citrix

Secure Web

Contents

Novedades en Secure Web

November 21, 2020

> **Nota:**
>
> A partir de junio de 2020, no se admiten las versiones de Android 6.x y iOS 11.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.

Novedades en la versión actual

Secure Web 20.11.0

Secure Web para iOS

Esta versión incluye correcciones de errores.

Novedades en versiones anteriores

Secure Hub 20.10.5

Secure Web para Android

Compatibilidad con bibliotecas AndroidX. Conforme a la recomendación de Google, Secure Web es compatible con las bibliotecas **AndroidX**, que sustituyen a las bibliotecas empaquetadas como **android.support**.

Secure Web 20.10.0

Secure Web para Android

Secure Web admite los requisitos actuales de la API de destino de Google Play para Android 10.

Secure Web 20.9.5

Secure Web para iOS

Esta versión incluye correcciones de errores.

Secure Web 20.9.0

Secure Web para Android

> **Nota:**
>
> Android 6.x dejó de admitirse el 15 de septiembre de 2020.

Secure Web 20.8.5

Secure Web para Android

Secure Web para Android es compatible con Android 11.

Secure Web 20.8.0

Secure Web para Android

Modo dual (vista previa) para la versión para Android de Secure Web. Dispone de un SDK de administración de aplicaciones móviles (MAM) para reemplazar áreas de funcionalidad MDX que no cubren las plataformas iOS y Android. La tecnología de empaquetado MDX está programada para alcanzar el final de su vida útil (EOL) en septiembre de 2021. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

A partir de la versión 20.8.0, las aplicaciones de Android se publican con MDX y el SDK de MAM en preparación para la estrategia de fin de vida de MDX mencionada anteriormente. El modo dual MDX está diseñado para ofrecer una forma de transición desde el antiguo MDX Toolkit a nuevos SDK de MAM. la funcionalidad de modo dual le permite continuar administrando aplicaciones con MDX Toolkit (ahora **MDX antiguo**) o cambiar al nuevo SDK de MAM.

Una vez que cambie al SDK de MAM para administrar las aplicaciones, Citrix implementará nuevos cambios y no se requiere intervención alguna por parte de los administradores.

Para obtener más información sobre el SDK de MAM (Vista previa), consulte los siguientes artículos:

- Introducción al SDK de MAM
- Sección de Citrix Developer sobre Administración de dispositivos
- entrada del blog de Citrix
- Descargue el SDK cuando inicie sesión en la página de descargas de Citrix

Requisitos previos

Para implementar correctamente la funcionalidad de modo dual, compruebe lo siguiente:

- Actualice Citrix Endpoint Management a las versiones 10.12 RP2 o posterior, o 10.11 RP5 o posterior.
- Actualice sus aplicaciones móviles a la versión 20.8.0 o posterior.
- Actualice el archivo de directivas a la versión 20.8.0 o posterior.

- Si su organización utiliza aplicaciones de terceros, asegúrese de incorporar el SDK de MAM en dichas aplicaciones antes de cambiar a la opción SDK de MAM para las aplicaciones móviles de productividad de Citrix. Todas las aplicaciones administradas deben transferirse al SDK de MAM al mismo tiempo.

> **Nota:**
>
> El SDK de MAM es compatible con todos los clientes basados en la nube.

Limitaciones

- El SDK de MAM solamente se admite con aplicaciones publicadas bajo la plataforma Android Enterprise en la implementación de Citrix Endpoint Management. Para las aplicaciones recién publicadas, el cifrado predeterminado es el basado en plataforma.
- El SDK de MAM solamente admite el cifrado basado en plataforma, y no el cifrado MDX.
- Si no actualiza Citrix Endpoint Management y los archivos de directiva se ejecutan en la versión 20.8.0 o posterior para las aplicaciones móviles, se crearán entradas duplicadas de la directiva de conexión en red para Secure Web.

Al configurar Secure Web en Citrix Endpoint Management, la funcionalidad de modo dual le permite continuar administrando aplicaciones con MDX Toolkit (ahora **MDX antiguo**) o cambiar al nuevo **SDK de MAM**. Citrix recomienda cambiar al **SDK de MAM**, ya que los SDK de MAM son más modulares y están pensados para permitirle usar solamente el subconjunto de la funcionalidad MDX que su organización utiliza. De este modo, se reduce la cantidad de datos binarios y el tiempo de ejecución de una aplicación.

En el **contenedor de directivas MDX o del SDK de MAM**, obtiene las siguientes opciones para la configuración de directivas:

- **SDK de MAM**
- **MDX antiguo**

En la directiva **Contenedor de directivas MDX o de SDK de MAM**, solo puede cambiar de la opción **MDX antiguo** a SDK de MAM. La posibilidad de cambiar de SDK de MAM a **MDX antiguo** no está permitida, y debe volver a publicar la aplicación. El valor predeterminado es MDX antiguo. Asegúrese de establecer el mismo modo de directiva para las aplicaciones Secure Mail y Secure Web que se ejecutan en el mismo dispositivo. No puede tener dos modos diferentes ejecutándose en un mismo dispositivo.

Secure Web 20.7.5

Esta versión incluye correcciones de errores.

Secure Web 20.7.0

Compatibilidad con multitarea. En Secure Web para iOS, use dos aplicaciones simultáneamente con Multitarea. Para habilitar esta funcionalidad, arrastre una aplicación fuera del Dock. Deslícela hacia el borde derecho o izquierdo de la pantalla para dividir y habilitar la pantalla para dos aplicaciones.

