Acerca de esta versión

Jun 22, 2016

Citrix Receiver para Mac ofrece a los usuarios acceso de autoservicio a recursos publicados en servidores XenApp y XenDesktop. Receiver es fácil de instalar y de usar y ofrece un acceso rápido y seguro a aplicaciones y escritorios virtuales alojados en servidores.

Puede descargar la versión más reciente desde la página de descarga de Citrix Receiver para Mac.

Novedades en la versión 12.1

Autenticación con tarjeta inteligente en NetScaler Gateway

Esta funcionalidad permite a Citrix Receiver acceder a aplicaciones y escritorios a través de NetScaler Gateway usando la autenticación con tarjeta inteligente. Consulte los Requisitos de la autenticación con tarjeta inteligente para obtener información sobre esta funcionalidad.

Respaldo de El Capitan para la división de pantalla

En la versión anterior de Citrix Receiver para Mac (12.0) se introdujo el respaldo para OS X El Capitan. En esta versión, incluimos respaldo completo para la función de división de pantalla de El Capitan.

Mejoras de fiabilidad de sesión y reconexión automática de clientes

Estas mejoras permiten una mayor interoperabilidad con CloudBridge y NetScaler Gateway. Una sesión se puede reconectar usando la reconexión automática de clientes y la fiabilidad de la sesión independientemente de la ruta de la conexión. Las mejoras específicas de esta versión son las siguientes:

Mensajes de conexión mejorados que notifican a los usuarios sobre el estado de sus conexiones, les informan cuando pierden la conexión, y les indican qué hacer a continuación.

Un contador de tiempo (en minutos y segundos) ahora indica cuanto tiempo queda antes de que se exceda el tiempo de espera de la sesión. La sesión finaliza cuando termina la cuenta atrás del contador. De forma predeterminada, el valor de tiempo de espera está establecido en 2 minutos. Puede cambiar el valor predeterminado en el parámetro **TransportReconnectMaxRetrySeconds** del archivo ICA.

> ### Nota
>
> Esta función ofrece respaldo para un parámetro adicional de administración de sesiones de XenApp and XenDesktop,**TransportReconnectRetryMaxTimeSeconds**.
>
> **TransportReconnectDelay** y **TransportReconnectRetries** ya no se utilizan. Para obtener más información, consulte Administración de sesiones.

Características introducidas en la versión 12.0

Cuando se usa conjuntamente con las capacidades de personalización centralizada y configuración de marcas que tiene StoreFront 3.0, los usuarios de esta versión de Receiver para Mac recibirán una experiencia de selección de aplicaciones y escritorios administrada de manera centralizada desde StoreFront. Se trata de la misma experiencia de usuario uniforme

que se puede obtener con el Receiver de escritorio de Windows y los Receivers para Web de HTML5 y Chrome cuando se los asocia con StoreFront 3.0.

Respaldo para OS X El Capitan (10.11).

Respaldo para cookies de sesión: Citrix Receiver para Mac 12.0 respalda las cookies de sesión Web para poder usar la nueva API Web requerida en StoreFront 3.0 y para dar respaldo al equilibrio de carga.

Mejoras de zona horaria: Citrix Receiver para Mac 12.0 detecta con mayor precisión las zonas horarias locales y de ciudad cuando se lo usa con la redirección de zonas horarias de XenApp. Para obtener más información, consulte: Configuraciones de directiva de Control de zona horaria.

Problemas resueltos en Citrix Receiver para Mac 12

Mar 01, 2016

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 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 resueltos en Citrix Receiver para Mac 12.1

- Se ha solucionado un problema por el cual si se está usando el respaldo de VPN integrado 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 12.1.100

- 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 conexiones IPV6 con NetScaler Gateway fallaban. [LC4512]
- 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 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 al intentar introducir un carácter en japonés o en chino simplificado no se mostraba ningún carácter en el escritorio de la sesión. [603635]

Problemas conocidos en Citrix Receiver para Mac 12

Jul 07, 2016

Problemas conocidos en Citrix Receiver para Mac 12

Se han observado los siguientes problemas conocidos en esta versión:

- En OS X El Capitan (10.11), los escritorios y aplicaciones virtuales no se muestran normalmente en el modo Split View. [#582397]
- La sesión de XenDesktop no se inicia cuando se usa autenticación con tarjeta inteligente. [#550781]
- Cuando se usa una tarjeta inteligente PIV, Receiver no se reconecta a una sesión de XenDesktop 5.6. [#550986]
- 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]
- 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]
- 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 OS X Mountain Lion (10.8) y se actualiza Receiver 11.9 o 11.9.15 a Receiver 12.0, al iniciar Receiver puede que se abran dos versiones de Receiver, la nueva versión y la versión 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 en 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]
- 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]
- Al cambiar la vista a pantalla completa mientras hay una aplicación DirectX o OpenGL ejecutándose, puede ocurrir que el cursor desaparezca. [#510745]
- 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]
- En una configuración con varios monitores, las aplicaciones integradas pueden moverse a la pantalla principal cuando se reconfigura cualquiera de las pantallas. [#506532]
- 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]
- 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.

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]
- Viewer 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]

Requisitos del sistema de Receiver 12.0 para Mac

Nov 03, 2016

Sistemas operativos respaldados para Citrix Receiver para Mac 12.0

- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)
- OS X Mountain Lion (10.8)

Las versiones de OS X anteriores a Mountain Lion no reciben respaldo.

Si necesita usar una versión de Citrix Receiver para Mac OS X Lion (10.7) o anterior, consulte Citrix Receiver para Mac 11.9.x.

Requisitos de hardware

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

Servidores respaldados

- XenApp (cualquiera de los productos siguientes):
  - Citrix XenApp 7.6 para Windows Server 2012 R2
  - Citrix XenApp 7,5 para Windows Server 2012 R2
  - Citrix XenApp 6.5 para Windows Server 2008 R2
- XenDesktop (cualquiera de los productos siguientes):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
- Citrix VDI-in-a-Box 5.4 y 5.3
- StoreFront:
  - StoreFront 3.0
  - StoreFront 2.6
  - StoreFront 2.5
  - StoreFront 2.1
- Interfaz Web:
  - Interfaz Web 5.4 para Windows con sitios de servicios XenApp, (también conocidos como servicios PNAgent), para acceder a aplicaciones desde Receiver en lugar de hacerlo desde un explorador Web.
- Para implementar Receiver:
  - Citrix Receiver para Web 2.1, 2.5 y 2.6
  - Interfaz Web de Citrix 5.4

Exploradores Web compatibles

- Safari 6.0 o posterior
- Mozilla Firefox 22.x o posterior
- Google Chrome 28.x o posterior

Conectividad

Si los usuarios ejecutan Citrix Receiver para Mac 12 en el sistema operativo OS X El Capitan y tienen problemas para conectar, es posible que necesiten actualizar el plugin de NetScaler Gateway. Para obtener más información, consulte este artículo de la página de descargas de Citrix: NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support).

Citrix Receiver para Mac admite conexiones HTTP, HTTPS e ICA sobre TLS con XenApp o XenDesktop mediante cualquiera de las siguientes configuraciones.

Para conexiones LAN:

- StoreFront con sitios de Receiver para Web o de servicios StoreFront
- Interfaz Web 5.4 para Windows, mediante los sitios de servicios XenApp

Para conexiones locales o remotas seguras:

- Citrix NetScaler Gateway 11.0 incluido VPX
- Citrix NetScaler Gateway 10.5 incluido VPX
- Citrix NetScaler Gateway 10.1 incluido VPX
- Citrix Access Gateway Enterprise Edition 10.x incluido VPX
- Citrix Access Gateway Enterprise Edition 9.x incluido VPX
- Citrix Access Gateway VPX
- Citrix Secure Gateway 3.x (solo para usarlo con la Interfaz Web)

Para obtener más información sobre cómo implementar Access Gateway o NetScaler Gateway con StoreFront, consulte la documentación de Access Gateway o NetScaler Gateway y la documentación de StoreFront.

Autenticación

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

	Receiver para Web usando exploradores Web	**Sitio de servicios StoreFront (nativo)**	**Sitio de servicios XenApp de StoreFront (nativo)**	**NetScaler a Receiver parar Web (explorador Web)**	**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 Tarjeta inteligente**	**Receiver para Web usando exploradores Web** Sí Sí	**Sitio de servicios StoreFront (nativo)**	**Sitio de servicios XenApp de StoreFront (nativo)**	Sí* **NetScaler a Receiver parar Web (explorador Web)** Sí* Sí*	Sí* **NetScaler a sitio de servicios StoreFront (nativo)** Sí* Sí*
Certificado de usuario				Sí (NetScaler Gateway Plugin)	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 usar tarjetas inteligentes en OS X 10.10, debe tener instalado OS X 10.10.2 o una versión posterior.

