Citrix Receiver para Mac 12.9

Contents

Novedades en la versión 12.9.1

October 9, 2019

Se ha publicado recientemente un nuevo certificado de seguridad para mejorar aún más la seguridad de Citrix Receiver. No obstante, este certificado inhabilita la funcionalidad de actualización automática de Receiver. Esta versión incluye la herramienta de actualización automática de Receiver para restaurar la funcionalidad de actualización automática.

Novedades en la versión 12.9

2 de mayo de 2018

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general.

> **Nota**
>
> A partir de Citrix Receiver para Mac 12.9, el modo de redirección de composición del escritorio (DCR) para la comunicación remota de gráficos se ha retirado. ThinWire Plus es el método preferido para la comunicación remota de gráficos de alto rendimiento.

Soporte para Citrix Analytics

La aplicación Citrix Workspace está equipada para transmitir registros de manera segura a Citrix Analytics. Los registros se analizan y almacenan en Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte la documentación de Citrix Analytics.

Problemas resueltos

October 9, 2019

Problemas resueltos en Citrix Receiver para Mac 12.9

Comparado con: Citrix Receiver para Mac 12.8.1

Citrix Receiver para Mac 12.9 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8 y 12.8.1, además de las siguientes correcciones nuevas:

- Al minimizar la ventana de ciertas aplicaciones de fondos de escritorio de terceros, la imagen del fondo de pantalla persiste incluso después de mover la ventana. [RFMAC-1300]
- El acceso directo de teclado ALT+TAB para seleccionar ventanas podría no funcionar para las aplicaciones publicadas. [RFMAC-1390]
- La operación de arrastrar y colocar puede no funcionar cuando se trabaja en un escritorio publicado. [RFMAC-1391]

Problemas resueltos en Citrix Receiver para Mac 12.8.1

Comparado con: Citrix Receiver para Mac 12.8

Citrix Receiver para Mac 12.8.1 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3,12.4, 12.5, 12.6, 12.7 y 12.8, además de las siguientes correcciones nuevas:

- El cursor del mouse podría desaparecer al cambiar de aplicaciones publicadas a aplicaciones nativas de Mac y viceversa. [RFMAC-1178]
- Al instalar por primera vez Citrix Receiver para Mac 12.8, es posible que RealTime Media Engine no funcione correctamente. [RFMAC-1287]
- Después de actualizar a Citrix Receiver para Mac 12.8, la tecla de comilla invertida (‘) y la tecla de acento circunflejo (^) muestran un carácter Unicode extendido en lugar del carácter básico. [RFMAC-1295]
- Es posible que el portapapeles no funcione correctamente con ciertas herramientas de terceros. [RFMAC-1299]

Problemas resueltos en Citrix Receiver para Mac 12.8

Comparado con: Citrix Receiver para Mac 12.7

Citrix Receiver para Mac 12.8 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5, 12.6 y 12.7, además de las siguientes correcciones nuevas:

- El cursor de cambio de tamaño para una ventana dentro de una sesión puede no cambiar, aunque el usuario pueda cambiar el tamaño de la ventana. [RFMAC-1039]
- Citrix Viewer puede cerrarse inesperadamente cuando se usa el editor IME local de coreano para enviar caracteres a una sesión ICA. [RFMAC-1079]
- En un sistema Mac con un teclado francés canadiense, el carácter circunflejo (^) no se asigna como debería en sesiones de VDA con Windows 7. [RFMAC-1107]
- Copiar y pegar dentro de una versión publicada de Microsoft Excel hace que la sesión deje de responder durante más tiempo de lo habitual. [RFMAC-1149]

- Cuando el manifiesto de Citrix Receiver de StoreFront incluye un archivo con un espacio en el nombre, la interfaz de usuario de la Web no se carga. [RFMAC-1158]
- Al usar una estación de acoplamiento, las sesiones pueden volverse inutilizables con el tiempo. [RFMAC-1232]
- Cuando se utiliza un teclado en español, los caracteres que se crean con la marca de acento grave eliminan el carácter anterior. [RFMAC-1238]
- Al agregar una carpeta al portapapeles, Citrix Receiver para Mac puede cerrarse inesperadamente. [RFMAC-1241]

Problemas resueltos en Citrix Receiver para Mac 12.7

Comparado con: Citrix Receiver para Mac 12.6

Citrix Receiver para Mac 12.7 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3, 12.4, 12.5 y 12.6, además de las siguientes correcciones nuevas:

- El lanzamiento de un VDA mediante una tarjeta inteligente puede no funcionar cuando se usa NetScaler. Citrix Viewer deja de responder y debe reiniciarse. [RFMAC-445]
- Al iniciar sesión en XenApp Essentials y utilizar la autenticación de dos factores, es posible que el diálogo para pedir el código de seguridad no aparezca. [RFMAC-976]
- Es posible que el archivo de configuración de redirección USB no se guarde correctamente al actualizar Citrix Receiver para Mac. [RFMAC-981]
- Las aplicaciones publicadas podrían no redireccionar las URL internas. [RFMAC-982]
- Citrix Viewer puede dejar de responder. [RFMAC-1050]
- El uso de gestos de deslizamiento en un Mac que ejecuta High Sierra puede provocar defectos gráficos. [RFMAC-1073]

Problemas resueltos en Citrix Receiver para Mac 12.6

Comparado con: Citrix Receiver para Mac 12.5

Citrix Receiver para Mac 12.6 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3, 12.4 y 12.5, además de las siguientes correcciones nuevas:

- Cuando se comparten pantallas con WebEx, puede aparecer una ventana en negro en la pantalla compartida. [RFMAC-689, LC6462]
- Después de compartir pantallas con WebEx, la aplicación puede no aparecer en primer plano del escritorio. [RFMAC-690, LC6255]

- En macOS Sierra, el par de teclas Mayús-Insert puede no funcionar. [RFMAC-696]
- Después de minimizar WebEx, la aplicación puede mostrarse incorrectamente cuando se intente ver de nuevo. [RFMAC-742, LC6840]
- Cuando se inicia una aplicación con Citrix Receiver desde Google Chrome, puede que no aparezca la ventana "Iniciando aplicación…". [RFMAC-744]
- Cuando se ejecuta una máquina virtual, las sesiones de XenDesktop pueden aparecer como una pantalla en negro. [RFMAC-808]
- La ventana emergente de carga de una aplicación sigue apareciendo aun después de iniciarla. Hacer clic en "Cancelar" en la ventana emergente hace que Citrix Receiver se cierre inesperadamente. [RFMAC-832, LC7682]
- Al usar la redirección de URL de servidor a cliente, las direcciones URL que contienen un "token de acceso de un solo uso" pueden iniciarse con el token ya caducado. [RFMAC-856]
- Las aplicaciones y los escritorios no se inician cuando se usa Safari en la versión beta pública de macOS Sierra 10.12.6 o en las compilaciones macOS High Sierra Developer Preview. [RFMAC-869]

Problemas resueltos en Citrix Receiver para Mac 12.5

Comparado con: Citrix Receiver para Mac 12.4

Citrix Receiver para Mac 12.5 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2, 12.3 y 12.4, además de las siguientes correcciones nuevas:

- Si utiliza tarjetas inteligentes para iniciar sesión en un cliente de escritorio remoto, en ocasiones aparece el error "No se encontraron certificados en la tarjeta". [RFMAC-432, 650298]
- La detección de almacenes falla cuando el servidor responde con una respuesta no UTF-8. [RFMAC-565]
- Cuando se inicia una aplicación SAML, puede producirse un error de "Solicitud no válida". [RFMAC-598, LC6558]
- ReceiverHelper puede cerrarse inesperadamente. El problema ocurre cuando CEIPRegistry.json contiene un JSON no válido. [RFMAC-639]
- Falla el inicio de una aplicación publicada desde Launchpad o Finder cuando la sesión de Citrix Receiver está cerrada. Aparece el mensaje de error: "No se puede conectar. No se puede comunicar con el servicio de Authentication Manager". [RFMAC-648]

Problemas resueltos en Citrix Receiver para Mac 12.4

Comparado con: Citrix Receiver para Mac 12.3

Citrix Receiver para Mac 12.4 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100, 12.2 y 12.3, además de las siguientes correcciones nuevas:

- Citrix Viewer no envía la distribución de teclado correcta al servidor. [581829]
- Cuando se usa Citrix Receiver para Mac 12.1, al cambiar de tamaño un escritorio o cambiar de un escritorio alojado a otro, la operación puede fallar al usar Split View. [604943]
- Al usar varias pantallas en una configuración donde la pantalla principal está en la parte inferior, las ventanas de la aplicación publicada de Citrix Receiver para Mac pueden parpadear.[652254]
- Es posible que los usuarios no puedan editar o guardar un archivo en una unidad de red al usar aplicaciones publicadas. [660657]
- Al guardar un archivo en una unidad de red, la sesión de VDA puede desconectarse. [660661]
- Al usar un teclado externo en una sesión de VDA o en una aplicación publicada, la tecla Insertar no funciona. [660669]
- Aunque se intente impedir que ciertas impresoras aparezcan en una sesión, éstas siguen presentes y disponibles. [667462]

Problemas resueltos en Citrix Receiver para Mac 12.3

Comparado con: Citrix Receiver para Mac 12.2

Citrix Receiver para Mac 12.3 contiene todas las correcciones incluidas en las versiones 12, 12.1, 12.1.100 y 12.2, además de la siguiente corrección nueva:

- Si Citrix Receiver para Mac está configurado para usar un servidor proxy, las conexiones SSL (Secure Socket Layer) pueden fallar. [640652]

Problemas resueltos en Citrix Receiver para Mac 12.2

Comparado con: Citrix Receiver para Mac 12.1.100

Citrix Receiver para Mac 12.2 contiene todas las correcciones incluidas en las versiones 12, 12.1 y 12.1.100, además de las siguientes correcciones nuevas:

- Se ha solucionado un problema por el cual los teclados de alemán (Austria) no liberaban la tecla ALT después de teclear ALT-l. [LC3796]
- Se ha resuelto un problema por el cual la redirección de contenido desde el servidor al cliente fallaba si la URL que se redirigía contenía caracteres no incluidos en ASCII. [LC4470]

- Esta versión solucionó un problema por el cual la ventana de una aplicación HDX podía mostrar objetos de dibujo después de minimizar y maximizar. [LC4668]
- Se ha solucionado un problema por el cual podía fallar la autenticación PassThrough con tarjeta inteligente. [LC4907]
- Se ha solucionado un problema por el cual el audio enviado de forma remota al servidor desde un micrófono sonaba entrecortado. [LC5157]
- Se resolvió un problema por el cual la combinación de teclado CTRL-TAB no se transfería a las sesiones de escritorio activas. [LC5367]
- Se ha solucionado un problema por el cual la asignación de teclado de la sesión se hacía incorrectamente al reconectar con una sesión existente. [LC5395]
- Se ha solucionado un problema por el cual las tarjetas inteligentes no eran accesibles en un Cliente de escritorio remoto de Microsoft ejecutado dentro de una sesión HDX. [LC5454]
- Esta versión solucionó un problema por el cual las sesiones no podían conectarse si la autenticación con certificado de usuario estaba configurada en NetScaler Gateway. [LC5455]
- Se ha resuelto un problema por el cual Receiver para Mac abría una sesión en modo de pantalla completa si el parámetro ScreenPercent estaba especificado en el archivo ICA. [605353]
- Se ha resuelto un problema que hacía que Receiver para Mac dejara de responder si una sesión se desconectaba mientras se usaba una cámara Web remota en una sesión activa. [612051]
- Esta versión solucionó un problema por el cual Receiver para Mac no usaba la configuración de proxy del sistema al descargar listas de revocación de certificados. [638176]

Problemas resueltos en Citrix Receiver para Mac 12.1.100

Comparado con: Citrix Receiver para Mac 12.1

Citrix Receiver para Mac 12.1.100 contiene todas las correcciones incluidas en las versiones de la 12 y 12.1, además de las siguientes correcciones nuevas:

- Se ha resuelto un problema por el cual una sesión de Receiver para Mac fallaba al conectar a través de una VPN SSL de Cisco ASA 9.32. [LC3887]
- Se ha resuelto un problema donde una sesión se interrumpía inesperadamente al iniciar una aplicación o un escritorio cuyo nombre empezaba con el carácter '@'. [LC4296]
- Se ha resuelto un problema por el cual las sesiones se desconectaban y se veía un mensaje de error donde se indicaba que el homólogo SSL remoto envió una alerta de MAC incorrecto. [LC4367]
- Se ha resuelto un problema por el cual las conexiones IPV6 con NetScaler Gateway fallaban. [LC4512]

- Se ha resuelto un problema por el cual al intentar introducir un carácter en japonés o en chino simplificado no se mostraba ningún carácter en el escritorio de la sesión.[603635]

Problemas resueltos en Citrix Receiver para Mac 12.1

Comparado con: Citrix Receiver para Mac 12

Citrix Receiver para Mac 12.1 contiene todas las correcciones incluidas en la versión 12, además de las siguientes correcciones nuevas:

- Se ha solucionado un problema por el cual si se está utilizando la función de VPN integrada en OS X, Citrix Receiver a veces no puede conectar con una cuenta configurada mientras la VPN está activa.
- Se ha solucionado un problema en OS X El Capitan, por el cual las sesiones no se muestran con normalidad al ponerlas en el modo Split View. [582397]
- Se ha solucionado un problema por el cual la detección de balizas falla cuando se intenta conectar externamente a través de un proxy F5. [582885]
- Se ha solucionado un problema por el cual los accesos directos del teclado configurados en las Preferencias de sistema no se aplican en la sesión. [583033]
- Se ha solucionado un problema con las señales de teclado '+' en Citrix Receiver para Mac 11.9.15 y 12, que hacen que el visor deje de responder. [586179, 577922]
- Se ha solucionado un problema por el cual después de iniciar una aplicación, Citrix Receiver pide autenticación para otra aplicación. [592460]
- Se ha solucionado un problema en sesiones de escritorio, por el cual la combinación de teclas Ctrl-Q no se pasaba correctamente. [600601]

Problemas resueltos en Citrix Receiver para Mac 12

Esta versión resuelve una serie de problemas relacionados con la integración de tarjetas inteligentes. Algunos problemas no se han resuelto aún pero continúan siendo investigados.