Para obtener la información más reciente sobre las aplicaciones móviles de productividad, consulte el artículo Anuncios recientes.

Secure Web 20.6.0

Esta versión incluye correcciones de errores.

Secure Web 20.5.0

Esta versión incluye correcciones de errores.

Secure Web 20.4.5

Vaya a los marcadores de las fichas nuevas. En Secure Web para iOS, puede ver, modificar y navegar por los marcadores al abrir una ficha nueva.

Secure Web 19.10.5 a 20.4.0

Estas versiones incluyen correcciones de errores.

Secure Web 19.10.0

Secure Web iOS y Android admiten la administración de cifrado. La administración de cifrado le permite utilizar la seguridad moderna de la plataforma del dispositivo para, al mismo tiempo, garantizar que dicho dispositivo permanezca en un estado suficiente para utilizar la seguridad de la plataforma de manera eficaz. Con la administración de cifrado, elimina la redundancia en el cifrado de datos locales, ya que son las plataformas Android y iOS correspondientes las que proporcionan el cifrado del sistema de archivos. Para habilitar esta función, un administrador debe configurar la directiva MDX **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos** en la consola de Citrix Endpoint Management.

La administración de cifrado le permite utilizar la seguridad moderna de la plataforma del dispositivo para, al mismo tiempo, garantizar que dicho dispositivo permanezca en un estado suficiente para utilizar la seguridad de la plataforma de manera eficaz. Con la administración de cifrado, elimina la redundancia en el cifrado de datos locales, ya que son las plataformas Android y iOS las que proporcionan el cifrado del sistema de archivos. Para habilitar esta función, un administrador debe configurar

la directiva MDX **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos** en la consola de Citrix Endpoint Management.

Tipo de cifrado

Para utilizar la función de administración de cifrado, en la consola de Citrix Endpoint Management, establezca la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**. Esto habilita la administración de cifrado, y todos los datos de las aplicaciones cifradas existentes en los dispositivos de los usuarios pasan directamente a un estado cifrado por el dispositivo y no por MDX. Durante esta transición, la aplicación se pausa para una única migración de datos. Una vez realizada correctamente la migración, la responsabilidad del cifrado de los datos almacenados localmente se transfiere de MDX a la plataforma del dispositivo. MDX continúa comprobando el cumplimiento de requisitos en el dispositivo durante cada inicio de la aplicación. Esta función opera tanto en entornos MDM + MAM como en solo MAM.

Cuando establece la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**, la nueva directiva reemplaza el cifrado MDX existente.

Para obtener información detallada acerca de las directivas MDX de administración de cifrado para Secure Web, consulte la sección **Cifrado** en:

- Directivas MDX para aplicaciones móviles de productividad para iOS
- Directivas MDX para aplicaciones móviles de productividad para Android

Comportamiento de dispositivos no conformes

Cuando un dispositivo no cumple todos los requisitos mínimos de conformidad, la directiva **Comportamiento de dispositivos no conformes** le permite seleccionar qué hacer al respecto:

- **Permitir aplicación**: Permite que la aplicación se ejecute normalmente.
- **Permitir aplicación después de la advertencia**: Advierte al usuario que una aplicación no cumple los requisitos mínimos de conformidad y permite que la aplicación se ejecute. Este es el valor predeterminado.
- **Bloquear aplicación**: Impide que la aplicación se ejecute.

Los siguientes criterios determinan si un dispositivo cumple los requisitos mínimos de conformidad.

Dispositivos con iOS:

- iOS 10: Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.
- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivo liberado por jailbreak: Una aplicación no se está ejecutando en un dispositivo liberado por jailbreak.
- Código de acceso del dispositivo: El código de acceso del dispositivo está activado.

- Uso compartido de datos: El uso compartido de datos no está habilitado para la aplicación.

Dispositivos con Android:

- Android SDK 24 (Android 7 Nougat): Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.
- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivos liberados por root: Una aplicación no se está ejecutando en un dispositivo liberado por root.
- Bloqueo de dispositivo: El código de acceso del dispositivo está activado.
- Dispositivo cifrado: Una aplicación se está ejecutando en un dispositivo cifrado.

Secure Web 19.9.5

Esta versión incluye correcciones de errores.

Secure Web 19.9.0

Secure Web para iOS

Secure Web para iOS es compatible con iOS 13.

Secure Web para Android

Esta versión incluye correcciones de errores.

Secure Web para Android 19.8.5

Secure Web para Android es compatible con Android Q.

Secure Web 19.8.0

Esta versión incluye correcciones de errores.

Secure Web 19.7.5

Secure Web para iOS

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Secure Web para Android

A partir de esta versión, Secure Web para Android solo se admite en dispositivos con Android 6 o una versión posterior.

Secure Web: De 19.3.0 a 19.6.5

En estas versiones se incluyen mejoras de rendimiento y correcciones de errores.

Secure Web 19.2.0

Permitir que los enlaces se abran en Secure Web y, al mismo tiempo, proteger los datos. Con Secure Web, un túnel VPN dedicado permite a los usuarios acceder a sitios con información confidencial de forma segura. Esta función ya estaba disponible para Secure Web para iOS. Esta versión cuenta con disponibilidad para Android. Para obtener más información detallada, consulte Funciones de Secure Web.

Secure Web: De 18.11.5 a 19.1.5

En estas versiones se incluyen mejoras de rendimiento y correcciones de errores.

Secure Web 18.11.0

En Secure Web para iOS, la lista de tamaño de caché de los sitios ya no se notifica y no aparece en la configuración de la aplicación. La funcionalidad predeterminada de almacenamiento en caché sigue siendo la misma.