Para conexiones con la Interfaz Web 5.4, Receiver 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			
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 (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.

**La tarjeta inteligente no recibe respaldo en OS X 10.10 debido a que Apple ha cambiado sus condiciones de respaldo para tarjetas inteligentes.

Para obtener información sobre la autenticación, consulte la documentación respectiva de NetScaler Gateway, Access

Gateway y StoreFront en la Documentación de productos Citrix. Para obtener información sobre otros métodos de autenticación admitidos en la Interfaz Web, consulte Configuración de la autenticación para la Interfaz Web en la documentación de la Interfaz Web, en la Documentación de productos Citrix.

Requisitos de la autenticación con tarjeta inteligente

Nov 13, 2015

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 XenDesktop 5.6 y versiones posteriores, o XenApp 6.5 y versiones posteriores usando acceso basado en explorador Web.
- 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: Receiver para Mac da respaldo al uso de 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.
- En sesiones de doble salto: Si es necesario el doble salto, se establece una conexión adicional entre Receiver y el escritorio virtual del usuario.

  Las implementaciones que respaldan el doble salto se describen en la documentación de XenApp y XenDesktop. Para obtener más información, consulte Implementaciones con tarjeta inteligente.

Acerca de la autenticación con tarjeta inteligente en NetScaler

Cuando se usa una tarjeta inteligente para autenticar una conexión y hay varios certificables utilizables en la tarjeta inteligente, Citrix Receiver pide al usuario que seleccione uno. Después de seleccionar uno, Citrix Receiver 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 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

Mediante las opciones avanzadas de configuración en la ventana de Preferencias de Citrix Receiver, se puede especificar el módulo PKCS#11 para la autenticación:

1. Seleccione **Preferencias** en Citrix Receiver.
2. En la ventana de Preferencias, haga clic en **Avanzadas**.
3. 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.
4. Después de seleccionar el módulo apropiado, haga clic en **Agregar**.

Perfiles de tarjeta inteligente, middleware y lectores respaldados

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

Lectores compatibles:

- Lectores de tarjeta inteligente de conexión USB comunes

Middleware respaldado:

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

Tarjetas inteligentes respaldadas:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

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

Restrictions

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- Receiver para Mac no guarda la selección de certificado de usuario.
- 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.
- 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, usando 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.

Para obtener más información

Consulte:

- Configuración de Citrix XenDesktop 7.6 y NetScaler Gateway 10.5 con autenticación por tarjeta inteligente de PIV (PDF)
- Respaldo para tarjeta inteligente con Citrix Receiver para Mac 11.9.15 en OS X 10.10.2

Instalación, configuración, actualización, implementación y eliminación de Receiver para Mac

Nov 03, 2016

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, Access Gateway y Secure Gateway.

En este artículo:

Instalación

Receiver se puede instalar de varias formas:

- Desde Citrix.com (instalación de usuario)
  - Un usuario que utiliza Receiver por primera vez y obtiene Receiver 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. Receiver 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 característica se conoce como detección de cuentas basada en correo electrónico.
    Nota: Un usuario nuevo es un usuario que no tiene Receiver instalado en su dispositivo.
  - La detección de cuentas basada en correo electrónico para un usuario nuevo no se aplica cuando Receiver 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 Receiver 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 Receiver por primera vez debe introducir una dirección URL de servidor para configurar una cuenta.

Instalación manual de Receiver para Mac

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

Para instalar Receiver para Mac

1. Descargue el archivo .dmg para la versión de Receiver que desea instalar del sitio Web de Citrix y abra ese archivo.
2. En la página 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 a Receiver 12.0 para Mac

Se respalda la actualización desde las versiones 10.x y 11.x del Online Plug-in para Mac. También es posible realizar la actualización desde las versiones 11.3, 11.4, 11.5, 11.6,11.7.x, 11.8.x, 11.9.x de Receiver para Mac.

