

Guía de instalación y configuración de VMware Horizon HTML Access

13 de diciembre de 2018

VMware Horizon HTML Access 4.10

VMware Horizon 7 7.7



vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

El sitio web de VMware también ofrece las actualizaciones de producto más recientes.

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2013–2018 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y marca comercial](#).

Contenido

Guía de instalación y configuración de VMware Horizon HTML Access 5

1 Instalación y configuración 6

- Requisitos del sistema para HTML Access 7
- Preparar el servidor de conexión y los servidores de seguridad 9
 - Reglas de firewall para acceder al navegador web cliente 10
- Configurar Horizon 7 para eliminar credenciales de la caché 11
- Preparar escritorios, grupos y granjas 12
- Requisitos de la función Session Collaboration 14
- Configurar los agentes HTML Access para usar nuevos certificados TLS 15
 - Agregar el complemento del certificado a MMC en un escritorio remoto 16
 - Importar un certificado para el agente HTML Access al almacén de certificados de Windows 16
 - Importar certificados raíz e intermedio para el agente HTML Access 17
 - Configurar la huella digital de certificado en el Registro de Windows 18
- Configurar los agentes HTML Access para usar conjuntos de cifrado específicos 19
- Configurar iOS para usar certificados firmados por una entidad de certificación 20
- Usar un certificado firmado por una CA con Unified Access Gateway 20
- Actualizar el software de HTML Access 20
- Desinstalar el componente HTML Access desde el servidor de conexión 21
- Configurar el uso compartido de datos de Horizon Client 21
 - Datos recopilados por VMware 21

2 Configurar HTML Access para usuarios finales 24

- Configurar la página del portal web de VMware Horizon para los usuarios finales 24
- Utilizar URI para configurar clientes web de HTML Access 28
 - Sintaxis para crear URI para HTML Access 28
 - Ejemplos de URI 31
- Configuración de las directivas de grupo de HTML Access 34

3 Administrar las conexiones de las aplicaciones publicadas y los escritorios remotos 35

- Conectarse a una aplicación publicada o a un escritorio remoto 35
- Confiar en un certificado raíz autofirmado 37
- Conectarse a un servidor en el modo Workspace ONE 38
- Utilizar la función Acceso sin autenticar para conectarse a aplicaciones publicadas 39
- Establecer la zona horaria 40
- Permitir la decodificación H.264 41
- Cerrar sesión o desconectarse 41

4 Usar un escritorio remoto o una aplicación publicada 43

Matriz de compatibilidad de funciones 43

Utilizar la barra lateral 45

Resolución de pantalla y monitores 49

Utilizar varios monitores 49

Resolución de pantalla 50

Usar la sincronización PPP 51

Usar el modo de pantalla completa 52

Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos 53

Usar la función Session Collaboration 54

Invitar a un usuario a que se una a una sesión de escritorio remoto 54

Administrar una sesión colaborativa 56

Unirse a una sesión colaborativa 57

Copiar y pegar texto 58

Usar la ventana Copiar y pegar 59

Transferir archivos entre el cliente y un escritorio remoto 61

Descargar archivos de un escritorio en el cliente 62

Cargar archivos del cliente a un escritorio 62

Habilitar el modo de sesión múltiple para las aplicaciones publicadas 63

Sonido 63

Combinaciones de teclas de método abreviado 64

Internacionalización 67

Teclados internacionales 68

5 Solucionar problemas relacionados con Horizon Client 69

Reiniciar un escritorio remoto 69

Restablecer un escritorio remoto o una aplicación publicada 70

Guía de instalación y configuración de VMware Horizon HTML Access

Esta guía, *Guía de instalación y configuración de VMware Horizon HTML Access*, describe cómo instalar, configurar y utilizar el software VMware Horizon[®] HTML Access[™] para conectarse a escritorios virtuales sin tener que instalar ningún software en un sistema cliente.

Este documento incluye información sobre los requisitos del sistema e instrucciones para instalar el software de HTML Access en un servidor de VMware Horizon 7 y en una máquina virtual del escritorio remoto para que los usuarios finales puedan usar un navegador web para acceder a los escritorios remotos.

Importante Esta información está destinada a administradores que ya tienen experiencia utilizando Horizon 7 y VMware vSphere. Si es un usuario sin experiencia en el uso de Horizon 7, es posible que tenga que consultar las instrucciones paso a paso de los procedimientos básicos en los documentos *Instalación de Horizon 7* y *Administración de Horizon 7*.

Instalación y configuración

La configuración de una implementación de Horizon 7 para HTML Access incluye la instalación de HTML Access en Horizon Connection Server, la apertura de los puertos necesarios y la instalación del componente HTML Access en la máquina virtual del escritorio remoto.

Los usuarios finales pueden acceder entonces a los escritorios remotos abriendo un navegador compatible y escribiendo la URL de Horizon Connection Server.

Este capítulo incluye los siguientes temas:

- [Requisitos del sistema para HTML Access](#)
- [Preparar el servidor de conexión y los servidores de seguridad](#)
- [Configurar Horizon 7 para eliminar credenciales de la caché](#)
- [Preparar escritorios, grupos y granjas](#)
- [Requisitos de la función Session Collaboration](#)
- [Configurar los agentes HTML Access para usar nuevos certificados TLS](#)
- [Configurar los agentes HTML Access para usar conjuntos de cifrado específicos](#)
- [Configurar iOS para usar certificados firmados por una entidad de certificación](#)
- [Usar un certificado firmado por una CA con Unified Access Gateway](#)
- [Actualizar el software de HTML Access](#)
- [Desinstalar el componente HTML Access desde el servidor de conexión](#)
- [Configurar el uso compartido de datos de Horizon Client](#)

Requisitos del sistema para HTML Access

Con HTML Access, un navegador admitido es el único software que necesita el sistema cliente. La implementación de Horizon 7 debe cumplir algunos requisitos de software.

Nota A partir de la versión 7.0, View Agent pasa a ser Horizon Agent.

Sistemas cliente o de navegador

Navegador	Versión
Chrome	69, 70
Internet Explorer	11
Safari	12
Firefox	62, 63
Microsoft Edge	42, 44

Nota

- En dispositivos Android, Chrome no admite la tecla Windows, el uso de varios monitores, las operaciones de copiar y pegar al sistema, la transferencia de archivos, la impresión, la decodificación H.264, la limpieza de credenciales ni el uso de un mouse externo. Las siguientes teclas y combinaciones de teclas tampoco funcionan en el teclado del software: Supr, Ctrl+A, Ctrl+C, Ctrl+V, Ctrl+X, Ctrl+Y, Ctrl+Z.
- En dispositivos móviles, Safari no admite el uso de un mouse externo, la tecla Windows, el uso varios monitores, las operaciones de copiar y pegar al sistema, la transferencia de archivos, la impresión, la decodificación H.264 ni la limpieza de credenciales.

Sistemas operativos cliente

Sistema operativo	Versión
Windows	7 SP1 (32 bits y 64 bits)
Windows	8.x (32 bits y 64 bits)
Windows	10.x (32 bits y 64 bits)
macOS	10.14.x (Mojave)
macOS	10.13.x (High Sierra)
iOS	10 o posterior
Chrome OS	28.x o posterior
Android	7 o posterior

Escritorios remotos

HTML Access necesita Horizon Agent 7.0 o versiones posteriores y es compatible con todos los sistemas operativos de escritorio que admite Horizon 7.0. Para obtener más información, consulte el tema "Sistemas operativos compatibles con Horizon Agent" de la versión 7.0 o posterior de *Instalación de Horizon 7*.

Configuración de grupo

HTML Access necesita la siguiente configuración de grupo en Horizon Administrator:

- La configuración **Resolución máxima de los monitores** debe ser una resolución de **1920 x 1200** o superior para que el escritorio remoto tenga al menos 17,63 MB de RAM de vídeo.

Si utiliza aplicaciones 3D o los usuarios finales utilizan un MacBook con pantalla Retina o un Chromebook Pixel de Google, consulte [Resolución de pantalla](#).

- La opción **HTML Access** debe estar habilitada.

Las instrucciones de configuración se encuentran en [Preparar escritorios, grupos y granjas](#).

Servidor de conexión

Se debe instalar en el servidor el servidor de conexión con la opción HTML Access.

Al instalar el componente HTML Access, la regla del **servidor de conexión de VMware Horizon View (integrado)** está habilitada en el firewall de Windows para que este se configure automáticamente y se permita el tráfico entrante al puerto TCP 8443.

Servidor de seguridad

Se debe instalar la misma versión que tenga el servidor de conexión en el servidor de seguridad.

Si los sistemas cliente se conectan desde fuera del firewall corporativo, use un servidor de seguridad. Con un servidor de seguridad, los sistemas cliente no necesitan una conexión VPN.

Nota Un único servidor de seguridad puede admitir hasta 800 conexiones simultáneas a clientes web.

Firewalls de terceros

Agregue reglas para permitir el siguiente tráfico:

- Servidores (como servidores de seguridad, de réplicas e instancias del servidor de conexión): tráfico entrante al puerto TCP 8443.

- Máquinas virtuales de escritorios remotos: tráfico entrante (de servidores) al puerto TCP 22443.

Protocolo de visualización para Horizon

VMware Blast

Cuando utilice un navegador web para acceder a un escritorio remoto, se utiliza el protocolo VMware Blast en lugar del protocolo PCoIP o Microsoft RDP. VMware Blast utiliza HTTPS (HTTP sobre SSL/TLS).

Preparar el servidor de conexión y los servidores de seguridad

Antes de que los usuarios finales puedan conectarse a un servidor y acceder a un escritorio remoto o a una aplicación publicada, un administrador de Horizon debe instalar el servidor de conexión y los servidores de seguridad, si son necesarios.

Puede utilizar dispositivos de Unified Access Gateway, en lugar de servidores de seguridad, para los accesos externos y seguros. Para obtener más información, consulte el documento *Implementación y configuración de Unified Access Gateway*.

A continuación, aparece una lista con las tareas que un administrador de Horizon debe realizar para usar HTML Access.

- 1 Instale el servidor de conexión con la opción **Instalar HTML Access** seleccionada en el servidor o en los servidores, esto comprende un grupo replicado del servidor de conexión. Esta opción instala el componente HTML Access. Esta opción está seleccionada en el instalador de forma predeterminada. Para obtener más información, consulte el documento *Instalación de Horizon 7*.

Para verificar que el componente HTML Access esté instalado, puede abrir el applet Desinstalar un programa de Windows y buscar **VMware Horizon 7 HTML Access** en la lista.
- 2 Si usa servidores de seguridad, instale el servidor de seguridad. La versión del servidor de seguridad debe coincidir con la del servidor de conexión. Para obtener más instrucciones de instalación, consulte el documento *Instalación de Horizon 7*.
- 3 Compruebe que cada instancia del servidor de conexión o del servidor de seguridad cuenten con un certificado TLS que se pueda verificar completamente con el nombre de host que introdujo en el navegador web. Para obtener más información, consulte el documento *Instalación de Horizon 7*.

- 4 Para usar una autenticación en dos fases, como autenticaciones RSA SecurID o RADIUS, compruebe que esta función esté habilitada en el servidor de conexión. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de Horizon 7*.

Importante Si habilita la opción **Ocultar la lista de dominios en la interfaz de usuario del cliente** y selecciona la autenticación de dos fases (RSA SecureID o RADIUS) para la instancia del servidor de conexión, no exija que coincidan los nombres de usuarios de Windows. Exigir que coincidan los nombres de usuario de Windows evita que siempre falle el inicio de sesión si los usuarios escriben la información del dominio en el cuadro de texto de nombre de usuario. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de Horizon 7*.

- 5 Si usa un firewall de terceros, configure las reglas para que permitan el tráfico entrante al puerto TCP 8443 en todos los servidores de seguridad y hosts del servidor de conexión en un grupo replicado y configure una regla para permitir el tráfico entrante (desde los servidores) al puerto TCP 22443 en las máquinas virtuales de escritorio remoto y hosts RDS del centro de datos. Si desea obtener más información, consulte [Reglas de firewall para acceder al navegador web cliente](#).
- 6 Para proporcionar acceso sin autenticar a las aplicaciones publicadas, habilite esta función en el servidor de conexión. Para obtener más información, consulte el documento *Administración de Horizon 7*.

Después de que se instalen los servidores, la opción **Puerta de enlace segura de Blast** se habilita en las instancias del servidor de conexión y en los servidores de seguridad aplicables de Horizon Administrator. Del mismo modo, la opción **URL externa de Blast** se configura para usar la puerta de enlace segura de Blast en las instancias de los servidores de seguridad y de los servidores de conexión en las que se aplican. De forma predeterminada, la URL incluye el FQDN de la URL externa del túnel seguro y el número del puerto predeterminado, 8443. La URL debe contener el FQDN y el número de puerto que un sistema cliente puede usar para acceder al host del servidor de conexión o el host del servidor de seguridad. Para obtener más información, consulte cómo configurar URL externas en una instancia del servidor de conexión en el documento *Instalación de Horizon 7*.

Nota Puede utilizar HTML Access con VMware Workspace ONE para permitir a los usuarios conectarse a sus escritorios a través de un navegador compatible con HTML5. Si desea obtener información sobre cómo instalar Workspace ONE y configurarlo para su uso con el servidor de conexión, consulte la documentación de Workspace ONE. Para obtener información sobre cómo emparejar el servidor de conexión con un servidor de autenticación SAML, consulte el documento *Administración de Horizon 7*.

Reglas de firewall para acceder al navegador web cliente

Si desea permitir que los navegadores web cliente establezcan conexiones con servidores de seguridad, instancias del servidor de conexión, escritorios remotos y aplicaciones publicadas, los firewalls deben permitir el tráfico entrante en algunos puertos TCP.

Las conexiones de HTML Access deben usar HTTPS y no se permiten conexiones HTTP.

De forma predeterminada, cuando instala una instancia del servidor de conexión o del servidor de seguridad, se habilita la regla **Servidor de conexión de VMware Horizon View (integrado en Blast)** en el Firewall de Windows, y dicho firewall se configura para permitir el tráfico de entrada al puerto TCP 8443.

Tabla 1-1. Reglas de firewall para acceder al navegador cliente

Origen	Puerto de origen predeterminado	Protocolo	Destino	Puerto de destino predeterminado	Notas
Navegador web cliente	TCP cualquier	tráfico	Instancia del servidor de conexión o del servidor de seguridad	TCP 443	Para establecer la conexión inicial, el navegador web de un dispositivo cliente se conecta a una instancia del servidor de conexión o del servidor de seguridad en el puerto TCP 443.
Navegador web cliente	TCP cualquier	tráfico	Puerta de enlace segura de Blast	TCP 8443	Después de establecer la conexión inicial, el navegador web de un dispositivo cliente se conecta a la puerta de enlace segura de Blast en el puerto TCP 8443. La puerta de enlace segura de Blast se debe habilitar en una instancia del servidor de conexión o del servidor de seguridad para permitir que se produzca esta segunda conexión.
Puerta de enlace segura de Blast	TCP cualquier	tráfico	HTML Access Agent	TCP 22443	Si la puerta de enlace segura de Blast está habilitada, después de que el usuario seleccione un escritorio remoto o una aplicación publicada, dicha puerta de enlace se conecta al agente HTML Access en el puerto TCP 22443 de la máquina virtual del escritorio remoto o del host RDS. Cuando se instala Horizon Agent, este componente del agente está incluido.
Navegador web cliente	TCP cualquier	tráfico	HTML Access Agent	TCP 22443	Si la puerta de enlace segura de Blast no está habilitada, después de que el usuario seleccione un escritorio remoto o una aplicación publicada, el navegador web de un dispositivo cliente establece una conexión directa con el agente HTML Access en el puerto TCP 22443 de la máquina virtual del escritorio remoto o el host RDS. Cuando se instala Horizon Agent, este componente del agente está incluido.

Configurar Horizon 7 para eliminar credenciales de la caché

Puede configurar Horizon 7 para quitar de la caché las credenciales de un usuario cuando este cierre una pestaña que establece la conexión con una aplicación publicada o escritorio remoto, o cierre la pestaña que establece la conexión con la ventana de selección de aplicaciones y escritorios.

Cuando esta función está deshabilitada (configuración predeterminada), las credenciales se mantienen en la caché.

Nota Si habilita esta función, las credenciales también se eliminan de la caché cuando un usuario actualiza la página de selección de la aplicación y del escritorio o la página de la sesión remota, o ejecuta un comando URI en la pestaña que contiene la sesión remota. Si el servidor presenta un certificado autofirmado, las credenciales se eliminan de la caché cuando un usuario inicie una aplicación publicada o un escritorio remoto y acepte el certificado cuando aparece la advertencia de seguridad.

Requisitos previos

Para usar esta función se necesita Horizon 7 7.0.2 o versiones posteriores.