Secure Web: De 18.9.0 a 18.10.5

En estas versiones se incluyen mejoras de rendimiento y correcciones de errores.

Secure Web 10.8.65

Las funciones siguientes son nuevas en Secure Web 10.8.65:

- **Tirar para actualizar**. En Secure Web para iOS, los usuarios pueden usar la función de tirar para actualizar sus datos en la pantalla.
- **Buscar con la opción Buscar en la página**. Puede buscar cadenas instantáneamente con la opción **Buscar en la página**. Esta opción resalta las palabras clave mientras busca y muestra las coincidencias totales en el lado derecho de la barra de herramientas. Tras el reinicio, esta función conserva las últimas palabras clave buscadas.
- **Desplazarse hacia arriba para ocultar las barras de encabezado y pie de página**. En Secure Web para iOS, las barras de encabezado y pie de página se ocultan a medida que el usuario se desplaza hacia arriba. Eso permite que se muestre más información en la pantalla del dispositivo móvil cuando se consultan páginas web.

Secure Web 10.8.60

- Disponible en polaco.

Secure Web 10.8.35

- **Tirar para actualizar**. En Secure Web para Android, los usuarios pueden usar la función de tirar para actualizar sus datos en la pantalla.

Secure Web 10.8.15

- **Secure Web admite Android Enterprise, anteriormente conocido como Android for Work**. Puede crear un perfil de trabajo independiente mediante aplicaciones Android Enterprise en Secure Mail. Para obtener información detallada, consulte Android Enterprise en Secure Mail.
- **Secure Web para Android puede generar páginas web en modo de escritorio**. En el menú de desbordamiento, seleccione **Solicitar sitio de escritorio**. Secure Web muestra la versión de escritorio del sitio web.

Secure Web 10.8.10

- **Secure Web para iOS puede generar páginas web en modo de escritorio.** En el menú de tres líneas, seleccione **Solicitar sitio de escritorio** y Secure Web mostrará la versión de escritorio del sitio web.

Secure Web 10.8.5

Secure Mail y Secure Web para iOS y Android cuentan con fuentes y colores mejorados, así como otras mejoras en la interfaz de usuario. Este cambio de cara ofrece una experiencia de usuario enriquecida, al mismo tiempo que se ajusta a la estética de la marca Citrix en todo nuestro conjunto de aplicaciones.

Problemas conocidos y problemas resueltos

November 21, 2020

Citrix admite actualizaciones desde las dos últimas versiones de las aplicaciones móviles de productividad.

Secure Web 20.11.0

Secure Web para iOS

No hay problemas conocidos ni resueltos en esta versión.

Secure Web 20.10.5

Secure Web para Android

No hay problemas conocidos ni resueltos en esta versión.

Secure Web 20.10.0

Secure Web para Android

No hay problemas conocidos ni resueltos en esta versión.

Problemas conocidos y problemas resueltos en versiones anteriores

Para consultar los problemas conocidos y solucionados en versiones anteriores de Secure Web, consulte Problemas conocidos y problemas resueltos en versiones anteriores.

Integrar e implementar Secure Web

July 6, 2020

Para integrar y entregar Secure Web, siga estos pasos generales:

1. Para habilitar el inicio SSO en la red interna, configure Citrix Gateway.

   Para el tráfico HTTP, Citrix ADC puede proporcionar SSO para todos los tipos de autenticación de proxy admitidos en Citrix ADC. Para el tráfico HTTPS, la directiva de caché de contraseñas web permite a Secure Web autenticar y proporcionar SSO al servidor proxy a través de MDX. MDX solo admite autenticación de proxy básica, implícita y NTLM. La contraseña se almacena en caché mediante MDX y se guarda en la caja fuerte compartida de Endpoint Management, que es una zona de almacenamiento segura para datos confidenciales de aplicación. Para obtener más información acerca de la configuración de Citrix Gateway, consulte Citrix Gateway.

2. Descargue Secure Web.
3. Determine cómo desea configurar las conexiones de usuario a la red interna.

4. Agregue Secure Web a Endpoint Management siguiendo los mismos pasos que se siguen para agregar otras aplicaciones MDX y después configure las directivas MDX. Para obtener más información acerca de las directivas específicas de Secure Web, consulte Acerca de las directivas de Secure Web.

Configurar conexiones de usuario

Secure Web admite las siguientes configuraciones para las conexiones de usuario:

- **Secure Browse:** Las conexiones por túnel a la red interna pueden utilizar una variante de VPN sin cliente conocida como "Secure Browse". Esta es la configuración predeterminada para la directiva **Modo preferido de VPN**. Se recomienda "Secure Browse" para conexiones que requieren Single Sign-On (SSO).
- **Túnel VPN completo:** Las conexiones por túnel a la red interna pueden usar un túnel VPN completo, configurado en la directiva **Modo preferido de VPN**. Se recomienda la opción "Túnel VPN completo" para conexiones que usan certificados de cliente o SSL de extremo a extremo con un recurso de la red interna. El túnel VPN completo gestiona cualquier protocolo por TCP y se puede usar con equipos con Windows y Mac, así como con dispositivos iOS y Android.
- La directiva **Permitir cambio de modo VPN** permite cambiar automáticamente entre el modo "Túnel VPN completo" y el modo "Secure Browse", según sea necesario. De manera predeterminada, esta directiva está desactivada. Si la directiva está activada, las solicitudes de red que no llegan a realizarse debido a una solicitud de autenticación que no se puede resolver en el modo preferido de VPN se vuelven a intentar en el modo alternativo. Por ejemplo, los desafíos de servidor ante certificados de cliente pueden aceptarse en el modo "Túnel VPN completo", pero no si se utiliza el modo "Secure Browse". Del mismo modo, los desafíos de autenticación HTTP son más propensos a resolverse con SSO cuando se utiliza el modo "Secure Browse".
- **Túnel VPN completo con archivo PAC:** Puede usar un archivo de configuración automática de proxy (PAC) con una implementación de túnel VPN completo para los dispositivos iOS y Android. Un archivo PAC contiene reglas que definen el modo en que los exploradores web seleccionan un proxy para acceder a una dirección URL especificada. Las reglas del archivo PAC pueden especificar cómo gestionar tanto sitios internos como sitios externos. Secure Web analiza las reglas del archivo PAC y envía la información del servidor proxy a Citrix Gateway.
- El rendimiento del túnel VPN completo cuando se usa con un archivo PAC es comparable al del modo Secure Browse. Para ver información detallada sobre la configuración de PAC, consulte Túnel VPN completo con archivo PAC.
- **Revertir túnel dividido:** En el modo **revertido**, el tráfico de las aplicaciones de intranet pasa por alto el túnel VPN, mientras que el tráfico restante pasa por el túnel VPN. Esta directiva se puede usar para registrar todo el tráfico de LAN no local.

Pasos de configuración para revertir túnel dividido

Para configurar el modo de túnel dividido revertido en Citrix Gateway, haga lo siguiente:

1. Vaya a **Policies > Session**.
2. Seleccione la directiva de Secure Hub y vaya a **Client Experience > Split Tunnel**.
3. Seleccione **Reverse**.

La directiva MDX "Lista de exclusión para revertir túnel dividido"

Puede configurar la directiva Modo de túnel dividido revertido con el intervalo "Exclusión" de Citrix Endpoint Management. El intervalo se basa en una lista, separada por comas, de sufijos DNS y FQDN. Esa lista define las URL para las cuales el tráfico debe enviarse por la red de área local (LAN) del dispositivo y no se enviará a Citrix ADC.

En la tabla siguiente, se indica si Secure Web pide credenciales al usuario en función de la configuración y del tipo de sitio:

Modo de conexión	Tipo de sitio	Caché de contraseñas	Single Sign-On configurado para Citrix Gateway	Secure Web pide credenciales en el primer acceso a un sitio web	Secure Web pide credenciales en un acceso posterior al sitio web	Secure Web pide credenciales después de un cambio de contraseña
Secure Browse	HTTP	No	Sí	No	No	No
Secure Browse	HTTPS	No	Sí	No	No	No
VPN completo	HTTP	No	Sí	No	No	No

Modo de conexión	Tipo de sitio	Caché de contraseñas	Single Sign-On configurado para Citrix Gateway	Secure Web pide credenciales en el primer acceso a un sitio web	Secure Web pide credenciales en un acceso posterior al sitio web	Secure Web pide credenciales después de un cambio de contraseña
VPN completo	HTTPS	Sí. Si la directiva MDX "Habilitar caché de contraseñas web" de Secure Web está activada.	No	Sí. Necesario para almacenar la credencial en caché de Secure Web.	No	Sí

Túnel VPN completo con archivo PAC

> Importante:
>
> Si Secure Web está configurado con un archivo PAC y Citrix ADC está configurado para funcionar con proxy, Secure Web agota el tiempo de espera. Quite las directivas de tráfico de Citrix Gateway configuradas para proxy antes de usar el túnel VPN completo con PAC.

Cuando se configura Secure Web para el túnel VPN completo con archivo PAC o servidor proxy, Secure Web envía todo el tráfico al proxy a través de Citrix Gateway. Citrix Gateway luego enruta el tráfico de acuerdo con las reglas de configuración del proxy. En esta configuración, Citrix Gateway no detecta el archivo PAC ni el servidor proxy. El flujo de tráfico es el mismo que para el túnel VPN completo sin PAC.

En el siguiente diagrama, se muestra el flujo de tráfico cuando los usuarios de Secure Web van a un sitio web:

En este ejemplo, las reglas del tráfico especifican que:

- Citrix Gateway se conecta directamente al sitio de la intranet `example1.net`.
- El tráfico al sitio de la intranet `example2.net` se redirige a través de servidores proxy internos.
- El tráfico externo se redirige a través de servidores proxy internos. Las reglas del proxy bloquean el tráfico externo a `Facebook.com`.

Para configurar el túnel VPN completo con PAC

1. Valide y haga pruebas con el archivo PAC.

   > Nota:
   >
   > Para obtener más información sobre cómo crear y usar archivos PAC, consulte https://findproxyforurl.com/.

   Valide el archivo PAC mediante una herramienta de validación de PAC como Pacparser. Al leer el archivo PAC, asegúrese de que los resultados de Pacparser son los que espera. Si el archivo PAC tiene un error de sintaxis, los dispositivos móviles ignoran el archivo de manera silenciosa, sin notificarlo. (Se almacena un archivo PAC en la memoria de los dispositivos móviles.)

   Se procesa un archivo PAC de arriba abajo y el procesamiento se detiene cuando una regla encaja en la consulta actual.

   Pruebe la dirección URL del archivo PAC en un explorador web antes de introducirla en el campo **PAC/Proxy** de Endpoint Management. Asegúrese de que el equipo puede tener acceso a la red donde se encuentra el archivo PAC.

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

   Las extensiones PAC probadas son .txt o .pac.

   El archivo PAC debe mostrar su contenido dentro del explorador web.

