endpoint Management:

Para integração do Endpoint Management com o Citrix Files: Para acessar uma conta pessoal do Citrix Files ou uma conta de terceiros do Citrix Files, os usuários devem usar uma versão não-MDX do Citrix Files no dispositivo.

Clientes móveis do Citrix Files:

Para integração do Endpoint Management com o Citrix Files: Disponível nos clientes do Citrix Files.

Políticas de dispositivo

Clientes Citrix Content Collaboration para Endpoint Management e clientes móveis Citrix Files:

As políticas de dispositivo do Endpoint Management e do Citrix Files se aplicam aos clientes Citrix Content Collaboration para Endpoint Management. Por exemplo, no console do Endpoint Management, você pode realizar uma limpeza de dispositivo. No console do Citrix Files, você pode limpar remotamente o aplicativo Citrix Files.

Políticas MDX

Clientes Citrix Content Collaboration para Endpoint Management:

As políticas MDX permitem configurar as definições no Citrix Endpoint Management™ que a loja de aplicativos do Endpoint Management impõe. As políticas disponíveis apenas através do MDX incluem a capacidade de bloquear a câmera, microfone, composição de e-mail, captura de tela e operações de recortar, copiar e colar da área de transferência.

Clientes móveis Citrix Files:

Não aplicável.

Criptografia de dados

Clientes Citrix Content Collaboration para Endpoint Management e clientes móveis Citrix Files:

Criptografa todos os dados armazenados usando AES-256 e protege os dados em trânsito com SSL 3.0 e um mínimo de criptografia de 128 bits.

Disponibilidade

Clientes Citrix Content Collaboration para Endpoint Management:

Os clientes Citrix Content Collaboration para Endpoint Management estão incluídos nas edições Advanced e Enterprise do Endpoint Management.

Clientes móveis Citrix Files:

Todas as edições do Endpoint Management incluem todos os recursos do Citrix Files. Você pode integrar o Endpoint Management com o conjunto completo de recursos do Citrix Files ou apenas com os conectores de zonas de armazenamento.

Integrando e entregando o Citrix Content Collaboration para clientes do Endpoint Management

Para integrar e entregar o Citrix Content Collaboration para clientes do Endpoint Management, siga estas etapas gerais:

1. Habilite o Endpoint Management como um IdP SAML para o Citrix Files, para fornecer SSO de clientes do Citrix Files para o Citrix Files. Para fazer isso, você deve configurar as informações da conta do Citrix Files no Endpoint Management. Para obter mais informações, consulte a seção "Para configurar as informações da conta do Citrix Files no Endpoint Management para SSO".

IMPORTANTE:

Para usar o Endpoint Management como um IdP SAML para clientes do Citrix Files que não são MDX, como o aplicativo web do Citrix Files e os clientes do Citrix Files Sync, é necessária uma configuração extra.

2. Baixe os clientes do Citrix Files.
3. Adicione os clientes do Citrix Files ao Endpoint Management. Para obter detalhes, consulte "Para adicionar o Citrix Files ao Endpoint Management" mais adiante neste artigo.

4. Valide sua configuração. Para obter detalhes, consulte "Para validar clientes do Citrix Files" mais adiante neste artigo.

Sobre as configurações:

- Domínio é o subdomínio do Citrix Files a ser usado para os clientes.
- Somente os usuários nos DGs selecionados têm acesso SSO ao Citrix Files a partir dos clientes.

Se um usuário em um DG não tiver uma conta do Citrix Files, o Endpoint Management provisionará o usuário no Citrix Files quando você adicionar o cliente do Citrix Files ao Endpoint Management.

- As informações de login da conta de administrador do Citrix Files são usadas pelo Endpoint Management para salvar as configurações SAML no plano de controle do Citrix Files.

IMPORTANTE:

A configuração que permite o SSO de clientes do Citrix Files para o Citrix Files não autenticar usuários em compartilhamentos de rede ou bibliotecas de documentos do SharePoint. O acesso a essas fontes de dados de conector requer autenticação no domínio do Active Directory no qual os compartilhamentos de rede ou servidores SharePoint residem.

Para configurar as informações da conta do Citrix Files no Endpoint Management para SSO

Para habilitar o SSO do Secure Hub para aplicativos de produtividade móvel, você especifica as informações da conta do Citrix Files e da conta de serviço do administrador do Citrix Files no console do Endpoint Management. Com essa configuração, o Endpoint Management atua como um IdP SAML para o Citrix Files, para clientes de aplicativos de produtividade móvel, clientes do Citrix Files e clientes do Citrix Files não-MDX. Quando um usuário inicia um cliente de aplicativo de produtividade móvel, o Secure Hub obtém um token SAML para o usuário do Endpoint Management e o envia para o cliente do Citrix Files.

No console do Endpoint Management, clique em **Configurar > Content Collaboration**, que é o nome anterior do Citrix Files.

Para adicionar clientes do Citrix Content Collaboration para Endpoint Management ao Endpoint Management

Ao adicionar clientes do Citrix Content Collaboration para Endpoint Management ao Endpoint Management, você pode habilitar o acesso SSO a fontes de dados do Conector a partir de clientes do Citrix Content Collaboration para Endpoint Management. Para fazer isso, configure a política de acesso à rede e a política de modo VPN preferencial, conforme descrito nesta seção.

Pré-requisitos

- O Endpoint Management deve ser capaz de alcançar seu subdomínio do Citrix Files. Para testar a conexão, faça ping no seu subdomínio do Citrix Files a partir do servidor Endpoint Management.
- O fuso horário configurado para sua conta do Citrix Files e para o hypervisor que executa o Endpoint Management deve ser o mesmo. Se o fuso horário for diferente, as solicitações de SSO podem falhar porque o token SAML pode não chegar ao Citrix Files dentro do prazo esperado. Para configurar o servidor NTP para o Endpoint Management, use a interface de linha de comando do Endpoint Management.

NOTA:

O host Hyper-V define a hora em uma VM Linux para o fuso horário local e não UTC.

- Faça login na conta do ShareFile como administrador e verifique as configurações de SSO SAML em **Configurações > Configurações de Administrador > Segurança > Política de Login e Segurança > Configuração de logon único / SAML 2.0**.

- Baixe os clientes do Citrix Content Collaboration para Endpoint Management.

Etapas:

1. No console do Endpoint Management, clique em **Configurar > Aplicativos** e, em seguida, clique em **Adicionar**.
2. Clique em **MDX**.
3. Insira um **Nome** e, opcionalmente, uma **Descrição** e **Categoria do aplicativo** para o aplicativo.
4. Clique em **Avançar** e, em seguida, carregue o arquivo .mdx para o cliente Citrix Content Collaboration for Endpoint Management.
5. Clique em **Avançar** para configurar as informações e políticas do aplicativo.