La integración con ShareFile se ha quitado a partir de la versión 11.8. Si integró 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 Receiver para Mac

Para implementaciones con StoreFront:

- Se recomienda configurar NetScaler Gateway y StoreFront 2.x según se describe en la documentación de esos productos en Citrix. 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 Receiver.
- 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 Receiver, 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 11.9, e indique a los usuarios cómo deben realizar la actualización de Receiver. 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 Receiver.

Distribución de Receiver desde Receiver para Web

Es posible distribuir Receiver 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 Receiver compatible, le solicita al usuario que descargue e instale Receiver. Para obtener más información, consulte la documentación de StoreFront.

Implementación de Receiver desde una pantalla de inicio de sesión de la Interfaz Web

Es posible distribuir Receiver 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 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.

Como opción alternativa, puede presentar mensajes de instalación a los usuarios; estos son enlaces que los usuarios ven en

su pantalla Mensajes. Los usuarios hacen clic en el enlace para iniciar el proceso de detección e instalación de clientes. También puede usar mensajes de instalación para permitir a los usuarios acceder al proceso de detección e instalación de clientes para actualizar sus clientes de Citrix con nuevas versiones de los mismos.

Para utilizar el proceso de detección e instalación de clientes, los archivos de instalación de Receiver deben estar disponibles en el servidor de la Interfaz Web. De forma predeterminada, la Interfaz Web asume que los nombres de los archivos de instalación de Receiver son los mismos que los de los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si desea descargar Receiver desde el sitio Web de Citrix o si planea distribuir versiones anteriores de Receiver, verifique que se especifiquen los nombres de los archivos de instalación de Receiver correctos para el parámetro ClientIcaMac en los archivos de configuración de los sitios Web XenApp.

Para obtener más información, consulte la documentación de la Interfaz Web.

Para quitar Receiver para Mac

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

Configuración de Receiver para Mac

Nov 13, 2015

Una vez instalado el software de Receiver, los usuarios pueden realizar los siguientes pasos de configuración para acceder a sus aplicaciones y escritorios alojados:

- Configure el entorno XenApp: Asegúrese de que el entorno XenApp está configurado correctamente. Familiarícese con las opciones y ofrezca descripciones de las aplicaciones útiles para sus usuarios.
- Configure el modo de autoservicio: Configure el modo de autoservicio, que permite a los usuarios suscribirse a aplicaciones desde la interfaz de usuario de Receiver.
- Configure StoreFront: Cree almacenes que enumeren y agrupen escritorios y aplicaciones desde sitios de XenDesktop y comunidades XenApp, habilitando estos recursos para los usuarios.
- Suministre a los usuarios la información de cuentas: Dé a los usuarios la información que necesitan para configurar su acceso a las cuentas que alojan sus aplicaciones y escritorios. En algunos entornos, los usuarios deben configurar manualmente el acceso a las cuentas.
- 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. Para obtener más información, consulte NetScaler Gateway.

Configuración de 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, 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 Receiver o configurando Receiver 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 o tienda 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 Receiver Tech Preview. Para obtener más información sobre la experiencia de usuario de Receiver Tech Preview, consulte Receiver y StoreFront 3.0 Technology 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.

Configuración del modo de autoservicio

Simplemente agregando una cuenta de StoreFront a Receiver o configurando Receiver para que apunte a un sitio de StoreFront, puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de Receiver. Esta experiencia de usuario mejorada es similar al uso de un almacén o tienda de aplicaciones móviles.

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

- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS:Auto a la descripción, cuando publique una 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 Receiver, 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 la Interfaz Web.

Configuración de StoreFront

Con StoreFront, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para Citrix Receiver. Cree almacenes que enumeren y agrupen escritorios y aplicaciones de sitios de XenDesktop y comunidades XenApp, habilitando 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 proporciona una plantilla que se puede usar para crear un sitio de descargas de Receiver.
2. Configure almacenes para CloudGateway de la misma forma que con otras aplicaciones de XenApp y XenDesktop. No se requiere una configuración especial para Receiver. 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:

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

Configuración de la detección de cuentas basada en direcciones de correo electrónico

Puede configurar Receiver 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 Receiver. Receiver determina el dispositivo NetScaler Gateway, Access Gateway o 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 o Access Gateway de modo que acepte conexiones de usuario mediante una dirección de correo electrónico para detectar la dirección URL de StoreFront, NetScaler Gateway o Access Gateway, consulte *— Conexión a StoreFront mediante detección basada en correo electrónico* en la documentación de NetScaler Gateway o Access 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 Receiver. Si se configuran sitios de Receiver para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de Receiver 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 Receiver, 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.