   > Importante:
   >
   > Cada vez que actualice el archivo PAC utilizado con Secure Web, indique a los usuarios que deben cerrar y volver a abrir Secure Web.

2. Configuración de Citrix Gateway:

   - Inhabilite el túnel dividido en Citrix Gateway. Si el túnel dividido está activado y hay un archivo PAC configurado, las reglas del archivo PAC anulan las reglas de división de túnel de Citrix ADC. Un proxy no invalida las reglas de túnel dividido de Citrix ADC.
   - Quite las directivas de tráfico de Citrix Gateway configuradas para proxy. Este paso es necesario para que Secure Web funcione correctamente. En la imagen siguiente se muestra un ejemplo de las reglas de directiva a quitar.

3. Configure las directivas de Secure Web:

   - Establezca la directiva “Modo preferido de VPN” con el valor **Túnel VPN completo**.
   - **Desactive** la directiva “Permitir cambio de modo VPN”.
   - Configure la directiva “URL del archivo PAC o servidor proxy”. Secure Web admite HTTP y HTTPS, además de puertos predeterminados y no predeterminados. Para HTTPS, la enti-

dad de certificación raíz debe estar instalada en el dispositivo si el certificado es autofirmado o no es de confianza.

Pruebe la URL o dirección del servidor proxy en un explorador web antes de configurar la directiva.

Ejemplos de URL de archivos PAC:

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

Ejemplos de servidores proxy (se necesita el puerto):

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

```
10.10.0.100:port
```

> Nota:
>
> Si configura un servidor proxy o un archivo PAC, no configure PAC en los parámetros de proxy del sistema para Wi-Fi.

- **Active** la directiva “Habilitar caché de contraseñas web”. El caché de contraseñas web gestiona el inicio de sesión SSO para sitios HTTPS.

  Citrix ADC puede realizar SSO para proxies internos si el proxy admite la misma infraestructura de autenticación.

Limitaciones de la compatibilidad con archivos PAC

Secure Web no admite:

- La conmutación por error de un servidor proxy a otro. La evaluación de un archivo PAC puede devolver varios servidores proxy para un nombre de host. Secure Web usa solamente el primer servidor proxy devuelto.
- Protocolos como FTP y gopher en un archivo PAC.
- Servidores proxy SOCKS en un archivo PAC.
- Protocolo WPAD (Web Proxy AutoDiscovery).

Secure Web ignora la función alert de los archivos PAC para poder analizar un archivo PAC que no incluya ese tipo de llamadas.

Directivas de Secure Web

Al agregar Secure Web, tenga en cuenta las directivas MDX que son específicas de Secure Web. Para todos los dispositivos móviles admitidos:

Sitios web permitidos o bloqueados

Secure Web normalmente no filtra enlaces web. Puede usar esta directiva para configurar una lista de sitios permitidos o bloqueados específicos. Puede configurar patrones de dirección URL para restringir los sitios web que el explorador puede abrir, mediante un formato de lista separada por comas. Cada patrón de la lista va precedido del signo Más (+) o del signo Menos (-). El explorador web coteja las direcciones URL con estos patrones en el orden indicado hasta que se produce una coincidencia. Cuando se encuentra una coincidencia, el prefijo determina de la siguiente forma la acción a tomar:

- Un signo Menos (-) como prefijo indica al explorador web que bloquee la URL. En este caso, la URL se trata como si la dirección del servidor web no pudiera resolverse.
- Un signo Más (+) como prefijo permite que la URL se procese normalmente.
- Si no figura ningún signo delante del patrón, se considera que va precedido del signo Más (+).
- Si una dirección URL no coincide con ningún patrón de la lista, la dirección URL se considera permitida

Para bloquear todas las demás URL, termine la lista con un signo menos seguido de un asterisco (-*). Por ejemplo:

- El valor de directiva `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permite direcciones URL con HTTP dentro del dominio `mycorp.com`, pero las bloquea en cualquier otro sitio; permite direcciones URL con HTTPS y FTP en cualquier lugar, pero bloquea todas las demás URL.
- El valor de directiva `+http://*.training.lab/*,+https://*.training.lab/*,-*` permite a los usuarios abrir cualquier sitio en el dominio Training.lab (intranet) a través de HTTP o HTTPS. El valor de directiva no permite a los usuarios abrir direcciones URL públicas, como Facebook, Google y Hotmail, independientemente del protocolo.

Está vacío de forma predeterminada (se permiten todas las URL).

Bloquear ventanas emergentes

Las ventanas emergentes son fichas nuevas que algunos sitios web abren sin su permiso. Esta directiva determina si Secure Web permite las ventanas emergentes. Cuando se activa, Secure Web impide que los sitios web abran ventanas emergentes. Esta opción está desactivada de forma predeterminada.

Marcadores precargados

Define un conjunto de marcadores precargados para el explorador Secure Web. La directiva es una lista de tuplas separadas por comas que incluyen el nombre de la carpeta, el nombre descriptivo y

la dirección web. Cada triplo debe seguir el formato carpeta, nombre, URL. El nombre y la carpeta pueden ir entre comillas dobles (“).

Por ejemplo, los valores de directiva ,”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 definen tres marcadores. El primero es un enlace primario (sin nombre de carpeta), titulado “Mycorp, Inc. home page”. El segundo enlace se colocará en una carpeta llamada “MyCorp Links” y se etiquetará “Account logon”. El tercero se colocará en una subcarpeta llamada “Investor Relations” dentro de la carpeta “MyCorp Links” y se mostrará como “Contact us”.