Procedimiento

- 1 En Horizon Administrator, seleccione **Configuración de View > Configuración global** y haga clic en **Editar** en el panel General.
- 2 Seleccione la casilla **Limpiar credencial al cerrar la pestaña para HTML Access**.
- 3 Para guardar los cambios, haga clic en **Aceptar**.

Los cambios se aplicarán de forma inmediata. No es necesario que reinicie el servidor de conexión.

Preparar escritorios, grupos y granjas

Antes de que los usuarios finales puedan acceder a una aplicación publicada o un escritorio remoto, un administrador de Horizon puede configurar las opciones de los grupos y las granjas, e instalar Horizon Agent en máquinas virtuales del escritorio y hosts RDS en el centro de datos.

El cliente HTML Access es una buena alternativa cuando el software Horizon Client no está instalado en el sistema cliente.

Nota El software Horizon Client ofrece más funciones y mejor rendimiento que el cliente HTML Access. Por ejemplo, con el cliente HTML Access, algunas combinaciones de teclas no funcionan en el escritorio remoto, pero sí lo hacen con Horizon Client.

Requisitos previos

- Verifique los componentes de Horizon cumplan los requisitos del sistema para HTML Access. Consulte [Requisitos del sistema para HTML Access](#).
- Compruebe que el componente HTML Access esté instalado con el servidor de conexión en el host o los hosts y que el firewall de Windows en las instancias del servidor de conexión y los servidores de seguridad permitan el tráfico entrante en el puerto TCP 8443. Consulte [Preparar el servidor de conexión y los servidores de seguridad](#).
- Si usa un firewall de terceros, configure una regla para permitir el tráfico entrante desde los servidores Horizon al puerto TCP 22443 en máquinas virtuales de escritorio y hosts RDS en el centro de datos. Consulte [Reglas de firewall para acceder al navegador web cliente](#).

- Verifique que la máquina virtual que pretende usar como origen de escritorio o el host RDS que aloje aplicaciones y escritorios remotos, tengan instalado un sistema operativo admitido y VMware Tools. Consulte [Requisitos del sistema para HTML Access](#).
- Familiarícese con los procedimientos para crear grupos y granjas, así como para autorizar usuarios. Consulte los documentos *Configurar escritorios virtuales en Horizon 7* y *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Para verificar que los usuarios finales pueden acceder a los escritorios remotos y las aplicaciones publicadas, instale Horizon Client para Windows en un sistema cliente. Puede utilizar Horizon Client para Windows para probar la conexión antes de intentar conectarse desde un navegador web. Para obtener más instrucciones de instalación, consulte el documento *Guía de instalación y configuración de VMware Horizon Client para Windows*.
- Compruebe que cuente con uno de los navegadores admitidos para acceder a un escritorio remoto o una aplicación publicada. Consulte [Requisitos del sistema para HTML Access](#).

Procedimiento

- 1 En las aplicaciones y los escritorios publicados, use Horizon Administrator para crear o editar grupos y granjas, y habilite la opción **Permitir HTML Access en los escritorios y las aplicaciones de esta granja** en la configuración de la granja.
- 2 En los grupos de escritorios virtuales, use Horizon Administrator para crear o editar el grupo de escritorios, por lo que el grupo se podrá usar con HTML Access.
 - a Habilitar **HTML Access** en la configuración del grupo de escritorios.
 - b En la configuración de los grupos, compruebe que el valor de **Resolución máxima de cualquier monitor** sea **1920x1200** o superior.

- 3 Después de que se creen los grupos, se recompongan o se actualicen para usar Horizon Agent con la opción **Permitir HTML Access en los escritorios y las aplicaciones de esta granja** o **HTML Access**, use Horizon Client para Windows para conectarse a un escritorio remoto o una aplicación publicada.

Con este paso, antes de intentar usar HTML Access, verifique que el grupo esté trabajando correctamente.

- 4 Abra un navegador compatible e introduzca una URL que lleve a la instancia del servidor de conexión.

Por ejemplo:

```
https://horizon.mycompany.com
```

Debe incluir **https** en la dirección URL.

- 5 En la página web que aparece, haga clic en **VMware Horizon HTML Access** e inicie sesión como lo haría con el software Horizon Client para Windows.

- 6 En el escritorio y la página de selección de la aplicación que aparece, haga clic en un icono al que conectarse.

Ahora puede acceder a un escritorio remoto o a una aplicación publicada desde un navegador web.

Pasos siguientes

Para obtener más seguridad, si las directivas de seguridad requieren que el agente HTML Access del escritorio remoto use un certificado TLS de una entidad de certificación, consulte [Configurar los agentes HTML Access para usar nuevos certificados TLS](#).

Requisitos de la función Session Collaboration

Con la función Session Collaboration, los usuarios pueden invitar a otros usuarios a que se unan a una sesión de escritorio remoto de Windows existente. Para admitir la función Session Collaboration, la implementación de Horizon debe cumplir ciertos requisitos.

Colaboradores de sesión

Para unirse a una sesión colaborativa, un usuario debe tener Horizon Client 4.7 para Windows, Mac o Linux instalado en el sistema cliente, o bien usar la versión 4.7 de HTML Access o una posterior.

Escritorios remotos Windows

- Se debe instalar Horizon Agent 7.4 o una versión posterior en el escritorio virtual Windows o en el host RDS para los escritorios publicados.
- Debe habilitarse la función Session Collaboration en el nivel de granja o grupo de escritorios. Para obtener más información sobre cómo habilitar la función Session Collaboration en los grupos de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7*. Para obtener más información sobre cómo habilitar la función Session Collaboration en una granja, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Puede utilizar la configuración de directiva de grupo de Horizon Agent para configurar la función Session Collaboration. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Escritorios remotos Linux

Para conocer los requisitos que se aplican a los escritorios remotos Linux, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

Servidor de conexión

Para usar la función Session Collaboration, la instancia del servidor de conexión debe usar una licencia empresarial.

Protocolos de visualización

VMware Blast

La función Session Collaboration no admite las sesiones de aplicaciones publicadas.

Configurar los agentes HTML Access para usar nuevos certificados TLS

Para cumplir la normativa de seguridad o del sector, puede reemplazar los certificados TLS predeterminados que genera el agente HTML Access por un certificado que firme una entidad de certificación (CA).

Cuando instala el agente HTML Access en un escritorio remoto, el servicio del agente HTML Access crea certificados autofirmados y predeterminados. El servicio presenta los certificados predeterminados para los navegadores que usen HTML Access.

Nota En el sistema operativo invitado del escritorio de la máquina virtual, este servicio se denomina VMware Blast.

Para reemplazar los certificados predeterminados por los certificados firmados que obtiene de una CA, debe importar el certificado al almacén de certificados del equipo local Windows en cada escritorio remoto. También debe configurar un valor de registro que permita que el agente HTML Access use el nuevo certificado.

Si reemplaza los certificados predeterminados del agente HTML Access por certificados firmados por una CA, configure un único certificado en cada escritorio. No configure un certificado firmado por una CA en una plantilla o una máquina virtual principal que use para crear un grupo de escritorios. Este enfoque tiene como resultado cientos o miles de escritorios remotos con los mismos certificados.

Procedimiento

1 [Agregar el complemento del certificado a MMC en un escritorio remoto](#)

Antes de poder agregar certificados al almacén de certificados del equipo local Windows, debe agregar el complemento de certificados en Microsoft Management Console (MMC) de los escritorios remotos donde el agente HTML Access está instalado.

2 [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#)

Para reemplazar un certificado predeterminado del agente HTML Access por un certificado firmado por una CA, debe importar este último al almacén de certificados del equipo local de Windows. Realice este procedimiento en cada escritorio remoto donde el agente HTML Access está instalado.

3 [Importar certificados raíz e intermedio para el agente HTML Access](#)

Si los certificados raíz e intermedio de la cadena de certificados no se importan junto con el certificado SSL ya importado para el agente HTML Access, debe incluirlos en el almacén de certificados del equipo local Windows.

4 [Configurar la huella digital de certificado en el Registro de Windows](#)

Para permitir que HTML Access Agent use un certificado firmado por una entidad de certificación que se importó en el almacén de certificados de Windows, debe configurar la huella digital de certificado en una clave del Registro de Windows. Debe realizar este paso en cada escritorio remoto en el que reemplace el certificado predeterminado por un certificado firmado por una entidad de certificación.

Agregar el complemento del certificado a MMC en un escritorio remoto

Antes de poder agregar certificados al almacén de certificados del equipo local Windows, debe agregar el complemento de certificados en Microsoft Management Console (MMC) de los escritorios remotos donde el agente HTML Access está instalado.

Requisitos previos

Compruebe que el complemento de certificados y MMC estén disponibles en el sistema operativo invitado de Windows donde está instalado el agente de HTML Access.

Procedimiento

- 1 En el escritorio remoto, haga clic en **Inicio** y escriba **mmc.exe**.
- 2 En la ventana **MMC**, diríjase a **Archivo > Agregar o quitar complemento**.
- 3 En la ventana **Agregar o quitar complementos**, seleccione **Certificados** y haga clic en **Agregar**.
- 4 En la ventana **Complemento Certificados**, seleccione **Cuenta de equipo**, haga clic en **Siguiente**, seleccione **Equipo local** y, a continuación, haga clic en **Finalizar**.
- 5 En la ventana **Agregar o quitar complementos**, haga clic en **Aceptar**.

Pasos siguientes

Importe el certificado SSL en el almacén de certificados del equipo local Windows. Consulte [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#).

Importar un certificado para el agente HTML Access al almacén de certificados de Windows

Para reemplazar un certificado predeterminado del agente HTML Access por un certificado firmado por una CA, debe importar este último al almacén de certificados del equipo local de Windows. Realice este procedimiento en cada escritorio remoto donde el agente HTML Access está instalado.

Requisitos previos

- Verifique que el agente HTML Access está instalado en el escritorio remoto.
- Verifique que se copió el certificado firmado por una CA al escritorio remoto.
- Verifique que el complemento Certificado se agregó a MMC. Consulte [Agregar el complemento del certificado a MMC en un escritorio remoto](#).

Procedimiento

- 1 En la ventana MMC del escritorio remoto, expanda el nodo **Certificados (equipo local)** y seleccione la carpeta **Personal**.
- 2 En el panel Acciones, diríjase a **Más acciones > Todas las tareas > Importar**.

- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenado el certificado.
- 4 Seleccione el archivo del certificado y haga clic en **Abrir**.

Para visualizar el tipo de archivo del certificado, puede seleccionar su formato en el menú desplegable **Nombre de archivo**.
- 5 Escriba la contraseña de la clave privada que se incluye en el archivo del certificado.
- 6 Seleccione **Marcar esta clave como exportable**.
- 7 Seleccione **Incluir todas las propiedades ampliables**.
- 8 Haga clic en **Siguiente** y en **Finalizar**.

El nuevo certificado aparece en la carpeta **Certificados (equipo local) > Personal > Certificados**.
- 9 Verifique que el nuevo certificado contiene una clave privada.
 - a En la carpeta **Certificados (equipo local) > Personal > Certificados**, haga doble clic en el nuevo certificado.
 - b En la pestaña General del cuadro de diálogo Información del certificado, verifique que aparece la siguiente afirmación: Tiene una clave privada correspondiente a este certificado.

Pasos siguientes

Si es necesario, importe el certificado raíz y los certificados intermedios al almacén de certificados de Windows. Consulte [Importar certificados raíz e intermedio para el agente HTML Access](#).

Configure la clave de registro apropiada con la huella digital del certificado. Consulte [Configurar la huella digital de certificado en el Registro de Windows](#).

Importar certificados raíz e intermedio para el agente HTML Access

Si los certificados raíz e intermedio de la cadena de certificados no se importan junto con el certificado SSL ya importado para el agente HTML Access, debe incluirlos en el almacén de certificados del equipo local Windows.

Procedimiento

- 1 En la consola MMC del escritorio remoto, expanda el nodo **Certificados (equipo local)** y diríjase a la carpeta **Entidades de certificación raíz de confianza > Certificados**.
 - Si el certificado raíz está en esta carpeta y no existen certificados intermedios en la cadena de certificados, omita este procedimiento.
 - Si el certificado raíz no se encuentra en esta carpeta, comience en el paso 2.
- 2 Haga clic con el botón secundario en la carpeta **Entidades de certificación raíz de confianza > Certificados** y, a continuación, en **Todas las tareas > Importar**.

- 3 En el asistente **Importación de certificado**, haga clic en **Siguiente** y busque la ubicación en la que está almacenada el certificado CA raíz.
- 4 Seleccione el archivo del certificado CA raíz y haga clic en **Abrir**.
- 5 Haga clic en **Siguiente**, vuelva a hacer clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
- 6 Si una CA intermedia firmó el certificado del servidor, importe todos los certificados intermedios a la cadena de certificados en el almacén de certificados del equipo local Windows.
 - a Diríjase a la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados**.
 - b Repita del paso 3 al 6 para cada certificado intermedio que se deba importar.

Pasos siguientes

Configure la clave de registro apropiada con la huella digital del certificado. Consulte [Configurar la huella digital de certificado en el Registro de Windows](#).

Configurar la huella digital de certificado en el Registro de Windows

Para permitir que HTML Access Agent use un certificado firmado por una entidad de certificación que se importó en el almacén de certificados de Windows, debe configurar la huella digital de certificado en una clave del Registro de Windows. Debe realizar este paso en cada escritorio remoto en el que reemplace el certificado predeterminado por un certificado firmado por una entidad de certificación.

Requisitos previos

Compruebe que el certificado firmado por una entidad de certificación se importó en el almacén de certificados de Windows. Consulte [Importar un certificado para el agente HTML Access al almacén de certificados de Windows](#).

Procedimiento

- 1 En la ventana MMC del escritorio remoto en el que agente HTML Access está instalado, diríjase a la carpeta **Certificados (equipo local) > Personal > Certificados**.
- 2 Haga doble clic en el certificado firmado por una entidad de certificación que importó en el almacén de certificados de Windows.
- 3 En el cuadro de diálogo Certificados, haga clic en la pestaña Detalles, desplácese hacia abajo y seleccione el icono **Huella digital**.
- 4 Copie la huella digital seleccionada en un archivo de texto.

Por ejemplo: 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

Nota Cuando copie la huella digital, no incluya el espacio inicial. Si lo pega accidentalmente con la huella digital en la clave del registro (paso 7), es posible que el certificado no se configure correctamente. Este problema se puede producir aunque el espacio inicial no se muestre en el cuadro de texto del valor del registro.

- 5 Inicie el editor del Registro de Windows en el escritorio en el que HTML Access Agent está instalado.
- 6 Diríjase a la clave del registro HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 7 Modifique el valor SslHash y pegue la huella digital de certificado en el cuadro de texto.
- 8 Reinicie Windows.

Cuando un usuario se conecte a un escritorio remoto a través de HTML Access, el agente HTML Access presenta el certificado firmado en el navegador del usuario.

Configurar los agentes HTML Access para usar conjuntos de cifrado específicos

Puede configurar el agente HTML Access para que use conjuntos de cifrado específicos en lugar de los predeterminados.

De forma predeterminada, el agente HTML Access necesita que las conexiones SSL entrantes usen una encriptación basada en ciertos cifrados para proporcionar una buena protección ante la falsificación y el espionaje telemático de la red. Puede configurar una lista alternativa de cifrados para que use el agente HTML Access. El conjunto de cifrados aceptados se expresa en formato OpenSSL, que se describe en <https://www.openssl.org/docs/manmaster/man1/ciphers.html>.

Procedimiento

- 1 Inicie el editor del Registro de Windows en el escritorio en el que HTML Access Agent está instalado.
- 2 Diríjase a la clave del registro HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config.
- 3 Agregue un nuevo valor de cadena (REG_SZ), SslCiphers, y copie la lista de cifrados en formato OpenSSL en el cuadro de texto.
- 4 Reinicie el servicio VMware Blast para que se apliquen los cambios.

En el sistema operativo invitado Windows, el servicio del agente HTML Access se denomina VMware Blast.

Para volver a usar la lista de cifrados predeterminados, elimine el valor SslCiphers y reinicie el servicio VMware Blast. No elimine simplemente los datos del valor, ya que el agente HTML Access tratará entonces a todos los cifrados como no aceptables, según la definición del formato de la lista de cifrados OpenSSL.

Cuando se inicia el agente HTML Access, este escribe la definición del cifrado en el archivo de registro del servicio VMware Blast. Puede saber la lista de cifrados predeterminada actual si revisa los registros cuando se inicia el servicio VMware Blast sin el valor SslCiphers configurado en el Registro de Windows.

La definición del cifrado predeterminado del agente HTML Access puede cambiar de una versión a la siguiente para ofrecer una mayor seguridad.

Configurar iOS para usar certificados firmados por una entidad de certificación

Para utilizar HTML Access en dispositivos iOS, debe instalar certificados SSL que estén firmados por una entidad de certificación (CA) en lugar de los certificados SSL predeterminados, generados por Horizon Connection Server o HTML Access Agent.

