citrix

Secure Web

Contents

O que há de novo no Secure Web

January 19, 2021

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

O que há de novo na versão atual

Secure Web 21.1.0

Esta versão inclui correções de bugs.

O que há de novo em versões anteriores

Secure Web 20.12.0

Secure Web para iOS

Esta versão inclui correções de bugs.

Secure Web 20.11.0

Esta versão inclui correções de bugs.

Secure Web 20.10.5

Secure Web para Android

Suporte para bibliotecas AndroidX. De acordo com a recomendação do Google, o Secure Web suporta as bibliotecas do **AndroidX**, que são um substituto para as bibliotecas empacotadas do **android.support**.

Secure Web 20.10.0

Secure Web para Android

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

Secure Web 20.9.5

Secure Web para iOS

Esta versão inclui correções de bugs.

Secure Web 20.9.0

Secure Web para Android

> **Nota:**
>
> O suporte para Android 6.x terminou em 15 de setembro de 2020.

Secure Web 20.8.5

Secure Web para Android

O Secure Web para Android suporta o Android 11.

Secure Web 20.8.0

Secure Web para Android

Modo duplo para a versão Android do Secure Web. Um SDK de gerenciamento de aplicativo móvel (MAM) está disponível para substituir áreas de funcionalidade MDX que não são cobertas pelas plataformas iOS e Android. A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.

A partir da versão 20.8.0, os aplicativos Android são lançados com o MDX e o MAM SDK para se preparar para a estratégia MDX EOL mencionada anteriormente. O modo duplo MDX destina-se a fornecer uma maneira de fazer a transição para novos SDKs MAM a partir do MDX Toolkit legado. O recurso de modo duplo permite que você continue gerenciando aplicativos usando o MDX Toolkit (agora **MDX herdado**) ou alterne para o novo SDK MAM para gerenciamento de aplicativos.

Depois que você mudar para o SDK MAM para gerenciamento de aplicativos, a Citrix implementará outras alterações, o que não requer nenhuma ação dos administradores.

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

- Visão geral do SDK MAM
- Seção do Citrix Developer sobre Gerenciamento de dispositivos
- Postagem no blog Citrix
- Baixar o SDK quando você entra no Downloads Citrix

Pré-requisitos

Para uma implantação bem-sucedida do recurso de modo duplo, assegure o seguinte:

- Atualize o 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 a sua organização usa aplicativos de terceiros, certifique-se de incorporar o SDK MAM em seus aplicativos de terceiros antes de mudar para a opção SDK MAM em seus aplicativos móveis de produtividade Citrix. Todos os seus aplicativos gerenciados devem ser movidos para o SDK MAM de uma só vez.

> **Nota:**
>
> O SDK MAM é compatível com todos os clientes baseados em nuvem.

Limitações

- O SDK MAM só é compatível com 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 SDK MAM suporta apenas criptografia baseada em plataforma, não criptografia MDX.
- Se você não atualizar o Citrix Endpoint Management e os arquivos da política estiverem sendo executados na versão 20.8.0 e posterior nos aplicativos móveis, serão criadas entradas duplicadas da política de Rede no Secure Web.

Quando você configura o Secure Web no Citrix Endpoint Management, o recurso de modo duplo permite que você continue gerenciando aplicativos usando o MDX Toolkit (agora **MDX herdado**) ou alterne para o novo **SDK MAM** para gerenciamento de aplicativos. A Citrix recomenda que você alterne para o **SDK MAM**, pois os SDKs MAM são mais modulares e têm o objetivo de permitir que você use apenas um subconjunto da funcionalidade de MDX que a sua organização usa. Reduz o volume geral em binário e em tempo de execução de um aplicativo.

Você tem as seguintes opções de configurações de política no **Contêiner de política MDX ou MAM SDK**:

- **SDK MAM**
- **MDX herdado**

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

Secure Web 20.7.5

Esta versão inclui correções de bugs.

Secure Web 20.7.0

Suporte para multitarefa. No Secure Web para iOS, use dois aplicativos simultaneamente com Multitarefa. Para ativar esse recurso, arraste um aplicativo para fora do Dock. Deslize-o para a borda direita ou esquerda da tela para dividir e ativar a tela para dois aplicativos.

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

Secure Web 20.6.0

Esta versão inclui correções de bugs.

Secure Web 20.5.0

Esta versão inclui correções de bugs.

Secure Web 20.4.5

Navegue até os indicadores nas novas guias. No Secure Web para iOS, você pode exibir, editar e navegar até os indicadores ao abrir uma nova guia.

Secure Web 19.10.5 a 20.4.0

Estas versões incluem correções de bugs.

