Acerca de esta versión

-
-
-
  -
  -
  -
  -
  -
-
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos de Citrix Receiver para Windows 4.0

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
  -
  -
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
  -
  -
  -
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
    -
    -
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
    -
    -
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
  -
  -
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas conocidos de Citrix Receiver para Windows 4

-
-
-
-

Problemas de instalación y actualización

-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

Problemas generales

-
-
-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-

Conexiones de escritorio

-
-
-
-

Problemas con Microsoft Lync 2013 VDI Plug-in

-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisitos del sistema

Sistema operativo

-
-
-
-

-
-

-
-
-
-
-

Hardware

-
-
-

-
  -
  -
  -
  -
  -
-
  -
  -
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
  -
  -
  -
  -
  -
  -
  -

Acerca de las conexiones seguras y los certificados SSL

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

-
-
-
-
-

-
-
-
-

-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
  -
  -
  -
-
-
  -
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de Receiver para Windows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación y desinstalación manual de Receiver para Windows

-
  -
  -
-
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

el elemento

-

-

-

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"

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Distribución de Receiver con Active Directory y scripts de inicio de ejemplo

-
-

-
```
set DesiredVersion= 3.3.0.XXXX
```
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Uso de los scripts de inicio de ejemplo por usuario

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Distribución de Receiver desde Receiver para Web

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de Receiver para Windows

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de la entrega de aplicaciones

-
-
  -
  -
  -
    -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-

-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración del respaldo USB para conexiones de XenDesktop

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
  -
  -
  -
  -
  -
  -
  -
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Impedir que la ventana de Desktop Viewer se atenúe

-
-

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar parámetros para varios usuarios y dispositivos

-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de StoreFront y AppController

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cómo proporcionar información de cuentas a los usuarios

-
-
-

-

-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
  -
  -

    NetScalerGatewayFQDN?MyStoreName

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Optimización del entorno de Receiver

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Reducción del tiempo de inicio de las aplicaciones

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Asignación de dispositivos del cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Respaldo para resolución de nombres DNS

Nov 20, 2015

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 activar 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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utilización de servidores proxy con conexiones de XenDesktop

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mejora de la experiencia del usuario

Nov 20, 2015

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

- Entrada de micrófono en el cliente
- Respaldo para varios monitores
- Anulación de parámetros de impresora en los dispositivos
- Teclas de acceso rápido
- Respaldo de Receiver para iconos de color de 32 bits
- Entrega de escritorios virtuales para usuarios de Receiver
- Entrada de teclado en sesiones de Desktop Viewer
- Conexión con escritorios virtuales

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entrada de micrófono en el cliente

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Respaldo para varios monitores

Nov 20, 2015

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 un 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 sobre el cálculo de los requisitos de memoria gráfica de XenApp y XenDesktop, consulte ctx115637.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Anulación de parámetros de impresora en los dispositivos

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Teclas de acceso rápido

Nov 20, 2015

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 deseadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Respaldo de Receiver para iconos de color de 32 bits

Nov 20, 2015

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 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. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entrega de escritorios virtuales para usuarios de Receiver

Nov 20, 2015

Las compañías presentan distintas necesidades empresariales, y las expectativas y requisitos relacionados con la forma en la que los usuarios acceden a los escritorios virtuales puede variar a medida que crecen y evolucionan sus necesidades. 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. Existen dos opciones para que los usuarios accedan a los escritorios virtuales: Desktop Viewer o Citrix Desktop Lock.

Utilice esta versión cuando los usuarios necesiten interactuar con el escritorio local y con el escritorio virtual. 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.
Para obtener más información sobre Desktop Lock, que está respaldado solo para CitrixReceiverEnterprise.exe, consulte la documentación de XenDesktop 7 en eDocs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entrada de teclado en sesiones de Desktop Viewer

Nov 20, 2015

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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión con escritorios virtuales

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Protección de las conexiones

Nov 20, 2015

Para maximizar la seguridad del entorno, las conexiones entre Receiver y los recursos que se publiquen deben ser seguras. Puede configurar diversos tipos de autenticación para el software de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de la autenticación con tarjeta inteligente

Nov 20, 2015

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). La autenticación bimodal requiere una configuración de StoreFront y NetScaler Gateway.
- **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 con la opción de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Receiver para Windows no guarda el PIN del usuario ni la selección de certificado.
- 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.
- La autenticación directa con tarjeta inteligente en App Controller no está respaldada. No obstante, puede implementar App Controller detrás de StoreFront para usar el servicio de autenticación de certificados de StoreFront. Las aplicaciones Web que usan autenticación con certificado de cliente requieren solicitudes de tarjeta inteligente aparte para el explorador, para crear su propia conexión SSL.
- 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.

Precaución: 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 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
- Defina SSONCheckEnabled como 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\

Para configurar StoreFront:

- En el archivo default.ica ubicado en el servidor StoreFront, defina Set DisableCtrlAltDel con el valor false.
- Cuando configure el servicio de autenticación en el servidor StoreFront, marque la casilla PassThrough de dominio y deje sin marcar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 SSL.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilitación de la comprobación de listas de revocación de certificados para mejorar la seguridad con Receiver

Nov 20, 2015

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 Receiver a realizar esta verificación, se puede mejorar la autenticación por cifrado del servidor, así como la seguridad general de las conexiones SSL/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 Receiver para que verifique sólo la lista local de certificados, o bien 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 Receiver, incluso 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 del 2 al 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 enSólo verifique CRL almacenados localmente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilitación de la autenticación PassThrough cuando los sitios no se encuentran en sitios de confianza o zonas de Intranet

Nov 20, 2015

Es posible que los usuarios requieran autenticación PassThrough (de paso de credenciales) al servidor con sus credenciales de inicio de sesión de usuario, pero no podrán agregar sitios a las zonas Sitios de confianza o Intranet. Habilite este parámetro para permitir la autenticación PassThrough en todos los sitios excepto los restringidos.

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 del 2 al 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 Authentication > Local user name and password.
7. En el menú de Propiedades de Local user name and password, seleccione Habilitada y después seleccione las casillas Enable pass-through authentication y Allow pass-through authentication for all ICA connections.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de autenticación PassThrough de dominio con Kerberos

Nov 20, 2015

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

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 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.

Receiver gestiona la autenticación PassThrough con Kerberos del siguiente modo, cuando 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 Receiver captura el PIN de la tarjeta inteligente.
2. Receiver usa IWA (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 authentication, 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 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.

Precaución: 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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:

  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, defina Set DisableCtrlAltDel por false.
- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Protección de las comunicaciones de Receiver

Nov 20, 2015

Para proteger la comunicación entre la los sitios de XenDesktop o las comunidades de servidores XenApp y Receiver, se pueden integrar las conexiones de Receiver a través de tecnologías de seguridad como las siguientes:

- Citrix NetScaler Gateway o Access Gateway. Para obtener más información, consulte los temas de esta sección además de la documentación de NetScaler Gateway, Access Gateway y StoreFront.
  Nota: Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores de 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, servidor proxy HTTPS o servidor proxy de canalización SSL). 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.
- Solamente para implementaciones de XenApp o la Interfaz Web; no se aplica a XenDesktop 7: soluciones de Traspaso SSL con los protocolos de capa de sockets seguros (SSL) y seguridad de la capa de transporte (TLS).