Para obtener más instrucciones, consulte el artículo sobre cómo configurar Horizon Client para iOS para que confíe en certificados intermedios y raíces en el documento *Instalación de Horizon 7*.

Usar un certificado firmado por una CA con Unified Access Gateway

Si utiliza un dispositivo de Unified Access Gateway en lugar de un servidor de conexión o un servidor de seguridad, debe instalar un certificado firmado por una CA que tiene un nombre alternativo del firmante (SAN) configurado.

Si usa un certificado firmado por una CA que no tenga ningún SAN configurado o un certificado autofirmado, los usuarios reciben un error "Su conexión no es privada" y no se pueden conectar con HTML Access.

Nota Si usa una instancia del servidor de conexión o del servidor de seguridad, los usuarios pueden seguir conectados haciendo clic en el vínculo `Proceed to dirección-ip (unsafe)`.

Para obtener más información sobre la instalación y la configuración de certificados para Horizon 7, consulte el documento *Instalación de Horizon 7*. Para obtener más información sobre cómo configurar que los agentes de HTML Access usen los certificados TLS, consulte [Configurar los agentes HTML Access para usar nuevos certificados TLS](#).

Actualizar el software de HTML Access

Para la mayoría de las versiones de HTML Access, actualizar implica simplemente actualizar Horizon Connection Server y Horizon Agent.

Cuando actualice HTML Access, compruebe que la versión correspondiente de Horizon Connection Server esté instalada en todas las instancias de un grupo replicado.

Cuando actualice el servidor de conexión, HTML Access se instala o se actualiza de forma automática.

Nota Para comprobar si el componente HTML Access está instalado, puede abrir el applet Desinstalar un programa del sistema operativo Windows y buscar HTML Access en la lista.

Desinstalar el componente HTML Access desde el servidor de conexión

Para eliminar el componente HTML Access, utilice el mismo método que para desinstalar cualquier otro software de Windows.

Procedimiento

- 1 En la instancia del servidor de conexión en los que esté instalado HTML Access, abra el applet Desinstalar un programa que proporciona el Panel de control de Windows.
- 2 Seleccione **VMware Horizon 7 HTML Access** y haga clic en **Desinstalar**.
- 3 (opcional) En el firewall de Windows de ese host, compruebe que el puerto TCP 8443 ya no permita el tráfico entrante.

Pasos siguientes

No permita el tráfico entrante al puerto TCP 8443 en el firewall de Windows de cualquier servidor de seguridad conectado. En los firewalls de terceros, cambie la reglas para no permitir tráfico entrante al puerto TCP 8443 de todos los servidores de seguridad conectados y esta instancia del servidor de conexión (si procede).

Configurar el uso compartido de datos de Horizon Client

Si el administrador de Horizon decidió participar en el programa de mejora de la experiencia de cliente, VMware recopila y recibe datos anónimos de los sistemas cliente para priorizar la compatibilidad entre el software y el hardware. Puede configurar si desea compartir información en el sistema cliente habilitando o deshabilitando una opción en Horizon Client.

El uso compartido de datos de Horizon Client está habilitado de forma predeterminada en el navegador web que se usa para la sesión cliente HTML Access. No puede cambiar la opción de uso compartido de datos de Horizon Client después de conectarse a un servidor.

Procedimiento

- 1 Haga clic en **Configuración** (icono de rueda dentada) en la página de inicio de sesión en VMware Horizon.
- 2 Para habilitar o deshabilitar el uso compartido de datos de Horizon Client, active o desactive la opción **Permitir el uso compartido de datos**.

Datos recopilados por VMware

Si su empresa participa en el programa de mejora de la experiencia de cliente y el uso compartido de datos cliente está habilitado, VMware recopila los datos sobre el sistema cliente.

VMware recopila datos de los clientes para priorizar la compatibilidad entre el hardware y el software. Si un administrador de Horizon decidió participar en el programa de mejora de la experiencia de cliente, VMware recopila datos anónimos acerca de la implementación para mejorar la respuesta de VMware a los requisitos del cliente. No se recopila ningún dato que identifique a su organización. La información de los clientes se envía primero al servidor de conexión y después a VMware, junto con los datos de los servidores, de los grupos de escritorios y de los escritorios remotos.

Para participar en el programa de mejora de la experiencia de cliente de VMware, el administrador que instala el servidor de conexión puede registrarse mientras se ejecuta el asistente de instalación del servidor de conexión o, también, el administrador puede configurar esta opción en Horizon Administrator después de la instalación.

Tabla 1-2. Datos de los clientes recopilados para el programa de mejora de la experiencia de cliente

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Compañía que desarrolló la aplicación	<proveedor_cliente>	No	VMware
Nombre de producto	<producto_cliente>	No	VMware Horizon HTML Access
Versión del producto del cliente	<versión_cliente>	No	4.10.0-número_compilación
Arquitectura binaria del cliente	<arquitectura_cliente>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ navegador ■ arm
Arquitectura nativa del navegador	<arquitectura_navegador>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81 (para utilizarse con Chrome de Android)
Cadena agente del usuario del navegador	<agente_usuario_navegador>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, like Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Cadena de la versión interna del navegador	<versión_navegador>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ 7.0.3 (para Safari), ■ 44.0 (para Firefox) ■ 13.10586 (para Edge)

Tabla 1-2. Datos de los clientes recopilados para el programa de mejora de la experiencia de cliente (Continuación)

Descripción	Nombre del campo	¿Es anónimo este campo?	Valor de ejemplo
Implementación del núcleo del navegador	<núcleo_navegador>	No	Los ejemplos incluyen los siguientes valores: <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Si los navegadores se ejecutan en un dispositivo portátil	<navegador_en_dispositivo portátil>	No	true

Configurar HTML Access para usuarios finales

2

Es posible cambiar la apariencia de la página web que los usuarios finales verán cuando introduzcan la URL de HTML Access. También puede establecer directivas de grupo que controlen la calidad de la imagen y los puertos utilizados, entre otras opciones.

Este capítulo incluye los siguientes temas:

- [Configurar la página del portal web de VMware Horizon para los usuarios finales](#)
- [Utilizar URI para configurar clientes web de HTML Access](#)
- [Configuración de las directivas de grupo de HTML Access](#)

Configurar la página del portal web de VMware Horizon para los usuarios finales

Puede configurar esta página web para que muestre u oculte el icono para descargar Horizon Client o el icono para conectarse a un escritorio remoto a través de HTML Access. También puede configurar otros vínculos a esta página.

De forma predeterminada, este portal web muestra un icono para descargar e instalar Horizon Client nativo y otro icono para conectarse a través de HTML Access. El vínculo de descarga utilizado se determina a partir de los valores predeterminados definidos en el archivo `portal-links-html-access.properties`.

En algunos casos, sin embargo, es posible que desee que los vínculos dirijan a un servidor web interno o que quiera tener disponibles versiones específicas del cliente en su propio servidor. Puede reconfigurar la página del portal para que dirija a otra URL de descarga modificando el contenido del archivo `portal-links-html-access.properties`. Si ese archivo no está disponible o está vacío y existe el archivo `oslinks.properties`, el archivo `oslinks.properties` se utiliza para determinar el valor de vínculo del archivo de instalador.

El archivo `oslinks.properties` se instala en la carpeta *directorio-de-instalación\VMware\VMware View\Server\broker\webapps\portal\WEB-INF*. Si falta este archivo durante la sesión de HTML Access, el vínculo de descarga redirigirá a los usuarios de forma predeterminada a <https://www.vmware.com/go/viewclients>. El archivo contiene los siguientes valores predeterminados:

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Puede crear vínculos de instalador para sistemas operativos de cliente específicos en el archivo `portal-links-html-access.properties` u `oslinks.properties`. Por ejemplo, si se dirige a la página del portal desde un sistema Mac OS X, aparece el vínculo del instalador Mac OS X nativo. En el caso de los clientes Windows o Linux, puede crear vínculos independientes para instaladores de 32 o 64 bits.

Importante Si actualiza desde el servidor de conexión de View 5.x o una versión anterior y no cuenta con el componente HTML Access instalado y, además, editó previamente la página del portal para que descargue Horizon Client en su propio servidor, estas personalizaciones se podrían ocultar después de instalar el servidor de conexión 6.0 o una versión posterior. Con Horizon 6 o una versión posterior, el componente HTML Access se instala automáticamente durante una actualización del servidor de conexión.

Si ya instaló el componente HTML Access por separado para Horizon 7 5.x, se conservan todas las personalizaciones que realizó para la página web. Si no cuenta con el componente HTML Access instalado, se ocultan todas las personalizaciones. Las personalizaciones de las versiones anteriores se encuentran en el archivo `portal-links.properties`, que ya no se utiliza.

Procedimiento

- 1 En el host del servidor de conexión, abra el archivo `portal-links-html-access.properties` con un editor de texto.

La ubicación de este archivo es `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. Para los sistemas operativos Windows Server 2008, el directorio `CommonAppDataFolder` es `C:\ProgramData`. Para que aparezca la carpeta `C:\ProgramData` en el Explorador de Windows, debe usar el cuadro de diálogo Opciones de carpeta para mostrar las carpetas ocultas.

Si no existe el archivo `portal-links-html-access.properties` y existe el archivo `oslinks.properties`, abra el archivo `<directorio-de-instalación>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` para modificar las URL para usar los archivos de instalador específicos de descarga.

Nota Las personalizaciones de Horizon 7.5.x y versiones anteriores se encuentran en el archivo `portal-links.properties`, que está en el mismo directorio `CommonAppDataFolder\VMware\VDM\portal\` que el archivo `portal-links-html-access.properties`.

2 Edite las propiedades de configuración para establecerlas correctamente.

De forma predeterminada, tanto el icono del instalador como el icono de HTML Access están habilitados y un vínculo lleva a la página de descargas del cliente en el sitio web de VMware. Para deshabilitar un icono, lo que supone que se elimine de la página web, configure la propiedad como `false`.

Nota El archivo `oslinks.properties` solo se puede utilizar para configurar los vínculos en los archivos de instalador específicos. No admite las otras opciones enumeradas debajo.

Opción	Configuración de propiedad
Deshabilitar HTML Access	<p><code>enable.webclient=false</code></p> <p>Si esta opción aparece como <code>false</code> pero <code>enable.download</code> está configurada como <code>true</code>, se envía al usuario a una página web para que se descargue el instalador de Horizon Client nativo. Si ambas opciones aparecen como <code>false</code>, el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".</p>
Deshabilitar la descarga de Horizon Client	<p><code>enable.download=false</code></p> <p>Si esta opción aparece como <code>false</code> pero la opción <code>enable.webclient</code> está configurada como <code>true</code>, se envía al usuario a la página web de inicio de sesión de HTML Access. Si ambas opciones se han establecido como <code>False</code>, el usuario verá el siguiente mensaje: "Póngase en contacto con el administrador local para obtener instrucciones sobre cómo acceder a este servidor de conexión".</p>
Cambiar la URL de la página web para descargar Horizon Client	<p><code>link.download=https://url_del_servidor_web</code></p> <p>Use esta propiedad si piensa crear su propia página web.</p>

Opción	Configuración de propiedad
Crear vínculos para instaladores específicos	<p>Los siguientes ejemplos muestran URL completas, pero puede usar URL relativas si coloca los archivos del instalador en el directorio downloads que se encuentra en el directorio C:\Program Files\VMware\VMware View\Server\broker\webapps\ del servidor de conexión, como se describe en el siguiente paso.</p> <ul style="list-style-type: none"> ■ Vínculo general para descargar el instalador: <div>link.download=https://server/downloads</div> ■ Instalador de Windows de 32 bits: <div>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</div> ■ Instalador para Windows de 64 bits: <div>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</div> ■ Instalador de Windows Phone: <div>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</div> ■ Instalador de Linux de 32 bits: <div>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</div> ■ Instalador de Linux de 64 bits: <div>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</div> ■ Instalador para Mac OS X: <div>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</div> ■ Instalador para iOS: <div>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</div> ■ Instalador para Android: <div>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</div> ■ Instalador de Chrome OS: <div>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</div>
Cambiar la URL para el vínculo Ayuda en la página de inicio de sesión	<p>link.help</p> <p>De forma predeterminada, este vínculo lleva a un sistema de ayuda alojado en el sitio web de VMware. El vínculo Ayuda aparece en la parte inferior de la página</p>

Opción	Configuración de propiedad
	de inicio de sesión.

- 3 Para hacer que los usuarios se descarguen instaladores de una ubicación diferente al sitio web de VMware, ponga los archivos del instalador en el servidor HTTP correspondiente.

Esta ubicación debe corresponderse con las URL que especificó en el archivo `portal-links-html-access.properties` o el archivo `oslinks.properties` durante el paso anterior. Por ejemplo, para situar los archivos en un directorio `downloads` en el host del servidor de conexión, use la siguiente ruta:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Los vínculos a los archivos del instalador pueden usar URL relativas con el formato `/downloads/nombre_archivo_instalador_de_cliente`.

- 4 Reinicie el servicio del componente web de Horizon.

Utilizar URI para configurar clientes web de HTML Access

Con los identificadores uniformes de recursos (URI), puede crear un correo electrónico o una página web con vínculos en los que los usuarios finales hacen clic para iniciar HTML Access Web client, conectarse a Horizon Connection Server y abrir una aplicación o un escritorio específicos con opciones de configuración concretas.

Para simplificar el proceso de conexión a una aplicación o un escritorio remotos, cree vínculos web o de correo electrónico para los usuarios finales. Para ello, deberá crear URI que ofrezcan toda la información (o parte de ella) que se indica a continuación para que los usuarios finales no tengan que proporcionarla:

- Horizon Connection Server dirección
- Número de puerto para Horizon Connection Server
- Nombre de usuario de Active Directory
- Nombre de usuario de RSA SecurID o RADIUS (si es distinto al nombre de usuario de Active Directory)
- Nombre de dominio
- Nombre del escritorio o de la aplicación para mostrar
- Acciones (como navegar, restablecer e iniciar o cerrar sesión)

Sintaxis para crear URI para HTML Access

La sintaxis incluye una parte de ruta para especificar el servidor y, de forma opcional, una consulta para especificar un usuario, escritorio o aplicación, así como opciones de configuración o acciones.

Especificación de URI

Use la siguiente sintaxis para crear los URI destinados a iniciar los clientes web de HTML Access:

```
https://authority-part[/?query-part]
```

authority-part

Especifica la dirección del servidor y, de manera opcional, un número de puerto no predeterminado. Los nombres de servidor deben adaptarse a la sintaxis de DNS.

Para especificar un número de puerto, utilice la siguiente sintaxis:

```
server-address:port-number
```

query-part

Especifica las opciones de configuración que se van a utilizar o las acciones que se van a realizar. Las consultas no distinguen entre mayúsculas y minúsculas. Para utilizar varias consultas, utilice el signo et (&) entre ellas. Si se produce un conflicto entre ellas, se utilizará la última consulta de la lista. Utilice la siguiente sintaxis:

```
query1=value1[&query2=value2...]
```

Tenga en cuenta las siguientes instrucciones al crear la parte de la consulta:

- Si no usa al menos una de las consultas admitidas, se mostrará la página del portal web de VMware Horizon predeterminada.
- En la parte de la consulta, algunos caracteres especiales no son compatibles y debe usar el formato de codificación URL de la siguiente manera: para el signo almohadilla (#) use %23, para el signo porcentaje (%) use %25, para el signo et (&) use %26, para el signo arroba (@) use %40 y para la barra diagonal inversa (\) use %5C.

Para obtener más información sobre la codificación URL, diríjase a http://www.w3schools.com/tags/ref_urlencode.asp.

- En la parte de la consulta, se debe codificar primero los caracteres que no sean ASCII según UTF-8 [STD63]. A continuación, cada octeto de la secuencia UTF-8 correspondiente se debe codificar con porcentaje para representarse como caracteres URI.

Para obtener información sobre la codificación de caracteres ASCII, consulte la referencia de codificación de URL de <http://www.utf8-chartable.de/>.