A configuração que permite o SSO de clientes Citrix Content Collaboration for Endpoint Management para o Citrix Files não autenticar usuários em compartilhamentos de rede ou bibliotecas de documentos do SharePoint.

6. Para habilitar o SSO entre a micro VPN do Secure Hub e o controlador de zonas de armazenamento, conclua a seguinte configuração de política:

- Defina a política de acesso à rede como **Tunneled to the internal network**.

Nesse modo, a estrutura MDX intercepta todo o tráfego de rede do cliente Citrix Content Collaboration for Endpoint Management. O tráfego de rede é então redirecionado através do Citrix Gateway usando uma micro VPN específica do aplicativo.

- Defina a política de modo VPN preferencial como **Tunneled – Web SSO**.

Nesse modo de tunelamento, a estrutura MDX encerra o tráfego SSL/HTTP de um aplicativo MDX, que então inicia novas conexões para conexões internas em nome do usuário. Essa configuração de política permite que a estrutura MDX detecte e responda a desafios de autenticação emitidos por servidores web.

7. Conclua as Aprovações e Atribuições de Grupo de Entrega (DG) conforme necessário.

Somente os usuários nos DGs selecionados têm acesso SSO ao Citrix Files a partir dos clientes Citrix Content Collaboration for Endpoint Management. Se um usuário em um DG não tiver uma conta do Citrix Files, o Endpoint Management provisiona o usuário no Citrix Files quando você adiciona o cliente Citrix Content Collaboration for Endpoint Management ao Endpoint Management.

Para validar clientes Citrix Content Collaboration for Endpoint Management

1. Após concluir a configuração descrita neste artigo, inicie o cliente Citrix Content Collaboration for Endpoint Management. O Citrix Files não solicitará que você faça login.
2. No Secure Mail, redija um e-mail e adicione um anexo do Citrix Files. Sua página inicial do Citrix Files será aberta, sem solicitar que você faça login.

NOTA:

- O Citrix Files para XenMobile atingiu o EOL em July 1, 2023. Para mais informações, consulte [Aplicativos EOL e descontinuados](#)

Aplicativos EOL e descontinuados

Os aplicativos a seguir atingiram o Fim de Vida Útil (EOL) ou estão prestes a atingir o status EOL. Quando um lançamento de produto atinge o EOL, você pode usar o produto dentro dos termos do seu contrato de licença de produto, mas as opções de suporte disponíveis são limitadas. Informações históricas aparecem no Knowledge Center ou em outros recursos online. A documentação não é mais atualizada e é fornecida no estado em que se encontra. Para obter mais informações sobre os marcos do ciclo de vida do produto, consulte a [Matriz de Produtos](#).

NOTA:

Para aviso prévio dos recursos do Citrix Endpoint Management que estão sendo desativados, consulte [Descontinuação](#).

Citrix Files for XenMobile® (MDX): O Citrix Files for XenMobile atingiu o EOL em July 1, 2023.

Recomendamos que os clientes usem o Citrix Files disponível na Apple App Store e no Google Play. Ele está pronto para o SDK MAM.

Secure Mail for Intune SDK (iOS & Android): O Secure Mail atingiu o EOL em April 30, 2023.

Citrix Files for Intune: Descontinuado em December 31, 2020.

Nós o encorajamos a explorar as opções de alavancar os recursos da plataforma para containerizar o aplicativo Citrix Files regular (disponível nas lojas de aplicativos) via Android Enterprise (com Perfil de Trabalho) e Registro de Usuário iOS.

ShareConnect: O ShareConnect atingiu o EOL em June 30, 2020.

Secure Notes: A data de ciclo de vida EOL foi December 31, 2018.

Se você precisar dos recursos do Secure Notes e do Secure Tasks, recomendamos o Notate para Citrix, um aplicativo de terceiros que você pode proteger com políticas MDX.

Se os usuários do Secure Notes e Secure Tasks armazenaram dados no Outlook, eles podem acessar os dados no Notate. Se os usuários armazenaram dados no ShareFile, agora Citrix Files, os dados não são migrados.

Os usuários podem continuar executando o Secure Notes após a data EOL, até que o sistema operacional da plataforma pare de suportar a interface do usuário. Não recomendamos, no entanto, que você use um produto sem suporte.

Secure Tasks: A data de ciclo de vida EOL foi December 31, 2018.

Secure Forms: A data de fim de vida (EOL) foi March 31, 2018. Os clientes são incentivados a fazer a transição para os Fluxos de Trabalho do Citrix ShareFile incluídos nas contas Citrix Files Platinum e Premium. Para obter detalhes, consulte [Fluxos de Trabalho do Citrix ShareFile](#).

ScanDirect: O ScanDirect atingiu o fim de vida (EOL) em September 1, 2018.

Full VPN tunnel: A data de fim de vida (EOL) foi setembro de 2021. Para obter mais informações, consulte [Descontinuação](#) na documentação do produto Citrix Endpoint Management.

Full VPN tunnel- Android: Descontinuado em março de 2020. A data de fim de vida (EOL) foi setembro de 2021. Recomendamos que os clientes usem o modo SSO da Web do MAM SDK como alternativa.

Permitir troca de modo VPN - Android: Descontinuado em março de 2020. A data de fim de vida (EOL) foi setembro de 2021.

Troca de Documentos de Entrada - Android: Descontinuado em março de 2020. A data de fim de vida (EOL) foi setembro de 2021.