Entrega de la información de cuenta para introducirla 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:

- Dirección URL del almacén de StoreFront o del sitio de servicios XenApp donde se alojan los recursos. Por ejemplo: https://nombre-del-servidor.ejemplo.com
- Para acceso mediante NetScaler Gateway o Access Gateway: la dirección, edición del producto y método de autenticación requerido para NetScaler Gateway o Access Gateway.
  Para obtener más información sobre cómo configurar NetScaler Gateway o Access Gateway, consulte la documentación de NetScaler Gateway o de Access Gateway.

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

Optimización del entorno de Receiver para Mac

Nov 13, 2015

Es posible optimizar el entorno y obtener el mejor rendimiento de Receiver haciendo lo siguiente:

- Reconectar usuarios automáticamente
- Cómo ofrecer fiabilidad de la sesión mediante HDX Broadcast
- Continuidad para los usuarios con perfil móvil
- Asignar dispositivos cliente

Reconectar usuarios

Reconectar usuarios automáticamente

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 de reconexión automática de clientes de HDX Broadcast, Receiver puede detectar desconexiones accidentales de las sesiones ICA y volver a conectar automáticamente 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. Receiver 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 de HDX Broadcast 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 característica 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, Receiver apaga el escritorio y vuelve a iniciarlo.

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

Cómo ofrecer fiabilidad de la sesión mediante HDX Broadcast

Con la función de fiabilidad de la sesión de HDX Broadcast, los usuarios continúan 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 de HDX Broadcast se configura mediante los parámetros de directiva en el servidor. Para obtener más información, consulte la documentación de XenDesktop y de XenApp.

Los usuarios de Receiver no pueden sobrescribir los parámetros del servidor para fiabilidad de sesión de HDX Broadcast.

Importante: Si la función de fiabilidad de sesión HDX Broadcast está habilitada, el puerto predeterminado que se utiliza 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 Receiver 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

Receiver 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

Tenga en cuenta que la asignación de sonido del cliente y la asignación de impresoras del cliente no necesitan 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.

Receiver 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 Receiver.

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

1. En la página de inicio de Receiver, 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.

Asignación de puertos COM del cliente

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones. Estas asignaciones se pueden usar como cualquier otra asignación de red.

Los puertos serie de Macintosh no ofrecen todas las líneas de señal de control que se utilizan en las aplicaciones de Windows. No se proporcionan las líneas DSR (Conjunto de datos preparado), DCD (Detección de operador de dispositivo), RI (Indicador de llamada) ni RTS (Solicitud de envío). Es posible que las aplicaciones de Windows que se basan en estas señales para el protocolo de enlace con el hardware y el control de flujo no funcionen. La implementación Macintosh de la comunicación por puertos serie se basa solo en líneas CTS (Listo para envío) y DTR (Terminal de datos preparado) para los protocolos de enlace de entrada y salida con el hardware.

Para asignar puertos COM del cliente

1. En la página de inicio de Receiver, haga clic en el icono con la flecha hacia abajo y seleccione Preferencias
2. Haga clic en Dispositivos.
3. Seleccione el puerto COM que desea asignar en la lista Puertos COM asignados. Este es el puerto COM virtual que se muestra en la sesión, no el puerto físico en el equipo local.
4. Seleccione el dispositivo para asociarlo con el puerto COM virtual en el menú emergente Dispositivo.
5. Inicie Receiver e inicie sesión en un servidor.
6. Ejecute un símbolo del sistema. En el símbolo del sistema, escriba
   net use comx: \\client\comz:

   donde x es el número del puerto COM del servidor (los puertos del 1 al 9 están disponibles para la asignación) y z es el número del puerto COM del cliente (los puertos del 1 al 4 están disponibles).

7. Para confirmar la operación, escriba:net use en el símbolo del sistema. Verá una lista de las unidades, los puertos LPT y los puertos COM asignados.

Mejora de la experiencia de usuario en Receiver para Mac

Nov 13, 2015

Es posible mejorar la experiencia de los usuarios a través de las siguientes funciones compatibles:

- Suavizado de fuentes ClearType
- Entrada de micrófono en el cliente
- Teclas especiales de Windows
- Accesos directos y combinaciones de teclas de Windows
- Uso de editores IME y distribuciones de teclado internacionales
- Uso de varios monitores
- Uso de la barra de herramientas del escritorio

Suavizado de fuentes ClearType

El suavizado de fuentes ClearType (también conocido como presentación de fuentes de subpixel) 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 Receiver.