Consultas admitidas

En este tema, se incluyen las consultas admitidas para HTML Access Web client. Si crea URI para varios tipos de clientes (por ejemplo, clientes móviles y de escritorio), consulte el documento *Uso de VMware Horizon Client* correspondiente a cada tipo de sistema cliente.

action

Tabla 2-1. Valores que se pueden utilizar con la consulta action

Valor	Descripción
browse	Muestra una lista de las aplicaciones y los escritorios disponibles y alojados en el servidor especificado. No tendrá que especificar un escritorio ni una aplicación al utilizar esta acción.
start-session	Inicia la aplicación o el escritorio especificados. Si no se proporciona ninguna consulta action y se facilita el nombre de la aplicación o el escritorio, start-session es la acción predeterminada.
reset	Cierra y reinicia el escritorio especificado. Se pierden los datos que no se hayan guardado. La acción de reiniciar un escritorio remoto es equivalente a pulsar el botón Reiniciar en un equipo físico. Esta acción no es válida para una aplicación.
logoff	Cierra la sesión del usuario en el sistema operativo invitado del escritorio remoto. Esta acción no es válida para una aplicación.
restart	Cierra y vuelve a iniciar el escritorio principal una vez que el usuario confirma la solicitud de operación de reinicio. Esta acción no es válida para una aplicación.

applicationId

El nombre de la aplicación para mostrar. El nombre para mostrar es el que se especifica en Horizon Administrator al crear el grupo de aplicaciones. Si el nombre para mostrar contiene un espacio, el navegador usa %20 para representar el espacio.

args

Especifica los argumentos de la línea de comandos que se agregarán al iniciar una aplicación remota. Utilice la sintaxis `args=value`, en el que *value* es una cadena. Utilice la codificación con porcentajes para los siguientes caracteres:

- Para los dos puntos (:), utilice %3A.
- Para una barra diagonal inversa (\), utilice %5C.
- Para un espacio (), utilice %20.
- Para unas comillas dobles ("), use %22.

Por ejemplo, para especificar el nombre de archivo "My new file.txt" para la aplicación Notepad++, utilice %22My%20new%20file.txt%22.

desktopId	El nombre del escritorio para mostrar. El nombre para mostrar es el que se especifica en View Administrator al crear el grupo de escritorios. Si el nombre para mostrar contiene un espacio, el navegador usa %20 para representar el espacio.
domainName	El nombre de dominio NETBIOS asociado al usuario que se conecta a la aplicación o al escritorio remotos. Por ejemplo, use mycompany en lugar de mycompany.com.
tokenUserName	El nombre de usuario RSA o RADIUS. Utilice esta consulta solo si el nombre de usuario de RSA o RADIUS es diferente al de Active Directory. Si no especifica esta consulta y se necesita la autenticación RSA o RADIUS, se utilizará el nombre de usuario de Windows.
userName	<p>El usuario de Active Directory que se conecta a la aplicación o al escritorio remotos. El nombre de usuario puede tener uno de los formatos siguientes:</p> <ul style="list-style-type: none"> ■ <i>Nombre de usuario</i> ■ <i>nombre de dominio%5Cnombre de usuario</i> ■ nombre principal de usuario (UPN), es decir, <i>nombre de usuario@nombre de dominio</i>
unauthenticatedAccessEnabled	Si esta opción está establecida como true , la función Acceso sin autenticar está habilitada de forma predeterminada. Se inicia HTML Access Web client y aparece una cuenta de un usuario anónimo. Un ejemplo de sintaxis es unauthenticatedAccessEnabled=true .
unauthenticatedAccessAccount	Establece la cuenta que se debe utilizar si la función Acceso sin autenticar está habilitada. Si la función Acceso sin autenticar está deshabilitada, esta consulta se ignora. Un ejemplo de sintaxis con la cuenta de usuario anonymous1 es unauthenticatedAccessAccount=anonymous1 .

Ejemplos de URI

Es posible crear botones o vínculos de hipertexto con un URI e incluir estos vínculos en un correo electrónico o en una página web. Los usuarios finales pueden hacer clic en estos vínculos para, por ejemplo, abrir una aplicación o un escritorio remotos con las opciones de inicio que especifique.

Ejemplos de sintaxis de URI

Cada ejemplo de URI aparece con una descripción sobre qué es lo que el usuario final ve después de hacer clic en el vínculo del URI. Las consultas no distinguen entre mayúsculas y minúsculas. Por ejemplo, puede usar **domainName** o **domainname**.

1

```
https://horizon.mycompany.com/?domainName=finance&userName=fred
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **fred** y el cuadro de texto **Dominio** se rellena con **finance**. El usuario solo debe proporcionar una contraseña.

2

```
https://horizon.mycompany.com/?userName=finance%5Cfred
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **horizon.mycompany.com**. El usuario solo debe proporcionar una contraseña.

3

```
https://horizon.mycompany.com/?userName=fred@finance
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. En el cuadro de inicio de sesión, el cuadro de texto **Nombre de usuario** se rellena con el nombre **fred@finance**. El usuario solo debe proporcionar una contraseña.

4

```
https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente se conecta al escritorio cuyo nombre para mostrar es **Escritorio primario** y el usuario inicia sesión en el sistema operativo cliente.

5

```
https://horizon.mycompany.com/?applicationId=Notepad&action=start-session
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, se inicia la aplicación Bloc de notas.

6

```
https://horizon.mycompany.com:7555/?desktopId=Primary%20Desktop
```

Este URI tiene el mismo efecto que el ejemplo anterior, excepto que usa el puerto 7555 no predeterminado para el servidor de conexión. (El puerto predeterminado es 443). Dado que se proporciona un identificador del escritorio, este se inicia aunque la acción `start-session` no se incluya en el URI.

7

```
https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop
```

El URI especifica tanto una aplicación como un escritorio. Cuando especifica una aplicación y un escritorio, solo se inicia este último.

8

```
https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset
```


El cliente web HTML Access se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para restablecer el Escritorio primario.

Nota Esta acción solo está disponible si el administrador de Horizon permite a los usuarios finales restablecer sus equipos.

9

```
https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22
```

Abre Notepad++ en el servidor `horizon.mycompany.com` y envía el argumento `My new file.txt` al comando que inicia la aplicación. El nombre del archivo aparece entre comillas dobles porque contiene espacios.

10

```
https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt
```

Abre Notepad++ 12 en el servidor `horizon.mycompany.com` y envía el argumento `a.txt b.txt` al comando que inicia la aplicación. Dado que los argumentos no están entre comillas dobles, un espacio separa los nombres de los archivos y ambos archivos se abren de forma independiente en Notepad++.

Nota Las aplicaciones pueden utilizar los argumentos de la línea de comandos de forma diferente. Por ejemplo, si envía el argumento `a.txt b.txt` a WordPad, este último solo abrirá un archivo, `a.txt`.

11

```
https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com`. El cuadro de inicio de sesión solicita un nombre de usuario, de dominio y una contraseña. Tras iniciar sesión correctamente, el cliente muestra un cuadro de diálogo que le solicita al usuario que confirme la operación para reiniciar el Escritorio primario.

Nota Esta acción solo está disponible si el administrador de Horizon permite a los usuarios finales reiniciar sus equipos.

12

```
https://horizon.mycompany.com/?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1
```

HTML Access Web client se inicia y se conecta al servidor `horizon.mycompany.com` mediante la cuenta **anonymous_user1**.

Ejemplos de códigos HTML

Si lo desea, puede utilizar los URI para hacer que los botones y los vínculos de hipertexto se incluyan en correos electrónicos o en páginas web. Los siguientes ejemplos muestran cómo usar el URI en el primer ejemplo de URI para codificar un vínculo de hipertexto que aparece como **Test Link** y un botón que aparece como **TestButton**.

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

Configuración de las directivas de grupo de HTML Access

HTML Access usa el protocolo VMware Blast. Puede configurar las directivas de grupo de HTML Access al establecer las directivas de grupo del protocolo VMware Blast.

Para obtener más información, consulte "Configurar directivas para grupos de escritorios y aplicaciones" y "Configuración de la directiva VMware Blast" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Administrar las conexiones de las aplicaciones publicadas y los escritorios remotos

3

Los usuarios finales pueden utilizar Horizon Client para conectarse a un servidor, iniciar o cerrar sesión en escritorios remotos y utilizar aplicaciones publicadas. Para solucionar problemas, los usuarios finales también pueden restablecer las aplicaciones publicadas y los escritorios remotos.

Este capítulo incluye los siguientes temas:

- [Conectarse a una aplicación publicada o a un escritorio remoto](#)
- [Confiar en un certificado raíz autofirmado](#)
- [Conectarse a un servidor en el modo Workspace ONE](#)
- [Utilizar la función Acceso sin autenticar para conectarse a aplicaciones publicadas](#)
- [Establecer la zona horaria](#)
- [Permitir la decodificación H.264](#)
- [Cerrar sesión o desconectarse](#)

Conectarse a una aplicación publicada o a un escritorio remoto

Use las credenciales de Active Directory para conectarse a las aplicaciones publicadas y los escritorios remotos para los que tenga autorización.

Requisitos previos

- Obtenga las credenciales de inicio de sesión, como el nombre de usuario y la contraseña de Active Directory, el nombre de usuario y el código de acceso de RSA SecurID o el nombre de usuario y el código de acceso de la autenticación RADIUS.
- Obtenga el nombre de dominio NETBIOS para iniciar sesión. Por ejemplo, puede usar `mycompany` en lugar de `mycompany.com`.

Procedimiento

- 1 Abra el navegador e introduzca la URL de la instancia del servidor de conexión.

En la URL, use **https** y el nombre de dominio completo, por ejemplo:
`https://horizon.company.com`.

Las conexiones al servidor de conexión siempre usan SSL. El puerto predeterminado para las conexiones SSL es 443. Si el servidor de conexión no está configurado para utilizar el puerto predeterminado, utilice el formato que se muestra en este ejemplo: **horizon.company.com:1443**.

Aparece el portal web de VMware Horizon. De forma predeterminada, esta página muestra un icono para descargar e instalar Horizon Client nativo y otro icono para conectarse a través de HTML Access.

- 2 (Opcional) Seleccione la casilla de verificación **Hacer clic aquí para omitir esta pantalla y usar siempre HTML Access**.

Su selección se almacena en el almacenamiento local del navegador que esté actualmente en uso. La próxima vez que introduzca la URL de la instancia del servidor de conexión con el mismo tipo de navegador y el mismo equipo cliente, se le dirigirá directamente a la pantalla de inicio de sesión. Si utiliza un tipo de navegador diferente en el mismo equipo cliente o si utiliza el mismo tipo de navegador en un equipo cliente diferente, aparece el portal web de VMware Horizon. Borre la caché del navegador si desea que el portal web de VMware Horizon aparezca.

- 3 Haga clic en el icono **VMware Horizon HTML Access**.

- 4 En el cuadro de diálogo de inicio de sesión, si se le solicita las credenciales RSA SecurID o las credenciales de la autenticación RADIUS, introduzca el nombre de usuario y el código de acceso y, a continuación, haga clic en **Iniciar sesión**.

El código de acceso puede incluir tanto un PIN como el número generado en el token.

- 5 Si se le solicita por segunda vez las credenciales RSA SecurID o las credenciales de autenticación RADIUS, introduzca el siguiente número generado en el token.

No introduzca su PIN ni tampoco el mismo número generado que ya introdujo anteriormente. Si es necesario, espere hasta que se genere un número nuevo.

Este paso solo se solicita cuando introduce de forma errónea el primer código de acceso o cuando las opciones de configuración cambian en el servidor RSA.

- 6 En el cuadro de diálogo de inicio de sesión, introduzca sus credenciales de inicio de sesión.
 - a En el cuadro de texto Nombre de usuario, introduzca su nombre de usuario válido de Active Directory con el formato *nombre de usuario, dominio\nombre de usuario*, o bien *nombre de usuario@dominio*.

Si el cuadro de texto Dominio está deshabilitado, debe utilizar el formato *dominio\nombre de usuario* o bien *nombre de usuario@dominio*.
 - b Introduzca la contraseña.
 - c (Opcional) Si el cuadro de texto Dominio está habilitado, seleccione un nombre de dominio, si aún no se rellenó correctamente.

Nota Para cancelar el proceso de inicio de sesión, haga clic en **Cancelar** antes de que dicho proceso finalice.

- 7 (opcional) Si necesita establecer manualmente la zona horaria que se utiliza en la aplicación publicada o el escritorio remoto, haga clic en la barra de herramientas **Configuración** que se encuentra en la esquina superior derecha del escritorio y la pantalla para seleccionar aplicaciones. Desactive la opción **Establecer la zona horaria automáticamente** y seleccione una de las zonas horarias del menú desplegable. Consulte [Establecer la zona horaria](#).
- 8 (opcional) En la pantalla para seleccionar aplicaciones y escritorios, antes de seleccionar el elemento al que desea acceder, haga clic en la estrella gris que aparece dentro del icono de la aplicación publicada o del escritorio para marcarlos como favoritos.

El icono de la estrella cambia de gris a amarillo. La próxima vez que inicie sesión, puede hacer clic en el icono de la estrella situado en la parte superior derecha de la ventana del navegador para mostrar únicamente los favoritos.
- 9 Haga clic en el icono de la aplicación publicada o el escritorio remoto a los que desea acceder.

La aplicación publicada o el escritorio remoto se muestran en el navegador. También está disponible una barra lateral de navegación. Puede hacer clic en la pestaña situada en el lado izquierdo de la ventana del navegador para mostrar la barra lateral. Puede usar esta barra lateral para acceder a otras aplicaciones publicadas y otros escritorios remotos, mostrar la ventana Configuración, copiar y pegar textos, entre otras acciones.

Pasos siguientes

Si, poco después de conectarse a un escritorio o una aplicación publicada, sufre una desconexión y aparece una solicitud que le pide que haga clic en un vínculo para aceptar el certificado de seguridad, puede seleccionar si desea confiar en ese certificado. Consulte [Confiar en un certificado raíz autofirmado](#).

Confiar en un certificado raíz autofirmado

A veces, al conectarse a una aplicación publicada o un escritorio remoto por primera vez, el navegador puede solicitarle que acepte el certificado autofirmado que la máquina remota usa. Debe confiar en el certificado antes de poder conectarse al escritorio remoto o a la aplicación publicada.

La mayoría de los navegadores le ofrecen la opción de confiar siempre en el certificado autofirmado. Si confía en el certificado siempre, debe verificar el certificado cada vez que reinicie el navegador. Si usa un navegador Safari, debe confiar siempre en el certificado de seguridad para establecer la conexión.

Procedimiento

- 1 Si el navegador presenta una advertencia sobre un certificado que no es de confianza o sobre una conexión que no es privada, examine el certificado para comprobar que coincide con el que usa su empresa.

Es posible que necesite ponerse en contacto con el administrador del sistema para obtener más ayuda. Por ejemplo, en Chrome, es necesario que realice el siguiente procedimiento.

- a Haga clic en el icono de bloqueo en la barra de direcciones.
- b Haga clic en el vínculo **Información del certificado**.
- c Verifique que el certificado coincida con el que usa su empresa.

Es posible que necesite ponerse en contacto con el administrador del sistema para obtener más ayuda.

- 2 Acepte el certificado de seguridad.

Cada navegador tiene sus propias solicitudes para aceptar un certificado o confiar siempre en él. Por ejemplo, en un navegador Chrome, puede hacer clic en el vínculo **Opciones avanzadas** de la página del navegador y hacer clic en **Acceder a nombre del servidor (sitio no seguro)**.

En un navegador Safari, use el siguiente procedimiento para confiar siempre en el certificado.

- a Haga clic en el botón **Mostrar certificado** cuando aparezca el cuadro de diálogo de un certificado que no es de confianza.
- b Seleccione la casilla **Confiar siempre** y haga clic en **Continuar**.
- c Cuando se le solicite, proporcione su contraseña y haga clic en **Actualizar ajustes**.

Se inicia el escritorio remoto o la aplicación publicada.

Conectarse a un servidor en el modo Workspace ONE

A partir de la versión 7.2 de Horizon 7, un administrador de Horizon podrá habilitar el modo Workspace ONE en una instancia del servidor de conexión.

Cuando se habilita el modo Workspace ONE, solo podrá conectarse al servidor a través del portal web de Workspace ONE. Se le redirecciona al portal web de Workspace ONE si intenta conectarse al servidor a través de HTML Access. Después de conectarse al servidor a través del portal web de Workspace ONE, solo podrá iniciar aplicaciones publicadas y escritorios remotos a través del portal web de Workspace ONE.

La barra lateral no muestra todas las autorizaciones cuando el modo Workspace ONE está habilitado. Solo muestra las aplicaciones publicadas y el escritorio en ejecución.

Es posible que se produzcan los siguientes problemas cuando está habilitado el modo de Workspace ONE.

- No se puede conectar al servidor a través de HTML Access. Es posible que no pueda comunicarse con el servidor o que vea un mensaje que indica que el servidor espera recibir sus credenciales de inicio de sesión desde otra aplicación o servidor.
- Después de iniciar una aplicación publicada o un escritorio remoto a través del portal web de Workspace ONE, no podrá ver ni iniciar las aplicaciones publicadas o los escritorios remotos en HTML Access.

Utilizar la función Acceso sin autenticar para conectarse a aplicaciones publicadas

Un administrador de Horizon puede utilizar la función Acceso sin autenticar para crear usuarios de acceso sin autenticar y autorizar a dichos usuarios a utilizar las aplicaciones publicadas en una instancia del servidor de conexión. Los usuarios con acceso sin autenticar pueden iniciar sesión en el servidor de forma anónima para conectarse a sus aplicaciones publicadas.