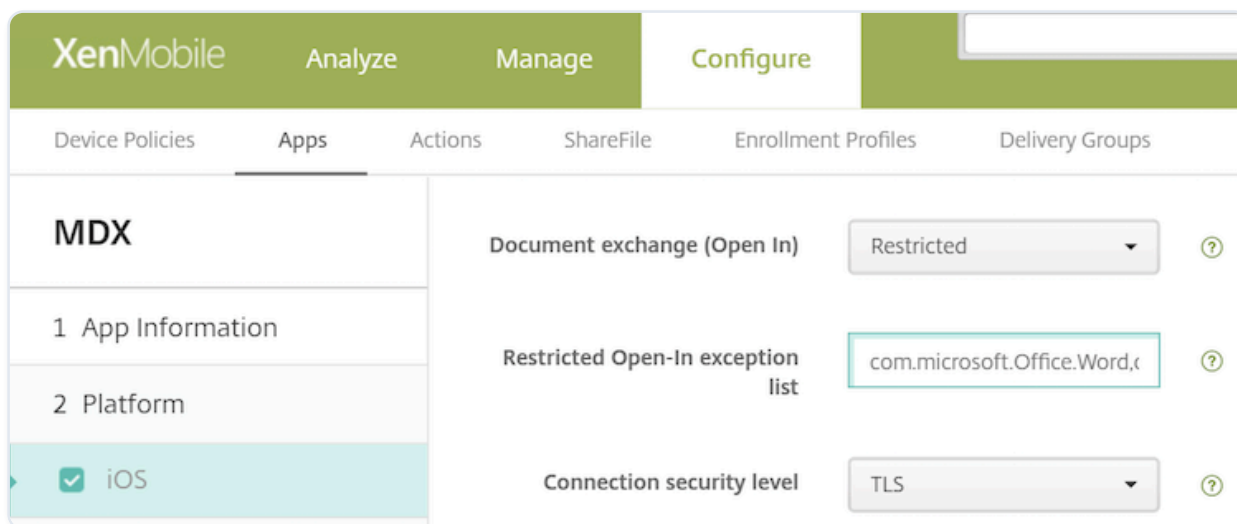
Permitindo interação segura com aplicativos do Office 365

O Citrix Secure Mail™, Citrix Secure Web e Citrix Files oferecem a opção de abrir o contêiner MDX para permitir que os usuários transfiram documentos e dados para aplicativos do Microsoft Office 365. Você gerencia essa capacidade para plataformas iOS e Android por meio das políticas de abertura no console do Endpoint Management.

Uma vez abertos em um aplicativo Microsoft, os dados não são mais protegidos ou criptografados no contêiner MDX. Considere as implicações de segurança antes de habilitar este recurso. Em particular, clientes preocupados com a prevenção de perda de dados ou que estão sujeitos a HIPAA ou outros requisitos de conformidade rigorosos devem ponderar as vantagens e desvantagens de abrir o contêiner.

Habilitando o Office 365 no iOS

1. Baixe as versões mais recentes dos aplicativos Secure Mail, Secure Web ou Citrix Files na [página de downloads do Endpoint Management](#).
2. Carregue os arquivos para o console do Endpoint Management.
3. Localize a política **Troca de documentos (Abrir em)** e defina-a como **Restrito**. Na **lista de exceções de abertura restrita**, Microsoft Word, Excel, PowerPoint, OneNote e Outlook são listados automaticamente. Por exemplo: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



Em registros MDM, mais controles estão disponíveis para dispositivos iOS.

Você pode carregar aplicativos do iTunes para o console do Endpoint Management e enviar os aplicativos para os dispositivos. Se você escolher esta opção, defina as seguintes políticas como **ATIVADO**:

- Remover aplicativo se o perfil MDM for removido
- Impedir backup de dados do aplicativo
- Forçar o gerenciamento do aplicativo (observe que uma limpeza seletiva remove o aplicativo e quaisquer dados)

Para evitar que documentos e dados fluam de aplicativos Microsoft para aplicativos não gerenciados no dispositivo, vá para **Configurar > Dispositivos > Restrições > iOS** no console do Endpoint Management e, em seguida, defina **Documentos de aplicativos gerenciados em aplicativos não gerenciados** e **Documentos de aplicativos não gerenciados em aplicativos gerenciados** como **DESATIVADO**.

Habilitando o Office 365 no Android

1. Baixe as versões mais recentes dos aplicativos Secure Mail, Secure Web ou Citrix Files na [página de downloads do Endpoint Management](#).
2. Carregue os arquivos para o console do Endpoint Management.
3. Role para baixo até a política de **Troca de documentos (Abrir em)** e selecione **Restrito**.
4. Na **Lista de exceções de Abrir em restrito**, adicione os seguintes IDs de pacote:

```
{package=com.microsoft.office.word} {package=com.microsoft.office.powerpoint}
{package=com.microsoft.office.excel}
```

5. Configure outras políticas de aplicativo como de costume e salve os aplicativos.

Os usuários devem salvar arquivos do Secure Mail, Secure Web ou Citrix Files em seus dispositivos e abri-los com um aplicativo do Office 365.

Para iOS e Android, os usuários podem abrir e editar os seguintes tipos de arquivos em seus dispositivos:

Formatos de arquivo suportados

Para os formatos de arquivo suportados, consulte a documentação do Microsoft Office.

Histórico de documentos de aplicativos móveis de produtividade

A tabela a seguir descreve mudanças importantes na documentação do produto de aplicativos móveis de produtividade. Para receber notificações sobre essas atualizações, assine o RSS feed.