Receiver es compatible con entornos en los que se utilizan las plantillas de seguridad de escritorio de Microsoft Specialized Security - Limited Functionality (SSLF). Estas plantillas se respaldan en las plataformas Microsoft Windows XP, Windows Vista y Windows 7. Consulte las guías de seguridad de Windows XP, Windows Vista y Windows 7 disponibles en http://technet.microsoft.com para obtener más información sobre las plantillas y su configuración.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión con NetScaler Gateway

Nov 20, 2015

Para permitir que los usuarios remotos se conecten mediante NetScaler Gateway, configure NetScaler Gateway para que funcione con StoreFront y App Controller (un componente de XenMobile App Edition).

- 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.
- Para implementaciones de AppController: puede permitir conexiones de usuarios remotos con App Controller integrando NetScaler Gateway y App Controller. Con esta implementación, los usuarios pueden conectarse a App Controller 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 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 eDocs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión con Access Gateway Enterprise Edition

Nov 20, 2015

Para permitir que los usuarios remotos se conecten mediante Access Gateway, configure Access Gateway 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 Access Gateway Plug-in.

Para obtener información sobre la configuración de estas conexiones, consulte Integrating Access Gateway with CloudGateway 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 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 el tema sobre la configuración de Access Gateway para la comunicación con la Interfaz Web Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface y los subtemas correspondientes en eDocs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión con Secure Gateway

Nov 20, 2015

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:

- Host name
- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión a través de un firewall

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cumplimiento de relaciones de confianza

Nov 20, 2015

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, SSL) 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).

Si se conecta a través de SSL, agregue el nombre de servidor con el formato: https://CN, donde CN es el nombre común que muestra el certificado SSL. De otra forma, utilice el formato que Receiver usa para conectarse; por ejemplo si Receiver utiliza una dirección IP, agregue la dirección IP del servidor.

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 del 2 al 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, expanda 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nivel de elevación y wfcrun32.exe

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión de Receiver a través de un servidor proxy

Nov 20, 2015

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexión con el Traspaso SSL (Secure Sockets Layer Relay)

Nov 20, 2015

Esta sección no se aplica a XenDesktop 7.

Puede integrar Receiver con los servicios de Traspaso SSL (Secure Sockets Layer Relay). Receiver admite ambos protocolos SSL y TLS.

- SSL proporciona cifrado avanzado para brindar mayor privacidad a las conexiones ICA y a la autenticación del servidor a través de certificados para garantizar que el servidor al que se conecta es un servidor válido.
- 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. Dado que solo existen pequeñas diferencias entre la versión 3.0 de SSL y la versión 1.0 de TLS, los certificados que utilice para SSL en su instalación también funcionarán con TLS. 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.

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor XenApp para las comunicaciones con seguridad SSL/TLS. Cuando el Traspaso SSL recibe una conexión SSL/TLS, descifra los datos antes de redirigirlos al servidor o al servicio Citrix XML Service (si el usuario ha seleccionado la exploración SSL/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 SSL/TLS habilitada y un servidor. Las conexiones que utilizan el cifrado SSL/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 información sobre cómo configurar el Traspaso SSL para proteger una instalación, consulte Configuración de SSL/TLS entre servidores y clientes en la documentación de XenApp.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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 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 del 2 al 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, a continuación, escriba una lista de servidores de confianza separada con comas y el número de puerto nuevo en el cuadro de texto Allowed SSL servers con el siguiente formato:
   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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

que se traduce a lo siguiente en el archivo appsrv.ini:
[Word]

SSLProxyHost=csghq.Test.com:443

[Excel]

SSLProxyHost=csghq.Test.com:444

[Notepad]

SSLProxyHost=fred.Test.com:443

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración y activación de Receiver para SSL y TLS

Nov 20, 2015

Este tema no se aplica a XenDesktop 7.

SSL y TLS se configuran de igual forma, porque utilizan los mismos certificados y se habilitan de forma simultánea.

Cuando SSL y TLS están habilitados, cada vez que se establece una conexión, Receiver primero intenta utilizar TLS y después SSL. Si no puede conectarse con SSL, la conexión falla y aparece un mensaje de error.

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 SSL/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.

Para usar SSL/TLS para proteger la seguridad de las comunicaciones entre Receiver con seguridad SSL/TLS y la comunidad de servidores, es necesario un certificado raíz en el dispositivo de usuario para que pueda verificar la firma de la entidad emisora de certificados 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 SSL/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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
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 SSL/TLS a TLS o para habilitar TLS elija Detect all. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS. Si la conexión que utiliza TLS falla, Receiver intenta conectarse usando SSL.
   - 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 del 3 al 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 SSL/TLS Version con el valor TLS o Detect all para habilitar TLS. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS. Si la conexión que utiliza TLS falla, Receiver intenta conectar usando SSL.
   - Configure SSL ciphersuite con Government.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 SSL/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 SSL/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 desea proteger.
2. Seleccione Avanzado > Opciones del cliente y asegúrese de seleccionar 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 SSL/TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

Es posible configurar Receiver para que use SSL/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.

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 SSL/TLS.
4. Haga clic en Actualizar para aplicar los cambios.
5. Habilite SSL/TLS en el explorador Web del dispositivo del usuario. Para obtener más información, consulte la Ayuda en línea del explorador.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de certificados raíz en los dispositivos de usuario

Nov 20, 2015

Para usar SSL/TLS para proteger la seguridad de las comunicaciones entre Receiver con seguridad SSL/TLS y la comunidad de servidores, es necesario un certificado raíz en el dispositivo de usuario para que pueda verificar la firma de la entidad emisora de certificados 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar la Interfaz Web para usar SSL/TLS con Receiver

Nov 20, 2015

1. Para usar SSL/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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar el respaldo para TLS

Nov 20, 2015

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 del 2 al 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 SSL/TLS a TLS o, para habilitar TLS, elija Detect all. Si selecciona Detect all, Receiver intenta conectar mediante el cifrado TLS. Si la conexión que utiliza TLS falla, Receiver intenta conectarse usando SSL.
   - 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para usar la plantilla de directivas de grupo en la Interfaz Web para cumplir con los requisitos de seguridad de FIPS 140

Nov 20, 2015

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 del 3 al 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 SSL/TLS Version con el valor TLS o Detect all para habilitar TLS. Si selecciona Detect all, Receiver intenta conectar usando el cifrado TLS. Si la conexión que utiliza TLS falla, Receiver intenta conectar usando SSL.
   - Establezca SSL ciphersuite en Government.
   - Establezca CRL verification en Require CRLs for connection.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar la Interfaz Web con SSL/TLS para las comunicaciones con Citrix Receiver

Nov 20, 2015

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 SSL/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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar Citrix XenApp con SSL/TLS para la comunicación con Citrix Receiver

Nov 20, 2015

Es posible configurar el servidor XenApp para que utilice SSL/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 desea proteger.
2. Seleccione Avanzado > Opciones del cliente y asegúrese de seleccionar 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 SSL/TLS para proteger la seguridad de las comunicaciones entre Receiver y el servidor Web.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar Citrix Receiver con SSL/TLS para las comunicaciones con el servidor que ejecuta la Interfaz Interfaz Web

Nov 20, 2015

Es posible configurar Receiver para que use SSL/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 información, consulte Instalación de certificados raíz en los 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 SSL/TLS.
4. Haga clic en Actualizar para aplicar los cambios.
5. Habilite SSL/TLS en el explorador Web del dispositivo del usuario. Para obtener más información, consulte la Ayuda en línea del explorador.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Protección ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza con ICA File Signing

Nov 20, 2015

Este tema solo es aplicable a entornos con Interfaz Web y plantillas administrativas antiguas.