Otros problemas resueltos en esta versión:

- En entornos de idioma japonés, aparecía un mensaje incorrecto en la ventana del diálogo de credenciales ("デモアカウントにログオンしてください", que significa "Inicie una sesión con la cuenta de demostración"). Este mensaje debería decir "Inicie una sesión en Mi escritorio virtual". [LC2682]
- Al montar varias imágenes de disco de Receiver simultáneamente es posible que se inicie el instalador incorrecto. [551605]

- Se ignoraban entradas con formato CIDR de omisión de proxy de OS X. [564250]
- Solo se usan los 256 primeros caracteres de la lista de omisión de proxy de OS X. [567089]
- La comprobación de falsos positivos de balizas internas podía fallar para ciertos ISP que tenían instalado un software de redirección de errores de DNS de Barefruit. [572456]

Problemas conocidos

October 9, 2019

Problemas conocidos en Citrix Receiver para Mac 12.9

Se han observado los siguientes problemas conocidos en esta versión:

- Cuando se ejecutan dos aplicaciones integradas, es posible que no se pueda redibujar la aplicación después de mover la ventana. [RFMAC-1308]

Problemas conocidos en Citrix Receiver para Mac 12.7

Se han observado los siguientes problemas conocidos en esta versión:

- Con la directiva "Habilitar la redirección de composición del escritorio" habilitada en una sesión de pantalla completa, Citrix Viewer pueden sufrir defectos gráficos. [RFMAC-1078]
- Citrix Viewer puede cerrarse inesperadamente cuando se usa el editor IME local de coreano para enviar caracteres a una sesión ICA. [RFMAC-1079]
- En un sistema Mac con un teclado francés canadiense, el carácter circunflejo (ˆ) no se asigna como sería de esperar cuando se conecta a un VDA con Windows 7. [RFMAC-1107]
- Los elementos de la interfaz de usuario del panel de Preferencias de dispositivo pueden aparecer cortados en algunos idiomas. [RFMAC-1113]

Problemas conocidos en Citrix Receiver para Mac 12.5

Se han observado los siguientes problemas conocidos en esta versión:

- Al usar una conexión proxy, falla la comunicación sobre Enlightened Data Transport (EDT). [664725, RFMAC-464]

- Citrix Viewer puede cerrarse inesperadamente en macOS 10.12 durante la desconexión de un escritorio desde la barra de menú. Este problema también ocurre si se selecciona el modo "Usar todas las pantallas en pantalla completa" cuando la sesión de escritorio está cerrada. [RFMAC-618]

Problemas conocidos en Citrix Receiver para Mac 12.4

Se han observado los siguientes problemas conocidos en esta versión:

- Al usar una conexión proxy, la comunicación sobre Enlightened Data Transport (EDT) falla. [664725]
- Al usar NetScaler Gateway configurado para EDT con un VDA versión 7.11 o anterior, la conexión a TCP falla porque el mecanismo de conmutación a TCP no funciona. [665617]

Problemas conocidos en Citrix Receiver para Mac 12.3

Se han observado los siguientes problemas conocidos en esta versión:

- Cuando hay un servidor proxy configurado en un dispositivo de usuario, la reconexión automática del cliente puede fallar con un VDA de SO de escritorio. [659683]
- En un entorno con IPV6, puede fallar el intento de abrir una sesión si Secure Socket Layer (SSL) está habilitado. [659700]

Problemas conocidos en Citrix Receiver para Mac 12.2

Se han observado los siguientes problemas conocidos en esta versión:

- Receiver puede colgarse si hay varias sesiones ejecutándose simultáneamente mientras se redirigen las tarjetas inteligentes. [511140]
- Es posible que los usuarios no puedan usar la función Split View de OS X con ventanas de aplicaciones HDX. [637963]
- Al redirigir una unidad USB de CD/DVD con la redirección USB genérica, la unidad puede ser expulsada. [645484]
- Algunos dispositivos USB pueden no funcionar en una sesión si la directiva de Optimización de USB está configurada para Capturar. [649082]
- En algunos casos, la pantalla de notificación de nuevo dispositivo USB puede mostrarse incorrectamente si se conecta un dispositivo USB durante el proceso de reconexión automática del cliente. [649714]

- Los usuarios pueden ver una petición de llavero cuando se conectan a una cuenta después de actualizar a Receiver para Mac 12.2. [649885]
- En sistemas que ejecutan Mac OS X 10.9, las tarjetas inteligentes pueden no ser accesibles al Cliente de escritorio remoto de Microsoft cuando se ejecuta dentro de una sesión HDX. [650298]
- Las acciones de teclado realizadas durante el proceso de reconexión de fiabilidad de la sesión pueden no reproducirse una vez que la sesión se ha reconectado. [652154]

Problemas conocidos en Citrix Receiver para Mac 12.1

Se han observado los siguientes problemas conocidos en esta versión:

- Si se cambia el tamaño de la ventana de un escritorio cuando se muestra un mensaje de inicio de sesión de Windows, la sesión puede dejar de responder. [525833]
- Puede ver un mensaje de error después de iniciar un escritorio virtual desde Chrome. [564961]
- El visor no envía la distribución de teclado correcta al servidor, lo que origina problemas de asignación de teclado. [581829]
- Cuando se mueve una sesión (mediante Smooth Roaming) a una máquina OS X 10.11 (El Capitan), la sesión no se reconecta correctamente. Use el comando de menú “Actualizar aplicaciones” para reconectar de nuevo con la sesión si falla la primera vez. [601542]

Problemas conocidos en Citrix Receiver para Mac 12

Se han observado los siguientes problemas conocidos en esta versión:

- Si una ventana del símbolo del sistema publicado está minimizada en el momento de desconectar de una sesión, el símbolo del sistema puede no reaparecer cuando se reconecta con la sesión. [411702]
- Las aplicaciones HDX pueden aparecer en negro. Si esto ocurre, arrastre las aplicaciones y ciérrelas haciendo clic en la zona donde debería verse el botón para cerrar. [426991]
- Los usuarios de equipos que ejecutan OS X Mountain Lion (10.8) pueden ver una superposición de la cadena de iniciar sesión y el icono junto a ella en la interfaz de usuario de Receiver. Si esto sucede, los usuarios pueden hacer clic en Iniciar sesión o en la cadena de nombre de usuario en lugar de usar el icono. [504302]
- En una configuración con varios monitores, las aplicaciones integradas pueden moverse a la pantalla principal cuando se reconfigura cualquiera de las pantallas. [506532]
- Al cambiar la vista a pantalla completa mientras hay una aplicación DirectX o OpenGL ejecutándose, puede ocurrir que el cursor desaparezca. [510745]

- SSL SDK puede indicar incorrectamente que una cadena de certificados ha caducado si hay varios certificados instalados y solo algunos de ellos están caducados. Para resolver el problema, elimine los certificados caducados en Acceso a Llaveros. [511574]
- Cuando el idioma del servidor es chino tradicional, es posible que los usuarios no puedan introducir "[" o "]" en la sesión. [511877]
- Al mover el cursor, el estado de Lync no cambia de Ausente a Disponible si el cambio de estado se debió a inactividad del usuario. Si esto sucede, los usuarios deben cambiar manualmente el estado a Disponible. [512074]
- Los nombres de aplicaciones vistos en Receiver pueden no reflejar actualizaciones hechas en el broker y StoreFront, si el usuario se suscribió a esas aplicaciones antes de que ocurrieran las actualizaciones. Si esto sucede, los usuarios pueden eliminar la aplicación y volver a suscribirse a ella. [515097]
- Si se cambia el tamaño de la ventana de un escritorio cuando se muestra un mensaje de inicio de sesión de Windows, la sesión puede dejar de responder. [525833]
- Cuando se usa una tarjeta inteligente Gemalto .NET para autenticarse en XenDesktop 5.6 puede fallar la apertura de sesiones. [550781]
- Cuando se usa una tarjeta inteligente PIV, Receiver no se reconecta a una sesión de XenDesktop 5.6. [550986]
- Cuando se usa OS X Mountain Lion (10.8) y Receiver 11.9 u 11.9.15 se actualiza a Receiver 12.0, al iniciar Receiver puede que se abran dos versiones de Receiver, la nueva y la antigua. [552496]
- Cuando se usa el explorador Google Chrome para OS X, al hacer doble clic en el archivo ICA en barra de descargas puede que se inicien varios archivos ICA y aparezca un mensaje de error. [564961]
- Cuando inician sesión con una cuenta PNA de Interfaz Web, es posible que los usuarios no puedan cambiar sus contraseñas caducadas. [568394]
  La parte inferior del botón de la barra de herramientas de XenDesktop puede aparecer cortada cuando un usuario entra en modo de pantalla completa durante una sesión de videollamada. [570480]
- En OS X El Capitan (10.11), los escritorios y aplicaciones virtuales no se muestran normalmente en el modo Split View. [582397]
- En OS X Yosemite (10.10), la versión actualizada de Safari puede bloquear Receiver como ventana emergente. El problema se resuelve habilitando las ventanas emergentes para que se abran los escritorios y aplicaciones.

Requisitos del sistema

October 9, 2019

Sistemas operativos compatibles

Citrix Receiver para Mac respalda los siguientes sistemas operativos:

- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Mac OS X El Capitan (10.11)

> **Nota:**
>
> Las versiones de Mac OS X anteriores a Mac OS X El Capitan no están disponibles.

Productos Citrix compatibles

Citrix Receiver para Mac es compatible con todas las versiones actualmente respaldadas de los siguientes productos Citrix. Para obtener más información acerca de la vida útil de los productos Citrix y para determinar cuándo deja Citrix de ofrecer versiones específicas de los productos, consulte la tabla de ciclos de vida de productos Citrix.

Exploradores compatibles

Citrix Receiver para Mac respalda los siguientes exploradores web:

- Safari 7.0 y versiones posteriores
- Mozilla Firefox 22.x y versiones posteriores
- Google Chrome 28.x y versiones posteriores

Requisitos de hardware

- 140.7 MB de espacio libre en el disco duro
- Una red o conexión de Internet en uso para conectarse con los servidores

Requisitos de software

- Interfaz Web:

  - Interfaz Web 5.4 para Windows con sitios de servicios XenApp, (también conocidos como servicios PNAgent), para acceder a aplicaciones desde Citrix Receiver para Mac en lugar de hacerlo desde un explorador web.
- Para implementar Citrix Receiver para Mac:
  - Citrix Receiver para Web 2.1, 2.5 y 2.6
  - Interfaz Web de Citrix 5.4
- StoreFront:
  StoreFront 2.x o una versión posterior para el acceso nativo a aplicaciones desde Citrix Receiver para Mac o desde un explorador web.

Conectividad

Citrix Receiver para Mac respalda las conexiones siguientes con XenApp o XenDesktop:

- HTTP
- HTTPS
- ICA sobre TLS

Citrix Receiver para Mac respalda las configuraciones siguientes:

Para conexiones LAN	Para conexiones locales o remotas seguras
StoreFront con servicios de StoreFront o Citrix Receiver para Mac para Web; Interfaz Web 5.4 para Windows, con sitios de Servicios XenApp	Citrix NetScaler Gateway 10.5-12.0, incluido VPX; Enterprise Edition 9.x-10.x, incluido VPX; VPX; Citrix Secure Gateway 3.x (para usar únicamente con la Interfaz Web)

Para obtener más información sobre la implementación de NetScaler Gateway con StoreFront, consulte la documentación de NetScaler Gateway y la documentación de StoreFront.

Autenticación

Para conexiones con StoreFront, Citrix Receiver para Mac respalda los siguientes métodos de autenticación:

	Receiver para Web mediante exploradores web	Sitio de servicios StoreFront (nativo)	Sitio de servicios XenApp de StoreFront (nativo)	NetScaler a Receiver para Web (explorador)	NetScaler a sitio de servicios StoreFront (nativo)
Anónimo	Sí	Sí			
Dominio	Sí	Sí		Sí*	Sí*
PassThrough de dominio					
Token de seguridad				Sí*	Sí*
Dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	Sí*
Tarjeta inteligente	Sí	Sí		Sí*	Sí
Certificado de usuario				Sí	Sí (NetScaler Gateway Plugin)

* Disponible solo para sitios de Receiver para Web y para implementaciones que incluyen NetScaler Gateway, con o sin el plug-in asociado en el dispositivo.