Secure Web 19.10.0

O Secure Web iOS e Android suportam o gerenciamento de criptografia. O gerenciamento de criptografia permite que você use a segurança moderna da plataforma de dispositivos, ao mesmo tempo que garante que o dispositivo permaneça em um estado adequado para usar a segurança da plataforma de forma eficaz. Usando o gerenciamento de criptografia, você elimina a redundância de criptografia de dados local, uma vez que a criptografia do sistema de arquivos é fornecida pela respectiva plataforma iOS ou Android. Para habilitar esse recurso, um administrador deve configurar a política MDX de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade** no console Citrix Endpoint Management.

O gerenciamento de criptografia permite que você use a segurança moderna da plataforma de dispositivos, ao mesmo tempo que garante que o dispositivo permaneça em um estado adequado para usar a segurança da plataforma de forma eficaz. Usando o gerenciamento de criptografia, você elimina a redundância de criptografia de dados local, uma vez que a criptografia do sistema de arquivos é fornecida pela plataforma iOS ou Android. Para habilitar esse recurso, um administrador deve configurar a política MDX de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade** no console Citrix Endpoint Management.

Tipo de criptografia

Para usar o recurso de gerenciamento de criptografia, no console Citrix Endpoint Management, defina a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**. Isso habilita o gerenciamento de criptografia e todos os dados de aplicativos criptografados existentes nos dispositivos dos usuários a fazer a transição perfeita para um estado que é criptografado pelo dispositivo e não pelo MDX. Durante essa transição, o aplicativo é pausado para uma migração de dados única. Após a migração bem-sucedida, a responsabilidade pela criptografia de dados armazenados localmente é transferida do MDX para a plataforma do dispositivo. O MDX continua a verificar a conformidade do dispositivo após cada inicialização do aplicativo. Esse recurso funciona em ambientes MDM + MAM e apenas MAM.

Quando você define a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**, a nova política substitui a sua criptografia MDX existente.

Para obter detalhes sobre as políticas MDX de gerenciamento de criptografia para Secure Web, consulte a seção **Criptografia** em:

- Políticas de MDX para aplicativos móveis de produtividade para iOS
- Políticas de MDX para aplicativos móveis de produtividade para Android

Comportamento do dispositivo não compatível

Quando um dispositivo fica abaixo dos requisitos mínimos de conformidade, a política de **Comportamento do dispositivo não compatível** permite que você selecione qual ação será executada:

- **Permitir aplicativo** — Permite que o aplicativo seja executado normalmente.
- **Permitir aplicativo após aviso** — Avisa ao usuário que um aplicativo não atende aos requisitos mínimos de conformidade e permite que o aplicativo seja executado. Este é o valor padrão.
- **Bloquear aplicativo** — Bloqueia a execução do aplicativo.

Os critérios a seguir determinam se um dispositivo atende aos requisitos mínimos de conformidade.

Dispositivos que executam o iOS:

- iOS 10: um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.

- Acesso ao depurador: um aplicativo não tem a depuração habilitada.
- Dispositivo com jailbroken: um aplicativo não está sendo executado em um dispositivo com jailbroken.
- Código secreto do dispositivo: o código secreto do dispositivo está ON.
- Compartilhamento de dados: o compartilhamento de dados não está habilitado para o aplicativo.

Dispositivos que executam o Android:

- Android SDK 24 (Android 7 Nougat): um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.
- Acesso ao depurador: um aplicativo não tem a depuração habilitada.
- Dispositivos com root: um aplicativo não está sendo executado em um dispositivo com root.
- Bloqueio do dispositivo: o código secreto do dispositivo está ON.
- Dispositivo criptografado: um aplicativo está sendo executado em um dispositivo criptografado.

Secure Web 19.9.5

Esta versão inclui correções de bugs.

Secure Web 19.9.0

Secure Web para iOS

O Secure Web para iOS suporta iOS 13.

Secure Web para Android

Esta versão inclui correções de bugs.

Secure Web para Android 19.8.5

O Secure Web para Android suporta o Android Q.

Secure Web 19.8.0

Esta versão inclui correções de bugs.

Secure Web 19.7.5

Secure Web para iOS

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Web para Android

A partir desta versão, o Secure Web para Android só é suportado em dispositivos que executam o Android 6 ou posterior.

Secure Web 19.3.0 a 19.6.5

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Web 19.2.0

Permitir que links sejam abertos no Secure Web mantendo os dados seguros. Com o Secure Web, um túnel VPN dedicado permite que os usuários acessem sites com informações confidenciais de forma segura. Esse recurso já estava disponível para o Secure Web para iOS. Esta versão adiciona suporte para Android. Para obter mais detalhes, consulte Recursos do Secure Web.

Versões do Secure Web de 18.11.5 a 19.1.5

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Web 18.11.0

No Secure Web para iOS, a lista de tamanhos de cache dos sites não é mais listada e não aparece nas configurações do aplicativo. A funcionalidade de armazenamento em cache padrão permanece a mesma.