Requisitos previos

- Realice las tareas administrativas descritas en [Preparar el servidor de conexión y los servidores de seguridad](#).
- Configurar usuarios de acceso sin autenticar en la instancia del servidor de conexión. Si desea obtener más información, consulte el tema sobre cómo proporcionar acceso sin autenticar para aplicaciones publicadas en el documento *Administración de Horizon 7*.

Procedimiento

- 1 Para conectarse a la instancia del servidor de conexión en la que tiene acceso sin autenticar a aplicaciones publicadas, abra un navegador y use una de las siguientes sintaxis del URI.

- `https://authority-part?unauthenticatedAccessEnabled=true`
- `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

authority-part especifica la dirección del servidor y, de manera opcional, un número de puerto no predeterminado. Los nombres de servidor deben adaptarse a una sintaxis de DNS. Para especificar un número de puerto, utilice la siguiente sintaxis: *dirección_de_servidor:número_de_puerto*. *anonymous_account* es la cuenta de usuario de Acceso sin autenticar creada para iniciar sesión de forma anónima.

Las conexiones al servidor de conexión siempre usan TLS. El puerto predeterminado para las conexiones TLS es 443. Si el servidor de conexión no está configurado para utilizar el puerto predeterminado, utilice el formato que se muestra en este ejemplo: **horizon.company.com:1443**.

- 2 (opcional) Si no se especifica la consulta `unauthenticatedAccessAccount`, seleccione una cuenta de usuario de Acceso sin autenticar en el menú desplegable de **Cuenta de usuario**, si es necesario, y haga clic en **Enviar**.

Si solo una cuenta de usuario de Acceso sin autenticar está disponible, dicha cuenta se selecciona de forma predeterminada.

Se mostrará la ventana de selección de aplicaciones.

- 3 Haga clic en el icono de la aplicación publicada a la que desea acceder.

La aplicación publicada aparece en el navegador. También está disponible una barra lateral de navegación. Puede hacer clic en la pestaña situada en el lado izquierdo del navegador para mostrar la barra lateral. Puede usar esta barra lateral para acceder a otras aplicaciones publicadas, mostrar la ventana **Configuración**, copiar y pegar textos, entre otras acciones.

Nota No puede volver a conectarse a las sesiones sin autenticar de aplicaciones. Al desconectarse del cliente, el host RDS cierra la sesión del usuario local de forma automática.

Establecer la zona horaria

La zona horaria que un escritorio remoto o una aplicación publicada usa se configura automáticamente a partir de la zona horaria del sistema local.

Cuando use el cliente HTML Access, si la zona horaria no se puede determinar correctamente debido a algunas directivas de horario de verano, es posible que tenga que establecer la zona horaria de forma manual.

Para establecer la información de zona horaria correcta que se debe utilizar antes de conectarse a una aplicación publicada o un escritorio remoto, haga clic en el botón de la barra de herramientas **Configuración** que se encuentra en la esquina superior derecha de la ventana de selección de aplicaciones y el escritorio. Desactive la opción **Establecer la zona horaria automáticamente** en la ventana **Configuración** y seleccione una de las zonas horarias del menú desplegable.

El valor que seleccione se guardará como su zona horaria preferida al conectarse a una aplicación publicada o a un escritorio remoto.

Si ya está conectado a una aplicación publicada o a un escritorio remoto, vuelva a la pantalla de selección de aplicaciones y el escritorio para cambiar la configuración de zona horaria actual.

La opción **Establecer la zona horaria automáticamente** no está disponible en la ventana **Configuración** a la que se puede acceder desde la barra lateral.

Nota Cuando utilice el navegador Chrome en un dispositivo Android, si se le asigna el valor `true` a la opción **Establecer la zona horaria automáticamente** y cambia la zona horaria del sistema Android, la zona horaria que estableció no se sincronizará automáticamente con el escritorio remoto. Este problema es una limitación de Chrome en el sistema Android. Debe reiniciar el dispositivo Android y el navegador Chrome para sincronizar la zona horaria seleccionada.

Permitir la decodificación H.264

Si utiliza un navegador Chrome, puede permitir la decodificación H.264 en el cliente para las sesiones de aplicaciones publicadas y de escritorios remotos.

Cuando permite la decodificación H.264, el cliente HTML Access usa la decodificación H.264 si el agente la admite. Si el agente no admite la decodificación H.264, el cliente HTML Access usa la decodificación JPEG/PNG.

Si está conectado a una aplicación publicada o un escritorio remoto, puede permitir la decodificación H.264 al activar la opción **Permitir la decodificación H.264** en la ventana **Configuración**, que se encuentra en la barra lateral. Debe desconectarse y volver a conectarse a la aplicación publicada o al escritorio remoto para que se aplique la nueva configuración.

Si no está conectado a una aplicación publicada o a un escritorio remoto, puede hacer clic en el botón de la barra de herramientas **Configuración**, situado en la esquina superior derecha de la ventana de selección de aplicaciones y escritorios, y activar la opción **Permitir la decodificación H.264** en la ventana **Configuración**. Se aplicará la nueva configuración en todas las sesiones que se conecten después de realizar los cambios.

Cerrar sesión o desconectarse

Si se desconecta de un escritorio remoto sin cerrar sesión, las aplicaciones de dicho escritorio pueden permanecer abiertas. También puede desconectarse de un servidor y dejar las aplicaciones publicadas ejecutándose.

Procedimiento

- Cerrar sesión en el servidor y desconectarse desde el escritorio remoto (pero sin cerrar sesión en él) o salir de la aplicación publicada en el host.

Opción	Acción
En la ventana para seleccionar la aplicación y el escritorio, antes de conectarse a una aplicación publicada o escritorio remoto	Haga clic en el botón Cerrar sesión de la barra de herramientas situado en la esquina superior derecha de la ventana.
En la barra lateral, cuando se conecta a una aplicación publicada o escritorio remoto	Haga clic en el botón Cerrar sesión de la barra de herramientas situado en la parte superior de la barra lateral.

- Cerrar una aplicación publicada

Opción	Acción
Desde la aplicación publicada	Salga de la aplicación publicada con el procedimiento habitual, por ejemplo, haciendo clic en el botón X (Cerrar) en la esquina de la ventana de la aplicación publicada.
En la barra lateral	Haga clic en la X que aparece junto al nombre de la aplicación publicada en la lista En ejecución de la barra lateral.

- Cerrar sesión o desconectarse desde un escritorio remoto.

Opción	Acción
Desde el escritorio remoto	Para cerrar sesión, utilice el menú Inicio de Windows para cerrar sesión.
En la barra lateral	<p>Para cerrar sesión y desconectarse, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio remoto en la lista En ejecución de la barra lateral y seleccione Cerrar sesión. Los archivos que estén abiertos en el escritorio remoto se cierran sin guardar.</p> <p>Para desconectarse sin cerrar sesión, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio remoto en la lista En ejecución y seleccione Cerrar.</p> <p>Nota Un administrador de Horizon puede establecer que el escritorio cierre sesión de forma automática cuando se desconecte. En ese caso, se detendrán todas las aplicaciones abiertas en el escritorio remoto.</p>

Usar un escritorio remoto o una aplicación publicada

4

El cliente proporciona una barra lateral de navegación con botones de la barra de herramientas para que pueda desconectarse fácilmente de una aplicación publicada o un escritorio remoto. También puede hacer clic en uno de los botones para enviar la acción equivalente a la combinación de teclas Ctrl+Alt+Supr.

Este capítulo incluye los siguientes temas:

- [Matriz de compatibilidad de funciones](#)
- [Utilizar la barra lateral](#)
- [Resolución de pantalla y monitores](#)
- [Usar el modo de pantalla completa](#)
- [Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos](#)
- [Usar la función Session Collaboration](#)
- [Copiar y pegar texto](#)
- [Transferir archivos entre el cliente y un escritorio remoto](#)
- [Habilitar el modo de sesión múltiple para las aplicaciones publicadas](#)
- [Sonido](#)
- [Combinaciones de teclas de método abreviado](#)
- [Internacionalización](#)
- [Teclados internacionales](#)

Matriz de compatibilidad de funciones

Cuando accede a una aplicación o un escritorio remotos desde el cliente HTML Access basado en el navegador, algunas funciones no están disponibles.

Compatibilidad de funciones para escritorios de máquinas virtuales de usuario único

Tabla 4-1. Funciones admitidas por HTML Access

Función	Escritorio de Windows 7	Escritorio de Windows 8.x	Escritorio de Windows 10	Escritorio de Windows Server 2008 R2	Escritorio de Windows Server 2012 R2	Escritorios de Windows Server 2016 o Windows Server 2019
RSA SecurID o RADIUS	X	X	X	X	X	X
Single Sign-On	X	X	X	X	X	X
Protocolo de visualización RDP						
Protocolo de visualización PCoIP						
Protocolo de visualización VMware Blast	X	X	X	X	X	X
Redireccionamiento USB						
Audio/vídeo en tiempo real (RTAV)	X	X	X	X	X	X
Wyse MMR						
Redireccionamiento multimedia (MMR) de Windows Media						
Impresión virtual						
Impresión basada en ubicación	X	X	X	X	X	X
Tarjetas inteligentes						
Varios monitores	X	X	X	X	X	X

Para las descripciones de estas funciones y sus limitaciones, consulte el documento acerca de *cómo planificar la arquitectura de Horizon 7*.

Compatibilidad de funciones para escritorios basados en sesiones y aplicaciones alojadas en hosts RDS

Los hosts RDS son equipos servidores con Servicios de Escritorio remoto de Windows y Horizon Agent instalados. Varios usuarios pueden tener sesiones de escritorio y de aplicaciones en un host RDS al mismo tiempo. Un host RDS puede ser un equipo físico o una máquina virtual.

Nota La siguiente tabla contiene filas únicamente para las funciones que están disponibles en hosts RDS si usa HTML Access. Existen funciones adicionales disponibles si usa Horizon Client instalado de forma nativa, como Horizon Client para Windows.

Tabla 4-2. Funciones compatibles con HTML Access para hosts RDS con View Agent 6.1.1 o posterior, o bien Horizon Agent 7.0 o posterior, instalados

Función	Host RDS con Windows Server 2008 R2	Host RDS con Windows Server 2012 o 2012 R2	Windows Server 2016	Windows Server 2019
RSA SecurID o RADIUS	X	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Single Sign-On	X	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Protocolo de visualización VMware Blast	X	X	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.7 y posterior
Impresión basada en ubicación	X (solo máquina virtual)	X (solo máquina virtual)	Horizon Agent 7.0.2 y posterior (solo máquina virtual)	Horizon Agent 7.7 y posterior
Audio/vídeo en tiempo real (RTAV)	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.2 y posterior	Horizon Agent 7.0.3 y posterior	Horizon Agent 7.7 y posterior
Varios monitores (solo para escritorios basados en sesiones)	X	X	X	X

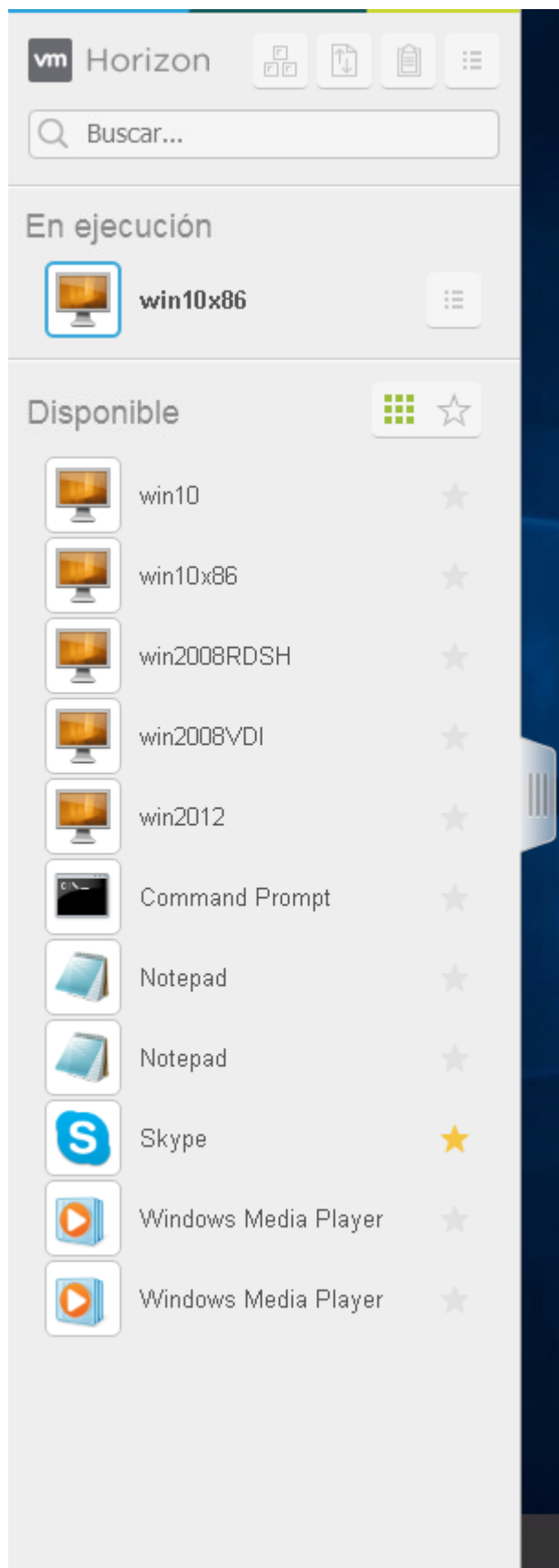
Para obtener información sobre las ediciones o service pack de cada sistema operativo invitado que son compatibles, consulte la información sobre sistemas operativos que admite Horizon Agent en el documento *Instalación de Horizon 7*.

Utilizar la barra lateral

Una vez que se conecte a un escritorio remoto o una aplicación publicada, puede usar la barra lateral para iniciar otros escritorios remotos y aplicaciones publicadas, cambiar entre escritorios remotos y aplicaciones publicadas y realizar otras acciones.

La barra lateral aparece en el lateral izquierdo de la ventana del escritorio remoto o la aplicación publicada. Para mostrar u ocultar la barra lateral haga clic en la pestaña de la barra lateral. También puede deslizar la pestaña hacia arriba y hacia abajo.

Figura 4-1. Barra lateral que aparece cuando inicia una aplicación publicada o un escritorio remoto



Para ver la lista de documentos que abre una aplicación publicada en ejecución, haga clic en la flecha para expandir que aparece junto a la aplicación publicada de la lista **En ejecución**.

Nota Si tiene dos documentos abiertos desde las mismas aplicaciones publicadas, pero estas son independientes y están alojadas en dos servidores diferentes, la aplicación publicada aparece dos veces en la lista **En ejecución** de la barra lateral.

Puede realizar muchas acciones desde la barra lateral.

Tabla 4-3. Acciones de la barra lateral

Acción	Procedimiento
Mostrar la barra lateral	Cuando se abre una aplicación publicada o un escritorio remoto, haga clic en la pestaña de la barra lateral. Cuando la barra lateral esté abierta, podrá seguir realizando acciones en la ventana del escritorio remoto o de la aplicación publicada.
Ocultar la barra lateral	Haga clic en la pestaña de la barra lateral.
Iniciar una aplicación publicada o un escritorio remoto	Haga clic en el nombre de una aplicación publicada o un escritorio remoto en la lista Disponible de la barra lateral. Los escritorios remotos aparecen primero en la lista.
Buscar una aplicación publicada o un escritorio remoto	<ul style="list-style-type: none"> ■ Haga clic en el cuadro Buscar y escriba el nombre de la aplicación publicada o del escritorio remoto. ■ Para iniciar una aplicación publicada o un escritorio remoto, haga clic en el nombre en los resultados de búsqueda. ■ Para volver a la vista inicial de la barra lateral, toque la X del cuadro de búsqueda.
Crear una lista de aplicaciones publicadas y escritorios remotos favoritos	Haga clic en la estrella de color gris situada junto al nombre del escritorio remoto o de la aplicación publicada de la lista Disponible de la barra lateral. A continuación, puede hacer clic en el botón Mostrar favoritos de la barra de herramientas (icono de estrella) situado junto a Disponible para mostrar una lista que contenga solo los favoritos.
Cambiar entre aplicaciones publicadas o escritorios remotos	Haga clic en el nombre de una aplicación publicada o un escritorio remoto en la lista En ejecución de la barra lateral.
Habilitar el modo de sesión múltiple para las aplicaciones publicadas	Haga clic en el botón Abrir menú , situado en la barra lateral, haga clic en Configuración y desplácese hacia abajo hasta la opción Inicio múltiple . Si desea obtener más información, consulte Habilitar el modo de sesión múltiple para las aplicaciones publicadas .
Abrir el panel Copiar y pegar	Haga clic en el botón Copiar y pegar situado en la parte superior de la barra lateral. Utilice este botón para copiar texto de aplicaciones y copiar texto en ellas en su sistema cliente local. Si desea obtener más información, consulte Copiar y pegar texto . En Safari para iOS, este botón no está disponible porque la función de copiar y pegar no es compatible.
Abrir la ventana Transferencia de archivos	Para descargar archivos del escritorio remoto o cargar archivos a dicho escritorio, haga clic en el botón Transferencia de archivos que aparece en la parte superior de la barra lateral. Para obtener más información, consulte Descargar archivos de un escritorio en el cliente y Cargar archivos del cliente a un escritorio .
Habilitar Comando-A, Comando-C, Comando-V y Comando-X	Esta opción aparece en la ventana Configuración solo si utiliza un equipo Mac. Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración . Cuando esta función está habilitada, la tecla Comando del equipo Mac se asigna a la tecla Ctrl en la aplicación o el escritorio remotos de Windows. Por ejemplo, pulsar Comando-A en un teclado de Mac será lo mismo que pulsar Ctrl+A en la aplicación o el escritorio remotos de Windows.

