Acerca de esta versión

Mar 08, 2016

Citrix Receiver para Windows ofrece a los usuarios un acceso seguro y de autoservicio a aplicaciones y escritorios virtuales suministrados por XenDesktop y XenApp.

Novedades de esta versión

Integración mejorada de RealTime Media Engine (RTME)

Esta versión introduce mejoras en el paradigma de instalación de Citrix Receiver para Windows al incorporar RTME en un único paquete de descarga e instalación. Anteriormente, los usuarios necesitaban instalar Citrix Receiver, y después ejecutar un paquete MSI de instalación aparte para integrar la funcionalidad de RTME en Receiver.

La experiencia del usuario era peor e impedía la adopción generalizada del HDX RealTime Optimization Pack en algunas organizaciones; los usuarios BYOD (Bring Your Own Device) tenían que instalar primero Citrix Receiver y luego volver a la página de descargas de Citrix para invocar otro instalador aparte para HDX RTME. Ahora hay un instalador único que combina la versión más reciente de Citrix Receiver para Windows con el instalador de HDX RTME.

Consulte el artículo de instalación para obtener información sobre cómo usar el instalador más reciente de Citrix Receiver con HDX RTME en un único archivo ejecutable.

Definición del nivel de transparencia usando la directiva de grupo de fiabilidad de la sesión

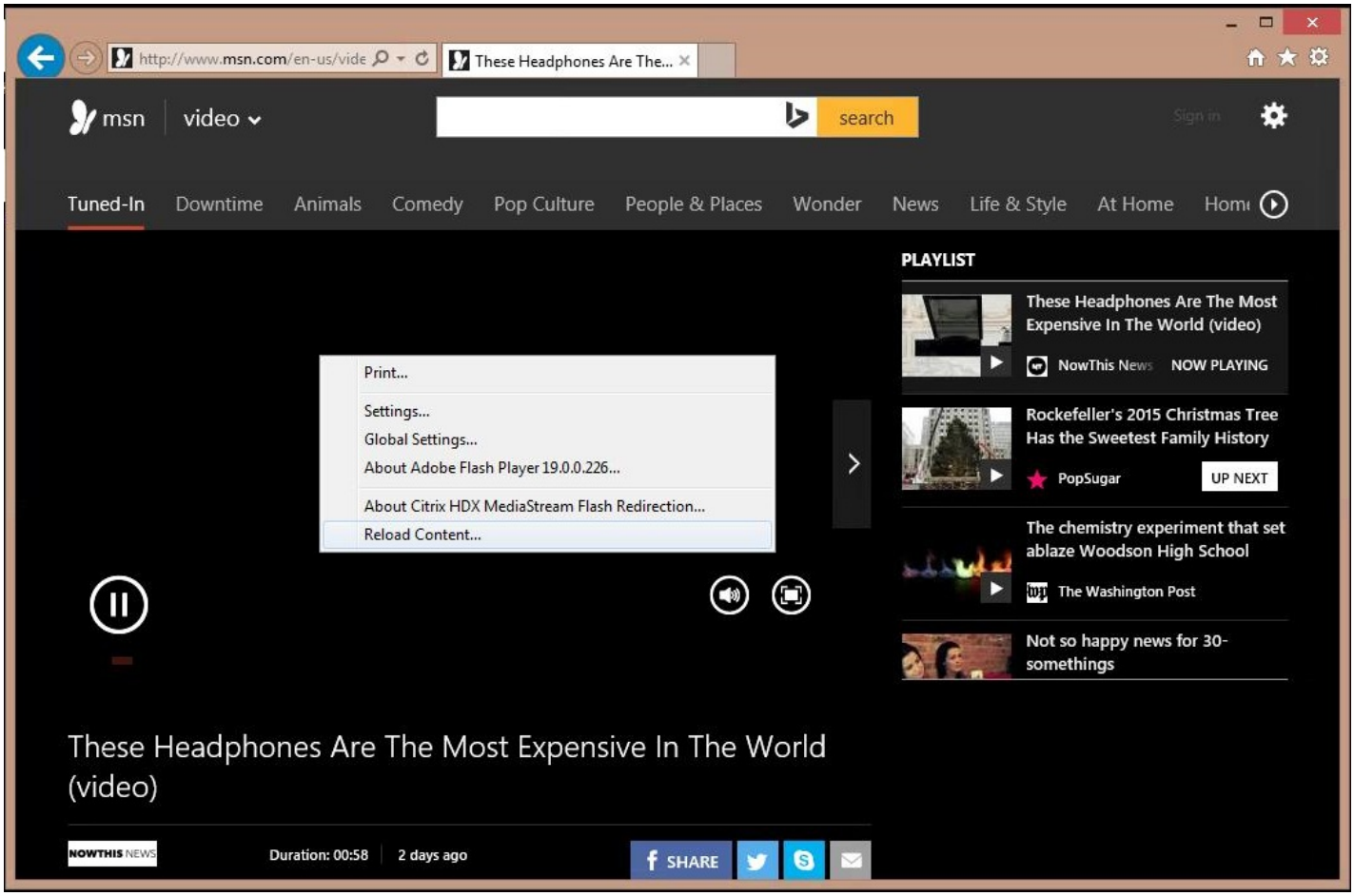
Esta versión incluye mejoras para la directiva de grupo de fiabilidad de la sesión. Al configurar la directivas de grupo de fiabilidad de la sesión, ahora se puede definir el nivel de transparencia que se aplica a un escritorio o una aplicación publicada durante el periodo de reconexión de fiabilidad de la sesión. Consulte **Fiabilidad de la sesión y directivas de grupo** en el tema Configuración de Receiver con la plantilla de objeto de directiva de grupo para obtener más información.

Alternativa manual para generación de contenido en el lado del servidor

En esta versión, Citrix Receiver implementa la opción de recurrir manualmente a la generación del servidor en el cliente En algunas situaciones, al ver contenido Flash, el cliente puede mostrar una pantalla en negro y no puede mostrar el vídeo de Flash. En la mayoría de los casos, si Flash no puede generarse en el cliente, recurrirá automáticamente a la generación en el lado del servidor. Sin embargo, en algunas ocasiones, la generación en el lado del cliente falla pero no puede recurrir automáticamente a la alternativa de generar el contenido en el servidor.

Para resolver estas situaciones, Citrix Receiver para Windows ahora ofrece una opción para que el usuario pueda actualizar la pantalla y forzar la generación del contenido Flash en el lado del servidor Para recurrir manualmente a la generación alternativa, coloque el cursor en la ventana de Flash en negro y haga clic para mostrar el menú contextual, que contiene la opción "Reload content". La imagen siguiente ilustra esta nueva funcionalidad.

> ### Nota
>
> Las directivas de prevención de vídeo definidas por el administrador se aplicarán obligatoriamente en el cliente. Para obtener más información, consulte Configuraciones de directiva de Multimedia y Configuraciones de directiva de Redirección de Flash.



Actualización de bibliotecas del SSL SDK para dar respaldo a NIST SP800-52

Citrix Receiver ofrece ahora una biblioteca de SSL SDK actualizada que incluye respaldo para NIST SP800-52. Esta funcionalidad permite a Receiver dar respaldo al modo de compatibilidad NIST SP800-52 para conexiones TLS. Para obtener más información, consulte Habilitación del modo de conformidad NIST SP 800-52 en el tema Para configurar los permisos del cliente. Consulte **Fiabilidad de la sesión y directivas de grupo** en el tema Configuración de Receiver con la plantilla de objeto de directiva de grupo para obtener más información sobre la fiabilidad de la sesión.

Proceso de actualización mejorado

Esta versión de Citrix Receiver para Windows ofrece un instalador actualizado que conserva los parámetros del cliente, lo que mejora la experiencia del usuario cuando actualiza el software desde versiones anteriores de Citrix Receiver. Además, el nuevo instalador actualiza el software directamente desde versiones instaladas previamente.

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.

Rendimiento de HDX mejorado

Citrix Receiver se ha actualizado para mejorar la aceleración por hardware en el lado del cliente. Esta funcionalidad mejora el rendimiento de HDX 3D Pro en clientes habilitando la aceleración de hardware. Para obtener más información sobre cómo configurar esta característica, consulte la sección Descodificación por hardware en el artículo de Experiencia del usuario.

Mejoras en la plataforma de autorización

Citrix Receiver para Windows integra ahora una funcionalidad que mejora cómo se puede verificar la manera en que los clientes se conectan a los servidores usando una versión TLS específica, incluida la verificación acerca del algoritmo de cifrado, el modo y el tamaño de la clave específicos, y si SecureICA está habilitado. Con esta funcionalidad también se puede ver el certificado de autenticación actual utilizado por el cliente durante una sesión activa. Para obtener más información, consulte este artículo de XenApp - XenDesktop que describe cómo se usa la criptografía.

Mensajes de diálogo de inicio mejorados

Esta versión mejora el modo en que Citrix Receiver para Windows utiliza diálogos de inicio para informar a los usuarios sobre cambios y actualizaciones relacionadas con el sistema. Ahora ofrece notificaciones sencillas que sustituyen a las notificaciones más largas de nivel de sistema que aparecían al iniciar una sesión.

Recopilación de información de diagnóstico mejorada

Esta versión integra una herramienta de diagnóstico mejorada que se puede usar para recopilar rápidamente información del sistema y distribuir la información creando un paquete único comprimido que puede transferirse o cargarse fácilmente en servicios como el CIS.

Problemas resueltos en esta versión

Importante: Si utiliza XenApp o XenDesktop 7.6, considere la conveniencia de instalar la revisión hotfix de VDA disponible en CTX142037, CTX142094 y CTX142095. Esta revisión hotfix soluciona problemas de sonido que se producen después de reconectar una sesión, y problemas relacionados con la respuesta de gráficos, la calidad de imagen y la corrupción de pantalla en algunas situaciones.

Problemas resueltos de Citrix Receiver para Windows 4.4

Jan 20, 2017

Receiver para Windows 4.4 CU3 (4.4.3000)

Comparado con: Citrix Receiver para Windows 4.4 CU2 (4.4.2000)

Receiver para Windows 4.4 CU3 (4.4.3000) contiene todas las correcciones que se incluyeron en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100, 4.4, 4.4 CU1 (4.4.1000) y 4.4 CU2 (4.4.2000), además de las correcciones siguientes:

Acceso a aplicaciones locales

- Ciertas aplicaciones SoftPhone o Chrome pueden no mostrarse correctamente cuando se usa el Acceso a aplicaciones locales.

  [#LC4327]

- Después de desconectarse de un escritorio de Acceso a aplicaciones locales y conectar a un escritorio de pantalla completa sin Acceso a aplicaciones locales, la barra de tareas del cliente puede mostrarse encima del escritorio de pantalla completa sin Acceso a aplicaciones locales.

  [#LC5966]

- Al cambiar una ventana de sesión desde pantalla completa al modo de ventana, no aparece un cuadro de diálogo similar al siguiente:
  "La sesión está en modo de ventana. Algunas funciones de Acceso a aplicaciones locales no funcionan en este modo".
  Al abrir una aplicación en modo de ventana, no aparece un cuadro de diálogo similar al siguiente:
  "Falló el inicio de la aplicación. La sesión está en modo de ventana. El inicio de aplicaciones en modo de Acceso a aplicaciones locales está prohibido en este modo. Cambie a pantalla completa si quiere abrir la aplicación".

  [#LC6291]

- Cuando el Acceso a aplicaciones locales está habilitado, la sesión de escritorio se inicia en modo de pantalla completa forzosamente.

  [#LC6294]

Optimización de CPU y memoria

- El proceso SelfServicePlugin.exe puede consumir altos niveles de memoria.

  [#LC4509]

Sesión/Conexión

- La asociación de tipos de archivo puede no funcionar al iniciar una sesión usando un perfil de usuario móvil y abrir una aplicación publicada.

  [#LC5184]

- Cuando se hace un dictado a SpeechMike junto con otra aplicación de reconocimiento de voz, SpeechMike podría dejar de funcionar.

  [#LC5632]

- El uso del proceso CleanUp.exe con el parámetro de ejecución silenciosa no vuelve a cargar Citrix Receiver correctamente.

  [#LC6039]

- HDX Engine puede cerrarse inesperadamente.

  [#LC6047]

- Al iniciar un escritorio desde un cliente ligero Wyse a través de NetScaler Gateway 11, puede aparecer el siguiente mensaje de error:

  "El cliente ha experimentado un problema con la autenticación en el servidor".

  [#LC6145]

- Las sesiones se pueden colgar o congelar cuando se mueve continuamente la ventana de la sesión.

  [#LC6403]

Tarjetas inteligentes

- Cuando está instalado Citrix Receiver para Windows 4.4, una aplicación publicada en XenApp 6.5 puede enviar una solicitud de transacción a una tarjeta inteligente para poner fin a una transacción que no está activa. Citrix Receiver para Windows puede responder de forma incorrecta a esta solicitud, lo que hace que el servidor XenApp espere la respuesta interminablemente, o que expire el valor de tiempo de espera de la transacción.

  [#LC5772]

Experiencia de usuario

- Esta solución mejora el respaldo para los sonidos que se reproducen durante un espacio corto de tiempo al usar el modo en tiempo real para el audio del cliente. Esta solución solo se aplica a la calidad de sonido media.

  [#LC4941]

- Es posible que la función de asociación de tipo de archivo no asocie el tipo de archivo al icono y la aplicación correctos

cuando se usan Windows 8.1 y Windows Server 2012 R2. Con esta solución, se incluyen dos directivas de grupo bajo Autoservicio.
1. Habilitar FTA predeterminada: Para habilitar o inhabilitar el comportamiento predeterminado de la asociación de tipos de archivo (FTA)
2. Habilitar FTA: Para habilitar o inhabilitar la funcionalidad de FTA
Para obtener el icono de asociación de tipo de archivo apropiado, inhabilite la directiva de grupo "Habilitar FTA predeterminada".

[#LC5485]

- El icono de asociación de tipo de archivo (FTA) puede comportarse como el icono de FTA predeterminado de Citrix Receiver para Windows cuando se inicia sesión en un escritorio publicado o si se restablece la configuración de Citrix Receiver para Windows.

  [#LC5730]

- Las cámaras Web de Surface Pro 4 y HP Elite pueden no redirigirse a una sesión. Nota: La redirección de cámaras Web también puede fallar si la cámara Web no respalda la resolución de pantalla.

  Para solucionarlo, use la siguiente clave del Registro:
  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Nombre: DefaultWidth
  Tipo: Dword
  Valor: <resolución respaldada por la cámara Web> Ejemplo (Surface Pro 4): 1920

  HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  Nombre: DefaultHeight
  Tipo: Dword
  Valor: <resolución respaldada por la cámara Web> Ejemplo (Surface Pro 4): 1080

  [#LC5750]

- Los escritorios asignados en función del nombre del cliente no se enumeran correctamente en la ventana de autoservicio. Este problema ocurre cuando se usa la experiencia unificada de StoreFront.

  [#LC5773]

Receiver para Windows 4.4 CU2 (4.4.2000)

Comparado con: Citrix Receiver para Windows 4.4 CU1 (4.4.1000)

Receiver para Windows 4.4 CU2 (4.4.2000) contiene todas las soluciones que se incluyeron en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100, 4.4 y 4.4 CU1 (4.4.1000) además de las soluciones siguientes:

Redirección de Flash HDX MediaStream	Experiencia de usuario
Teclado	Interfaz de usuario
Acceso a aplicaciones locales	Interfaz Web

Redirección de Flash HDX MediaStream

- El contenido Flash no se reproduce correctamente desde ProofHQ.com cuando SOLFileHook está habilitado.

  [#LC4866]

- Cuando se usan las versiones 22 o 18.0.0.360 de Adobe Flash Player y se navega por sitios Web con contenido Flash, las URL de los sitios Web se añaden a la lista negra dinámica y se generan en el servidor en lugar de hacerlo en el dispositivo de usuario.

  [#LC5626]

Teclado

- Cuando está habilitada la directiva de teclas de acceso directo y el proceso wfica32 está ejecutándose en un dispositivo de usuario, puede aparecer una ventana de diálogo con información sobre herramientas (tooltip) donde se indica que se está saliendo del modo de pantalla completa. La ventana de diálogo no acepta las entradas de teclado y mouse.

  [#LC4445]

- El teclado local en pantalla puede aparecer en la sesión de Citrix Receiver para Windows cada vez que se introduce texto al usar un dispositivo Microsoft Surface Pro con un teclado inalámbrico o USB externo.

  [#LC5093]

Acceso a aplicaciones locales

- Cuando está habilitado el Acceso a aplicaciones locales, si las aplicaciones se abren dentro de una sesión remota en modo de ventana o de pantalla completa, los iconos de la aplicación pueden no mostrarse en la barra de tareas de la sesión VDA. El dispositivo de punto final puede mostrar varios iconos de aplicación en la barra de tareas en lugar de uno solo.

  [#LC4217]

- Cuando se abre una sesión de escritorio publicado con el Acceso a aplicaciones locales habilitado, la barra de herramientas de Desktop Viewer puede desaparecer.

  [#LC5064]

- Cuando se está conectado a un VDA habilitado con Acceso a aplicaciones locales, el Conmutador de tareas del dispositivo de punto final aparece de manera intermitente en la sesión del VDA cuando se presiona ALT+TAB.

  [#LC5084]

- Un escritorio habilitado con Acceso a aplicaciones locales podría no generarse correctamente al cambiar del modo de ventana al modo de pantalla completa.

[#LC5091]

- Al desconectarse de un VDA que tiene habilitado el Acceso a aplicaciones locales, la barra de tareas puede quedar en modo de ocultación automática.

  [#LC5183]

Sesión/Conexión

- Al intentar cancelar la petición de certificado cuando la autenticación con certificados de cliente de NetScaler está configurada como "Opcional", puede fallar el inicio de una aplicación publicada, con el error desconocido de cliente 1110.

  [#LC4169]

- Una sesión con varias pantallas y cambio de usuario rápido puede mostrar la sesión solo en una pantalla después de reconectarse a la máquina cliente.

  [#LC4382]

- Si se abre una aplicación integrada desde el dispositivo del usuario 1 y luego se conecta a ese dispositivo de usuario desde otro dispositivo de usuario 2 sobre RDP, la aplicación integrada abierta puede pasar a modo de pantalla completa y tapar la barra de tareas del dispositivo de usuario 1. El problema continúa después de minimizar y restaurar la ventana de la aplicación.

  [#LC4682]

- Las sesiones conectadas a través de NetScaler Gateway pueden dejar de responder y consumir un alto porcentaje de ancho de banda.

  [#LC4710]

- Al usar algunos programas de software externos tales como Cisco WAAS, las sesiones de Citrix Receiver para Windows pueden desconectarse.

  [#LC4805]

- Esta corrección soluciona un problema de memoria en un componente subordinado.

  [#LC4903]

- Después de actualizar a Citrix Receiver parar Windows 4.4, el intento de abrir aplicaciones puede fallar de forma intermitente al iniciar sesión por primera vez hasta que se reinicia Citrix Receiver para Windows. Aparece el siguiente mensaje de error:

  "Cannot start app. Please contact your help desk."

  [#LC4975]

- El acceso a aplicaciones a través de Citrix Receiver desde StoreFront puede fallar desde ciertos dispositivos de usuario. Después de agregar un almacén correctamente, puede aparecer el siguiente mensaje de error durante el proceso de enumeración:

  "Cannot Connect to Server

Please check your network and try again
Try Again"

[#LC5039]

- El proceso de Single Sign-on (SSONSvr.exe) puede cerrarse inesperadamente o puede que las credenciales no se transfieran automáticamente a la pantalla de inicio de sesión, lo que hace que aparezca un diálogo para introducir manualmente las credenciales.

  [#LC5123]

- Citrix Receiver ignora la lista de omisión de proxys en Internet Explorer.

  [#LC5131]

- Después de instalar Citrix Receiver para Windows y configurar un almacén a través de una entrada de Registro o un con un objeto de directiva de grupo (GPO), al iniciar sesión por primera vez después de reiniciar la máquina virtual (VM), es posible que las aplicaciones no se enumeren.

  [#LC5198]

- Con la opción "Detectar la configuración automáticamente" habilitada en Microsoft Internet Explorer, la enumeración de aplicaciones en Citrix Receiver puede ser muy lenta.

  [#LC5224]

- Cuando Framehawk está habilitado, el botón de desplazamiento del mouse puede no ejecutar acción alguna en una sesión de VDA de XenDesktop 7.8. Hay una corrección disponible para el VDA en XenDesktop 7.9.

  [#LC5302]

- El inicio de aplicaciones haciendo clic en iconos del menú Inicio puede fallar de forma intermitente aunque se haya iniciado ya la sesión.

  [#LC5306]

- El proceso wfica32.exe puede cerrarse inesperadamente en la sesión del primer salto cuando se usa Citrix Receiver para Windows 4.4 y cuando el dispositivo del usuario es un dispositivo Android. El problema ocurre cuando se intenta abrir una aplicación publicada en un escenario de doble salto dentro de la sesión de usuario.

  [#LC5391]

- Durante un gesto de tocar y arrastrar, el botón del mouse puede quedar permanentemente en estado presionado cuando se usa una aplicación integrada EPIC. Al liberar el toque fuera de la ventana de la aplicación EPIC, la sesión puede dejar de responder.

  [#LC5644]

Excepciones del sistema

- Citrix Receiver para Windows puede cerrarse de manera inesperada y devolver el siguiente mensaje de error:

  "Citrix HDX Engine ha dejado de funcionar".

[#LC4100]

- Cuando se reproduce repetidamente un archivo .avi en el Reproductor de Windows Media, el proceso wfica32.exe puede bloquearse y cerrarse inesperadamente.

  [#LC4587]

- Al iniciar una aplicación publicada a través de proxy, Citrix Receiver para Windows puede cerrarse de manera inesperada y devolver el siguiente mensaje de error:

  "Citrix HDX Engine ha dejado de funcionar".

  [#LC5149]

- Citrix Authentication Manager (AuthMgrSvr.exe) puede cerrarse inesperadamente cuando se intenta agregar una cuenta después de instalar Citrix Receiver para Windows 4.4 en Windows Vista.

  [#LC5242]

Experiencia de usuario

- Cuando el Acceso a aplicaciones locales está habilitado, la ventana de la sesión puede posicionarse fuera de la ventana de Desktop Viewer cuando se restaura desde un estado maximizado.

  [#LC2930]

- Durante un gesto de tocar y arrastrar, el toque desde Citrix Receiver para Windows puede enviar eventos de mouse accidentales al servidor. Esto puede hacer que la aplicación integrada EPIC deje de responder.

  [#LC5459]

Interfaz de usuario

- Los intentos de abrir contenido no suscrito a través de StoreFront con la experiencia unificada pueden fallar, con el siguiente error:

  "No se pudo iniciar la aplicación porque el software requerido no está instalado."

  [#LC4308]

- En sistemas operativos de idiomas distintos del inglés, el texto del error de protocolo 1030 que aparece en Receiver para Windows puede aparecer confuso.

  [#LC4687]

- Al usar VLC Media Player con modo de máscara (skin) y con el Acceso a aplicaciones locales habilitado, el dispositivo de punto final puede mostrar varios accesos directos de barra de tareas en lugar de uno solo.

  [#LC4744]

- El icono de GoToMeeting no se muestra en la barra de tareas cuando se abre usando la URL de GoToMeeting en una instancia publicada de Microsoft Internet Explorer en modo integrado.

  [#LC4810]

- Al cambiar entre usuarios de la API de FastConnect, aparece el siguiente error:

  "Sus aplicaciones no están disponibles en este momento". Inténtelo de nuevo dentro de unos minutos."

  Además, cuando se inicia sesión usando la API de FastConnect, los accesos directos del usuario anterior no se quitan del escritorio.

  [#LC5602]

Interfaz Web

- La página de instalación de Citrix Receiver para Windows no aparece en la Interfaz Web si hay una versión anterior de Citrix Receiver instalada en el dispositivo del usuario.

  [#LC4242]

Otros problemas

- El proceso wfica32.exe puede consumir hasta un 100% de la CPU.

  [#LC4520]

- Al crear un almacén usando el comando "SelfService.exe command, -init –createprovider", por ejemplo: "C:\Archivos de programa (x86)\Citrix\ICA Client\SelfServicePlugin\SelfService.exe -init -createprovider store https://<URL de StoreFront>/Citrix/store/discovery", las claves de Registro relacionadas se crean correctamente. Pero si se hace clic en el icono de Receiver en el área de notificación para acceder a la interfaz de usuario de autoservicio, el almacén se borra del Registro y puede aparecer el cuadro de diálogo "Agregar cuenta".

  [#LC5096]

- El proceso wfica32.exe puede consumir hasta un 100% de la CPU.

  [#LC5189]

- Los parámetros de Client Selective Trust (CST) pueden perderse en lugar de conservarse y aparecer el diálogo "Acceso a archivos de HDX" durante el primero y los siguientes usos incluso aunque se haya seleccionado la opción "No preguntar de nuevo para este escritorio virtual". El problema ocurre siempre que se crean nuevas claves de Registro para el mismo VDA en la clave "HKEY_Current_User\Software\Citrix\Ica Client\Client Selective Trust" incluso después de seleccionarse esa opción.

  [#LC5598]

- La configuración de NetScaler con TLSv1.2 puede impedir que los dispositivos de usuario externos con Windows 7 agreguen una cuenta de StoreFront. Puede aparecer el siguiente mensaje de error:

  "The Authentication Service could not be contacted."

  [#LC5737]

Receiver para Windows 4.4 CU1 (4.4.1000)

Comparado con: Citrix Receiver para Windows 4.4

Receiver para Windows 4.4 CU1 (4.4.1000) contiene todas las soluciones que se incluyeron en Receiver para Windows 4.0,

4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3, 4.3.100 y 4.4 además de las soluciones siguientes:

Problemas en el dispositivo cliente

- Al usar Citrix Receiver para Windows 4.3, los dispositivos conectados a través de USB 3.0, incluidos los teclados y mouse, pueden dejar de funcionar y mostrar el error DRIVER_POWER_STATE_FAILURE (0x9f).

  [#LC4542]

- Los dispositivos Surface Pro Type/Touch Cover están disponibles para la redirección de USB. Después de la redirección de USB, el teclado o el cursor del mouse pueden dejar de funcionar fuera de la sesión. Actualmente, se ha agregado una regla de denegación (Deny) en el momento de la instalación para impedir la redirección de los dispositivos Surface Pro Type/Touch Cover. Consulte CTX137939 para obtener más detalles sobre cómo funcionan estas reglas.

  Nota: La solución actual está limitada solamente a instalaciones nuevas de Receiver. Para actualizaciones, es necesario agregar manualmente esta regla Deny en la clave de Registro que se indica a continuación.

  Para sistemas operativos de 32 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

  Para sistemas operativos de 64 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

  Modifique el valor de DeviceRules y agregue las reglas Deny específicas para el dispositivo USB.
  DENY:vid=045e pid=079A # Microsoft Surface Pro TouchCover
  DENY:vid=045e pid=079c # Microsoft Surface Pro Type Cover
  DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
  DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
  DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer

  Siga el mismo procedimiento agregando el VID y PID para aquellos dispositivos a los que sea necesario impedir la redirección.
  La regla DENY: vid=xxxx pid=xxxx para dispositivos específicos tiene que estar en la parte superior de la lista en DeviceRules.

[#LC4992]

HDX MediaStream

- Al abrir Internet Explorer dentro de una sesión de Acceso a aplicaciones locales, navegar a una página Web que tiene contenido Flash, y abrir una aplicación y maximizarla, el contenido del contenedor de Flash del explorador Web permanece en pantalla.

  [#LC4527]

Instalación, desinstalación y actualización

- Cuando se intenta suprimir la ventana "Agregar cuenta", la operación puede fallar al seguir las instrucciones indicadas en el artículo CTX135438 de Knowledge Center. Con esta solución, la ventana "Agregar cuenta" puede volver a aparecer incluso tras cerrarla después de restablecer o reiniciar Citrix Receiver.

  [#LC4593]

Teclado

- Si una aplicación publicada usa combinación de teclas de acceso rápido de Ctrl+Alt+[Tecla], y si Alt+[Tecla] o Ctrl+[Tecla] es una tecla de acceso rápido de Citrix, la combinación no se envía al servidor.

  [#LC3592]

- Cuando se usan aplicaciones o sesiones integradas, los clics del mouse no funcionan a veces como se espera.

  [#LC4779]

Acceso a aplicaciones locales

- Después de instalar el plug-in de redirección de URL para el explorador Web Mozilla Firefox Portable, puede aparecer un cuadro blanco grande en la parte inferior del explorador.

  [#LC4351]

- Cuando se ejecuta redirector.exe para registrar o anular el registro de exploradores Web en una sesión, aparece una ventana emergente con información que muchos usuarios consideran superflua. Con esta mejora, la ventana emergente ya no aparece a menos que se ejecute el comando redirector.exe con la opción /verbose.

  [#LC4480]

- Cuando se conecta con un escritorio publicado con el Acceso a aplicaciones locales habilitado, la ventana de la sesión puede no responder o puede desaparecer.

  [#LC4689]

- El proceso CDViewer.exe puede no responder cuando el Acceso a aplicaciones locales y la redirección USB están habilitadas en Citrix Receiver.

  [#LC5018]

Impresión

- A veces, la incrustación de fuentes falla cuando se usan fuentes con símbolos incrustados con controladores de impresora EMF.

  [#LC3334]

Ventanas integradas

- Cuando se abre y se minimiza una aplicación integrada, no se la puede restaurar ni maximizar desde la barra de tareas.

  [#LC3990]

Sesión/Conexión

- La sesión no se reconecta correctamente a través de un proxy usando WPAD. Al reconectar con la sesión desconectada, aparece un mensaje como el siguiente: "The network connection to your application was interrupted. Try to access your application later or contact your help desk."

  [#LC3077]

- No se puede agregar una URL de Storefront a una región distinta de la configuración específica de los sitios de confianza para esa región.

  [#LC3281]

- Para usar la asociación de tipos de archivo, use la siguiente clave de Registro. La siguiente clave de Registro está definida como True de manera predeterminada. Cuando la clave tiene el valor True, el icono del archivo local cambia al icono de Citrix Receiver si no hay ningún otro programa asociado con ese archivo en la máquina cliente. HKEY_CURRENT_USER\Software\Citrix\Dazzle\EnabledDefaultFTAs=false (REG_SZ)

  [#LC4096]

- Después de una desconexión por tiempo de espera de la fiabilidad de la sesión y reconexión automática de clientes, el inicio de la sesión se demora y el uso compartido de sesiones no funciona.

  [#LC4143]

- El tamaño de una unidad de cliente asignada puede aparecer incorrectamente y no pueden copiarse archivos en la unidad, si supera 1 TB. Con esta solución, la unidad mostrará 0.99TB si supera 1TB. El tamaño de una unidad de cliente asignada solo se muestra cuando está seleccionada la opción de asignación de unidades de cliente antigua.

  [#LC4214]

- Con el Acceso a aplicaciones locales (LAA) y Desktop Lock habilitados, la reconexión con una sesión de escritorio de servidor publicado, en pantalla completa, puede hacer que la sesión pierda el foco y deje de responder.

  [#LC4253]

- Cuando se usa la opción de inicio de sesión de Windows "Cambiar de usuario", se cambia la resolución de la sesión del escritorio virtual.

  [#LC4452]

- Cuando se usa Citrix Receiver, el inicio de aplicaciones puede no funcionar con el ICO SDK.

[En RcvrForWin4.4_14.4.1000] [#LC4550]

- Cuando un usuario inicia sesión en StoreFront a través de Self Service Plug-in, el proceso SelfService.exe puede quitar el foco de las otras ventanas activas intermitentemente, cada hora.

  [#LC4628]

- Las aplicaciones Epic pierden a veces el foco en la transición entre redes.

  [#LC4731]

- El proceso wfica32.exe puede cerrar inesperadamente al intentar abrir una aplicación, y puede aparecer un mensaje de error como el siguiente "La conexión con falló, con el estado (Error de cliente desconocido 0)".

  [#LC4768]

- El parámetro de Registro NotificationDelay controla la demora con la que aparece la barra de progreso de la conexión para conexiones integradas. A veces no funciona la configuración de este Registro si se usa el Self-Service Plug-in para iniciar la aplicación. Esta solución se ocupa de este problema.

  En Windows de 32 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Nombre: NotificationDelay
  Tipo: REG_DWORD
  Datos:

  En Windows de 64 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  Nombre: NotificationDelay
  Tipo: REG_DWORD
  Datos:

  [#LC4969]

Excepciones del sistema

- Cuando se actualizan las direcciones URL de los servicios XenApp mediante un objeto de directiva de grupo (GPO) y se aplica un nuevo GPO con nuevos valores de almacén (por ejemplo, store1 y store2), Citrix Receiver para Windows puede cerrarse inesperadamente.

  [#LC4145]

- Es posible que el proceso de wfica32.exe sufra una infracción de acceso y se cierre de forma inesperada.

  [#LC4482]

- El proceso SelfService.exe puede consumir hasta un 100% de la CPU.

  [#LC4494]

- Las sesiones con el cambio a GPU habilitado en el dispositivo de punto final pueden dejar de responder.

  [#LC4562]

Experiencia de usuario

- Esta solución mejora el respaldo para los sonidos que se reproducen durante un espacio corto de tiempo al usar el modo en tiempo real para el audio del cliente. Esta solución solo se aplica a la calidad de sonido baja.

  [#LC2783]

- Los sonidos del sistema de Windows pueden a veces ser inaudibles en XenApp 7.5.

  [#LC3926]

- En un entorno de red inestable aparecen mensajes como los siguientes: "Sus aplicaciones no están disponibles en este momento. Inténtelo de nuevo en unos minutos o póngase en contacto con la asistencia técnica con la información siguiente: Ocurrió un error al contactar con [nombre de servidor]" y "The network connection to your application was interrupted. Try to access your application later or contact your help desk." Esta solución agrega respaldo para la siguiente clave de Registro, que le permite inhabilitar los mensajes emergentes.

  En Windows de 32 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
  Nombre: SuppressDisconnectMessage
  Tipo: REG_DWORD
  Datos: 24(0x18)

  En Windows de 64 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
  Nombre: SuppressDisconnectMessage
  Tipo: REG_DWORD
  Datos: 24(0x18)

  [#LC4378]

Interfaz de usuario

- En ocasiones, los accesos directos no vuelven a aparecer si se los elimina manualmente y después se actualizan las aplicaciones.

  [#LC4020]

Receiver para Windows 4.4

Comparado con: Citrix Receiver para Windows 4.3.100

Receiver para Windows 4.4 contiene todas las soluciones que se incluyeron en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2, 4.1.100, 4.1.200, 4.2, 4.2.100, 4.3 y 4.3.100 además de las soluciones siguientes:

Instalación, desinstalación y actualización	Sesión/Conexión
Teclado	Excepciones del sistema
Acceso a aplicaciones locales	Experiencia de usuario

Inicio de sesión/Autenticación | Interfaz de usuario

Otros problemas

Instalación, desinstalación y actualización

- Después de desinstalar Citrix Receiver, Citrix HDX WMI Provider podría dejar de funcionar.

  [#LC3943]

Teclado

- Cuando la fiabilidad de la sesión está habilitada, la funcionalidad de "Ajustar a" no funciona en las sesiones reconectadas. La funcionalidad "Ajustar a" es un parámetro de mouse/teclado que se configura en **Panel de control** > **Mouse** > **Opciones de puntero** > **Mover automáticamente el puntero al botón predeterminado en un cuadro de diálogo**.

  [#LC1252]

- Al pasar de una ventana a otra usando las teclas Alt+Tab, se activan los menús de aplicación en una sesión de escritorio publicado.

  [#LC2947]

- Las sesiones de Citrix Receiver y RDP comparten la misma combinación de teclas de acceso directo "Ctrl+Alt+Fin" para invocar la combinación de teclas "Ctrl+Alt+Supr" en una sesión de terminal. Como resultado de ello, la combinación de teclas de acceso directo para la sesión RDP no tiene efecto cuando se ejecuta dentro de una sesión de Citrix Receiver.