Secure Web 18.9.0 a 18.10.5

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Web 10.8.65

Os recursos a seguir são novos no Secure Web 10.8.65:

- **Puxar para atualizar.** No Secure Web for iOS, os usuários podem usar o recurso de puxar para atualizar seus dados na tela.
- **Pesquisar usando a opção Localizar na página.** Você pode procurar por cadeias de caracteres instantaneamente usando a opção **Localizar na página**. Esta opção destaca as palavras-chave à medida que você pesquisa e exibe todas as correspondências no lado direito da barra de ferramentas. Ao reiniciar, esse recurso mantém as últimas palavras-chave pesquisadas.

- **Role para cima para ocultar as barras de cabeçalho e rodapé.** Na Secure Web for iOS, as barras de cabeçalho e rodapé ficam ocultas enquanto você rola a tela para cima. Isso permite que mais informações sejam exibidas na tela do seu celular ao visualizar páginas da web.

Secure Web 10.8.60

- Suporte para idioma polonês

Secure Web 10.8.35

- **Puxar para atualizar.** No Secure Web for Android, os usuários podem usar o recurso de puxar para atualizar seus dados na tela.

Secure Web 10.8.15

- **Secure Web oferece suporte para Android Enterprise, conhecido anteriormente como Android for Work**. Você pode criar um perfil de trabalho separado usando os aplicativos Android Enterprise no Secure Mail. Para obter detalhes, consulte Android Enterprise no Secure Mail.
- **O Secure Web para Android pode processar páginas da web no modo de área de trabalho**. No menu flutuante, selecione **Solicitar site para área de trabalho**. O Secure Web exibe a versão de área de trabalho do site.

Secure Web 10.8.10

- **O Secure Web para iOS pode processar páginas da web no modo de área de trabalho.** No menu de hambúrguer, selecione **Solicitar site de área de trabalho** para que o Secure Web exiba a versão de área de trabalho do site.

Secure Web 10.8.5

O Secure Mail e Secure Web para iOS e Android modernizaram as fontes, cores e introduziram outras melhorias de interface do usuário. Esse aprimoramento fornece uma experiência do usuário melhor, alinhando-se com a estética do Citrix marca entre nosso conjunto completo de aplicativos.

Problemas conhecidos e resolvidos

January 19, 2021

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

Secure Web 21.1.0

Não há problemas conhecidos nem resolvidos nesta versão.

Secure Web 20.12.0

Secure Web para iOS

Não há problemas conhecidos nem resolvidos nesta versão.

Secure Web 20.11.0

Não há problemas conhecidos nem resolvidos nesta versão.

Problemas conhecidos e resolvidos em versões mais antigas

Para ver os problemas conhecidos e resolvidos em versões mais antigas do Secure Web, consulte Problemas conhecidos e resolvidos em versões mais antigas.

Integração e implantação do Secure Web

January 20, 2021

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

1. Para ativar o SSO na rede interna, configure Citrix Gateway.

   Para o tráfego HTTP, o Citrix ADC pode fornecer SSO para todos os tipos de autenticação proxy com suporte pelo Citrix ADC. Para o tráfego HTTPS, a política de cache de senha da Web permite ao Secure Web autenticar e fornecer SSO para o servidor proxy por meio de MDX. O MDX dá suporte apenas a autenticação basic, digest e NTLM proxy. A senha é armazenada em cache usando MDX e armazenada no cofre compartilhado do Endpoint Management, uma área de armazenamento segura para os dados confidenciais de aplicativo. Para obter detalhes sobre a configuração do Citrix Gateway, consulte Citrix Gateway.

2. Baixar o Secure Web.

3. Determine como você deseja configurar conexões de usuário para a rede interna.

4. Adicione o Secure Web ao Endpoint Management usando as mesmas etapas que para outros aplicativos MDX e configure as políticas de MDX. Para obter detalhes sobre as políticas específicas para o Secure Web, consulte Sobre as políticas do Secure Web.

Configurando conexões de usuário

O Secure Web oferece suporte para as seguintes configurações para conexões de usuário:

- **Navegação segura:** Conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, chamada de navegação segura. Esta é a configuração padrão especificada para a política de **modo VPN preferencial**. A navegação segura é recomendada para conexões que exigem um logon único (SSO).
- **Túnel VPN completo:** Conexões que fazem túnel para a rede interna podem usar um túnel VPN, configurado pela política de modo **VPN preferencial**. Túnel VPN completo é recomendado para conexões que usam certificados de cliente ou SSL de ponta a ponta a um recurso na rede interna. O túnel VPN completo manipula qualquer protocolo por TCP e pode ser usado com computadores Windows e Mac, além de dispositivos iOS e Android.
- A política **Permitir comutação de modo VPN** permite a comutação automática entre os modos de túnel VPN completo e navegação segura, conforme necessário. Como padrão, esta política está Desativada. Quando esta política está ativada, uma solicitação de rede que falhar devido a uma solicitação de autenticação que não possa ser processada no modo VPN preferido é repetida no modo alternativo. Por exemplo, o modo de túnel VPN completo, mas não o modo de navegação segura, pode acomodar desafios do servidor para certificados de cliente. Da mesma forma, os desafios de autenticação HTTP têm maior probabilidade de serem atendidos pelo SSO ao usar o modo navegação segura.
- **Túnel VPN completo com PAC:** Você pode usar um arquivo PAC com uma implantação de túnel VPN completo para dispositivos iOS e Android. Um arquivo PAC contém regras que definem como os navegadores selecionam um proxy para acessar uma URL especificada. O arquivo de regras PAC pode especificar a manipulação tanto para sites internos quanto externos. O WorxWeb analisa o arquivo de regras PAC e envia as informações do servidor proxy para o Citrix Gateway.
- O desempenho de full VPN quando um arquivo PAC é usado é comparável ao modo navegação segura. Para obter detalhes sobre a configuração de PAC, consulte Túnel VPN completo com PAC.
- **Reverse Split Tunnel:** no modo **REVERSE**, o tráfego para aplicativos de intranet ignora o túnel VPN enquanto outro tráfego passa pelo túnel VPN. Essa política pode ser usada para criar o log de todo o tráfego de LAN não local.

Etapas de configuração de reversão do túnel dividido

Para configurar o modo Reverse de túnel dividido no Citrix Gateway:

1. Navegue até a política em **Políticas > Sessão**.
2. Selecione a política do Secure Hub e navegue até **Client Experience > Túnel dividido**.
3. Selecione **REVERSE**.

A política do MDX da Lista de exclusão de reverse split tunnel

Você configura a política de Modo Reverse de túnel dividido com o intervalo de exclusão Exclusion de dentro do Citrix Endpoint Management. O intervalo é baseado em uma lista de sufixos DNS e FQDN separados por vírgulas. Essa lista define as URLs para as quais o tráfego na rede local (LAN) do dispositivo deve ser enviado e não para o Citrix ADC.

A tabela a seguir indica se o Secure Web pede as credenciais de um usuário, com base na configuração de site e tipo:

Modo de conexão	Tipo de Site	Senha em cache	SSO configurado para o Citrix Gateway	Secure Web solicita credenciais no primeiro acesso de um site	Secure Web solicita credenciais no acesso subsequente do site	Secure Web solicita credenciais após a alteração da senha
Navegação segura	HTTP	Não	Sim	Não	Não	Não
Navegação segura	HTTPS	Não	Sim	Não	Não	Não
VPN completa	HTTP	Não	Sim	Não	Não	Não
VPN completa	HTTPS	Sim, se a política Secure Web MDX Enable web password caching está definida como On.	Não	Sim. É necessário para armazenar em cache as credenciais no Secure Web.	Não	Sim

Túnel VPN completo com PAC

> Importante:
>
> Se o Secure Web estiver configurado com um arquivo PAC e o Citrix ADC estiver configurado para operação de proxy, o Secure Web atingirá o tempo limite. Remova as políticas de tráfego do Citrix Gateway configuradas para proxy antes de usar túnel VPN completo com PAC.

Quando você configura o Secure Web para um túnel VPN completo com seu arquivo PAC ou servidor proxy, o Secure Web envia todo o tráfego para o proxy através do Citrix Gateway. O Citrix Gateway então roteia o tráfego de acordo com as regras de configuração do proxy. Nessa configuração, o Citrix Gateway não reconhece o arquivo PAC nem o servidor proxy. O fluxo de tráfego é o mesmo que túnel completo de VPN sem PAC.

O seguinte diagrama mostra o fluxo do tráfego quando os usuários do Secure Web usuários navegam para um site:

Neste exemplo, as regras de tráfego especificam que:

- O Citrix Gateway se conecta diretamente ao site de intranet `example1.net`.
- O tráfego para o site de intranet `example2.net` tem proxy por meio de servidores proxy internos.
- O tráfego externo está com proxy por meio de servidores proxy internos. As regras de proxy bloqueiam tráfego externo para `Facebook.com`.

Para configurar o túnel VPN completo com PAC

1. Valide e teste o arquivo PAC.

   > Nota:
   >
   > Para obter detalhes sobre como criar e usar arquivos PAC, acesse *findproxyforurl.com/*.

   Valide o arquivo PAC com uma ferramenta de validação de PAC como Pacparser. Quando você lê seu arquivo PAC, verifique se os resultados do Pacparser são os esperados. Se o arquivo de PAC tiver um erro de sintaxe, os dispositivos móveis vão ignorar o arquivo PAC de modo silencioso. (Um arquivo PAC é armazenado somente na memória em dispositivos móveis.)

   Um arquivo PAC é processado de cima para baixo e o processamento para quando uma regra corresponde à solicitação atual.

   Teste a URL do arquivo PAC com um navegador da Web antes de inserir no campo **PAC/Proxy** do Endpoint Management. Certifique-se de que o computador pode acessar a rede onde o arquivo PAC está localizado.