Tabla 4-3. Acciones de la barra lateral (Continuación)

Acción	Procedimiento
Cerrar un escritorio remoto en ejecución	<p>Haga clic en el botón Abrir menú, situado junto al nombre del escritorio de la lista En ejecución de la barra lateral, y seleccione una acción.</p> <ul style="list-style-type: none"> ■ Seleccione Cerrar para desconectarse del escritorio remoto sin cerrar sesión en el sistema operativo. Un administrador de Horizon puede establecer que un escritorio cierre sesión de forma automática cuando se desconecte. En ese caso, los cambios que no se guardaron en las aplicaciones abiertas se pierden. ■ Seleccione Cerrar sesión para cerrar sesión en el sistema operativo y desconectarse del escritorio remoto. Los cambios que no se guardaron en las aplicaciones abiertas se pierden.
Cerrar una aplicación publicada en ejecución	<p>Haga clic en la X situada junto al nombre del archivo en el nombre de la aplicación publicada de la lista En ejecución de la barra lateral. Haga clic en la X situada junto al nombre de la aplicación publicada para salir de ella y cerrar todos los archivos abiertos de dicha aplicación.</p> <p>Se le solicitará que guarde los cambios realizados en los archivos.</p>
Restablecer un escritorio remoto	Haga clic en el botón Abrir menú situado junto al nombre del escritorio remoto de la lista En ejecución de la barra lateral y seleccione Restablecer . Los archivos que estén abiertos en el escritorio remoto se cierran sin guardar. Solo puede restablecer un escritorio remoto si un administrador de Horizon habilitó esta función.
Reiniciar un escritorio remoto	Haga clic en el botón Abrir menú situado junto al nombre del escritorio remoto de la lista En ejecución de la barra lateral y seleccione Reiniciar . El sistema operativo del escritorio remoto le suele pedir que guarde los datos que no guardó antes de reiniciar. Solo puede reiniciar un escritorio remoto si un administrador de Horizon habilitó esta función.
Restablecer todas las aplicaciones publicadas en ejecución	Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración y Restablecer todas las aplicaciones en ejecución . Los cambios que no se hayan guardado se perderán.
Utilizar combinaciones de teclas que incluyan la tecla Windows	Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Habilitar la tecla Windows para los escritorios . Si desea obtener más información, consulte Combinaciones de teclas de método abreviado .
Enviar Ctrl+Alt+Supr al área de trabajo actual	Haga clic en el botón Enviar Ctrl+Alt+Supr de la barra de herramientas situado en la parte superior de la barra lateral.
Desconectarse de un servidor	Haga clic en el botón Abrir menú de la barra de herramientas en la parte superior de la barra lateral y haga clic en Cerrar sesión .
Utilizar el modo de alta resolución en equipos con una pantalla de alta resolución, por ejemplo, un Macbook Pro con pantalla Retina	Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Modo de alta resolución .
Permitir la decodificación H.264	(Solo Chrome) Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral, seleccione Configuración y habilite la opción Permitir la decodificación H.264 . Si desea obtener más información, consulte Permitir la decodificación H.264 .
Utilizar varios monitores	(Versión 55 de Chrome o posteriores) Haga clic en el botón Abrir menú de la barra de herramientas situado en la parte superior de la barra lateral y seleccione Configuración de pantalla . Para obtener más información, consulte Utilizar varios monitores

Tabla 4-3. Acciones de la barra lateral (Continuación)

Acción	Procedimiento
Mostrar u ocultar el teclado en pantalla	(Solo Safari para iOS) Haga clic en el icono de teclado situado en la parte superior de la barra lateral. También puede mostrar u ocultar el teclado en pantalla. Para ello, toque la pantalla con tres dedos.
Mostrar temas de ayuda	Haga clic en el botón Abrir menú de la barra de herramientas en la parte superior de la barra lateral, seleccione Configuración y haga clic en Ayuda . También puede hacer clic en el logotipo de Horizon situado en la parte superior de la barra lateral y haga clic en Ayuda .
Mostrar el cuadro de diálogo Acerca de VMware Horizon Client	Haga clic en el botón Abrir menú de la barra de herramienta o en el logotipo de Horizon en la parte superior de la barra lateral y haga clic en Acerca de . También puede hacer clic en el logotipo de Horizon situado en la parte superior de la barra lateral.
Mostrar una aplicación publicada o un escritorio remoto en modo de pantalla completa	Haga clic en el botón Abrir menú de la barra de herramientas en la parte superior de la barra lateral y haga clic en Pantalla completa .
Salga del modo de pantalla completa	Haga clic en el botón Abrir menú de la barra de herramientas en la parte superior de la barra lateral y haga clic en Salir de pantalla completa .
Puede enviar ESC a una aplicación publicada o un escritorio remoto cuando está en modo de pantalla completa	Haga clic en el botón Abrir menú de la barra de herramientas en la parte superior de la barra lateral y haga clic en Enviar ESC .

Resolución de pantalla y monitores

Es posible ampliar un escritorio remoto o una aplicación publicada a varios monitores. Si cuenta con un monitor de alta resolución, puede ver la aplicación publicada o el escritorio remoto en máxima resolución.

Utilizar varios monitores

Puede usar varios monitores en HTML Access Web client para mostrar una ventana del escritorio remoto con un navegador Chrome (versión 55 o posteriores).

Puede agregar hasta un monitor adicional a su monitor principal para mostrar la ventana actual del escritorio remoto al que está conectado. Por ejemplo, si dispone de tres monitores, puede especificar que la ventana del escritorio remoto solo aparezca en dos de esos monitores. Se deben seleccionar monitores adyacentes para la configuración de varios monitores. Los monitores pueden estar colocados uno junto al otro o bien apilados de forma vertical.

A partir de la versión 4.5 de HTML Access Web client, la sincronización PPP por dispositivo se aplica cuando se habilita la función de varios monitores. Si utiliza dos monitores que tienen diferentes configuraciones PPP, la configuración PPP del agente HTML Access se establece con el mismo valor PPP del monitor del equipo cliente que se usó para iniciar la sesión de HTML Access Web client.

Procedimiento

- 1 Inicie Horizon Client e inicie sesión en un servidor.

- 2 En la ventana de selección de aplicaciones y escritorios, haga clic en el icono del escritorio remoto al que desea acceder.
- 3 Para mostrar la barra lateral, haga clic en la pestaña de la barra lateral.
- 4 Haga clic en el botón **Abrir menú** de la barra de herramientas situado en la parte superior de la barra lateral y seleccione **Configuración de pantalla**.
- 5 En el cuadro de diálogo Configuración de pantalla, haga clic en **Agregar pantalla**.

Nota Si la ventana del navegador Selector de pantallas no aparece, agregue la dirección FQDN del servidor Horizon en la sección Excepciones de elementos emergentes de la ventana **Configuración de contenido** de su navegador.

- 6 Arrastre la ventana Selector de pantallas para que aparezca en la pantalla del otro monitor que desea utilizar.

El mensaje de la ventana del navegador Selector de pantallas cambiará y se agregará un icono gris rectangular.
- 7 En la ventana del navegador Selector de pantallas, haga clic en el icono del monitor + para confirmar que desea utilizar la pantalla del monitor actual.

El mensaje Esperando otras pantallas aparecerá en la pantalla del monitor actual y el icono gris de monitor de la ventana Configuración de pantalla de la pantalla principal cambiará a verde.
- 8 Haga clic en **Aceptar** en la ventana Configuración de pantalla una vez que agregue las pantallas del monitor que desee utilizar para la sesión.

Si la ventana Configuración de pantalla desaparece, el mensaje Esperando otras pantallas se borrará de la pantalla del monitor que no sea el principal y se mostrará en la ventana del escritorio remoto.
- 9 Para salir del modo de varios monitores, pulse Esc y haga clic en **Sí** en el cuadro de diálogo **Cerrar el modo de pantallas múltiples** para confirmar.

Nota Cada vez que tenga que utilizar la tecla Esc en el escritorio remoto, abra la barra lateral, haga clic en el botón **Abrir menú** de la barra de herramientas situado en la parte superior de la barra lateral y seleccione **Enviar ESC**.

Resolución de pantalla

Si Horizon Administrator configura un escritorio remoto con la cantidad correcta de RAM de vídeo, el cliente web puede cambiar el tamaño de un escritorio remoto para adaptarlo al tamaño de la ventana del navegador. La configuración predeterminada es 36 MB de RAM de vídeo, que es una cantidad bastante superior al mínimo requerido de 16 MB si no usa aplicaciones 3D.

Si usa un navegador o un dispositivo Chrome que tenga una resolución con alta densidad de píxeles, como un Macbook con Retina Display o un Google Chromebook Pixel, puede configurar la aplicación o el escritorio remotos para que usen dicha resolución. Active la opción **Modo de alta resolución** en la ventana Configuración, que se encuentra en la barra lateral. (Esta opción solo aparece en la ventana Configuración si utiliza una pantalla de alta resolución o una pantalla normal con una escala superior al 100 %.)

Para usar la función de procesamiento 3D, debe asignar suficiente VRAM en cada escritorio remoto.

- La función de gráficos acelerados por software, disponible con vSphere 5.0 o versiones posteriores, le permite utilizar aplicaciones 3D como, por ejemplo, los temas de Aero de Windows o Google Earth. Para utilizar estas funciones se necesitan entre 64 MB y 128 MB de VRAM.
- La función de gráficos acelerados por hardware compartida (vSGA), disponible con vSphere 5.1 o versiones posteriores, le permite utilizar aplicaciones 3D para actividades multimedia, de diseño y de modelado. Para utilizar esta función se necesitan entre 64 MB y 512 MB de VRAM. La cantidad predeterminada son 96 MB.
- La función de gráficos acelerados por el hardware dedicada (vDGA), disponible en vSphere 5.5 o versiones posteriores, asigna una GPU (unidad de procesamiento gráfico) física única en un host ESXi para una máquina virtual única. Use esta función si necesita gráficos de estación de trabajo acelerados por hardware de alta gama. Para utilizar esta función se necesitan entre 64 MB y 512 MB de VRAM. La cantidad predeterminada son 96 MB.

Cuando el procesamiento 3D está habilitado, el número máximo de monitores es 1 y la resolución máxima es 3840 x 2160.

De forma similar, si usa un navegador en un dispositivo que tenga una resolución con alta densidad de píxeles, como un Macbook con Retina Display o un Google Chromebook Pixel, debe asignar suficiente VRAM para cada escritorio remoto.

Importante El cálculo de la cantidad de VRAM que necesita para el protocolo de visualización VMware Blast es similar al cálculo de la cantidad de VRAM necesaria para el protocolo de visualización PCoIP. Para obtener más instrucciones, consulte la sección "Tamaño de RAM para configuraciones de monitores específicas al utilizar PCoIP", que se encuentra dentro del tema "Cómo calcular los requisitos de memoria para escritorios virtuales", en el documento *Planificación de la arquitectura de Horizon 7*.

Usar la sincronización PPP

La función Sincronización de PPP garantiza que la configuración de PPP en una aplicación publicada o un escritorio remoto coincida con la del sistema cliente. Cuando se inicia una nueva sesión, Horizon Agent establece el valor de PPP de esa sesión remota para que coincida con el del sistema cliente.

La función Sincronización PPP no puede cambiar la configuración PPP para las sesiones remotas activas. Si vuelve a conectarse a una sesión remota existente, la función de escala de pantalla ajusta la aplicación publicada o escritorio remoto de forma apropiada.

La función Sincronización PPP se habilita si la opción Modo de alta resolución está deshabilitada en la ventana Configuración. A partir de la versión 4.5 de HTML Access, si un administrador de Horizon deshabilita la opción de directiva de grupo **Sincronización de PPP**, la función de sincronización de PPP se puede deshabilitar, pero no la función Ajuste de escala de la pantalla. Debe cerrar sesión e iniciarla de nuevo para que se realicen los cambios en la configuración. Para obtener más información sobre la opción de la directiva de grupo **Sincronización de PPP**, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para utilizar la función Sincronización de PPP, es necesario Windows 7 o versiones posteriores en los escritorios de una sesión única, Windows Server 2008 R2 o versiones posteriores para escritorios publicados y aplicaciones publicadas en hosts RDS, Horizon Agent 7.0.2 o versiones posteriores y HTML Access 4.4 o versiones posteriores.

A continuación le mostramos algunos consejos para usar la función Sincronización de PPP.

- Si cambia la configuración PPP en el sistema cliente, deberá cerrar sesión y volverla a iniciar para que Horizon Client reconozca la nueva configuración PPP. Este requisito se aplica aunque el sistema cliente ejecute Windows 10.
- Si inicia una sesión remota en un sistema cliente que tenga una configuración PPP de más del 100 % y utiliza la misma sesión en otro sistema cliente que tenga una configuración PPP diferente de más del 100 %, debe cerrar la sesión remota y volver a iniciarla en el segundo sistema cliente para hacer que la sincronización de PPP funcione en dicho sistema.
- Aunque los sistemas con Windows 10 y Windows 8.x admitan distintas configuraciones PPP en los distintos monitores, la función Sincronización de PPP utiliza el valor PPP que se configuró en el monitor del sistema cliente en el que se encuentra el navegador web que se utilizó para iniciar la sesión de cliente de HTML Access. HTML Access no admite diferentes configuraciones de PPP en monitores diferentes.
- Si desea sincronizarse con otro monitor utilizando otra configuración PPP, debe cerrar sesión en el escritorio remoto o la aplicación publicada, arrastrar al otro monitor el navegador web utilizado para iniciar la sesión de cliente de HTML Access y volver a iniciar sesión en la aplicación publicada o el escritorio remoto para que las configuraciones PPP del sistema cliente y la aplicación publicada o el escritorio remoto coincidan.

Usar el modo de pantalla completa

Puede mostrar una aplicación publicada o un escritorio remoto en modo de pantalla completa.

No puede usar el modo de pantalla completa en las siguientes situaciones.

- Si está utilizando varios monitores.
- Si el navegador está en modo de pantalla completa o se maximizó arrastrando el mouse.
- Si está utilizando Safari.

Requisitos previos

Conéctese al escritorio remoto o a una aplicación publicada.

Procedimiento

- Para mostrar el escritorio remoto o una aplicación publicada en el modo de pantalla completa, haga clic en el botón **Abrir menú**, situado en la parte superior de la barra lateral y, a continuación, haga clic en **Pantalla completa**.
- Para salir del modo de pantalla completa, haga clic en el botón **Abrir menú**, situado en la parte superior de la barra lateral y, a continuación, haga clic en **Salir de pantalla completa**.

También puede pulsar la tecla Esc en el teclado del sistema cliente.

Utilizar la función Audio/vídeo en tiempo real para las cámaras web y los micrófonos

Con la función Audio/vídeo en tiempo real, puede utilizar el micrófono o la cámara web de la máquina cliente en un escritorio remoto o aplicación publicada. La función de Audio/vídeo en tiempo real es compatible con las aplicaciones de conferencias estándares y las aplicaciones de vídeo basadas en explorador. Además, admite entrada de audio analógica, dispositivos de audio USB y cámaras web estándar.

La función Audio/vídeo en tiempo real solo es compatible en Chrome, Microsoft Edge y Firefox. La resolución de vídeo predeterminada es 320 x 240. La configuración Audio/vídeo en tiempo real predeterminada funciona correctamente con la mayoría de aplicaciones de audio y de cámaras web.

Para obtener más información sobre cómo cambiar la configuración Audio/vídeo en tiempo real, consulte "Configurar la directiva de grupo de Audio/vídeo en tiempo real" en el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Cuando una aplicación publicada o un escritorio remoto estén conectados al micrófono o a la cámara web del equipo cliente, antes de que la aplicación publicada o el escritorio remoto puedan usar la cámara web o el micrófono, el navegador pedirá permiso. No todos los navegadores tienen el mismo comportamiento.