Para conexiones con la Interfaz Web 5.4, Citrix Receiver para Mac respalda los siguientes métodos de autenticación:

> **Nota:**
>
> La Interfaz Web usa el término
> Explícita para la autenticación con dominio y token de seguridad.

	Interfaz Web (exploradores web)	Sitio de servicios XenApp de Interfaz Web	NetScaler a Interfaz Web (explorador web)	NetScaler a sitio de servicios XenApp de Interfaz Web
Anónimo	Sí			

	Interfaz Web (exploradores web)	Sitio de servicios XenApp de Interfaz Web	NetScaler a Interfaz Web (explorador web)	NetScaler a sitio de servicios XenApp de Interfaz Web
Dominio	Sí	Sí	Sí	Sí
PassThrough de dominio				
Token de seguridad			Sí*	Sí
Dos factores (dominio con token de seguridad)			Sí*	Sí
SMS			Sí*	Sí
Tarjeta inteligente	Sí		Sí	
Certificado de usuario			Sí (requiere el NetScaler Gateway Plugin)	Sí (requiere el NetScaler Gateway Plugin)

* Disponible solo en implementaciones que incluyen NetScaler Gateway, con o sin el plug-in asociado en el dispositivo.

Instalación y configuración

October 9, 2019

Instalación

Esta versión de Citrix Receiver para Mac contiene un solo paquete de instalación, CitrixReceiver.dmg, y respalda el acceso remoto a través de NetScaler Gateway y Secure Gateway.

Un usuario puede instalar Citrix Receiver para Mac desde el sitio web de Citrix, ya sea automáticamente a partir de Receiver para Web o de la Interfaz Web, o bien con la ayuda de una herramienta de distribución electrónica de software (ESD).

Desde Citrix.com (instalación de usuario)

- Un usuario que utiliza Citrix Receiver para Mac por primera vez y obtiene Citrix Receiver para Mac desde Citrix.com o desde un sitio de descarga puede configurar una cuenta mediante la introducción de una dirección de correo electrónico en lugar de una dirección URL de servidor. Citrix Receiver para Mac determina el servidor NetScaler Gateway o StoreFront asociado con esa dirección de correo electrónico y pide al usuario que inicie una sesión para continuar con la instalación. Esta función se conoce como detección de cuentas basada en correo electrónico.

> **Nota:**
>
> Un usuario nuevo es un usuario que no tiene Citrix Receiver para Mac instalado en su dispositivo.

- La detección de cuentas basada en correo electrónico para un usuario nuevo no se aplica cuando Citrix Receiver para Mac se descarga desde una ubicación distinta a Citrix.com (como, por ejemplo, un sitio de Receiver para Web).
- Si el sitio requiere la configuración de Receiver, utilice un método de implementación alternativo.

Automáticamente desde Receiver para Web o desde la Interfaz Web

- Un usuario que utiliza Citrix Receiver para Mac por primera vez puede configurar una cuenta introduciendo la dirección URL de un servidor, o descargando un archivo de aprovisionamiento.

Mediante una herramienta de distribución electrónica de software (ESD)

- Un usuario que utiliza Citrix Receiver para Mac por primera vez debe introducir una dirección URL de servidor para configurar una cuenta.

Instalación manual de Citrix Receiver para Mac

Los usuarios pueden instalar Citrix Receiver para Mac desde la Interfaz Web, desde un recurso compartido de red. o directamente en el dispositivo de usuario mediante la descarga de un archivo CitrixReceiver.dmg desde el sitio web de Citrix, en http://www.citrix.com.

Para instalar Citrix Receiver para Mac:

1. Descargue el archivo .dmg para la versión de Citrix Receiver para Mac que desea instalar desde el sitio web de Citrix y abra ese archivo.
2. En la página de Introducción, haga clic en **Continuar**.
3. En la página **Licencia**, haga clic en **Continuar**.
4. Haga clic en **Aceptar** para aceptar los términos del contrato de licencia.

5. En la página **Tipo de instalación**, haga clic en **Instalar**.
6. Introduzca el nombre de usuario y la contraseña de un administrador del dispositivo local.

Actualización de Citrix Receiver para Mac

Se respalda la actualización desde la versión 11.x del Online Plug-in para Mac. Puede actualizar Citrix Receiver para Mac desde cualquiera de las versiones anteriores de Citrix Receiver para Mac.

> **Importante**
>
> La integración con ShareFile se ha quitado a partir de la versión 11.8. Si integró Citrix Receiver para Mac con ShareFile, al actualizar se le pedirá que descargue la aplicación de ShareFile para poder continuar accediendo a sus datos remotos.

Acerca de la implementación y configuración de Citrix Receiver para Mac

Para implementaciones con StoreFront:

- Se recomienda configurar NetScaler Gateway y StoreFront 3.x según se describe en la documentación de NetScaler Gateway y StoreFront. Adjunte el archivo de aprovisionamiento creado por StoreFront en un mensaje de correo electrónico e informe a los usuarios de cómo realizar la actualización y cómo abrir el archivo de aprovisionamiento después de instalar Citrix Receiver para Mac.
- Como alternativa al uso de un archivo de aprovisionamiento, indique a los usuarios que introduzcan la URL de NetScaler Gateway. Si configuró la detección de cuentas basada en correo electrónico según se describe en la documentación de StoreFront, indique a los usuarios que introduzcan su dirección de correo electrónico.
- Otro método consiste en configurar un sitio de Receiver para Web, según se describe en la documentación de StoreFront. Indique a los usuarios cómo pueden actualizar Citrix Receiver para Mac, acceder al sitio de Receiver para Web y descargar el archivo de aprovisionamiento desde la interfaz de Receiver para Web (haciendo clic en el nombre de usuario y luego en Activar).

Para implementaciones con la Interfaz Web:

- Actualice el sitio de Interfaz Web con Receiver para Mac, e indique a los usuarios cómo deben realizar la actualización de Citrix Receiver para Mac. Por ejemplo, puede presentar unos mensajes de instalación en su pantalla de Mensajes para advertirles de que deben actualizar a la versión más reciente de Citrix Receiver para Mac.

Implementación de Citrix Receiver para Mac desde Receiver para Web

Es posible implementar Citrix Receiver para Mac desde Receiver para Web para asegurarse de que los usuarios tengan Receiver instalado antes de que intenten conectarse con una aplicación desde un explorador web. Los sitios de Receiver para Web permiten que los usuarios accedan a almacenes de StoreFront a través de una página web. Si el sitio de Receiver para Web detecta que un usuario no dispone de una versión de Citrix Receiver para Mac compatible, le solicita al usuario que descargue e instale Citrix Receiver para Mac. Para obtener más información, consulte la documentación de StoreFront.

Implementación de Citrix Receiver para Mac desde una pantalla de inicio de sesión de la Interfaz Web

Esta función solo está disponible para versiones de XenDesktop y XenApp que respaldan la Interfaz Web.

Es posible implementar Citrix Receiver para Mac desde una página web para asegurarse de que los usuarios tengan Receiver instalado antes de que intenten utilizar la Interfaz Web. La Interfaz Web ofrece un proceso de detección e instalación de clientes que detecta los clientes Citrix que pueden instalarse en el entorno de cada usuario y, posteriormente, guía a los usuarios a través del proceso de instalación.

Puede configurar el proceso de detección e instalación de clientes para que se ejecute automáticamente cuando los usuarios accedan a un sitio web de XenApp. Si la Interfaz Web detecta que un usuario no dispone de una versión de Receiver compatible, le solicita al usuario que descargue e instale Receiver.

Desinstalación de Citrix Receiver para Mac

Si desea desinstalar manualmente Citrix Receiver para Mac, abra el archivo CitrixReceiver.dmg, seleccione **Desinstalar Citrix Receiver** y siga las instrucciones en pantalla.

Configuración

October 9, 2019

Una vez instalado el software de Citrix Receiver para Mac, los usuarios pueden seguir estos pasos de configuración para acceder a sus aplicaciones y escritorios alojados:

Si tiene usuarios que se conectan desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet o desde ubicaciones remotas), configure la autenticación a través de NetScaler Gateway.

Configurar la redirección USB

La redirección de dispositivos USB de HDX permite redirigir dispositivos USB hacia y desde un dispositivo de usuario. Por ejemplo, un usuario puede conectar una unidad flash a un equipo local y acceder a ella de forma remota desde un escritorio virtual o desde una aplicación alojada en el escritorio. Durante una sesión, los usuarios pueden conectar dispositivos Plug and Play, incluidos dispositivos PTP (Picture Transfer Protocol) tales como cámaras digitales, dispositivos MTP (Media Transfer Protocol) tales como reproductores de sonido digital o reproductores multimedia portátiles, dispositivos de punto de venta (POS) y otros dispositivos como punteros 3D Space, escáneres, paneles de firma electrónica, etc.

> **Nota:**
>
> El doble salto de USB no está respaldado para sesiones de aplicaciones alojadas en escritorios.

La redirección de USB está disponible para Citrix Receiver:

- Windows
- Linux
- Mac

De manera predeterminada, se permite la redirección de USB para ciertas clases de dispositivos USB, y se rechaza para otras. Se puede restringir los tipos de dispositivos USB disponibles para un escritorio virtual actualizando la lista de dispositivos USB respaldados para la redirección, según se describe más adelante en este tema.

> **Sugerencia**
>
> En los entornos donde es necesario hacer una separación de seguridad entre el servidor y el dispositivo de usuario, Citrix recomienda dar instrucciones a los usuarios sobre los tipos de dispositivos USB que deben evitar.

Hay canales virtuales optimizados disponibles para redirigir los dispositivos USB utilizados con más frecuencia y proporcionar un rendimiento superior y mayor eficiencia del ancho de banda sobre redes WAN. Los canales virtuales optimizados suelen ser la mejor opción, especialmente en entornos de alta latencia.

> **Nota:**
>
> A efectos de redirección de USB, Citrix Receiver para Mac gestiona los paneles SMART igual que un mouse.

El producto respalda el uso de canales virtuales optimizados con dispositivos USB 3.0 y puertos USB 3.0, tales como un canal virtual CDM utilizado para ver archivos en una cámara o para proporcionar el sonido en unos auriculares). El producto también respalda la Redirección de USB genérico de dispositivos USB 3.0 conectados a puertos USB 2.0.

Algunas funciones avanzadas específicas de ciertos productos, como los botones HID (Human Interface Device) de una cámara Web, pueden no funcionar del modo esperado cuando se usa el canal virtual optimizado; si esto supone un problema, use el canal virtual USB genérico.

Algunos dispositivos no se redireccionan de manera predeterminada y solo están disponibles en la sesión local. Por ejemplo, no sería adecuado redireccionar una tarjeta de interfaz de red que está conectada directamente por USB interno.

Para usar la redirección de USB:

1. Conecte el dispositivo USB al dispositivo donde está instalado Receiver.
2. Se le pedirá que seleccione los dispositivos USB disponibles en el sistema local.
3. Seleccione el dispositivo que quiere conectar y haga clic en **Conectar**. Si la conexión falla, aparece un mensaje de error.
4. El dispositivo USB aparecerá listado en el panel USB, en la ventana **Preferencias**, en la ficha **Dispositivos**:
5. Seleccione el tipo de canal virtual para el dispositivo USB, *Genérico* u *Optimizado*.
6. Aparecerá un mensaje. Haga clic para conectar el dispositivo USB a su sesión:

Usar y quitar dispositivos USB

Los usuarios pueden conectar un dispositivo USB antes o después de iniciar una sesión virtual. Cuando se usa Citrix Receiver para Mac, ocurre lo siguiente:

- Los dispositivos conectados después haber iniciado la sesión aparecen inmediatamente en el menú USB de Desktop Viewer.
- Si un dispositivo USB no se redirige correctamente, a veces se puede resolver el problema esperando para conectar el dispositivo hasta después de que la sesión virtual se ha iniciado.
- Para evitar la pérdida de datos, use el menú de Windows **Extracción segura** antes de quitar el dispositivo USB.

Configuración de Enlightened Data Transport (EDT)

De manera predeterminada, EDT está habilitado en Citrix Receiver para Mac.

Citrix Receiver para Mac lee los parámetros de EDT según están definidos en el archivo default.ica y los aplica.

Para inhabilitar EDT, ejecute este comando en un terminal:

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

Configuración de la fiabilidad de la sesión y la reconexión automática de clientes

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Con la función de fiabilidad de la sesión, la sesión permanece activa en el servidor. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela hasta que se recupera la conectividad. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

> **Importante**
>
> Los usuarios de Citrix Receiver para Mac no pueden anular la configuración del servidor.

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS).

> **Nota**
>
> TLS cifra solo los datos enviados entre el dispositivo de usuario y NetScaler Gateway.

Uso de directivas de fiabilidad de la sesión

La configuración de directiva **conexiones de fiabilidad de la sesión** permite o impide la fiabilidad de la sesión.