Está vacío de forma predeterminada.

URL de página de inicio

Define el sitio web que Secure Web carga al iniciarse. Está vacío de forma predeterminada (página de inicio predeterminada).

Solo para dispositivos Android e iOS admitidos:

Interfaz de usuario del explorador web

Establece el comportamiento y la visibilidad de los controles de la interfaz de usuario del explorador para Secure Web. Normalmente están disponibles todos los controles del explorador. Estos incluyen los controles para avanzar, retroceder, barra de dirección y actualizar/detener la carga de la página. Esta directiva se puede configurar para restringir el uso y la visibilidad de algunos de estos controles. El valor predeterminado es Todos los controles visibles.

Opciones:

- **Todos los controles visibles.** Todos los controles están visibles y no se restringe su uso para los usuarios.
- **Barra de direcciones de solo lectura.** Todos los controles están visibles, pero los usuarios no pueden modificar el campo de dirección del explorador web.
- **Ocultar barra de direcciones.** Oculta la barra de direcciones, pero no los demás controles.
- **Ocultar todos los controles.** Oculta toda la barra de herramientas para proporcionar una experiencia de exploración sin marcos.

Habilitar caché de contraseñas web

Cuando los usuarios de Secure Web introducen sus credenciales al abrir o solicitar un recurso Web, esta directiva determina si Secure Web guarda la contraseña en caché silenciosamente en el dispositivo. Esta directiva se aplica a las contraseñas introducidas en diálogos de autenticación y no a las contraseñas introducidas en formularios Web.

Si el valor es **Sí**, Secure Web guarda todas las contraseñas que los usuarios introducen cuando solicitan un recurso Web. Si tiene el valor No, Secure Web no guarda en caché las contraseñas y elimina las contraseñas que se hayan guardado previamente. Esta opción está **desactivada** de forma predeterminada.

Esta directiva solo se habilita cuando la directiva "Modo preferido de VPN" se establece en "Túnel VPN completo" para esta aplicación.

Servidores proxy

También puede configurar los servidores proxy de Secure Web cuando se usa el modo "Secure Browse". Para obtener más información, consulte este entrada del blog.

Sufijos DNS

En Android, si los sufijos DNS no están configurados, es posible que la VPN falle. Para obtener más información sobre la configuración de sufijos DNS, consulte Soporte para consultas DNS mediante sufijos DNS para dispositivos Android.

Preparar sitios de intranet para Secure Web

Esta sección está dirigida a desarrolladores de sitios web que necesitan preparar un sitio de intranet para usarlo con Secure Web para Android y para iOS. Los sitios de intranet diseñados para exploradores de escritorio requieren ciertos cambios para que funcionen correctamente en dispositivos Android e iOS.

Secure Web se basa en Android WebView e iOS WkWebView para ofrecer tecnologías web. Algunas de las tecnologías web que admite Secure Web son:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets (solo en modo no restringido)

Algunas de las tecnologías web que no admite Secure Web son:

- Flash
- Java

En la siguiente tabla, se muestran las funcionalidades y las tecnologías de generación de HTML que admite Secure Web. X indica que la función está disponible para una combinación de plataforma, explorador web y componente.

Tecnología	Secure Web en iOS	Secure Web en Android 5.x/6.x/7.x
Motor de JavaScript	JavaScriptCore	V8
Almacenamiento local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
API de requestAnimationFrame		X
API de Navigation Timing		X
API de Resource Timing		X

Las tecnologías funcionan del mismo modo en todos los dispositivos. No obstante, Secure Web devuelve distintas cadenas de agente de usuario en los distintos dispositivos. Para determinar la versión del explorador usada para Secure Web, puede ver la cadena del agente de usuario. Desde Secure Web, vaya a https://whatsmyuseragent.com/.

Solucionar problemas en sitios de intranet

Para solucionar problemas de representación cuando el sitio de intranet se ve en Secure Web, compare cómo se genera el sitio web en Secure Web y en un explorador web de terceros compatible.

Para iOS, los exploradores de terceros compatibles para realizar pruebas son Chrome y Dolphin.

Para Android, el explorador de terceros compatible para realizar pruebas es Dolphin.

> Nota:
>
> Chrome es un explorador nativo en Android. No lo utilice para la comparación.

En iOS, asegúrese de que los marcadores admiten VPN en el nivel de dispositivo. Esto se puede configurar en los parámetros del dispositivo, en **Ajustes > VPN > Agregar configuración VPN**.

También puede usar aplicaciones de cliente VPN disponibles en el App Store, como Citrix VPN, Cisco AnyConnect, o Pulse Secure.

- Si una página web aparece igual en los dos exploradores, el problema reside en el sitio web. Actualice el sitio y asegúrese de que funciona bien para el sistema operativo.
- Si el problema en la página web solo aparece cuando se abre en Secure Web, póngase en contacto con el equipo de asistencia de Citrix para abrir un tíquet de asistencia. Proporcione los pasos detallados del problema, incluida la información de qué tipos de explorador web y sistema operativo ha utilizado. Si tiene problemas al generar páginas en Secure Web para iOS, incluya un archivo web de la página según se describe en los pasos siguientes. Esto ayudará a Citrix a resolver el problema más rápidamente.

Para crear un archivo web

Con Safari en macOS 10.9 o posterior, puede guardar una página web como archivo web (denominado Lista de lectura). El archivo web incluye todos los archivos vinculados, como imágenes, CSS y JavaScript.