  Con esta solución, la combinación de teclas de acceso directo "Ctrl+Alt+Fin" no es una tecla predeterminada para las sesiones de Citrix Receiver y se puede habilitar configurando la siguiente clave de Registro:

  - *En Windows de 32 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Nombre: EnableCtrlAltEnd
    Tipo: DWORD
    Valor: 1

  - *En Windows de 64 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    Nombre: EnableCtrlAltEnd
    Tipo: DWORD
    Valor: 1 (Si el valor es 0, la tecla Ctrl+Alt+Fin se usa dentro de la sesión RDP).

  [#LC3131]

- Después de actualizar a la versión 4.2 de Citrix Receiver, los clics del puntero en escenarios de doble salto pueden ser erráticos.

  [#LC3770]

Acceso a aplicaciones locales

- Cuando el Acceso a aplicaciones locales está habilitado, al hacer clic con el mouse para cambiar de tamaño una sesión en una máquina virtual, ésta puede dejar de responder.

  [#LC1853]

Inicio de sesión/Autenticación

- El inicio de sesión con Single Sign-on puede no funcionar cuando se intenta iniciar una sesión usando un nombre de dominio completo (FQDN) guardado en caché para las credenciales.

  [#LC3305]

- Cuando Receiver está configurado para usar la autenticación PassThrough para un servidor de Interfaz Web o StoreFront en una sesión de escritorio publicado, puede que Receiver no pase las credenciales y, en su lugar, las pida.

  [#LC3388]

Sesión/Conexión

- Con el preinicio de sesiones configurado, si se intenta reconectar a una sesión donde hay una aplicación publicada ejecutándose, se añade una instancia adicional de dicha aplicación publicada a la misma sesión.

  [#LC1701]

- Es posible que la sesión de Windows ejecutándose en primer plano pierda el enfoque de forma inesperada.

  [#LC2198]

- En la directiva, establezca **ProxyEnabled = false** bajo el subárbol del Registro **HKEY_LOCAL_MACHINE\SOFTWARE\\Citrix\AuthManager**, lo que omitirá el servidor proxy configurado en IE. El subárbol **Wow6432Node** no está disponible si se usa una arquitectura de SO de 32 bits.

  [#LC3129]

- En una configuración multipuerto o multisecuencia donde los datos de audio y vídeo están configurados en puertos distintos, el audio y el vídeo pueden aparecer desincronizados.

  [#LC3181]

- Los usuarios autenticados en Receiver para Windows 4.2 mediante una tarjeta inteligente pueden ver un mensaje de solicitud de autenticación con PIN al iniciar aplicaciones publicadas de XenApp.

  [#LC3187]

- La configuración "KEYWORDS:prefer" para una aplicación publicada puede no tener efecto. Esto puede ocurrir cuando el usuario cierra la sesión en Receiver y el proceso SelfService.exe se cierra inesperadamente.

  [#LC3190]

- Después de iniciar sesión en Citrix Receiver, los accesos directos de aplicaciones pueden tardar bastante tiempo en aparecer en el menú Inicio y en el escritorio del dispositivo del usuario.

[#LC3323]

- Los intentos de abrir archivos .wmv de vídeo de Windows Media desde un mensaje de correo electrónico en una instancia publicada de Microsoft Outlook pueden fallar.

  [#LC3453]

- Cuando Desktop Viewer cambia del modo de pantalla completa al modo de ventana, puede aparecer una barra de herramientas flotante en la sesión de XenDesktop mientras se usa Receiver.

  [#LC3526]

- Las sesiones de escritorio pueden desconectarse en lugar de permanecer activas cuando el sistema que está instalado con Desktop Lock y Receiver 4.3 está bloqueado.

  Para habilitar la corrección, establezca la siguiente clave de Registro:

  - *En Windows de 32 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
    Nombre: LiveInDesktopDisconnectonLock
    Tipo: REG_SZ
    Valor: False
  - *En Windows de 64 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
    Nombre: LiveInDesktopDisconnectonLock
    Tipo: REG_SZ
    Valor: False

  [#LC3579]

- Si está suscrito a una aplicación distribuida por streaming hacia el cliente para Citrix Receiver que no tiene instalado el Citrix Offline Plug-in, puede aparecer un mensaje de error como el siguiente al actualizar las aplicaciones dentro de Citrix Receiver:

  "Sus aplicaciones no están disponibles en este momento".

  [#LC3609]

- Cuando se inicia una sesión con Citrix Receiver para Windows, pueden aparecer múltiples sesiones de preinicio en distintos servidores de trabajo en el mismo grupo de entrega para un mismo usuario.

  [#LC3676]

- Después de desacoplar la barra de herramientas de Thomson Reuters Eikon en una sesión con varios monitores, el espacio que ocupaba la barra de herramientas no se devuelve a la sesión.

  [#LC3773]

- Si un dispositivo tiene instalada una versión de Receiver para Windows anterior a la 4.3 y el usuario actualiza el sistema operativo a Windows 10 desde Windows 7, Windows 8 o Windows 8.1, la desinstalación de Receiver mediante el panel de

Agregar o quitar programas puede fallar. Los intentos de actualizar a Receiver para Windows 4.3 también fallan.

[#LC3789]

- El proceso wfica32.exe puede cerrarse inesperadamente al intentar iniciar una nueva sesión.

  [#LC3795]

- Cuando se abren aplicaciones desde un escritorio publicado a través de Citrix Receiver y se cambia la carpeta "%appdata%" a otro servidor de archivos, puede aparecer el siguiente mensaje de error:

  "Error 1046: El controlador virtual no se ha cargado".

  [#LC3981]

- La ventana de alarma de una instancia de Lotus Notes instalada localmente puede quitar el foco del teclado a las aplicaciones publicadas.

  [#LC3889]

- Pueden aparecer iconos en carpetas de categorías en el menú Inicio y en el escritorio. No debe haber una carpeta de categorías para el escritorio. El problema ocurre cuando se usa la clave del Registro "UseCategoryAsStartMenuPath" para controlar iconos en carpetas de categorías para el menú Inicio y para el escritorio.

  Para habilitar la corrección, debe establecer las siguientes claves de Registro:

  - Cuando la clave del Registro "UseDifferentPathsforStartmenuAndDesktop" tiene el valor "false", la clave "UseCategoryAsStartMenuPath" controla la creación de carpetas de categorías tanto para el menú Inicio como para el escritorio.
  - Cuando la clave del Registro "UseDifferentPathsforStartmenuAndDesktop" tiene el valor "true", la clave "UseCategoryAsStartMenuPath" controla la creación de una carpeta de categorías de iconos en el menú Inicio. La clave "UseCategoryAsDesktopPath" controla la creación de una carpeta de categorías de iconos en el escritorio.

  [#LC4052]

- Los intentos de cambiar una contraseña en Citrix Receiver pueden fallar con el siguiente mensaje de error:

  "La contraseña anterior introducida es incorrecta".

  [#LC4081]

Excepciones del sistema

- Mientras se está utilizando Microsoft AX Dynamics 2009 o Excel 2007, Citrix Receiver 4.x puede cerrarse inesperadamente con un mensaje de error como el siguiente:

  "Citrix HDX Engine ha dejado de funcionar".

  [#LC3776]

Experiencia de usuario

- Al intentar agregar iconos de accesos directos al escritorio en una sesión de Citrix Receiver, ciertos iconos pueden no mostrar el icono específico de la aplicación. En su lugar, aparece el icono de página en blanco genérico.

[#LC4097]

- Aunque "EnableFTU" tenga el valor "false", el asistente de conexiones de Citrix Receiver no se puede inhabilitar.

  Para evitar que aparezca el asistente de conexiones, inhabilite la configuración de directiva EnableFTU usando la plantilla Receiver.adm/Receiver.admx:

  Configuración del equipo > Plantillas administrativas > Citrix Components > Citrix Receiver > SelfService > Enable FTU

  [#LC4133]

Interfaz de usuario

- Después de instalar el plug-in de redirección de URL para el explorador Web Mozilla Firefox, puede aparecer un cuadro blanco grande en la parte inferior del explorador.

  [#LC3409]

- Cuando la marca de sesión integrada del Registro "ENABLE COLOR SYNC" está definida, es posible que una sesión integrada no pueda heredar algunos de los colores del dispositivo del usuario y, en su lugar, muestre negro.

  Para habilitar la corrección, establezca la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/wfshell/TWI
  Nombre: SeamlessFlags
  Tipo: REG_DWORD
  Valor: 0x10

  [#LC3768]

- Al cambiar la URL de StoreFront, si se abre y se cierra la interfaz de usuario del Self-service Plug-in de Citrix Receiver, las aplicaciones que se configuraron como inhabilitadas pueden aparecer como iconos fantasma en lugar de aparecer atenuados.

  [#LC3863]

- Ciertas aplicaciones pueden no enumerarse en ocasiones; en su lugar, aparece un icono vacío en lugar del icono asociado a la aplicación en cuestión.

  [#LC4065]

- Si cambia el icono de una aplicación publicada en Citrix Studio, el acceso directo del escritorio para la aplicación no se actualiza.

  [#LC4124]

Otros problemas

- Cuando se agrega una cuenta a Citrix Receiver en un equipo que está ubicado detrás de un proxy, Citrix Receiver no usa los parámetros del proxy al contactar con las balizas: la ubicación se establece en "ninguna", en lugar de externa o interna.

[#LC2100]

- Al quitar el valor de Registro "ConnectionCenter" de la clave siguiente, se puede forzar una reparación de Citrix Receiver:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

  [#LC3751]

Nota: Esta versión de Citrix Receiver también incluye todas las soluciones que se incluyeron en las versiones 4.3, 4.2, 4.1 y 4.0.

Problemas conocidos de Citrix Receiver para Windows 4.4

Jan 20, 2017

Problemas conocidos de Citrix Receiver para Windows 4.4 CU3 (4.4.3000)

Se ha detectado el siguiente problema conocido en esta versión, junto con los problemas conocidos de Citrix Receiver para Windows 4.4, 4.4 CU1 (4.4.1000) y 4.4 CU2 (4.4.2000):

- Pueden fallar los intentos de cerrar Citrix Receiver después de excederse el tiempo de espera de ACR/SR. Como solución alternativa, cierre la sesión en Citrix Receiver y vuelva a iniciarla, finalice el proceso wfcrun32. [#336, #4115]

Problemas conocidos de Citrix Receiver para Windows 4.4 CU2 (4.4.2000)

Se ha detectado el siguiente problema conocido en esta versión, junto con los problemas conocidos de la versión Citrix Receiver para Windows 4.4 y 4.4 CU1 (4.4.1000):

- Cuando se inicia un escritorio publicado en una sesión de Escritorio remoto sin una barra de herramientas de Desktop Viewer, es posible que no aparezca la ventana de diálogo que indica que sale del modo de pantalla completa. Con la combinación del acceso directo de teclado "Mayús + F2", se controla si aparece la barra de título de la ventana de sesión. Como solución temporal, presione "Mayús + F2" para ver su escritorio y, a continuación, minimice la ventana de la sesión.

  [#LC4445, #639585]

Problemas conocidos de Citrix Receiver para Windows 4.4 CU1 (4.4.1000)

Se han detectado los siguientes problemas conocidos en esta versión, junto con los problemas conocidos de la versión Citrix Receiver para Windows 4.4:

- Después de desinstalar Citrix Receiver para Windows, el valor de Registro "Installer" bajo la clave de Registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ (en sistemas de 32 bits) y HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ (en sistemas de 64 bits) puede no eliminarse.

  [#635242]

Problemas conocidos en Citrix Receiver para Windows 4.4

Se han observado los siguientes problemas conocidos en esta versión:

- Al cambiar la orientación de una aplicación alojada en dispositivos Windows 10 Surface Pro aparece una pantalla con un cuadro de información sobre herramientas (tooltip) donde se indica que se está saliendo del modo de pantalla completa. Para resolver este problema, inhabilite los mensajes de información de este tipo configurando el siguiente parámetro de Registro:

  HKEY_CURRENT_USER\Software\Citrix\ica client\keyboard mappings\tips

  Para inhabilitar las sugerencias use el valor 1 y para habilitarlas use el valor 0; cuando el valor del Registro es 1, se inhabilitan todas las sugerencias.

  [#608346]

Advertencia

Si edita el Registro de forma incorrecta pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

- En las sesiones de VDA en clientes Windows 7 se pueden notar problemas de presentación gráfica que hacen que aparezca un fondo blanco detrás del texto en pantalla. Este problema ocurre cuando el cliente no tiene instalados los controladores GFX más recientes. Para resolver este problema cuando el cliente tiene controladores NVIDIA más antiguos.

  Para resolver este problema cuando el cliente tiene controladores NVIDIA más antiguos:

  1. Vaya al panel de control de NVIDIA.
  2. Vaya a los parámetros de vídeo.
  3. En la sección "How do you make color adjustments?", seleccione "With NVIDIA Settings."
  4. En los parámetros de NVIDIA, seleccione la ficha Advanced.
  5. En la ficha Advanced, para el parámetro Dynamic Range, seleccione el valor "Full (0-255)".

  Si lo prefiere, puede omitir la solución alternativa propuesta, y actualizar la máquina cliente con los controladores GFX más actualizados.

  [#610197]

Nota

Para obtener más información sobre el uso de controladores NVIDIA, consulte la página Dynamic RGB Range Capability en el sitio de asistencia técnica de NVIDIA.

- Degradación del rendimiento cuando se está conectado a un VDA de Windows 2008 R2 en modo de gráficos H.264 y la descodificación por hardware está habilitada en el cliente. Citrix recomienda usar el modo de gráficos antiguos en el VDA para evitar este problema.

  [#609292, 611580]

- ACR no puede reconectar con una sesión después de varios ciclos de desconexión/reconexión en el cliente, lo que obliga a los usuarios a volver a iniciar una sesión en StoreFront.

  [#567938]

- El plug-in de análisis de punto final (EPA) de NetScaler Gateway no ofrece respaldo para los dispositivos Receiver nativos de Windows.

  [#534790]

- Cuando se cierra la sesión de un usuario anónimo, Desktop Viewer muestra un mensaje que no está relacionado con un inicio de sesión anónimo. En tales casos, Receiver cierra automáticamente las sesiones anónimas en cuanto el usuario se desconecta. Debido a que no hay ninguna autenticación para inicios de sesión como esos, las sesiones anónimas no admiten las reconexiones, la movilidad entre clientes ni el control del área de trabajo.

  [#481561]

- En algunas instancias traducidas (por ejemplo, si Citrix Receiver se ejecuta en chino), es posible que un escritorio virtual y una aplicación no se inicien si las credenciales de inicio de sesión localizadas contienen pares suplentes en un nombre de usuario.

  [#556174]

- Si instala Receiver como administrador de dominio y selecciona la opción "Habilitar CEIP" durante la instalación, la ventana de CEIP aparece atenuada en el menú Acerca de.

  [#556179]

- Es posible que, en sesión, los controles de volumen no funcionen para RealTimes de RealPlayer debido a problemas de compatibilidad con RAVE.

  [#573549]

- Cuando se usa el modo sin conexión, Receiver se topa con los siguientes problemas:
  - La pérdida de conectividad de red no da como resultado un mensaje de error que indique al usuario cuál es el problema. No es posible actualizar aplicaciones o suscribirse o cancelar la suscripción a una aplicación cuando Receiver se usa en el modo sin conexión. [#559792, #560091, #560360]
  - Los cambios realizados a escritorios o aplicaciones mientras Receiver está sin conexión no se sincronizan cuando se vuelve a establecer la conectividad de la red. [#560362]

- Tras cerrar sesión en Receiver y volverla a iniciar, el nombre de usuario no aparece en la esquina superior derecha de la interfaz.

  [#562107]

- La autorización de tarjetas inteligentes no funciona con los sitios de servicios XenApp; sin embargo, sí funciona con los sitios de StoreFront. Para resolver este problema, haga que la autorización de tarjeta inteligente apunte a un sitio de StoreFront.

- Es posible que aún queden etiquetas con referencias a SSL en la interfaz de usuario. Por ejemplo: **TLS and Compliance Mode Configuration**. Estas etiquetas se actualizarán en una versión futura del software.

- La barra de idioma no aparece en la pantalla de inicio de sesión del cliente de Desktop Lock. Como solución alternativa, use la barra de idioma flotante.

  [#502678]

- Las opciones de Acceso directo de Citrix Desktop Viewer no funcionan cuando la sesión se abre en modo de ventana.

  [#510529]

- El mensaje de alerta de Desktop Viewer durante la desconexión no es aplicable a las sesiones de usuarios anónimos. Esto ha sido diseñado así.

  [#481561]

- Receiver para Windows no se puede instalar en una máquina con Windows 2012 R2 con una cuenta de usuario normal (no administrador).

  Para solucionar este problema:

  1. Haga clic en **Iniciar**, escriba **regedit** y presione **Entrar**.
  2. Busque el siguiente parámetro:

  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

  Cree: DisableMSI Tipo: REG_DWORD valor = 0 (0 permite la instalación)

  [#492508]

- A veces pueden verse notificaciones de la bandeja del sistema en el modo Desktop Lock.

  [#488620]

- El teclado virtual no se muestra automáticamente para el VDA de Terminal Server. La solución es abrir el teclado virtual mediante el icono en la barra de herramientas de Desktop Viewer o para aplicaciones, desde el icono de teclado virtual en la barra de tareas.

[#502774]

- La calidad del sonido es inferior a la esperada durante el uso remoto de unos auriculares USB (Logitech USB H340) con USB genérico. Esto ha sido diseñado así. No se realiza una optimización de audio en la redirección de USB. Esto se tendrá en cuenta para incluirlo como mejora en una futura versión del software.

  [#469670]

- Los gestos de pellizco y zoom no funcionan en las aplicaciones que se usan de modo remoto mediante versiones de XenApp y XenDesktop anteriores a la 7.0, o en XenApp y XenDesktop 7.0 o posterior en Windows 2008 R2.

  [#517877]

Requisitos del sistema y compatibilidad

Nov 03, 2016

Dispositivo

Sistema operativo

- Windows 10
- Windows 8.1, ediciones de 32 y 64 bits (y Embedded Edition)
- Windows 8, ediciones de 32 y 64 bits (y Embedded Edition)
- Windows 7, ediciones de 32 y 64 bits (y Embedded Edition)
- Windows Vista, ediciones de 32 y 64 bits
- Windows Thin PC
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2012, Standard y Datacenter Edition
- Windows Server 2008 R2, edición de 64 bits
- Windows Server 2008, ediciones de 32 y 64 bits

Hardware

- Adaptador de vídeo SVGA o VGA con monitor en color
- Tarjeta de sonido compatible con Windows para la compatibilidad de sonido (opcional)
- Una tarjeta de interfaz de red (NIC) y el software de transporte de red correspondiente, para las conexiones en red con la comunidad de servidores.
- Las máquinas cliente deben tener los controladores GFX más recientes para poder disfrutar del mejor rendimiento de gráficos.

Dispositivos de uso táctil

Citrix Receiver para Windows 4.4 se puede usar en portátiles, tabletas y monitores con Windows 7 y 8.1 habilitados para uso táctil con XenApp y XenDesktop 7 o versiones posteriores, y con agentes VDA (Virtual Desktop Agent) de Windows 7, 8 y 2012.

Servidores Citrix

- XenApp (cualquiera de los productos siguientes):
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5 Feature Pack 2 para Windows Server 2008 R2
  - Citrix XenApp 6.5 Feature Pack 1 para Windows Server 2008 R2
  - Citrix XenApp 6.5 para Windows Server 2008 R2
  - Citrix XenApp 4 Feature Pack 2, para sistemas operativos Unix
- XenDesktop (cualquiera de los productos siguientes):
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2

- Se puede usar el acceso de explorador Web de Citrix Receiver para Windows 4.4 junto con Receiver para Web de StoreFront y la Interfaz Web, con o sin NetScaler Gateway Plug-in.
  StoreFront:
  - StoreFront 3.0.x, 2.6, 2.5 y 2.1
    Para acceder directamente a almacenes de StoreFront.
  - StoreFront configurado con un sitio de Receiver para Web
    Para acceder a los almacenes de StoreFront a través de un explorador Web. Para ver las limitaciones de esta implementación, consulte "Consideraciones importantes" en Sitios de Receiver para Web.

  Interfaz Web junto con cliente NetScaler VPN:
  - Sitios Web de Interfaz Web 5.4 para Windows.
    Da acceso a aplicaciones y escritorios virtuales desde un explorador Web.
  - Interfaz Web 5.4 para Windows con sitios de servicios XenApp o sitios de servicios XenDesktop.
- Formas de implementar Citrix Receiver para los usuarios:
  - Habilitar a los usuarios para descargarlo desde receiver.citrix.com y, a continuación, configurarlo mediante el uso de una dirección de correo electrónico o de servicios junto con StoreFront.
  - Ofrecer la instalación desde el sitio de Citrix Receiver para Web (configurado con StoreFront).
  - Ofrecer la instalación de Receiver desde la Interfaz Web de Citrix 5.4.
  - Implementar mediante objetos de directiva de grupo (GPO) de Active Directory (AD).
  - Implementar mediante Microsoft System Center 2012 Configuration Manager.

Browser

- Internet Explorer
  Las conexiones con Citrix Receiver para Web o con la Interfaz Web respaldan el modo de 32 bits de Internet Explorer. Para ver las versiones de Internet Explorer respaldadas, consulte los requisitos del sistema para StoreFront y los requisitos del sistema para la Interfaz Web.

- Mozilla Firefox 18.x (versión mínima respaldada)
- Google Chrome versión 21 ó 20 (requiere StoreFront).

> **Nota**
>
> Para obtener más información sobre cambios en el respaldo para Google Chrome NPAPI, consulte el artículo del blog de Citrix, Preparing for NPAPI being disabled by Google Chrome.

Conectividad

Citrix Receiver para Windows respalda conexiones HTTPS e ICA sobre TLS a través de las siguientes configuraciones:

- Para conexiones LAN:
  - StoreFront con sitios de Receiver para Web o de servicios StoreFront
  - Interfaz Web 5.4 para Windows, usando la Interfaz Web o sitios de servicios XenApp.

  Para obtener más información sobre dispositivos unidos a un dominio y dispositivos no unidos a un dominio, consulte la documentación de XenDesktop 7.

- Para conexiones locales o remotas seguras:
  - Citrix NetScaler Gateway 11.x

- Citrix NetScaler Gateway 10.5

Se respalda el uso de dispositivos administrados unidos a dominios (locales o remotos, con o sin VPN) y de dispositivos que no pertenecen a un dominio (con o sin VPN).

Para obtener información sobre las versiones de NetScaler Gateway y Access Gateway respaldadas en StoreFront, consulte los requisitos del sistema para StoreFront.

> **Nota**
>
> Las referencias a NetScaler Gateway en este tema también son aplicables a Access Gateway, a menos que se indique lo contrario.

Acerca de las conexiones seguras y los certificados

> **Nota**
>
> Para obtener más información sobre certificados de seguridad, consulte los temas en las secciones Conexiones seguras y Comunicaciones seguras.

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 ignorar la advertencia y continuar con la conexión, se mostrará la lista de aplicaciones pero no se podrán iniciar.

Instalación de certificados raíz en los dispositivos de los usuarios

Para obtener más información sobre cómo instalar certificados raíz en los dispositivos de los usuarios además de configurar la Interfaz Web para el uso de certificados, consulte Protección de las comunicaciones de Receiver.

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. Citrix Receiver para Windows respalda el uso de certificados comodín, aunque deben usarse solo de acuerdo con la directiva de seguridad de la organización. En la práctica, se puede considerar la posibilidad de usar alternativas a certificados comodines, como por ejemplo, un certificado que contenga la lista de nombres de servidor dentro de la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Estos certificados pueden ser emitidos por entidades de certificación tanto privadas como públicas.

Certificados intermedios y NetScaler Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá añadir este certificado intermedio al certificado de servidor de NetScaler Gateway. Para obtener información, consulte Configuración de certificados intermedios.

Autenticación

Para conexiones con StoreFront, Citrix 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*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*
Dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	Sí*
Tarjeta inteligente	Sí	Sí	No		
Certificado de usuario				Sí (NetScaler Plug-in)	Sí (NetScaler Plug-in)

* Con o sin NetScaler plug-in instalado en el dispositivo.

> **Nota**
>
> Citrix Receiver para Windows 4.4 admite la autenticación de dos factores (dominio y token de seguridad) a través de NetScaler Gateway en el servicio nativo de StoreFront.

Para conexiones con la Interfaz Web 5.4, Citrix Receiver respalda los siguientes métodos de autenticación (en la Interfaz Web se usa el término "Explícita" para la autenticación de dominio y token de seguridad):

	Interfaz Web (exploradores	Sitio de servicios XenApp de	NetScaler a Interfaz Web	NetScaler a sitio de servicios XenApp de

	Web)	Interfaz Web	(explorador Web)	Interfaz Web
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí	Sí		
Token de seguridad			Sí*	
Dos factores (dominio con token de seguridad)			Sí*	
SMS			Sí*	
Tarjeta inteligente	Sí	No		
Certificado de usuario			Sí (NetScaler Plug-in)	

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

Para obtener información acerca de la autenticación, consulte Configuración de la autenticación y la autorización en la documentación de NetScaler Gateway, y los temas de la sección Administración en la documentación de StoreFront. Para obtener más información acerca de otros métodos de autenticación respaldados por la Interfaz Web, consulte Configuración de la autenticación para la Interfaz Web.

Actualizaciones

Se puede usar Citrix Receiver para Windows 4.x para actualizar Receiver para Windows 3.x así como el Citrix Online plug-in 12.x. Para obtener más información sobre la actualización, consulte Consideraciones sobre la actualización.

> **Nota**
>
> Si va a actualizar Citrix Receiver desde la versión 3.4 a la versión 4.2.100, siga las instrucciones facilitadas en Guía de actualización de Receiver 3.4 a Receiver 4.2.100 (en inglés). La versión 4.2.100 no admite las actualizaciones en contexto que lleve a cabo el usuario final. El administrador de TI debe preparar el entorno de modo que todos los usuarios de la red puedan completar la actualización correctamente. La información de la guía de actualización proporciona instrucciones paso a paso.

Otros

- **Requisitos de .NET Framework**
  - El Self-Service Plug-in necesita .NET 3.5 Service Pack 1; este plug-in permite a los usuarios suscribirse a escritorios y

aplicaciones, e iniciarlos desde la ventana de Receiver o desde la línea de comandos. Para obtener más información, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.
    - Se necesitan .NET 2.0 Service Pack 1 y Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package para que el icono de Receiver se muestre correctamente. El paquete de Microsoft Visual C++ 2005 Service Pack 1 se incluye en .NET 2.0 Service Pack 1, .NET 3.5 y .NET 3.5 Service Pack 1; también puede obtenerse por separado.
    - En conexiones de XenDesktop, para usar Desktop Viewer se necesita .NET 2.0 Service Pack 1 o una versión posterior. Esta versión es necesaria debido a que si no está disponible el acceso a Internet, las comprobaciones de revocación de certificados ralentizan los tiempos de inicio de conexión. Las comprobaciones se pueden desactivar y mejorar los tiempos de inicio con esta versión de Framework, pero no con .NET 2.0.
- Para obtener información sobre cómo usar Receiver con Microsoft Lync Server 2013 y Microsoft Lync 2013 VDI Plug-in para Windows, consulte XenDesktop, XenApp and Citrix Receiver Support for Microsoft Lync 2013 VDI Plug-in.

- **Transportes de red y métodos de conexión compatibles:**
    - TCP/IP+HTTP
      Consulte CTX 134341 para ver valores adicionales que puedan ser necesarios.

    - TLS+HTTPS

> ## Important
>
> Si hay almacenes configurados en StoreFront con un Tipo de transporte de HTTP, debe agregar el siguiente valor a la clave de Registro HKLM\Software\[Wow6432Node\]Citrix\AuthManager: ConnectionSecurityMode=Any.

> ## Advertencia
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Instalación

Aug 25, 2016

El paquete CitrixReceiver.exe puede ser instalado:

- Por un usuario, desde Citrix.com o desde un sitio de descarga
  - 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 dispositivo NetScaler Gateway (o Access Gateway), o el servidor StoreFront, que está asociado con la dirección de correo electrónico, y después pide al usuario que inicie una sesión y continúe con la instalación. Esta característica se conoce como "detección de cuentas basada en correo electrónico".
    Nota: Un usuario nuevo es aquel que no tiene Receiver instalado en el 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 distribución alternativo.
- Automáticamente desde Receiver para Web o desde la página de inicio de sesión de 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 (CR).
- Mediante una herramienta de distribución electrónica de software (ESD)
  - Un usuario que utiliza Receiver por primera vez debe introducir una dirección URL de servidor o abrir un archivo de aprovisionamiento para configurar una cuenta.

Receiver no requiere derechos de administrador para la instalación a menos que vaya a usar autenticación PassThrough.

HDX RealTime Media Engine (RTME)

Ahora hay un instalador único que combina la versión más reciente de Citrix Receiver para Windows con el instalador de HDX RTME. Al instalar la versión más reciente de Citrix Receiver, HDX RTME viene incluido en el archivo ejecutable (.exe).

> **Nota**
>
> La instalación de la versión más reciente de Citrix Receiver con el RTME integrado requiere privilegios administrativos en el host.

Tenga en cuenta los problemas siguientes de HDX RTME al instalar o actualizar Citrix Receiver:

- La última versión de Citrix Receiver contiene la versión más reciente de HDX RTME (versión 1.0.0.1); no se requieren más instalaciones si quiere instalar RTME.
- Se admite la actualización desde una versión de Receiver anterior a la versión empaquetada más reciente (Citrix Receiver con RTME). Las versiones anteriores de RTME instaladas se sobrescribirán con la versión más reciente; no se admite la actualización desde la misma versión de Receiver incluida en la versión empaquetada más reciente (por ejemplo, actualizar desde Receiver 4.4 a Receiver 4.4 con RTME).
- Si tiene una versión anterior de RTME, cuando instale la versión más reciente de Receiver, RTME se actualizará automáticamente en el dispositivo cliente.
- Si tiene una versión más reciente de RTME, el programa de instalación la conservará.

> **Important**

El HDX RealTime Connector en los servidores XenApp/XenDesktop debe tener la versión 2.0.0.417 (versión GA) como mínimo para la compatibilidad con el nuevo paquete RTME; es decir, RTME 2.0 no se puede usar con el 1.8 RTME Connector.

Actualización manual a Citrix Receiver para Windows

Para implementaciones con StoreFront:

- Se recomienda que los usuarios de BYOD (Bring Your Own Device), es decir usuarios que traen sus propios dispositivos, configuren las últimas versiones de NetScaler Gateway y StoreFront según se describe en la documentación correspondiente en el sitio de documentación de productos. Adjunte el archivo de aprovisionamiento creado por StoreFront en un mensaje de correo electrónico e informe a los usuarios de cómo realizar la actualización e indíqueles que abran el archivo de aprovisionamiento después de instalar Receiver.
- Como alternativa al envío de un archivo de aprovisionamiento, indique a los usuarios que deben introducir la URL de NetScaler Gateway (o Access Gateway Enterprise Edition). O, 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 y completar la configuración que se describe en Implementación de Receiver para Windows desde Receiver para Web. Informe a los usuarios sobre cómo actualizar Receiver, cómo acceder al sitio de Receiver para Web y cómo descargar el archivo de aprovisionamiento desde 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 Windows y complete la configuración que se describe en Implementación de Receiver para Windows desde una pantalla de inicio de sesión de la Interfaz Web. Indique a los usuarios cómo actualizar Receiver. Por ejemplo, puede crear un sitio de descargas donde los usuarios pueden obtener el instalador de Receiver con el nuevo nombre.

Consideraciones sobre la actualización

Sugerencia

El proceso para configurar la autenticación PassThrough (inicio de sesión único o Single Sign-on) cambió en Receiver para Windows 4.x. Para obtener más información, consulte la descripción de /includeSSON en Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

Se puede usar Citrix Receiver para Windows 4.x para actualizar Receiver para Windows 3.x así como el Citrix Online plug-in 12.x.

Si el Receiver para Windows 3.x fue instalado por equipo, no se respalda una actualización por usuario (realizada por un usuario sin privilegios administrativos).

Si el Receiver para Windows 3.x fue instalado por usuario, no se respalda la actualización por equipo.

Instalación y desinstalación manual de Receiver para Windows

Jan 29, 2016

Receiver puede instalarse desde discos de instalación, un recurso compartido de red, Windows Explorer o en la línea de comandos, ejecutando el paquete de instalación CitrixReceiver.exe. Para obtener información acerca de los parámetros de instalación y los requisitos de espacio, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

> ## Important
>
> El proceso para configurar la autenticación PassThrough (inicio de sesión único o Single Sign-on) cambió en Receiver para Windows 4.x. Para obtener más información, consulte la descripción de /includeSSON en Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

Si las directivas de su organización prohíben el uso de archivos .exe, consulte Cómo extraer, instalar y quitar manualmente archivos .msi individuales.

Instalación y configuración manuales de Receiver para la autenticación PassThrough

Receiver se puede usar en casos de autenticación PassThrough con XenApp y XenDesktop. Esta sección también describe cómo instalar y configurar CitrixReceiver.exe para usar la autenticación PassThrough para una conexión con un servidor de Interfaz Web o StoreFront.

Cuando esté correctamente instalado y configurado, los usuarios de XenApp/XenDesktop podrán acceder a sus recursos sin tener que introducir sus credenciales de nuevo. Las credenciales de la máquina cliente se transfieren automáticamente al punto final.

Tenga en cuenta los requisitos siguientes para la autenticación PassThrough:

- El paquete de instalación de Citrix Receiver para Windows es CitrixReceiver.exe.
- Cargue los archivos de directivas de grupo como corresponde:
  - receiver.adm (que se encuentra en la carpeta %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration de una máquina Windows donde está instalado Citrix Receiver); el archivo receiver.adm debe estar presente en Windows XP, Windows 2003 y clientes ligeros.
  - receiver.admx, receiver.adml (ubicados en la carpeta %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration en la máquina Windows donde está instalado Citrix Receiver); para cargar el archivo ADMX en un objeto de directiva de grupo (GPO), consulte la sección "Acerca de las plantillas ADMX" en Configuración de Receiver con la plantilla de objeto de directiva de grupo.
- Se necesitan privilegios administrativos locales en el dispositivo cliente para permitir la instalación y configuración del software.
  Nota: los archivos .adm solo se usan si se ejecuta el sistema operativo XPe para cliente ligero.

Hay dos formas de implementación diferentes para lograr la autenticación PassThrough en XenApp/XenDesktop cuando no se usan las herramientas de implementación de software de la empresa (tales como Citrix Merchandising Server o

Microsoft System Center Configuration Manager):

1. Instale Citrix Receiver manualmente y configúrelo mediante la directiva de grupo local (importando receiver.adm, receiver.admx, receiver.adml) en varias máquinas de forma individual.
   Nota: Esta es la práctica recomendada para entornos muy pequeños.

2. Instale Citrix Receiver mediante la directiva de grupo de Active Directory (por ejemplo, con la ayuda de **CheckAndDeployCitrixReceiverEnterpriseStartupScript.bat**, que se incluye con XenApp). A continuación, se puede aplicar la configuración mediante **receiver.adm, receiver.admx, receiver.adml**. Para ello, utilice la administración de directivas de grupo de Active Directory para una gran cantidad de máquinas administradas de forma centralizada.

Esta opción no se describe en este artículo por su mayor grado de complejidad. Para obtener más información, consulte CTX134280, How to Deploy Citrix Receiver Enterprise for Pass-Through Authentication Using Active Directory Group Policy.

Nota: Citrix recomienda encarecidamente que los pasos descritos en este artículo se comprueben y se validen en entornos que no sean de producción antes de usarlos.