- Microsoft Edge le pedirá permiso en cada ocasión. No es posible cambiar este comportamiento. Si desea obtener más información, consulte <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>.
- Firefox le pedirá permiso en cada ocasión. Es posible cambiar este comportamiento. Si desea obtener más información, consulte <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>.
- Chrome le pedirá permiso la primera vez. Si permite que se use el dispositivo, Chrome no le volverá a pedir permiso.

Cuando un escritorio remoto está conectado al micrófono o la cámara web de un equipo cliente, aparece un icono de cada dispositivo en la parte superior de la barra lateral. También aparece un signo de interrogación rojo sobre el icono del dispositivo en la barra lateral para indicar la solicitud de permiso. Si permite que se use un dispositivo, desaparece este signo. Si rechaza una solicitud de permiso, desaparece el icono del dispositivo.

Si se usa la función Audio/vídeo en tiempo real en una sesión de aplicación publicada o de escritorio remoto, abre una conexión a una segunda aplicación publicada o un segundo escritorio remoto, y si aparece una advertencia de seguridad (por ejemplo, si no se instaló un certificado válido), si ignora esta advertencia y continúa con el proceso de conexión del segundo escritorio remoto o la segunda aplicación publicada, esta función dejará de funcionar en la primera sesión.

Usar la función Session Collaboration

Puede usar la función Session Collaboration para invitar a otros usuarios a que se unan a una sesión de escritorio remoto existente.

Invitar a un usuario a que se una a una sesión de escritorio remoto

Cuando se habilita la función Session Collaboration en un escritorio remoto, puede invitar a otros usuarios para que se unan a una sesión de escritorio remoto.

De forma predeterminada, puede enviar invitaciones de Session Collaboration por correo electrónico, por mensaje instantáneo (solo para escritorios remotos Windows) o copiando un vínculo al portapapeles y enviándolo a los usuarios. Para usar el método de invitación por correo electrónico, debe estar instalada una aplicación de correo electrónico. Para usar el método de invitación por IM en un escritorio remoto Windows, Skype Empresarial debe estar instalado y configurado. Solo puede invitar a usuarios que pertenezcan a un dominio que el servidor admita para la autenticación. De forma predeterminada, puede invitar hasta cinco usuarios.

La función Session Collaboration tiene las siguientes limitaciones.

- Si tiene varios monitores, los colaboradores de sesión solo ven el monitor principal.
- Debe seleccionar el protocolo de visualización VMware Blast cuando cree una sesión de escritorio remoto. La función Session Collaboration no admite sesiones RDP ni PCoIP.
- No se admite la codificación H.264 de hardware. Si el propietario de la sesión usa la codificación de hardware y un colaborador se une a la sesión, ambos recurrirán a la codificación de software.
- No se admite la colaboración anónima. Los colaboradores de la sesión se deben identificar mediante mecanismos de autenticación que Horizon admita.
- Los colaboradores de sesión deben tener instalado Horizon Client 4.7 para Windows, Mac o Linux, o bien usar la versión 4.7 de HTML Access o una posterior.
- Si un colaborador de sesión tiene una versión no admitida de Horizon Client, aparece un mensaje de error cuando el usuario hace clic en un vínculo de colaboración.
- No puede usar la función Session Collaboration para compartir sesiones de aplicaciones publicadas.

Requisitos previos

Si desea invitar a usuarios para que se unan a una sesión de escritorio remoto, un administrador de Horizon debe habilitar la función Session Collaboration.


En escritorios Windows, esta tarea incluye habilitar la función Session Collaboration en el nivel de granja o de grupo de escritorios. También puede incluir el uso de directivas de grupo para configurar las funciones que se incluyen en Session Collaboration, como los métodos de invitación disponibles. Para conocer todos los requisitos, consulte [Requisitos de la función Session Collaboration](#).

Para obtener más información sobre cómo habilitar la función Session Collaboration en escritorios Windows, consulte el documento *Configurar escritorios virtuales en Horizon 7*. Para obtener más información sobre cómo habilitar la función Session Collaboration en una granja, consulte el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. Si desea obtener más información sobre cómo usar las opciones de la directiva de grupo para configurar la función Session Collaboration, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Para obtener más información sobre cómo habilitar la función Session Collaboration en escritorios Linux, consulte el documento *Configurar escritorios de Horizon 7 for Linux*.

Procedimiento

- 1 Debe conectarse a un escritorio remoto para el que la función Session Collaboration esté habilitada. Debe utilizar el protocolo de visualización VMware Blast.

- 2 En la bandeja del sistema del escritorio remoto, haga clic en el icono **Colaboración de VMware Horizon**, por ejemplo, .

El icono de colaboración es diferente según la versión del sistema operativo.

- 3 Cuando se abra el cuadro de diálogo Colaboración de VMware Horizon, escriba el nombre de usuario (por ejemplo, **testuser** o **domain\testuser**), o bien la dirección de correo electrónico del usuario que quiere que se una a la sesión de escritorio remoto.

La primera vez que escriba el nombre de usuario o la dirección de correo electrónico de un usuario en concreto, debe hacer clic en **Buscar "usuario"**, escribir una coma (,) o pulsar la tecla **Entrar** para validar al usuario. La función Session Collaboration recuerda al usuario la próxima vez que escriba el nombre o la dirección de correo electrónico del usuario.

De forma predeterminada, puede invitar hasta cinco usuarios. Un administrador de Horizon puede cambiar el número máximo de usuarios a los que puede invitar.

4 Seleccione un método de invitación.

Es posible que no todos los métodos de invitación estén disponibles.

Opción	Acción
Correo electrónico	Copia la invitación de colaboración al portapapeles y abre un nuevo mensaje de correo electrónico en la aplicación de correo electrónico predeterminada. Para usar este método de invitación, debe estar instalada una aplicación de correo electrónico.
IM	(Solo para escritorios remotos Windows) Copia la invitación de colaboración al portapapeles y abre una nueva ventana en Skype Empresarial. Pulse Ctrl+V para pegar el vínculo en la ventana de Skype Empresarial. Skype Empresarial debe estar instalado y configurado para usar este método de invitación.
Copiar vínculo	Copia la invitación de colaboración en el portapapeles. De forma manual, debe abrir otra aplicación, como Bloc de notas, y pulsar Ctrl+V para pegar la invitación.

Después de enviar una invitación, el icono Colaboración de VMware Horizon también aparece en el escritorio y la interfaz de usuario de Session Collaboration pasa a ser un panel de control que muestra el estado actual de la sesión de colaboración, y le permite realizar ciertas acciones.

Cuando un colaborador de sesión acepta la invitación y se une a la sesión de escritorio remoto Windows, recibe una notificación de la función Session Collaboration y aparece un punto rojo en el icono Colaboración de VMware Horizon de la bandeja del sistema. Esta función no está disponible para sesiones de escritorios remotos Linux.

Pasos siguientes

Administre la sesión colaborativa en el cuadro de diálogo Colaboración de VMware Horizon. Consulte [Administrar una sesión colaborativa](#).

Administrar una sesión colaborativa

Después de enviar una invitación para colaborar en una sesión, la interfaz de usuario de Session Collaboration pasa a ser un panel de control que muestra el estado actual de la sesión colaborativa, y le permite realizar ciertas acciones.

Requisitos previos

Inicie una sesión de colaboración. Consulte [Invitar a un usuario a que se una a una sesión de escritorio remoto](#).

Procedimiento

- 1 En el escritorio remoto, haga clic en el icono **Colaboración de VMware Horizon** de la bandeja del sistema.

Los nombres de todos los colaboradores de la sesión aparecen en la columna Nombre y sus estados aparecen en la columna Estado.

- 2 Utilice el panel de control VMware Horizon Session Collaboration para administrar la sesión colaborativa.

Opción	Acción
Revocar una invitación o eliminar un colaborador	Haga clic en Eliminar en la columna Estado.
Transferir el control a un colaborador de la sesión	Después de que el colaborador de la sesión se una, cambie el conmutador de la columna Control a Activado . Para reanudar el control de la sesión, haga doble clic o pulse cualquier tecla. El colaborador de la sesión también puede devolver el control. Para ello deberá cambiar el conmutador de la columna Control a Desactivado o hará clic en el botón Devolver el control .
Agregar colaborador	Haga clic en Agregar colaboradores .
Cerrar la sesión colaborativa	Haga clic en Finalizar la colaboración . Se desconectan todas las colaboraciones activas. En escritorios remotos Windows, también puede finalizar la sesión colaborativa si hace clic en el botón Detener que aparece junto al icono VMware Horizon Session Collaboration . El botón Detener no está disponible en escritorios remotos Linux.

Unirse a una sesión colaborativa

Para unirse a una sesión colaborativa, puede hacer clic en el vínculo de una invitación de colaboración. El vínculo puede estar en un correo electrónico o un mensaje instantáneo, o bien en un documento que el propietario de la sesión le envíe. Además, puede iniciar sesión en el servidor y hacer doble clic en el icono de la sesión colaborativa de la ventana para seleccionar la aplicación y el escritorio.

Este procedimiento describe cómo unirse a una sesión colaborativa a partir de una invitación de colaboración.

Nota En un entorno arquitectura Cloud Pod, no puede unirse a una sesión colaborativa iniciando sesión en el servidor, a menos que inicie sesión en el pod del propietario de la sesión.

No puede usar las siguientes funciones de escritorio remoto en una sesión colaborativa.

- Audio/vídeo en tiempo real (RTAV)
- Impresión basada en ubicación
- Redireccionamiento del portapapeles

No puede cambiar la resolución de escritorio remoto en una sesión colaborativa.

Requisitos previos

Para unirse a una sesión colaborativa, debe tener Horizon Client 4.7 para Windows, Mac o Linux instalado en el sistema cliente, o bien debe usar la versión 4.7 de HTML Access o una versión posterior.

Procedimiento

- 1 Haga clic en el vínculo de la invitación de colaboración.
Horizon Client se abre en el sistema cliente.
- 2 Introduzca sus credenciales para iniciar sesión en Horizon Client.
Después de autenticarse correctamente, comienza la sesión colaborativa y puede ver el escritorio remoto del propietario de la sesión. Si el propietario de la sesión le transfiere el control del teclado y del mouse, puede usar el escritorio remoto.
- 3 Para devolver el control del teclado y del mouse al propietario de la sesión, haga clic en el icono **Colaboración de VMware Horizon** de la bandeja del sistema y cambie el conmutador de la columna Control a **Desactivado**, o haga clic en el botón **Devolver el control**.
- 4 Para salir de la sesión colaborativa, haga clic en **Cerrar** en la barra lateral.

Copiar y pegar texto

Puede copiar texto sin formato y enriquecido con formato HTML de un dispositivo cliente a una aplicación publicada o un escritorio remoto y pegarlo en ellos. Un administrador de Horizon puede configurar esta función para que sea posible realizar estas operaciones del sistema cliente a una aplicación publicada o un escritorio remoto, de una aplicación publicada o un escritorio remoto al sistema cliente, ambas posibilidades o ninguna.


Los administradores de Horizon configuran la posibilidad de copiar y pegar utilizando directivas de grupo que pertenecen a View Agent o a Horizon Agent en los escritorios remotos. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#).

Al copiar y pegar texto enriquecido, se aplican las siguientes restricciones

- No se admite copiar y pegar imágenes.
- Si copia texto enriquecido desde el dispositivo cliente y el destino es la aplicación WordPad, solo se copia y pega el texto sin formato.
- No se puede copiar y pegar texto enriquecido cuando se utiliza HTML Access en un navegador Internet Explorer (IE), Microsoft Edge o Safari. Debe usar la ventana Copiar y pegar. Consulte [Usar la ventana Copiar y pegar](#).
- Horizon Administrator también puede usar directivas de grupo para restringir los formatos del portapapeles durante operaciones de copiado y pegado. Debido a que HTML Access admite únicamente la transferencia de texto en el portapapeles, solo los filtros de texto funcionan con el cliente HTML Access. Para obtener información sobre directivas de filtro de formato de portapapeles, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Si utiliza HTML Access con un navegador Chrome o Firefox, a continuación le mostramos algunos consejos para usar la función del portapapeles.

- Tras conectarse a un escritorio remoto o una aplicación publicada por primera vez, aparecerá el cuadro de diálogo Guía de usuario del portapapeles. Haga clic en **Aceptar** para cerrar el cuadro de diálogo y que no vuelva a aparecer.

- De forma predeterminada, el icono del portapapeles  de la barra lateral está activado y aparece en color gris.
 - Si se selecciona el icono del portapapeles, al copiar texto de una aplicación publicada o un escritorio remoto, aparecerá un cuadro de diálogo que le pedirá confirmación para copiar el texto en el portapapeles del sistema cliente local. Haga clic en **Aceptar**.
 - Si el icono del portapapeles no está seleccionado, no aparecerá el cuadro de diálogo de confirmación al copiar texto desde el escritorio remoto o la aplicación publicada en el portapapeles del sistema cliente local.
- Al colocar el cursor sobre el icono del portapapeles en la barra lateral, la información sobre herramientas explica qué hace la función del portapapeles.

El portapapeles puede acumular un máximo de 1 MB de datos para todo tipo de operaciones de copiado y pegado. Si el texto sin formato y el texto enriquecido juntos utilizan un tamaño menor al máximo permitido para el portapapeles, se pegará el texto con formato. En ocasiones, el texto enriquecido no se puede truncar; de tal forma que, si el texto y el formato utilizan un tamaño mayor que el máximo permitido para el portapapeles, se rechazará el texto enriquecido y se pegará el texto sin formato. Si no puede pegar todo el texto con formato seleccionado en una operación, es posible que tenga que copiar y pegar cantidades menores en cada operación.

No puede copiar y pegar gráficos. Tampoco puede copiar y pegar archivos entre un escritorio remoto y el sistema de archivos de su equipo cliente.

Nota La función para copiar y pegar no se admite en iOS Safari ni en dispositivos Android.

Usar la ventana Copiar y pegar

Para copiar y pegar texto en un navegador Safari, Microsoft Edge o Internet Explorer (IE), debe utilizar el botón **Copiar y pegar** situado en la parte superior de la barra lateral para mostrar la ventana Copiar y pegar.

Este procedimiento describe cómo usar la ventana Copiar y pegar para copiar texto desde un navegador IE, Edge o Safari del sistema cliente a una aplicación remota o cómo copiar texto desde una aplicación remota al sistema cliente local. Sin embargo, si copia y pega texto entre escritorios y aplicaciones remotas, puede realizar la acción como lo hace habitualmente y no es necesario usar la ventana Copiar y Pegar.

Al utilizar un navegador IE, Edge o Safari, la ventana Copiar y pegar, que puede abrir con el botón situado en la parte superior de la barra lateral de HTML Access, es necesaria únicamente para sincronizar el portapapeles del sistema local con el portapapeles del equipo remoto.

El texto en la ventana Copiar y pegar muestra uno de los siguientes mensajes para indicar en qué dirección el usuario puede copiar y pegar contenido.

- Use este panel para copiar y pegar contenido entre el cliente local y la aplicación o el escritorio remotos.

- Use el panel para copiar y pegar contenido desde el cliente local a la aplicación o el escritorio remotos.
- Use el panel para copiar y pegar contenido desde la aplicación o el escritorio remotos al cliente local.

Nota La opción predeterminada de la directiva de grupo de redireccionamiento del portapapeles solo le permite copiar de sistemas clientes y pegarlos en la aplicación publicada o el escritorio remoto. La opción de la directiva debe estar habilitada en ambas direcciones para poder copiar desde la aplicación publicada o el escritorio remotos al sistema cliente. Póngase en contacto con el administrador de Horizon para obtener ayuda.

Requisitos previos

Si utiliza un equipo Mac, compruebe que tiene habilitada la opción para asignar la tecla Comando a la tecla Ctrl de Windows cuando use las combinaciones de teclas para seleccionar, copiar y pegar texto. Haga clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y active **Habilitar Comando-A, Comando-C, Comando-V y Comando-X**. (Esta opción aparece en la ventana Configuración solo si utiliza un equipo Mac.)

El administrador de Horizon debe mantener la directiva predeterminada en funcionamiento, lo que permite a los usuarios copiar desde sistemas cliente y pegar a aplicaciones y escritorios remotos, o bien configurar otra directiva que permita el copiado y el pegado. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#).

Procedimiento

- Siga estos pasos para copiar texto desde el sistema cliente a la aplicación o el escritorio remoto:
 - a Copie el texto en la aplicación cliente local.
 - b En el navegador IE, Edge o Safari, haga clic en la pestaña de la barra lateral de HTML Access para abrirla y, a continuación, haga clic en **Copiar y pegar**, en la parte superior de la barra lateral.