La configuración de directiva **tiempo de espera de fiabilidad de la sesión** tiene un tiempo predeterminado de 180 segundos, o tres minutos. Aunque puede ampliar la cantidad de tiempo que la fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no pedirá a éste que repita la autenticación.

> **Sugerencia**
>
> Si se alarga la cantidad de tiempo que una sesión se mantiene abierta, se incrementa el riesgo de que un usuario se distraiga, se aleje del dispositivo y con ello facilite a usuarios no autorizados el acceso a la sesión.

Las conexiones entrantes con la función de fiabilidad de la sesión utilizan el puerto 2598 a menos que cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.

Si no desea que los usuarios se reconecten con sesiones interrumpidas sin tener que repetir la autenticación, use la función Reconexión automática de clientes. Puede definir la configuración de directiva Autenticación para reconexión automática de clientes para que solicite a los usuarios que repitan la autenticación cuando vuelvan a conectarse a las sesiones interrumpidas.

Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La fiabilidad de la sesión cierra o desconecta la sesión de un usuario una vez trascurrido el tiempo que se especifica en la configuración de directiva Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

> **Nota**
>
> De forma predeterminada, la fiabilidad de sesión se habilita en el servidor. Para inhabilitar esta función, configure la directiva administrada por el servidor.

Configuración de la fiabilidad de la sesión

De forma predeterminada, la fiabilidad de la sesión está habilitada.

Para inhabilitar la fiabilidad de la sesión:

1. Abra Citrix Studio.
2. Abra la directiva **Conexiones de fiabilidad de la sesión**.
3. Establezca la directiva en **Prohibida**.

Configuración del tiempo de espera de la fiabilidad de la sesión

De forma predeterminada, el tiempo de espera de la fiabilidad de la sesión tiene un valor de 180 segundos.

> **Nota:**
>
> La directiva tiempo de espera de fiabilidad de la sesión se puede configurar solo en XenApp/XenDesktop 7.11 y versiones posteriores.

Para modificar el tiempo de espera de la fiabilidad de la sesión:

1. Abra Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Configuración de la reconexión automática de clientes

De forma predeterminada, la reconexión automática de clientes está habilitada.

Para inhabilitar la reconexión automática de clientes

1. Abra Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Establezca la directiva en **Prohibida**.

Configuración del tiempo de espera de la reconexión automática de clientes

De forma predeterminada, el tiempo de espera para la reconexión automática de clientes tiene un valor de 120 segundos.

> **Nota:**
>
> La directiva de tiempo de espera de reconexión automática de clientes solo se puede configurar con XenApp/XenDesktop 7.11 y versiones posteriores.

Para modificar el tiempo de espera de la reconexión automática de clientes:

1. Abra Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Limitaciones:

En un VDA de Terminal Server, Citrix Receiver para Mac usa 120 segundos como tiempo de espera independientemente de cómo se configuren los parámetros del usuario.

Configuración del nivel de transparencia de la interfaz de usuario durante la reconexión

La interfaz de usuario durante una sesión se muestra en pantalla durante los intentos de conexión de la función de fiabilidad de la sesión y la reconexión automática de clientes. El nivel de transparencia de la interfaz de usuario se puede modificar mediante directiva en Studio.

De manera predeterminada, el nivel de transparencia de la interfaz de usuario es del 80%.

Para modificar el nivel de transparencia de la interfaz de usuario durante una reconexión:

1. Abra Citrix Studio.
2. Abra la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**.
3. Cambie el valor.
4. Haga clic en **Aceptar**.

Interacción entre la fiabilidad de sesión y la reconexión automática de clientes

La movilidad entre varios puntos de acceso, las interrupciones de la red y los tiempos de espera excedidos debido a problemas de latencia en el entorno, dificultan el mantenimiento de la integridad de los vínculos de las sesiones activas de Citrix Receiver. Para solucionar este problema, Citrix ha mejorado las tecnologías de fiabilidad de la sesión y reconexión automática presentes en esta versión de Receiver para Mac.

La reconexión automática de clientes, junto con la fiabilidad de la sesión, permiten a los usuarios reconectarse automáticamente con sus sesiones de Citrix Receiver después de recuperarse de una interrupción en la red. Estas funciones se habilitan mediante directivas en Citrix Studio y se pueden utilizar para mejorar sustancialmente la experiencia del usuario.

> **Nota:**
>
> Los valores de tiempo de espera de la reconexión automática del cliente y la fiabilidad de la sesión se pueden modificar en el archivo **default.ica** de StoreFront.

Reconexión automática de clientes

La reconexión automática de clientes se puede habilitar o inhabilitar mediante las directivas de Citrix Studio. De manera predeterminada, esta función está habilitada. Para obtener más información sobre cómo modificar esta directiva, consulte la sección sobre la reconexión automática de clientes más arriba en este artículo.

Use el archivo default.ica de StoreFront para modificar el tiempo de espera del parámetro AutoClientReconnect; de manera predeterminada, el tiempo de espera tiene un valor de 120 segundos (o dos minutos).

Parámetro	Ejemplo	URL predeterminadas
TransportReconnectRetryMaxTi	TransportReconnectRetryMaxTi	120

Fiabilidad de la sesión

La fiabilidad de la sesión se puede habilitar o inhabilitar mediante las directivas de Citrix Studio. De manera predeterminada, esta función está habilitada.

Use el archivo **default.ica** de StoreFront para modificar el tiempo de espera de la fiabilidad de la sesión; de manera predeterminada, el tiempo de espera tiene un valor de 180 segundos (o tres minutos).

Parámetro	Ejemplo	URL predeterminadas
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Cómo funcionan la reconexión automática de clientes y la fiabilidad de la sesión

Cuando la reconexión automática de clientes y la fiabilidad de la sesión están habilitadas en Citrix Receiver para Mac, tenga en cuenta lo siguiente:

- La ventana de la sesión se oscurece mientras tiene lugar una reconexión; aparece un temporizador donde se muestra el tiempo que falta para que se reconecte la sesión. Cuando se supera el tiempo de espera, la sesión se desconecta.

De manera predeterminada, la cuenta atrás del temporizador de notificación de lar reconexión empieza con 5 minutos; este valor representa los valores combinados del temporizador de reconexión automática del cliente y del temporizador de fiabilidad de la sesión (2 y 3 minutos, respectivamente). En la imagen siguiente se puede ver la notificación de cuenta atrás del temporizador, que aparece en la sección superior derecha de la interfaz de la sesión:

> **Sugerencia**
>
> Se puede modificar el brillo de la escala de grises utilizado para una sesión inactiva, mediante la interfaz de comandos. Por ejemplo: defaults write com.citrix.receiver.nomas NetDisruptBrightness 80. De forma predeterminada, este valor está establecido en 80. El valor máximo es 100 (esto indica una ventana transparente) y el valor mínimo es 0 (esto indica una pantalla en negro).

- Los usuarios ven una notificación cuando la sesión se reconecta correctamente (o cuando la sesión se desconecta). Esta notificación aparece en la sección superior derecha de la interfaz de la sesión:
- La ventana de una sesión que está bajo el control de las funciones de reconexión automática de clientes y fiabilidad de la sesión presenta un mensaje informativo donde se indica el estado de la conexión de la sesión. Haga clic en **Cancelar reconexión** para volver a una sesión activa.

Configuración de CEIP

CEIP está programado para obtener y enviar datos de forma segura a Citrix en un intervalo de 7 días de manera predeterminada. Puede cambiar su participación en el programa CEIP cuando quiera desde la pantalla **Seguridad > Preferencias** de Citrix Receiver para Mac.

> **Sugerencia**
>
> Cuando el programa CEIP está inhabilitado, se envía información mínima que solo contiene la versión de Citrix Receiver para Mac que está instalada. Esto tiene lugar solo una vez. Esta información mínima es valiosa para Citrix porque le permite conocer la distribución de las distintas versiones utilizadas por los clientes. Esto tiene lugar solo una vez después de inhabilitar CEIP.

Para inhabilitar el programa CEIP, o para cancelar su participación:

1. En la ventana **Preferencias**, seleccione **Seguridad y privacidad**.
2. Seleccione la ficha **Privacidad**.
3. Seleccione la opción correspondiente. Por ejemplo, para inhabilitar el programa CEIP, haga clic en "**No, gracias**."
4. Haga clic en **Aceptar**.

Configurar la entrega de aplicaciones

Cuando entregue aplicaciones con XenDesktop o XenApp, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a las aplicaciones:

Modo de acceso Web

Sin necesidad de configuración, Citrix Receiver para Mac ofrece el modo de acceso Web: acceso mediante un explorador web a las aplicaciones y escritorios. Los usuarios simplemente abren un explorador web para ir a un sitio de Receiver para Web o sitio de Interfaz Web y allí seleccionan y usan las aplicaciones que deseen. En el modo de acceso Web, no se colocan accesos directos de aplicaciones en la carpeta de Aplicaciones del dispositivo de usuario.

Modo de autoservicio

Agregando una cuenta de StoreFront a Citrix Receiver para Mac o configurando Citrix Receiver para Mac para que apunte a un sitio de StoreFront, puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones mediante Receiver. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles. En el modo de autoservicio se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias. Cuando uno de sus usuarios selecciona una aplicación, se coloca un acceso directo para esa aplicación en la carpeta Aplicaciones del dispositivo del usuario.

Cuando acceden a un sitio de StoreFront 3.0, los usuarios obtienen una experiencia de usuario de Citrix Receiver para Mac Tech Preview.

Cuando publique aplicaciones en las comunidades XenApp, para mejorar la experiencia de los usuarios que acceden a esas aplicaciones mediante almacenes de StoreFront, asegúrese de incluir descripciones claras para las aplicaciones publicadas. Las descripciones estarán visibles para los usuarios a través de Citrix Receiver para Mac.

Configurar el modo de autoservicio

Como se ha mencionado antes, simplemente agregando una cuenta de StoreFront a Citrix Receiver para Mac o configurando Citrix Receiver para Mac para que apunte a un sitio de StoreFront, se puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones mediante la interfaz de usuario de Receiver. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles.

En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS:Auto a la descripción que proporcionará cuando publique la aplicación en XenApp. Cuando los usuarios inicien sesión en el almacén, la aplicación se suministrará automáticamente sin necesidad de que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Para anunciar aplicaciones a los usuarios o facilitar la búsqueda de las aplicaciones más utilizadas mediante su incorporación a la lista Destacados de Citrix Receiver para Mac, agregue la cadena KEYWORDS:Featured a la descripción de la aplicación.

Para obtener más información, consulte la documentación de StoreFront.

Si la Interfaz Web de la implementación de XenApp no dispone de un sitio de servicios XenApp, cree uno. El nombre del sitio y la forma de crearlo depende de la versión de la Interfaz Web que tenga instalada. Para obtener más información, consulte la documentación de Interfaz Web.

Configurar StoreFront

Con StoreFront, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para Citrix Receiver para Mac. Cree almacenes que enumeren y agrupen escritorios y aplicaciones de sitios de XenDesktop y comunidades XenApp para, así, habilitar estos recursos para los usuarios.

1. Instale y configure StoreFront. Para obtener más información, consulte la documentación de StoreFront.

   Nota: Para los administradores que necesitan más control, Citrix ofrece una plantilla que se puede usar para crear un sitio de descargas de Citrix Receiver para Mac.

2. Configure almacenes para CloudGateway de la misma forma que con otras aplicaciones de XenApp y XenDesktop. No se requiere ninguna configuración especial de Citrix Receiver para Mac. Para más información, consulte Configuración de los almacenes en la documentación de StoreFront.

Cómo proporcionar información de cuentas a los usuarios

Después de la instalación, es necesario proporcionar a los usuarios la información de cuenta que necesitan para acceder a sus aplicaciones y escritorios alojados. Puede proporcionarles esta información de las siguientes formas:

- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Proporcionar un archivo de aprovisionamiento a los usuarios
- Entregando a los usuarios una dirección URL de configuración generada automáticamente
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Configurar la detección de cuentas basada en direcciones de correo electrónico

Puede configurar Citrix Receiver para Mac para que use la detección de cuentas basada en correo electrónico. Cuando está configurada, los usuarios introducen su dirección de correo electrónico, en lugar de una dirección URL de servidor, durante la instalación y configuración inicial de Citrix Receiver para Mac. Citrix Receiver para Mac determina el dispositivo NetScaler Gateway o el servidor StoreFront que está asociado con esa dirección de correo electrónico, en función de los registros de servicio (SRV) de sistema de nombres de dominio (DNS) y, posteriormente, solicita a los usuarios que inicien sesión para obtener acceso a sus aplicaciones y escritorios alojados.

Para configurar su servidor DNS para que respalde la detección basada en correo electrónico, consulte el tema Configuración de la detección de cuentas basada en correo electrónico en la documentación de StoreFront.

Para configurar NetScaler Gateway para que acepte conexiones de usuario mediante una dirección de correo electrónico para detectar la URL de StoreFront o NetScaler Gateway, consulte Conexión a StoreFront mediante detección basada en correo electrónico en la documentación de NetScaler Gateway.