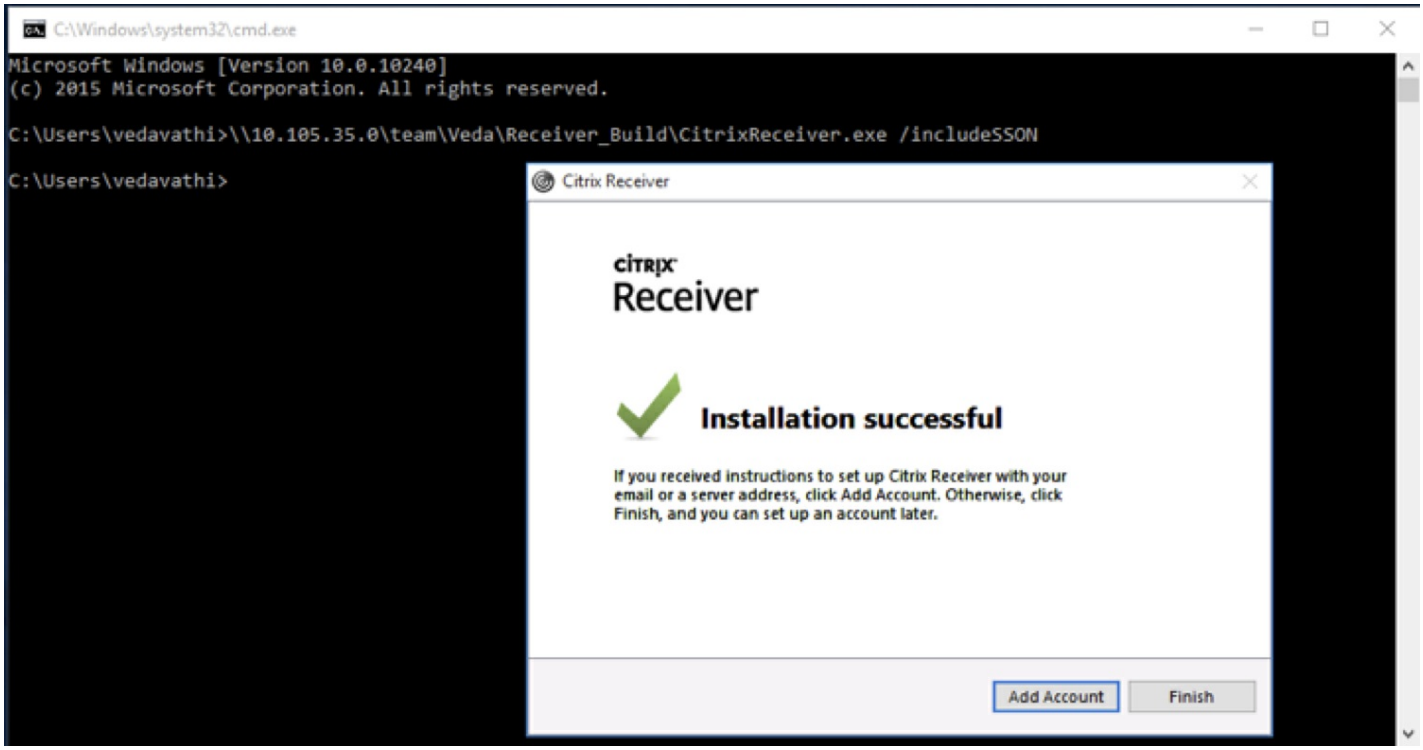
Para instalar y configurar Receiver manualmente para la autenticación PassThrough:

1. Ejecute el comando siguiente usando PowerShell en el Controller: **Set-BrokerSite -TrustedRequestsSentToTheXmlServicePort $True**
2. Inicie sesión en la máquina cliente como usuario con derechos administrativos.
3. Desinstale las instalaciones existentes de Online Plug-in o Citrix Receiver para Windows en la máquina cliente antes de iniciar el proceso de instalación.
4. Descargue el paquete de instalación de Citrix Receiver para Windows (CitrixReceiver.exe) desde Citrix Downloads.

   Use la implementación de instalación apropiada, usando la línea de comandos o la interfaz gráfica de usuario.

Para usar la línea de comandos:

1. Abra el **símbolo del sistema de Windows** y cambie el directorio donde se encuentra CitrixReceiver.exe.
2. En el **Símbolo del sistema**, ejecute el comando siguiente para instalar Citrix Receiver con la función Single Sign-on (SSON) habilitada: **CitrixReceiver.exe /includeSSON**. Tenga en cuenta la información contenida en el artículo Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos; el parámetro /includeSSON habilita Single Sign-on para el Receiver de la versión Standard (CitrixReceiver.exe). Esta opción no está respaldada para Receiver Enterprise (CitrixReceiverEnterprise.exe), ya que este instala Single Sign-On de manera predeterminada
3. Una vez finalizada la instalación, se muestra el mensaje emergente: "La instalación se completó con éxito".



Para usar la interfaz gráfica de usuario:

1. Haga doble clic en CitrixReceiver.exe.
2. En el asistente de instalación Habilitar Single Sign-on, marque la casilla Habilitar Single Sign-on para instalar Citrix Receiver con la característica SSON habilitada. Esto es equivalente a instalar Receiver usando la línea de comandos con el indicador /includeSSON.

Nota: El asistente de instalación para Habilitar Single Sign-on solo está disponible en instalaciones nuevas en máquinas unidas a dominios cuando la instalación la hace un administrador local.

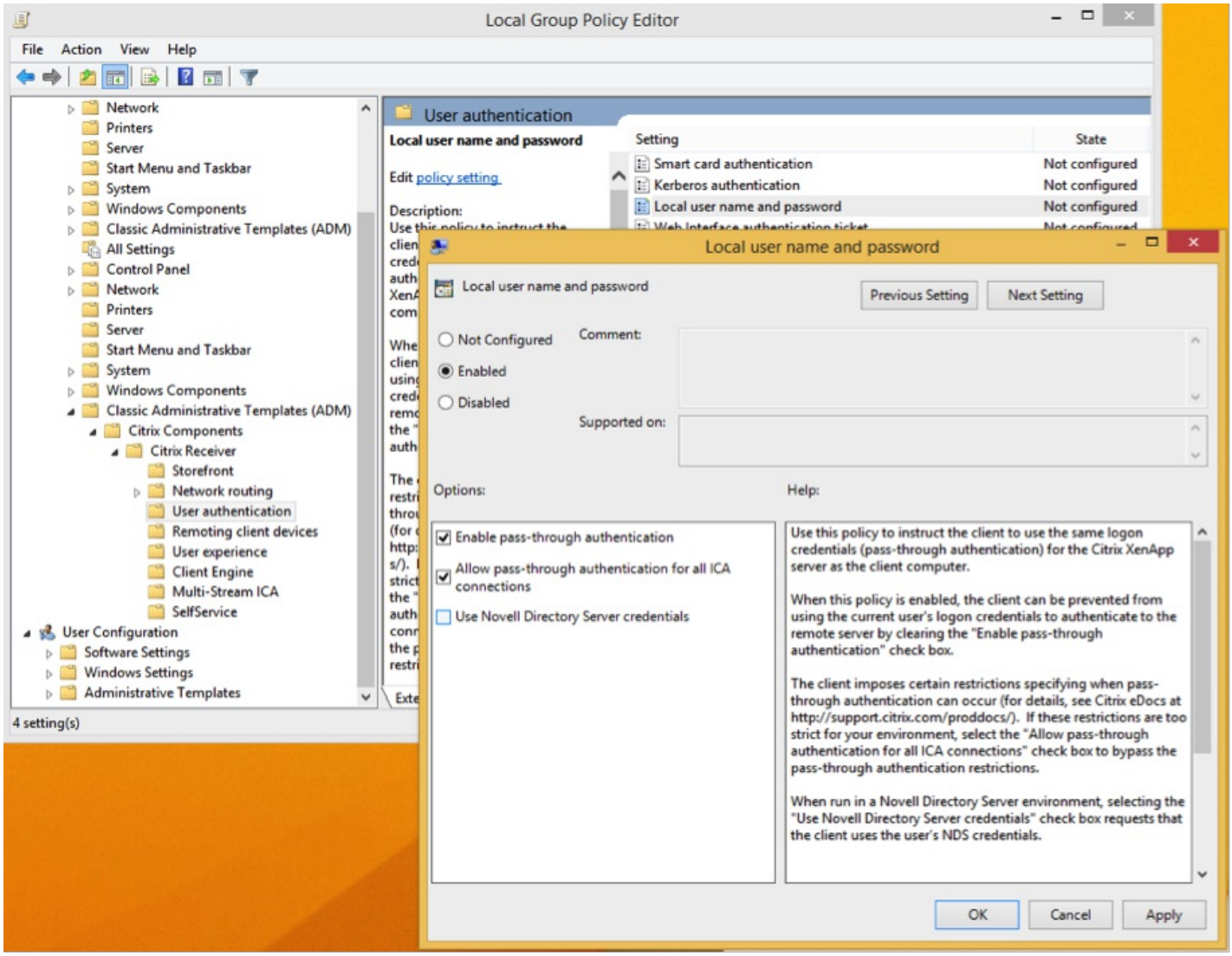
Configuración de SSON mediante el Editor de directivas de grupo local (GPO)

De manera predeterminada, la directiva de grupo para SSON es **Enable pass-through authentication**; esto es suficiente para que el inicio de sesión SSON funcione cuando no se usan Desktop Viewer y Receiver para Web. Cuando se usa Desktop Viewer, habilite el objeto de directiva de grupo para permitir la autenticación PassThrough para todas las conexiones ICA (**Allow pass-through authentication for all ICA connections**).

Para usar el archivo ADM para configurar la autenticación de usuarios

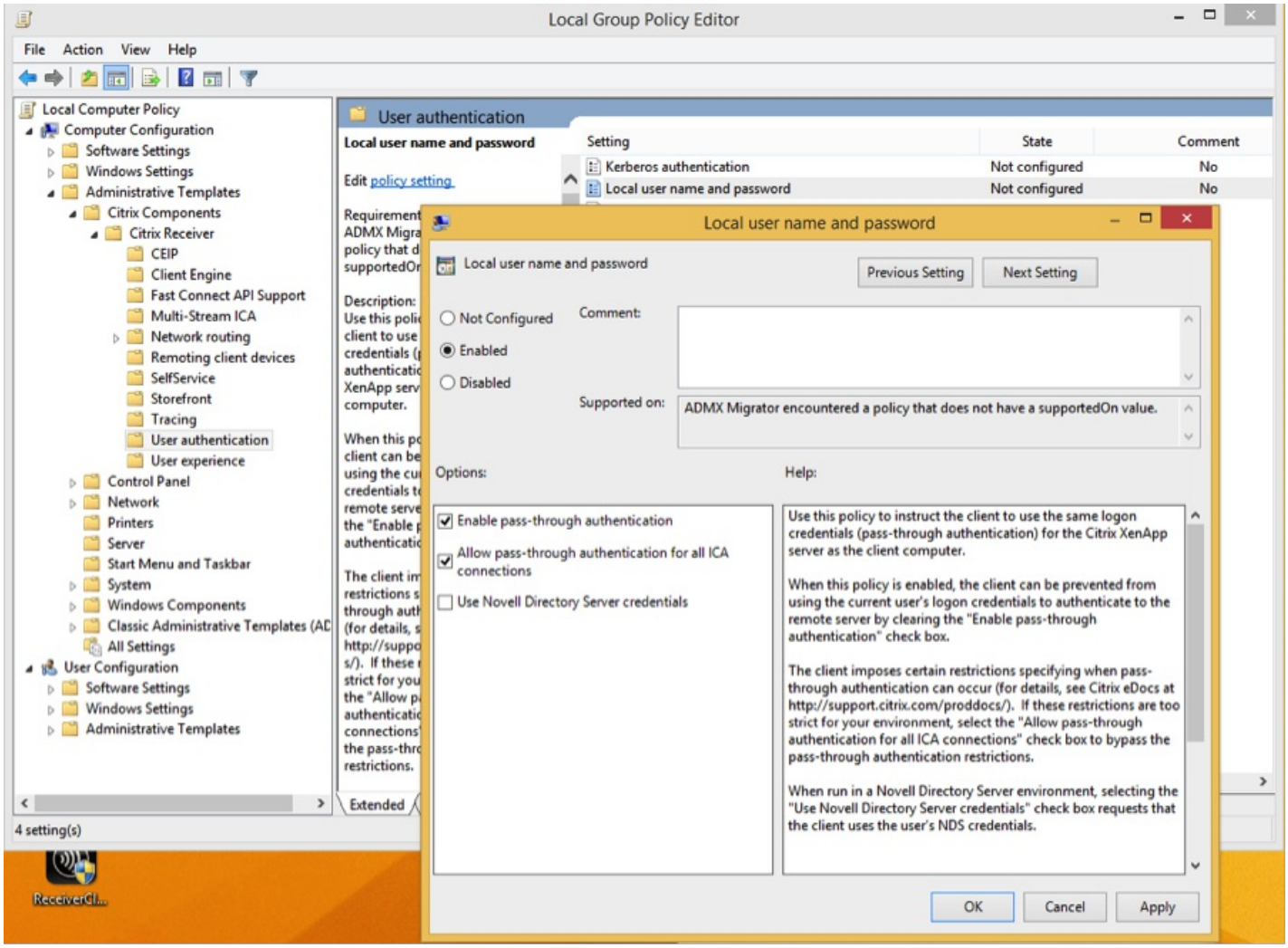
1. Para abrir el Editor de directivas de grupo local, ejecute el comando **gpedit.msc** o busque "Modificar directiva de grupo" en Inicio.
2. Agregue la plantilla receiver.adm al Editor de directivas de grupo local. Para ello, seleccione Configuración del equipo, haga clic con el botón secundario en Plantillas administrativas, seleccione Agregar o quitar plantillas y haga clic en **Agregar**.
3. Después de agregar la plantilla receiver.adm, expanda Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication.

Nota: Dependiendo de cómo estén definidos los parámetros de configuración y seguridad de StoreFront/Receiver para Web, es posible que sea necesario seleccionar la opción de permitir la autenticación PassThrough para todas las conexiones ICA (**Allow pass-through authentication for all ICA connections**) para que la autenticación PassThrough funcione.



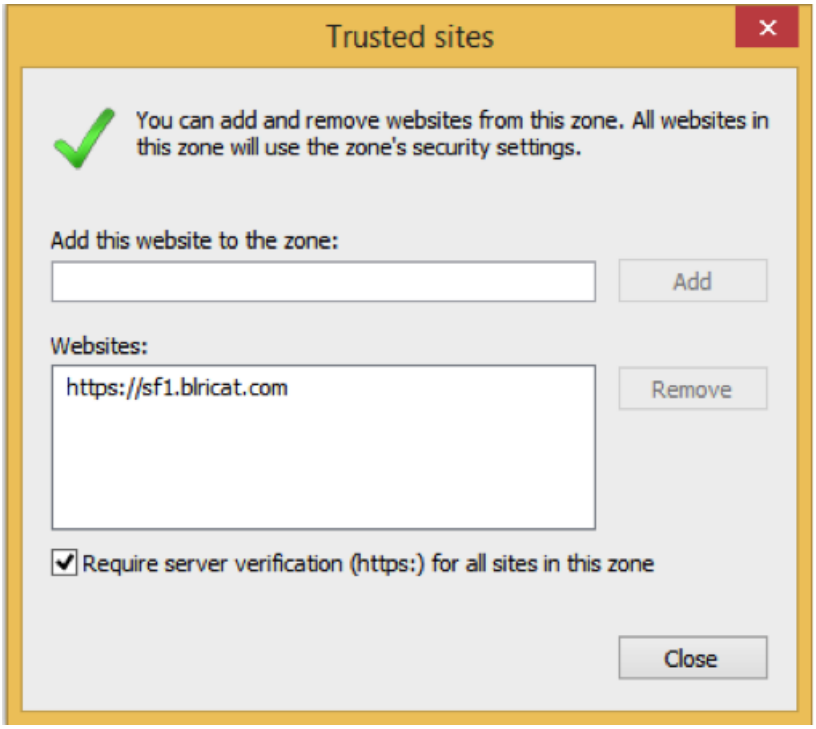
Uso de un archivo ADMX para la autenticación PassThrough

1. Agregue la plantilla receiver.admx y receiver.adml al Editor de directivas de grupo local. Consulte la sección "Acerca del uso de plantillas ADMX" en Configuración de Receiver con la plantilla de objeto de directiva de grupo.
2. Después de agregar correctamente la plantilla receiver.admx y receiver.adml, expanda Configuración del equipo > Plantillas administrativas > Citrix Components > Citrix Receiver > User Authentication.
3. Seleccione la configuración **Local user name password**.
4. Seleccione las opciones Enable pass-through authentication y Allow pass-through authentication for all ICA connections cuando habilite la directiva anterior.



Agregar el nombre de dominio completo (FQDN) a la lista de sitios de confianza

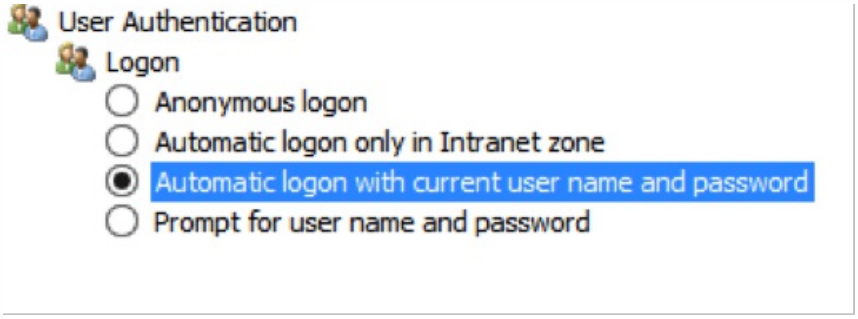
1. En el dispositivo cliente, inicie Internet Explorer.
2. En Internet Explorer, haga clic en Herramientas > Opciones de Internet > Sitios de confianza.
3. Haga clic en **Agregar** para agregar un nombre FQDN a la lista de sitios de confianza (por ejemplo, https://sf1.blricat.com). Una vez agregado, el sitio aparece en la lista de sitios Web:



Después de agregar un sitio Web a la lista de sitios de confianza, seleccione un método de autenticación de usuarios adecuado:

1. En la ficha Seguridad de Opciones de Internet, seleccione Sitios de confianza.
2. Elija **Nivel personalizado**.
3. En la lista, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.
4. Reinicie el dispositivo cliente para aplicar los cambios.

Nota: El inicio de sesión automático con el nombre de usuario y la contraseña actuales es un parámetro específico de cada usuario; si estos parámetros no se configuran localmente por el administrador local, cada usuario debe configurar su propia opción. Para aplicar este parámetro globalmente, configure un objeto de directiva de grupo (GPO) añadiendo este valor en el Nivel personalizado de los Sitios de confianza y de los Sitios de Internet.



Consideraciones importantes para la actualización usando Single Sign-on (SSON)

La tabla siguiente contenga información sobre la actualización de Receiver usando la línea de comandos con SSON:

SSON instalado antes de la actualización	Opción de SSON durante la instalación del nuevo Receiver	Comportamiento

	(Línea de comandos - /includeSSON o la opción de interfaz de usuario marcada)	
Sí	Sí	Componentes SSON actualizados Clave de Registro creada SSON funciona: no hay que hacer nada más para habilitarlo
Sí	No	Componentes SSON actualizados Clave de Registro creada SSON funciona: no hay que hacer nada más para habilitarlo
No	Sí	Componentes SSON actualizados Clave de Registro creada SSON inhabilitado: el usuario tiene que desinstalar Receiver y volver a instalarlo con la opción de SSON seleccionada mediante la opción de línea de comandos /includeSSON, o marcando la casilla correspondiente en la interfaz gráfica de usuario
No	No	Componente SSON no instalado

Nota: El asistente de instalación para habilitar Single Sign-on no está disponible cuando se actualiza una versión existente de Citrix Receiver.

Cómo quitar Receiver para Windows

Puede desinstalar Receiver con la herramienta Programas y características (Agregar o quitar programas) de Windows.

Para eliminar Receiver mediante la línea de comandos

También es posible desinstalar Receiver desde una línea de comandos escribiendo el comando siguiente:

CitrixReceiver.exe /uninstall

Después de desinstalar Receiver del dispositivo de usuario, las claves del Registro personalizadas creadas por Receiver.adm/Receiver.adml o Receiver.admx permanecen en el directorio Software\Policies\Citrix\ICA Client en HKEY_LOCAL_MACHINE y HKEY_LOCAL_USER. Si reinstala Receiver, estas directivas podrían aplicarse y es posible que resulten en un comportamiento inesperado. Para quitar estas personalizaciones, elimínelas manualmente.

Advertencia

El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos

Aug 25, 2016

Puede personalizar el instalador de Citrix Receiver especificando sus opciones en la línea de comandos. El paquete de instalación se descomprime automáticamente en el directorio temporal del usuario antes de iniciar el programa de instalación y requiere aproximadamente 57,8 MB de espacio libre en el directorio %temp%. El requisito de espacio incluye espacio para archivos de programa, datos de usuarios y directorios temporales después de iniciar varias aplicaciones.

> ## Advertencia
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Para instalar Citrix Receiver para Windows desde la interfaz de comandos, use la siguiente sintaxis:

CitrixReceiver.exe [Opciones]

Mostrar información de uso

Opción	/? o /help
Descripción	Este conmutador muestra información de uso
Ejemplo de uso	CitrixReceiver.exe /? CitrixReceiver.exe /help

Omitir el reinicio durante las instalaciones con interfaz de usuario

Opción	/noreboot
Descripción	Omite el reinicio durante las instalaciones con interfaz de usuario. Esta opción no es necesaria para instalaciones silenciosas. Si suprime las solicitudes de reinicio, los dispositivos USB que estén en estado suspendido cuando Receiver se instala no serán reconocidos por Receiver hasta que se reinicie el dispositivo del usuario.
Ejemplo de uso	CitrixReceiver.exe /noreboot

Instalación silenciosa

Opción	/silent
Descripción	Inhabilita los cuadros de diálogo de error y progreso para ejecutar una instalación completamente silenciosa.
Ejemplo de uso	CitrixReceiver.exe /silent

Habilitar autenticación Single Sign-on

Opción	/includeSSON
Descripción	Instala Single Sign-On (autenticación PassThrough). Esta opción es necesaria para los inicios de sesión Single Sign-on con tarjeta inteligente. La opción relacionada, ENABLE_SSON, se habilita cuando /includeSSON figura en la línea de comandos. Si usa ADDLOCAL= para especificar funciones y quiere instalar Single Sign-On, también tiene que especificar el valor ENABLE_SSON. Para habilitar la autenticación PassThrough en un dispositivo de usuario, es necesario instalar Receiver con derechos de administrador local desde una línea de comandos que incluya la opción /includeSSON. En el dispositivo del usuario, es necesario también habilitar estas directivas ubicadas en Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication: • Local user name and password • Enable pass-through authentication • Allow pass-through authentication for all ICA (puede que sea necesario, dependiendo de cómo esté configurada la Interfaz Web y los parámetros de seguridad) Una vez hechos los cambios, reinicie el dispositivo del usuario. Para obtener más información, consulte How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication. Nota: Las directivas de Tarjeta inteligente, Kerberos y Nombre de usuario local y contraseña son interdependientes. El orden de configuración es importante. Le recomendamos que inhabilite primero las directivas que no desee usar y, a continuación, habilite las directivas que necesite. Compruebe los resultados con atención.
Ejemplo de uso	CitrixReceiver.exe /includeSSON

Habilitar Single Sign-on cuando /includeSSON está especificado

Opción	ENABLE_SSON={Yes | No}

Descripción	Habilita el inicio de sesión único (Single Sign-on) cuando /includeSSON está especificado. El valor predeterminado es Yes. Habilita el inicio de sesión único (Single Sign-on) cuando /includeSSON también está especificado. Esta propiedad es necesaria para los inicios de sesión Single Sign-on con tarjeta inteligente. Tenga en cuenta que, después de realizar una instalación con la autenticación Single Sign-on habilitada, los usuarios deberán cerrar y volver a iniciar sus sesiones en los dispositivos. Requiere derechos de administrador.
Ejemplo de uso	CitrixReceiver.exe /ENABLE_SSON=Yes

Always-on tracing (seguimiento permanente)

Opción	/EnableTracing={true | false}
Descripción	Esta función está activada de forma predeterminada. Use esta propiedad para habilitar o inhabilitar explícitamente la función Always-on tracing. La función Always-on tracing ayuda a recopilar registros importantes en el momento de la conexión. Esos registros pueden resultar de utilidad en la resolución de problemas de conectividad intermitente. La directiva Always-on tracing sobrescribe este parámetro. De forma predeterminada, los archivos de registro de Always-on Tracing están en el directorio *C:\Users\\AppData\Local\Temp\CTXReceiverLogs\\xxx.etl*.
Ejemplo de uso	CitrixReceiver.exe /EnableTracing=true

Uso del programa Customer Experience Improvement Program de Citrix (CEIP)

Opción	/EnableCEIP={true | false}
Descripción	Cuando habilita la participación en el programa CEIP de mejora de la experiencia del usuario (Customer Experience Improvement Program), se envían estadísticas e información de uso anónimas a Citrix para ayudar a Citrix a mejorar la calidad y el rendimiento de sus productos.
Ejemplo de uso	CitrixReceiver.exe /EnableCEIP=true

Especificar el directorio de instalación

Opción	INSTALLDIR=
Descripción	Especifica la ruta de instalación, donde Directorio de instalación es la ubicación donde se instalará la mayor parte del software de Receiver. El valor predeterminado es C:\Archivos de programa\Citrix\Receiver. Los siguientes componentes de Receiver se instalan en la ruta C:\Archivos de programa\Citrix: Authentication Manager, Citrix Receiver y Self-Service plug-in.

	Si se usa esta opción y se especifica un Directorio de instalación, debe instalar RIInstaller.msi en el directorio Directorio de instalación\Receiver y los otros archivos .msi en el Directorio de instalación.
Ejemplo de uso	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identificar un dispositivo de usuario ante una comunidad de servidores

Opción	CLIENT_NAME=<*Nombre_del_cliente*>
Descripción	Especifica el nombre del cliente, donde Nombre_del_ cliente identifica el dispositivo de usuario en la comunidad de servidores. El valor predeterminado es %COMPUTERNAME%
Ejemplo de uso	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

Nombre dinámico del cliente

Opción	ENABLE_CLIENT_NAME=Yes | No
Descripción	La función de nombre de cliente dinámico permite que el nombre del cliente sea el mismo que el nombre del equipo. Cuando los usuarios cambian el nombre de su equipo, el nombre de cliente también cambia. El valor predeterminado es Yes. Si quiere inhabilitar el respaldo para usar el nombre dinámico del cliente, defina esta propiedad con el valor No y especifique un valor para la propiedad CLIENT_NAME.
Ejemplo de uso	CitrixReceiver.exe DYNAMIC_NAME=Yes

Instalar componentes especificados

Opción	ADDLOCAL=
	Instala uno o varios componentes especificados. Cuando quiera especificar varios parámetros, separe cada parámetro con una coma y no incluya espacios. Los nombres distinguen mayúsculas de minúsculas. Si no especifica este parámetro, todos los componentes se instalarán de forma predeterminada. Nota: Se requiere la instalación previa de ReceiverInside e ICA_Client para todos los demás componentes. Nota: Cuando ADDLOCAL no se indica, salvo SSON, se instalan todos los demás componentes predeterminados. Los componentes incluyen: • ReceiverInside. Instala el entorno de experiencia de uso de Citrix Receiver (componente requerido para el funcionamiento de Receiver). • ICA_Client. Instala el Citrix Receiver estándar (componente requerido para el funcionamiento de Receiver).

Descripción	• WebHelper. Instala el componente WebHelper. Este componente recupera el archivo ICA de StoreFront y lo pasa al motor de HDX. Además, comprueba los parámetros del entorno y los comparte con StoreFront (similar a la detección de cliente ICO). • SSON. Instala el inicio de sesión con Single Sign-On. Requiere derechos de administrador. • AM. Instala Authentication Manager. • SELFSERVICE. Instala Self-Service Plug-in. El valor AM debe especificarse en la línea de comandos, y .NET 3.5 Service Pack 1 tiene que estar instalado en el dispositivo del usuario. El Self-Service Plug-in no está disponible para dispositivos Windows Thin PC, que no respaldan .NET 3.5. • Para obtener información acerca de scripts de Self-Service Plug-in (SSP) y una lista de los parámetros disponibles en Receiver para Windows 4.2 y versiones posteriores, consulte http://support.citrix.com/article/CTX200337. • El Self-Service Plug-in permite a los usuarios acceder a aplicaciones y escritorios virtuales desde la ventana de Receiver o desde una línea de comandos, según se describe más adelante en esta sección, en Para iniciar una aplicación o un escritorio virtual desde una línea de comandos. • USB. Instala el respaldo para USB. Requiere derechos de administrador. • DesktopViewer. Instala Desktop Viewer. • Flash. Instala el componente HDX MediaStream para Flash. • Vd3d. Habilita la interfaz de Windows Aero (para los sistemas operativos que lo respaldan).
Ejemplo de uso	CitrixReceiver.exe ADDLOCAL=ReceiverInside, ICA_Client, SSON

Configurar almacenes que no están configurados en entregas de Merchandising Server

Opción	ALLOWADDSTORE={N | S | A}
Descripción	Especifica si los usuarios pueden agregar o quitar almacenes que no han sido configurados a través de entregas de Merchandising Server; los usuarios pueden habilitar o inhabilitar almacenes configurados por entregas de Merchandising Server, pero no pueden quitar dichos almacenes o cambiar el nombre de las URL). El valor predeterminado es S. Entre las opciones se incluyen: • N: No permite nunca que los usuarios agreguen o quiten su propio almacén. • S: Permite que los usuarios agreguen o quiten solamente almacenes seguros (configurados con HTTPS). • A: Permite que los usuarios agreguen o quiten tanto almacenes seguros (HTTPS) como almacenes no seguros (HTTP). No se aplica si Citrix Receiver se instaló mediante una instalación por usuario. También puede controlar esta característica actualizando la clave de Registro HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore. Nota: De forma predeterminada, únicamente se permiten almacenes seguros (HTTPS) y se recomienda utilizar éstos para entornos de producción. Para entornos de pruebas, puede usar conexiones a almacenes HTTP mediante la siguiente configuración: 1. Establezca HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore con el valor A para permitir que los usuarios agreguen almacenes no seguros. 2. Establezca HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd con el valor A para

	permitir que los usuarios guarden las contraseñas de almacenes no seguros. 3. Para permitir agregar un almacén configurado en StoreFront con un Tipo de transporte de HTTP, agregue a HKLM\Software\[Wow6432Node\]Citrix\AuthManager el valor ConnectionSecurityMode (tipo REG_SZ) y establézcalo en Any. 4. Salga de Citrix Receiver y reinícielo.
Ejemplo de uso	CitrixReceiver.exe ALLOWADDSTORE=N

Guardar las credenciales de los almacenes localmente usando el protocolo PNAgent

Opción	ALLOWSAVEPWD={N | S | A}
Descripción	Especifica si los usuarios pueden agregar o quitar almacenes que no han sido configurados a través de entregas de Merchandising Server; los usuarios pueden habilitar o inhabilitar almacenes configurados por entregas de Merchandising Server, pero no pueden quitar dichos almacenes o cambiar el nombre de las URL). El valor predeterminado es S. Entre las opciones se incluyen: • N: Nunca se permite que los usuarios guarden sus contraseñas. • S: Se permite que los usuarios guarden contraseñas solamente para almacenes seguros (configurados con HTTPS). • A: Se permite que los usuarios guarden contraseñas tanto para almacenes seguros (HTTPS) como almacenes no seguros (HTTP). También puede controlar esta característica actualizando la clave de Registro HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd. Nota: Si AllowSavePwd no funciona, debe agregarse manualmente la siguiente clave de Registro: • Clave para clientes con SO de 32 bits: HKLM\Software\Citrix\AuthManager • Clave para clientes con SO de 64 bits: HKLM\Software\wow6432node\Citrix\AuthManager • Tipo: REG_SZ • Valor: never - nunca se permite que los usuarios guarden sus contraseñas. secureonly - se permite que los usuarios guarden contraseñas solamente para almacenes seguros (configurados con HTTPS). always - se permite que los usuarios guarden contraseñas tanto para almacenes seguros (HTTPS) como almacenes no seguros (HTTP).
Ejemplo de uso	CitrixReceiver.exe ALLOWSAVEPWD=N

Seleccionar el certificado

Opción	AM_CERTIFICATESELECTIONMODE={Prompt | SmartCardDefault | LatestExpiry}
	Use esta opción para seleccionar un certificado. El valor predeterminado es Prompt, que pide al usuario que elija un certificado de la lista. Cambie esta propiedad para seleccionar la opción de certificado

Descripción	predeterminado (según lo indique el proveedor de la tarjeta inteligente) o la opción de certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible. También puede controlar esta característica actualizando la clave de Registro HKCU o HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }. Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.
Ejemplo de uso	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

Usar componentes del proveedor CSP para administrar la entrada del PIN de tarjeta inteligente

Opción	AM_SMARTCARDPINENTRY=CSP
Descripción	Usar los componentes del proveedor de servicios criptográficos (CSP) para administrar la entrada del PIN de la tarjeta inteligente. De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de Citrix Receiver en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. Receiver pide a los usuarios que introduzcan un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Especifique esta propiedad para usar los componentes del proveedor CSP para gestionar la introducción del PIN, incluidas las solicitudes de PIN.
Ejemplo de uso	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Usar Kerberos

Opción	ENABLE_KERBEROS={Yes | No}
Descripción	El valor predeterminado es No. Especifica si el motor HDX debe usar autenticación Kerberos y se aplica solo cuando la autenticación Single Sign-on (PassThrough) está habilitada. Para obtener más información, consulte Configuración de autenticación PassThrough de dominio con Kerberos.
Ejemplo de uso	CitrixReceiver.exe ENABLE_KERBEROS=No

Mostrar iconos de FTA antiguos

Opción	LEGACYFTAICONS={False | True}
	Use esta opción para mostrar los iconos de asociación de tipos de archivos (FTA) antiguos. El valor predeterminado es False. Especifique si se muestran los iconos de aplicación para aquellos documentos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Cuando el parámetro está

Descripción	configurado como False, Windows genera iconos para documentos que no tienen un icono específico asignado a ellos. Los iconos generados por Windows consisten en un icono de documento genérico superpuesto con un icono de la aplicación de tamaño más pequeño. Citrix recomienda habilitar esta opción si planea entregar aplicaciones de Microsoft Office a usuarios que ejecutan Windows 7.
Ejemplo de uso	CitrixReceiver.exe LEGACYFTAICONS=False

Habilitar el preinicio de sesiones

Opción	ENABLEPRELAUNCH={False | True}
Descripción	El valor predeterminado es False. Para obtener información sobre el preinicio de sesiones, consulte Reducción del tiempo de inicio de las aplicaciones.
Ejemplo de uso	CitrixReceiver.exe ENABLEPRELAUNCH=False

Especificar el directorio para los accesos directos del menú Inicio

Opción	STARTMENUDIR={Nombre del directorio}
Descripción	De forma predeterminada, las aplicaciones aparecen en Inicio > Todos los programas. Se puede especificar una ruta relativa bajo la carpeta de programas para contener los accesos directos a las aplicaciones suscritas. Por ejemplo, para colocar accesos directos en Inicio > Todos los programas > Receiver, especifique STARTMENUDIR=\Receiver\. Los usuarios pueden cambiar el nombre de la carpeta o mover la carpeta cuando lo deseen. También se puede controlar esta característica mediante una clave de Registro. Para ello, cree la entrada REG_SZ para StartMenuDir y otórguele el valor "\RelativePath". Ubicación: HKLM\Software\[Wow6432Node\]Citrix\Dazzle HKCU\Software\Citrix\Dazzle Para aplicaciones publicadas a través de XenApp con el elemento Carpeta de aplicaciones del cliente (también llamado Carpeta de Program Neighborhood) especificado, se puede configurar para que esa carpeta se agregue a la ruta de accesos directos. Para ello, cree la entrada REG_SZ para UseCategoryAsStartMenuPath y otórguele el valor "true". Use las mismas ubicaciones de Registro señaladas anteriormente. Nota: Windows 8/8.1 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con XenApp. Ejemplos

	• Si la carpeta de aplicaciones del cliente es \office, UseCategoryAsStartMenuPath tiene el valor "true", y no se especifica un directorio StartMenuDir, los accesos directos se colocan en Inicio > Todos los programas > Office. • Si la carpeta de aplicaciones del cliente es \office, UseCategoryAsStartMenuPath tiene el valor "true" y el directorio StartMenuDir es \Receiver, los accesos directos se colocan en Inicio > Todos los programas > Receiver > Office. Los cambios que se hagan a estos parámetros no tienen impacto alguno en los accesos directos ya creados. Para mover accesos directos, es necesario desinstalar y volver a instalar las aplicaciones.
Ejemplo de uso	CitrixReceiver.exe STARTMENUDIR=\Office

Especificar el nombre del almacén

Opción	STOREx="nombre_almacén;http[s]://nombre_servidor.dominio/ubicación_IIS/discovery;[On | Off];[descripción_almacén]" [STOREy="..."]
Descripción	Use esta opción para especificar el nombre del almacén. Especifica hasta 10 almacenes para usar con Citrix Receiver. Valores: • x,y: Acepta valores enteros entre 0 y 9. • nombre_almacén: El valor predeterminado es store. Este valor debe coincidir con el nombre configurado en el servidor StoreFront. • nombre_servidor.dominio: El nombre de dominio completo del servidor que aloja el almacén. • ubicación_IIS: La ruta al almacén en IIS. La URL del almacén debe coincidir con la URL en los archivos de aprovisionamiento de StoreFront. Las direcciones URL de almacén tienen el formato "/Citrix/store/discovery". Para obtener la dirección URL, exporte un archivo de aprovisionamiento desde StoreFront, ábralo en el bloc de notas y copie la dirección URL desde el elemento . • On | Off: El parámetro de configuración Off opcional permite distribuir almacenes inhabilitados, lo que ofrece a los usuarios la opción de acceso. Cuando el estado del almacén no se especifica, el parámetro predeterminado es On (habilitado). • descripción_almacén: Una descripción optativa del almacén, por ejemplo "Almacén de aplicaciones de RRHH". Nota: En esta versión, es importante incluir "/discovery" en la URL del almacén para que la autenticación PassThrough se realice correctamente.
Ejemplo de uso	CitrixReceiver.exe STORE0="Store;https://test.xx.com/Citrix/Store/Discovery"

Habilitar la redirección de URL en los dispositivos de los usuarios

Opción	ALLOW_CLIENTHOSTEDAPPSURL=1
	Habilita la característica de redirección de URL en los dispositivos de los usuarios. Requiere derechos de administrador. Requiere que Citrix Receiver se instale para Todos los usuarios. Para obtener información

Descripción	sobre la redirección de URL, consulte Acceso a aplicaciones locales y sus temas secundarios, en la documentación de XenDesktop 7.
Ejemplo de uso	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

Habilitar el modo de autoservicio

Opción	SELFSERVICEMODE={False | True}
Descripción	El valor predeterminado es True. Cuando el administrador establece la marca SelfServiceMode con el valor False, el usuario deja de tener acceso a la interfaz de usuario de autoservicio de Citrix Receiver. En su lugar, el usuario puede acceder a las aplicaciones suscritas desde el menú Inicio y a través de accesos directos de escritorio, lo que se conoce como "modo de acceso directo solamente".
Ejemplo de uso	CitrixReceiver.exe SELFSERVICEMODE=False

Especificar el directorio para los accesos directos de escritorio

Opción	DESKTOPDIR=
Descripción	Coloca todos los accesos directos en una misma carpeta. Se respalda el uso de CategoryPath para los accesos directos de escritorio. Nota: Cuando se usa la opción DESKTOPDIR, configure la clave PutShortcutsOnDesktop con el valor True.
Ejemplo de uso	CitrixReceiver.exe DESKTOPDIR=\Office

Actualizar desde una versión de Citrix Receiver no respaldada

Opción	/rcu
Descripción	Permite actualizar una versión no respaldada a la versión más reciente de Citrix Receiver.
Ejemplo de uso	CitrixReceiver.exe /rcu

Mostrar un cuadro de diálogo de instalación finalizada durante las instalaciones desatendidas

Cuando la instalación finaliza, aparece un diálogo donde se indica que la instalación fue correcta, seguido de la pantalla **Agregar cuenta**. Para los usuarios nuevos, el diálogo Agregar cuenta requiere la introducción de una dirección de servidor o

de correo electrónico para configurar una cuenta.