Receiver detecta automáticamente la configuración de suavizado de fuentes de los dispositivos de usuario y la envía al servidor. La sesión se conecta usando 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

Receiver 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.

Receiver brinda respaldo para dictado digital. Para obtener información sobre la configuración de esta función, consulte la documentación de XenApp y XenDesktop.

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 Receiver:

- Usar mi micrófono y cámara Web
- No usar mi micrófono ni 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

Receiver 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 usando” permite seleccionar si se desean 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 usando” 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 usando 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**
INSERT	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
SUPRIMIR	Punto decimal en el teclado numérico. La tecla Bloq num debe estar desactivada; es posible activarla y desactivarla mediante la tecla Borrar. 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, Receiver 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 Receiver 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)

Tecla o combinación de teclas de Windows	Equivalentes de Mac
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
Ctrl+Alt+Supr	Control-Opción-Suprimir Control-Opción-Fn-Eliminar (en teclados MacBook) Seleccione Teclado > Enviar Ctrl-Alt-Supr
Eliminar	Eliminar Seleccione Teclado > Enviar tecla > Eliminar Fn-Retroceso (Fn-Eliminar en algunos teclados para Estados Unidos)
Fin	Fin 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	Inicio Fn-Flecha izquierda
Insert (insertar)	Seleccione Teclado > Enviar tecla > Insertar
Bloq num	Borrar
Av Pág	Av Pág Fn-Tecla abajo

Re Pág **Tecla o combinación de teclas de Windows**	Re Pág **Equivalentes de Mac** Fn-Tecla arriba
Barra espaciadora	Seleccione Teclado > Enviar tecla > Espacio
Fichas	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

Receiver 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.

Receiver también permite que los usuarios especifiquen la distribución del teclado que desean utilizar.

Para habilitar el editor IME en el cliente

1. En la barra de menú 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 menú 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

Receiver 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 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 usando los comandos siguientes:
  - Cmd-Tab para cambiar a la aplicación activa anterior.
  - Ctrl-Flecha izquierda para cambiar al espacio anterior.
  - Usando 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.  o 
  - En OS X 10.7, 10.8 y 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.

Protección de las comunicaciones de Receiver

Mar 08, 2016

En este artículo:

Para proteger la comunicación entre la comunidad de servidores y Receiver, se pueden integrar las conexiones de Citrix Receiver a la comunidad de servidores con diversas tecnologías de seguridad, que incluyen:

- Citrix NetScaler Gateway o Citrix Access Gateway. Para obtener más información sobre cómo configurar estos elementos con Citrix StoreFront, consulte la documentación de StoreFront.
  Nota: Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores 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 respalda protocolos de proxy seguro y SOCKS.
- 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 Receiver 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 las direcciones externas.

Acerca de los certificados

Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, el certificado raíz de la entidad de certificación de la organización debe estar instalado en el dispositivo de usuario para poder acceder correctamente a los recursos de Citrix mediante Receiver.

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. Receiver para Mac admite certificados comodín.

Certificados intermedios con Access Gateway o NetScaler Gateway

Si la cadena de certificados incluye un certificado intermedio, es necesario asignar ese certificado al certificado del servidor Access Gateway o NetScaler Gateway. Para obtener información sobre esta tarea, consulte la documentación de NetScaler Gateway. Para obtener información equivalente con respecto a Access Gateway, consulte el artículo de Knowledge Base que coincida con su edición de ese producto:

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition (disponible solo en inglés)

Conexión con NetScaler Gateway o Access Gateway Enterprise Edition

Para permitir que los usuarios remotos se conecten a la implementación de CloudGateway mediante NetScaler Gateway o Access Gateway, puede configurar esos elementos para que funcionen con StoreFront (componente de CloudGateway). El método que se debe utilizar para habilitar el acceso depende de la edición de CloudGateway en la implementación.

Si implementa CloudGateway Express en su red, permita las conexiones de usuarios internos o remotos con StoreFront a través de NetScaler Gateway o Access Gateway integrando NetScaler Gateway o Access Gateway con StoreFront. 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.