Entrega de un archivo de aprovisionamiento a los usuarios

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Estos archivos se ponen a disposición de los usuarios para que puedan configurar Receiver de forma automática. Después de la instalación, los usuarios simplemente abren el archivo para configurar Citrix Receiver para Mac. Si se configuran sitios de Receiver para Web,

los usuarios también pueden obtener los archivos de aprovisionamiento de Citrix Receiver para Mac desde esos sitios.

Para obtener más información, consulte la documentación de StoreFront.

Entrega de una dirección URL de configuración generada automáticamente a los usuarios

Es posible utilizar Setup URL Generator de Citrix Receiver para Mac para crear una dirección URL que contenga información de las cuentas. Después de la instalación de Citrix Receiver para Mac, los usuarios simplemente pueden hacer clic en la dirección URL para configurar la cuenta y acceder a los recursos. Utilice esta utilidad para configurar los parámetros de las cuentas y enviar por correo electrónico o publicar esa información a todos los usuarios de una sola vez.

Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Si va a entregar a los usuarios los datos de sus cuentas para que luego los introduzcan manualmente, asegúrese de distribuir la siguiente información para permitirles conectar con éxito con sus aplicaciones y escritorios alojados en servidores:

- La dirección URL del almacén de StoreFront o del sitio de servicios XenApp que aloja los recursos; por ejemplo: `https://servername.example.com`
- Para el acceso mediante NetScaler Gateway: dirección de NetScaler Gateway, edición del producto y método de autenticación requerido

  Para obtener más información sobre cómo configurar NetScaler Gateway, consulte la documentación de NetScaler Gateway.

Cuando un usuario introduce la información de una cuenta nueva, Receiver intenta verificar la conexión. Si la conexión es satisfactoria, Citrix Receiver para Mac solicita al usuario que se conecte a la cuenta.

Configurar la actualización automática

Configurar mediante la interfaz gráfica de usuario

Un usuario individual puede anular la configuración de Actualizaciones de Citrix Receiver desde el diálogo **Preferencias**. Se trata de una configuración específica de usuario y los parámetros se aplican solamente al usuario actual.

1. Vaya al cuadro de diálogo **Preferencias** en Citrix Receiver para Mac.
2. En el panel **Avanzado**, haga clic en **Actualización automática**. Aparecerá el cuadro de diálogo Actualizaciones de Citrix Receiver.

3. Seleccione una de estas opciones:
    - Sí, notificarme
    - No, no notificarme
    - Usar parámetros especificados por el administrador
4. Cierre el cuadro de diálogo para guardar los cambios.

Configurar Actualizaciones de Citrix Receiver mediante StoreFront

Los administradores pueden configurar las Actualizaciones de Citrix Receiver con StoreFront. Citrix Receiver solo usa esta configuración para los usuarios que han seleccionado "Usar parámetros especificados por el administrador". Para configurarlo manualmente, siga estos pasos.

1. Use un editor de texto para abrir el archivo web.config. La ubicación predeterminada es C:\inetpub\wwwroot\Citrix\Roaming\web.config.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación)

    Por ejemplo: <account id=… name="Store">

    Antes de la etiqueta *</account>*, vaya a las propiedades de esa cuenta de usuario:

    <properties>

    <clear />
    </properties>
3. Agregue la etiqueta de actualización automática después de *<clear />*.

auto-update-Check

Esto determina que Citrix Receiver puede detectar si las actualizaciones están disponibles.

Valores válidos:

- Auto. Con esta opción, recibirá notificaciones cuando existan actualizaciones disponibles.
- Manual. Con esta opción, no recibirá notificaciones cuando existan actualizaciones disponibles. Los usuarios deben buscar manualmente las actualizaciones. Para ello, deberán seleccionar **Comprobar actualizaciones**.
- Inhabilitada. Con esta opción, se inhabilitan las actualizaciones de Citrix Receiver.

auto-update-DeferUpdate-Count

Determina la cantidad de veces que el usuario final recibirá notificaciones para actualizar Citrix Receiver antes de obligarlo a actualizar a la versión más reciente. El valor predeterminado es 7.

Valores válidos:

- -1. El usuario final siempre tendrá la opción de recibir un recordatorio más tarde cuando una actualización esté disponible.
- 0. Se obligará al usuario final a que actualice a la versión más reciente de Citrix Receiver tan pronto como la actualización esté disponible.
- Número entero positivo. El final usuario recibirá esta cantidad de recordatorios antes de que se le obligue a actualizar. Citrix recomienda no establecer este valor a más de 7.

auto-update-Rollout-Priority

Determina lo rápido que un dispositivo detectará que hay una actualización disponible.

Valores válidos:

- Auto – El sistema de actualizaciones de Citrix Receiver decidirá cuándo entregar a los usuarios las actualizaciones disponibles.
- Fast (Rápido). Las actualizaciones disponibles se aplicarán a los usuarios con prioridad alta de la manera que lo determine Citrix Receiver.
- Medium (Medio). Las actualizaciones disponibles se aplicarán a los usuarios con prioridad media de la manera que lo determine Citrix Receiver.
- Slow (Lento). Las actualizaciones disponibles se aplicarán a los usuarios con prioridad baja de la manera que lo determine Citrix Receiver.

Configurar el IME de cliente mejorado utilizando el archivo de configuración

El IME de cliente mejorado depende de la función de sincronización de la distribución del teclado. De forma predeterminada, la función de IME mejorado está habilitada cuando se activa la funcionalidad de sincronización de distribución de teclado. Para controlar esta función de manera independiente, abra el archivo **Config** en la carpeta ~/**Library**/**Application Support**/**Citrix Receiver**/, busque el parámetro "**EnableIMEEnhancement**" y active o desactive la función, mediante "true" o "false," respectivamente.

> **Nota:**
>
> El cambio de este parámetro tiene efecto después de reiniciar la sesión.

Sincronización de la distribución de teclado

La sincronización de la distribución del teclado permite a los usuarios cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada.

Para habilitar la sincronización de la distribución de teclado, vaya a **Preferencias > Teclado** y seleccione “Usar la distribución de teclado local, en lugar de la distribución de teclado del servidor remoto”.

> **Nota**:
>
> 1. El uso de la opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Si los usuarios que trabajan en japonés, chino y coreano prefieren usar el editor IME del servidor, deben inhabilitar la opción de distribución de teclado local en **Preferencias > Teclado**. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.
> 2. Esta función funciona en la sesión solo cuando está activada en el cliente y la función correspondiente está habilitada en el VDA; se agrega un elemento de menú, **Usar la distribución de teclado del cliente**, en **Dispositivos** > **Teclado** > **Internacional**, para mostrar el estado habilitado.

Limitaciones:

- Las distribuciones de teclado que figuran en “**Distribuciones de teclado compatibles en Mac**” funcionan al usar esta función. Cuando se cambia la distribución de teclado del cliente a una distribución que no es compatible, es posible que se sincronice la distribución en el VDA, pero no se puede confirmar la funcionalidad.
- Las aplicaciones remotas que se ejecutan con privilegios elevados (por ejemplo, al ejecutar aplicaciones como administrador) no se pueden sincronizar con la distribución de teclado del cliente. Para solucionar este problema, cambie manualmente la distribución del teclado en el VDA o inhabilite el control de cuentas de usuario (UAC).
- Cuando RDP se implementa como una aplicación y el usuario está trabajando en una sesión RDP, no es posible cambiar la distribución del teclado con los accesos directos Alt + Mayús. Para solucionar este problema, los usuarios pueden usar la barra de idioma en la sesión RDP para cambiar la distribución del teclado.

Optimizar

October 9, 2019

Reconexión automática de usuarios

Las sesiones se pueden desconectar debido a redes poco fiables, una latencia en la red muy variable o limitaciones en el alcance de los dispositivos inalámbricos. Con la función Reconexión automática

de clientes, Citrix Receiver para Mac puede detectar desconexiones accidentales de las sesiones ICA y volver a conectar automáticamente a los usuarios de las sesiones afectadas.

Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando. Citrix Receiver para Mac intenta repetidamente reconectar la sesión hasta que lo logra o hasta que el usuario cancela los intentos de reconexión. Si es necesaria la autenticación del usuario, aparece un cuadro de diálogo para ingresar las credenciales durante la reconexión automática. La reconexión automática no se produce si los usuarios salen de las aplicaciones sin realizar el cierre de la sesión.

La configuración de la reconexión automática de clientes se realiza mediante el ajuste de los parámetros de directivas en el servidor. Para obtener más información, consulte la documentación de XenApp y XenDesktop.

Reinicio de escritorios

Los usuarios pueden reiniciar un escritorio virtual si ese escritorio no se inicia, tarda demasiado tiempo en conectarse, o se daña. Esta función se configura en XenDesktop.

El elemento de menú contextual **Reiniciar** se encuentra disponible en todos los escritorios a los que los usuarios se suscriben y en la página Aplicaciones de cada usuario. El elemento de menú está inhabilitado si el reinicio no está habilitado para el escritorio. Cuando el usuario elige Reiniciar, Citrix Receiver para Mac apaga el escritorio y vuelve a iniciarlo.

> **Importante**
>
> Notifique a los usuarios que el reinicio de los escritorios puede provocar una pérdida de datos.

Brindar fiabilidad de sesiones

Con la funcionalidad Fiabilidad de la sesión, los usuarios siguen viendo las ventanas de aplicaciones y escritorios alojados cuando la conexión se interrumpe. Por ejemplo, los usuarios inalámbricos que pasen por un túnel pueden perder la conexión al entrar pero volverán a conectarse al salir del túnel. Durante tales interrupciones, la función de fiabilidad de la sesión permite que se vea la ventana mientras se restablece la conexión.

Se puede configurar el sistema para que muestre un cuadro de diálogo cuando la conexión no está disponible.

La Fiabilidad de la sesión se configura mediante los parámetros de directiva en el servidor. Para obtener más información sobre la fiabilidad de la sesión y la interacción de Receiver, consulte este documento sobre cómo garantizar la mejor calidad de servicio y fiabilidad.

Para obtener información adicional específica sobre las directivas, consulte Configuraciones de directiva de Reconexión automática de clientes y Configuraciones de directiva de Fiabilidad de la sesión.

> **Sugerencia**
>
> Los usuarios de Citrix Receiver para Mac no pueden sobrescribir los parámetros del servidor para fiabilidad de sesión.
>
> **Importante**
>
> Si la fiabilidad de la sesión está habilitada, el puerto predeterminado para la comunicación de la sesión cambia de 1494 a 2598.

Continuidad para los usuarios con perfil móvil

El control del área de trabajo permite a los escritorios y las aplicaciones seguir a los usuarios mientras éstos cambian de un dispositivo a otro. Esto permite, por ejemplo, que los médicos en los hospitales se trasladen de una estación de trabajo a otra sin tener que reiniciar sus escritorios ni aplicaciones en cada dispositivo.

Las directivas y asignaciones de las unidades del cliente cambian cuando se traslada a un dispositivo de usuario nuevo. Las directivas y asignaciones se aplican de acuerdo con el dispositivo de usuario donde se inicia la sesión. Por ejemplo, si un trabajador cierra la sesión desde un dispositivo de usuario en el área de Urgencias del hospital, y luego inicia sesión en una estación de trabajo del Laboratorio de rayos X, las directivas, las asignaciones de impresora y las asignaciones de unidades del cliente apropiadas para la sesión en el Laboratorio de rayos X entran en efecto en el momento que el usuario inicia sesión en el dispositivo de usuario de ese laboratorio.

Para configurar los parámetros de control del área de trabajo

1. Haga clic en el icono con la flecha hacia abajo en la ventana de Citrix Receiver para Mac y elija **Preferencias**.
2. Haga clic en la ficha **General**.
3. Elija una de las siguientes opciones:
   - Reconectar aplicaciones al iniciar Receiver. Permite que los usuarios se vuelvan a conectar a aplicaciones desconectadas cuando inician Receiver.
   - Reconectar aplicaciones al iniciar o actualizar las aplicaciones. Permite que los usuarios se vuelvan a conectar a aplicaciones desconectadas cuando inician las aplicaciones o cuando seleccionan Actualizar aplicaciones en el menú de Citrix Receiver.

Asignar dispositivos cliente

Citrix Receiver para Mac asigna automáticamente unidades y dispositivos locales para que estén disponibles dentro de una sesión. Cuando se habilita en el servidor, la función de asignación de dispositivos del cliente permite que una aplicación o un escritorio remoto que se ejecuta en un servidor acceda a los dispositivos conectados al dispositivo de usuario local. Puede:

- Acceder a las unidades, los puertos COM y las impresoras locales
- Escuchar sonido (sonidos del sistema y archivos de sonido) reproducido en la sesión

> **Nota**
>
> La asignación de sonido del cliente y la asignación de impresoras del cliente no necesita ningún tipo de configuración en el dispositivo de usuario.

Asignación de unidades del cliente

La asignación de unidades del cliente permite acceder a las unidades locales en el dispositivo de usuario como las unidades de CD-ROM, DVD y los dispositivos de memoria USB durante las sesiones. Cuando un servidor se configura para permitir la asignación de unidades del cliente, los usuarios pueden acceder a los archivos almacenados localmente, trabajar con esos archivos durante las sesiones y guardarlos nuevamente en una unidad local o en una unidad del servidor.