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 Administrator 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 del 2 al 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. En 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de un explorador Web y un archivo ICA para habilitar Single Sign-on y administrar conexiones seguras a servidores de confianza

Nov 20, 2015

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de los permisos de los recursos del cliente

Nov 20, 2015

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 en Receiver, el procedimiento .ini disponible en las versiones anteriores del plug-in/Receiver se ha reemplazado por estos procedimientos.
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. 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
PdaSecurityPermission	Dispositivos PDA
ScannerAndDigitalCameraSecurityPermission	USB y otros dispositivos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Clave de recurso	Recurso

Valor	Descripción
0	Sin acceso
1	Acceso de solo lectura
2	Acceso completo
3	Solicitar acceso al usuario

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos de Receiver para Windows 4.x

Jan 20, 2017

Comparado con: Citrix Receiver para Windows 4.1.100

Receiver para Windows 4.1.200 contiene todas las correcciones incluidas en Receiver para Windows 4.0, 4.0.1, 4.1, 4.1.2 y 4.1.100, además de las siguientes correcciones nuevas:

Redirección de Flash HDX MediaStream

- Al explorar ciertos sitios Web con la redirección de Flash de HDX MediaStream habilitada, es posible que Internet Explorer deje de responder.

  Para habilitar esta corrección, también debe instalar la corrección #LA4151 de VDA/HDX MediaStream para Flash y definir la siguiente clave de Registro en el servidor XenApp/VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: SupportedUrlHeads
  Type: REG_MULTI_SZ
  Data: <*cada valor va en una línea independiente, y los valores null van separados*>
  http://
  https://
  file://

  [En RcvrForWin4.1_14.1.200] [#LA5255]

- Inhabilitar el retorno inteligente de Flash en una sesión puede provocar que Internet Explorer deje de responder.

  [En RcvrForWin4.1_14.1.200] [#LA5404]

Impresión

- El controlador de impresora de Citrix (UPD) no imprime fuentes de código de barras. La fuente aparece en blanco o con caracteres aleatorios al imprimir documentos con el controlador de impresora de Citrix (cpviewer.exe) o con una impresora de código de barras.

  [En RcvrForWin4.1_14.1.200] [#LC0141]

Administración de servidores/comunidades de servidores

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si las directivas "Límite de ancho de banda de redirección de archivos" y "Límite de ancho de banda global de la sesión" están establecidas, es posible que la sesión se cierre de forma inesperada.

  Para solucionar este problema, debe instalar una actualización de servidor y de Receiver que contenga la corrección #LA5925 y, a continuación, definir la siguiente clave de Registro en el servidor:

  - Cree la siguiente clave de Registro:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    Name: DisableHighThroughput
    Type: DWORD
    Value: 1
  - Cambie la siguiente clave de Registro:
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    Name: MaxNetCommands
    Type: DWORD
    Value: un valor menor

  [En RcvrForWin4.1_14.1.200] [#LA5925]

Sesión/conexión

- Si la conexión de red con un VDA se desconecta y, a continuación, se vuelve a conectar, los clics con el puntero no funcionan.

  [En RcvrForWin4.1_14.1.200] [#LA5743]

- La redirección de puertos COM puede fallar y generar el siguiente mensaje de error:

  "Error en OpenPort: Comport 'COM4'".

  [En RcvrForWin4.1_14.1.200] [#LC0434]

- Cuando un dispositivo de punto final conectado a un VDA se reanuda desde el estado de suspensión, el puntero y el teclado ya no funcionan en la sesión de VDA.

  [En RcvrForWin4.1_14.1.200] [#LC0085]

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

  [En RcvrForWin4.1_14.1.200] [#LA5489]

Excepciones del sistema

- La reproducción de vídeos en un reproductor multimedia dentro de una sesión PassThrough puede provocar que la sesión se cierre de forma inesperada.

  [En RcvrForWin4.1_14.1.200] [#LC0553]

Experiencia de utilización

- Las aplicaciones integradas a pantalla completa se mueven con problemas, pueden no quedarse quietas y, al moverse, muestran el fondo de escritorio en los bordes.

  [En RcvrForWin4.1_14.1.200] [#LC0696]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- En redes inalámbricas, la ventana de la sesión puede ponerse temporalmente de un color gris sólido.

  [En RcvrForWin4.1_14.1.200] [#LC0530]

- En sesiones de usuario controladas por una directiva que establece la calidad de sonido en **Sonido de alta calidad; menor rendimiento** (**Configuración avanzada** > **Propiedades** > **Dispositivos cliente** > **Recursos** > **Audio** > **Calidad de sonido** > **Sonido de alta calidad; menor rendimiento**), no se oye ningún sonido.

  [En RcvrForWin4.1_14.1.200] [#LC0329]

- Cuando se reproducen en bucle archivos multimedia en sesiones de escritorio de RDS, las secuencias de audio y vídeo se detienen después de que el archivo lleve una hora o más reproduciéndose en bucle.

  [En RcvrForWin4.1_14.1.200] [#LC0641]

- El preinicio de sesiones solamente funciona la primera vez que se inicia Receiver para Windows, no cuando se ha configurado.

  [En RcvrForWin4.1_14.1.200] [#LC0701]

Comparado con: Citrix Receiver para Windows 4.1

Receiver para Windows 4.1.100 contiene todas las correcciones incluidas en Receiver para Windows 4.0, 4.0.1, 4.1 y 4.1.2, además de las siguientes correcciones nuevas:

HDX 3D Pro	Administración de servidores/comunidades de servidores
HDX MediaStream	Sesión/conexión
HDX Plug-n-Play	Excepciones del sistema
HDX RealTime	Experiencia de utilización
Instalación, desinstalación y actualización	Interfaz de usuario
Impresión	Varios

HDX 3D Pro

- Después de varias horas de uso, el proceso de wfica32.exe puede consumir el 100 % de la CPU al usar HDX 3D Pro con el códec H.264 y el seguimiento de texto inhabilitado.

  [En RcvrForWin4.1_14.1.100] [#LA5554]

HDX MediaStream

- Al intentar ver vídeos por streaming a través de un explorador Web como, por ejemplo, Internet Explorer, es posible que

© 1999-2017 Citrix Systems, Inc. All rights reserved.

no se pueda debido a un error en la redirección de Flash de HDX MediaStream.

Para habilitar la corrección, establezca las siguientes claves de Registro:

- *En Windows de 32 bits*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  Name: FallbackIfFlashNotExist
  Type: REG_DWORD
  Data: 0
- *En Windows de 64 bits*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  Name: FallbackIfFlashNotExist
  Type: REG_DWORD
  Data: 0

[En RcvrForWin4.1_14.1.100] [#LA5278]

- Con la versión 1.0 de HDX MediaStream para Flash (redirección de Flash de primera generación) habilitada, es posible que Microsoft Internet Explorer se cierre de forma inesperada si se ha instalado Adobe Flash Player 11.8 o una versión posterior.

  [En RcvrForWin4.1_14.1.100] [#LA5421]

HDX Plug-n-Play

- Después de instalar Receiver para Windows 4.0 en Windows XP SP3, los puertos USB de la base de acoplamiento ya no se pueden redirigir.

  [En RcvrForWin4.1_14.1.100] [#LA4582]

HDX RealTime

- Es posible que el redireccionamiento de la compresión de vídeo de cámara Web de HDX RealTime no admita la resolución de pantalla (320 x 240) de QVGA y puede provocar que el proceso de wfica32.exe se cierre de forma inesperada.