> **Nota**
>
> Si no se ha sido definido un almacén común con el argumento STOREx de más arriba, o con un objeto de directiva de grupo, los usuarios que no han iniciado una sesión previamente en un equipo donde Citrix Receiver esté instalado, pueden ver el diálogo Agregar cuenta. Para eliminar este diálogo, cree un valor de REG_DWORD EnableFTU en la clave HKLM\Software\Citrix\Receiver y defina el valor como 0.

Solución de problemas de la instalación

Si existe un problema con la instalación, busque en el directorio %TEMP%/CTXReceiverInstallLogs del usuario para consultar los registros que tengan el prefijo CtxInstall- o TrolleyExpress- . Por ejemplo:

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

Ejemplos de instalación mediante la línea de comandos

Para instalar todos los componentes de manera silenciosa y especificar dos almacenes de aplicaciones:

CitrixReceiver.exe /silent STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;Almacén de aplicaciones de RRHH" STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Almacén de respaldo de RRHH"

Para especificar autenticación con Single Sign-on (PassThrough de credenciales) y agregar un almacén que haga referencia a una URL de servicios XenApp:

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

Para iniciar una aplicación o un escritorio virtual desde la línea de comandos

Citrix Receiver crea una aplicación de código auxiliar (stub) para cada aplicación o escritorio suscrito. Es posible usar una aplicación de código auxiliar para iniciar una aplicación o un escritorio virtual desde la línea de comandos. Las aplicaciones de código auxiliar se encuentran en %appdata%\Citrix\SelfService. El nombre de archivo de una aplicación de código auxiliar es el nombre simplificado de la aplicación con los espacios eliminados. Por ejemplo, el nombre de archivo de la aplicación de código auxiliar para Internet Explorer es InternetExplorer.exe.

Implementación de Receiver para Windows mediante Active Directory y scripts de inicio de ejemplo

Jan 29, 2016

Los scripts de directiva de grupo de Active Directory se pueden usar para realizar la distribución inicial de Receiver en sistemas basados en la estructura de organización de Active Directory presente. Citrix recomienda usar los scripts en lugar de extraer los archivos .msi, dado que los scripts permiten la instalación, actualización y desinstalación desde una sola ubicación, así como consolidar las entradas de Citrix en Programas y características, y facilitar la detección de la versión de Receiver que se va a distribuir. Use el parámetro Scripts en la Consola de administración de directivas de grupo (GPMC) que se encuentra en Configuración del equipo o Configuración de usuario. Para obtener información general acerca de los scripts de inicio, consulte la documentación de Microsoft.

Citrix incluye ejemplos de scripts de inicio por equipos para instalar y desinstalar CitrixReceiver.exe. Estos scripts se encuentran en el soporte de instalación reciente de XenApp y XenDesktop, en la carpeta Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Cuando los scripts se ejecutan al inicio o cierre de una directiva de grupo de Active Directory, se pueden crear archivos de configuración personalizados en el perfil de usuario predeterminado (Default User) del sistema. Si no se eliminan, estos archivos de configuración pueden impedir que los usuarios accedan al directorio de registros de Receiver. Los scripts de ejemplo de Citrix incluyen funciones para eliminar correctamente dichos archivos de configuración.

Para usar los scripts de inicio para distribuir Receiver con Active Directory

1. Cree la unidad organizativa (UO) para cada script.
2. Cree un objeto de directiva de grupo (GPO) para la unidad organizativa recién creada.

Para modificar los scripts de ejemplo

Modifique los scripts editando estos parámetros en la sección del encabezado de cada archivo:

- **Current Version of package** (Versión actual del paquete). El número de versión especificado se valida y, si no existe, se lleva a cabo la distribución. Por ejemplo: set DesiredVersion= 3.3.0.XXXX para que coincida exactamente con la versión especificada. Por ejemplo, si especifica la versión parcial 3.3.0, esa versión coincidirá con cualquier versión que contenga ese prefijo (3.3.0.1111, 3.3.0.7777, y así sucesivamente).
- **Package Location/Deployment directory** (Ubicación del paquete/directorio de distribución). Especifica el recurso compartido de red que contiene los paquetes (el script no realiza la autenticación). La carpeta compartida debe tener permisos de lectura para todos (EVERYONE).
- **Script Logging Directory** (Directorio de registros del script). Especifique el recurso compartido de red donde se copiarán los registros de instalación (el script no realiza la autenticación). La carpeta compartida debe tener permisos de lectura y escritura para todos (EVERYONE).
- **Package Installer Command Line Options** (Opciones de línea de comandos del instalador). Estas opciones de línea de comandos se envían al programa de instalación. Para obtener más información acerca de la sintaxis de la línea de comandos, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

Para agregar scripts de inicio de equipo

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione Configuración del equipo > Directivas > Configuración de Windows > Scripts (inicio o apagado).
3. En el panel de la derecha de la consola, seleccione Inicio
4. En el menú Propiedades, haga clic en Mostrar archivos, copie el script apropiado a la carpeta que se muestra y después cierre la ventana.
5. En el menú Propiedades, haga clic en Agregar y use la opción Examinar para buscar y agregar los scripts recientemente creados.

Para distribuir Receiver por equipos

1. Mueva los dispositivos de usuario designados para recibir esta distribución a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie una sesión como cualquier usuario.
3. Verifique que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) contiene el paquete recientemente instalado.

Para quitar Receiver de equipos particulares

1. Mueva los dispositivos de usuario designados para la eliminación a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie una sesión como cualquier usuario.
3. Compruebe que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) haya quitado el paquete anteriormente instalado.

Uso de los scripts de inicio de ejemplo por usuario

Citrix recomienda usar scripts de inicio por equipo. No obstante, en el caso de que necesite implementaciones de Receiver por usuario, hay dos scripts de Receiver incluidos en los medios de instalación de XenDesktop y XenApp en la carpeta Citrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scripts.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

Para configurar scripts de inicio por usuario

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione Configuración de usuario > Directivas > Configuración de Windows > Scripts.
3. En el panel de la derecha de la consola, seleccione Iniciar sesión
4. En el menú Propiedades de inicio de sesión, haga clic en Mostrar archivos, copie el script apropiado a la carpeta que se muestra y después cierre la ventana.
5. En el menú Propiedades de inicio de sesión, haga clic en Agregar y use la opción Examinar para buscar y agregar los scripts recientemente creados.

Para distribuir Receiver a usuarios particulares

1. Mueva los usuarios designados para recibir esta implementación a la unidad organizativa que ha creado.
2. Reinicie el dispositivo de usuario e inicie una sesión como el usuario especificado.
3. Verifique que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) contiene el paquete recientemente instalado.

Para quitar Receiver de usuarios particulares

1. Mueva los usuarios designados a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie una sesión como el usuario especificado.
3. Compruebe que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) haya quitado el paquete anteriormente instalado.

Implementación de Receiver para Windows desde Receiver para Web

Jan 29, 2016

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 a los usuarios acceder 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 Sitios de Receiver para Web en la documentación de StoreFront.

La detección de cuentas basada en correo electrónico no se aplica cuando Receiver se distribuye desde Receiver para Web. Si la detección de cuentas basada en correo electrónico está configurada y un usuario nuevo instala Receiver desde Citrix.com, Receiver pide al usuario una dirección de correo electrónico o de servidor. Al introducir una dirección de correo electrónico, aparece el mensaje de error: "Your email cannot be used to add an account" (Su dirección de correo electrónico no puede usarse para agregar cuentas). Use la siguiente configuración para que se solicite únicamente la dirección del servidor.

1. Descargue CitrixReceiver.exe en el equipo local.
2. Cambie el nombre de CitrixReceiver.exe por CitrixReceiverWeb.exe.
   Importante: El nombre CitrixReceiverWeb.exe distingue entre mayúsculas y minúsculas.
3. Distribuya el ejecutable con el nuevo nombre usando su método de distribución habitual. Si usa StoreFront, consulte Configuración de los sitios de Receiver para Web mediante los archivos de configuración en la documentación de StoreFront.

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

Jan 29, 2016

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

Para obtener más información, consulte Configuración de la implementación de clientes en la documentación de la Interfaz Web.

La detección de cuentas basada en correo electrónico no se aplica cuando Receiver se distribuye desde la Interfaz Web. Si la detección de cuentas basada en correo electrónico está configurada y un usuario nuevo instala Receiver desde Citrix.com, Receiver pide al usuario una dirección de correo electrónico o de servidor. Al introducir una dirección de correo electrónico, aparece el mensaje de error: "Your email cannot be used to add an account" (Su dirección de correo electrónico no puede usarse para agregar cuentas). Use la siguiente configuración para que se solicite únicamente la dirección del servidor.

1. Descargue CitrixReceiver.exe en el equipo local.
2. Cambie el nombre de CitrixReceiver.exe por CitrixReceiverWeb.exe.
   Importante: El nombre CitrixReceiverWeb.exe distingue entre mayúsculas y minúsculas.
3. Especifique el nuevo nombre de archivo en el parámetro ClientIcaWin32 en los archivos de configuración de los sitios Web de XenApp.
   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.
4. Agregue los sitios desde donde descargará el archivo CitrixReceiverWeb.exe a la zona de sitios de confianza.
5. Distribuya el ejecutable con el nuevo nombre usando su método de distribución habitual.

Configuración de Citrix Receiver para Windows

Aug 25, 2016

Cuando se utiliza el software Receiver para Windows, los siguientes pasos de configuración permiten a los usuarios acceder a sus aplicaciones y escritorios alojados:

- Configure la entrega de aplicaciones y su entorno de XenDesktop. Asegúrese de que el entorno de XenApp está configurado correctamente. Familiarícese con las opciones y ofrezca descripciones de las aplicaciones útiles para sus usuarios.
- Configure el modo de autoservicio agregando una cuenta de StoreFront a Receiver. Este modo permite a los usuarios suscribirse a aplicaciones desde la interfaz de usuario de Receiver.
- Configure el modo de accesos directos solamente, que incluye:
  - Uso de una plantilla de objeto de directiva de grupo (GPO) para personalizar los accesos directos.
  - Uso de claves del Registro para personalizar los accesos directos.
  - Configuración de accesos directos basándose en los parámetros de cuenta de StoreFront
- Proporcione la información de cuentas a los usuarios. Proporcione a los usuarios la información que necesiten para configurar el acceso a las cuentas donde se alojan sus aplicaciones y escritorios virtuales. 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, Citrix Receiver para Windows 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

Si agrega la cuenta de un sitio de StoreFront o Interfaz Web a Receiver para Windows, puede configurar el modo de autoservicio, que permite a los usuarios suscribirse a las aplicaciones a través de 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.

Al acceder a un sitio de StoreFront 3.0, la experiencia de los usuarios es la de Receiver. Para obtener más información sobre la experiencia de usuario de Receiver, 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

Tal y como se ha indicado anteriormente, si agrega una cuenta de StoreFront a Receiver o si configura Receiver para que apunte a un sitio de servicios XenApp o Interfaz Web, 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 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 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.

> **Nota**
>
> Al iniciar una sesión usando el modo de autoservicio, la conexión automática está habilitada de manera predeterminada.

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 ofrece una plantilla que se puede usar para crear un sitio de descargas de Receiver.

Configuración de la entrega de aplicaciones

Nov 03, 2016

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 configuración, Receiver para Windows 4.4 ofrece acceso basado en 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 para seleccionar y usar las aplicaciones que deseen. En este modo, no se colocan accesos directos en el escritorio del usuario.
- 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 se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

Nota: De forma predeterminada, Receiver para Windows 4.4 permite a los usuarios seleccionar las aplicaciones que quieran mostrar en el menú Inicio.

- Modo de accesos directos solamente: Como administrador de Receiver, puede configurar Receiver para Windows 4.4 para que coloque automáticamente accesos directos de aplicaciones y escritorios en el menú Inicio o en el escritorio, de una manera similar al modo en que lo hace Receiver para Windows 3.4 Enterprise. El nuevo modo de *acceso directo solamente* permite a los usuarios buscar todas sus aplicaciones publicadas dentro del esquema de navegación de Windows estándar al que están acostumbrados.

Para obtener información acerca de la entrega de aplicaciones mediante XenApp y XenDesktop 7, consulte Creación de una aplicación para un grupo de entrega.

Nota: Incluya descripciones claras para las aplicaciones de los grupos de entrega. Las descripciones están visibles para los usuarios de Receiver cuando usan el acceso Web o el modo de autoservicio.
Para obtener más información sobre cómo configurar los accesos directos en el menú Inicio o en el escritorio, consulte Configuración del modo de accesos directos solamente en la documentación de productos de Citrix.

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.

Nota: De forma predeterminada, Receiver para Windows 4.4 permite a los usuarios seleccionar las aplicaciones que quieran mostrar en el menú Inicio.
En el modo de autoservicio se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

Agregue palabras clave en las descripciones de las aplicaciones de los grupos de entrega:

- Para hacer obligatoria una aplicación concreta, de forma que no pueda ser eliminada de Receiver para Windows, agregue la cadena KEYWORDS:Mandatory a la descripción de la aplicación. Los usuarios no tienen la opción Quitar para cancelar la suscripción a las aplicaciones obligatorias.
- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS:Auto a la descripción. 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.

Personalización de la ubicación de los accesos directos de las aplicaciones

El modo de integración de accesos directos en el menú Inicio y en el escritorio solamente le permite colocar los **accesos directos** de las aplicaciones publicadas en el menú Inicio y en el escritorio de Windows. De esta forma, los usuarios no tienen que suscribirse a las aplicaciones desde la interfaz de usuario de Receiver. La administración de la integración de accesos directos en el menú Inicio y en el escritorio proporciona una experiencia de escritorio perfecta para grupos de usuarios que necesitan acceder a un conjunto básico de aplicaciones de manera consistente.

Como administrador de Receiver, puede usar una marca de instalación en la línea de comandos, objetos de directiva de grupo, o parámetros del Registro para inhabilitar la interfaz normal de "autoservicio" de Receiver y sustituirla por un menú Inicio preconfigurado. El indicador se llama SelfServiceMode y está establecido en true de forma predeterminada. Cuando el administrador establece el indicador SelfServiceMode en false, el usuario pierde el acceso a la interfaz de usuario de autoservicio de Receiver. En su lugar, el usuario puede acceder a las aplicaciones suscritas desde el menú Inicio y a través de accesos directos de escritorio, lo que se conoce como **modo de acceso directo solamente**.

Los usuarios y los administradores pueden usar una serie de parámetros de Registro para personalizar el modo en que se configuran los accesos directos. Consulte Uso de las claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones.

Cómo trabajar con accesos directos

- Los usuarios no pueden quitar las aplicaciones. Todas las aplicaciones son obligatorias cuando se trabaja con el indicador SelfServiceMode establecido en false (modo de acceso directo solamente). Si el usuario quita un icono de acceso directo en el escritorio, el icono vuelve a aparecer cuando selecciona Actualizar en el icono de Receiver en la bandeja del sistema.
- Los usuarios solo pueden configurar un almacén. Las opciones Cuenta y Preferencias no están disponibles. Esto es para evitar que el usuario pueda configurar más almacenes. El administrador puede dar a un usuario privilegios especiales para agregar más de una cuenta usando la plantilla de objeto de directiva de grupo, o agregando manualmente una clave de Registro (HideEditStoresDialog) en la máquina cliente. Cuando el administrador da este privilegio a un usuario, el usuario tiene la opción Preferencias en el icono de la bandeja del sistema, desde donde puede agregar y quitar cuentas.
- Los usuarios no pueden quitar las aplicaciones mediante el Panel de control de Windows.
- Puede agregar accesos directos de escritorio a través de un parámetro de Registro personalizable. Los accesos directos de escritorio no se agregan de forma predeterminada. Después de realizar cualquier cambio en la configuración del Registro, Receiver debe reiniciarse.
- Los accesos directos se crean en el menú Inicio con una ruta de categoría predeterminada: UseCategoryAsStartMenuPath.

Nota: Windows 8/8.1 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con XenApp.

- Puede agregar un indicador [/DESKTOPDIR="nombre de directorio"] durante la instalación para reunir todos los accesos directos en una misma carpeta. CategoryPath se admite para los accesos directos de escritorio.
- La reinstalación automática de aplicaciones modificadas es una funcionalidad que se puede habilitar mediante la clave de Registro AutoReInstallModifiedApps. Cuando AutoReInstallModifiedApps está habilitada, los cambios que se hagan en los atributos de aplicaciones y escritorios publicados en el servidor se reflejarán en la máquina cliente. Cuando AutoReInstallModifiedApps está inhabilitada, los atributos de las aplicaciones y escritorios no se actualizan y los accesos directos no vuelven a aparecer al actualizar, si han sido eliminados del cliente. De manera predeterminada, AutoReInstallModifiedApps está habilitada. Consulte Uso de las claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones.

Uso de la plantilla de objetos de directiva de grupo para personalizar las ubicaciones de los accesos directos de aplicaciones

Nota: Debe realizar cambios en las directivas de grupo antes de configurar un almacén. Siempre que usted o un usuario quieran personalizar las directivas de grupo, deben restablecer Receiver, configurar la directiva de grupo en cuestión y luego reconfigurar el almacén.

Como administrador, puede configurar los accesos directos mediante directivas de grupo.

1. Para abrir el Editor de directivas de grupo local, ejecute el comandogpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar, vaya a la carpeta Configuration de Receiver y seleccione receiver.admx (o receiver.adml). Para obtener más información acerca de la plantilla ADMX, consulte About ADMX Template Usage.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para volver al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Self Service.
7. Seleccione Manage SelfServiceMode para habilitar o inhabilitar la interfaz de usuario de autoservicio de Receiver.
8. Elija Manage App Shortcut para habilitar o inhabilitar:
   - Accesos directos en el escritorio
   - Accesos directos en el menú Inicio
   - Directorio en el escritorio
   - Directorio en el menú Inicio
   - Ruta de categoría para accesos directos
   - Quitar aplicaciones al cerrar la sesión
   - Quitar aplicaciones al salir
9. Elija Allow users to Add/Remove account para dar a los usuarios privilegios para agregar o quitar más de una cuenta.

Uso de las claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones

> **Nota**
>
> De forma predeterminada, las claves del Registro usan un formato de cadena.

Puede usar parámetros del Registro para personalizar los accesos directos. Puede establecer las claves del Registro en las siguientes ubicaciones. Cuando son aplicables, se aplican en el orden de preferencia listado.

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden obligar a instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Nota: Debe realizar cambios en las claves de Registro antes de configurar un almacén. Siempre que usted o un usuario quieran personalizar las claves de Registro, deben restablecer Receiver, configurar las claves del Registro y luego reconfigurar el almacén.
Claves de Registro para máquinas de 32 bits

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
		HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
DefaultDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	True en SelfServiceMode y False en NonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	El Registro no se crea durante la instalación.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE \Citrix\Dazzle

Claves de Registro para máquinas de 64 bits

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
		+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
		HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+IDAlmacén +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKCU\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
HideEditStoresDialog	True en SelfServiceMode y False en NonSelfServiceMode	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties
WSCSupported	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectAll	True	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal +\Properties

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
		HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	El Registro no se crea durante la instalación.	HKCU\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + IDalmacénPrincipal+\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

Uso de los parámetros de cuenta de StoreFront para personalizar las ubicaciones de los accesos directos de aplicaciones

Puede configurar accesos directos en el menú Inicio y en el escritorio desde el sitio de StoreFront. Se puede agregar la siguiente configuración en el archivo web.config en C:\inetpub\wwwroot\Citrix\Roaming en la sección :

- Para poner los accesos directos en el escritorio, use PutShortcutsOnDesktop. Parámetros: "true" o "false" (predeterminado: false).
- Para poner los accesos directos en el menú Inicio, use PutShortcutsInStartMenu. Parámetros: "true" o "false" (predeterminado: true).
- Para usar la ruta de categoría en el menú Inicio, UseCategoryAsStartMenuPath. Parámetros: "true" o "false" (predeterminado: true).

Nota: Windows 8/8.1 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con XenApp.

- Para establecer un único directorio para todos los accesos directos en el menú Inicio, use StartMenuDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para volver a instalar aplicaciones modificadas, use AutoReinstallModifiedApps. Parámetros: "true" o "false" (predeterminado: true).
- Para mostrar un único directorio para todos los accesos directos en el escritorio, use DesktopDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para no crear una entrada en el panel 'Agregar o quitar programas' del cliente, use DontCreateAddRemoveEntry. Parámetros: "true" o "false" (predeterminado: false).
- Para quitar los accesos directos y el icono de Receiver de una aplicación que previamente estuvo disponible en el almacén pero ya no lo está, use SilentlyUninstallRemovedResources. Parámetros: "true" o "false" (predeterminado: false).

En el archivo web.config, los cambios se deben agregar en la sección XML de la cuenta. Para encontrar esta sección, busque la etiqueta de apertura:

La sección termina con la etiqueta .
Antes del final de la sección , en la primera sección de propiedades:

Se pueden agregar propiedades a esta sección después de la etiqueta , una por línea, con el nombre y el valor. Por ejemplo:

Nota: Los elementos de propiedad agregados antes de la etiqueta pueden invalidarlos. Puede optar por quitar la etiqueta al agregar un nombre y un valor de propiedad.
El siguiente es un ejemplo ampliado para esta sección:

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Uso de los parámetros de aplicación en XenApp y XenDesktop 7.x para personalizar las ubicaciones de los accesos directos de las aplicaciones

Receiver puede configurarse para que coloque automáticamente los accesos directos de los escritorios y aplicaciones directamente en el menú Inicio o en el escritorio. Esta función era similar a las versiones anteriores de Receiver. Sin embargo, la versión 4.4 incluyó la capacidad de controlar la ubicación de los accesos directos de las aplicaciones mediante los parámetros de aplicación de XenApp. Esta función resulta útil en entornos donde hay unas cuantas aplicaciones que es necesario mostrar en ubicaciones coherentes.

Si desea establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros de aplicación de XenApp:

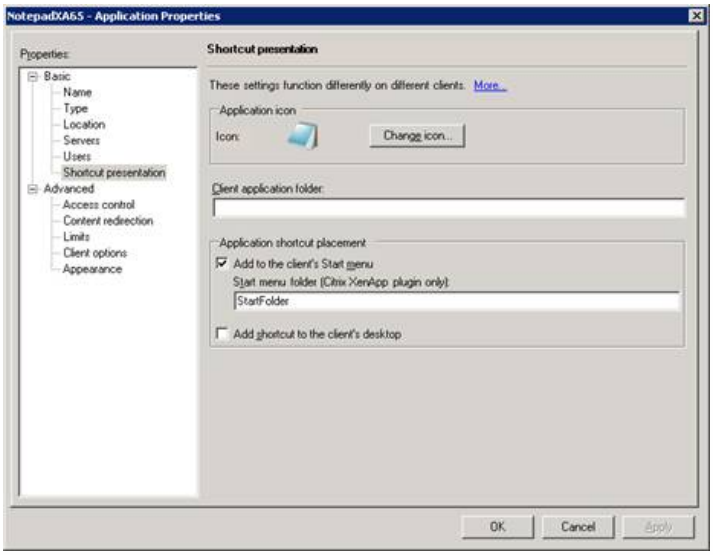
Si quiere usar parámetros de aplicación para determinar dónde se colocarán las aplicaciones, independientemente de si se usa el modo de autoservicio o el modo de menú Inicio...	configure Receiver con **PutShortcutsInStartMenu=false** y habilite los parámetros por aplicación. Nota: Este parámetro solo es aplicable a sitios de Interfaz Web.

Nota: El parámetro **PutShortcutsInStartMenu=false** es aplicable a XenApp 6.5 y XenDesktop 7.x.

Configurar parámetros de aplicación en XenApp 6.5

Para configurar un acceso directo de publicación para cada aplicación en XenApp 6.5:

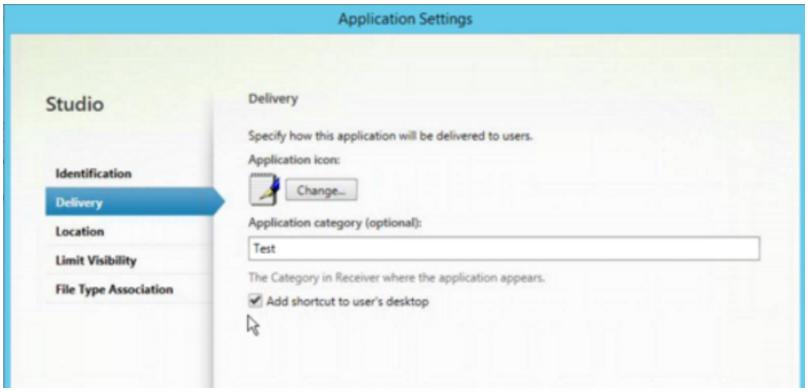
1. En la pantalla Propiedades de la aplicación de XenApp, expanda las propiedades Básicas.
2. Seleccione la opción de Presentación del acceso directo.
3. En la sección Ubicación del acceso directo de la aplicación en la pantalla Presentación del acceso directo, seleccione Agregar al menú Inicio del cliente. Después de seleccionar la casilla de verificación, escriba el nombre de la carpeta donde desea colocar el acceso directo. Si no se especifica un nombre de carpeta, XenApp coloca el acceso directo en el menú Inicio, sin carpeta.
4. Seleccione Agregar un acceso directo en el escritorio del cliente para incluir el acceso directo en el escritorio de la máquina cliente.
5. Haga clic en Aplicar.
6. Haga clic en OK.



Uso de los parámetros de aplicación en XenApp 7.6 para personalizar las ubicaciones de los accesos directos de las aplicaciones

Para configurar un acceso directo de publicación para cada aplicación en XenApp 7.6:

1. En Citrix Studio, busque la pantalla Configuración de la aplicación.
2. En la pantalla Configuración de la aplicación, seleccione Entrega. En esta pantalla, puede especificar cómo se entregarán las aplicaciones a los usuarios.
3. Seleccione el icono adecuado para la aplicación. Haga clic en Cambiar para buscar la ubicación de un icono.
4. En el campo de Categoría de la aplicación, de forma optativa, puede especificar la categoría de Receiver en la que aparece la aplicación. Por ejemplo, si está agregando accesos directos a aplicaciones de Microsoft Office, escriba Microsoft Office.
5. Marque la casilla Agregar acceso directo al escritorio del usuario.
6. Haga clic en Aceptar.



Disminuir las demoras de enumeración o firma digital de código auxiliar de aplicaciones

Si los usuarios notan demoras en la enumeración de aplicaciones en cada inicio de sesión, o si hay necesidad de firmar digitalmente código auxiliar (stubs) de aplicaciones, Receiver proporciona funcionalidad para copiar los .EXE de código auxiliar desde un recurso compartido de red.

Esta funcionalidad requiere una serie de pasos a seguir:

1. Cree el código auxiliar de cada aplicación en la máquina cliente.
2. Copie el código auxiliar de las aplicaciones en una ubicación común, accesible desde un recurso compartido de red.

3. Si es necesario, prepare una lista blanca, o firme el código auxiliar con un certificado de empresa.
4. Agregue una clave del Registro para dejar que Receiver cree el código auxiliar copiándolo desde el recurso compartido de red.

Si RemoveappsOnLogoff y RemoveAppsonExit están habilitados, y los usuarios notan demoras en la enumeración de aplicaciones cada vez que inician una sesión, use la siguiente solución para reducir las demoras:

1. Use regedit para agregar HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true".
2. Use regedit para agregar HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true". HKCU tiene preferencia sobre HKLM.

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden obligar a instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Permita que una máquina use archivos ejecutables de código auxiliar almacenados en el recurso compartido de red:

1. En una máquina cliente cree ejecutables de código auxiliar para todas las aplicaciones. Para lograr esto, agregue todas las aplicaciones a la máquina mediante Receiver, Receiver genera los archivos ejecutables.
2. Después, tome los archivos stub de los ejecutables que encontrará en %APPDATA%\Citrix\SelfService. Solamente necesita los archivos .exe.
3. Copie los archivos ejecutables a un recurso compartido de red.
4. Ahora, para cada máquina cliente que se va a bloquear, establezca las siguientes claves del Registro:
    1. Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"
    2. Reg add HKLM\Software\Citrix\Dazzle /v
    3. CopyStubsFromCommonStubDirectory /t REG_SZ /d "true". También es posible configurar estos parámetros en HKCU, si lo prefiere. HKCU tiene preferencia sobre HKLM.
    4. Salga de Receiver y reinícielo para probar la configuración.

Ejemplo de casos de uso

Este tema proporciona casos de uso para los accesos directos de aplicaciones.

Permitir a los usuarios elegir lo que quieran ver en el menú Inicio (Autoservicio)

Si tiene decenas (o incluso cientos) de aplicaciones, es mejor permitir que los usuarios seleccionen qué aplicaciones quieren ver como favoritas y agregarlas al menú Inicio:

Si quiere que el usuario elija las aplicaciones que desea tener en su menú Inicio...	configure Receiver en modo de autoservicio. En este modo, también deberá configurar los parámetros de palabra clave *auto* (aprovisionada automáticamente) y *mandatory* (obligatoria) para las aplicaciones, según sea necesario.
Si desea que el usuario elija las aplicaciones que quiera colocar en su menú Inicio, pero también quiere colocar accesos directos específicos en el escritorio...	configure Receiver sin opciones y, a continuación, use parámetros para cada una de las aplicaciones que quiera mostrar en el escritorio. Use aplicaciones aprovisionadas automáticamente (*auto*) y obligatorias (*mandatory*), según sea necesario.

Menú Inicio sin accesos directos de aplicaciones

Si el usuario utiliza un equipo doméstico que usa toda la familia, es posible que no sea necesario o conveniente colocar accesos directos. En tales casos, lo más sencillo es usar el acceso por explorador Web; instale Receiver sin configuración alguna y vaya a Receiver para Web o a la Interfaz Web. También puede configurar Receiver para el acceso de autoservicio sin colocar accesos

directos en ningún lugar.

Si desea evitar que Receiver coloque accesos directos de aplicaciones en el menú Inicio automáticamente...	configure Receiver con PutShortcutsInStartMenu=False. Receiver no colocará aplicaciones en el menú Inicio, incluso en el modo de autoservicio, a menos que usted los coloque usando los parámetros de cada aplicación.

Todos los accesos directos de aplicaciones en el menú Inicio o en el escritorio

Si el usuario tiene solo unas cuantas aplicaciones, puede colocarlas todas en el menú Inicio o todas en el escritorio, o en una carpeta del escritorio.

Si desea que Receiver coloque todos los accesos directos de las aplicaciones en el menú Inicio automáticamente...	configure Receiver con SelfServiceMode=False. Todas las aplicaciones disponibles aparecerán en el menú Inicio.
Si quiere que se coloquen accesos directos de todas las aplicaciones en el escritorio...	configure Receiver con PutShortcutsOnDesktop = true. Todas las aplicaciones disponibles aparecerán en el escritorio.
Si quiere que todos los accesos directos se coloquen dentro de una carpeta en el escritorio...	configure Receiver con DesktopDir=Nombre de la carpeta de escritorio donde quiera las aplicaciones.

Parámetros de aplicación en XenApp 6.5 o 7.x

Si desea establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros de aplicación de XenApp:

Si quiere usar parámetros de aplicación para determinar dónde se colocarán las aplicaciones, independientemente de si se usa el modo de autoservicio o el modo de menú Inicio...	configure Receiver con **PutShortcutsInStartMenu=false** y habilite los parámetros por aplicación. Nota: Este parámetro solo es aplicable a sitios de Interfaz Web.

Aplicaciones en carpetas de categorías o en carpetas específicas

Si desea mostrar las aplicaciones en carpetas específicas use las siguientes opciones:

Si desea que los accesos directos de aplicaciones que Receiver coloca en el menú Inicio se muestren en su categoría (carpeta) asociada...	configure Receiver con UseCategoryAsStartMenuPath=True. Nota: Windows 8/8.1 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con XenApp.
Si quiere que las aplicaciones que Receiver coloca en el menú Inicio aparezcan en una carpeta específica...	configure Receiver con StartMenuDir=el nombre de la carpeta del menú Inicio.

Quitar aplicaciones al cerrar la sesión o al salir

Si no desea que un usuario pueda ver las aplicaciones de otro usuario cuando van a compartir un dispositivo de punto final, puede hacer que las aplicaciones se eliminen cuando el usuario cierra la sesión y sale:

Si desea que Receiver quite todas las aplicaciones al cerrar la sesión...	configure Receiver con RemoveAppsOnLogoff=True.
Si desea que Receiver quite las aplicaciones al salir...	configure Receiver con RemoveAppsOnExit=True.