Para obtener información sobre la configuración de estas conexiones con NetScaler Gateway, consulte el tema Configuring NetScaler Gateway Settings with the Remote Access Wizard. Para obtener información sobre la configuración de estas conexiones con Access Gateway, consulte el tema Integrating Access Gateway with CloudGateway.

Para permitir que los usuarios remotos se conecten mediante Access Gateway a la implementación de la Interfaz Web, configure Access Gateway para que funcione con la Interfaz Web, como se describe en la sección Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface y demás temas de esa sección.

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 Receiver y el servidor. No se necesita ninguna configuración de Receiver si se utiliza Secure Gateway en el modo Normal y los usuarios se conectan a través de la Interfaz Web.

Receiver 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 Receiver, 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 Relay. Para obtener más información sobre el modo de traspaso, consulte la documentación de XenApp (Secure Gateway).

Si se utiliza el modo Relay, el servidor Secure Gateway funciona como un proxy y es necesario configurar Receiver 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 (ejemplo.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 la red, y para administrar conexiones entre Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.

En la comunicación con el servidor XenApp o XenDesktop, Receiver 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, Receiver 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 servidor de seguridad en el entorno, Receiver debe poder comunicarse a través del servidor de seguridad con el servidor Web y el servidor Citrix. El servidor de seguridad 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 servidor de seguridad debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

Si el servidor de seguridad 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 Receiver. A continuación, Receiver se conecta con el servidor mediante la dirección externa y el número de puerto. Para obtener más información, consulte la documentación de la Interfaz Web.

Conexión con el Traspaso SSL (Secure Sockets Layer Relay)

Puede integrar el servicio de Traspaso SSL (Secure Sockets Layer) con Receiver para Mac 12.0, que da respaldo a TLS 1.0, 1.1 y 1.2 con los siguientes conjuntos de cifrado para conexiones TLS entre Citrix Receiver y XenApp/XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Transport Layer Security (TLS) es la versión estándar más reciente del protocolo SSL. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de SSL 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 las comunicaciones de datos seguras. Estas organizaciones pueden exigir también el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor Citrix para las comunicaciones protegidas con SSL/TLS. Cuando el Traspaso SSL recibe una conexión TLS, descifra los datos antes de redirigirlos al servidor o a Citrix XML Service (si el usuario ha seleccionado la exploración TLS+HTTPS).

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

- Entre una instancia de Receiver habilitada para usar TLS y un servidor.
- Con un servidor que ejecuta la Interfaz Web, entre el equipo que ejecuta el servidor XenApp y el servidor Web.

Para obtener información sobre la configuración y el uso del Traspaso SSL para proteger la instalación, o sobre la configuración del servidor de la Interfaz Web para utilizar el cifrado TLS, consulte la documentación de XenApp y la Interfaz Web.

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

Configuración y habilitación de Receiver 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. Para obtener más información, consulte la documentación de XenApp y la Interfaz Web.
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 Receiver 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 OK.
4. Escriba su contraseña en el cuadro de diálogo Autenticar y haga clic en OK.

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

Acerca de las directivas de SSL

Esta sección proporciona información sobre cómo configurar directivas de seguridad para sesiones ICA sobre SSL en Citrix Receiver para Mac versión 12.0. Puede configurar ciertos parámetros de SSL utilizados para las conexiones ICA en Citrix Receiver. Estos parámetros no están expuestos en la interfaz del usuario; para cambiarlos hay que ejecutar un comando en el dispositivo que ejecuta Receiver.

> ### Nota
>
> Las directivas SSL pueden administrarse 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 SSL incluyen las siguientes:

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:

- **None**. 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

Configuración de SecurityComplianceMode con el valor SP800-52: COPIAR

```
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.

Configuración de SecurityAllowedTLSVersions con los valores TLS 1.1 y TLS 1.2: COPIAR

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

SSLCertificateRevocationCheckPolicy. Esta característica mejora la authentication 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 sólo 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".

Configuración de SSLCertificateRevocationCheckPolicy con el valor FullAccessCheckAndCRLRequired: COPIAR

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

Configuración de directivas de SSL

Para configurar los parámetros de SSL 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

Donde:

: El nombre del parámetro según se describe arriba.

: 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.

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

Por ejemplo: COPIAR

```
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

Donde:

: El nombre del parámetro según se describe arriba.

Por ejemplo: COPIAR

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