  [En RcvrForWin4.1_14.1.100] [#LA5232]

Instalación, desinstalación y actualización

- Al actualizar a una versión más reciente de Receiver para Windows sin tener conexión a Internet, la versión anterior no se desinstala del todo y no se realiza la instalación de la versión más reciente.

  [En RcvrForWin4.1_14.1.100] [#LA4896]

Impresión

- Esta corrección soluciona un problema en que la impresión a dos caras falla cuando se ha configurado el controlador de impresora universal y dicha impresión debe realizarse de forma manual.

  [En RcvrForWin4.1_14.1.100] [#261552]

- Para cierto tipo de fuentes, la impresión de documentos HTML con Internet Explorer 9 puede salir distorsionada en Citrix Print Viewer (cpviewer.exe) y en las copias impresas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[En RcvrForWin4.1_14.1.100] [#LA3962]

Administración de servidores/comunidades de servidores

- Si StoreFront está configurado con un almacén no autenticado, la detección de cuentas puede fallar al usar Receiver para Windows.

  [En RcvrForWin4.1_14.1.100] [#LC0004]

- Esta mejora respalda la creación automática de accesos directos para las aplicaciones preferidas mediante un directorio de plantillas de preferencia. Para estas aplicaciones, además de las reglas de preferencia existentes, el Self-service Plug-in busca los accesos directos en el directorio de plantillas de preferencia. Si coincide con las reglas de preferencia, copia el acceso directo al menú Inicio del usuario.

  De forma predeterminada, este directorio es uno de los siguientes:

  - "%systemdrive%:\Archivos de programa\Citrix\shortcuts"
  - "%systemdrive%:\Archivos de programa (x86)\Citrix\shortcuts" para la instalación por dispositivo de usuario
  - "%systemdrive%:\Usuarios\\AppData\Local\Citrix\SelfService\shortcuts" para la instalación por usuario

  La ubicación predeterminada del directorio de plantillas de preferencia se puede especificar en el Registro.

  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle o HKEY_CURRENT_USER\Software\Citrix\Dazzle
  Name: PreferTemplateDirectory
  Type: REG_SZ
  Data: cualquier ruta (por ejemplo, "%systemroot%:\Shortcuts")

  Si se cancela la suscripción de la aplicación o esta se quita del almacén, el acceso directo copiado del directorio de preferencia se elimina.

  [En RcvrForWin4.1_14.1.100] [#LC0005]

Sesión/conexión

- Al usar Citrix Receiver dentro de una sesión de escritorio virtual, no se puede iniciar aplicaciones publicadas de XenApp y aparece el siguiente mensaje de error:

  "Esta versión de Citrix Receiver no respalda el cifrado seleccionado. Póngase en contacto con el administrador. [Error 1029: Carga de DLL no válida]".

  [En RcvrForWin4.1_14.1.100] [#LA4743]

- Con la actualización acumulativa 2 de Receiver para Windows 13.4, cuando el enfoque se halla en una aplicación integrada, el idioma de entrada de la barra de idioma cambia al presionar Alt + Tab para cambiar las ventanas activas.

  [En RcvrForWin4.1_14.1.100] [#LA4963]

- Con la opción "Agrupar los botones similares de la barra de tareas" seleccionada en "Propiedades de la barra de tareas y del menú Inicio" de un sistema con Windows XP, el inicio de aplicaciones puede ser lento.

  [En RcvrForWin4.1_14.1.100] [#LA4191]

- Después de actualizarse de la versión 12.2 de Citrix Online Plug-in a la versión 3.x de Citrix Receiver para Windows, es posible que las conexiones proxy con sitios Web externos no se inicien con la autenticación de proxy NTLM habilitada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[En RcvrForWin4.1_14.1.100] [#LA3781]

- Si el dispositivo de usuario no tiene conectada una cámara Web, es posible que, al iniciar una instancia publicada de Microsoft Lync 2010, la aplicación se conecte y se desconecte varias veces antes de establecer una conexión final e iniciarse. Esto puede ocurrir si instala una aplicación que instale una cámara Web cuando no hay más cámaras Web instaladas, como, por ejemplo, el paquete de Motorola Bluetooth.

  [En RcvrForWin4.1_14.1.100] [#LA4867]

- Al iniciar una aplicación o un escritorio publicados, es posible que la autenticación Kerberos no funcione cuando se usa la autenticación PassThrough en una red IPv4. Esta versión corrige únicamente el problema para las redes IPv4.

  [En RcvrForWin4.1_14.1.100] [#LA5026]

- Esta corrección va dirigida a los problemas de audio/vídeo relacionados con el complemento Infraestructura de escritorio virtual (VDI) de Microsoft Lync 2013 para Windows. Mejora la experiencia de usuario para los usuarios de Lync. Para obtener más información, consulte el artículo de Knowledge Center CTX138408.

  [En RcvrForWin4.1_14.1.100] [#LA5314]

- Si el adaptador de red USB CANcaseXL se redirige a un escritorio virtual, parece no funcionar correctamente en el Administrador de dispositivos de Windows. Este dispositivo USB no admite el controlador de redirección USB de Citrix. El VDA necesita la instalación de la corrección #LA5022 para funcionar correctamente.

  [En RcvrForWin4.1_14.1.100] [#LA5022]

- Esta corrección vuelve a procesar la corrección #LA1257, la cual no consigue solucionar completamente el siguiente problema:

  Con Desktop Viewer inhabilitado, una sesión de cliente a pantalla completa no ajusta la resolución de pantalla de Virtual Desktop Agent en respuesta a un cambio de resolución de la pantalla del dispositivo de punto final.

  [En RcvrForWin4.1_14.1.100] [#LA4000]

- Cuando se pierde la conectividad con una sesión de XenDesktop durante más tiempo que el tiempo de espera de la fiabilidad de la sesión, Desktop Viewer permanece en pantalla de forma indefinida. Como es de esperar, la propia sesión desaparece de la Central de conexiones después de que se agote el tiempo de espera de la fiabilidad de la sesión.

  [En RcvrForWin4.1_14.1.100] [#LA4856]

Excepciones del sistema

- El proceso de wfica32.exe puede cerrarse de forma inesperada, tras lo que aparece el siguiente mensaje de error:

  "Citrix HDX Engine detectó un problema y debe cerrarse".

  [En RcvrForWin4.1_14.1.100] [#LA3964]

- El proceso de wfica32.exe puede cerrarse de forma inesperada, tras lo que aparece el siguiente mensaje de error:

  "Citrix HDX Engine detectó un problema y debe cerrarse".

  [En RcvrForWin4.1_14.1.100] [#LA4695]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Es posible que el proceso de wfica32.exe se cierre de forma inesperada al iniciar una sesión PassThrough del escritorio de XenApp 6.5 a la aplicación publicada de XenApp 4.5.

  [En RcvrForWin4.1_14.1.100] [#LA5193]

- Si la directiva de multisecuencia está habilitada, las aplicaciones pueden dejar de responder al acceder al puerto COM.

  [En RcvrForWin4.1_14.1.100] [#LA5543]

- En los casos de doble salto, iniciar Microsoft Outlook o Communicator puede provocar que Receiver para Windows se cierre de forma inesperada.

  [En RcvrForWin4.1_14.1.100] [#LA4813]

Experiencia de utilización

- Al conectarse o volver a conectarse a una sesión hospedada en XenApp para Unix, no se producen ninguna actualización de pantalla durante 90 segundos.