1. En Safari, vacíe la carpeta **Lista de lectura**. En el **Finder**, haga clic en el menú **Ir** de la barra **Menú**, elija **Ir a la carpeta**, introduzca la ruta ~/Library/Safari/ReadingListArchives/. A continuación, elimine todas las carpetas de esa ubicación.
2. En la barra **Menú**, vaya a **Safari > Preferencias > Avanzado** y habilite la opción **Mostrar el menú Desarrollo** en la barra de menú.
3. En la barra **Menú**, vaya a **Desarrollo > Agente de usuario** e introduzca el agente de usuario de 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 (compilación 1.4.0) Safari/8536.25).
4. En Safari, abra el sitio web que quiere guardar como una lista de lectura (archivo web).
5. En la barra **Menú**, vaya a **Marcadores > Agregar a la lista de lectura**. Esta operación puede tardar varios minutos. El archivado se ejecuta en el segundo plano.
6. Busque la lista de lectura archivada: en la barra **Menú**, vaya a **Visualización > Mostrar barra lateral de lista de lectura**.
7. Verifique el archivado:
   - Desactive la conectividad de red en el Mac.
   - Abra el sitio web desde la lista de lectura.

     El sitio web se genera al completo.
8. Comprima el archivo web: En el **Finder**, haga clic en el menú **Ir** en la barra **Menú**, elija **Ir a la carpeta** e introduzca la ruta ~/Library/Safari/ReadingListArchives/. Luego, comprima la carpeta que tiene como nombre una cadena hexadecimal aleatoria. Éste es el archivo que puede enviar a la asistencia técnica de Citrix cuando abra un tíquet de asistencia.

Funciones de Secure Web

Secure Web utiliza las tecnologías de intercambio de datos móviles para crear un túnel VPN dedicado para el acceso de los usuarios a sitios web internos y externos, y a todos los demás sitios web. Los sitios incluyen sitios con información confidencial en un entorno protegido por las directivas de su organización.

La integración de Secure Web con Secure Mail y Citrix Files ofrece una experiencia de usuario fluida, contenida en el entorno seguro de Endpoint Management. Éstos son algunos ejemplos de las funciones de integración:

- Cuando los usuarios tocan enlaces **mailto**, se abre un nuevo mensaje de correo electrónico en Secure Mail sin necesidad de volver a autenticarse.
- **Permitir que los enlaces se abran en Secure Web y, al mismo tiempo, proteger los datos**. Con Secure Web para iOS y Android, un túnel VPN dedicado permite a los usuarios acceder a sitios con información confidencial de forma segura. Pueden hacer clic en enlaces desde Secure Mail, desde Secure Web o desde una aplicación de terceros. El vínculo se abre en Secure Web y los datos están contenidos de forma segura. También pueden abrir un enlace interno que tenga el esquema ctxmobilebrowser en Secure Web. Al abrirlo, Secure Web transforma el prefijo `ctxmobilebrowser://` en `http://`. Para abrir un enlace HTTPS, Secure Web transforma `ctxmobilebrowsers://` en `https://`.

Esta función depende de una directiva MDX de Interacción entre aplicaciones denominada **Intercambio de documentos entrantes**. La directiva se establece en **Sin restricciones** de forma predeterminada. Esta configuración permite que las URL se abran en Secure Web. Puede cambiar la configuración de directiva para que solo las aplicaciones que incluya en una lista de permitidos puedan comunicarse con Secure Web.

- Cuando los usuarios hacen clic en un enlace de intranet dentro de un mensaje de correo electrónico, Secure Web va a ese sitio de la intranet sin necesidad de volver a autenticarse.
- Los usuarios pueden cargar archivos en Citrix Files, que pueden descargar de la Web mediante Secure Web.

Asimismo, los usuarios de Secure Web pueden realizar las siguientes acciones:

- Bloquear ventanas emergentes.

  > Nota:
  >
  > Mucha de la carga de memoria de Secure Web se dedica a la generación de ventanas emergentes, de modo que el rendimiento suele mejorar si se selecciona la opción de bloqueo de las ventanas emergentes en los Parámetros.

- Agregar sus sitios favoritos como Marcadores.
- Descargar archivos.

- Guardar páginas sin conexión.
- Guardado automático de contraseñas.
- Borrar caché, historial y cookies.
- Inhabilitar cookies y almacenamiento local de HTML5.
- Compartir dispositivos de forma segura con otros usuarios.
- Hacer búsquedas desde la barra de direcciones.
- Permitir que las aplicaciones web que los usuarios ejecutan dentro de Secure Web accedan a su ubicación.
- Exportar e importar parámetros.
- Abrir archivos directamente en Citrix Files, sin necesidad de descargarlos. Para habilitar esta función, agregue **ctx-sf**: a la directiva "Direcciones URL permitidas" en Endpoint Management.
- En iOS, puede usar acciones de 3D Touch para abrir una nueva ficha y acceder a páginas sin conexión, sitios favoritos y descargas directamente desde la pantalla inicial.
- En iOS, puede descargar archivos de cualquier tamaño y abrirlos en Citrix Files y otras aplicaciones.

  > Nota:
  >
  > Si Secure Web se pone en segundo plano, la descarga se detiene.

- Buscar un término en la vista de la página actual con la opción **Buscar en la página**.

Secure Web también admite el texto dinámico, por lo que muestra la fuente que los usuarios configuran en sus dispositivos.

Proteger datos en iOS

January 3, 2020

Las empresas que deban cumplir las normas de protección de datos del ASD (Australian Signals Directorate) pueden usar las directivas **Habilitar protección de datos de iOS** para Secure Mail y Secure Web. De forma predeterminada, esas directivas están **desactivadas**.