   ```
   https://webserver.local/GenericPAC.pac
   ```
   ```
   https://webserver.local/GenericPAC.pac
   ```


As extensões PAC testadas são .txt ou .pac.

O arquivo PAC deve exibir seu conteúdo dentro do navegador da Web.

> Importante:
>
> Cada vez que você atualizar o arquivo PAC usado com o Secure Web, informe os usuários de que eles devem fechar e reabrir o Secure Web.

2. Configure o Citrix Gateway:
   - Desativar o túnel dividido do Citrix Gateway. Se o túnel dividido estiver ativado e um arquivo PAC estiver configurado, as regras de arquivo PAC substituem as regras de túnel dividido do Citrix ADC. Um proxy não substitui as regras de túnel dividido do Citrix ADC.
   - Remova as políticas de tráfego do Citrix Gateway configuradas para o proxy. Esse passo é necessário para que o Secure Web funcione corretamente. A figura a seguir mostra um exemplo de regras de política para remover.
3. Defina as políticas do Secure Web:
   - Definir a política de modo Preferred VPN para **Full VPN tunnel**.
   - Definir a política Permit VPN mode switching como **Off**.
   - Configurar a URL do arquivo PAC ou a política de servidor proxy. O Secure Web dá suporte a HTTP e HTTPS, bem como a portas padrão e não padrão. No caso do HTTPS, a autoridade de certificação de raiz deve ser instalada no dispositivo se o certificado for autoassinado ou não confiável.

     Não deixe de testar a URL ou o endereço do servidor proxy em um navegador da Web antes de configurar a política.

     Exemplo de URLs de arquivo PAC:

     ```
     http[s]://example.com/proxy.pac
     http[s]://10.10.0.100/proxy.txt
     ```

     Exemplo de servidores proxy (a porta é obrigatória):

     ```
     myhost.example.com:port
     ```

     ```
     10.10.0.100:port
     ```

     > Nota:
     >
     > Se você configurar um arquivo PAC ou servidor proxy, não configure PAC nas configurações de sistema proxy para Wi-Fi.

   - Defina a política Enable web password caching como **On**. O armazenamento de senha Web lida com SSO para sites HTTPS.

O Citrix ADC pode executar SSO para proxies internos se o proxy der suporte à mesma infraestrutura de autenticação.

Limitações de suporte a arquivos PAC

O Secure Web não oferece suporte a:

- Failover de um servidor proxy para outro. A avaliação de arquivo PAC arquivo avaliação pode retornar vários servidores proxy para um nome de host. O Secure Web usa apenas o primeiro servidor proxy retornado.
- Protocolos como FTP e gopher em um arquivo PAC.
- Servidores proxy SOCKS em um arquivo PAC
- Protocolo WPAD (Web Proxy AutoDiscovery).

O Secure Web ignora o alerta de função do arquivo PAC de modo que o Secure Web pode analisar um arquivo PAC que não inclui essas chamadas.

Políticas do Secure Web

Ao adicionar o Secure Web, leve em consideração essas políticas de MDX que são específicas para o Secure Web. Para todos os dispositivos móveis com suporte:

Websites permitidos ou bloqueados

O Secure Web normalmente não filtra links da Web. Você pode usar essa política para configurar uma lista específica de sites permitidos ou bloqueados. Você pode configurar padrões de URL para restringir os sites que o navegador pode abrir, formatado como uma lista de itens separados por vírgula. Um sinal de mais (+) ou menos (-) precede cada padrão na lista. O navegador compara uma URL conforme com os padrões na ordem listada antes que uma correspondência seja encontrada. Quando uma ocorrência é encontrada, o prefixo determina a ação executada da seguinte maneira:

- Um prefixo menos instrui o navegador para bloquear o URL. Nesse caso, o URL é tratado como se o endereço do servidor não pudesse ser resolvido.
- Um prefixo de mais (+) permite que o URL seja processado normalmente.
- Se nem + ou - for fornecido com o padrão, fica presumido + (permitir).
- Se o URL não corresponder a nenhum padrão na lista, o URL é permitido

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

- O valor da política `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permite URLs de HTTP no domínio `mycorp.com`, mas os bloqueia nos demais lugares, permite URLs de HTTPS e FTP em qualquer lugar, e bloqueia todos os outros URLs.

- O valor da política `+http://*.training.lab/*,+https://*.training.lab/*,-*` permite que os usuários abram qualquer site no domínio Training.lab (intranet) via HTTP ou HTTPS. O valor da política não permite que os usuários abram URLs públicas, como Facebook, Google, Hotmail, independentemente do protocolo.

O valor padrão é vazia (todas os URLs são permitidos).

Bloquear pop-ups

Os pop-ups são novas guias que os sites abrem sem a sua permissão. Esta política determina se o Secure Web permite pop-ups. Se o valor for Ativado, o Secure Web impedirá que os sites abram pop-ups. O valor padrão é Desativado.