  [En RcvrForWin4.1_14.1.100] [#LA5244]

Interfaz de usuario

- Un cambio introducido en la versión 12.1 del Online Plug-in provocaba una demora en la aparición de la barra de progreso de conexión de las conexiones integradas. Sin embargo, para las sesiones que se conectan a servidores más lentos, este comportamiento no siempre es conveniente. Esta mejora incluye respaldo para la siguiente clave de Registro, que permite configurar la duración de la demora:

  En Windows de 32 bits:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <*retraso en milisegundos*>

  En Windows de 64 bits:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  Name: NotificationDelay
  Type: REG_DWORD
  Data: <*retraso en milisegundos*>

  [En RcvrForWin4.1_14.1.100] [#LA0678]

- Después de cambiar la combinación de colores del escritorio del color azul predeterminado a otro color, como el verde oliva o el plateado (**Escritorio** > **Propiedades** > **ficha Apariencia** > **Combinación de colores**), el texto y el color de fondo del Self-service Plug-in se vuelven idénticos, con lo que no se pueden leer los elementos del menú.

  [En RcvrForWin4.1_14.1.100] [#LA5121]

Varios

- Al usar la detección por correo electrónico, si el registro SRV creado en el sistema DNS incluye un puerto que no sea el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

443, Receiver ignora el puerto especificado en el registro SRV y procede a conectarse a la URL de Access/NetScaler Gateway a través del puerto 443.

[En RcvrForWin4.1_14.1.100] [#LA4491]

Comparado con: Citrix Receiver para Windows 4.1

Receiver para Windows 4.1.2 contiene todas las correcciones incluidas en Receiver para Windows 4.0, 4.0.1 y 4.1, además de las siguientes correcciones nuevas:

Microsoft Lync 2013 VDI Plug-in | Instalación, desinstalación y actualización

Microsoft Lync 2013 VDI Plug-in

- Cuando se mueve la ventana de conversación de Lync a un segundo monitor, no se muestra el vídeo.

  [#LA5314, #399447]

- Cuando se mueve una ventana de presentación de pizarra a otro usuario, el vídeo del otro usuario no aparece en la ventana de conversación.

  [#LA5314, #399465]

- Receiver puede cerrarse de forma inesperada en llamadas de vídeo con varios usuarios o al terminar las conferencias de vídeo.

  [#LA5314, #426035]

- En algunos dispositivos cliente, el vídeo de las videollamadas no está disponible de forma intermitente en el modo de pantalla completa de VDA.

  [#LA5314, #418675]

- Si la ventana de una conferencia de vídeo se mueve, es posible que el vídeo se distorsione.

  [#LA5314, #419898]

Instalación, desinstalación y actualización

- Al actualizar a una versión más reciente de Receiver para Windows sin tener conexión a Internet, la versión anterior no se desinstala del todo y no se realiza la instalación de la versión más reciente.

  [#LA4896]

Comparado con: Citrix Receiver para Windows 4.0.1

Receiver para Windows 4.1 contiene todas las correcciones incluidas en Receiver para Windows 4.0 y 4.0.1, además de las siguientes correcciones nuevas:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de Flash de HDX MediaStream

- Al reproducir varios archivos multimedia de forma rápida y sucesiva en http://www.youtube.com/ con la redirección de Flash de HDX MediaStream habilitada, es posible que el proceso de PseudoContainer2.exe se cierre de forma inesperada.

  [#LA3846

Redirección de Windows Media de HDX MediaStream

- En la versión 3.4 de Receiver para Windows con la redirección de HDX MediaStream para Windows Media habilitada, se puede dar un retraso de hasta diez segundos antes de que los archivos multimedia comiencen a reproducirse.

  [#LA4141]

HDX Plug-n-Play

- Al hacer clic en Dispositivos, en Desktop Viewer, para seleccionar un dispositivo USB con el fin de controlarlo de forma remota mediante la redirección de dispositivos USB de HDX Plug-n-Play, puede provocar que la ventana de Desktop Viewer deje de responder.

  [#LA3348]

Instalación, desinstalación y actualización

- Cuando los usuarios no administrativos intentan actualizar la versión de Receiver para Windows, es posible que, si es un administrador el que instaló Receiver, la instalación solo es parcial.

  Con esta corrección, los usuarios no administrativos que intenten actualizar dispositivos Receiver instalados por un administrador reciben un mensaje de error y el proceso de instalación finaliza.

  [#LA3425]

Teclado

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Al usar la versión 3.3 de Receiver para Windows, presionar la tecla Alt puede provocar que la tecla permanezca inactiva. Como consecuencia, presionar la tecla "E" puede invocar el Explorador de Windows.

  [#LA3288]

- Al hacer clic en la barra de herramientas de Desktop Viewer con la tecla de Windows presionada en modo de pantalla completa, es posible que la tecla permanezca inactiva. Como consecuencia, presionar la tecla "E" invoca el Explorador de Windows.

  [#LA3349]

- Esta corrección soluciona un problema que puede provocar que, en las sesiones ICA, el estado de las teclas Bloq Mayús, Bloq Num o Bloq Despl no esté sincronizado. Esta corrección presenta un nuevo parámetro que permite forzar la sincronización del estado de los LED del teclado entre el cliente y el servidor. Para habilitar esta opción, agregue la entrada "KeyboardForceLEDUpdate = On" a la sección [WFClient] del archivo appsrv.ini en la ubicación del perfil de usuario local o del archivo default.ica en el sitio correspondiente de la Interfaz Web.

  [#LA3682]

- Esta corrección soluciona un problema de sincronización de los LED que puede provocar que el estado de las teclas Bloq Mayús, Bloq Num o Bloq Despl no esté sincronizado entre el cliente y el servidor.

  [#LA4293]

Acceso a aplicaciones locales

- Con el acceso a aplicaciones locales habilitado, hacer clic en Desktop Viewer provoca que la barra de tareas local del cliente aparezca sin necesidad.

  [#LA3049]

Inicio de sesión/autenticación

- Es posible que la autenticación PassThrough no funcione después de instalar VDA de XenDesktop 7 en Windows Server 2008 R2. El problema se produce porque el proceso de ssonsvr.exe no se puede iniciar.

  [#LA4685]

Impresión

- Al enviar varios trabajos de impresión desde Adobe Acrobat a una impresora de sesión, se pueden perder páginas aleatorias o trabajos de impresión enteros.

  [#LA3643]

- La enumeración de la impresora de sesión puede tardar una cantidad excesiva de tiempo.

  [#LA3951]

Sesión/conexión

- Cuando un dispositivo cliente se encuentra en estado de suspensión o hibernación durante un período de tiempo prolongado con una sesión activa de XenDesktop, al reanudarlo, es posible que la sesión no se vuelva a conectar según lo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

esperado y se quede atascada en una fase de reconexión que requiere que la ventana de la sesión se cierre manualmente.

Esta corrección soluciona el problema de modo que, al reanudar el dispositivo cliente, la ventana de la sesión se cierre correctamente cuando la reconexión falla.

[#LA2748]

- Al iniciar una aplicación publicada en modo integrado, la ventana de la barra de progreso permanece en el fondo.

  Para habilitar la corrección, establezca las siguientes claves de Registro en el lado del cliente:

  - *Para sistemas con Windows de 32 bits:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    Name: ForegroundProgressBar
    Type: DWORD
    Data: 1
  - *Para sistemas con Windows de 64 bits:*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    Name: ForegroundProgressBar
    Type: DWORD
    Data: 1

  [#LA3491]

- Receiver con Desktop Lock muestra una pantalla gris cada vez que se produce un error de hardware o si la VM se cierra de manera forzada desde el hipervisor.