DATA	ALTERAÇÃO	DESCRIÇÃO
30 May 2025	EAR do Secure Mail para iOS 25.5.0	Prévia da próxima versão
30 May 2025	EAR do Secure Web para iOS 25.5.0	Prévia da próxima versão
21 May 2025	Lançamento do Secure Hub para Android versão 25.4.0	Novidades na versão atual
02 Apr 2025	Lançamento do Secure Mail para Android versão 25.3.0	Novidades na versão atual
02 Apr 2025	Lançamento do Secure Web para Android versão 25.3.0	Novidades na versão atual
17 Feb 2025	Lançamento do Secure Mail para Android versão 25.1.0	Novidades na versão atual
17 Feb 2025	Lançamento do Secure Hub para iOS versão 25.1.0	Novidades na versão atual
12 Feb 2025	Lançamento do Secure Mail para iOS versão 25.1.0	Novidades na versão atual
10 Feb 2025	Lançamento do Secure Hub para Android versão 25.1.0	Novidades na versão atual
10 Feb 2025	Lançamento do Secure Web para iOS versão 25.1.0	Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
10 Feb 2025	Lançamento do Secure Web para Android versão 25.1.0	Novidades na versão atual
09 Dec 2024	Lançamento do Secure Mail para iOS versão 24.11.0	Novidades na versão atual
09 Dec 2024	Lançamento do Secure Hub para iOS versão 24.11.0	Novidades na versão atual
06 Dec 2024	Lançamento do Secure Web para iOS versão 24.11.0	Novidades na versão atual
05 Dec 2024	Lançamento do Secure Mail para Android versão 24.11.0	Novidades na versão atual
04 Dec 2024	EAR do Secure Mail para Android 24.11.0	Prévia da próxima versão
04 Dec 2024	EAR do Secure Mail para iOS 24.11.0	Prévia da próxima versão
26 Nov 2024	EAR do Secure Web para iOS 24.11.0	Prévia da próxima versão
26 Nov 2024	EAR do Secure Hub para iOS 24.11.0	Prévia da próxima versão
25 Nov 2024	Novo capítulo: Gerenciamento de sinalizadores de recursos	Gerenciamento de sinalizadores de recursos
05 Nov 2024	Lançamento do Secure Hub para Android versão 24.10.0	Novidades na versão atual
24 Oct 2024	EAR do Secure Hub para Android 24.10.0	Prévia da próxima versão
22 Oct 2024	Lançamento do Secure Mail para Android versão 24.9.1	Novidades na versão atual
15 Oct 2024	Lançamento do Secure Hub para iOS versão 24.9.0	Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
09 Oct 2024	Lançamento do Secure Web para Android versão 24.9.0	Novidades na versão atual
09 Oct 2024	Lançamento do Secure Mail para Android versão 24.9.0	Novidades na versão atual
09 Oct 2024	EAR do Secure Hub para iOS 24.9.0	Prévia da próxima versão
27 Sep 2024	EAR do Secure Web para Android 24.9.0	Prévia da próxima versão
27 Sep 2024	EAR do Secure Mail para Android 24.9.0	Prévia da próxima versão
20 Sep 2024	Lançamento do Secure Mail para iOS versão 24.9.0	Novidades na versão atual
16 Sep 2024	Lançamento do Secure Web para iOS versão 24.9.0	Novidades na versão atual
06 Sep 2024	Foi revisado o lançamento do Secure Hub para Android versão 24.8.0	Novidades na versão atual
04 Sep 2024	EAR do Secure Mail para iOS 24.9.0	Prévia da próxima versão
03 Sep 2024	EAR do Secure Web para iOS 24.9.0	Prévia da próxima versão
02 Sep 2024	Lançamento do Secure Hub para Android versão 24.8.0	Novidades na versão atual
28 Aug 2024	Lançamento do Secure Web para Android versão 24.8.0	Novidades na versão atual
23 Aug 2024	EAR of Secure Web para Android versão 24.8.0	Prévia da próxima versão
21 Aug 2024	EAR do Secure Hub para Android versão 24.8.0	Prévia da próxima versão