Configuración de aplicaciones para el acceso a aplicaciones locales

Al configurar aplicaciones para acceso a aplicaciones locales:

- Para especificar que se debe usar una aplicación instalada localmente en lugar de una aplicación disponible en Receiver, añada la cadena KEYWORDS:prefer="patrón". Esta característica se conoce como Acceso a aplicaciones locales.
  Antes de instalar una aplicación en un equipo de usuario, Receiver busca los patrones especificados para ver si la aplicación está instalada localmente. Si lo está, Receiver se suscribe a la aplicación y no crea ningún acceso directo. Cuando el usuario inicia la aplicación desde la ventana de Receiver, Receiver inicia la aplicación instalada localmente (preferida).

  Si un usuario desinstala una aplicación preferida desde fuera de Receiver, la próxima vez que Receiver se actualiza, cancela la suscripción a la aplicación. Si un usuario desinstala una aplicación preferida desde dentro de la ventana de Receiver, Receiver cancela la suscripción a la aplicación pero no la desinstala.

  Nota: La palabra clave prefer se aplica cuando Receiver se suscribe a una aplicación. Si se añade la palabra clave después de haberse suscrito a la aplicación, esto no tiene efecto alguno.
  Puede especificar la palabra clave prefer varias veces para una aplicación. Solo se necesita una vez para aplicar la palabra clave a una aplicación. Estos patrones pueden usarse en cualquier combinación:

  - prefer="Nombre de aplicación"
    El patrón del nombre de la aplicación hará coincidir cualquier aplicación que contenga dicho nombre en el nombre del archivo de acceso directo. El nombre de aplicación puede ser una palabra o una frase. Para introducir frases hay que usar comillas. No se hacen coincidir palabras o rutas de archivo incompletas, y la coincidencia no distingue entre mayúsculas y minúsculas. El patrón de coincidencia de nombre de aplicación resulta útil para sobrescritura de parámetros realizadas manualmente por un administrador.

KEYWORDS:prefer=	**Acceso directo en Programas**	**¿Coincide?**
Word	\Microsoft Office\Microsoft **Word** 2010	Sí
"Microsoft Word"	\Microsoft Office**Microsoft Word** 2010	Sí

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
Consola	\McAfee\VirusScan **Console**	Sí
Virus	\McAfee\VirusScan Console	No
McAfee	\McAfee\VirusScan Console	No

- prefer="\\Carpeta1\Carpeta2\...\Nombre de aplicación"
  El patrón de la ruta absoluta coincide con la ruta completa del archivo de acceso directo, además del nombre completo de la aplicación en el menú Inicio. La carpeta Programas es una subcarpeta del directorio del menú Inicio, de modo que hay que incluirla en la ruta absoluta si el destino es una aplicación de esa carpeta. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación en XenDesktop.

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
"\\Programs\Microsoft Office\Microsoft Word 2010"	**\Programs\Microsoft Office\Microsoft Word 2010**	Sí
"\\Microsoft Office\"	\Programs\Microsoft Office\Microsoft Word 2010	No
"\\Microsoft Word 2010"	\Programs\Microsoft Office\Microsoft Word 2010	No
"\\Programs\Microsoft Word 2010"	**\Programs\Microsoft Word 2010**	Sí

- prefer="\Carpeta1\Carpeta2\...\Nombre de aplicación"
  El patrón de la ruta relativa coincide con la ruta relativa del archivo de acceso directo en el menú Inicio. La ruta relativa suministrada debe contener el nombre de la aplicación y puede, de manera optativa, incluir las carpetas donde reside el acceso directo. La coincidencia es correcta si la ruta del archivo de acceso directo termina con la ruta relativa suministrada. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación.

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
"\Microsoft Office\Microsoft Word 2010"	**\Microsoft Office\Microsoft Word 2010**	Sí
"\Microsoft Office\"	\Microsoft Office\Microsoft Word 2010	No
"\Microsoft Word 2010"	\Microsoft Office**\Microsoft Word 2010**	Sí
"\Microsoft Word"	\Microsoft Word 2010	No

Para obtener más información sobre otras palabras clave, consulte las "Recomendaciones adicionales" en Optimización de la

experiencia de usuario, en la documentación de StoreFront.

Configuración del entorno de XenDesktop

Jul 07, 2016

Los temas de esta sección describen cómo configurar el respaldo para USB, evitar que se atenúe la ventana de Desktop Viewer y configurar parámetros para varios usuarios y dispositivos.

Configuración del respaldo para USB en conexiones de XenDesktop y XenApp

El respaldo USB permite a los usuarios interactuar con una amplia variedad de dispositivos USB cuando se conectan con un escritorio virtual. Los usuarios pueden conectar dispositivos USB a sus equipos y esos dispositivos se pueden usar de manera remota en su escritorio virtual. Los dispositivos USB disponibles para la comunicación remota son, entre otros, las unidades flash, los teléfonos inteligentes, las impresoras, los escáneres, los reproductores MP3, los dispositivos de seguridad y las PC tabletas. Los usuarios de Desktop Viewer pueden controlar si los dispositivos USB se encuentran disponibles en el escritorio virtual utilizando una preferencia de la barra de herramientas.

Las características asíncronas de los dispositivos USB tales como cámaras Web, micrófonos, altavoces y auriculares reciben respaldo en entornos LAN típicos de baja latencia y alta velocidad. Esto permite a estos dispositivos interactuar con paquetes tales como Microsoft Office Communicator y Skype.

Los siguientes tipos de dispositivos reciben respaldo directamente en una sesión XenDesktop y XenApp, y por lo tanto no utilizan respaldo USB:

- Teclados
- Punteros (ratones)
- Tarjetas inteligentes

Nota: Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y punteros 3D) pueden configurarse para utilizar respaldo USB. Para obtener información sobre cómo configurar los teclados Bloomberg, consulte Configuración de teclados Bloomberg. Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte CTX 119722.
De manera predeterminada, ciertos tipos de dispositivos USB no reciben respaldo para comunicaciones remotas a través de XenDesktop y XenApp. Por ejemplo, un usuario puede tener una tarjeta de interfaz de red conectada a la placa del sistema mediante un dispositivo USB interno. Colocar este dispositivo en comunicación remota no sería apropiado. Los siguientes tipos de dispositivos USB no tienen respaldo predeterminado para ser utilizados en una sesión de XenDesktop:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Concentradores USB
- Adaptadores gráficos USB

Los dispositivos USB conectados a un concentrador se pueden conectar remotamente pero no el concentrador.

Los siguientes tipos de dispositivos USB no tienen respaldo predeterminado para ser utilizados en una sesión de XenApp:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Concentradores USB
- Adaptadores gráficos USB
- Dispositivos de sonido

- Dispositivos de almacenamiento masivo

Para obtener instrucciones sobre cómo modificar la gama de dispositivos USB disponibles para los usuarios, consulte Actualización de la lista de dispositivos USB que se encuentran disponibles para la comunicación remota.

Para obtener instrucciones sobre la redirección automática de dispositivos USB específicos, consulte CTX123015.

Funcionamiento del respaldo USB

Cuando un usuario conecta un dispositivo USB, éste se comprueba con la directiva USB y, si se lo admite, se lo coloca en comunicación remota con el escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, sólo estará disponible para el escritorio local.

Cuando un usuario conecta un dispositivo USB, se muestra una notificación para informar al usuario sobre el nuevo dispositivo. El usuario puede decidir qué dispositivos USB se comunican de forma remota con el escritorio virtual seleccionando los dispositivos de la lista cada vez que se conectan. También, el usuario puede configurar el respaldo USB para que todos los dispositivos USB que se conecten antes o durante una sesión se comuniquen automáticamente de forma remota con el escritorio virtual que esté en uso.

Dispositivos de almacenamiento masivo

Solo para dispositivos de almacenamiento masivo, además del respaldo USB, el acceso remoto está disponible mediante la asignación de unidades del cliente, que configura a través de la siguiente directiva de Citrix Receiver: Comunicación remota de dispositivos cliente > Asignación de unidades de cliente. Cuando se aplica esta directiva, en el momento en que los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas con letras de unidades asignadas.

Las principales diferencias entre los dos tipos de directivas de comunicación remota son las siguientes:

Función	**Asignación de unidades del cliente**	**Respaldo USB**
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de sólo lectura	Sí	No
Dispositivo para quitar con seguridad durante una sesión	No	Sí, si un usuario hace clic en Quitar hardware con seguridad en el área de notificación.

Si se habilitan las directivas de USB genérico y de asignación de unidades del cliente, y se inserta un dispositivo de almacenamiento masivo antes del inicio de una sesión, se lo redirigirá primero mediante la asignación de unidades del cliente antes de ser considerado para la redirección de USB genérico. Si se introduce después del inicio de una sesión, se redirigirá a través del respaldo USB antes de la asignación de unidades del cliente.

Clases de dispositivos USB que se admiten de manera predeterminada

Las reglas de directivas USB predeterminadas admiten distintas clases de dispositivos USB:

A pesar de que se encuentran enumeradas en esta lista, algunas clases están solo disponibles de forma remota en las sesiones de XenDesktop y XenApp después de una configuración adicional. Estos parámetros no se pueden configurar.

- Sonido (clase 01). Incluye los dispositivos de entrada de sonido (micrófonos), los dispositivos de salida de sonido y los controladores MIDI. Los dispositivos de sonido modernos generalmente utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior. El sonido (Class01) no es aplicable a XenApp, ya que estos dispositivos no están disponibles para la comunicación remota en XenApp mediante el respaldo USB.
  Nota: Algunos dispositivos específicos (por ejemplo, teléfonos VOIP) requieren una configuración adicional. Para obtener instrucciones adicionales, consulte CTX123015.
- Dispositivos de interfaz física (clase 05). Estos dispositivos son similares a los dispositivos de interfaz de usuario (HID) pero en general proporcionan respuesta o información en "tiempo real". Estos incluyen joystick con fuerza de respuesta, plataformas de movimiento y exoesqueletos con fuerza de respuesta.
- Digitalización de imágenes fijas (clase 06). Abarca los escáneres y las cámaras digitales. Las cámaras digitales suelen admitir la clase de digitalización de imagen fija que utiliza el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP) para transferir imágenes a un equipo u otro dispositivo periférico. Las cámaras también pueden aparecer como dispositivos de almacenamiento masivo y puede ser posible configurar una cámara para que utilice cualquiera de las clases mediante los menús de configuración que proporciona la cámara propiamente dicha. Tenga en cuenta que si una cámara se muestra como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se requiere respaldo USB.

- Impresoras (clase 07). En general, la mayoría de las impresoras se incluyen en esta clase, aunque algunas utilizan protocolos específicos del fabricante (clase ff). Las impresoras multifunción pueden tener un concentrador interno o ser dispositivos compuestos. En ambos casos, el elemento de impresión generalmente utiliza la clase de la impresora y el elemento de fax o de escaneado utiliza otra clase, por ejemplo, la digitalización de imágenes fijas.
  Las impresoras normalmente funcionan de forma adecuada sin el respaldo USB.

  Nota: Esta clase de dispositivo (en particular impresoras con funciones de escaneado) requiere configuración adicional. Para obtener instrucciones adicionales, consulte CTX123015.
- Almacenamiento masivo (clase 08). Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros incluyen las unidades de disco duro con conexión USB, las unidades de CD/DVD y los lectores de tarjetas SD/MMC. Existe una amplia variedad de dispositivos con almacenamiento interno que también presentan una interfaz de almacenamiento masivo y que incluyen los reproductores multimedia, las cámaras digitales y los teléfonos celulares. El almacenamiento masivo (clase 08) no es aplicable a XenApp, ya que estos dispositivos no están disponibles para la comunicación remota en XenApp mediante el respaldo USB. Las subclases conocidas, entre otras, son:
  - 01 Dispositivos flash limitados
  - 02 Dispositivos CD/DVD típicos (ATAPI/MMC-2)
  - 03 Dispositivos de cinta típicos (QIC-157)
  - 04 Unidades de disquete típicas (UFI)
  - 05 Unidades de disquete típicas (SFF-8070i)
  - 06 La mayoría de los dispositivos de almacenamiento masivo utiliza esta variante de SCSI

  A menudo se puede acceder a los dispositivos de almacenamiento masivo a través de la asignación de unidades del cliente y por lo tanto no se requiere el respaldo USB.

  Importante: Se sabe que algunos virus se propagan en forma activa utilizando todos los tipos de almacenamiento masivo. Considere cuidadosamente si existe o no una necesidad comercial de permitir el uso de los dispositivos de almacenamiento masivo, ya sea a través de la asignación de unidades del cliente o mediante el respaldo USB.
- Seguridad del contenido (clase 0d). Los dispositivos para seguridad del contenido aplican la protección del contenido, generalmente para la administración de derechos digitales o para la gestión de licencias. Esta clase incluye las llaves.

- Vídeo (clase 0e). La clase vídeo abarca los dispositivos que se utilizan para controlar vídeos o material relacionado con vídeos, como las cámaras web, videograbadoras digitales, conversores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión por secuencias de vídeo.
  Nota: La mayoría de los dispositivos de streaming por vídeo utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior. Algunos dispositivos de vídeo (por ejemplo, cámaras Web con detección de movimiento) requieren una configuración adicional. Para obtener instrucciones adicionales, consulte CTX123015.
- Atención médica personal (clase 0f). Estos dispositivos incluyen los dispositivos de atención médica personal como los sensores de presión arterial, los monitores de frecuencia cardíaca, podómetros, monitores de píldoras y espirómetros.
- Específico del proveedor y de la aplicación (clases fe y ff). Muchos dispositivos utilizan protocolos específicos del proveedor o protocolos no estandarizados por el consorcio USB, que generalmente se muestran como específicos del proveedor (clase ff).

Clases de dispositivos USB que se rechazan de manera predeterminada

Las siguientes clases de dispositivo USB se rechazan por las reglas de directiva de USB predeterminadas:

- Comunicaciones y control CDC (clases 02 y 0a) La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al propio escritorio virtual.
- Dispositivos de interfaz humana (HID) (clase 03) Incluye una amplia variedad de dispositivos de entrada y de salida. Los dispositivos de interfaz humana (HID, por su sigla en inglés) típicos son los teclados, punteros (como el ratón o Mouse), los dispositivos señaladores, las tabletas gráficas, los controladores de juegos, los botones y las funciones de control.
  La subclase 01 se conoce como la clase de "interfaz de arranque" y se utiliza para los teclados y punteros.

  La directiva USB predeterminada no permite teclados USB (clase 03, subclase 01, protocolo 1) ni punteros USB (clase 03, subclase 01, protocolo 2). Esto se debe a que la mayoría de los teclados y punteros se gestionan de manera apropiada sin respaldo USB y a que normalmente es necesario utilizar estos dispositivos de forma local y de forma remota cuando se conecta con un escritorio virtual.

- Concentradores USB (clase 09) Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.
- Tarjeta inteligente (clase 0b) Los lectores de tarjeta inteligente abarcan los lectores de tarjeta inteligente con contacto y sin contacto, y los tokens USB con un chip inteligente incluido que equivale a la tarjeta.
  Se accede a los lectores de tarjeta inteligente utilizando la comunicación remota de la tarjeta inteligente y no se requiere respaldo USB.

- Controlador inalámbrico (clase e0) Es posible que algunos de estos dispositivos proporcionen acceso de red crítico o conecten periféricos importantes, tales como punteros o teclados Bluetooth.
  La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso usando el respaldo USB.

- **Varios dispositivos de red (Clase ef, subclase 04)**. Es posible que algunos de estos dispositivos proporcionen acceso de red crítico. La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso usando el respaldo USB.

Actualización de la lista de dispositivos USB que se encuentran disponibles para la comunicación remota

Puede actualizar el rango de dispositivos USB disponibles para el acceso remoto a los escritorios en el archivo icaclient_usb.adm. Esto permite realizar cambios a Receiver mediante directivas de grupo. El archivo se localiza en la carpeta de instalación siguiente:

:\Archivos de programa\Citrix\ICA Client\Configuration\

O bien, se puede editar el Registro en cada dispositivo de usuario, agregando la siguiente clave de Registro:

HKLM\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden obligar a instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Las reglas predeterminadas del producto se almacenan en:

HKLM\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules" Value=

No edite las reglas predeterminadas del producto.

Para obtener más información acerca de las reglas y su sintaxis, consulte http://support.citrix.com/article/ctx119722/.

Configuración de teclados Bloomberg

Las sesiones de XenDesktop y XenApp respaldan el uso de teclados Bloomberg (pero no otros teclados USB). Los componentes obligatorios se instalan automáticamente cuando se instala el plug-in, pero se debe habilitar esta función durante la instalación o más tarde cambiando una clave del Registro.

No se recomienda iniciar varias sesiones con teclados Bloomberg en un único dispositivo de usuario. El teclado funciona correctamente en entornos de una sesión.

Para habilitar o inhabilitar el respaldo para teclados Bloomberg

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

1. Busque la siguiente clave en el Registro:
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. Lleve a cabo una de las siguientes acciones:
   - Para habilitar esta función, configure la entrada DWORD y el nombre EnableBloombergHID con el valor 1.
   - Para inhabilitar esta función, establezca el valor en 0.

Para impedir que la ventana de Desktop Viewer se atenúe

Si utiliza varias ventanas de Desktop Viewer, de manera predeterminada se atenúan los escritorios que no están activos. Si necesita ver varios escritorios de forma simultánea, esto puede hacer que la información que se incluye en ellos sea ilegible. Se puede desactivar el comportamiento predeterminado e impedir que la ventana de Desktop Viewer se atenúe editando el Registro.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

1. En el dispositivo de usuario, cree un registro REG_DWORD denominado DisableDimming en una de las siguientes claves

dependiendo de si quiere impedir la atenuación para el usuario actual del dispositivo o para el dispositivo propiamente dicho. Ya existe un registro si Desktop Viewer se ha utilizado en el dispositivo:

- HKCU\Software\Citrix\XenDesktop\DesktopViewer
- HKLM\Software\Citrix\XenDesktop\DesktopViewer

O bien, en lugar de controlar la atenuación con los parámetros de dispositivo o de usuario anteriores, puede definir una directiva local creando el mismo registro REG_WORD en una de las siguientes claves:

- HKCU\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKLM\Software\Policies\Citrix\XenDesktop\DesktopViewer

El uso de estas claves es opcional porque los administradores de XenDesktop, en lugar de los usuarios o administradores de plug-ins, generalmente controlan los parámetros de la directiva mediante las directivas de grupo. Por lo tanto, antes de utilizar estas claves, compruebe si el administrador de XenDesktop ha establecido una directiva para esta función.

2. Establezca la entrada en cualquier valor distinto de cero, como 1 o true (verdadero).

   Si no se especifican entradas o si esta se establece en 0, la ventana de Desktop Viewer se atenúa. Si se especifican varios registros, se utiliza la siguiente prioridad. El primer registro que se ubica en esta lista, y su valor, determinan si la ventana se atenúa:

   1. HKCU\Software\Policies\Citrix\...
   2. HKLM\Software\Policies\Citrix\...
   3. HKCU\Software\Citrix\...
   4. HKLM\Software\Citrix\...

Para configurar parámetros para varios usuarios y dispositivos

Además de las opciones de configuración de la interfaz de usuario de Receiver, se puede utilizar el Editor de directivas de grupo y el archivo de plantilla icaclient.adm para configurar los parámetros. Con el Editor de directivas de grupo se puede:

- Extender la plantilla icaclient para que cubra todos los parámetros de Receiver mediante la modificación del archivo icaclient.adm. Consulte la documentación de directivas de grupo de Microsoft para mayor información sobre la modificación de los archivos .adm y sobre la aplicación de parámetros en determinados equipos.
- Realizar cambios que se aplican solamente a usuarios específicos o a todos los usuarios de un dispositivo cliente.
- Configurar parámetros para varios dispositivos de usuario.

Citrix recomienda la utilización de directivas de grupo para configurar los dispositivos de usuario de forma remota; sin embargo, es posible utilizar cualquier método, incluso el Editor del Registro, que actualiza las entradas correspondientes del Registro.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.

   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.

6. En el nodo Configuración de usuario o el nodo Configuración del equipo, modifique los parámetros pertinentes según sea necesario.

Configuración de StoreFront

Jul 19, 2016

Citrix StoreFront autentica a los usuarios en XenDesktop, XenApp y VDI-in-a-Box, y enumera y agrupa los escritorios y las aplicaciones disponibles en almacenes, a los que los usuarios acceden mediante Citrix Receiver.

Además de la configuración resumida en esta sección, es necesario configurar NetScaler Gateway o Access Gateway para permitir que los usuarios se conecten desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet o ubicaciones remotas).

> **Nota**
>
> Citrix Receiver para Windows siempre muestra la interfaz de usuario de StoreFront antigua (con el diseño de burbujas verdes) en lugar de la interfaz de usuario actualizada después de seleccionar la opción para mostrar Todas las cuentas.

Para configurar StoreFront

1. Instale y configure StoreFront como se describe en la documentación de StoreFront. Receiver para Windows necesita una conexión HTTPS. Si el servidor StoreFront está configurado para HTTP, es necesario definir una clave de Registro en el dispositivo de usuario, según se describe en Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos, bajo la descripción de la propiedad ALLOWADDSTORE.
   Nota: Para los administradores que necesitan más control, Citrix ofrece una plantilla que se puede usar para crear un sitio de descargas de Receiver.

Administrar la reconexión del control del área de trabajo

El control del área de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo. Esto permite, por ejemplo, que los médicos, en los hospitales, se trasladen de una estación de trabajo a otra sin tener que reiniciar sus aplicaciones en cada dispositivo. En Receiver para Windows, el control del área de trabajo en los dispositivos cliente se administra mediante la modificación del Registro. Esto también puede llevarse a cabo con Directivas de grupo en dispositivos que pertenecen a dominios.

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

Cree WSCReconnectModeUser y modifique la clave de Registro existente WSCReconnectMode en la imagen maestra de escritorio o en el host del servidor XenApp. El escritorio publicado puede cambiar el comportamiento de Receiver.

Parámetros de clave de WSCReconnectMode para Receiver para Windows:

- 0 = No reconectar ninguna sesión existente
- 1 = Reconectar al iniciar una aplicación
- 2 = Reconectar al actualizar una aplicación
- 3 = Reconectar al iniciar o actualizar una aplicación
- 4 = Reconectar cuando se abra la interfaz de Receiver
- 8 = Reconectar al iniciar sesión en Windows
- 11 = Combinación de las opciones 3 y 8

Inhabilitación del control del área de trabajo para Receiver para Windows

Para inhabilitar el control del área de trabajo para Receiver para Windows, cree la siguiente clave:

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle para (32 bits)

Nombre: **WSCReconnectModeUser**

Tipo: REG_SZ

Información del valor: 0

Modifique la clave siguiente desde el valor predeterminado de 3 a cero

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle (32 bits)

Nombre: **WSCReconnectMode**

Tipo: REG_SZ

Información del valor: 0

Nota: Si lo prefiere, puede definir el valor REG_SZ de WSCReconnectAll como "false" para no crear una clave nueva.

Cambio del tiempo de espera del indicador de estado

Puede cambiar el tiempo que se muestra el indicador de estado cunado el usuario inicia una sesión. Para cambiar el tiempo de espera, cree el valor REG_DWORD: SI INACTIVE MS, en HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\. El valor REG_DWORD puede establecerse en 4 si quiere que el indicador de estado desparezca más pronto.

Advertencia

Si edita el Registro de forma incorrecta pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

Configuración de Receiver con la plantilla de objeto de directiva de grupo

Jan 20, 2017

Agregar o especificar almacenes mediante un objeto de directiva de grupo (GPO)

Citrix recomienda usar el objeto de directiva de grupo y el archivo de plantilla receiver.admx, receiver.adm o receiver.adml (según el sistema operativo) para configurar los parámetros relacionados con Citrix Receiver para Windows.

Nota

El archivo receiver.admx o receiver.adml está disponible en Windows Vista, Windows Server 2008 o una versión posterior. Los archivos ADM están disponibles únicamente en las plataformas Windows XP Embedded.

Nota

Si Citrix Receiver para Windows se configura mediante la instalación de VDA, los archivos ADMX o ADML se encuentran en el directorio de instalación de Citrix Receiver para Windows. Por ejemplo: <directorio de instalación>\online plugin\Configuration.

Consulte la tabla siguiente para ver información sobre los archivos de plantillas de Citrix Receiver para Windows y su ubicación respectiva.

Tipo de archivo	Ubicación del archivo
receiver.adm	<Directorio de instalación>\ICA Client\Configuration
receiver.admx	<Directorio de instalación>\ICA Client\Configuration
receiver.adml	<Directorio de instalación>\ICA Client\Configuration\[MUIculture]

Nota

Citrix recomienda usar los archivos de plantilla proporcionados con la versión más reciente de Citrix Receiver para Windows. Los parámetros que tenga se conservan aunque importe archivos de versiones más recientes.

Para agregar archivos de plantilla ADM al objeto de directiva de grupo local

Nota: Puede utilizar archivos de plantilla ADM para configurar los objetos de directiva de grupo locales y objetos de directiva de grupo basados en dominios.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
Nota: Si ya ha importado la plantilla de Citrix Receiver para Windows en el Editor de directivas de grupo, puede omitir los pasos de 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione "Agregar" y vaya a la ubicación del archivo de plantilla <Directorio de instalación>\ICA Client\Configuration\receiver.adm
5. Seleccione "Abrir" para agregar la plantilla y, luego, haga clic en "Cerrar" para volver al Editor de directivas de grupo.
El archivo de la plantilla de Citrix Receiver para Windows estará disponible en el objeto de directiva de grupo local, en Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver.
Una vez que los archivos de plantilla ADM se agreguen al objeto de directiva de grupo local, aparecerá el siguiente mensaje: "The following entry in the [strings] section is too long and has been truncated" (La siguiente entrada en la sección [cadenas] es demasiado larga y se ha cortado):
Haga clic en Aceptar para ignorar el mensaje.

Para agregar archivos de plantilla ADMX o ADML al objeto de directiva de grupo local

NOTA: Puede utilizar archivos de plantilla ADMX o ADML para configurar los objetos de directiva de grupo locales y/o aquellos que utilizan dominios. Consulte aquí el artículo de Microsoft MSDN acerca de la administración de archivos ADMX.
1. Después de instalar Citrix Receiver para Windows, copie los archivos de plantilla.

ADMX:
De: <Directorio de instalación>\ICA Client\Configuration\receiver.admx
A: %systemroot%\policyDefinitions

ADML:
De: <Directorio de instalación>\ICA Client\Configuration\[MUIculture]receiver.adml
A: %systemroot%\policyDefinitions\[MUIculture]

El archivo de plantilla de Citrix Receiver para Windows está disponible en el objeto de directiva de grupo local, en el directorio Plantillas administrativas > Componentes de Citrix > Citrix Receiver.

Citrix recomienda usar el archivo de plantilla de objeto de directiva de grupo (GPO) icaclient.adm para configurar reglas para enrutamiento de red, servidores proxy, configuración de servidores de confianza, enrutamiento de usuarios, dispositivos de usuario remotos y experiencia de usuario.

Puede utilizar el archivo de plantilla icaclient.adm con directivas de dominio y de equipos locales. Para las directivas de dominio, importe el archivo de plantilla mediante la Consola de administración de directivas de grupo. Esto resulta de gran ayuda para aplicar la configuración de Citrix Receiver a diferentes dispositivos de usuario en la empresa. Para afectar un solo dispositivo de usuario, importe el archivo de plantilla mediante el Editor de directivas de grupo local del dispositivo.

Configuración de Receiver con la plantilla de objetos de directiva de grupo

Nota

Citrix recomienda usar los archivos de plantilla de objetos de directiva de grupo (GPO) proporcionados con la versión más reciente de Citrix Receiver. Los parámetros anteriores se conservan aunque importe archivos de versiones más recientes.

Acerca de TLS y las directivas de grupo

Use esta directiva para configurar las opciones de TLS que garantizan que Citrix Receiver identifique de forma segura el servidor al que se está conectando; úsela también para cifrar todas las comunicaciones con el servidor. Citrix recomienda que se use TLS en las conexiones a través de redes no seguras. Citrix admite protocolos TLS 1.0, TLS 1.1 y TLS 1.2 entre Receiver y XenApp o XenDesktop.

Si esta directiva está habilitada, puede forzar Receiver a que use TLS para todas las conexiones a aplicaciones y escritorios publicados. Para ello, marque la casilla "Requerir SSL para todas las conexiones".

Citrix Receiver identifica al servidor por el nombre que figura en el certificado de seguridad que el servidor presenta. Este tiene el formato de nombre DNS (por ejemplo, www.citrix.com). Puede restringir Receiver para que se conecte solo a determinados servidores, especificados mediante una lista separada por comas en el parámetro de servidores SSL permitidos (Allowed SSL servers). Aquí se pueden indicar comodines y números de puerto; por ejemplo, *.citrix.com:4433 permite la conexión a un servidor cuyo nombre común termine en .citrix.com en el puerto 4433. La precisión de la información que contenga un certificado de seguridad es responsabilidad del emisor del certificado. Si Receiver no reconoce ni confía en el emisor de un certificado, se rechaza la conexión.

En las conexiones con el protocolo TLS, el servidor puede configurarse para exigir que Receiver proporcione un certificado de seguridad que lo identifique. Use el parámetro de autenticación de cliente (Client Authentication) para definir si la identificación se proporciona automáticamente o si se notifica al usuario. Entre las opciones se incluyen:

- nunca proporcionar identificación
- usar solo el certificado configurado aquí
- solicitar siempre al usuario que seleccione un certificado
- solicitar al usuario solo si se pueden elegir los certificados que se van a facilitar

Sugerencia

Use el parámetro "Client Certificate" para especificar la huella digital del certificado de identificación para evitar tener que preguntar al usuario innecesariamente.

Cuando verifique el certificado de seguridad del servidor, puede configurar el plug-in para que se ponga en contacto con el emisor del certificado y se obtenga una lista de revocación de certificados (CRL). De esta manera, se puede comprobar que el certificado del servidor no haya sido revocado. Esto permite que los emisores puedan invalidar un certificado si este pone el sistema en peligro. Use el parámetro de verificación de la lista de revocación de certificados (CRL verification) para configurar el plug-in con el objetivo de:

- no comprobar las listas de revocación de certificados
- solo comprobar las listas de revocación de certificados que ya se hayan obtenido del emisor
- obtener activamente una lista de revocación de certificados actualizada

- no conectarse a menos que se pueda obtener una lista de revocación de certificados actualizada

Las empresas que configuran TLS para una serie de productos pueden optar por identificar servidores pensados para plug-ins de Citrix al especificar un identificador de objeto de directivas de certificados como parte del certificado de seguridad. Si se configura aquí un identificador de objeto de directivas, Receiver solo aceptará los certificados que declaren una directiva compatible.

Algunas directivas de seguridad presentan requisitos relacionados con los algoritmos de cifrado usados para una conexión. Puede restringir el plug-in para que use solo las versiones 1.0, 1.1 y 1.2 de TLS con el parámetro de versión de TLS (TLS version). Del mismo modo, puede restringir el plug-in para que use solo determinados conjuntos de cifrado. Estos conjuntos de cifrado son:

Conjuntos de cifrado gubernamentales:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384

Conjuntos de cifrado comerciales:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_AES_128_GCM_SHA256

Conformidad con el estándar FIPS de seguridad

Citrix Receiver para Windows 4.4 introduce TLS y opciones de configuración del modo de conformidad con estándares para configurar FIPS (Federal Information Processing Standards). Use esta función para asegurarse de que solo se utiliza la criptografía aprobada por FIPS (Publication 140-2) para todas las conexiones ICA.

Hay un nuevo modo de conformidad con estándares de seguridad para dar respaldo a NIST SP 800-52. De forma predeterminada, este modo está inhabilitado (tiene el valor NONE).

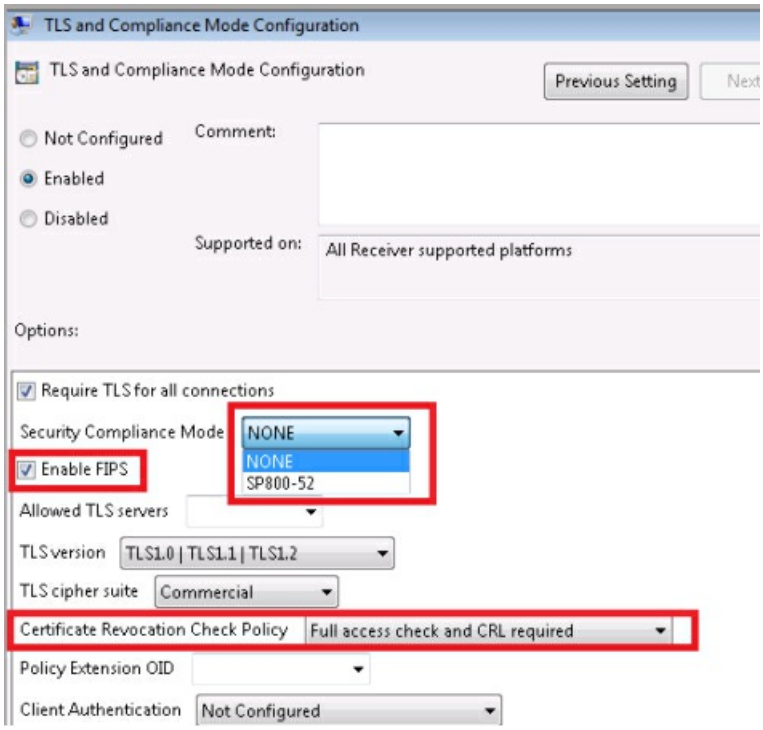
> **Nota**
>
> Para obtener información adicional sobre el modo de conformidad requerido para NIST SP 800-52, consulte la página de NIST que describe las directrices a seguir para implementaciones de TLS.

Esta versión de Citrix Receiver también permite definir la versión de TLS, que determina el protocolo TLS para las conexiones ICA. Se seleccionará la versión más alta que esté mutuamente disponible entre el cliente y el servidor.

Al usar estas características, en la pantalla TLS and Compliance Mode Configuration:

- Marque la casilla Enable FIPS para usar la criptografía aprobada para todas las sesiones ICA.
- Defina Security Compliance Mode con el valor SP 800-52.
- Seleccione la versión de TLS.

La imagen siguiente ilustra las opciones de FIPS:



> ## Nota
>
> De manera predeterminada, FIPS está inhabilitado (no está marcado).

Configuración de FIPS

Para configurar la criptografía de FIPS entre todos los clientes ICA:

1. Seleccione Configuración del equipo > Plantillas administrativas > Citrix Components > Network Routing > **TLS and Compliance Mode Configuration**.
2. En la pantalla TLS and Compliance Mode Configuration, seleccione **Enable FIPS**.
3. En la sección Security Compliance Mode, seleccione **SP 800-52** en el menú desplegable. Al configurar esta opción:
   - El modo de conformidad SP 800-52 requiere conformidad FIPS; cuando se habilita SP 800-52, el modo FIPS también se habilita independientemente de cómo esté configurado el parámetro FIPS.
   - La directiva Certificate Revocation Check es *Full access check and CRL required* o *Full access check and CRL required all*.
4. Seleccione la versión adecuada del protocolo TLS para las conexiones ICA; se seleccionará la versión más alta que esté mutuamente disponible en el cliente y el servidor. Las opciones son:
   - TLS 1.0 | TLS 1.1 | TLS 1.2 (valor predeterminado)
   - TLS 1.1 | TLS 1.2
   - TLS 1.2

Acerca del uso de plantillas ADMX

Con la publicación de StoreFront 3.0 y Citrix Receiver 4.3, Citrix XenApp y XenDesktop admiten el nuevo formato de Microsoft diseñado para mostrar opciones de configuración de directiva basadas en el Registro mediante un formato de

archivo XML basado en estándares, conocido como archivos ADMX.

En Windows Vista/Windows Server 2008 o versiones posteriores, estos archivos sustituyen a los archivos ADM, que utilizaban su propio lenguaje de marcado. Los archivos ADM siguen estando disponibles para las plataformas Windows XP Embedded. Las herramientas administrativas que se necesitan, el Editor de objetos de directiva de grupo y la Consola de administración de directivas de grupo no presentan grandes cambios. En la mayoría de los casos, no notará la presencia de los archivos ADMX durante las tareas diarias de administración de directivas de grupo.