Si la directiva **Habilitar protección de datos de iOS** tiene el valor **Sí** para Secure Web, este aplica el nivel de protección de Clase A a todos los archivos del sandbox. Para obtener información detallada sobre la protección de datos de Secure Mail, consulte Protección de datos del Australian Signals Directorate. Si habilita esta directiva, se aplicará la clase más alta de protección de datos, de modo que no hay necesidad de especificar también la directiva **Minimum data protection class**.

Para cambiar la directiva **Habilitar protección de datos de iOS**:

1. Use la consola de Endpoint Management para cargar los archivos MDX de Secure Web y Secure Mail en Endpoint Management. Para una nueva aplicación, vaya a **Configurar > Aplicaciones > Agregar** y haga clic en **MDX**. Para realizar una actualización, consulte Actualizar aplicaciones MDX o de empresa.
2. Use la consola de Endpoint Management para cargar los archivos MDX en Endpoint Management. Para una nueva aplicación, vaya a **Configurar > Aplicaciones > Agregar** y haga clic en **MDX**. Para realizar una actualización, consulte Agregar aplicaciones.
3. Para Secure Mail, vaya a **Parámetros de aplicación**, busque la directiva **Habilitar protección de datos de iOS** y **actívela**. Los dispositivos que ejecutan versiones anteriores del sistema operativo no se verán afectados cuando se habilite esta directiva.
4. Para Secure Web, vaya a Parámetros de **aplicación**, busque la directiva **Habilitar protección de datos de iOS** y **actívela**. Los dispositivos que ejecutan versiones anteriores del sistema operativo no se verán afectados cuando se habilite esta directiva.
5. Configure las directivas de aplicación de la manera habitual y guarde los parámetros para implementar la aplicación en el almacén de aplicaciones de Endpoint Management.

Funciones de Secure Web

June 18, 2020

Secure Web utiliza las tecnologías de intercambio de datos móviles para crear un túnel VPN dedicado para el acceso de los usuarios a sitios web internos y externos, y a todos los demás sitios web. Los sitios incluyen sitios con información confidencial en un entorno protegido por las directivas de su organización.

La integración de Secure Web con Secure Mail y Citrix Files ofrece una experiencia de usuario fluida, contenida en el entorno seguro de Endpoint Management. Éstos son algunos ejemplos de las funciones de integración:

- Cuando los usuarios tocan en enlaces mailto, se abre un nuevo mensaje de correo electrónico en Secure Mail sin necesidad de volver a autenticarse.
- **Permitir que los enlaces se abran en Secure Web y, al mismo tiempo, proteger los datos**. Con Secure Web para iOS y Android, un túnel VPN dedicado permite a los usuarios acceder a sitios con información confidencial de forma segura. Pueden hacer clic en enlaces desde Secure Mail, desde Secure Web o desde una aplicación de terceros. El vínculo se abre en Secure Web y los datos están contenidos de forma segura. También pueden abrir un enlace interno que

tenga el esquema ctxmobilebrowser en Secure Web. Al abrirlo, Secure Web transforma el prefijo `ctxmobilebrowser://` en `http://`. Para abrir un enlace HTTPS, Secure Web transforma `ctxmobilebrowsers://` en `https://`.

Esta función depende de una directiva MDX de Interacción entre aplicaciones denominada **Intercambio de documentos entrantes**. La directiva se establece en **Sin restricciones** de forma predeterminada. Esta configuración permite que las URL se abran en Secure Web. Puede cambiar la configuración de directiva para que solo las aplicaciones que incluya en una lista de permitidos puedan comunicarse con Secure Web.

- Cuando los usuarios hacen clic en un enlace de intranet dentro de un mensaje de correo electrónico, Secure Web va a ese sitio de la intranet sin necesidad de volver a autenticarse.
- Los usuarios pueden cargar archivos en Citrix Files, que pueden descargar de la Web mediante Secure Web.

Asimismo, los usuarios de Secure Web pueden realizar las siguientes acciones:

- Bloquear ventanas emergentes.

  > Nota:
  >
  > Mucha de la carga de memoria de Secure Web se dedica a la generación de ventanas emergentes, de modo que el rendimiento suele mejorar si se selecciona la opción de bloqueo de las ventanas emergentes en los Parámetros.

- Agregar sus sitios favoritos como Marcadores.
- Descargar archivos.
- Guardar páginas sin conexión.
- Guardado automático de contraseñas.
- Borrar caché, historial y cookies.
- Inhabilitar cookies y almacenamiento local de HTML5.
- Compartir dispositivos de forma segura con otros usuarios.
- Hacer búsquedas desde la barra de direcciones.
- Permitir que las aplicaciones web que los usuarios ejecutan dentro de Secure Web accedan a su ubicación.
- Exportar e importar parámetros.
- Abrir archivos directamente en Citrix Files, sin necesidad de descargarlos. Para habilitar esta función, agregue **ctx-sf**: a la directiva “Direcciones URL permitidas” en Endpoint Management.
- En iOS, puede usar acciones de 3D Touch para abrir una nueva ficha y acceder a páginas sin conexión, sitios favoritos y descargas directamente desde la pantalla inicial.

- En iOS, puede descargar archivos de cualquier tamaño y abrirlos en Citrix Files y otras aplicaciones.

  > Nota:
  >
  > Si Secure Web se pone en segundo plano, la descarga se detiene.

- Buscar un término en la vista de la página actual con la opción **Buscar en la página**.

Secure Web también admite el texto dinámico, por lo que muestra la fuente que los usuarios configuran en sus 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