DATA	ALTERAÇÃO	DESCRIÇÃO
29 Jul 2024	Lançamento do Secure Mail para Android versão 24.7.0	Secure Mail 24.7.0: Novidades na versão atual
16 Jul 2024	EAR do Secure Mail para Android 24.7.0	Prévia da próxima versão
01 Jul 2024	Lançamento do Secure Hub para Android versão 24.6.0	Secure Hub 24.6.0: Novidades na versão atual
06 May 2024	Lançamento do Secure Hub para iOS versão 24.5.0	Secure Hub 24.5.0: Novidades na versão atual
22 Apr 2024	Foi revisado o lançamento do Secure Hub para Android versão 24.3.0 com uma nova função.	Secure Hub 24.3.0: Novidades na versão atual
22 Apr 2024	Foi revisado o lançamento do Secure Hub para Android versão 23.12.0 com novas funções.	Secure Hub 23.12.0: Novidades na versão atual
11 Apr 2024	Lançamento do Secure Hub para Android versão 24.3.0	Secure Hub 24.3.0: Correções de bugs
25 Mar 2024	Lançamento do Secure Web para iOS versão 24.3.0	Secure Web 24.3.0: Correções de bugs
25 Mar 2024	Lançamento do Secure Mail para iOS versão 24.3.0	Secure Mail 24.3.0: Correções de bugs
18 Mar 2024	Lançamento do Secure Web para Android versão 24.3.0	Secure Web 24.3.0: Correções de bugs
21 Feb 2024	Lançamento do Secure Web para iOS versão 24.2.0	Secure Web 24.2.0: Correções de bugs
21 Feb 2024	Lançamento do Secure Web para iOS versão 24.2.0	Secure Web 24.2.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
21 Feb 2024	Lançamento do Secure Mail para iOS versão 24.2.0	Secure Mail 24.2.0: Correções de bugs
21 Feb 2024	Lançamento do Secure Mail para iOS versão 24.2.0	Secure Mail 24.2.0: Novidades na versão atual
19 Feb 2024	Lançamento do Secure Web para Android versão 24.1.0	Secure Web 24.1.0: Correções de bugs
19 Feb 2024	Lançamento do Secure Mail para Android versão 24.1.0	Secure Mail 24.1.0: Correções de bugs
19 Feb 2024	Lançamento do Secure Mail para Android versão 24.1.0	Secure Mail 24.1.0: Novidades na versão atual
16 Jan 2024	Lançamento do Secure Hub para iOS versão 24.1.0	Secure Hub 24.1.0: Novidades na versão atual
16 Jan 2024	Lançamento do Secure Hub para iOS versão 24.1.0	Secure Hub 24.1.0: Correções de bugs
16 Jan 2024	Lançamento do Secure Hub para Android versão 23.12.0	Secure Hub 23.12.0: Novidades na versão atual e Correções de bugs
04 Dec 2023	Foi adicionada a documentação da tela obscura	Secure Mail: Conteúdo obscuro da tela
28 Nov 2023	Lançamento do Secure Hub para iOS versão 23.11.0	Secure Hub 23.11.0: Novidades na versão atual
28 Nov 2023	Lançamento do Secure Hub para iOS versão 23.11.0	Secure Hub 23.11.0: Correções de bugs
17 Nov 2023	Lançamento do Secure Web para Android versão 23.10.0	Secure Web 23.10.0: Novidades na versão atual
17 Nov 2023	Lançamento do Secure Mail para Android versão 23.10.0	Secure Mail 23.10.0: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
27 Oct 2023	Lançamento do Secure Mail para Android versão 23.8.2	Secure Mail 23.8.2: Novidades na versão atual
19 Oct 2023	Lançamento do Secure Hub para Android versão 23.10.0	Secure Hub 23.10.0: Novidades na versão atual
04 Oct 2023	Lançamento do Secure Mail para Android versão 23.7.0	Secure Mail 23.7.0: Novidades na versão atual
04 Oct 2023	Lançamento do Secure Mail para iOS versão 23.7.0	Secure Mail 23.7.0: Novidades na versão atual
29 Sep 2023	Lançamento do Secure Mail para Android versão 23.8.1	Secure Mail 23.8.1: Novidades na versão atual
20 Sep 2023	Lançamento do Secure Web para iOS versão 23.9.0	Secure Web 23.9.0: Novidades na versão atual
20 Sep 2023	Lançamento do Secure Mail para iOS versão 23.9.0	Secure Mail 23.9.0: Novidades na versão atual
20 Sep 2023	Lançamento do Secure Web para Android versão 23.8.0	Secure Web 23.8.0: Novidades na versão atual
20 Sep 2023	Lançamento do Secure Mail para Android versão 23.8.0	Secure Mail 23.8.0: Novidades na versão atual
01 Sep 2023	Lançamento do Secure Hub para Android versão 23.9.0	Secure Hub 23.9.0: Novidades na versão atual
25 Aug 2023	Lançamento do Secure Hub para iOS versão 23.8.1	Secure Hub 23.8.1: Novidades na versão atual
08 Aug 2023	Lançamento do Secure Hub para iOS versão 23.8.0	Secure Hub 23.8.0: Novidades na versão atual
31 Jul 2023	Lançamento do Secure Web para Android versão 23.7.0	Secure Web 23.7.0: Novidades na versão atual
31 Jul 2023	Lançamento do Secure Mail para Android versão 23.7.0	Secure Mail 23.7.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
26 Jul 2023	Lançamento do Secure Hub para Android versão 23.7.0	Secure Hub 23.7.0: Novidades na versão atual
07 Jul 2023	Lançamento do Secure Hub para iOS versão 23.4.0	Secure Hub 23.4.0: Novidades na versão atual
22 Jun 2023	Foi adicionado o problema conhecido CXM-110137	Secure Mail para Android Problemas conhecidos
07 Jun 2023	Lançamento do Secure Mail para Android versão 23.6.0	Secure Mail 23.6.0: Novidades na versão atual
31 May 2023	Lançamento do Secure Web para iOS versão 23.5.0	Secure Web 23.5.0: Novidades na versão atual
31 May 2023	Lançamento do Secure Mail para iOS versão 23.5.0	Secure Mail 23.5.0: Novidades na versão atual
26 May 2023	Lançamento do Secure Hub para Android versão 23.4.0	Secure Hub 23.4.0: Novidades na versão atual
23 May 2023	Lançamento do Secure Hub para Android versão 23.2.0	Secure Hub 23.2.0: Novidades na versão atual
12 Apr 2023	Lançamento do Secure Web para Android versão 23.3.5	Foi adicionado um problema conhecido
28 Mar 2023	Lançamento do Secure Web para Android versão 23.3.5	Secure Web 23.3.5: Novidades na versão atual
28 Mar 2023	Lançamento do Secure Mail para Android versão 23.3.5	Secure Mail 23.3.5: Novidades na versão atual
09 Jan 2023	Lançamento do Secure Hub para Android versão 22.11.0	Secure Hub 22.11.0: Novidades na versão atual
01 Feb 2023	Lançamento do Secure Web para iOS e Android versão 23.2.0	Secure Web 23.2.0: Novidades na versão atual
01 Feb 2023	Lançamento do Secure Mail para Android versão 23.2.0	Secure Mail 23.2.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
28 Oct 2022	Lançamento do Secure Mail para Android versão 22.11.0	Secure Mail 22.11.0: Novidades na versão atual
12 Oct 2022	Lançamento do Secure Hub para Android versão 22.9.0	Secure Hub 22.9.0: Novidades na versão atual
28 Sep 2022	Lançamento do Secure Mail para Android versão 22.9.0	Secure Mail 22.9.0: Novidades na versão atual
28 Sep 2022	Lançamento do Secure Web para Android versão 22.9.0	Secure Web 22.9.0: Novidades na versão atual
08 Sep 2022	Lançamento do Secure Web para iOS versão 22.9.1	Secure Web 22.9.1: Novidades na versão atual
07 Sep 2022	Lançamento do Secure Web para iOS versão 22.9.0	Secure Web 22.9.0: Novidades na versão atual
07 Sep 2022	Lançamento do Secure Mail versão 22.9.0	Secure Mail 22.9.0: Novidades na versão atual
01 Sep 2022	Lançamento do Secure Web para iOS versão 22.9.0	O Secure Web 22.9.0 foi revertido em 2 de setembro de 2022. Estamos trabalhando ativamente em uma correção e anunciaremos o lançamento em breve.
01 Sep 2022	Lançamento do Secure Mail versão 22.9.0	O Secure Mail 22.9.0 foi revertido em 2 de setembro de 2022. Estamos trabalhando ativamente em uma correção e anunciaremos o lançamento em breve.
26 Jul 2022	Lançamento do Secure Hub para Android versão 22.7.0	Secure Hub 22.7.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
13 Jul 2022	Lançamento do Secure Web para iOS versão 22.6.0	Secure Web 22.6.0: Novidades na versão atual
14 Jun 2022	Lançamento do Secure Mail versão 22.6.0	Secure Mail 22.6.0: Novidades na versão atual
14 Jun 2022	Lançamento do Secure Web para Android versão 22.6.0	Secure Web 22.6.0: Novidades na versão atual
14 Jun 2021	Lançamento do Secure Hub para Android versão 22.6.0	Secure Hub 22.6.0: Novidades na versão atual
09 Feb 2022	Lançamento do Secure Mail versão 22.2.0	Secure Mail 22.2.0: Novidades na versão atual
09 Feb 2022	Lançamento do Secure Web versão 22.2.0	Secure Web 22.2.0: Novidades na versão atual
08 Dec 2021	Lançamento do Secure Mail versão 21.12.0	Secure Mail 21.12.0: Novidades na versão atual
08 Dec 2021	Lançamento do Secure Web versão 21.12.0	Secure Web 21.12.0: Novidades na versão atual
27 Oct 2021	Lançamento do Secure Mail versão 21.10.5	Secure Mail 21.10.5: Novidades na versão atual
27 Oct 2021	Lançamento do Secure Web versão 21.10.5	Secure Web 21.10.5: Novidades na versão atual
13 Oct 2021	Lançamento do Secure Hub versão 21.10.0	Secure Hub 21.10.0: Novidades na versão atual
13 Oct 2021	Lançamento do Secure Mail versão 21.10.0	Secure Mail 21.10.0: Novidades na versão atual
13 Oct 2021	Lançamento do Secure Web versão 21.10.0	Secure Web 21.10.0: Novidades na versão atual
20 Sep 2021	Lançamento do Secure Mail versão 21.9.1	Secure Mail 21.9.1: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
20 Sep 2021	Lançamento do Secure Web versão 21.9.1	Secure Web 21.9.1: Novidades na versão atual
08 Sep 2021	Lançamento do Secure Mail versão 21.9.0	Secure Mail 21.9.0: Novidades na versão atual
08 Sep 2021	Lançamento do Secure Web versão 21.9.0	Secure Web 21.9.0: Novidades na versão atual
24 Aug 2021	Lançamento do Secure Mail para Android versão 21.8.5	Secure Mail 21.8.5: Novidades na versão atual
24 Aug 2021	Lançamento do Secure Web para Android versão 21.8.5	Secure Web 21.8.5: Novidades na versão atual
13 Aug 2021	Lançamento do Secure Hub para iOS versão 21.8.0	Secure Hub 21.8.0: Novidades na versão atual
13 Aug 2021	Lançamento do Secure Mail versão 21.8.0	Secure Mail 21.8.0: Novidades na versão atual
13 Aug 2021	Lançamento do Secure Web versão 21.8.0	Secure Web 21.8.0: Novidades na versão atual
10 Aug 2021	Lançamento do Secure Hub para Android versão 21.7.1	Secure Hub 21.7.1: Novidades na versão atual
15 Jul 2021	Lançamento do Secure Mail versão 21.7.0	Secure Mail 21.7.0: Novidades na versão atual
15 Jul 2021	Lançamento do Secure Web versão 21.7.0	Secure Web 21.7.0: Novidades na versão atual
07 Jul 2021	Lançamento do Secure Hub para iOS versão 21.7.0	Secure Hub 21.7.0: Novidades na versão atual
06 Jul 2021	Lançamento do Secure Hub para Android versão 21.7.0	Secure Hub 21.7.0: Novidades na versão atual
24 Jun 2021	Lançamento do Secure Mail para iOS versão 21.6.0	Secure Mail 21.6.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
16 Jun 2021	Lançamento do Secure Hub versão 21.6.0	Secure Hub 21.6.0: Novidades na versão atual
16 Jun 2021	Lançamento do Secure Mail para Android versão 21.6.0	Secure Mail 21.6.0: Novidades na versão atual
16 Jun 2021	Lançamento do Secure Web versão 21.6.0	Secure Web 21.6.0: Novidades na versão atual
20 May 2021	Lançamento do Secure Hub versão 21.5.1	Secure Hub 21.5.1: Novidades na versão atual
12 May 2021	Lançamento do Secure Hub versão 21.5.0	Secure Hub 21.5.0: Novidades na versão atual
12 May 2021	Lançamento do Secure Mail versão 21.5.0	Secure Mail 21.5.0: Novidades na versão atual
12 May 2021	Lançamento do Secure Web para iOS versão 21.5.0	Secure Web 21.5.0: Correções de bugs
04 May 2021	Lançamento do Secure Mail para Android versão 21.4.5	Secure Mail 21.4.5: Novidades na versão atual
04 May 2021	Lançamento do Secure Web para Android versão 21.4.5	Secure Web 21.4.5: Correções de bugs
15 Apr 2021	Lançamento do Secure Hub versão 21.4.0	Secure Hub 21.4.0: Novidades na versão atual
15 Apr 2021	Lançamento do Secure Mail para iOS versão 21.4.0	Secure Mail 21.4.0: Correções de bugs
31 Mar 2021	Lançamento do Secure Hub para iOS versão 21.3.2	Secure Hub 21.3.2: Correções de bugs
30 Mar 2021	Lançamento do Secure Mail para Android versão 21.3.5	Secure Mail 21.3.5: Novidades na versão atual
30 Mar 2021	Lançamento do Secure Web para Android versão 21.3.5	Secure Web 21.3.0: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
22 Mar 2021	Lançamento do Secure Mail para iOS versão 21.3.0	Secure Mail 21.3.0: Novidades na versão atual
17 Mar 2021	Lançamento do Secure Hub versão 21.3.0	Secure Hub 21.3.0: Correções de bugs
17 Mar 2021	Lançamento do Secure Mail para Android versão 21.3.0	Secure Mail 21.3.0: Novidades na versão atual
17 Mar 2021	Lançamento do Secure Web para Android versão 21.3.0	Secure Web 21.3.0: Correções de bugs
24 Feb 2021	Lançamento do Secure Mail versão 21.2.0	Secure Mail 21.2.0: Novidades na versão atual
24 Feb 2021	Lançamento do Secure Web versão 21.2.0	Secure Web 21.2.0: Novidades na versão atual
18 Feb 2021	Lançamento do Secure Hub para Android versão 21.2.0	Secure Hub 21.2.0: Correções de bugs
01 Feb 2021	Lançamento do Secure Mail para iOS versão 21.1.5	Secure Mail 21.1.5: Correções de bugs
01 Feb 2021	Lançamento do Secure Web para iOS versão 21.1.5	Secure Web 21.1.5: Correções de bugs
14 Jan 2021	Lançamento do Secure Mail versão 21.1.0	Secure Mail 21.1.0: Correções de bugs
14 Jan 2021	Lançamento do Secure Web versão 21.1.0	Secure Web 21.1.0: Correções de bugs
12 Jan 2021	Lançamento do Secure Hub versão 21.1.0	Secure Web 21.1.0: Correções de bugs
15 Dec 2020	Lançamento do Secure Hub versão 20.12.0	Secure Hub 20.12.0: Novidades na versão atual
15 Dec 2020	Lançamento do Secure Mail para iOS versão 20.12.0	Secure Mail 20.12.0: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
15 Dec 2020	Lançamento do Secure Web para iOS versão 20.12.0	Secure Web 20.12.0: Correções de bugs
19 Nov 2020	Lançamento do Secure Hub para Android versão 20.11.0	Secure Hub 20.11.0: Novidades na versão atual
19 Nov 2020	Lançamento do Secure Mail para Android versão 20.11.0	Secure Mail 20.11.0: Novidades na versão atual
19 Nov 2020	Lançamento do Secure Web para Android versão 20.11.0	Secure Web 20.11.0: Correções de bugs
17 Nov 2020	Lançamento do Secure Mail para iOS versão 20.11.0	Secure Mail 20.11.0: Novidades na versão atual
17 Nov 2020	Lançamento do Secure Web para iOS versão 20.11.0	Secure Web 20.11.0: Correções de bugs
27 Oct 2020	Lançamento do Secure Mail versão 20.10.5	Secure Mail 20.10.5: Novidades na versão atual
27 Oct 2020	Lançamento do Secure Web para Android versão 20.10.5	Secure Web 20.10.5: Novidades na versão atual
27 Oct 2020	Lançamento do Secure Hub para iOS versão 20.10.5	Secure Hub 20.10.5: Correções de bugs
21 Oct 2020	Lançamento do Secure Hub para Android versão 20.10.5	Secure Hub 20.10.5: Correções de bugs
15 Oct 2020	Lançamento do Secure Mail versão 20.10.0	Secure Mail 20.10.0: Novidades na versão atual
15 Oct 2020	Lançamento do Secure Web para Android versão 20.10.0	Secure Mail 20.10.0: Novidades na versão atual
29 Sep 2020	Lançamento do Secure Mail para Android versão 20.9.5	Secure Mail 20.9.5: Correções de bugs
29 Sep 2020	Lançamento do Secure Web para iOS versão 20.9.5	Secure Web 20.9.5: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
17 Sep 2020	Lançamento do Secure Mail versão 20.9.0	Secure Mail 20.9.0: Correções de bugs
17 Sep 2020	Lançamento do Secure Web para Android versão 20.9.0	Secure Web 20.9.0: Novidades na versão atual
04 Sep 2020	Lançamento do Secure Hub versão 20.9.0	Secure Hub 20.9.0: Novidades na versão atual
27 Aug 2020	Lançamento do Secure Mail versão 20.8.5	Secure Mail 20.8.5: Novidades na versão atual
27 Aug 2020	Lançamento do Secure Web versão 20.8.5	Secure Web 20.8.5: Novidades na versão atual
20 Aug 2020	Lançamento do Secure Hub versão 20.7.5	Secure Hub 20.7.5: Novidades na versão atual
19 Aug 2020	Lançamento do Secure Mail versão 20.8.0	Secure Mail 20.8.0: Novidades na versão atual
19 Aug 2020	Lançamento do Secure Web versão 20.8.0	Secure Web 20.8.0: Novidades na versão atual
12 Aug 2020	O Citrix ShareConnect atingiu o fim da vida útil (EOL).	Para obter detalhes, consulte os marcos do ciclo de vida do produto em Product Matrix .
29 Jul 2020	Lançamento do Secure Mail versão 20.7.5	Secure Mail 20.7.5: Novidades na versão atual
29 Jul 2020	Lançamento do Secure Web versão 20.7.5	Secure Web 20.7.5: Correções de bugs
14 Jul 2020	Lançamento do Secure Mail versão 20.7.0	Secure Mail 20.7.0: Correções de bugs
14 Jul 2020	Lançamento do Secure Web versão 20.7.0	Secure Web 20.7.0: Novidades na versão atual
10 Jul 2020	Ative um proxy configurado em dispositivos iOS para	Veja detalhes em Novidades no Secure Hub