Indicadores pré-carregados

Define um conjunto de indicadores para o navegador Secure Web. A política é uma lista separada por vírgulas de tuplas que incluem um nome de pasta, o nome amigável e o endereço da Web. Cada tripleto deve ter o formato de pasta, nome, url em que a pasta e o nome podem ser, opcionalmente, colocados 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 marcadores. O primeiro é um link primário (sem nome de pasta) intitulado “Mycorp, Inc. home page”. O segundo link é colocado em uma pasta chamada “MyCorp Links” e intitulado “Account logon”. O terceiro é colocado na subpasta “Investor Relations” da pasta “MyCorp Links” e exibido como “Contact us”.

O valor padrão é vazio.

URL da página inicial

Define o site que o Secure Web carrega quando iniciado. O valor padrão é vazio (página inicial padrão).

Apenas para dispositivos Android e iOS com suporte:

Interface do usuário de navegador

Determina o comportamento dos controles da interface do usuário do navegador para o Secure Web. Normalmente, todos os controles de navegação estão disponíveis. Estes incluem avançar, retroceder, barra de endereços e os controles para atualizar/parar. 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 endereços de somente leitura.** Todos os controles estão visíveis, mas os usuários não podem editar o campo de endereço do navegador.
- **Ocultar barra de endereços.** Oculta a barra de endereços, mas não outros controles.
- **Ocultar todos os controles.** Suprime toda a barra de ferramentas para fornecer uma experiência de navegação sem molduras.

Ativar armazenamento em cache de senha da web

Quando os usuários do Secure Web digitam credenciais ao acessas ou solicitar um recurso da Web, esta política determina se o Secure Web armazena silenciosamente em cache a senha no dispositivo. Esta política se aplica a senhas inseridas nos diálogos de autenticação e não para senhas inseridas em formulários da Web.

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

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

Servidores proxy

Você também pode configurar servidores proxy para o WorxWeb quando usado no modo navegação segura. Para obter detalhes, consulte este postagem no blog.

Sufixos DNS

Em Android, se os sufixos DNS não estiverem configurados, a VPN poderá falhar. Para obter detalhes sobre como configurar sufixos DNS, consulte Suporte a consultas de DNS usando sufixos DNS para dispositivos Android.

Preparação de sites de intranet para o Secure Web

Esta seção é para desenvolvedores de sites que necessitam preparar um site da intranet para uso com o Secure Web para Android e iOS. Sites de Intranet feitos para navegadores de desktop requerem alterações para funcionar corretamente em dispositivos Android e iOS.

Secure Web utiliza o Android WebView e o iOS WkWebView para oferecer suporte à tecnologia da Web. Algumas das tecnologias com suporte pelo Secure Web são:

- AngularJS

- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets (somente no modo irrestrito)

Algumas das tecnologias sem suporte pelo Secure Web são:

- Flash
- Java

A tabela a seguir mostra recursos de renderização HTML e tecnologias com suporte para o Secure Web. X indica que o recurso está disponível para uma plataforma, navegador e combinação de componentes.

Tecnologia	iOS Secure Web	Android 5.x/6.x/7.x Secure Web
Mecanismo de JavaScript	JavaScriptCore	V8
Armazenamento local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

As tecnologias funcionam do mesmo modo nos diferentes dispositivos, no entanto, o Secure Web retorna cadeias de caracteres de agente diferentes para dispositivos diferentes. Para determinar a versão do navegador usada para o Secure Web, você pode ver a sua sequência de caracteres de e agente de usuário. No Secure Web, navegue até https://whatsmyuseragent.com/.

Solução de problemas de sites da Intranet

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

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

Para o Android, o navegador de terceiro compatível para teste é o Dolphin.

> Nota:
>
> Chrome é um navegador nativo no Android. Não o use para a comparação.

No OS, verifique se os navegadores têm suporte a VPN no nível de dispositivo. Você pode configurar esse suporte no dispositivo em **Ajustes > VPN > Adicionar configuração de VPN**.

Você também pode usar aplicativos de cliente VPN disponíveis na App Store, como Citrix VPN, Cisco AnyConnect ou Pulse Secure.

- Se uma página da Web é renderizada do mesmo modo nos dois navegadores, o problema é no seu site. Atualize seu site e verifique se ela funciona bem para o sistema operacional.
- Se o problema em uma página da Web aparecer somente no Secure Web, entre em contato com o suporte da Citrix para abrir um tíquete de suporte. Forneça as etapas de solução de problemas, incluindo o navegador e os tipos de sistema operacional testados. Se o Secure Web para iOS tiver problemas de exibição, inclua um arquivo da web da página como descrito nas seguintes etapas. Isso ajuda a Citrix resolver o problema de com mais rapidez.