Citrix Receiver para Mac supervisa los directorios en los que los dispositivos de hardware como CD-ROM, DVD y los dispositivos de memoria USB se montan normalmente en el dispositivo de usuario, y asigna automáticamente los dispositivos nuevos que aparecen durante una sesión a la siguiente letra de unidad disponible en el servidor.

Es posible configurar el nivel de acceso de lectura y escritura para las unidades asignadas mediante las preferencias de Citrix Receiver para Mac.

Para configurar el acceso de lectura y escritura de las unidades asignadas

1. En la página de inicio de Citrix Receiver para Mac, haga clic en el icono con la flecha hacia abajo y seleccione **Preferencias**.
2. Haga clic en **Dispositivos**.
3. Seleccione el nivel de acceso de lectura y escritura para las unidades asignadas mediante las siguientes opciones:
    - Lectura y escritura
    - Solo lectura
    - Sin acceso
    - Preguntar siempre
4. Cierre las sesiones abiertas y vuelva a conectarse para aplicar los cambios.

Mejora de la experiencia del usuario

October 9, 2019

Programa para la mejora de la experiencia del usuario (CEIP)

El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información anónima de uso y de configuración de Citrix Receiver para Mac y envía esos datos automáticamente a Citrix. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de Citrix Receiver para Mac.

Suavizado de fuentes ClearType

El suavizado de fuentes ClearType (también conocido como presentación de fuentes de subpíxel) mejora la calidad de las fuentes en pantalla más allá de las posibilidades que permite el suavizado de fuentes estándar o "anti-aliasing".

Aunque se habilite el suavizado de fuentes ClearType en el servidor, no se obliga a los dispositivos de usuario a utilizar ese suavizado. Simplemente, se le indica al servidor que admita el suavizado de fuentes ClearType en los dispositivos de usuario que han habilitado localmente esta opción y que utilizan Citrix Receiver para Mac.

Citrix Receiver para Mac detecta automáticamente la configuración de suavizado de fuentes de los dispositivos de usuario y la envía al servidor. La sesión se conecta mediante esta configuración. Cuando se desconecta o se cierra la sesión, la configuración del servidor vuelve a los valores originales.

Entrada de micrófono en el cliente

Citrix Receiver para Mac admite varias entradas de micrófono en el cliente. Los micrófonos instalados localmente se pueden usar para:

- Actividades en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

Citrix Receiver para Mac brinda respaldo para dictado digital. Para obtener información sobre cómo configurar esta función, consulte la información de Funciones de audio en el sitio de la documentación del producto.

Para definir si desea utilizar o no los micrófonos conectados al dispositivo de usuario en las sesiones, seleccione una de las siguientes opciones en la ficha Micrófono y cámara Web de las Preferencias de Citrix Receiver para Mac:

- Usar mi micrófono y cámara Web
- No usar mi micrófono y cámara Web
- Preguntar siempre

Si selecciona la opción **Preguntar siempre**, se muestra un cuadro de diálogo cada vez que se conecta a una aplicación o un escritorio alojado donde se le pregunta si desea utilizar el micrófono en esa sesión.

Teclas especiales de Windows

Citrix Receiver para Mac ofrece diversas opciones adicionales y formas fáciles de sustituir teclas especiales, como las teclas de función de las aplicaciones de Windows, por teclas de Mac. Para configurar las opciones que desea usar, utilice la ficha Teclado de la siguiente manera:

- "Enviar el carácter Control mediante" permite seleccionar si se quieren enviar combinaciones de teclas Comando-tecla de carácter como combinaciones Ctrl+tecla de carácter dentro de una sesión. Si se selecciona "Comando o Control" en el menú emergente, es posible enviar combinaciones de teclas Comando-tecla de carácter o Ctrl-tecla de carácter conocidas de Mac a los PC como combinaciones Ctrl+tecla de carácter. Si se selecciona Control, se deben usar combinaciones de teclas Ctrl+tecla de carácter.
- "Enviar el carácter Alt mediante" permite seleccionar la forma de replicar la tecla Alt dentro de una sesión. Si se selecciona Comando-Opción, es posible enviar combinaciones de teclas Comando-Opción como combinaciones de teclas Alt+ dentro de una sesión. De forma alternativa, si se selecciona Comando, es posible usar la tecla Comando como la tecla Alt.
- "Enviar tecla con el logotipo de Windows mediante Comando (a la derecha)" permite enviar la tecla del logotipo de Windows a las aplicaciones y los escritorios remotos al presionar la tecla Comando ubicada a la derecha del teclado. Si esta opción se encuentra inhabilitada, la tecla Comando de la derecha presenta el mismo comportamiento que la tecla Comando de la izquierda según la configuración de los dos parámetros anteriores en el panel de preferencias, pero todavía es posible enviar la tecla del logotipo de Windows mediante el menú Teclado; seleccione Teclado > Enviar acceso directo de Windows > Inicio.
- "Enviar teclas especiales sin cambios" permite inhabilitar la conversión de teclas especiales. Por ejemplo, la combinación Opción-1 (en el teclado numérico) es equivalente a la tecla especial F1. Es posible modificar este comportamiento y establecer que esta tecla especial represente 1 (el número uno en el teclado) en la sesión. Para eso, se debe seleccionar la casilla de verificación "Enviar teclas especiales sin cambios". De forma predeterminada, esta casilla de verificación no está seleccionada, así que Opción-1 se envía a la sesión como F1.

El menú Teclado permite enviar teclas de función y otras teclas especiales a una sesión.

Si el teclado incluye un teclado numérico, también es posible usar las siguientes pulsaciones de teclas:

Acción o tecla de PC	Opciones de Mac
Insertar	0 (el número cero) en el teclado numérico. La tecla Bloq num debe estar desactivada; es posible activarla y desactivarla mediante la tecla Borrar; Opción-Ayuda
ELIMINAR	Punto decimal en el teclado numérico. La tecla Bloq num debe estar desactivada; es posible activarla y desactivarla mediante la tecla Borrar.
De F1 a F9	Opción-1 a -9 (los números del uno al nueve) en el teclado numérico
F10	Opción-0 (el número cero) en el teclado numérico
F11	Opción-signo menos en el teclado numérico
F12	Opción-signo más en el teclado numérico

Accesos directos y combinaciones de teclas de Windows

Las sesiones remotas reconocen la mayoría de las combinaciones de teclado Mac para la entrada de texto, como Opción-G para introducir el símbolo de copyright ©. No obstante, algunas pulsaciones de teclado que se realizan durante una sesión no se muestran en la aplicación o el escritorio remoto y se interpretan en el sistema operativo Mac. Esto puede provocar que las teclas generen respuestas de Mac.

Es posible que necesite usar ciertas teclas de Windows, como la tecla Insertar, que no existen en muchos teclados de Mac. De forma similar, algunos accesos directos de teclado de Windows 8 muestran botones de acceso y comandos de aplicación, y permiten acoplar y cambiar aplicaciones. Los teclados Mac no imitan de forma nativa estos accesos directos, pero permiten enviarlos a una aplicación o un escritorio remoto mediante el menú Teclado.

Los teclados y la configuración de las teclas pueden diferir considerablemente de un equipo a otro. Por ese motivo, Citrix Receiver para Mac ofrece diversas opciones para garantizar que las pulsaciones de teclado puedan enviarse correctamente a las aplicaciones y los escritorios alojados. Esas opciones se detallan en la tabla. Se describe el comportamiento predeterminado. Si se ajustan los valores predeterminados (mediante las preferencias de Citrix Receiver para Mac u otro programa), es posible que

se reenvíen combinaciones de teclas diferentes y se observen otros comportamientos en el equipo remoto.

> **Importante**
>
> Ciertas combinaciones de teclas detalladas en la tabla no se encuentran disponibles cuando se utilizan teclados Mac más nuevos. En la mayoría de estos casos, las entradas de teclado se pueden enviar a la sesión mediante el menú Teclado.

Convenciones utilizadas en la tabla:

- Las teclas de letras figuran en mayúscula, pero no implican que sea necesario presionar simultáneamente la tecla Mayús.
- Los guiones entre las pulsaciones de teclado indican que las teclas se deben presionar juntas (por ejemplo, Control-C).
- Las teclas de caracteres generan entradas de texto y contienen todas las letras, los números y los signos de puntuación. Las teclas especiales no generan entradas por sí mismas, pero funcionan como modificadores o controladores. Las teclas especiales incluyen Control, Alt, Mayús, Comando, Opción, teclas de flecha y teclas de función.
- Las instrucciones para los menús corresponden a los menús de la sesión.
- Según la configuración del dispositivo de usuario, es posible que algunas combinaciones de teclas no funcionen de la forma esperada y se enumeren combinaciones alternativas.
- Fn hace referencia a la tecla Fn (Función) en un teclado Mac; las teclas de función hacen referencia a las teclas F1 a F12 en los teclados de PC o Mac.

Tecla o combinación de teclas de Windows	Equivalentes de Mac
Alt+tecla de carácter	Comando-Opción-tecla de carácter (por ejemplo, utilice Comando-Opción-C para enviar Alt-C)
Alt+tecla especial	Opción-tecla especial (por ejemplo, Opción-Tab); Comando-Opción-tecla especial (por ejemplo, Comando-Opción-Tab)
Ctrl+tecla de carácter	Comando-tecla de carácter (por ejemplo, Comando-C); Control-tecla de carácter (por ejemplo, Control-C)
Ctrl+tecla especial	Control-tecla especial (por ejemplo, Control-F4); Comando-tecla especial (por ejemplo, Comando-F4)
Ctrl/Alt/Mayús/Logotipo de Windows+tecla de función	Seleccione Teclado > Enviar tecla de función > Control/Alt/Mayús/Comando-tecla de función
Ctrl + Alt	Control-Opción-Comando

Tecla o combinación de teclas de Windows	Equivalentes de Mac
Ctrl+Alt+Suprimir	Control-Opción-Suprimir; Control-Opción-Fn-Delete (en teclados MacBook); Control-Opción-Fn-Eliminar (en teclados MacBook)> Enviar Ctrl-Alt-Del
Eliminar	Eliminar; Seleccione Teclado > Enviar clave > Eliminar; Fn-Retroceso (Fn-Eliminar en algunos teclados para Estados Unidos)
Finalizar	Finalizar; Fn-Flecha derecha
ESC	Escape; Seleccione Teclado > Enviar tecla > Escape
De F1 a F12	De F1 a F12; Seleccione Teclado > Enviar tecla de función > De F1 a F12
Inicio	Página; Fn-Tecla izquierda
Insertar	Seleccione Teclado > Enviar tecla > Insertar
Bloq num	Borrar
Av Pág	Av Pág; Fn-Tecla abajo
Re Pág	Re Pág; Fn-Tecla arriba
Barra espaciadora	Seleccione Teclado > Enviar tecla > Espacio
Ficha	Seleccione Teclado > Enviar tecla > Tab
Logotipo de Windows	Tecla de comando a la derecha (una preferencia de teclado habilitada de forma predeterminada); Seleccione Teclado > Enviar acceso directo de Windows > Inicio
Combinación de teclas para mostrar botones de acceso	Seleccione Teclado > Enviar acceso directo de Windows > Botones de acceso
Combinación de teclas para mostrar comandos de aplicación	Seleccione Teclado > Enviar acceso directo de Windows > Comandos de aplicación
Combinación de teclas para acoplar aplicaciones	Seleccione Teclado > Enviar acceso directo de Windows > Acoplar
Combinación de teclas para cambiar aplicaciones	Seleccione Teclado > Enviar acceso directo de Windows > Cambiar aplicaciones

Uso de editores IME y distribuciones de teclado internacionales

Citrix Receiver para Mac permite utilizar un editor de métodos de entrada (IME) en el dispositivo de usuario o en el servidor.

Cuando el editor IME en el cliente está habilitado, los usuarios pueden introducir texto en el punto de inserción en lugar de en una ventana aparte.

Citrix Receiver para Mac también permite que los usuarios especifiquen la distribución del teclado que quieren utilizar.

Para habilitar el editor IME en el cliente

1. En la barra de menús Citrix Viewer, elija **Teclado > Internacional > Usar IME del cliente**.
2. Asegúrese de que el editor IME en el servidor esté establecido en el modo alfanumérico o de entrada directa.
3. Utilice el IME de Mac para introducir texto.

Para indicar de forma explícita el punto de partida al introducir texto

- En la barra de menús Citrix Viewer, elija **Teclado > Internacional > Usar marca de composición**.

Para usar el editor IME en el servidor

- Asegúrese de que el editor IME en el cliente esté establecido en el modo alfanumérico.

Teclas de modo de entrada asignadas para el editor IME en el servidor

Citrix Receiver para Mac ofrece asignaciones de teclado para las teclas de modo de entrada para el editor IME de Windows en el servidor que no se encuentran disponibles en los teclados Mac. En los teclados Mac, la tecla Opción se asigna a las siguientes teclas de modo de entrada para el editor IME en el servidor, según la configuración regional en el servidor:

Configuración regional del sistema en el servidor	Tecla de modo de entrada para el editor IME en el servidor
Japonés	Tecla Kanji (Alt + Hankaku/Zenkaku en un teclado japonés)
Coreano	Tecla Alt derecha (alternancia hangul/inglés en un teclado coreano)

Para utilizar distribuciones internacionales de teclado

- Asegúrese de que las distribuciones de teclado en el cliente y en el servidor tengan la misma configuración regional que el idioma de entrada predeterminado en el servidor.