DATA	ALTERAÇÃO	DESCRIÇÃO
	usar servidores proxy configurados nas configurações Wi-Fi .	
06 Jul 2020	Transição de 32 bits para 64 bits para aplicativos. Atualize os dispositivos Android para o Secure Hub versão 20.6.5 para evitar a reautenticação ao atualizar para versões posteriores.	Veja detalhes em Novidades no Secure Hub
01 Jul 2020	Lançamento do Secure Hub versão 20.6.5	Secure Hub 20.6.5: Correções de bugs
01 Jun 2020	Lançamento do Secure Mail versão 20.6.5	Secure Mail 20.6.5: Correções de bugs
19 Jun 2020	Criptografia de plataforma para QuickEdit	Veja detalhes em Criptografia para QuickEdit
16 Jun 2020	Lançamento do Secure Mail versão 20.6.0	Secure Mail 20.6.0: Correções de bugs
16 Jun 2020	Lançamento do Secure Web versão 20.6.0	Secure Web 20.6.0: Correções de bugs
02 Jun 2020	O fim da vida útil da criptografia do MDX está se aproximando rapidamente. Todos os dispositivos devem passar para a criptografia da plataforma antes de 1º de setembro de 2020	Veja detalhes em anúncios recentes
19 May 2020	Lançamento do Secure Mail para iOS versão 20.5.0	Secure Mail 20.5.0: Correções de bugs
19 May 2020	Lançamento do Secure Web para iOS versão 20.5.0	Secure Web 20.5.0: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
11 May 2020	Lançamento do Secure Mail para iOS versão 20.4.5	Secure Mail 20.4.5: Novidades na versão atual
11 May 2020	Lançamento do Secure Web para iOS versão 20.4.5	Secure Web 20.4.5: Novidades na versão atual
28 Apr 2020	Lançamento do Secure Mail para Android versão 20.4.5	Secure Mail 20.4.5: Novidades na versão atual
28 Apr 2020	Lançamento do Secure Web para Android versão 20.4.5	Secure Web 20.4.5: Correções de bugs
21 Apr 2020	Lançamento do Secure Mail para iOS versão 20.4.0	Secure Mail 20.4.0: Novidades na versão atual
21 Apr 2020	Lançamento do Secure Web para iOS versão 20.4.0	Secure Web 20.4.0: Correções de bugs
14 Apr 2020	Lançamento do Secure Mail para Android versão 20.4.0	Secure Mail 20.4.0: Novidades na versão atual
14 Apr 2020	Lançamento do Secure Web para Android versão 20.4.0	Secure Web 20.4.0: Correções de bugs
31 Mar 2020	Lançamento do Secure Hub para iOS versão 20.3.0	Secure Hub 20.3.0: Novidades na versão atual
24 Mar 2020	Lançamento do Secure Mail versão 20.3.0	Secure Mail 20.3.0: Novidades na versão atual
24 Mar 2020	Lançamento do Secure Web versão 20.3.0	Secure Web 20.3.0: Correções de bugs
11 Feb 2020	Lançamento do Secure Hub para iOS versão 20.2.0	Secure Hub 20.2.0: Correções de bugs
11 Feb 2020	Lançamento do Secure Mail versão 20.2.0	Secure Mail 20.2.0: Novidades na versão atual
29 Jan 2020	Lançamento do Secure Hub versão 20.1.5	Secure Hub 20.1.5: Correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
29 Jan 2020	Lançamento do Secure Mail versão 20.1.5	Secure Mail 20.1.5: Novidades na versão atual
07 Jan 2020	Lançamento do Secure Mail versão 20.1.0	Secure Mail 20.1.0: Novidades na versão atual
12 Dec 2019	Lançamento do Secure Hub versão 19.12.5	Secure Hub 19.12.5: Correções de bugs
12 Dec 2019	Lançamento do Secure Mail versão 19.12.5	Secure Mail 19.12.5: Novidades na versão atual
12 Dec 2019	Lançamento do Secure Web versão 19.10.5	Secure Web 19.12.5: Correções de bugs
13 Nov 2019	Lançamento do Secure Mail versão 19.11.5	Secure Mail 19.11.5: Novidades na versão atual
13 Nov 2019	Lançamento do Secure Web versão 19.11.5	Secure Web 19.11.5: Correções de bugs
06 Nov 2019	Lançamento do Secure Hub versão 19.11.5	Secure Hub 19.11.5: Correções de bugs
22 Oct 2019	Lançamento do Secure Mail para iOS versão 19.10.6	Secure Mail para iOS 19.10.6: Correções de bugs
15 Oct 2019	Lançamento do Secure Mail versão 19.10.5	Secure Mail 19.10.5: Novidades na versão atual
15 Oct 2019	Lançamento do Secure Web versão 19.10.5	Secure Web 19.10.5: Correções de bugs
14 Oct 2019	Lançamento do Secure Hub para Android versão 19.10.5	Secure Hub 19.10.5: Novidades na versão atual
03 Oct 2019	Lançamento do Secure Hub para iOS versão 19.10.0	Secure Hub 19.10.0: Correções de bugs
03 Oct 2019	Lançamento do Secure Mail para iOS versão 19.10.0	Secure Mail 19.10.0: Novidades na versão atual