Para criar um arquivo web

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

1. No Safari, esvazie a pasta de **Lista de leitura**: no **Finder**, clique no menu **Ir** na barra **Menu**, selecione **Ir para a pasta** e digite o nome do caminho ~/Library/Safari/ReadingListArchives/. Agora exclua todas as pastas nesse local.
2. Na barra **Menu**, vá para **Safari > Preferências > Avançado** e ative **Mostrar menu Desenvolvedor** na barra de menus.
3. Na barra **Menu**, vá para **Desenvolvedor > Agente do Usuário** e insira o agente de usuário do Secure Web: (Mozilla/5.0 (iPad; CPU OS 8_3, como macOS) AppleWebKit/600.1.4 (KHTML, como 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 lista de leitura (arquivo da Web arquivado).
5. Na barra **Menu**, vá até **Favoritos > Adicionar à lista de leitura**. Esse passo pode levar alguns minutos. O arquivamento ocorre em segundo plano.
6. Localize a lista de leitura arquivada: na barra **Menu**, vá até **Visualizar > Mostrar Barra Lateral da Lista de Leitura**.
7. Verifique o arquivo:

- Desative a conectividade de rede para o seu Mac.
- Abrir o site a partir da lista de leitura.

  O site renderiza completamente.

8. Compactar o arquivo morto: no **Finder**, clique no menu **Ir** na barra **Menu**, escolha **Ir para a pasta** e digite o nome do caminho ~/Library/Safari/ReadingListArchives/. Em seguida, compacte a pasta que tem uma cadeia de caracteres hexadecimal aleatória como um nome de arquivo. Este é o arquivo que você pode enviar para o suporte Citrix quando abrir um tíquete de suporte.

Recursos do Secure Web

O Secure Web usa tecnologias de troca de dados móveis para criar um túnel VPN para que os usuários acessem sites internos e externos e todos os outros sites. Os sites incluem 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 excelente no contêiner seguro do Endpoint Management. Veja a seguir alguns exemplos de recursos de integração:

- Quando os usuários tocam em links **Mailto**, uma nova mensagem de email é aberta no Secure Mail sem a necessidade de mais nenhuma autenticação.
- **Permitir que links sejam abertos no Secure Web mantendo os dados seguros**. Com o Secure Web para iOS e Android, um túnel VPN dedicado permite que os usuários acessem sites com informações confidenciais de forma segura. Eles podem clicar em links do Secure Mail, de dentro do Secure Web, ou de um aplicativo de terceiros. O link é aberto no Secure Web e os dados são contidos de forma segura. Os usuários podem abrir um link interno que tenha o esquema ctxmobilebrowser no Secure Web. Ao fazê-lo, o Secure Web transforma o prefixo `ctxmobilebrowser://` em `http://`. Para abrir um link HTTPS, o Secure Web transforma `ctxmobilebrowsers://` em `https://`.

Esse recurso depende de uma política MDX de interação de aplicativos chamada **Troca de documentos recebidos**. A política é definida como **Irrestrito** por padrão. Essa configuração permite que URLs sejam abertas no Secure Web. Você pode alterar a configuração da política para que somente aplicativos incluídos em uma lista de permissão possam se comunicar com o Secure Web.

- Quando os usuários clicam em um link de intranet contido em uma mensagem de email, o Secure Web vai para aquele site sem que seja necessária nenhuma 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 executar as seguintes ações:

- Bloquear pop-ups.

> Nota:
>
> Grande parte da memória do Secure Web é usada para exibir pop-ups, portanto, o desempenho muitas vezes pode ser melhorado com o bloqueio de pop-ups em Configurações.

- Marcar seus sites favoritos.
- Baixar arquivos.
- Salvar páginas offline.
- Senhas de salvamento automático.
- Excluir cache/histórico/cookies.
- Desabilitar cookies e armazenamento local de HTML5.
- Compartilhar dispositivos com outros usuários de modo seguro.
- Pesquisar na barra de endereços.
- Permitir que aplicativos da Web sejam executados com o Secure Web para acessar a respectiva localização.
- Exportação e importação de configurações.
- Abrir arquivos diretamente no Citrix Files sem a necessidade de fazer o download de arquivos. Para habilitar esse recurso, adicione **ctx-sf**: à política URLs permitidas no Endpoint Management.
- No iOS, use Ações de toque 3D para abrir uma nova guia e acessar páginas offline, sites favoritos e downloads diretamente da tela inicial.
- No iOS, baixar arquivos de qualquer tamanho e abri-los no Citrix Files ou em outros aplicativos.

  > Nota:
  >
  > Se o Secure Web for colocado em segundo plano, o download é interrompido.

- Pesquisar um termo no modo de exibição de página atual usando **Find in Page**.

O Secure Web também dá suporte a texto dinâmico, de modo que ele exibe a fonte que os usuários definem em seus dispositivos.

Proteção de dados de iOS

June 12, 2019

As empresas que devem cumprir os requisitos de proteção de dados da Australian Signals Directorate (ASD) podem usar as novas políticas de **Ativar proteção de dados de iOS** para o Secure Mail e o Secure Web. Por padrão, as políticas estão definidas como **Desativado**.