Uso de varios monitores

Los usuarios pueden configurar Citrix Receiver para Mac para que funcione en modo de pantalla completa abarcando varios monitores, mediante la opción de menú: **Usar todas las pantallas en pantalla completa**.

Limitaciones conocidas

El modo de pantalla completa solo se respalda en uno o en todos los monitores, y esto puede configurarse mediante una opción de menú.

Uso de la barra de herramientas del escritorio

Los usuarios ahora pueden acceder a la barra de herramientas del escritorio tanto en modo de ventana como en modo de pantalla completa. Antes, la barra de herramientas solo estaba visible en el modo de pantalla completa. Otros cambios en la barra de herramientas incluyen lo siguiente:

- El botón **Inicio** se ha quitado de la barra de herramientas. Esta función se puede ejecutar mediante los comandos siguientes:
  - Cmd-Tab para cambiar a la aplicación activa anterior.
  - Ctrl-Flecha izquierda para cambiar al espacio anterior.
  - Mediante el trackpad integrado o gestos de Magic Mouse para cambiar a un espacio diferente.
  - Al mover el cursor hacia el borde de la pantalla cuando se está en modo de pantalla completa, aparecerá un Dock donde se puede elegir las aplicaciones que se quiere activar.
- El botón **En una ventana** se ha quitado de la barra de herramientas. Para salir del modo de pantalla completa y pasar al modo de ventana se puede seguir alguno de estos métodos:
  - En OS X 10.10, haga clic en el botón de ventana verde en la barra de menú desplegable.
  - En OS X 10.9, haga clic en el botón de menú azul en la barra de menú desplegable.
  - Para todas las versiones de OS X, seleccione **Salir de pantalla completa** en el menú **Visualización** de la barra de menú desplegable.
- El comportamiento de arrastre de la barra de herramientas se ha actualizado para dar respaldo al arrastre entre ventanas de pantalla completa con varios monitores.

Proteger comunicaciones

October 9, 2019

Para proteger la comunicación entre la comunidad de servidores y Citrix Receiver para Mac, puede integrar las conexiones a la comunidad de servidores con la ayuda de diversas tecnologías de seguridad, incluido Citrix NetScaler Gateway. Para obtener más información sobre cómo configurar Citrix StoreFront, consulte la documentación de
StoreFront.

> **Nota:**
>
> Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores de StoreFront y los dispositivos de los usuarios.

- Un servidor proxy SOCKS o un servidor proxy de seguridad (también conocido como servidor proxy seguro o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Citrix Receiver y los servidores. Citrix Receiver para Mac respalda el uso de SOCKS y protocolos de proxy seguro.
- Secure Gateway. Puede utilizar Secure Gateway junto con la Interfaz Web para proporcionar un punto de acceso único, seguro y cifrado a Internet para los servidores situados en las redes internas de la organización.
- Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security)
- Un firewall. Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si desea utilizar Citrix Receiver para Mac a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red, NAT), configure la dirección externa.

Acerca de los certificados

Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, se debe disponer de un certificado raíz para la entidad de certificación de la empresa en el dispositivo con el fin de poder acceder correctamente a los recursos Citrix mediante Citrix Receiver para Mac.

> **Nota:**
>
> Si el certificado de la puerta de enlace remota no se puede verificar en la conexión (debido a que no se incluyó el certificado raíz en el almacén de claves local), se muestra un mensaje de advertencia sobre la presencia de un certificado que no es de confianza. Si un usuario elige continuar, haciendo caso omiso del mensaje, aún se mostrará la lista de aplicaciones pero no se podrán

> iniciar.

Importación de certificados raíz en dispositivos con Receiver para Mac

Obtenga el certificado raíz de la autoridad emisora de certificados y envíelo por correo electrónico a una cuenta configurada en el dispositivo. Al seleccionar el adjunto, se le solicitará que importe el certificado raíz.

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. Citrix Receiver para Mac admite certificados comodín.

Certificados intermedios con NetScaler Gateway

Si la cadena de certificados contiene un certificado intermedio, deberá añadir este certificado intermedio al certificado de servidor de NetScaler Gateway. Para obtener más información sobre esta tarea, consulte la documentación de NetScaler Gateway. Para obtener más información sobre cómo instalar y vincular un certificado intermedio con una CA principal en un dispositivo de NetScaler Gateway, consulte el artículo How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway (Cómo instalar y vincular un certificado intermedio con una CA principal en NetScaler Gateway).

Directiva de validación conjunta de certificados de servidor

Esta versión de Citrix Receiver para Mac tiene una directiva más estricta para validar los certificados de servidor.

> **Importante**
>
> Antes de instalar esta versión de Citrix Receiver para Mac, confirme que los certificados presentes en el servidor o la puerta de enlace se han configurado correctamente como se describe aquí. Las conexiones pueden fallar si:
>
> - la configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
> - la configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
> - la configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
> - la configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Cuando valida un certificado de servidor, Citrix Receiver para Mac usa ahora **todos** los certificados suministrados por el servidor (o la puerta de enlace) para validarlo. Al igual que en las versiones anteriores, esta versión de Citrix Receiver para Mac también comprueba posteriormente que los certificados son de confianza. Si no todos los certificados son de confianza, la conexión falla.

Esta directiva es más estricta que la directiva de certificados presente en los exploradores web. Muchos exploradores web incluyen un gran conjunto de certificados raíz en los que confían.

El servidor (o la puerta de enlace) debe estar configurado con el conjunto correcto de certificados. Un conjunto incorrecto de certificados puede provocar que falle la conexión de Citrix Receiver para Mac.

Supongamos que se configura una puerta de enlace con estos certificados válidos. Esta configuración se recomienda para los clientes que requieren una validación más estricta, que necesitan determinar exactamente cuál es el certificado raíz usa Citrix Receiver para Mac:

- "Certificado de servidor - ejemplo"
- "Certificado intermedio - ejemplo"
- "Certificado raíz - ejemplo"

A continuación, Citrix Receiver para Mac comprobará que todos los certificados son válidos. Citrix Receiver para Mac comprobará también que ya confía en "Certificado raíz de ejemplo". Si Citrix Receiver para Mac no confía en "Certificado raíz de ejemplo", la conexión falla.

> **Importante**
>
> Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados ("DigiCert"/"GTE CyberTrust Global Root", and "DigiCert Baltimore Root"/"Baltimore CyberTrust Root") que pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible ("DigiCert Baltimore Root" o "Baltimore CyberTrust Root"). Si configura "GTE CyberTrust Global Root" en la puerta de enlace, fallarán las conexiones de Citrix Receiver para Mac en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.
>
> **Nota**
>
> Algunos servidores y puertas de enlace nunca envían el certificado raíz, aunque se haya configurado. En esos casos, esta validación más estricta no es posible.

Supongamos ahora que se configura una puerta de enlace con estos certificados válidos. Esta configuración, sin certificado raíz, es la que se suele recomendar:

- "Certificado de servidor - ejemplo"
- "Certificado intermedio - ejemplo"

Citrix Receiver para Mac usará esos dos certificados. Luego, buscará un certificado raíz en el dispositivo del usuario. Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, “Certificado raíz - ejemplo”), la conexión se realiza correctamente. De lo contrario, la conexión falla. Tenga en cuenta que esta configuración proporciona el certificado intermedio que necesita Citrix Receiver para Mac, pero también permite que Citrix Receiver para Mac elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una puerta de enlace con estos certificados:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”
- “Certificado raíz incorrecto”

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, Citrix Receiver para Mac no ignorará el certificado raíz incorrecto y la conexión fallará.

Algunas entidades de certificación usan más de un certificado intermedio. En este caso, la puerta de enlace se configura normalmente con todos los certificados intermedios (pero sin el certificado raíz):

- “Certificado de servidor - ejemplo”
- “Certificado intermedio 1 - ejemplo”
- “Certificado intermedio 2 - ejemplo”

> **Importante**
>
> Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Este tipo de certificado está pensado para situaciones en las que hay más de un certificado raíz: un certificado raíz anterior se usa al mismo tiempo que un certificado raíz posterior. En este caso, habrá al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio correspondiente de firmas cruzadas “VeriSign Class 3 Public Primary Certification Authority - G5”. No obstante, un certificado raíz posterior correspondiente “VeriSign Class 3 Public Primary Certification Authority - G5” también está disponible y reemplaza a “Class 3 Public Primary Certification Authority”. El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.
>
> **Nota**
>
> El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo Nombre de sujeto (Emitido para), pero el certificado intermedio con firmas cruzadas tiene otro Nombre de emisor (Emitido por). Esto distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como “Certificado intermedio 2 - ejemplo”).

Esta configuración, sin certificado raíz y sin certificado intermedio con firmas cruzadas, es la que se suele recomendar:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque seleccionará el certificado raíz anterior:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”
- “Certificado intermedio con firmas cruzadas de ejemplo” [no se recomienda]

No se recomienda configurar la puerta de enlace solamente con el certificado del servidor:

- “Certificado de servidor - ejemplo”

En este caso, si Citrix Receiver para Mac no puede localizar todos los certificados intermedios, la conexión fallará.

Conexión con NetScaler Gateway

Para permitir que los usuarios remotos se conecten a su implementación de XenMobile mediante NetScaler Gateway, puede configurar las conexiones para que funcionen con StoreFront. El método que se debe utilizar para habilitar el acceso depende de la edición de XenMobile existente en la implementación.

Si implementa XenMobile en la red, integre NetScaler Gateway con StoreFront para permitir las conexiones de usuarios internos y usuarios remotos a StoreFront a través de NetScaler Gateway. Con esta implementación, los usuarios pueden conectarse a StoreFront para acceder a las aplicaciones publicadas desde XenApp y a los escritorios virtuales desde XenDesktop. Los usuarios se pueden conectar mediante Citrix Receiver.

Conexión con Secure Gateway

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Es posible usar Secure Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre Citrix Receiver para Mac y el servidor. No es necesario configurar Citrix Receiver para Mac si se utiliza Secure Gateway en el modo Normal y los usuarios se conectan a través de la Interfaz Web.

Citrix Receiver para Mac usa parámetros que se configuran de forma remota en el servidor de la Interfaz Web para conectarse con los servidores que ejecutan Secure Gateway. Para obtener más información sobre la configuración de los parámetros de servidores proxy para Citrix Receiver para Mac, consulte la documentación de la Interfaz Web.

Si se instala Secure Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Gateway Proxy en modo de traspaso (Relay). Para obtener más información sobre el modo Relay de traspaso, consulte la documentación de XenApp y Secure Gateway.

Si se utiliza el modo Relay, el servidor Secure Gateway funciona como un proxy y es necesario configurar Citrix Receiver para Mac para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Secure Gateway.
- El número de puerto del servidor Secure Gateway. Tenga en cuenta que el modo Relay no recibe respaldo en la versión 2.0 de Secure Gateway.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo, mi_equipo.ejemplo.com es un nombre de dominio completo (FQDN), ya que contiene una secuencia de nombre de host (mi_equipo), dominio intermedio (ejemplo) y dominio superior (com). Por lo general, la combinación de nombre de dominio intermedio y dominio superior (`example.com`) se conoce como nombre de dominio.

Conexión a través de un servidor proxy

Los servidores proxy se usan para limitar el acceso hacia y desde una red, y para ocuparse de las conexiones entre Citrix Receiver para Mac y los servidores. Citrix Receiver para Mac admite los protocolos SOCKS y proxy seguro.

En la comunicación con el servidor XenApp o XenDesktop, Citrix Receiver para Mac utiliza los parámetros del servidor proxy configurados de forma remota en el servidor de la Interfaz Web. Para obtener más información sobre la configuración de los parámetros de servidores proxy para Receiver, consulte la documentación de la Interfaz Web.

En la comunicación con el servidor web, Citrix Receiver para Mac utiliza los parámetros del servidor proxy configurados para el explorador web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros del servidor proxy para el explorador web predeterminado en el dispositivo de usuario según corresponda.

Conexión a través de un firewall

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si se utiliza un firewall en el entorno, Citrix Receiver para Mac debe poder comunicarse a través del mismo con el servidor web y el servidor Citrix. El firewall debe permitir el tráfico HTTP para la comunicación entre el dispositivo de usuario y el servidor web (normalmente mediante un puerto HTTP 80 estándar o 443 si se usa un servidor web seguro). Para las

comunicaciones entre Receiver y el servidor Citrix, el firewall debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

Si el firewall se ha configurado para la traducción de direcciones de red (NAT), es posible usar la Interfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos. Por ejemplo, si el servidor XenApp o XenDesktop no se ha configurado con una dirección alternativa, es posible configurar la Interfaz Web para proporcionar una dirección alternativa a Citrix Receiver para Mac. A continuación, Citrix Receiver para Mac se conecta con el servidor mediante la dirección externa y el número de puerto. Para obtener más información, consulte la documentación de Interfaz Web.