  [#LA3499]

- Con la agrupación de barras de tareas habilitada en el dispositivo cliente, TaskbarGrpXpVista.dll (dentro de wfica32.exe) envía consultas de forma innecesaria al dispositivo cliente para obtener información sobre las aplicaciones publicadas que se ejecutan en la sesión. Por ejemplo, al ejecutar una instancia publicada de cmd.exe, TaskbarGrpXpVista.dll envía una consulta a C:\Windows\System32\cmd.exe para obtener información sobre el archivo ejecutable. En los casos en que la aplicación publicada se ejecuta desde el recurso compartido remoto, puede haber un consumo de ancho de banda no deseado.

  [#LA3661]

- Con un parámetro de objeto de directiva de grupo (GPO) para evitar la agrupación de barras de tareas, hacer clic en los iconos de las barras de tareas en dispositivos cliente con Windows XP o Vista no cambia el enfoque de las ventanas asociadas.

  [#LA3889]

- Receiver puede dejar de responder al hacer clic en el botón Dispositivos de la barra de herramientas de Desktop Viewer, mientras aparece el cuadro de diálogo "Citrix Receiver: Acceso de dispositivo". Este cuadro de diálogo aparece si la preferencia de acceso de dispositivo se ha establecido en "Preguntar siempre" en lugar de la opción predeterminada "No hacer nada".

  [#LA3899]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Es posible que los procesos de Desktop Viewer (CDViewer.exe) y de wfica32.exe se cierren de forma inesperada durante la reconexión a una sesión de escritorio virtual.

  [#LA3944]

- Con esta corrección, la API de IsReconnectInProgress() se integra con Citrix Fast Connect 2.0. Esta característica determina si el proceso de reconexión está en curso o no mientras la función de reconexión automática de clientes está habilitada.

  [#LA4080]

- Esta corrección permite que las aplicaciones PassThrough puedan volver a conectarse y habilita el control del área de trabajo para dichas aplicaciones.

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

  Para habilitar el control del área de trabajo en el modo PassThrough:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
  Name: ForceEnableWSC
  Type: DWORD
  Data = 1

  Para permitir que las aplicaciones PassThrough puedan volver a conectarse:

  HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
  Name: BypassPassThruMode
  Type: DWORD
  Data = 1

  Nota: Esta corrección solo funciona en las siguientes condiciones:

  - Los dos o más saltos de conexión no pueden tener lugar en el mismo sitio o comunidad de servicios XenApp. En otras palabras, el dispositivo Receiver de punto final puede conectarse a un VDA de XenDesktop publicado en un sitio A de servicios XenApp y, a continuación, el cliente PassThrough de dicho VDA puede conectarse a un escritorio o una aplicación publicados en *otro* sitio de servicios XenApp (el sitio B).
  - El segundo salto de conexión debe realizarse a una sesión de terminal de Xen App. No puede realizarse a un VDA de XenDesktop.

  [#LA4206]

- Al usar software de asistencia remota en un escritorio publicado para representar un porcentaje impar de la pantalla del cliente (por ejemplo, un 95 %), es posible que la sesión de asistencia remota aparezca distorsionada.

  [#LA4313]

- Esta mejora de compatibilidad amplía el respaldo de la redirección de dispositivos USB de HDX Plug-n-Play para dispositivos USB adicionales.

  [#LA4335]

- Un interbloqueo en wfcrun32.exe puede impedir que se inicien correctamente nuevas sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LA4344]

- Es posible que falle la conexión con servidores XenApp mediante la herramienta de inicio rápido de Citrix o mediante archivos ICA estáticos que especifiquen "HTTPBrowserAddress=ServerName_Or_IP:Port" (por ejemplo: "HTTPBrowserAddress=192.168.1.10:8080").

  [#LA4585]

Excepciones del sistema

- El proceso de wfica32.exe puede cerrarse de forma inesperada, tras lo que aparece el siguiente mensaje de error:

  "Citrix HDX Engine detectó un problema y debe cerrarse".

  [#LA3412]

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

  [#LA3639]

- Es posible que el proceso de wfica32.exe se cierre de forma inesperada.

  [#LA4208]

Experiencia de utilización

- Esta corrección elimina la aparición innecesaria de avisos de inicio de sesión cuando Receiver 4.0 se usa con StoreFront.

  [#LA4652]

Interfaz de usuario

- La aplicación no consigue iniciarse si el nombre de aplicación y el nombre simplificado de la aplicación publicada no coinciden.

  [#LA3891]

Varios

- Esta versión incluye la versión más reciente del SSLSDK, versión 12.1.13.

  [#LA3804]

- Esta corrección mejora la funcionalidad de la función TerminateUser de Receiver para Windows en algunos entornos.

  [#LA3881]

Comparado con: Citrix Receiver para Windows 4.0

Receiver para Windows 4.0.1 contiene todas las correcciones incluidas en Receiver para Windows 4.0, además de las siguientes correcciones nuevas:

- Esta corrección elimina la aparición innecesaria de avisos de inicio de sesión cuando Receiver 4.0 se usa con StoreFront.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#LA4652]

Comparado con: Citrix Receiver para Windows 3.4

Receiver para Windows 4.0 contiene las siguientes correcciones en comparación con Citrix Receiver para Windows 3.4:

Redirección de Flash HDX MediaStream

- Si se mueve una ventana de vídeo fuera de la pantalla completa o parcialmente mientras el archivo de vídeo se está generando, esta puede dejar una zona oscura en la pantalla. La zona oscura permanece así aun después de devolver la ventana de vídeo a su sitio.

  [#LA0599]

- **Importante:** Antes de aplicar esta corrección en un dispositivo cliente, consulte en Knowledge Center el artículo CTX126817 para obtener información importante sobre cómo afecta la función de lista negra dinámica a la redirección de Flash del lado del cliente.

  En los casos en que la directiva *Habilitar obtención de contenido del lado del servidor* está habilitada en el servidor y el parámetro *Lista de URL para obtener contenido Flash del lado del servidor* se ha configurado para la directiva de redirección de Flash en el cliente, no se puede reproducir contenido Flash si la URL del contenido contiene caracteres Unicode o multibyte, algo común en los idiomas asiáticos.

  Para habilitar esta corrección en su totalidad, debe instalar una revisión hotfix de cliente que incluya la corrección #LA1621, además de:

  - *Para XenApp:* una revisión hotfix de HDX Flash que incluya la corrección #LA1621
  - *Para XenDesktop:* una revisión hotfix de Virtual Desktop Agent que incluya la corrección #LA1621

  Nota: Esta corrección también requiere que las páginas de códigos del idioma correspondiente estén instaladas en el cliente y el servidor. De forma predeterminada, el sistema operativo de Windows instala las páginas de códigos. Por ejemplo, la distribución de Windows 7 en japonés instala, de forma predeterminada, las páginas de códigos en japonés. Sin embargo, si utiliza una URL con caracteres en japonés en una distribución de Windows 7 en inglés, las páginas de códigos en japonés deben instalarse de forma explícita. Esto se aplica tanto al cliente como al servidor porque las URL se

© 1999-2017 Citrix Systems, Inc. All rights reserved.

transfieren desde el cliente al servidor cuando la obtención de contenido del lado del servidor está habilitada.

[#LA1621]

- Ciertas interacciones de los usuarios con contenido Flash, como hacer clic en botones, pueden provocar que Pseudocontainer2.exe se cierre de forma inesperada.