DATA	ALTERAÇÃO	DESCRIÇÃO
03 Oct 2019	Lançamento do Secure Web para iOS versão 19.10.0	Secure Web 19.10.0: Novidades na versão atual
01 Oct 2019	Lançamento do Secure Mail para Android versão 19.10.0	Secure Mail 19.10.0: Novidades na versão atual
01 Oct 2019	Lançamento do Secure Web para Android versão 19.10.0	Secure Web 19.10.0: Novidades na versão atual
24 Sep 2019	Lançamento do Secure Hub para Android versão 19.10.0	Secure Hub 19.10.0: Correções de bugs
19 Sep 2019	Lançamento do Secure Mail para iOS versão 19.9.5	Secure Mail 19.9.5: Novidades na versão atual
19 Sep 2019	Lançamento do Secure Web para iOS versão 19.9.5	Secure Web 19.9.5: Correções de bugs
17 Sep 2019	Lançamento do Secure Mail para Android versão 19.9.5	Secure Mail 19.9.5: Novidades na versão atual
17 Sep 2019	Lançamento do Secure Web para Android versão 19.9.5	Secure Web 19.9.5: Novidades na versão atual
11 Sep 2019	Lançamento do Secure Hub para Android versão 19.9.5	Secure Hub 19.9.5: Novidades na versão atual
04 Sep 2019	Lançamento do Secure Mail versão 19.9.0	Secure Mail 19.9.0: Novidades na versão atual
04 Sep 2019	Lançamento do Secure Web versão 19.9.0	Secure Web 19.9.0: Novidades na versão atual
03 Sep 2019	Lançamento do Secure Hub versão 19.9.0	Secure Hub 19.9.0: Novidades na versão atual
23 Aug 2019	Lançamento do Secure Hub versão 19.8.5	Secure Hub 19.8.5: Novidades na versão atual
23 Aug 2019	Lançamento do Secure Mail para Android versão 19.8.5	Secure Mail 19.8.5: Aprimoramentos de