Una de las principales ventajas de utilizar los nuevos archivos ADMX es el almacén central. Se le ofrece esta opción cuando administra objetos de directiva de grupo basados en un dominio, aunque el almacén central no se usa de forma predeterminada. A diferencia de los casos en los que se utilizaban archivos ADM, el Editor de objetos de directiva de grupo no copiará los archivos ADMX a cada objeto de directiva de grupo modificado, sino que proporcionará la capacidad de lectura tanto desde una ubicación única de nivel de dominio en el volumen del sistema del controlador de dominio (no configurable por el usuario) como desde la estación de trabajo administrativa local si el almacén central no está disponible. Para compartir un archivo ADMX personalizado, debe copiar ese archivo al almacén central, lo que hace que esté disponible automáticamente para todos los administradores de directiva de grupo en un dominio. Esta función simplifica la administración de directivas y mejora la optimización del almacenamiento de archivos GPO.

Los archivos ADMX se dividen en recursos independientes de idioma (ADMX) y específicos de idioma (ADML), disponibles para todos los administradores de directivas de grupo. Estos factores permiten que las herramientas de directiva de grupo ajusten la interfaz de usuario de acuerdo con el idioma configurado del administrador.

Nota

Puede obtener más información en este artículo de Microsoft MSDN acerca de la administración de archivos ADMX.

Ubicaciones y nombres de archivos ADMX y ADML

Se ha mejorado la convención de nomenclatura de los archivos ADM (proporcionados en la versión anterior de Receiver). En la tabla siguiente, se muestra la asignación de los archivos ADM a sus nuevos nombres de archivo ADMX:

Versión de Citrix Receiver (anterior a 4.3)	Versión de Citrix Receiver (4.3 y posteriores)
Icaclient.adm	receiver.admx \ receiver.adm
Icaclient_usb.adm	receiver_usb.admx \ receiver_usb.adm
ica-file-signing.adm	ica-file-signing.admx \ ica-file-signing.admx
HdxFlash-Client.adm	HdxFlash-Client.admx \ HdxFlash-Client.admx

Nota

Use los archivos .admx en Windows Vista/Windows Server 2008 y versiones posteriores; use los archivos .adm en las demás plataformas.

Puede copiar archivos ADMX y ADML personalizados y distribuidos al almacén central con el programa de instalación de Citrix Receiver, lo que hace que estén disponibles automáticamente para todos los administradores de directivas de grupo presentes en un dominio. En la tabla siguiente, se muestra la ubicación donde se deben copiar los archivos ADMX y ADML:

Tipo de archivo	Ubicación de archivos
receiver.admx	\ICA Client\Configuration
ica-file-signing.admx	\ICA Client\Configuration
receiver_usb.admx	\ICA Client\Configuration\en
HdxFlash-Client.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration
ica-file-signing.adml	\ICA Client\Configuration
receiver_usb.adml	\ICA Client\Configuration\en
HdxFlash-Client.adml	\ICA Client\Configuration\[MUIculture]

Nota

Si Citrix Receiver se configura mediante la instalación de VDA, los archivos ADMX o ADML se pueden encontrar en el directorio de instalación. Por ejemplo: \online plugin\Configuration.

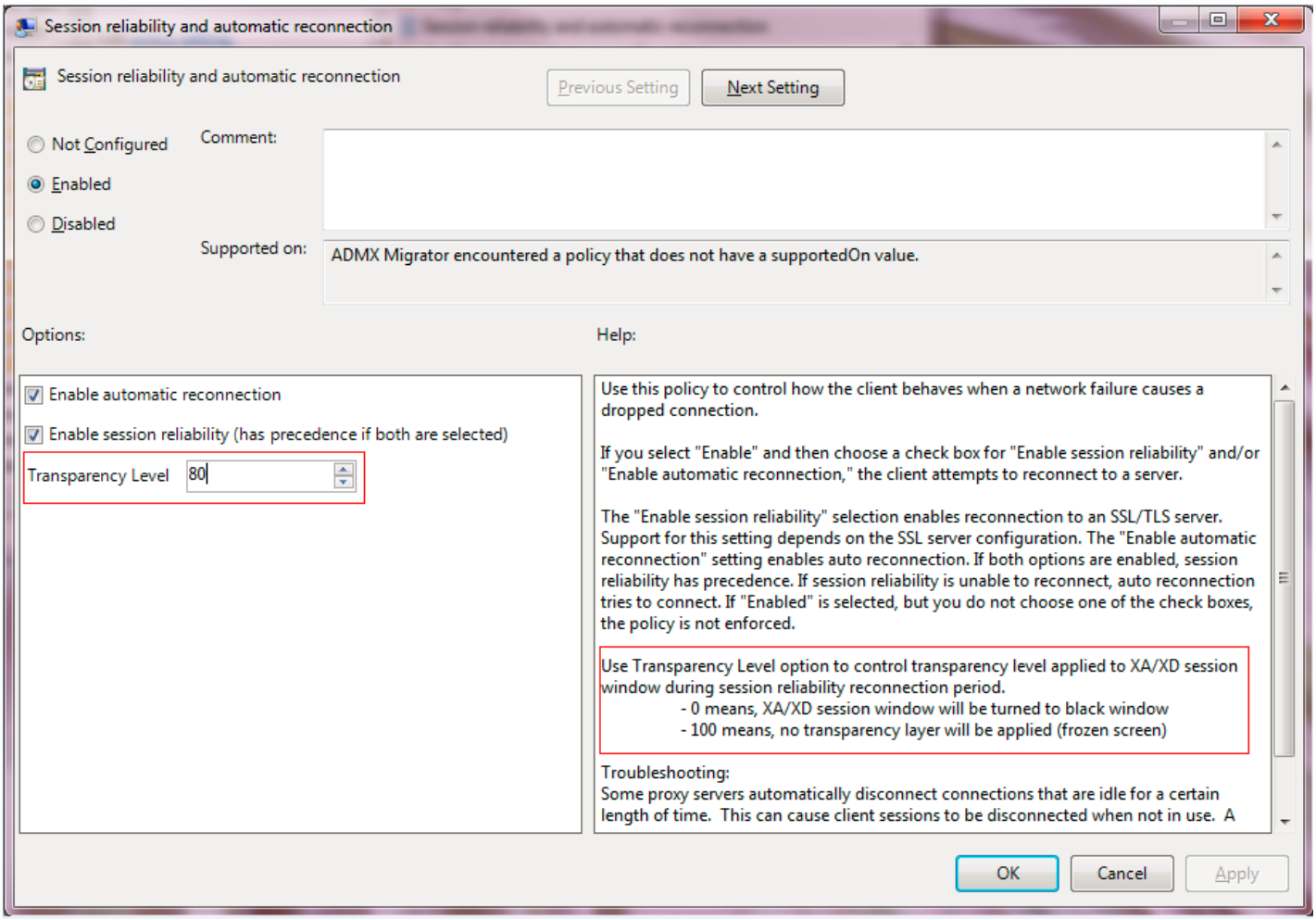
Directiva de grupo de fiabilidad de la sesión

Al configurar la directiva de grupo de fiabilidad de la sesión, puede definir el nivel de transparencia. Con esta opción se puede controlar el nivel de transparencia que se aplica a un escritorio o una aplicación publicada durante el periodo de reconexión de fiabilidad de la sesión.

Para configurar el nivel de transparencia, seleccione **Configuración del equipo -> Plantillas administrativas -> Citrix Components -> Network Routing -> Session reliability and automatic reconnection -> Transparency Level**.

Nota

De forma predeterminada, el nivel de transparencia está definido en 80.



Cómo proporcionar información de cuentas a los usuarios

Jan 29, 2016

Tiene que dar a los usuarios la información de cuenta necesaria para que puedan acceder a sus escritorios y aplicaciones virtuales. Puede proporcionarles esta información de las siguientes formas:

- Configurando la detección de cuentas basada en direcciones de correo electrónico
- Entregándoles un archivo de aprovisionamiento
- Entregándoles la información de cuenta para que la introduzcan manualmente

> ## Important
>
> Avise a los usuarios que usan Citrix Receiver por primera vez que deben reiniciar Receiver después de instalarlo. Al reiniciar Receiver los usuarios pueden agregar cuentas y Receiver puede detectar los dispositivos USB que estaban suspendidos cuando se instaló.

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

Cuando se configura Receiver para la detección de cuentas basada en direcciones de correo electrónico, 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 o Access 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 virtuales.

> ## Nota
>
> La detección de cuentas basada en correo electrónico no está respaldada en implementaciones con la Interfaz Web.

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

Para configurar NetScaler Gateway, consulte Conexión a StoreFront usando la detección basada en correo electrónico en la documentación de NetScaler Gateway.

Entrega de un archivo de aprovisionamiento a los usuarios

StoreFront proporciona los archivos de aprovisionamiento que los usuarios pueden abrir para conectar con almacenes.

- 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 Para exportar archivos de aprovisionamiento para los usuarios en la

documentación de StoreFront.

Entrega de la información de cuenta para introducirla manualmente

Para permitir que los usuarios configuren sus cuentas manualmente, distribúyales la información que necesitan para conectarse con sus escritorios y aplicaciones virtuales.

- Para las conexiones con un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: https://nombreservidor.empresa.com.
  Para implementaciones con Interfaz Web, proporcione la dirección URL del sitio de servicios XenApp.

- Para conexiones a través de NetScaler Gateway, primero determine si el usuario necesita ver todos los almacenes configurados o solo el almacén que tiene habilitado el acceso remoto para un NetScaler Gateway concreto.
  - Para presentarles todos los almacenes configurados, suministre a sus usuarios el nombre de dominio completo de NetScaler Gateway.
  - Para limitar el acceso a un almacén en concreto, suministre a sus usuarios el nombre de dominio completo de NetScaler Gateway y el nombre del almacén, con el formato:
    NetScalerGatewayFQDN?MyStoreName

    Por ejemplo, si tiene un almacén llamado "AplicacionesVentas" con acceso remoto habilitado para servidor1.com, y un almacén llamado "AplicacionesRRHH" con acceso remoto habilitado para servidor2.com, el usuario deberá introducir servidor1.com?AplicacionesVentas si quiere acceder AplicacionesVentas, o introducir servidor2.com?AplicacionesRRHH si quiere acceder a AplicacionesRRHH. Esta característica requiere que el usuario cree una cuenta cuando usa el producto por primera vez, introduciendo una dirección URL, y no está disponible para la detección basada en correo electrónico.

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.

Para administrar cuentas, un usuario de Receiver abre la página de inicio de Receiver, hace clic en el , y a continuación en **Cuentas**.

Cómo compartir varias cuentas de almacén automáticamente

Si dispone de más de una cuenta de almacén, puede configurar Citrix Receiver para Windows para que se conecte automáticamente con todas las cuentas al establecer una sesión. Para ver automáticamente todas las cuentas al abrir Receiver:

En sistemas de 32 bits, cree la clave "CurrentAccount":

Ubicación: HKLM\Software\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG_SZ

En sistemas de 64 bits, cree la clave "CurrentAccount":

Ubicación: HKLM\Software\Wow6432Node\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG_SZ

Advertencia

El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Optimización del entorno de Citrix Receiver

Nov 03, 2016

El entorno en el que funciona Receiver para los usuarios puede optimizarse con lo siguiente.

- Reducción del tiempo de inicio de las aplicaciones
- Asignar dispositivos cliente
- Respaldo para resolución de nombres DNS
- Utilización de servidores proxy con conexiones de XenDesktop
- Respaldo para usuarios de NDS
- Uso de Receiver con XenApp para UNIX
- Habilitar acceso a aplicaciones anónimas

Para obtener más información sobre otras opciones de optimización, consulte los temas de la documentación de XenDesktop relacionados con el mantenimiento de la actividad de la sesión y la optimización de la experiencia de HDX.

Reducción del tiempo de inicio de las aplicaciones

Jan 29, 2016

La función de preinicio o inicio previo de sesiones permite reducir el tiempo que tardan en abrirse las aplicaciones durante los periodos de mucho tráfico o tráfico normal, mejorando así la experiencia del usuario. La función de inicio previo permite crear una sesión de preinicio cuando un usuario inicia una sesión en Receiver o en un momento específico programado si el usuario ya ha iniciado una sesión.

Esta sesión de inicio previo reduce el tiempo que tarda en iniciarse la primera aplicación. Cuando un usuario agrega una nueva conexión de cuenta a Receiver, el inicio previo de sesiones no tiene efecto hasta la siguiente sesión. La aplicación predeterminada ctxprelaunch.exe se ejecuta en esta sesión, pero no es visible para el usuario.

El inicio previo de sesiones está respaldado en implementaciones de StoreFront a partir de la versión StoreFront 2.0. En implementaciones con la Interfaz Web, asegúrese de usar la opción Guardar contraseña para evitar que aparezcan diálogos de inicio de sesión. El inicio previo de sesiones no está respaldado en implementaciones de XenDesktop 7.

El inicio previo de sesiones está inhabilitado de forma predeterminada. Para habilitar el inicio previo de sesiones, especifique el parámetro ENABLEPRELAUNCH=true en la línea de comandos de Receiver o defina la clave de Registro EnablePreLaunch en true. El parámetro predeterminado es Null y significa que el inicio previo está inhabilitado.

Nota: Si la máquina cliente se ha configurado para dar respaldo a la autenticación PassThrough de dominio (SSON), el preinicio está habilitado automáticamente. Si desea usar la autenticación PassThrough de dominio (Single Sign-on) sin la función de preinicio, establezca el valor de la clave de Registro EnablePreLaunch en false.
Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Las ubicaciones en el Registro son:

HKLM\Software\[Wow6432Node\]Citrix\Dazzle

HKCU\Software\Citrix\Dazzle

Existen dos tipos de inicio previo:

- **Inicio previo a petición**. El inicio previo se lleva a cabo inmediatamente después de que se autentican las credenciales del usuario, independientemente del tráfico de la red. Por lo general, se usa en periodos de tráfico normal. Un usuario puede provocar un preinicio en un momento dado, reiniciando Receiver.
- **Inicio previo programado**. El inicio previo ocurre a una hora programada. El inicio previo programado ocurre solo cuando el dispositivo de usuario ya se está ejecutando y se ha autenticado. Si no se cumplen estas dos condiciones cuando llega la hora del inicio previo programado, no se inicia la sesión. La sesión se inicia en una ventana a la hora programada lo que permite distribuir la carga de red y del servidor. Por ejemplo, si el inicio previo se ha programado para la 1:45 p. m., la sesión en realidad se inicia entre la 1:15 p. m. y la 1:45 p. m. Por lo general, se usa en periodos de mucho tráfico.

La configuración del inicio previo en el servidor XenApp consiste en crear, modificar o eliminar aplicaciones de inicio previo, así como actualizar las configuraciones de directivas de usuario que controlan el inicio previo de aplicaciones. Consulte "Para realizar el inicio previo de aplicaciones en los dispositivos de los usuarios" en la documentación de XenApp si quiere ver información sobre cómo configurar inicios previos de sesiones en el servidor XenApp.

No se respalda el uso del archivo icaclient.adm para personalizar la función de inicio previo. No obstante, se puede cambiar la configuración del inicio previo modificando valores del Registro durante o después de la instalación de Receiver. Hay tres valores HKLM y dos valores HKCU:

- Los valores HKLM se escriben durante la instalación del cliente.
- Los valores HKCU permiten dar diferentes parámetros a los distintos usuarios de un mismo equipo. Los usuarios pueden cambiar los valores HKCU sin necesidad de permisos de administrador. Se pueden proporcionar scripts a los usuarios para lograr este resultado.

Valores de Registro HKLM

Para Windows 7 y 8 de 64 bits:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Para todos los demás sistemas operativos Windows de 32 bits que sean compatibles:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Nombre: UserOverride

Valores:

0: Usa los valores de HKEY_LOCAL_MACHINE, incluso si ya existen valores de HKEY_CURRENT_USER.

1: Usa los valores de HKEY_CURRENT_USER si ya existen; de lo contrario, usa los valores de HKEY_LOCAL_MACHINE.

Nombre: State

Valores:

0: Inhabilita el inicio previo.

1: Habilita el inicio previo a petición. (El inicio previo ocurre después de autenticar las credenciales).

2: Habilita el inicio previo programado. (El inicio previo ocurre a la hora configurada en Schedule.)

Nombre: Schedule

Valor:

Hora (en formato de 24 horas) y días de la semana para los inicios previos programados, con el formato siguiente:

HH:MM|M:T:W:TH:F:S:SU donde HH y MM son las horas y los minutos. M:T:W:TH:F:S:SU son los días de la semana. Por ejemplo, para habilitar el inicio previo programado los lunes, miércoles y viernes a la 1:45 p. m., configure Schedule en Schedule=13:45|1:0:1:0:1:0:0. En realidad, la sesión se inicia entre la 1:15 p. m. y la 1:45 p. m.

Valores de Registro HKCU

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Las claves State y Schedule tienen los mismos valores que para HKLM.

Asignar dispositivos cliente

Jan 29, 2016

Receiver admite la asignación de dispositivos en los dispositivos de usuario de manera que estén disponibles desde una sesión. Los usuarios pueden:

- Tener acceso imperceptible a las unidades locales, impresoras y puertos COM.
- Cortar y pegar entre sesiones y el portapapeles de Windows local.
- Escuchar sonido (sonidos del sistema y archivos .wav) reproducido en la sesión.

Durante el inicio de sesión, Receiver informa al servidor sobre las unidades cliente, puertos COM y puertos LPT disponibles. De forma predeterminada, a las unidades del cliente se les asignan letras de unidad del servidor y se crean colas de impresión de servidor para impresoras cliente de manera que parezca que están directamente conectadas a la sesión. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual. Se las elimina cuando el usuario cierra la sesión y se vuelven a crear la próxima vez que el usuario inicia una sesión.

Puede usar las configuraciones de directiva de redirección de Citrix para asignar los dispositivos de usuario que no se hayan asignado automáticamente al iniciar la sesión. Para obtener más información, consulte la documentación de XenDesktop o XenApp.

Desactivar la asignación de dispositivos de usuario

Es posible configurar las opciones de asignación de dispositivos de usuario para controladores, impresoras y puertos con la herramienta Administración del servidor de Windows. Para mayor información sobre las opciones disponibles, consulte la documentación de Servicios de Terminal Server.

Redirección de carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Cuando se habilita solo la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de usuario, solo se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecerán como enlaces UNC dentro de las sesiones, en lugar de aparecer todo el sistema de archivos del dispositivo del usuario. Si se inhabilitan los enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión. Para obtener más información sobre cómo configurar la redirección de carpetas del cliente para los dispositivos de usuario, consulte la documentación de XenDesktop 7.

Asignación de unidades del cliente a letras de unidad del host

La asignación de unidades del cliente permite redirigir letras de unidad del host a unidades existentes en el dispositivo del usuario. Por ejemplo, la unidad H de una sesión de un usuario de Citrix se puede asignar a la unidad C del dispositivo del usuario que ejecuta Receiver.

La asignación de unidades del cliente está incorporada de forma imperceptible en las funciones estándar de redirección de dispositivos de Citrix. Para el Administrador de archivos, el Explorador de Windows y sus aplicaciones se ven como cualquier otra asignación de red.

El servidor que aloja las aplicaciones y los escritorios virtuales se puede configurar durante la instalación para que asigne

unidades del cliente automáticamente a un grupo determinado de letras de unidad. La instalación predeterminada asigna letras de unidad a las unidades del cliente comenzando por la V y letras subsiguientes en orden descendente, asignando una letra de unidad a cada unidad de disco fija y de CD-ROM. (A las unidades de disquete se les asignan las letras de unidad existentes.) Este método da como resultado las siguientes asignaciones de unidad en la sesión:

Letra de unidad del cliente	**El servidor accede a ella como:**
A	A
B	B
C	V
D	U

El servidor se puede configurar para que sus respectivas letras de unidad no entren en conflicto con las del cliente; en este caso, las letras de unidad del servidor se cambian por otras posteriores en orden alfabético. Por ejemplo, si se cambian las unidades C y D del servidor por M y N, respectivamente, los equipos cliente pueden acceder a sus unidades C y D directamente. Este método proporciona las siguientes asignaciones de unidad en una sesión:

Letra de unidad del cliente	**El servidor accede a ella como:**
A	A
B	B
C	C
D	D

La letra de unidad utilizada para sustituir la unidad C del servidor se define durante la configuración. El resto de las letras de unidad de disco duro y de CD-ROM se sustituyen por letras de unidad secuenciales (por ejemplo; C > M, D > N, E > O). Estas letras de unidad no deben entrar en conflicto con otras asignaciones de unidad de red existentes. Si a una unidad de red se le asigna la misma letra de unidad que la de un servidor, la asignación de unidad de red no será válida.

Cuando un dispositivo cliente se conecta con un servidor, se restablecen las asignaciones del cliente a menos que la asignación automática de dispositivos del cliente esté inhabilitada. La asignación de unidades del cliente está habilitada de forma predeterminada. Para cambiar esta configuración, use la herramienta de Configuración de Servicios de Escritorio remoto (Servicios de Terminal Server). Es también posible usar directivas para tener mayor control sobre cómo se aplica la asignación de dispositivos del cliente. Para obtener más información sobre directivas, consulte la documentación de XenDesktop o XenApp en eDocs.

Redirección de dispositivos USB de HDX Plug and Play

Actualizado: 27-01-2015

La redirección de dispositivos USB de HDX Plug-n-Play permite la redirección dinámica de varios dispositivos, incluyendo cámaras, escáneres, reproductores multimedia y dispositivos de punto de venta (POS) al servidor. Al mismo tiempo, se puede impedir la redirección de todos o algunos dispositivos. Edite las directivas en el servidor o aplique directivas de grupo en el dispositivo de usuario para configurar los parámetros de la redirección. Para obtener más información, consulte Consideraciones sobre unidades del cliente y USB en la documentación de XenApp y XenDesktop.

Importante: Si se prohíbe el uso de la redirección de dispositivos USB Plug-n-Play en una directiva de servidor, el usuario no puede anular dicha configuración de directiva.
Un usuario puede definir permisos en Receiver para permitir o rechazar siempre la redirección de dispositivos, o para que se le pregunte cada vez que se conecta un dispositivo. El parámetro solo afecta a los dispositivos que se conectan después de que el usuario cambia el parámetro.

Para asignar un puerto COM del cliente a un puerto COM del servidor

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 utilizar de la misma forma que cualquier otra asignación de red.

Es posible asignar puertos COM de cliente desde una interfaz de comandos. También se puede controlar la asignación de puertos COM de cliente desde la herramienta Configuración de Escritorio remoto (Servicios de Terminal Server) o a través de directivas. Para obtener más información sobre directivas, consulte la documentación de XenDesktop o XenApp.

Importante: La asignación de puertos COM no es compatible con TAPI. Los dispositivos TAPI no pueden asignarse a puertos COM del cliente.

1. En implementaciones de XenDesktop 7, habilite la configuración de directiva Redirección de puertos COM del cliente.
2. Inicie una sesión en Receiver.
3. Escriba lo siguiente en una interfaz de comandos:

   net use comx: \\client\comz:

   donde x es el número del puerto COM del servidor (los puertos 1 a 9 están disponibles para ser asignados) y z es el número del puerto COM del cliente que se desea asignar.

4. Para confirmar la operación, escriba:

   net use

   en la interfaz de comandos. Aparecerá la lista de las unidades, puertos LPT y puertos COM asignados.

   Para utilizar este puerto COM en una sesión de aplicación o escritorio virtual, instale el dispositivo con el nombre asignado. Por ejemplo, si asigna COM1 en el cliente a COM5 en el servidor, instale el dispositivo de puerto COM en COM5 durante la sesión. Utilice este puerto COM asignado del mismo modo que lo haría con un puerto COM del dispositivo del usuario.

Respaldo para resolución de nombres DNS

Jan 29, 2016

Puede configurar los dispositivos Receiver que usen Citrix XML Service para solicitar un nombre DNS para un servidor en lugar de una dirección IP.

Importante: A menos que el entorno DNS esté configurado específicamente para utilizar esta función, Citrix recomienda no habilitar la resolución de nombres DNS en la comunidad de servidores.

Los dispositivos Receiver que se conectan a aplicaciones publicadas a través de la Interfaz Web también usan Citrix XML Service. En el caso de los dispositivos Receiver que se conectan a través de la Interfaz Web, el servidor Web resuelve los nombres DNS para Receiver.

La resolución de nombres DNS está inhabilitada de forma predeterminada en la comunidad de servidores y está habilitada de forma predeterminada en Receiver. Cuando la resolución de nombres DNS está inhabilitada en la comunidad, cualquier solicitud de Receiver de un nombre DNS devuelve una dirección IP. No hay necesidad de inhabilitar la resolución de nombres DNS en Receiver.

Para inhabilitar la resolución de nombres DNS para dispositivos cliente específicos

Si su implementación de servidores usa DNS para la resolución de nombres y tiene problemas con algunos dispositivos de usuario, puede inhabilitar la resolución de nombres DNS para esos dispositivos.

Precaución: El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

1. Agregue una clave de Registro xmlAddressResolutionType a HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing.
2. El valor debe ser IPv4-Port.
3. Repita el proceso para cada usuario de los dispositivos de usuario.

Utilización de servidores proxy con conexiones de XenDesktop

Jan 29, 2016

Si no utiliza servidores proxy en su entorno, corrija los parámetros de proxy de Internet Explorer en los dispositivos de usuario que ejecutan Internet Explorer 7.0 con Windows XP. De manera predeterminada, esta configuración detecta automáticamente los parámetros de proxy. Si no se utilizan servidores proxy, los usuarios experimentarán demoras innecesarias durante el proceso de detección. Para obtener instrucciones para modificar los parámetros de proxy, consulte la documentación de Internet Explorer. O bien, puede modificar los parámetros de proxy mediante la Interfaz Web. Para más información, consulte la documentación de la Interfaz Web.

Mejora de la experiencia del usuario

Jan 29, 2016

Es posible mejorar la experiencia de uso mediante las siguientes funciones:

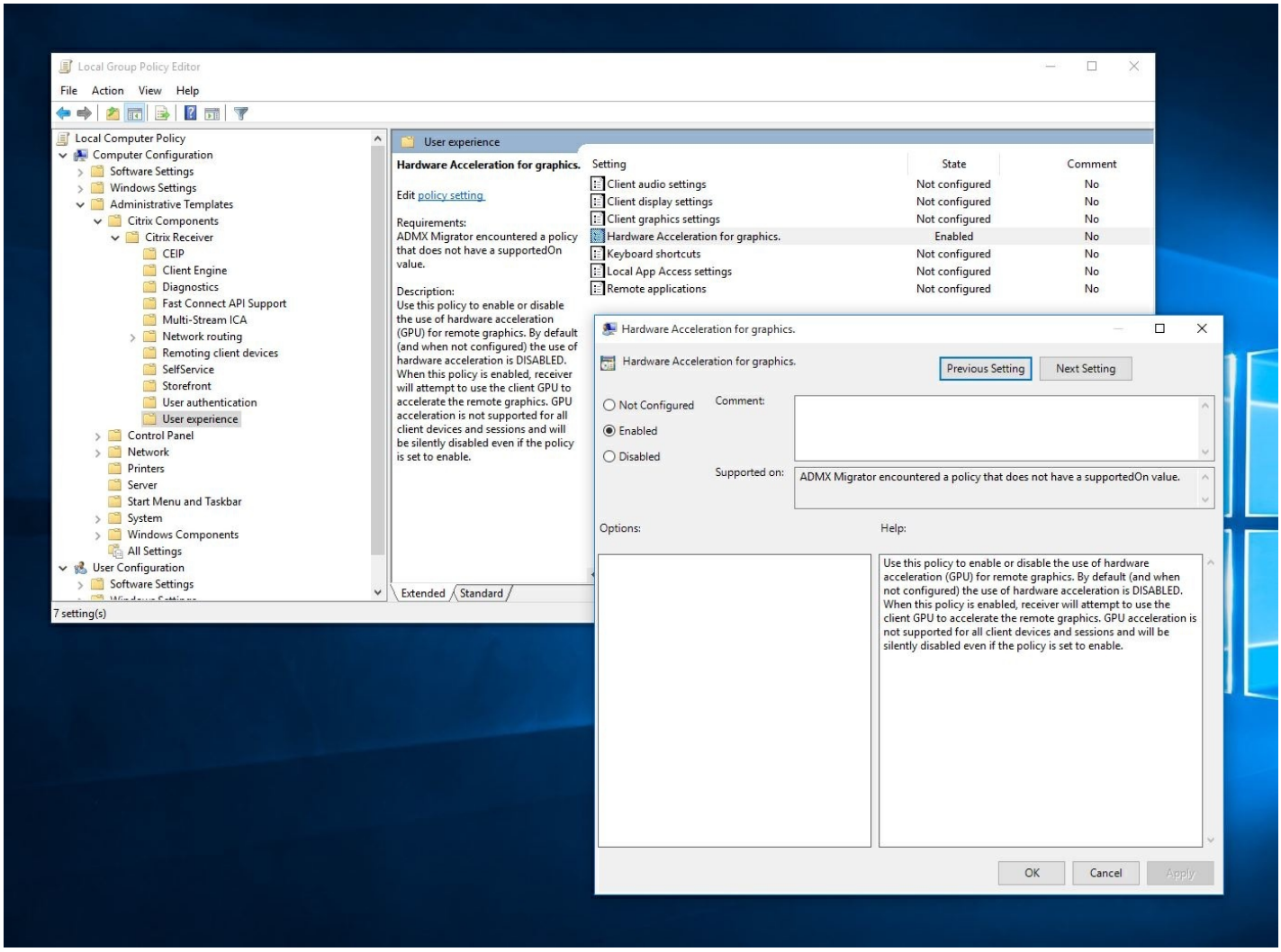
Cuando se usa Citrix Receiver para Windows versión 4.4 (con HDX Engine 14.4), la GPU se puede usar para la descodificación H.264 donde esté disponible en el cliente. La capa de API utilizada para la descodificación por GPU es DXVA (DirectX Video Acceleration).

Para obtener más información, consulte el artículo de blog Improved User Experience: Hardware Decoding for Citrix Windows Receiver.

> ## Nota
>
> De manera predeterminada, la característica de descodificación por hardware está desactivada; se la puede habilitar mediante directivas del lado del cliente.

Para habilitar la descodificación por hardware:

1. Copie “receiver.adml” desde “root\Citrix\ICA Client\Configuration\en” en “C:\Windows\PolicyDefinitions\en-US”.
2. Copie “receiver.admx” desde “root\Citrix\ICA Client\Configuration” en “C:\Windows\PolicyDefinitions\”.
3. Vaya al **Editor de directivas de grupo local**.
4. En Configuración del equipo -> Plantillas administrativas -> Citrix Receiver -> User Experience, abra **Hardware Acceleration for graphics**.
5. Seleccione **Habilitada** y haga clic en **Aceptar**.



Para validar si la directiva se aplicó y la aceleración por hardware se está utilizando en una sesión ICA activa, busque las entradas de Registro siguientes:

Ruta del Registro: HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\

> ## Sugerencia
>
> El valor de **Graphics_GfxRender_Decoder** y **Graphics_GfxRender_Renderer** debe ser 2. Si el valor es 1, esto significa que se está usando la descodificación por CPU.

Cuando use la característica de descodificación por hardware, tenga en cuenta que existen las limitaciones siguientes:

- Si el cliente tiene dos unidades GPU y si uno de los monitores está activo en la segunda GPU, se usará la descodificación basada en CPU.
- Al conectar con un servidor XenApp 7.x que ejecuta Windows Server 2008 R2, Citrix recomienda no usar la descodificación por hardware en el dispositivo Windows del usuario. Si se habilita, pueden observarse problemas como un rendimiento lento al resaltar texto y un parpadeo de pantalla.

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.

Los usuarios de Receiver pueden seleccionar si quieren usar los micrófonos conectados a sus dispositivos, cambiando un parámetro en la Central de conexiones. Los usuarios de XenDesktop también pueden usar las Preferencias de XenDesktop Viewer para inhabilitar sus micrófonos y cámaras Web.

Actualizado: 28-11-2014

Se pueden usar hasta ocho monitores con Receiver.

Cada monitor en una configuración de varios monitores tiene su propia resolución, configurada por el fabricante. Los monitores pueden ofrecer diferentes resoluciones y orientaciones durante las sesiones.

Las sesiones pueden distribuirse entre varios monitores de dos formas:

- En modo de pantalla completa, con varios monitores en la sesión; las aplicaciones se presentan en los monitores como lo harían localmente.
  XenDesktop: Puede mostrar la ventana de Desktop Viewer en cualquier subconjunto de rectángulos de monitores; para ello, cambie el tamaño de la ventana en cualquier parte de los monitores y presione el botón Maximizar.

- En modo de ventanas, con una única imagen de monitor para la sesión; las aplicaciones no se muestran en monitores individuales.

XenDesktop: cuando posteriormente se inicia cualquier escritorio en la misma asignación (anteriormente "grupo de escritorios"), se mantiene el parámetro de ventana y se muestra el escritorio en los mismos monitores. En la medida en que la distribución de monitores sea rectangular, se pueden mostrar varios escritorios virtuales en un dispositivo. Si la sesión de XenDesktop usa el monitor principal en el dispositivo, éste será el monitor principal de la sesión. De lo contrario, el monitor con el número más bajo en la sesión se convierte en el monitor principal.

Para habilitar el respaldo de varios monitores, asegúrese de lo siguiente:

- El dispositivo de usuario está configurado para respaldar el uso de varios monitores.
- El sistema operativo del dispositivo de usuario debe ser capaz de detectar cada monitor. Para verificar que esta detección ocurre en el dispositivo de usuario en las plataformas Windows, confirme que cada monitor aparece por separado en la ficha Configuración del cuadro de diálogo Configuración de pantalla.
- Después de detectar los monitores:
  - **XenDesktop:** Configure el límite de memoria gráfica con el parámetro Límite de memoria de presentación de Directivas de equipo Citrix.
  - **XenApp:** Según la versión del servidor XenApp que tenga instalada:
    - Configure el límite de memoria de pantalla con el parámetro Límite de memoria de presentación de Directivas de equipo Citrix.
    - En la consola de administración Citrix del servidor XenApp, seleccione la comunidad y, en el panel de tareas, seleccione Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > HDX Broadcast > Presentación (o Modificar las propiedades del servidor > Modificar todas las propiedades >

Predeterminadas del servidor > ICA > Presentación) y configure el parámetro Memoria máxima que se puede utilizar en cada uno de los gráficos de las sesiones.

Asegúrese de que el parámetro es lo suficientemente amplio (en kilobytes) para ofrecer suficiente memoria gráfica. Si este parámetro no es lo suficientemente grande, el recurso publicado se restringirá al subconjunto de monitores que cubra el tamaño especificado.

Para obtener información acerca del cálculo de los requisitos de memoria gráfica de XenApp y XenDesktop, consulte ctx115637.

Si en la configuración de directiva Valores predeterminados de optimización de impresión universal está habilitada la opción Permitir a los no administradores modificar estos parámetros, los usuarios pueden anular las opciones Compresión de imágenes y Almacenamiento en caché de imágenes y fuentes especificadas en esa configuración de directiva.

Para sobrescribir los parámetros de la impresora en el dispositivo de usuario

1. En el menú Imprimir de la aplicación del dispositivo de usuario, elija Propiedades.
2. En la ficha Parámetros del cliente, haga clic en Optimizaciones avanzadas y realice cambios a las opciones Compresión de imagen y Almacenamiento en caché de imágenes y fuentes.

Para habilitar el acceso táctil a las aplicaciones y escritorios virtuales desde tabletas Windows, Receiver muestra automáticamente el teclado en pantalla al activar un campo de entrada de texto, y cuando el dispositivo está en modo tienda o tableta.

En algunos dispositivos y en algunas circunstancias, Receiver no puede detectar el modo en que se encuentra un dispositivo, y es posible que el teclado en pantalla aparezca cuando no sea necesario.

Para impedir que aparezca el teclado en pantalla al usar un dispositivo convertible (tableta con teclado extraíble), cree un valor de REG_DWORD con DisableKeyboardPopup en HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver y establezca el valor en 1.
Nota: En una máquina x64, cree el valor en HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Se pueden configurar combinaciones de teclas para que Receiver las interprete como una funcionalidad especial. Cuando se habilita la directiva de teclas de acceso directo, se pueden especificar las teclas de acceso directo de Citrix, el comportamiento de las teclas de acceso directo de Windows y la disposición del teclado para las sesiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.