  [#LA1948]

- La redirección de contenido del lado del cliente puede fallar para ciertos tipos de contenido Flash y volver a la generación en el lado del servidor, incluidos los casos en que:

  1. El contenido Flash intenta descargar otro archivo Flash que no existe o no se encuentra
  2. El contenido Flash creado por Adobe Captive no pasa algunas comprobaciones lógicas de la función de redirección de contenido del lado del cliente
  3. El contenido Flash provoca que la función de redirección de contenido del lado del cliente envíe de forma remota interfaces no compatibles al servidor remoto
  4. El cliente intenta obtener contenido Flash aunque la URL esté configurada en la lista negra de direcciones URL de ServerContentFetching

  Para habilitar esta corrección, debe instalar una revisión hotfix de HDX Flash y de Receiver para Windows que incluya la corrección #LA2198. Para habilitar esta corrección para el problema n.º 1 anteriormente mencionado, también debe establecer la siguiente clave de Registro en el cliente:

  - *En Windows de 32 bits*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Type: REG_DWORD
    Data: 0
  - *En Windows de 64 bits*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    Name: FallbackIfFlashNotExist
    Type: REG_DWORD
    Data: 0

  [#LA2198]

- Al cambiar el enfoque de la ventana de Flash (una ventana secundaria de una ventana integrada con explorador Web) a una ventana local y cambiar el enfoque de nuevo a la barra de direcciones de la ventana integrada del explorador, es posible que no se pueda escribir en la barra de direcciones del explorador.

  [#LA2685]

- Importante: Antes de aplicar esta corrección en un dispositivo cliente, consulte en Knowledge Center el artículo CTX126817 para obtener información importante sobre cómo afecta la función de lista negra dinámica a la redirección de Flash del lado del cliente.

  Es posible que la función de redirección de Flash de HDX MediaStream no funcione en vídeos de Dailymotion (http://www.dailymotion.com) y genere un error. Este problema ocurre cuando el cliente y el servidor están ubicados en ubicaciones geográficas distintas.

  Para habilitar esta corrección, debe crear la siguiente clave de Registro:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
Name: DisableRegionFiltering
Type: REG_DWORD
Data: 1

[#LA3134]

HDX Plug-n-Play

- Esta mejora modifica el comportamiento predeterminado de la redirección USB de la siguiente manera:
  - Cuando Desktop Viewer se habilita, los usuarios pueden redirigir manualmente cualquier dispositivo USB.
  - Cuando Desktop Viewer no se habilita, los dispositivos USB se redirigen automáticamente.

  [#LA0108]
- Tras varios intentos incorrectos de asignar ciertos dispositivos USB a una sesión de escritorio virtual, los dispositivos desaparecen de Device Manager hasta reiniciar el dispositivo de punto final.

  [#LA0954]
- Al hacer clic en Dispositivos, en Desktop Viewer, para seleccionar un dispositivo USB con el fin de controlarlo de forma remota mediante la redirección de dispositivos USB de HDX Plug-n-Play, puede provocar que la ventana de Desktop Viewer deje de responder.

  [#LA3348]

Instalación, desinstalación y actualización

- Después de actualizarse a Receiver 3.*x*, los usuarios no pueden iniciar aplicaciones publicadas, y aparece el siguiente mensaje de error:

  "Esta versión de Citrix Receiver no respalda el cifrado seleccionado. Póngase en contacto con el administrador. Error 1046: El controlador virtual no se ha cargado".

  [#LA3120]

Teclado

- Minimizar una sesión de escritorio virtual con un clic en Inicio en Desktop Viewer puede provocar, de forma intermitente, que la tecla de tabulación deje de funcionar en el dispositivo de punto final hasta que la sesión se desconecte.

  [#LA2925]
- A partir de la versión 3.0 de Receiver para Windows, el valor del parámetro KeyboardTimer establecido en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard ya no funciona. Esta corrección restablece la funcionalidad.

  [#LA2949]
- Esta corrección soluciona un problema que puede provocar que el estado de las teclas Bloq Mayús, Bloq Num o Bloq Despl no esté sincronizado entre el cliente y el servidor en sesiones PassThrough activas en primer plano.

  [#LA3288]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Esta corrección soluciona un problema que puede provocar que el estado de las teclas Bloq Mayús, Bloq Num o Bloq Despl no esté sincronizado entre el cliente y el servidor en sesiones PassThrough activas en segundo plano.

  [#LA3310]

Impresión

- Al hacer clic en **Parámetros de impresora local**, en la ficha **Parámetros del cliente** de una hoja **Propiedades** de la impresora UPD y, a continuación, cerrar el cuadro de diálogo de los parámetros puede provocar que la hoja **Propiedades** deje de responder.

  [#259485]

Ventanas integradas

- Al usar la Central de conexiones o la Interfaz Web para cerrar una sesión integrada con datos sin guardar, aparece una ventana en negro con el siguiente mensaje:

  "Todavía deben cerrarse programas" con estas dos opciones: "Forzar cierre de sesión" y "Cancelar". La opción "Cancelar" no funciona.

  Después de instalar esta corrección, la opción "Cancelar" funciona como es debido. Después de usar el botón Cancelar, Citrix recomienda guardar los datos y, a continuación, cerrar la sesión para evitar futuras demoras de rendimiento.

  [#LA0318]

Sesión/conexión

- Después de desconectarse de una sesión de escritorio virtual y de volver a conectarse a ella, es posible que no se pueda grabar audio dentro de la sesión. Para habilitar esta corrección en su totalidad, debe instalar una revisión hotfix de servidor y de cliente que incluya la corrección #LA0821.

  [#LA0821]

- El tiempo necesario para las transferencias de archivos en una sesión de cliente puede ser mayor que en una sesión RDP.

  Para habilitar esta corrección en su totalidad, debe instalar una revisión hotfix de servidor y de cliente que incluya la corrección #LA1263.

  [#LA1263]

- En determinadas condiciones, cambiar la resolución de una sesión de escritorio virtual antes de que la sesión se desconecte de forma inesperada, como, por ejemplo, debido a una interrupción de la red, puede provocar que la resolución de la sesión no sea la esperada después de volver a conectarse.

  [#LA1377]

- Los escáneres de códigos de barras de los puertos serie no pueden procesar etiquetas si el tamaño de los datos de estas supera los 512 bytes. Para habilitar esta corrección, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: CommBufferSize
  Type: REG_DWORD

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Data: intervalo entre 512 (valor mínimo) y 2048 (valor máximo)

[#LA1695]

- Inhabilitar el servicio de lista de redes y/o el servicio de reconocimiento de ubicación de red tal y como se describe en el artículo de Knowledge Center CTX131577 provoca que la versión 12.3 de Online Plug-in pierda conectividad.

  [#LA2024]

- Es posible que, al iniciar una aplicación integrada publicada en una ruta UNC a través de una conexión con poco ancho de banda, tarde más de dos minutos en completarse.

  [#LA2170]

- Invocar el método de entrada de una sesión integrada mediante el comando Ctrl + Mayús puede cambiar también el método de entrada local del lado del cliente. Para evitar este problema, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  Name: Showlocallanguagebar
  Type: REG_DWORD
  Data: 1 ; 0

  [#LA2180]

- Cuando la redirección automática de clientes está habilitada, después de seleccionar Hibernar, es posible que no se pueda volver a conectar cuando el cliente se cierra automáticamente.

  Con esta corrección, el sistema puede suspenderse o colocarse en modo de hibernación con la redirección de dispositivos USB, y se puede volver a conectar automáticamente después de que el sistema vuelva del modo de espera.