DATA	ALTERAÇÃO	DESCRIÇÃO
		desempenho e correções de bugs
23 Aug 2019	Lançamento do Secure Web para Android versão 19.8.5	Secure Web 19.8.5: Aprimoramentos de desempenho e correções de bugs
09 Aug 2019	Lançamento do Secure Mail para Android versão 19.8.0	Secure Mail 19.8.0: Novidades na versão atual
09 Aug 2019	Lançamento do Secure Web para Android versão 19.8.0	Secure Web 19.8.0: Aprimoramentos de desempenho e correções de bugs
31 Jul 2019	Lançamento do Secure Hub versão 19.8.0	Secure Hub 19.8.0: Novidades na versão atual
02 Aug 2019	Lançamento do Secure Mail para iOS versão 19.8.0	Secure Mail 19.8.0: Novidades na versão atual
02 Aug 2019	Lançamento do Secure Web para iOS versão 19.8.0	Secure Web 19.8.0: Aprimoramentos de desempenho e correções de bugs
18 Jul 2019	Lançamento do Secure Hub versão 19.7.5	Secure Hub 19.7.5: Novidades na versão atual
18 Jul 2019	Lançamento do Secure Mail versão 19.7.5	Secure Mail 19.7.5: Novidades na versão atual
18 Jul 2019	Lançamento do Secure Web versão 19.7.5	Secure Web 19.7.5: Aprimoramentos de desempenho e correções de bugs
30 Jun 2019	Lançamento do Secure Hub versão 19.6.6 para iOS	Secure Hub para iOS 19.6.6: Aprimoramentos de desempenho e correções de bugs

DATA	ALTERAÇÃO	DESCRIÇÃO
27 Jun 2019	Lista de novas funções do Secure Mail 19.6.5 para Android	Secure Mail 19.6.5: Novidades na versão atual
27 Jun 2019	Lançamento do Secure Web versão 19.6.5	Secure Web 19.6.5: Aprimoramentos de desempenho e correções de bugs
26 Jun 2019	Lançamento do Secure Hub versão 19.6.5	Secure Hub 19.6.5: problemas conhecidos
17 Jun 2019	Lista de novas funções do Secure Mail 19.5.5 para iOS	Secure Mail 19.5.5: Novidades na versão atual
05 Jun 2019	Lançamento do Secure Hub, Secure Mail e Secure Web versão 19.5.5 para Android	Para entender o processo de lançamento em fases do Secure Mail e do Secure Web, consulte Cronograma de lançamento de aplicativos móveis de produtividade
23 May 2019	Vídeo de um minuto sobre a função de sincronização de rascunhos do Secure Mail para Android	Foi adicionado um vídeo sobre o recurso de sincronização de pastas de rascunhos do Secure Mail para Android, lançado na versão 19.5.0: Sincronização automática de pastas de rascunhos
08 May 2019	Lançamento do Secure Hub versão 19.5.0	Secure Hub 19.5.0: problemas conhecidos e corrigidos
08 May 2019	Lançamento do Secure Mail versão 19.5.0	Secure Mail 19.5.0: problemas corrigidos
08 May 2019	Lançamento do Secure Web 19.5.0	Secure Web 19.5.0: problemas corrigidos

DATA	ALTERAÇÃO	DESCRIÇÃO
05 Apr 2019	Lançamento do Secure Hub versão 19.3.5	Secure Hub 19.3.5: problemas conhecidos e corrigidos
05 Apr 2019	Lançamento do Secure Mail versão 19.3.5	Secure Mail 19.3.5: problemas corrigidos
05 Apr 2019	Lançamento do Secure Web 19.3.5	Secure Web 19.3.5: problemas corrigidos