   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.

5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User Experience > Keyboard shortcuts.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y luego elija las opciones pertinentes.

Receiver respalda los iconos de color de alta densidad (de 32 bits) y selecciona automáticamente la profundidad de color de las aplicaciones que se muestran en el cuadro de diálogo Central de conexiones de Citrix, en el menú Inicio y en la barra de tareas para proporcionar una integración total.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.
Para establecer una profundidad preferida, se puede agregar la clave de Registro TWIDesiredIconColor a HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences y establecerla en el valor deseado. Las profundidades de color posibles son 4, 8, 16, 24 y 32 bits por píxel. Si la conexión de la red es lenta, los usuarios pueden seleccionar valores de profundidad de color menores para los iconos.

Cada empresa tiene sus propias necesidades de negocio. Los requisitos para el acceso por parte de los usuarios a los escritorios virtuales pueden variar de usuario a usuario y a medida que evolucionan las necesidades de la empresa. La experiencia del usuario a la hora de conectarse con los escritorios virtuales, así como su interacción en la configuración de las conexiones depende de cómo se configure Receiver para Windows.

Use **Desktop Viewer** cuando los usuarios necesiten interactuar con el escritorio virtual. El escritorio virtual del usuario pueden ser un escritorio virtual publicado, o un escritorio compartido o escritorio dedicado. En este modo de acceso, las funciones de la barra de herramientas de Desktop Viewer permiten al usuario abrir un escritorio virtual en una ventana y, desplazar y cambiar el tamaño de ese escritorio dentro del escritorio local. Los usuarios pueden definir preferencias y conectarse con más de un escritorio utilizando varias conexiones XenDesktop en el mismo dispositivo de usuario.

Nota: Los usuarios deben usar Citrix Receiver para cambiar la resolución de pantalla en sus escritorios virtuales. No pueden cambiar la resolución de pantalla usando el Panel de control de Windows.

En las sesiones de Desktop Viewer, la combinación de la tecla con el logotipo de Windows+L se transfiere al equipo local.

Ctrl+Alt+Supr se transfiere al equipo local.

Las pulsaciones de teclas que activan StickyKeys, FilterKeys y ToggleKeys (características de accesibilidad de Microsoft) siempre se transfieren al equipo local.

Como una funcionalidad de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

Ctrl+Esc se envía al escritorio virtual remoto.

Nota: De forma predeterminada, Alt+Tab transfiere el foco entre las ventanas de la sesión si Desktop Viewer está maximizado. Si Desktop Viewer se muestra en una ventana, Alt+Tab transfiere el foco entre las ventanas fuera de la sesión. Las secuencias de teclas de acceso rápido son combinaciones de teclas diseñadas por Citrix. Por ejemplo, la secuencia

Ctrl+F1 reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2 cambia entre el modo de pantalla completa y de ventanas en las aplicaciones. No puede usar las secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer (en sesiones de XenDesktop), pero puede usarlas con aplicaciones publicadas (en sesiones de XenApp).

Los usuarios no pueden conectarse con el mismo escritorio virtual desde una sesión de escritorio. Si se intenta, se desconectará la sesión de escritorio existente. Por lo tanto, Citrix recomienda lo siguiente:

- Los administradores no deben configurar a los clientes de un escritorio para que se conecten con un sitio que publica el mismo escritorio.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio si el sitio se configura para reconectar a los usuarios automáticamente con las sesiones existentes.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio e intentar ejecutarlo.

Tenga en cuenta que un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea las conexiones con ese escritorio.

Si los usuarios se conectan con aplicaciones virtuales (publicadas con XenApp) desde un escritorio virtual y la organización dispone de un administrador de XenApp independiente, Citrix sugiere aunar esfuerzos para definir la asignación de dispositivos para que los dispositivos de escritorio se asignen siempre dentro de las sesiones de aplicación y escritorio. Debido a que las unidades locales se muestran como unidades de red en las sesiones de escritorio, el administrador de XenApp necesita modificar la directiva de asignación de unidades para que incluya las unidades de red.

Puede cambiar el tiempo que se muestra el indicador de estado cunado el usuario inicia una sesión. Para cambiar el tiempo de espera, cree el valor REG_DWORD: SI INACTIVE MS, en HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\. El valor REG_DWORD puede establecerse en 4 si quiere que el indicador de estado desparezca más pronto.

Precaución: Si edita el Registro de forma incorrecta pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

Protección de las conexiones

Jan 29, 2016

Para maximizar la seguridad del entorno, las conexiones entre Citrix Receiver y los recursos que se publiquen deben ser seguras. Puede configurar diversos tipos de autenticación para el software de Citrix Receiver, incluidos: autenticación con tarjeta inteligente, comprobación de lista de revocación de certificados y autenticación PassThrough con Kerberos.

La autenticación mediante Desafío/Respuesta de Windows NT (NTLM) recibe respaldo de manera predeterminada en los equipos Windows.

Configuración de autenticación PassThrough de dominio

Jan 29, 2016

Este tema explica cómo habilitar la autenticación PassThrough de dominio para Citrix Receiver con XenDesktop o XenApp.

> ## Nota
>
> En este ejemplo, la instalación de Citrix Receiver, la aplicación de directivas de equipo y la configuración de un sitio de confianza en el sistema operativo del cliente se llevan a cabo manualmente. Una vez creada una plantilla de objeto de directiva de grupo (GPO), se la puede aplicar a cualquier máquina cliente del dominio que tenga instalado Citrix Receiver.

Hay dos maneras de habilitar el paso de credenciales PassThrough de dominio (SSON) cuando se instala Citrix Receiver:

- mediante una instalación con la línea de comandos
- mediante la interfaz gráfica de usuario

Habilitación de PassThrough de dominio usando la interfaz de línea de comandos

Para habilitar el paso de credenciales de dominio PassThrough (SSON) usando la interfaz de línea de comandos:

1. Instale Citrix Receiver 4.x con la opción **/includeSSON**.
   - Instale uno o varios almacenes de StoreFront (puede completar este paso más adelante); la instalación de almacenes de StoreFront no es un requisito obligatorio para configurar la autenticación PassThrough de dominio.
   - Verifique que la autenticación PassThrough está habilitada iniciando Citrix Receiver, y confirmando que el proceso ssonsvr.exe se está ejecutando en el administrador de tareas después de reiniciar el dispositivo de punto final donde está instalado Citrix Receiver.

> ## Nota
>
> Para obtener información acerca de la sintaxis para agregar uno o varios almacenes de StoreFront, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

Habilitación de PassThrough de dominio usando la interfaz gráfica

Para habilitar el paso de credenciales PassThrough de dominio usando la interfaz gráfica:

1. Busque el archivo de instalación de Citrix Receiver (CitrixReceiver.exe).
2. Haga doble clic en **CitrixReceiver.exe** para iniciar el instalador.
3. En el asistente de instalación Habilitar Single Sign-on, marque la casilla Habilitar Single Sign-on para instalar Citrix Receiver con la característica SSON habilitada; esto equivale a instalar Citrix Receiver usando la opción de línea de comandos

/includeSSON.

La imagen siguiente ilustra cómo habilitar Single Sign-on:

> **Nota**
>
> El asistente de instalación Habilitar Single Sign-on solo está disponible en instalaciones nuevas en máquinas unidas a dominios.

Verifique que la autenticación PassThrough está habilitada iniciando Citrix Receiver, y confirmando que el proceso **ssonsvr.exe** se está ejecutando en el administrador de tareas después de reiniciar el dispositivo de punto final donde está instalado Citrix Receiver.

Use la información en esta sección para configurar parámetros de directiva de grupo para la autenticación con SSON.

> **Nota**
>
> El valor predeterminado de la configuración de directiva del objeto de directiva de grupo (GPO) relacionado con SSON es **Enable pass-through authentication**, y es suficiente para que SSON funcione. Use el procedimiento siguiente para modificar esta configuración.

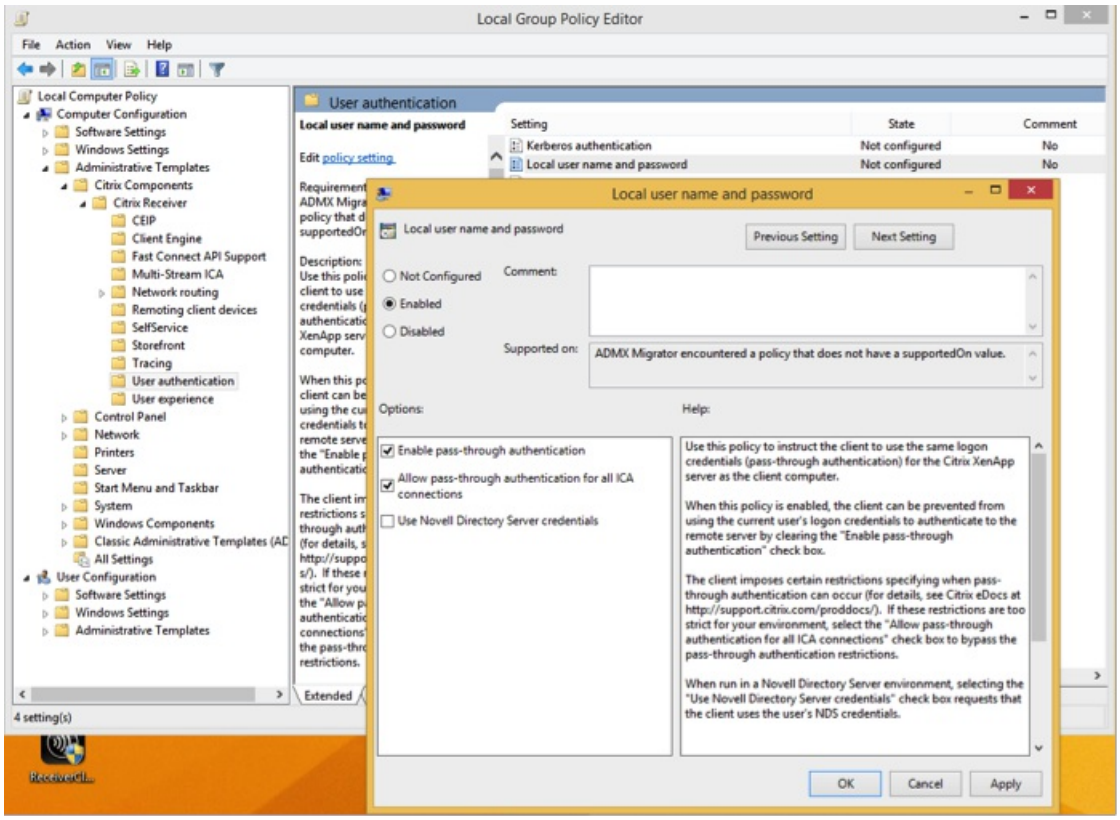
Uso de un archivo ADMX para la directivas de grupo de SSON

Use el procedimiento siguiente para configurar parámetros de directiva de grupo usando el archivo ADMX:

1. Cargue los archivos de directivas de grupo. En instalaciones de Citrix Receiver 4.3 y versiones posteriores, use **Receiver.ADMX** o **Receiver.ADML**, ubicados en la carpeta %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration.
2. Abra **gpedit.msc**, haga clic con el botón secundario en **Configuración del equipo -> Plantillas administrativas ->**

Citrix Components -> Citrix Receiver -> User Authentication.

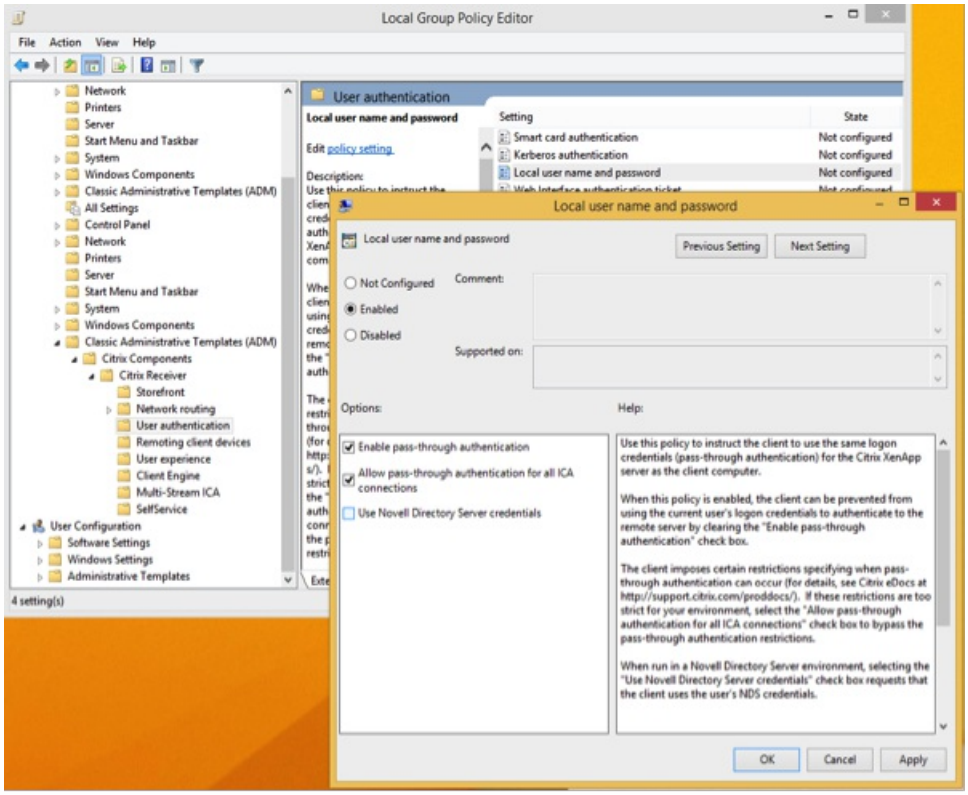
3. Habilite las siguientes configuraciones de GPO de equipo local (en la máquina local del usuario y/o en la imagen maestra del VDA de escritorio):
   - Elija Local user name and password.
   - Seleccione **Habilitada**.
   - Seleccione **Enable pass-through authentication**.
4. Reinicie el dispositivo de punto final (dispositivo donde está instalado Citrix Receiver) o la imagen maestra del VDA de escritorio.



Uso de un archivo ADM para la directiva de grupo de SSON

Use el procedimiento siguiente para configurar parámetros de directiva de grupo usando el archivo ADM:

1. Abra el editor de directivas de grupo local seleccionando **Configuración del equipo > Haga clic con el botón secundario en Plantillas administrativas > Elija Agregar o quitar plantillas**.
2. Haga clic en **Agregar** para agregar una plantilla ADM.
3. Después de agregar la plantilla **receiver.adm**, expanda **Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication**.



4. Abra Internet Explorer en la máquina local y/o en la imagen maestra del VDA de escritorio.

5. En **Opciones de Internet > Seguridad > Sitios de confianza**, agregue a la lista el nombre de dominio completo (FQDN) de los servidores StoreFront, sin la ruta del almacén. Por ejemplo: https://storefront.ejemplo.com

> ## Nota
>
> También puede agregar el servidor StoreFront a los Sitios de confianza usando un GPO de Microsoft. El GPO se llama **Lista de asignación de sitio a zona** y la encontrará en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página Seguridad**.

6. Cierre la sesión y vuelva a iniciarla en el dispositivo de punto final de Citrix Receiver.

Cuando se abre Citrix Receiver, si el usuario actual tiene una sesión iniciada en el dominio, sus credenciales de usuario se transferirán a StoreFront, junto con las aplicaciones y escritorios enumerados dentro de Citrix Receiver, incluidos los parámetros del menú Inicio del usuario. Cuando el usuario hace clic en un icono, Citrix Receiver transfiere las credenciales de dominio del usuario al Delivery Controller y la aplicación o el escritorio seleccionados se abren.

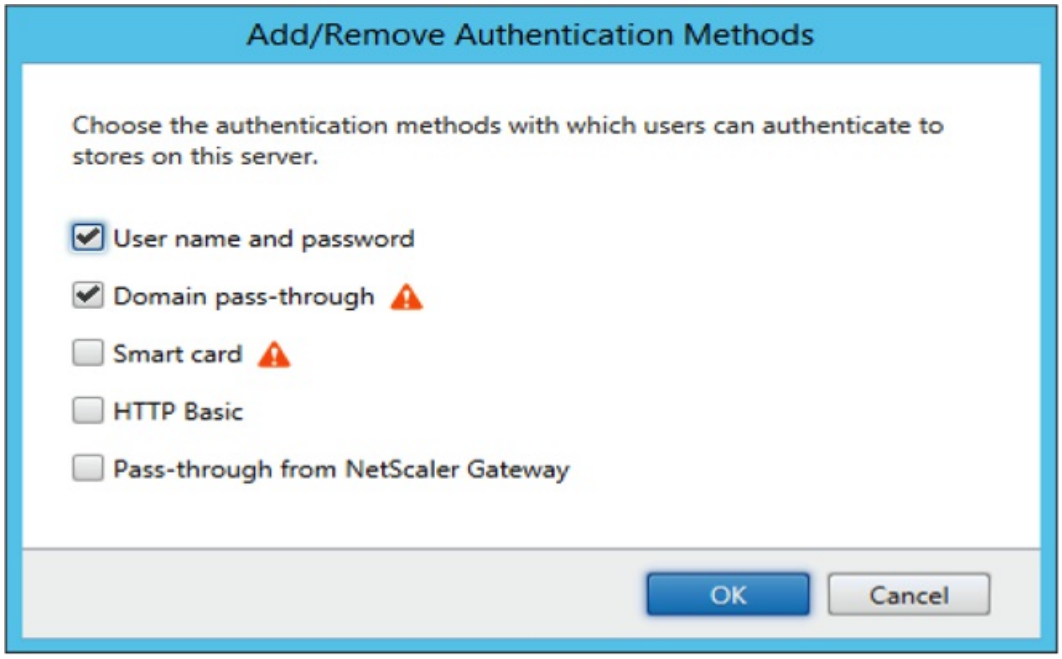
Use el procedimiento siguiente para configurar SSON en StoreFront y la Interfaz Web

1. Inicie una sesión en el (o los) Delivery Controller como administrador.
2. Abra Windows PowerShell (con privilegios administrativos). Usando PowerShell, emitirá comandos para hacer que el Delivery Controller confíe en las solicitudes XML enviadas desde StoreFront.

3. Si aún no están cargados, cargue los cmdlets de Citrix escribiendo **Add-PSSapin Citrix*** y presione **Entrar**.
4. Presione Entrar.
5. Escriba **Add-PSSnapin citrix.broker.admin.v2** y presione **Entrar**.
6. Escriba **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**, y presione **Entrar**.
7. Cierre PowerShell.

Configuración de StoreFront

Para configurar SSON en StoreFront y la Interfaz Web, abra Studio en el servidor StoreFront y seleccione **Autenticación -> Agregar o quitar métodos**. Seleccione **PassThrough de dominio**.



Configuración de la Interfaz Web

Para configurar SSON en la Interfaz Web, seleccione **Administración de la Interfaz Web de Citrix -> Sitios de servicios XenApp -> Métodos de autenticación** y habilite **Paso de credenciales**.

La API de FastConnect usa el método de autenticación básica HTTP, que frecuentemente se confunde con métodos de autenticación asociados con el paso de credenciales de dominio (PassThrough), Kerberos y la autenticación integrada de Windows (IWA). Citrix recomienda inhabilitar IWA en StoreFront y en la directiva de grupo ICA.

Configuración de autenticación PassThrough de dominio con Kerberos

Jan 29, 2016

Este tema se aplica solo a conexiones entre Citrix Receiver y StoreFront, XenDesktop o XenApp.

Citrix Receiver para Windows respalda Kerberos para la autenticación PassThrough de dominio en implementaciones que usan tarjetas inteligentes. Kerberos es uno de los métodos de autenticación incluidos en la autenticación de Windows integrada (IWA).

Cuando la autenticación Kerberos está habilitada, Kerberos autentica sin contraseña para Citrix Receiver, y así impide ataques de tipo troyano que intentan tener acceso a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar una sesión en el dispositivo de usuario con cualquier método de autenticación; por ejemplo, un autenticador biométrico, tal como un lector de huellas digitales, y aún acceder a los recursos publicados sin necesidad de otra autenticación.

Citrix Receiver gestiona la autenticación PassThrough con Kerberos del siguiente modo, cuando Citrix Receiver, StoreFront, XenDesktop y XenApp están configurados para usar autenticación con tarjeta inteligente y el usuario inicia una sesión con una de ellas:

1. El servicio Single Sign-on de Citrix Receiver captura el PIN de la tarjeta inteligente.
2. Citrix Receiver usa la autenticación integrada de Windows (Kerberos) para autenticar al usuario en StoreFront. A continuación, StoreFront entrega a Receiver la información referente a las aplicaciones y escritorios virtuales disponibles. Nota: No tiene que usar autenticación Kerberos para este paso. Solo se necesita habilitar Kerberos en Receiver para evitar que se vuelva a pedir el PIN. Si no usa la autenticación Kerberos, Receiver autentica en StoreFront usando las credenciales de la tarjeta inteligente.
3. El motor de HDX (antes conocido como cliente ICA) pasa el PIN de la tarjeta inteligente a XenDesktop o XenApp para iniciar la sesión Windows del usuario. A continuación, XenDesktop o XenApp entregan los recursos solicitados.

Para usar autenticación Kerberos con Citrix Receiver, asegúrese de que la configuración de Kerberos cumple lo siguiente.

- Kerberos solo funciona entre Receiver y servidores que pertenecen a los mismos dominios de Windows o a dominios que son de confianza. Los servidores también deben ser fiables para la delegación, una opción que se configura mediante la herramienta de administración de usuarios y equipos de Active Directory.
- Kerberos debe estar habilitado en el dominio y en XenDesktop y XenApp. Para mayor seguridad y para asegurarse de que se utiliza Kerberos, inhabilite las demás opciones que no sean Kerberos IWA en el dominio.
- El inicio de sesión con Kerberos no está disponible para conexiones de Servicios de escritorio remoto configuradas para usar autenticación Básica, para usar siempre la información de inicio de sesión especificada o para pedir siempre una contraseña.

El resto de este tema describe cómo configurar la autenticación PassThrough de dominio para los escenarios de uso más frecuentes. Si migra a StoreFront desde la Interfaz Web y previamente utilizó una solución de autenticación personalizada, póngase en contacto con un representante del servicio de asistencia de Citrix Support para obtener más información.

> ## Advertencia
>
> Parte de la configuración descrita en este tema incluye modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que

los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Si no está familiarizado con implementaciones de tarjeta inteligente en un entorno XenDesktop, le recomendamos que consulte la información sobre tarjetas inteligentes que figura en la sección Protección de la seguridad del entorno de la documentación de XenDesktop antes de continuar.

Cuando instale Citrix Receiver, incluya la opción siguiente en la línea de comandos:

- /includeSSON
  Esta opción instala el componente Single Sign-on en el equipo unido a un dominio, lo que habilita a Receiver para autenticarse en StoreFront usando IWA (Kerberos). El componente Single Sign-on guarda el PIN de la tarjeta inteligente, que luego es utilizado por el motor HDX cuando comunica de forma remota el hardware de tarjeta inteligente y las credenciales a XenDesktop. XenDesktop selecciona automáticamente un certificado desde la tarjeta inteligente y obtiene el PIN desde el motor de HDX.

  Hay una opción relacionada, ENABLE_SSON, que está habilitada de manera predeterminada y debe dejarse así.

  Si hay una directiva de seguridad que impide la habilitación del Single Sign-on en un dispositivo, configure Receiver con la directiva siguiente:

  Vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password

  Nota: En este caso, usted quiere permitir que el motor de HDX use la autenticación de tarjeta inteligente y no Kerberos, de modo que no use la opción ENABLE_KERBEROS=Yes, ya que forzaría al motor de HDX a usar Kerberos.

Para aplicar la configuración, reinicie Receiver en el dispositivo del usuario.

Para configurar StoreFront:

- En el archivo default.ica, ubicado en el servidor StoreFront, establezca DisableCtrlAltDel con false.
  Nota: Este paso no es necesario si todas las máquinas cliente ejecutan Receiver para Windows versión 4.2 o posterior.
- Cuando configure el servicio de autenticación en el servidor StoreFront, marque la casilla PassThrough de dominio. Este parámetro habilita la autenticación de Windows integrada (IWA). No es necesario marcar la casilla Tarjeta inteligente a menos que también tenga clientes que no estén unidos a un dominio conectándose a StoreFront con tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configuración del servicio de autenticación en la documentación de StoreFront.

La API de FastConnect usa el método de autenticación básica HTTP, que frecuentemente se confunde con métodos de autenticación asociados con el paso de credenciales de dominio (PassThrough), Kerberos y la autenticación integrada de Windows (IWA). Citrix recomienda inhabilitar IWA en StoreFront y en la directiva de grupo ICA.

Configuración de la autenticación con tarjeta inteligente

Jan 29, 2016

Receiver para Windows respalda las siguientes funciones de autenticación con tarjeta inteligente. Para obtener información sobre la configuración de XenDesktop y StoreFront, consulte la documentación de esos componentes. Este tema describe la configuración de Receiver para Windows para usar tarjetas inteligentes.

- **Autenticación PassThrough (Single Sign-on)**: La autenticación PassThrough captura las credenciales de la tarjeta inteligente cuando los usuarios inician una sesión en Receiver. Receiver usa de este modo las credenciales capturadas:
  - Los usuarios de dispositivos que pertenecen a un dominio que inician una sesión en Receiver usando una tarjeta inteligente pueden iniciar aplicaciones y escritorios virtuales sin necesidad de volver a autenticarse.
  - Los usuarios de dispositivos que no pertenecen a un dominio que inician una sesión en Receiver usando una tarjeta inteligente deben introducir de nuevo sus credenciales para poder iniciar aplicaciones y escritorios virtuales.

  La autenticación PassThrough requiere una configuración de StoreFront y Receiver.

- **Autenticación bimodal**: La autenticación bimodal ofrece a los usuarios la opción de usar una tarjeta inteligente o introducir su nombre de usuario y contraseña. Esta función resulta útil cuando no se puede usar la tarjeta inteligente por alguna razón (por ejemplo, si el usuario la olvidó en casa o el certificado de inicio de sesión caducó). Los almacenes dedicados deben configurarse uno por sitio. Para ello, mediante el método DisableCtrlAltDel establecido en False para permitir el uso de tarjetas inteligentes. La autenticación bimodal requiere una configuración de StoreFront. Si hay un dispositivo NetScaler Gateway en la implementación, también será necesario configurarlo.
  Con la autenticación bimodal, administrador de StoreFront tiene ahora la oportunidad de ofrecer al usuario la posibilidad de autenticarse con nombre y contraseña o con tarjeta inteligente en un mismo almacén, seleccionando estas opciones en la consola de StoreFront. Consulte la documentación de StoreFront.

- **Varios certificados:** Puede haber varios certificados disponibles para una única tarjeta inteligente y si se utilizan varias tarjetas inteligentes. Cuando un usuario introduce una tarjeta inteligente en el lector de tarjetas, los certificados están disponibles para todas las aplicaciones ejecutadas en el dispositivo del usuario, incluido Receiver. Para cambiar cómo se seleccionan los certificados, configure Receiver.
- **Autenticación por certificado del cliente**: La autenticación por certificado del cliente requiere la configuración de NetScaler Gateway/Access Gateway y StoreFront.
  - Para acceder a los recursos de StoreFront a través de NetScaler Gateway/Access Gateway, es posible que los usuarios tengan que volver a autenticarse después de extraer una tarjeta inteligente.
  - Cuando la configuración SSL de NetScaler Gateway/Access Gateway está definida como autenticación por certificado de cliente obligatoria, la operación es más segura. No obstante, la autenticación por certificado de cliente obligatoria no es compatible con la autenticación bimodal.
- **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 XenDesktop.
- **Aplicaciones habilitadas para el uso de tarjeta inteligente**: Las aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, permiten a los usuarios firmar digitalmente o cifrar documentos disponibles en las sesiones de aplicación o escritorio virtual.

Requisitos previos

Este tema presupone que el lector conoce los temas sobre tarjetas inteligentes en la documentación de XenDesktop y StoreFront.

Limitaciones

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- Receiver para Windows no guarda la elección de certificado del usuario, pero puede guardar el PIN si se configura así. El PIN solo se almacena en caché en la memoria no paginada durante la sesión del usuario. No se guarda en disco en ningún momento.
- Receiver para Windows no reconecta sesiones cuando se introduce una tarjeta inteligente.
- Cuando está configurado para la autenticación con tarjeta inteligente, Receiver para Windows no respalda Single Sign-on en redes privadas virtuales (VPN) ni el inicio previo de sesiones. 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.
- Las comunicaciones de Receiver para Windows Updater con citrix.com y Merchandising Server no son compatibles con la autenticación con tarjeta inteligente en NetScaler Gateway.

> **Advertencia**
>
> Parte de la configuración descrita en este tema incluye modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Para configurar Receiver, incluya la siguiente opción de línea de comandos cuando lo instale:

- ENABLE_SSON=Yes
  Single Sign-on es otro término para el paso de credenciales/autenticación PassThrough. Cuando se habilita este parámetro Receiver no muestra una segunda petición de PIN al usuario.

O, puede realizar la configuración a través de esta directiva y unos cambios en el Registro:

- Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
- Establezca SSONCheckEnabled con false en cualquiera de estas claves de Registro si el componente Single Sign-On no está instalado. La clave impide que el Authentication Manager en Receiver compruebe el componente Single Sign-on, lo que permite a Receiver autenticarse con StoreFront.
  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

De forma alternativa, es posible habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos. Para habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos, instale Receiver con las opciones de la línea de comandos que se muestran más abajo. Esto requiere privilegios de administrador. La máquina no necesita estar unida a un dominio.

- /includeSSON instala Single Sign-On (autenticación PassThrough). Habilita el almacenamiento en caché de credenciales y el uso de la autenticación PassThrough de dominio.
- Si el usuario está iniciando una sesión en el punto final con otro método distinto de la tarjeta inteligente para la autenticación en Receiver (por ejemplo, con nombre de usuario y contraseña), la línea de comandos es:
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  Esto evita que se capturen las credenciales al iniciar la sesión y permite a Receiver guardar el PIN al iniciar una sesión en Receiver.

- Vaya a Directiva > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User authentication > Local user name and password
  Enable pass-through authentication. Dependiendo de la configuración y los parámetros de seguridad, puede que tenga que seleccionar la opción Allow pass-through authentication for all ICA para que la autenticación PassThrough funcione.

Para configurar StoreFront:

- Al configurar el servicio de autenticación, marque la casilla Tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte Configuración del servicio de autenticación en la documentación de StoreFront.

1. Importe el certificado raíz de la entidad de certificación en el almacén de claves del dispositivo.
2. Instale el middleware de su proveedor de servicios criptográficos.
3. Instale y configure Receiver para Windows.

De manera predeterminada, si hay varios certificados que son válidos, Receiver pide al usuario que elija uno de la lista. De manera alternativa, puede configurar Receiver para usar el certificado predeterminado (según lo indique el proveedor de la tarjeta inteligente) o el certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible.

Un certificado válido debe reunir estas características:

- La fecha y hora actuales según el reloj del equipo local está dentro del periodo de validez del certificado.
- La clave pública Sujeto debe usar el algoritmo de RSA y tener una longitud de 1024, 2048 ó 4096 bits.
- El campo Uso de la clave debe contener Firma digital.
- El Nombre alternativo del sujeto debe contener el nombre principal del usuario (UPN).
- El campo Uso mejorado de claves debe contener Inicio de sesión de tarjeta inteligente y Autenticación del cliente o Todos los usos de la clave.
- Una de las entidades de certificación en la cadena de emisores del certificado debe coincidir con uno de los nombres distinguidos (DN) enviado por el servidor durante el protocolo de enlace TLS.

Cambie el modo en que se seleccionan los certificados, usando alguno de estos métodos:

- En la línea de comandos de Receiver, especifique la opción AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }.
  La opción predeterminada es "Prompt" (Preguntar). Para SmartCardDefault (predeterminado de la tarjeta inteligente) o LatestExpiry (fecha de caducidad más lejana), si hay varios certificados que cumplen esos criterios, Receiver pide al usuario que elija uno.

- Agregue el siguiente valor a la clave de Registro en HKCU o HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }.
  Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.

De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de Receiver en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. Receiver pide a los usuarios que introduzcan un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Si el sitio o la tarjeta inteligente tiene unos requisitos de seguridad más estrictos como, por ejemplo, prohibir el almacenamiento del PIN en caché por proceso o por sesión, puede configurar Receiver para que use los componentes del CSP para gestionar las entradas de PIN, incluida la solicitud del PIN.

Cambie el modo en que se gestiona la entrada del PIN, usando alguno de estos métodos:

- En la línea de comandos de Receiver, especifique la opción AM_SMARTCARDPINENTRY=CSP.
- Agregue el siguiente valor a la clave de Registro HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP.

Cómo habilitar la comprobación de la lista de revocación de certificados

Jan 29, 2016

Cuando está habilitada la comprobación de la lista de revocación de certificados (CRL), Receiver verifica si el certificado del servidor se ha revocado. Al obligar a Citrix Receiver a realizar esta verificación, se puede mejorar la autenticación criptográfica del servidor, así como la seguridad general de las conexiones TLS entre los dispositivos de usuario y el servidor.

Se pueden habilitar varios niveles de verificación de revocación de certificados (CRL). Por ejemplo, se puede configurar Citrix Receiver para que verifique solo la lista local de certificados, o para que verifique las listas de certificados locales y de red. Además, se puede configurar la verificación de certificados para permitir que los usuarios inicien sesiones solo cuando se verifiquen todas las listas de revocación de certificados.

Si va a realizar este cambio en un equipo local, salga de Receiver si se está ejecutando. Compruebe que todos los componentes de Citrix Receiver, incluida la Central de conexiones, estén cerrados.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades y seleccione Habilitada.
8. En el menú desplegable Verificación CRL, elija una de las opciones.
   - Inhabilitada No se lleva a cabo la verificación de revocación.
   - Sólo verifique CRL almacenados localmente. CRL que se instalaron o descargaron anteriormente y que se utilizan en la validación del certificado. Si se revoca el certificado, la conexión falla.
   - Requiere CRL para la conexión. Se verifican los CRL locales y de los emisores de certificados pertinentes en la red. Si se revoca el certificado o no se encuentra, la conexión falla.
   - Obtenga los CRL de la red. Se verifican los CRL de los emisores de certificados pertinentes. Si se revoca el certificado, la conexión falla.

   Si no establece la verificación CRL, se establecerá de forma predeterminada en Sólo verifique CRL almacenados localmente.

Protección de las comunicaciones de Receiver

Jan 29, 2016

Para proteger la comunicación entre los sitios de XenDesktop o las comunidades de servidores XenApp y Citrix Receiver, se pueden integrar las conexiones de Citrix Receiver a través de tecnologías de seguridad como las siguientes:

- Citrix NetScaler Gateway (Access Gateway). Para obtener más información, consulte los temas de esta sección además de la documentación de NetScaler Gateway y StoreFront.
  Nota: Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores StoreFront y los dispositivos de los usuarios.
- 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.
- Configuración de confianza del servidor.
- Solamente para implementaciones de XenApp o la Interfaz Web; no se aplica a XenDesktop 7: un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.
- Para implementaciones de XenApp o Interfaz Web solamente; no se aplica a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 o XenApp 7.5: Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security).
- Para XenApp 7.6 y XenDesktop 7.6, puede habilitar una conexión SSL directamente entre los usuarios y los VDA. (Consulte SSL para ver información sobre cómo configurar SSL para XenApp 7.6 o XenDesktop 7.6).

Citrix Receiver es compatible y funciona con entornos en los que se utilizan las plantillas de seguridad de escritorio de Microsoft Specialized Security - Limited Functionality (SSLF). Estas plantillas reciben respaldo en varias plataformas de Windows. Consulte las guías de seguridad de Windows disponibles en http://technet.microsoft.com para obtener más información sobre las plantillas y su configuración.

Conexión con NetScaler Gateway

Jan 29, 2016

Para permitir que los usuarios remotos se conecten a través de NetScaler Gateway, configúrelo para que funcione con StoreFront.