  [#LA3061]

- Es posible que las aplicaciones publicadas no consigan iniciarse si la compresión ICA se ha establecido en "OFF" en Citrix Receiver para Windows 3.x en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off.

  [#LA3072]

- En un entorno de varios monitores, es posible que la barra de herramientas de Desktop Viewer ya no sea visible al cambiar la pantalla a un monitor secundario en el modo de pantalla completa.

  [#LA3083]

- En configuraciones con doble monitor con conexión a un Virtual Desktop Agent y donde el monitor principal es un equipo portátil, apagar y encender la pantalla del equipo portátil provoca que la sesión solo se muestre en el monitor principal.

  [#LA3202]

- Al usar la versión 3.3 de actualización acumulativa 1 o la versión 3.4 de Receiver para Windows en una estación de trabajo de Windows XP con Internet Explorer 8, es posible que la aplicación inicial no se inicie desde la Interfaz Web.

  [#LA3234]

- Las sesiones de consola y de XenDesktop pueden dejar de responder (se atascan en la pantalla de bienvenida) al intentar

© 1999-2017 Citrix Systems, Inc. All rights reserved.

volver a conectarse a una sesión de escritorio virtual mediante Receiver para Linux. El problema ocurre cuando el controlador WDDM se habilita en el Virtual Desktop Agent y hay otra sesión de escritorio virtual activa en la sesión.

[#LA3241]

- Es posible que la versión 3.4 de Receiver para Windows no pueda iniciarse si en "Configuración regional y de idioma" de Windows 7 se ha establecido "Kazajo (Kazajistán)".

  [#LA3517]

Excepciones del sistema

- El proceso de wfica32.exe puede cerrarse de forma inesperada en entornos en los que se haya implementado EdgeSight for Load Testing.

  [#LA0289]

- El proceso de wfcrun.exe puede cerrarse de forma inesperada en entornos en los que se haya implementado HP LoadRunner.

  [#LA0859]

- Con la directiva de sonido configurada como sonido de alta definición, el proceso de wfica32.exe puede cerrarse de forma inesperada al reproducir archivos de sonido aleatorios de muestra en el Panel de control de Sonido de los escritorios publicados.

  [#LA1000]

- Es posible que la versión 12.3 de Online Plug-in se cierre de forma inesperada durante la desconexión de una sesión desde un sitio de la Interfaz Web con una hoja de cálculo de Microsoft Excel 2007 abierta.

  [#LA2274]

- Con el acceso a aplicaciones locales habilitado, es posible que no se pueda conectar con los Virtual Desktop Agents si hay avisos legales configurados para Virtual Desktop Agent.

  [#LA2351]

- El proceso de Pnamain.exe puede cerrarse de forma inesperada al volver a conectar con una sesión.

  [#LA2704]

- Las sesiones de monitor único y los dispositivos cliente con Windows con estilo Aero pueden desconectarse de forma inesperada. El problema puede ocurrir cuando una vista previa, como parte de la función de vista previa de ventanas dinámicas, se envía al cliente; en ese momento, un subproceso de twi3.dll puede finalizar el proceso de Winlogon.exe, que a su vez provoca que la sesión se desconecte.

  Para resolver este problema en su totalidad, debe instalar una revisión hotfix de XenApp y de Receiver que incluya la corrección #LA2858.

  [#LA2858]

- Es posible que el proceso de wfica32.exe se cierre de forma inesperada. El problema ocurre debido a una desreferencia de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

memoria no válida.

[#LA2860]

- Al imprimir en ciertos casos de doble salto, aparece el siguiente mensaje de error y el proceso de wfica32.exe se cierra de forma inesperada: "Citrix HDX Engine ha dejado de funcionar". El problema se debe a los nombres de los puertos que superan los 260 caracteres de longitud.

  Para solucionar este problema, debe instalar una revisión hotfix para servidores y para Receiver que incluye la corrección #LA3009 (XA650R01W2K8R2X64056, RcvrForWin3.3_13.3.104 o las revisiones hotfix que las sustituyan).

  [#LA3009]

- Citrix Receiver puede generar varias instancias del proceso de selfserviceplugin.exe, lo que provoca que el sistema se quede sin memoria.

  [#LA3460]

- Es posible que Desktop Viewer se cierre de forma inesperada durante el cierre de sesión.

  [#LA3567]

- PNMain.exe puede cerrarse de forma inesperada al usar Online Plug-in como el cliente PassThrough.

  [#LA0785]

Experiencia de utilización

- Al usar la redirección USB, es posible que los dispositivos USB SpaceMouse desaparezcan de las sesiones de escritorio virtual después de usarlos unas horas.

  [#LA2256]

- Esta mejora para la versión 3.4 de Receiver para Windows permite suprimir el siguiente mensaje de autenticación de inicios de sesión en redes VPN que aparece cuando el usuario cambia de conexión de red.

  Para suprimir el mensaje, cree la siguiente clave de Registro:

  - *En Windows de 32 bits*:
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    Name: AutoSecureConnection
    Type: REG_DWORD
    Value: 0 (inhabilita la ventana emergente de la red VPN)
  - *En Windows de 64 bits*:
    HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
    Name: AutoSecureConnection
    Type: REG_DWORD
    Value: 0 (inhabilita la ventana emergente de la red VPN)

  [#LA3772]

Interfaz de usuario

- Esta corrección modifica la traducción coreana del título del icono de "Escritorio inicial" de la barra de herramientas de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Desktop Viewer para una mayor precisión.

[#232198]

- Al hacer clic en **Cancelar**, en el cuadro de diálogo que aparece cuando se ejecuta un acceso directo a un grupo de escritorios en un dispositivo de punto final, aparece el siguiente mensaje de error impreciso y confuso:

  "La aplicación o el escritorio no se han podido iniciar. Compruebe la conexión de red".

  [#259081]

- En una ventana de sesión maximizada, es posible que la barra de herramientas de Desktop Viewer no aparezca correctamente si hace clic en **Conectar** en el cuadro de diálogo de USBMultiInsertDialogue *después* de que desaparezca la pantalla Conexión de sesión.

  [#260390]

- El tema de ayuda sobre la asignación de unidades del cliente de icaclient.adm señala incorrectamente que las directivas no sobrescriben las selecciones de los usuarios. Las directivas sí sobrescriben las selecciones de los usuarios.

  [#LA0398]

- Con ciertas aplicaciones personalizadas, el cuadro de modificación de la repetición local del texto de la reducción de latencia SpeedScreen muestra una barra negra al escribir.

  [#LA0544]

- Los mensajes de bienvenida y/o de estado completado tras la primera entrega desde Merchandising Server no aparecen.

  [#LA2277]

- El icono de Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO) en el área de notificaciones de la barra de tareas de Windows puede desaparecer de forma inesperada al iniciar una aplicación publicada.

  [#LA3190]

- La barra de tareas no es accesible si se configura para ocultarse automáticamente y, a continuación, se mueve de su ubicación predeterminada a la parte superior, izquierda o derecha de la pantalla.

  [#LA3400]

Varios

- Al reproducir secuencias de audio UDP, el número de identificadores del proceso de wfica32.exe puede aumentar significativamente.

  [#LA3094]

- Esta corrección quita una limitación en un solo sitio de la Interfaz Web 5.4 de Program Neighborhood en Receiver para Web 3.3.

  [#LA3142]

© 1999-2017 Citrix Systems, Inc. All rights reserved.