Quando **Ativar proteção de dados do iOS** estiver **Ativa** para o Secure Web, o Secure Web usa nível de proteção de Classe A para todos os arquivos na área restrita. Para obter detalhes sobre a proteção de dados do Secure Mail, consulte Proteção de dados da Australian Signals Directorate. Se você habilitar esta política, será usada a classe de proteção de dados mais alta, portanto não é necessário especificar a política **Classe de proteção de dados mínima**.

Para alterar a política **Ativar proteção de dados de iOS**:

1. Use o console Endpoint Management para carregar os arquivos MDX do Secure Web e Secure Mail para o Endpoint Management: para um novo aplicativo, navegue até **Configurar > Aplicativos > Adicionar** e clique em **MDX**. Para fazer a atualização, consulte Atualizar aplicativos MDX ou empresariais.
2. Use o console Endpoint Management para carregar os arquivos MDX para o Endpoint Management: para um novo aplicativo, navegue até **Configurar > Aplicativos > Adicionar** e clique em **MDX**. Para fazer a atualização, consulte Adicionar aplicativos.
3. Para o Secure Mail, navegue até as configurações de **Aplicativo**, localize a política **Ativar proteção de dados de iOS** e defina-a como **Ativada**. Os dispositivos que usam versões anteriores do sistema operacional não são afetados quando esta política está ativada.
4. Para o Secure Web, navegue até as configurações de **Aplicativo**, localize a política **Ativar proteção de dados de iOS** e defina-a como **Ativada**. Os dispositivos que usam versões anteriores do sistema operacional não são afetados quando esta política está ativada.
5. Configure as políticas do aplicativo como faz habitualmente e salve suas configurações para implantar o aplicativo na loja de aplicativos do Endpoint Management.

Recursos do Secure Web

June 22, 2020

O Secure Web usa tecnologias de troca de dados móveis para criar um túnel VPN para que os usuários acessem sites internos e externos e todos os outros sites. Os sites incluem 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 excelente no contêiner seguro do Endpoint Management. Veja a seguir alguns exemplos de recursos de integração:

- Quando os usuários tocam em links mailto, uma nova mensagem de email é aberta no Secure Mail sem a necessidade de mais nenhuma autenticação.
- **Permitir que links sejam abertos no Secure Web mantendo os dados seguros**. Com o Secure Web para iOS e Android, um túnel VPN dedicado permite que os usuários acessem sites com informações confidenciais de forma segura. Eles podem clicar em links do Secure Mail, de dentro do Secure Web, ou de um aplicativo de terceiros. O link é aberto no Secure Web e os dados são contidos de forma segura. Os usuários podem abrir um link interno que tenha o esquema ctxmobilebrowser(s) no Secure Web. Ao fazê-lo, o Secure Web transforma o prefixo `ctxmobilebrowser://` em `http://`. Para abrir um link HTTPS, o Secure Web transforma `ctxmobilebrowsers://` em `https://`.

Esse recurso depende de uma política MDX de interação de aplicativos chamada **Troca de documentos recebidos**. A política é definida como **Irrestrito** por padrão. Essa configuração permite que URLs sejam abertas no Secure Web. Você pode alterar a configuração da política para que somente aplicativos incluídos em uma lista de permissão possam se comunicar com o Secure Web.

- Quando os usuários clicam em um link de intranet contido em uma mensagem de email, o Secure Web vai para aquele site sem que seja necessária nenhuma 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 executar as seguintes ações:

- Bloquear pop-ups.

  > Nota:
  >
  > Grande parte da memória do Secure Web é usada para exibir pop-ups, portanto, o desempenho muitas vezes pode ser melhorado com o bloqueio de pop-ups em Configurações.

- Marcar seus sites favoritos.
- Baixar arquivos.
- Salvar páginas offline.
- Senhas de salvamento automático.
- Excluir cache/histórico/cookies.
- Desabilitar cookies e armazenamento local de HTML5.
- Compartilhar dispositivos com outros usuários de modo seguro.
- Pesquisar na barra de endereços.
- Permitir que aplicativos da Web sejam executados com o Secure Web para acessar a respectiva localização.
- Exportação e importação de configurações.

- Abrir arquivos diretamente no Citrix Files sem a necessidade de fazer o download de arquivos. Para habilitar esse recurso, adicione **ctx-sf**: à política URLs permitidas no Endpoint Management.
- No iOS, use Ações de toque 3D para abrir uma nova guia e acessar páginas offline, sites favoritos e downloads diretamente da tela inicial.
- No iOS, baixar arquivos de qualquer tamanho e abri-los no Citrix Files ou em outros aplicativos.

  > Nota:
  >
  > Se o Secure Web for colocado em segundo plano, o download é interrompido.

- Pesquisar um termo no modo de exibição de página atual usando **Find in Page**.

O Secure Web também dá suporte a texto dinâmico, de modo que ele exibe a fonte que os usuários definem em seus dispositivos.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States