Conexión mediante TLS

Citrix Receiver para Mac 12.3 respalda el uso de TLS 1.0, 1.1 y 1.2 con los siguientes conjuntos de cifrado para las conexiones TLS con XenApp/XenDesktop:

TLS:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

DTLS:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Nota:**
>
> Citrix Receiver para Mac ejecutado en Mac OS Sierra no respalda los siguientes conjuntos de cifrado TLS:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

Transport Layer Security (TLS) es la versión estándar más reciente del protocolo TLS. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de TLS como un estándar abierto.

TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Estas organizaciones pueden exigir también el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

Citrix Receiver para Mac respalda claves RSA de 1024, 2048 y 3072 bits. También se admiten certificados raíz con claves RSA de 4096 bits.

> **Nota**
>
> Citrix Receiver para Mac usa criptografía de plataforma (OS X) para las conexiones entre Citrix Receiver para Mac y StoreFront.

Configuración y habilitación de Citrix Receiver para Mac para TLS

La configuración de TLS consta de dos pasos:

1. Configure el Traspaso SSL en el servidor XenApp o XenDesktop y en el servidor de la Interfaz Web. Obtenga e instale el certificado de servidor necesario.
2. Instale el certificado raíz equivalente en el dispositivo de usuario.

Instalación de certificados raíz en los dispositivos de los usuarios

Si se desea usar TLS para proteger la seguridad de las comunicaciones entre las instancias de Citrix Receiver para Mac habilitadas con TLS y la comunidad de servidores, se necesita un certificado raíz en el dispositivo de usuario que pueda verificar la firma de la entidad de certificación en el certificado del servidor.

Mac OS X incluye aproximadamente 100 certificados raíz comerciales ya instalados, pero si desea utilizar otro certificado, puede obtenerlo de la entidad de certificación e instalarlo en cada dispositivo de usuario.

Según los procedimientos y las directivas de la empresa, se puede instalar el certificado raíz en cada dispositivo de usuario en lugar de solicitar a los usuarios que lo instalen. La opción más fácil y segura es agregar los certificados raíz a las llaves de Mac OS X.

Para agregar un certificado raíz a las llaves

1. Haga doble clic en el archivo que contiene el certificado. Esto inicia automáticamente la aplicación Acceso a llaves.
2. En el cuadro de diálogo Añadir certificados, elija una de las siguientes opciones en el menú emergente Llavero:

- Inicio de sesión (el certificado se aplica solamente al usuario actual).
- Sistema (el certificado se aplica a todos los usuarios de un dispositivo).

3. Haga clic en Aceptar.
4. Escriba su contraseña en el cuadro de diálogo Autenticar y haga clic en OK.

Se instalará el certificado raíz. Los clientes compatibles con TLS y todas las aplicaciones que utilicen TLS podrán usar el certificado raíz.

Acerca de las directivas de TLS

Esta sección proporciona información sobre cómo configurar directivas de seguridad para sesiones ICA sobre TLS en Citrix Receiver para Mac. Puede configurar ciertos parámetros de TLS utilizados para las conexiones ICA en Citrix Receiver para Mac. Estos parámetros no están expuestos en la interfaz del usuario; para cambiarlos hay que ejecutar un comando en el dispositivo donde se ejecuta Citrix Receiver para Mac.

> **Nota**
>
> Las directivas TLS se pueden administrar de otras maneras, por ejemplo, cuando los dispositivos están controlados por OS X Server o alguna otra solución de administración de dispositivos móviles.

Las directivas TLS incluyen los siguientes parámetros:

SecurityComplianceMode. Define el modo de conformidad de seguridad para la directiva. Si no se configura SecurityComplianceMode, se usa FIPS como valor predeterminado. Los valores aplicables para este parámetro son:

- **Nada**. No se impone ningún modo de conformidad
- **FIPS**. Se usan módulos criptográficos de FIPS
- **SP800-52**. Se imponen las normas de conformidad NIST SP800-52r1

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions. Este parámetro especifica las versiones del protocolo TLS que deben aceptarse durante la negociación de protocolos. Esta información está representada por una matriz y se respalda cualquier combinación de los valores posibles. Cuando este parámetro no está configurado, se usan los valores TLS10, TLS11 y TLS12 como valores predeterminados. Los valores aplicables para este parámetro son:

- **TLS10**. Especifica que se permite el protocolo TLS 1.0.
- **TLS11**. Especifica que se permite el protocolo TLS 1.1.
- **TLS12**. Especifica que se permite el protocolo TLS 1.2.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```


SSLCertificateRevocationCheckPolicy. Esta función mejora la autenticación criptográfica del servidor Citrix y mejora la seguridad global de las conexiones SSL/TLS entre clientes y servidores. Este parámetro controla cómo se trata una entidad de certificación raíz durante un intento de abrir una sesión remota a través de SSL cuando se usa el cliente para OS X.

Cuando se habilita este parámetro, el cliente comprueba si el certificado del servidor está revocado o no. Existen varios niveles de comprobación de la lista de revocación de certificados. Por ejemplo, se puede configurar el cliente para que verifique solo la lista local de certificados, o para que compruebe las listas de certificados locales y de red. Además, se puede configurar la comprobación de certificados para permitir que los usuarios inicien sesiones solo cuando se hayan comprobado todas las listas de revocación de certificados.

La comprobación de listas de revocación de certificados (listas CRL) es una funcionalidad avanzada respaldada por algunos emisores de certificados. Permite que un administrador revoque certificados de seguridad (no válidos después de su fecha de caducidad) en el caso de exista un riesgo criptográfico para la clave privada, o simplemente si ha habido un cambio inesperado en el nombre DNS.

Los valores aplicables para este parámetro son:

- **NoCheck**. No comprueba la lista de revocación de certificados.
- **CheckWithNoNetworkAccess**. Se hace una comprobación de listas de revocación de certificados. Solo se usan almacenes locales de listas de revocación de certificados. Se ignoran todos los puntos de distribución. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de Traspaso SSL/Secure Gateway de destino.
- **FullAccessCheck**. Se hace una comprobación de listas de revocación de certificados. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de Traspaso SSL/Secure Gateway de destino.
- **FullAccessCheckAndCRLRequired**. Se hace una comprobación de listas de revocación de certificados, excluyendo la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
- **FullAccessCheckAndCRLRequiredAll**. Se hace una comprobación de listas de revocación de certificados, incluida la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.

> **Nota**
>
> Si no se configura SSLCertificateRevocationCheckPolicy, el valor predeterminado que se usa es "FullAccessCheck".
>
> `defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy`


```
FullAccessCheckAndCRLRequired
```

Configuración de directivas TLS

Para configurar los parámetros de TLS en un equipo no administrado, ejecute el comando **defaults** en Terminal.app.

defaults es una aplicación de línea de comandos que se puede usar para agregar, modificar y eliminar parámetros de aplicación en un archivo plist de preferencias de OS X.

Para cambiar parámetros:

1. Abra Aplicaciones > Utilidades > Terminal.
2. En Terminal, ejecute el comando:

```
defaults write com.citrix.receiver.nomas \<name\> \<type\> \<value\>
```

Dónde:

<name>: El nombre del parámetro según se describe arriba.

<type>: Un conmutador que identifica el tipo de parámetro. Puede ser -string o -array. Si el parámetro es de tipo “string” (cadena), el conmutador se puede omitir.

<value>: El valor del parámetro. Si el valor es una matriz (array) y se están especificando varios valores, éstos deben ir separados por espacios.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```

Volver a la configuración predeterminada

Para restablecer un parámetro con su valor predeterminado:

1. Abra Aplicaciones > Utilidades > Terminal.
2. En Terminal, ejecute el comando:

```
defaults delete com.citrix.receiver.nomas \<name\>
```

Dónde:

<name>: El nombre del parámetro según se describe arriba.

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```


Uso de la interfaz de usuario para configurar las opciones de seguridad

En la versión 12.3 de Citrix Receiver para Mac, se han introducido numerosas mejoras, que incluyen lo siguiente:

- interfaz de usuario de configuración de seguridad mejorada. En versiones anteriores, la línea de comandos era el método recomendado para hacer cambios en los parámetros de seguridad; ahora los parámetros para configurar la seguridad son más sencillos y accesibles desde la interfaz de usuario, lo que mejora la experiencia del usuario creando un método sencillo para la definición de preferencias relacionadas con la seguridad.
- ver conexiones TLS. Citrix Receiver para Mac le permite verificar conexiones hechas con servidores que usan una versión específica de TLS, con información adicional que incluye el algoritmo de cifrado utilizado para la conexión, el modo, el tamaño de la clave y si SecureICA está habilitado. Además, puede ver el certificado del servidor para las conexiones TLS.

La pantalla mejorada de **Seguridad y privacidad** ofrece las siguientes opciones nuevas en la ficha **TLS**:

- Definir el modo de conformidad
- Configurar el módulo de criptografía
- Seleccionar la versión de TLS adecuada
- Seleccionar la lista de revocación de certificados
- habilitar parámetros para todas las conexiones TLS

En la imagen siguiente, aparecen las opciones de la pantalla Seguridad y privacidad a las que se puede acceder desde la interfaz de usuario:

Requisitos de la autenticación con tarjeta inteligente

October 9, 2019

Citrix Receiver para Mac respalda la autenticación con tarjeta inteligente en las configuraciones siguientes:

- La autenticación con tarjeta inteligente en Receiver para Web/StoreFront 2.x y versiones posteriores, y XenDesktop 7.1 y versiones posteriores o XenApp 6.5 y versiones posteriores.
- Las aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, permiten a los usuarios firmar o cifrar digitalmente los documentos disponibles en las sesiones de aplicación o escritorio virtual.
- Con varios certificados: Citrix Receiver para Mac da respaldo a múltiples certificados con una única tarjeta inteligente o con varias de ellas. Cuando el usuario introduce una tarjeta

inteligente en el lector de tarjetas, los certificados están disponibles para todas las aplicaciones ejecutadas en el dispositivo, incluido Citrix Receiver para Mac.

- En sesiones de doble salto: Si es necesario el doble salto, se establece una conexión adicional entre Citrix Receiver para Mac y el escritorio virtual del usuario.

Acerca de la autenticación con tarjeta inteligente en NetScaler

Cuando se usa una tarjeta inteligente para autenticar una conexión y hay varios certificados que se pueden utilizar en la tarjeta inteligente, Citrix Receiver para Mac pide al usuario que seleccione uno. Después de seleccionar uno, Citrix Receiver para Mac solicita la introducción de la contraseña de la tarjeta inteligente; una vez realizada la autenticación, la sesión se inicia.

Si solo hay un certificado adecuado en la tarjeta inteligente, Citrix Receiver para Mac usa ese certificado y no pide seleccionarlo. No obstante, aún hay que introducir la contraseña asociada con la tarjeta inteligente para autenticar la conexión y que se inicie la sesión.

Especificación de un módulo PKCS#11 para la autenticación con tarjeta inteligente

> **Nota:**
>
> La instalación del módulo PKCS#11 no es obligatoria. Esta sección se aplica solo a las sesiones ICA. No se aplica el acceso de Citrix Receiver a NetScaler Gateway o StoreFront donde se necesita una tarjeta inteligente.

Para especificar un módulo PKCS#11 para la autenticación con tarjeta inteligente:

1. Seleccione **Preferencias** en Citrix Receiver.
2. Haga clic en **Seguridad y privacidad**.
3. En la sección **Seguridad y privacidad**, haga clic en **Tarjeta inteligente**.
4. En el campo **PKCS#11**, seleccione el módulo apropiado; haga clic en **Otros** para buscar la ubicación del módulo PKCS#11 si el módulo que quiere usar no aparece en la lista.
5. Después de seleccionar el módulo apropiado, haga clic en **Agregar**.

Perfiles de tarjeta inteligente, middleware y lectores respaldados

Citrix Receiver para Mac respalda la mayoría de los lectores de tarjeta inteligente y middleware criptográfico compatibles con macOS. Citrix ha comprobado y validado el funcionamiento con lo siguiente.

Lectores admitidos:

- Lectores de tarjeta inteligente de conexión USB comunes

Middleware respaldado:

- Clariify
- Versión cliente de Activeidentity
- Versión cliente de Charismathics

Tarjetas inteligentes compatibles:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)
- Tarjetas Gemalto .NET

Siga las instrucciones del proveedor del middleware criptográfico y lector de tarjeta inteligente compatibles con macOS para configurar los dispositivos de usuario.

Restricciones

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- Citrix Receiver para Mac no guarda la selección de certificado de usuario.
- Citrix Receiver para Mac no guarda ni almacena el PIN de la tarjeta inteligente del usuario. Las adquisiciones del PIN son gestionadas por el sistema operativo, que puede tener su propio mecanismo de caché.
- Citrix Receiver para Mac no reconecta sesiones cuando se introduce una tarjeta inteligente.
- Para usar túneles VPN con autenticación con tarjeta inteligente, los usuarios deben instalar el NetScaler Gateway Plug-in e iniciar una sesión a través de una página web, mediante sus tarjetas inteligentes y números PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con NetScaler Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.

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