- Para implementaciones de StoreFront: puede permitir conexiones de usuarios remotos o internos en StoreFront a través de NetScaler Gateway integrando NetScaler Gateway y StoreFront. Esta implementación permite que los usuarios se conecten con StoreFront para obtener acceso a las aplicaciones y los escritorios virtuales. Los usuarios se conectan mediante Citrix Receiver.

> ## Nota
>
> El plug-in de análisis de punto final o EPA (End Point Analysis) de NetScaler Gateway no respalda el uso de Receiver para Windows nativo.

Para obtener información sobre la configuración de estas conexiones, consulte Integración de NetScaler Gateway con XenMobile App Edition y los demás temas incluidos en ese nodo en Citrix eDocs. En los siguientes temas, se ofrece información sobre los parámetros que se requieren en Receiver para Windows:

- Configuración de perfiles y directivas de sesión para XenMobile App Edition
- Creación del perfil de sesión para Receiver para XenMobile App Edition
- Configuración de directivas personalizadas de acceso sin cliente para Receiver

Para permitir que los usuarios remotos se conecten mediante NetScaler Gateway a la implementación de la Interfaz Web, configure NetScaler Gateway para que funcione con la Interfaz Web, como se describe en Cómo dar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web y los temas secundarios correspondientes en Citrix eDocs.

Conexión con NetScaler Gateway Enterprise Edition

Aug 25, 2016

Para permitir que los usuarios remotos se conecten a través de NetScaler Gateway, configúrelo para que funcione con StoreFront y AppController (un componente de CloudGateway).

- Para implementaciones de StoreFront: puede permitir conexiones de usuarios remotos o internos en StoreFront a través de Access Gateway integrando Access Gateway y StoreFront. Esta implementación permite que los usuarios se conecten con StoreFront para obtener acceso a las aplicaciones y los escritorios virtuales. Los usuarios se conectan mediante Citrix Receiver.
- Para implementaciones de AppController: puede permitir conexiones de usuarios remotos con AppController integrando Access Gateway y AppController. Con esta implementación, los usuarios pueden conectarse a AppController para obtener aplicaciones Web y de software como servicio (SaaS), y pueden usar los servicios de ShareFile Enterprise con Receiver. Los usuarios se conectan mediante Receiver o mediante el NetScaler Gateway Plug-in.

Para obtener información sobre la configuración de estas conexiones, consulte Integrating NetScaler Gateway with CloudGateway y los demás temas incluidos en ese nodo del sitio de documentación de productos de Citrix. En los siguientes temas, se ofrece información sobre los parámetros que se requieren en Receiver para Windows:

- Configuración de directivas de sesión y perfiles de CloudGateway
- Creación del perfil de sesión destinado a Receiver para CloudGateway Enterprise
- Creación del perfil de sesión destinado a Receiver para CloudGateway Express
- Configuración de directivas personalizadas de acceso sin cliente para Receiver

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 Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface y los subtemas correspondientes en Citrix eDocs.

Conexión con Secure Gateway

Jan 29, 2016

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 es necesario configurar Receiver si se utiliza Secure Gateway en 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 que ejecuta la Interfaz Web para conectarse a los servidores que ejecutan Secure Gateway. Consulte los temas de la Interfaz Web para obtener información sobre la configuración de los parámetros del servidor proxy para Receiver.

Si se instala Secure Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Gateway Proxy en modo Relay. Consulte los temas de Secure Gateway a fin de obtener más información sobre el modo Relay.

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.mi_empresa.com es un nombre de dominio completo porque contiene el nombre de host (mi_equipo), un dominio intermedio (mi_empresa) y un dominio superior (com). Por lo general, la combinación de nombre de dominio intermedio y dominio superior (mi_empresa.com) se conoce como nombre de dominio.

Conexión a través de un firewall

Jan 29, 2016

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.

Cumplimiento de relaciones de confianza

Jan 29, 2016

La configuración de confianza del servidor está diseñada para identificar y forzar relaciones de confianza en las conexiones de Receiver. La relación de confianza aumenta la sensación de seguridad de los administradores y usuarios de Receiver respecto a la integridad de la información en los dispositivos de usuario y evita el uso fraudulento o malintencionado de las conexiones de Receiver.

Cuando esta función está habilitada, los clientes pueden especificar los requisitos de confianza y determinar si confían en la conexión con el servidor. Por ejemplo, si Receiver se conecta a una dirección determinada (como, por ejemplo, https://*.citrix.com) con un tipo de conexión específico (por ejemplo, TLS) se redirige a una zona de confianza en el servidor.

Cuando se habilita la configuración de servidor de confianza, los servidores conectados deben residir en la zona de sitios de confianza de Windows. (Para ver instrucciones detalladas sobre cómo agregar servidores a la zona de sitios de confianza de Windows, consulte la ayuda en pantalla de Internet Explorer).

Para habilitar las configuraciones de confianza del servidor

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Expanda la carpeta Plantillas administrativas en el nodo Configuración del usuario.
7. Desde el Editor de directivas de grupo, vaya a Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > Configure trusted server configuration.
8. En el menú Acción, elija Propiedades y seleccione Habilitada.

Nivel de elevación y wfcrun32.exe

Jan 29, 2016

Cuando se habilita el control de cuentas de usuario (UAC) en los dispositivos que ejecutan Windows 8, Windows 7 o Windows Vista, sólo los procesos que se encuentren en el mismo nivel de integridad o elevación que wfcrun32.exe pueden iniciar las aplicaciones virtuales.

Ejemplo 1:

Cuando wfcrun32.exe se ejecuta como un usuario normal (no elevado), otros procesos como Receiver deben ejecutarse como usuario normal para poder iniciar aplicaciones a través de wfcrun32.

Ejemplo 2:

Cuando wfcrun32.exe se ejecuta en modo elevado, otros procesos como Receiver, la Central de conexiones y aplicaciones de terceros que usan el objeto Cliente ICA y que se están ejecutando en modo no elevado no se pueden comunicar con wfcrun32.exe.

Conexión de Receiver a través de un servidor proxy

Jan 29, 2016

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

Los servidores proxy se usan para limitar el acceso hacia y desde la red, y para administrar conexiones entre los dispositivos Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.

En la comunicación con la comunidad de servidores, Receiver utiliza los parámetros de servidor proxy configurados de forma remota en el servidor que ejecuta Receiver para Web o la Interfaz Web. Para obtener más información sobre la configuración de servidores proxy, consulte la documentación de StoreFront o de la Interfaz Web.

En la comunicación con el servidor Web, Receiver utiliza los parámetros de servidor proxy configurados a través de la configuración de Internet del explorador Web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros de Internet del explorador Web predeterminado en el dispositivo de usuario según corresponda.

Conexión con el Traspaso SSL (Secure Sockets Layer Relay)

Nov 03, 2016

Este tema se aplica solo a XenDesktop 7.6 o versiones posteriores, o XenApp 7.5.

Puede integrar Receiver con los servicios de Traspaso SSL (Secure Sockets Layer Relay). Receiver respalda los protocolos TLS. Receiver para Windows 4.2 solo respalda TLS 1.0.

- TLS (Transport Layer Security) 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 también pueden exigir el uso de cifrado validado, como FIPS 140 (Estándar federal de procesamiento de información). FIPS 140 es un estándar para cifrado.

Este tema se aplica solo a XenDesktop 7.6 o versiones posteriores, o XenApp 7.5.

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

Si configuró el Traspaso SSL en un puerto de escucha que no sea 443, debe especificar en el plug-in el puerto de escucha no estándar.

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

- Entre los clientes con seguridad TLS habilitada y un servidor. Las conexiones que utilizan el cifrado TLS están marcadas con un icono de candado en la Central de conexiones de Citrix.
- Con un servidor que ejecuta la Interfaz Web, entre el equipo que ejecuta el servidor XenApp y el servidor Web.

Para obtener más información sobre la configuración del Traspaso SSL para proteger la instalación, consulte la documentación de XenApp.

Requisitos del dispositivo del usuario

Además de los requisitos del sistema, debe asegurarse de que:

- El dispositivo de usuario admita el cifrado de 128 bits
- El dispositivo de usuario disponga de un certificado raíz instalado que pueda verificar la firma de la entidad emisora de certificados con el certificado del servidor
- Receiver conoce el número de puerto de escucha TCP utilizado por el servicio de Traspaso SSL en la comunidad de servidores.
- Se han aplicado todos los Service Packs y actualizaciones recomendadas por Microsoft.

Si utiliza Internet Explorer y no conoce el nivel de cifrado del sistema, vaya al sitio Web de Microsoft en

http://www.microsoft.com para instalar un Service Pack que proporcione el cifrado de 128 bits.

Importante: Receiver admite longitudes de claves de certificado de hasta 4096 bits. Asegúrese de que las longitudes de bits de los certificados intermedios y del certificado raíz de la entidad emisora de certificados y de los certificados del servidor no excedan la longitud en bits que admite Receiver, dado que podría fallar la conexión.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration del plug-in (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y, a continuación, escriba un número de puerto nuevo en el cuadro de texto Allowed SSL servers con el siguiente formato: servidor:número de puerto de traspaso SSL, donde número de puerto de traspaso SSL es el número del puerto de escucha. Puede utilizar un comodín para especificar varios servidores. Por ejemplo, *.Test.com:número de puerto de traspaso SSL hace coincidir todas las conexiones Test.com a través del puerto especificado.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya agregó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada, e introduzca una lista de servidores de confianza, separados por comas, y el nuevo número de puerto en el cuadro Allowed SSL servers con el formato siguiente: nombre-de-servidor:número-de-puerto-de-Traspaso-SSL,nombre-de-servidor:número-de-puerto-de-Traspaso-SSL, donde número-de-puerto-de-Traspaso-SSL es el número del puerto de escucha. Puede especificar una lista de servidores SSL de confianza separados por comas similar a este ejemplo:
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
   que se traduce a lo siguiente en el archivo appsrv.ini de ejemplo: [Word]
   SSLProxyHost=csghq.Test.com:443

   [Excel]

```
SSLProxyHost=csghq.Test.com:444

[Notepad]
SSLProxyHost=fred.Test.com:443
```

Configuración y habilitación de Receiver para TLS

Nov 03, 2016

Este tema se aplica solo a XenDesktop 7.6 o versiones posteriores, o XenApp 7.5.

Para forzar la conexión de Receiver con TLS, se debe especificar TLS en el servidor Secure Gateway o en el servicio Traspaso SSL. Para obtener más información, consulte los temas de la documentación de Secure Gateway o del servicio Traspaso de SSL.

Además, asegúrese de que el dispositivo de usuario cumple todos los requisitos del sistema.

Para usar el cifrado TLS para todas las comunicaciones de Receiver, configure el dispositivo de usuario, Receiver, y el servidor que ejecuta la Interfaz Web (en caso de que use la Interfaz Web). Para obtener más información sobre cómo proteger las comunicaciones con StoreFront, consulte los temas de "Seguridad" en la documentación de StoreFront, en la Documentación de productos Citrix.

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.

Receiver respalda entidades emisoras de certificados compatibles con Windows. Los certificados raíz para estas entidades se instalan con Windows y se administran a través de las utilidades de Windows. Estos certificados son los mismos que utiliza Microsoft Internet Explorer.

Si utiliza su propia entidad emisora de certificados, debe obtener un certificado raíz de esa entidad emisora de certificados e instalarlo en cada dispositivo de usuario. Microsoft Internet Explorer y Receiver utilizarán este certificado.

Puede instalar el certificado raíz a través de otros métodos de administración y distribución, como:

- Con el administrador de perfiles y el asistente de configuración del Kit de administración de Internet Explorer (IEAK) de Microsoft.
- Con herramientas de distribución de terceros.

Asegúrese de que los certificados instalados por Windows cumplen los requisitos de seguridad de su organización; o bien, utilice los certificados emitidos por la entidad emisora de certificados de la organización.

1. Para usar TLS con el fin de cifrar los datos de enumeración e inicio de aplicaciones enviados entre Receiver y el servidor que ejecuta la Interfaz Web, configure los parámetros apropiados mediante la Interfaz Web. Debe incluir el nombre de equipo del servidor XenApp donde está el certificado SSL.
2. Para usar una conexión HTTP segura (HTTPS) para cifrar la información de configuración que se envía entre Receiver y el servidor que ejecuta la Interfaz Web, introduzca la dirección URL del servidor con el formato https://nombre_servidor. En el área de notificación de Windows, haga clic con el botón secundario en el icono de Receiver y seleccione Preferencias.
3. Haga clic con el botón secundario en la entrada Online Plug-in de Estado del plug-in y elija Cambiar servidor.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar esto en un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a usar Active Directory.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y luego, elija la configuración TLS en los menús desplegables.
   - Configure la versión de TLS a TLS o para habilitar TLS elija Detect all. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS.
   - Configure el conjunto de cifrado SSL (SSL ciphersuite) con Detect version para que Receiver pueda negociar un conjunto de cifrado gubernamental y comercial adecuado. Puede restringir el conjunto de cifrado, ya sea a uno gubernamental o a uno comercial.
   - Configure la verificación CRL (CRL verification) con el valor Require CRLs for connection que requiere que Receiver intente obtener listas de revocación de certificados (CRL) de los emisores de certificado relevantes.

Si cambia esto en un equipo local, cierre todos los componentes de Receiver, incluso la Central de conexiones.
Para cumplir con los requisitos de seguridad FIPS 140, utilice la plantilla de directivas de grupo a fin de configurar los parámetros o incluya los parámetros en el archivo Default.ica en el servidor donde se ejecuta la Interfaz Web. Para obtener más información sobre el archivo Default.ica, consulte la información sobre la Interfaz Web.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla icaclient al Editor de directivas de grupo, puede omitir los pasos 3 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione icaclient.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, expanda Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > Network routing > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y del menú elija la configuración correcta.
   - Configure TLS Version con el valor TLS o Detect all para habilitar TLS. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS.
   - Configure SSL ciphersuite con Government.
   - Configure CRL verification con Require CRLs for connection.

Al utilizar la Interfaz Web, especifique el nombre de equipo del servidor que aloja el certificado SSL. Consulte la información sobre la Interfaz Web para obtener más detalles sobre cómo usar TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

1. En el menú Configuración, seleccione Configuración del servidor.
2. Elija Usar SSL/TLS para las comunicaciones entre los clientes y el servidor Web.
3. Guarde los cambios.

La elección de SSL/TLS hace que las direcciones URL pasen a usar el protocolo HTTPS.

Es posible configurar el servidor XenApp para que utilice TLS a fin de proteger las comunicaciones entre Receiver y el servidor.

1. En la consola de administración de Citrix para el servidor XenApp, abra el cuadro de diálogo Propiedades para la aplicación que quiera proteger.
2. Seleccione Avanzado > Opciones del cliente y Habilitar SSL y TLS.
3. Repita estos pasos para cada aplicación que desee proteger.

Al utilizar la Interfaz Web, especifique el nombre de equipo del servidor que aloja el certificado SSL. Consulte la información sobre la Interfaz Web para obtener más detalles sobre cómo usar TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

Es posible configurar Receiver para que use TLS con el fin de proteger la seguridad de las comunicaciones entre Receiver y el servidor que ejecuta la Interfaz Web.

En este procedimiento se presupone que existe un certificado raíz válido instalado en el dispositivo de usuario. Para obtener más detalles, consulte Instalación de certificados raíz en dispositivos de usuario.

1. En el área de notificación de Windows, haga clic con el botón secundario en el icono de Receiver y seleccione Preferencias.
2. Haga clic con el botón secundario en la entrada Online Plug-in de Estado del plug-in y elija Cambiar servidor.
3. La pantalla Cambiar servidor muestra la dirección URL configurada. Introduzca la dirección URL del servidor en el cuadro de texto siguiendo el formato https://nombre_de_servidor para cifrar los datos de configuración mediante TLS.
4. Haga clic en Actualizar para aplicar los cambios.
5. Habilite TLS en el explorador Web del dispositivo del usuario. Para obtener más información, consulte la Ayuda en línea del explorador.

Protección ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza con ICA File Signing

Jan 29, 2016

Este tema solo es aplicable a implementaciones con Interfaz Web que usan Plantillas administrativas.

La función ICA File Signing (firma de archivos ICA) permite proteger a los usuarios ante inicios de escritorios y aplicaciones no autorizados. Citrix Receiver verifica si el inicio de la aplicación o del escritorio fue generado desde una fuente de confianza, basándose en una directiva de administración, y protege al usuario frente a inicios originados en servidores que no son de confianza. Esta directiva de seguridad de Receiver para la verificación de firmas de inicio de aplicaciones o escritorios se puede configurar mediante objetos de directiva de grupo, StoreFront o Citrix Merchandising Server. La función ICA File Signing no está habilitada de forma predeterminada. Para obtener más información sobre cómo habilitar ICA File Signing para StoreFront, consulte la documentación de StoreFront.

En los entornos con Interfaz Web, la Interfaz Web habilita y configura los inicios de escritorios y aplicaciones para incluir una firma durante el proceso de inicio mediante el servicio Citrix ICA File Signing. Este servicio permite firmar los archivos ICA con un certificado del almacén de certificados personal del equipo.

Citrix Merchandising Server con Receiver permite configurar e iniciar la verificación de firmas mediante el asistente de la consola de administración Citrix Merchandising Server Adminstrator Console > Deliveries para agregar sellos de certificados de confianza.

Para usar objetos de directiva de grupo para habilitar y configurar la verificación de firmas de inicio de aplicaciones o escritorios, siga este procedimiento:

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de gpedit.msc localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.
   Nota: Si ya importó la plantilla ica-file-signing.adm al Editor de directivas de grupo, puede omitir los pasos 2 a 5.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta de configuración de Receiver (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione ica-file-signing.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, vaya a Plantillas administrativas> Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver y vaya a Enable ICA File Signing.
7. Si elige Habilitada, podrá agregar sellos de certificados con firma a la lista blanca de certificados de confianza, o bien quitar los sellos de certificados con firma de la lista blanca haciendo clic en Mostrar y luego use la ventana Mostrar contenido. Puede copiar y pegar los sellos de certificados con firma desde las propiedades de los certificados. Use el menú desplegable Directiva para seleccionar Permitir inicios con firma solamente (más seguro) o Preguntar al usuario en inicios sin firma (menos seguro).

Opción	Descripción
Permitir inicios	Permite inicios de escritorios o aplicaciones con firma solamente desde servidores de confianza.

Opción	Descripción
con firma solamente (más seguro)	Si un inicio de escritorio o aplicación no dispone de una firma válida, se mostrará al usuario un mensaje de advertencia de seguridad en Receiver. El usuario no podrá continuar y se bloqueará el inicio no autorizado.
Preguntar al usuario en inicios sin firma (menos seguro)	Pregunta al usuario cada vez que se realizan intentos de inicio de aplicación o escritorio sin firma o con una firma no válida. El usuario tiene la opción de continuar el inicio de la aplicación o cancelar el inicio (valor predeterminado).

Cuando se seleccione un certificado de firma digital, Citrix recomienda elegir a partir de la lista siguiente, en el orden siguiente:

1. Adquiera un certificado con firma de código o un certificado con firma SSL a partir de una entidad de certificados pública (AC).
2. Si su empresa dispone de una entidad de certificados privada, cree un certificado con firma de código o un certificado con firma SSL a través de la entidad de certificados privada.
3. Utilice un certificado SSL existente, como el certificado del servidor de la Interfaz Web.
4. Cree un certificado raíz nuevo y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

Configuración de un explorador Web y un archivo ICA para habilitar Single Sign-on y administrar conexiones seguras a servidores de confianza

Jan 29, 2016

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

Para usar Single Sign-on (SSO) y administrar conexiones seguras en servidores de confianza, agregue la dirección del sitio del servidor Citrix en la Intranet local o las zonas de Sitios de confianza en Herramientas > Opciones de Internet > Seguridad de Internet Explorer del dispositivo de usuario. La dirección puede incluir los formatos de comodines (*) admitidos por Internet Security Manager (ISM) o pueden ser específicos como protocolo ://URL[:puerto].

Se debe usar el mismo formato tanto en el archivo ICA como en las entradas de sitios. Por ejemplo, si especificó un nombre completo de dominio (FQDN) en el archivo ICA, deberá especificar un FQDN en la entrada de zonas de sitios. Las conexiones XenDesktop solo usan un formato de nombre de grupo de escritorio.

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://nombre_host

http[s]://fqdn.ejemplo.com

http[s]://*.ejemplo.com

http[s]://nombre-empresa.*.ejemplo.com

http[s]://*.ejemplo.co.uk

escritorio://nombre-20grupo

ica[s]://servidorxa1

ica[s]://servidorxa1.ejemplo.com

Agregue la dirección exacta al sitio de la Interfaz Web en la zona de sitios.

Ejemplos de direcciones de sitios Web

https://mi.empresa.com

http://10.20.30.40

http://servidor-host:8080

https://traspaso-SSL:444

Agregue la dirección con el formato escritorio://Nombre de grupo de escritorio. Si el nombre del grupo contiene espacios, sustituya cada espacio con -20.

Use uno de los formatos siguientes en el archivo ICA para la dirección del sitio del servidor Citrix. Use el mismo formato para agregarlo a las zonas Intranet local o Sitios de confianza en Herramientas > Opciones de Internet > Seguridad de Internet Explorer del dispositivo de usuario.

Ejemplo de entrada HttpBrowserAddress en archivo ICA

HttpBrowserAddress=XMLBroker.ServidorXenapp.ejemplo.com:8080

Ejemplos de entradas de dirección de servidor XenApp en archivo ICA

Si el archivo ICA contiene solo el campo **Dirección** del servidor XenApp, use uno de los formatos de entrada siguientes:

icas://10.20.30.40:1494

icas://mi.servidor-xenapp.empresa.com

ica://10.20.30.40

Configuración de los permisos de los recursos del cliente

Mar 08, 2016

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

Puede configurar los permisos de recursos del cliente utilizando áreas para sitios restringidos y de confianza mediante:

- La adición del sitio de la Interfaz Web a la lista de sitios de confianza.
- La modificación de los parámetros nuevos del Registro

> ## Nota
>
> Debido a las mejoras recientes introducidas en Citrix Receiver, el procedimiento .ini disponible en las versiones anteriores del plug-in/Receiver se ha reemplazado con estos procedimientos.

> ## Advertencia
>
> Si edita el Registro de forma incorrecta pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

1. En el menú Herramientas de Internet Explorer, seleccione Opciones de Internet > Seguridad.
2. Seleccione el icono Sitios de confianza y haga clic en el botón Sitios.
3. En el campo de texto Agregar este sitio Web a la zona de, escriba la URL del sitio de la Interfaz Web y haga clic en Agregar.
4. Descargue los parámetros de Registro desde http://support.citrix.com/article/CTX133565 y haga los cambios necesarios en el Registro. Use SsonRegUpx86.reg para los dispositivos de usuario de Win32 y SsonRegUpx64.reg para los dispositivos de usuario de Win64.
5. Cierre la sesión y luego inicie una sesión nuevamente en el dispositivo de usuario.

1. Descargue los parámetros de Registro desde http://support.citrix.com/article/CTX133565 e importe los parámetros en cada uno de los dispositivos de usuario. Use SsonRegUpx86.reg para los dispositivos de usuario de Win32 y SsonRegUpx64.reg para los dispositivos de usuario de Win64.
2. En el editor del Registro, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust y en las áreas apropiadas, cambie el valor predeterminado a los valores de acceso requeridos para cualquiera de los recursos siguientes:

Clave de recurso	Recurso
FileSecurityPermission	Unidades del cliente
MicrophoneAndWebcamSecurityPermission	Micrófonos y cámaras Web
ScannerAndDigitalCameraSecurityPermission	USB y otros dispositivos

Valor	Descripción
0	Sin acceso
1	Acceso de solo lectura
2	Acceso completo
3	Solicitar acceso al usuario

Cuando Citrix Receiver está enumerando aplicaciones y comunicándose con Storefront, se usa la criptografía de la plataforma Windows.

Para conexiones TCP entre Citrix Receiver y XenApp/XenDesktop, Citrix Receiver respalda el uso de TLS 1.0, 1.1 y 1.2 con los conjuntos de cifrado siguientes:

- 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
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

Para conexiones basadas en UDP, Citrix Receiver respalda DTLS 1.0 con los siguientes conjuntos de cifrado:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Habilitación del modo de conformidad SP 800-52

Se ha introducido una nueva casilla de verificación en la sección Configuración del equipo -> Plantillas administrativas -> Citrix Components -> Network Routing -> TLS and Compliance Mode Configuration, con la etiqueta **Enable FIPS**. Esto permite asegurarse de que solo se use la criptografía aprobada por FIPS para todas las conexiones ICA. De manera

predeterminada, esta opción estará inhabilitada o sin marcar.

Se ha introducido un nuevo modo de conformidad de seguridad llamado SP 800-52. De manera predeterminada, esta opción tiene el valor NONE y no está habilitada. Siga el enlace que describe la conformidad requerida para NIST SP 800-52: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295.

> **Nota**
>
> El modo de conformidad SP800-52 requiere conformidad con FIPS. Cuando SP800-52 está habilitado, el modo FIPS también se habilita, independientemente del parámetro FIPS. Los valores permitidos en la directiva 'Certificate Revocation Check' son 'Full access check and CRL required' o 'Full access check and CRL required All'.

Limitación de versiones de TLS y conjuntos de cifrado

Puede configurar Citrix Receiver para limitar las versiones de TLS y los conjuntos de cifrado. Se proporciona una opción para seleccionar las versiones permitidas del protocolo TLS, que determina el protocolo TLS utilizado para las conexiones ICA. Se seleccionará la versión más alta de TLS que esté mutuamente disponible entre el cliente y el servidor. Entre las opciones se incluyen:

- TLS 1.0 | TLS 1.1 | TLS 1.2 (valor predeterminado).
- TLS 1.1 | TLS 1.2
- TLS 1.2

Hay una opción disponible para la selección del conjunto de cifrado de TLS. Citrix Receiver puede elegir entre:

- Cualquiera
- Comerciales
- Gubernamentales

Conjuntos de cifrado comerciales

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Conjuntos de cifrado gubernamentales

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Nota**
>
> Si la opción **Require TLS for all connections** está habilitada, las solicitudes de conexión con StoreFront también deben ser HTTPS; no se puede agregar un almacén como HTTP, y los VDA que no tienen SSL habilitado (XenDesktop y XenApp) no se pueden iniciar.

Receiver Desktop Lock

Aug 25, 2016

Puede usar Receiver Desktop Lock cuando los usuarios no necesiten interactuar con el escritorio local. Los usuarios pueden seguir usando Desktop Viewer (si está habilitado), pero solo verán el conjunto de opciones que sean estrictamente necesarias en la barra de herramientas: Ctrl+Alt+Supr, Preferencias, Dispositivos y Desconectar.

Citrix Receiver Desktop Lock funciona en máquinas unidas a dominios, que están habilitadas para el inicio de sesión con SSON (Single Sign-on) y configuradas con un almacén; también se puede usar en máquinas que no pertenecen a ningún dominio y no tienen SSON habilitado. No respalda sitios de PNA. Las versiones anteriores de Desktop Lock no reciben respaldo después de actualizar a Receiver para Windows 4.2.x.

Debe instalar Citrix Receiver para Windows con la opción /includeSSON . Debe configurar el almacén y Single Sign-on, ya sea usando el archivo adm/admx o con opciones de línea de comandos. Para obtener más información, consulte Instalación y configuración de Citrix Receiver mediante la línea de comandos.

A continuación, instale Receiver Desktop Lock como administrador usando el archivo CitrixReceiverDesktopLock.MSI disponible en citrix.com/downloads.

Requisitos del sistema para Citrix Receiver Desktop Lock

- Respaldado en Windows 7 (incluido Embedded Edition), Windows 7 Thin PC, Windows 8 y Windows 8.1.
- Los dispositivos de usuario deben estar conectados a una red de área local (LAN) o a una red de área extensa (WAN).

Acceso a aplicaciones locales

> ### Important
>
> Si se habilita el acceso a aplicaciones locales se puede permitir el acceso al escritorio local, a menos que se haya aplicado un bloqueo completo mediante una plantilla de objeto de directiva de grupo o una directiva similar. Consulte Configuración del acceso a aplicaciones locales y la redirección de URL en XenApp y XenDesktop para obtener más información.

Cómo trabajar con Receiver Desktop Lock

- Receiver Desktop Lock puede usarse con las siguientes características de Receiver para Windows:
  - 3Dpro, Flash, USB, HDX Insight, plug-in de Microsoft Lync 2013 y acceso a aplicaciones locales
  - Solo autenticación de dominio, autenticación de dos factores o autenticación con tarjeta inteligente.
- Al desconectar la sesión de Receiver Desktop Lock se cierra la sesión del dispositivo final.
- La redirección de Flash está inhabilitada en Windows 8 y versiones posteriores. La redirección de Flash está habilitada en Windows 7.
- Desktop Viewer está optimizado para Receiver Desktop Lock y no incluye las propiedades Inicio, Restaurar, Maximizar ni Pantalla.
- Ctrl+Alt+Supr está disponible en la barra de herramientas de Desktop Viewer.
- La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota, excepto Windows+L Para ver más información, consulte Paso de las teclas de acceso directo de Windows a la sesión remota.
- Ctrl+F1 activa Ctrl+Alt+Supr cuando se inhabilita la conexión o Desktop Viewer para conexiones de escritorio.

Para instalar Receiver Desktop Lock

Este procedimiento instala Receiver para Windows de forma que los escritorios virtuales se muestren mediante Receiver Desktop

Lock. Para las implementaciones donde se usan tarjetas inteligentes, consulte Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Receiver Desktop Lock.

1. Inicie sesión con una cuenta de administrador local.
2. En el símbolo del sistema, ejecute el siguiente comando (ubicado en los medios de instalación, en la carpeta Citrix Receiver y Plug-ins > Windows > Receiver).
   Por ejemplo:
   CitrixReceiver.exe /includeSSON STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   Para ver detalles del comando, consulte la documentación de instalación de Receiver para Windows en Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.
3. En la misma carpeta de los medios de instalación, haga doble clic en CitrixReceiverDesktopLock.msi. Se abrirá el asistente de Desktop Lock. Siga las indicaciones.
4. Cuando se complete la instalación, reinicie el dispositivo de usuario. Si dispone de permisos para acceder a un escritorio e inicia sesión como un usuario de dominio, el dispositivo se muestra mediante Receiver Desktop Lock.

Para poder administrar el dispositivo de usuario una vez finalizada la instalación, la cuenta que se utilizó para instalar CitrixReceiverDesktopLock.msi se excluye del shell sustituto. Si, más adelante, esa cuenta se elimina, no podrá iniciar sesión ni administrar el dispositivo.

Para ejecutar una **instalación silenciosa** de Receiver Desktop Lock, use la siguiente línea de comandos: msiexec /i CitrixReceiverDesktopLock.msi /qn

Para configurar Receiver Desktop Lock

Otorgue acceso solamente a un escritorio virtual de Receiver Desktop Lock por usuario.

Mediante directivas de Active Directory, impida que los usuarios pongan a hibernar los escritorios virtuales.

Para configurar Receiver Desktop Lock, use la misma cuenta de administrador que utilizó para instalarlo.

- Compruebe que los archivos Receiver.admx (o Receiver.adml) y Receiver_usb.admx (.adml) se han cargado en las Directivas de grupo (las directivas aparecen en: Configuración del equipo o Configuración de usuario > Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Componentes de Citrix). Los archivos .admx están ubicados en %ProgramFiles%\Citrix\ICA Client\Configuration\.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual, por lo que no se requiere ninguna interacción por parte del usuario. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.
  - Habilite la regla de directivas USB.
  - En Citrix Receiver > Remoting client devices > Generic USB Remoting, habilite y configure las directivas Existing USB Devices y New USB Devices.
- Asignación de unidades. En Citrix Receiver > Remoting client devices, habilite y configure la directiva Client drive mapping.
- Micrófono. En Citrix Receiver > Remoting client devices, habilite y configure la directiva Client microphone.

Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Receiver Desktop Lock

1. Configure StoreFront.
   1. Configure XML Service para usar resolución de direcciones DNS para dar respaldo a Kerberos.
   2. Configure los sitios de StoreFront para el acceso mediante HTTPS, cree un certificado de servidor firmado por la entidad de certificación de su dominio y agregue un enlace HTTPS al sitio Web predeterminado.
   3. Compruebe que está habilitada la autenticación PassThrough con tarjeta inteligente (está habilitada de manera predeterminada).
   4. Habilite Kerberos.
   5. Habilite Kerberos y PassThrough con tarjeta inteligente.

6. Habilite el Acceso anónimo en el sitio Web predeterminado de IIS y use la Autenticación de Windows integrada.
7. Asegúrese de que el sitio Web predeterminado de IIS no requiera SSL e ignore los certificados de cliente.

2. Use la Consola de administración de directivas de grupo para configurar las directivas de equipo local en el dispositivo de usuario.
   1. Importe la plantilla Receiver.admx desde %ProgramFiles%\Citrix\ICA Client\Configuration\.
   2. Expanda Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Citrix Components > Citrix Receiver > User authentication.
   3. Habilite Smart card authentication.
   4. Habilite Local user name and password.
3. Configure el dispositivo del usuario antes de instalar Receiver Desktop Lock.
   1. Agregue la dirección URL de Delivery Controller en la lista de Sitios de confianza de Internet Explorer en Windows.
   2. Agregue la URL del primer grupo de entrega a la lista de sitios de confianza de Internet Explorer en el formato escritorio://nombre-de-grupo-de-entrega.
   3. Permita a Internet Explorer que utilice el inicio de sesión automático en caso de sitios de confianza.

Cuando Receiver Desktop Lock está instalado en el dispositivo de usuario, se impone una directiva de extracción de tarjeta inteligente coherente. Por ejemplo, si la directiva de extracción de tarjetas inteligentes de Windows se establece en Forzar cierre de sesión para el escritorio, el usuario debe cerrar la sesión del dispositivo de usuario también, independientemente de cuál sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Esto garantiza que el dispositivo de usuario no quede en un estado inconsistente. Esto se aplica solo a los dispositivos de usuario con Receiver Desktop Lock.

Para quitar Receiver Desktop Lock

Quite los dos componentes de la siguiente lista.

1. Inicie sesión con la misma cuenta de administrador local que se usó para instalar y configurar Receiver Desktop Lock.
2. Con la función de Windows para quitar o cambiar programas:
   - Quite Citrix Receiver Desktop Lock.
   - Quite Citrix Receiver.

Paso de las teclas de acceso directo de Windows a la sesión remota

La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota. Esta sección describe algunas de las más comunes.

Windows

- Win+D: Minimizar todas las ventanas en el escritorio.
- Alt+Tab: Cambiar la ventana activa.
- Ctrl+Alt+Supr: A través de Ctrl+F1 y la barra de herramientas de Desktop Viewer.
- Alt+Mayús+Tab
- Windows+Tab
- Windows+Mayús+Tab
- Windows+Todas las teclas de caracteres

Windows 8

- Win+C: Abrir accesos.
- Win+Q: Acceso Buscar.
- Win+H: Acceso Compartir.
- Win+K: Acceso Dispositivos.
- Win+I: Acceso Configuración.
- Win+Q: Buscar en Aplicaciones.
- Win+W: Buscar en Configuración.
- Win+F: Buscar en Archivos.

Aplicaciones de Windows 8

- Win+Z: Ir a opciones de la aplicación.
- Win+. : Acoplar aplicación a la izquierda.
- Win+Shift+. : Acoplar aplicación a la derecha.
- Ctrl+Tab: Navegar en ciclo por el historial de aplicaciones.
- Alt+F4: Cerrar una aplicación.

Escritorio

- Win+D: Abrir escritorio.
- Win+,: Vistazo de escritorio.
- Win+B: Volver al escritorio.

Otros

- Win+U: Abrir el Centro de accesibilidad.
- Ctrl+Esc: Pantalla Inicio.
- Win+Entrar: Abrir el Narrador de Windows.
- Win+X: Abrir el menú de configuración de herramientas del sistema.
- Win+ImprPant: Toma una captura de pantalla y la guarda en Imágenes.
- Win+Tab: Abre una lista de cambio de ventana.
- Win+T: Vista previa de ventanas abiertas en la barra de tareas.