Aparece la ventana Copiar y pegar. Si el texto copiado anteriormente ya aparece en la ventana, este texto se reemplaza cuando pegue el nuevo texto copiado.
 - c Para pegar el texto en la ventana Copiar y pegar, pulse Ctrl+V (o Comando-V en equipos Mac).

Aparece brevemente el siguiente mensaje: "Portapapeles remoto sincronizado".
 - d Haga clic en la aplicación remota en la que desea pegar el texto y pulse Ctrl+V.

El texto se pega en la aplicación remota.

- Siga estos pasos para copiar texto desde la aplicación o el escritorio remotos al sistema cliente:

- a Copie el texto en la aplicación remota.
- b En el navegador IE, Edge o Safari, haga clic en la pestaña de la barra lateral de HTML Access para abrirla y, a continuación, haga clic en **Copiar y pegar**, en la parte superior de la barra lateral.

La ventana Copiar y pegar aparece con el texto ya pegado. Aparece brevemente el siguiente mensaje: "Portapapeles remoto sincronizado".

- c Para volver a copiar el texto, haga clic en la ventana Copiar y pegar y pulse Ctrl+C (o Comando-C en equipos Mac).

Al realizar esta acción, no se selecciona el texto y tampoco lo puede seleccionar usted mismo. Aparece brevemente el siguiente mensaje: "Copiado del panel del portapapeles".

- d En el sistema cliente, haga clic donde desee pegar el texto y pulse Ctrl+V.

El texto se pega en la aplicación del sistema cliente.

Transferir archivos entre el cliente y un escritorio remoto

Con la función de transferencia de archivos, puede transferir (cargar y descargar) archivos entre el cliente y un escritorio remoto. No se admite la transferencia de archivos entre las aplicaciones publicadas.

Nota Esta función no está disponible para usarla con escritorios remotos de Linux, dispositivos Android ni sesiones de aplicaciones remotas.

El administrador de Horizon puede configurar la capacidad de permitir, prohibir o permitir solo en una dirección la transferencia de archivos al modificar la configuración de la directiva de grupo **Configurar la transferencia de archivos** del protocolo de VMware Blast. La opción predeterminada es únicamente la carga. Si el valor **Deshabilitar tanto cargar como descargar** está seleccionado en la opción de la directiva de grupo **Configurar la transferencia de archivos** para el protocolo VMware Blast, el botón **Transferencia de archivos** está deshabilitado. Si el valor **Solo carga de archivos habilitada** está seleccionado, solo se muestra la pestaña **Cargar** en la ventana de diálogo **Transferir archivos**. Si el valor **Solo descarga de archivos habilitada** está seleccionado, solo se muestra la pestaña **Descargar** en la ventana de diálogo **Transferir archivos**. Si desea obtener más información, consulte [Configuración de las directivas de grupo de HTML Access](#).

Puede descargar un archivo que tenga como máximo 500 MB de tamaño y cargar un archivo de hasta 2 GB de tamaño. En Internet Explorer 11 de 32 bits, es posible que se produzca un error al descargar un archivo con un tamaño superior a 300 MB. Para solucionar este problema, ejecute Internet Explorer 11 en modo de 64 bits.

No puede descargar o cargar carpetas ni archivos que tengan un tamaño cero.

Safari en iOS y Safari 8 no permiten cargar ni descargar. Safari 9 y sus versiones posteriores no admiten la descarga.


Si la transferencia de archivos está en curso en una sesión de escritorio, el usuario abre una conexión en un segundo escritorio y se muestra una advertencia de seguridad (esto puede suceder si no se instaló ningún certificado válido, por ejemplo), si ignora esta advertencia y continúa con el proceso de conexión del segundo escritorio, se anulará la transferencia de archivos en la primera sesión del escritorio. Este es un comportamiento previsto.

Nota La capacidad de descarga se ve afectada por la configuración de la directiva de grupo del redireccionamiento del portapapeles. Si el redireccionamiento del portapapeles está deshabilitado del servidor al cliente, la descarga de archivos también lo estará.

Descargar archivos de un escritorio en el cliente

Con Horizon Client puede descargar archivos en el equipo cliente desde un escritorio remoto.


Procedimiento

- 1 Haga clic en el icono de transferencia de archivos  situado en la parte superior de la barra lateral. Se abrirá la ventana **Transferir archivos**.
- 2 Haga clic en **Descargar**.
- 3 Seleccione uno o varios archivos en el escritorio remoto.
- 4 Pulse Ctrl+C para iniciar la descarga.
- 5 Tras completarse la descarga, haga clic en el icono de descarga para guardar los archivos en el equipo cliente.

Cargar archivos del cliente a un escritorio

Horizon Client le permite cargar archivos desde el equipo cliente a un escritorio remoto.

Procedimiento

- 1 Haga clic en el icono de transferencia de archivos  situado en la parte superior de la barra lateral. Se abrirá la ventana **Transferir archivos**.
- 2 Haga clic en **Cargar**.
- 3 Arrastre y suelte los archivos dentro de la ventana **Transferir archivos** y haga clic en **Elegir archivos** para seleccionarlos.

Los archivos seleccionados se cargan en la carpeta Documentos.

Con Internet Explorer 11 y Chrome en ChromeBook, si arrastra y suelta carpetas, archivos de tamaño cero o superiores a 2 GB, se le mostrará un mensaje de error esperado. Después de descartar el mensaje de error, ya no podrá arrastrar ni soltar archivos que se puedan transferir.

Habilitar el modo de sesión múltiple para las aplicaciones publicadas

Cuando se habilita el modo de sesión múltiple para una aplicación publicada, puede utilizar varias sesiones de la misma aplicación al iniciar sesión en el servidor desde diferentes dispositivos cliente.

Por ejemplo, si abre una aplicación publicada en modo de sesión múltiple en el cliente A y abre la misma aplicación publicada en el cliente B, la aplicación publicada sigue abierta en el cliente A y se abre una nueva sesión de la aplicación publicada en el cliente B. Por el contrario, cuando el modo de sesión múltiple está deshabilitado (modo de sesión única), la sesión de la aplicación publicada en el cliente A se desconecta y se vuelve a conectar en el cliente B.

La función del modo de sesión múltiple tiene las siguientes limitaciones.

- El modo de sesión múltiple no funciona para aplicaciones que no admiten varias instancias, como Skype Empresarial.
- Si la sesión de aplicación se desconecta mientras utiliza una aplicación publicada en modo de sesión múltiple, se cierra la sesión automáticamente y se pierden los datos que no se guardaron.

Requisitos previos

Un administrador de Horizon debe habilitar el modo de sesión múltiple en el grupo de aplicaciones. Los usuarios no pueden modificar el modo de sesión múltiple para una aplicación publicada, a menos que el administrador de Horizon lo permita. Consulte *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para usar esta función se necesita Horizon 7 7.7 o versiones posteriores.

Procedimiento

- 1 Conéctese a un servidor.
- 2 Haga clic en el botón de la barra de herramientas **Configuración** situado en la esquina superior derecha de la ventana para seleccionar la aplicación y el escritorio, desplácese hacia la opción **Inicio múltiple** y haga clic en **Establecer**.

De forma alternativa, si inició previamente un escritorio remoto o una aplicación publicada, puede hacer clic en el botón **Abrir menú** de la barra lateral, hacer clic en **Configuración** y desplazarse hasta la opción **Inicio múltiple**. Si ninguna aplicación publicada se puede usar en modo de sesión múltiple, la opción **Inicio múltiple** aparece atenuada.

- 3 Seleccione las aplicaciones publicadas que quiere usar en modo de sesión múltiple y haga clic en **Aceptar**.

Si un administrador de Horizon aplicó el modo de sesión múltiple para una aplicación publicada, no puede cambiar esta opción.

Sonido

Puede reproducir sonido en escritorios remotos y aplicaciones publicadas, pero se pueden aplicar algunas limitaciones.

De forma predeterminada, la reproducción de sonidos está habilitada para las aplicaciones publicadas y los escritorios remotos, pero un administrador de Horizon puede establecer una directiva para deshabilitar la reproducción de sonidos.

Las siguientes limitaciones se aplican a la reproducción de sonido en los escritorios remotos y las aplicaciones publicadas.

- Para subir el volumen, use el control de sonido en el sistema cliente, no el control de sonido en el escritorio remoto.
- De forma ocasional, se puede perder la sincronización del sonido con el vídeo.
- En condiciones de tráfico de red intenso o si los navegadores realizan un gran número de tareas, es posible que la calidad del sonido disminuya. En este sentido, algunos navegadores trabajan mejor que otros.

Combinaciones de teclas de método abreviado

Algunas combinaciones de teclas no se pueden enviar a ningún escritorio remoto ni aplicación publicada, independientemente del idioma que use.

Los navegadores web permiten que se envíen algunas teclas presionadas y combinaciones de teclas al sistema de destino y al sistema cliente. Para otras teclas y combinaciones, la entrada se procesa únicamente de forma local y no se envía al sistema de destino. Las combinaciones de teclas que funcionan en el sistema dependen del software del explorador, del sistema operativo cliente y de la configuración del idioma.

Nota Si utiliza un equipo Mac, puede asignar la tecla Comando a la tecla Ctrl de Windows cuando use las combinaciones de teclas para seleccionar, copiar y pegar texto. Para habilitar esta función, haga clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y activar **Habilitar Comando-A, Comando-C, Comando-V y Comando-X**. Esta opción aparece en la ventana **Configuración** solo si utiliza un sistema cliente Mac.

Las siguientes teclas y combinaciones del teclado no suelen funcionar en escritorios remotos.

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Tecla Comando
- Alt+Entrar
- Ctrl+Alt+cualquier_tecla

Importante Para usar Ctrl+Alt+Supr, use el botón de la barra de herramientas **Enviar Ctrl+Alt+Supr**, situado en la parte superior de la barra lateral.

- Bloq mayús+tecla_modificadora (como Alt o Mayús)

- Teclas de función de un Chromebook
- Combinaciones de teclas de Windows

Si habilita la tecla Windows para los escritorios remotos, las siguientes combinaciones de teclas de Windows no funcionan en los escritorios remotos. Para habilitarla, haga clic en el botón de la barra de herramientas **Abrir ventana Configuración**, situado en la barra lateral, y activar **Habilitar la tecla Windows para los escritorios**.

Importante Después de activar **Habilitar la tecla Windows para los escritorios**, debe presionar Ctrl+Win (en sistemas Windows), Ctrl+Comando (en sistemas Mac) o Ctrl+Tecla de búsqueda (en sistemas Chromebook) para simular la acción de pulsar la tecla Windows.

Estas combinaciones de teclas no funcionan para las aplicaciones publicadas. Estas combinaciones de teclas funcionan para los escritorios publicados y los escritorios remotos de Windows Server 2008 R2, Windows Server 2012 R2 y Windows Server 2016.

Algunas combinaciones de teclas que funcionan en escritorios remotos con sistemas operativos Windows 8.x o Windows Server 2012 R2 no funcionan en escritorios remotos con sistemas operativos Windows 7, Windows Server 2008 R2 o Windows 10.

Tabla 4-4. Combinaciones de teclas de Windows para escritorios remotos con Windows 10 y escritorios remotos con Windows Server 2016

Teclas	Acción	Limitaciones
Win	Abrir o cerrar Inicio.	
Win+A	Abrir Centro de actividades.	
Win+E	Abrir Explorador de archivos.	
Win+G	Abrir la barra de juegos cuando hay uno abierto.	
Win+H	Abrir el acceso a Compartir.	
Win+I	Abrir el acceso a Configuración.	
Win+K	Abrir la acción rápida Conectar.	
Win+M	Minimizar todas las ventanas.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+S	Abrir Buscar.	
Win+X	Abrir el menú Vínculo rápido .	
Win+, (coma)	Vista temporal del escritorio remoto.	
Win+Pausa	Mostrar el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook o Mac no cuentan con la tecla Pausa.
Win+Mayús+M	Restaurar las ventanas minimizadas en el escritorio remoto.	No funciona en Safari.
Win+Alt+Num	Abrir el escritorio remoto y la lista de accesos directos de aplicaciones anclada en la barra de tareas en la posición indicada por el número.	No funciona en equipos Chromebook.
Win+Intro	Abrir Narrador.	

Tabla 4-5. Combinaciones de teclas de Windows para escritorios remotos con Windows 8.x y Windows Server 2012 R2

Teclas	Acción	Limitaciones
Win+F1	Abrir Ayuda y soporte técnico de Windows.	No funciona en Safari.
Win	Mostrar u ocultar la ventana Inicio.	
Win+B	Llevar el foco al área de notificaciones.	
Win+C	Abrir el panel Accesos.	
Win+D	Mostrar y ocultar el escritorio remoto.	No funciona en Safari. Puse Comando-D en Mac.
Win+E	Abrir Explorador de archivos.	
Win+H	Abrir el acceso a Compartir.	
Win+I	Abrir el acceso a Configuración.	
Win+K	Abrir el acceso a Dispositivos.	
Win+M	Minimizar todas las ventanas.	
Win+Q	Para buscar en cualquier lugar o en la aplicación abierta, si la aplicación admite la búsqueda, abra el acceso a Búsqueda.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+S	Para buscar en Windows y en la Web, abra el acceso a Búsqueda.	
Win+X	Abrir el menú Vínculo rápido .	
Win+Z	Mostrar los comandos disponibles en la aplicación.	
Win+, (coma)	Mostrar el escritorio remoto durante el tiempo que se mantengan pulsadas las teclas.	No funciona en sistemas operativos Windows 2012 R2.
Win+Pausa	Mostrar el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook y Mac no tienen la tecla Pausa.
Win+Mayús+M	Restaurar las ventanas minimizadas en el escritorio remoto.	No funciona en Safari. Puse Comando-D en Mac.
Win+Alt+Num	Abrir el escritorio remoto y la lista de accesos directos de aplicaciones anclada en la barra de tareas en la posición indicada por el número.	No funciona en equipos Chromebook.
Win+Flecha arriba	Maximizar la ventana.	No funciona en equipos Chromebook.
Win+Flecha abajo	Eliminar la aplicación actual de la pantalla o minimizar la ventana del escritorio remoto.	No funciona en equipos Chromebook.
Win+Flecha izquierda	Maximizar la ventana de la aplicación o del escritorio remoto en el lado izquierdo de la pantalla.	No funciona en equipos Chromebook.
Win+Flecha derecha	Maximizar la ventana de la aplicación o del escritorio remoto en el lado derecho de la pantalla.	No funciona en equipos Chromebook.
Win+Inicio	Minimizar todas las ventanas excepto la del escritorio remoto activo (restaura todas las ventanas cuando se vuelve a pulsar Win+Inicio).	No funciona en navegadores Safari.
Win+Mayús+Flecha arriba	Ampliar la ventana del escritorio remoto hasta la parte de arriba y de abajo de la pantalla.	No funciona en equipos Chromebook.

Tabla 4-5. Combinaciones de teclas de Windows para escritorios remotos con Windows 8.x y Windows Server 2012 R2 (Continuación)

Teclas	Acción	Limitaciones
Win+Mayús +Flecha abajo	Restaurar la ventana del escritorio remoto de forma vertical, mientras se mantiene el ancho, después de pulsar Win+Mayús +Flecha arriba para ampliar la pantalla, o minimizar la ventana del escritorio remoto activa.	No funciona en equipos Chromebook.
Win+Intro	Abrir Narrador.	

Tabla 4-6. Combinaciones de teclas de Windows para escritorios remotos con Windows 7 y Windows Server 2008 R2

Teclas	Acción	Limitaciones
Win	Abrir o cerrar el menú Inicio .	
Win+Pausa	Mostrar el cuadro de diálogo Propiedades del sistema.	Los equipos Chromebook y Mac no tienen la tecla Pausa.
Win+D	Mostrar y ocultar el escritorio remoto.	No funciona en Safari. Puse Comando-D en Mac.
Win+M	Minimizar todas las ventanas.	
Win+E	Abrir la carpeta Equipo.	
Win+R	Abrir el cuadro de diálogo Ejecutar.	
Win+Flecha arriba	Maximizar la ventana.	No funciona en equipos Chromebook.
Win+Flecha abajo	Minimizar la ventana.	No funciona en equipos Chromebook.
Win+Flecha izquierda	Maximizar la ventana de la aplicación o del escritorio remoto en el lado izquierdo de la ventana.	No funciona en equipos Chromebook.
Win+Flecha derecha	Maximizar la ventana de la aplicación o del escritorio remoto en el lado derecho de la ventana.	No funciona en equipos Chromebook.
Win+Inicio	Minimizar todas las ventanas excepto la del escritorio remoto activo.	No funciona en Safari.
Win+Mayús +Flecha arriba	Ampliar la ventana del escritorio remoto hasta la parte de arriba y de abajo de la pantalla.	No funciona en equipos Chromebook.
Win+G	Seleccionar entre los gadgets del escritorio remoto en ejecución.	
Win+U	Abrir el Centro de accesibilidad.	

Internacionalización

La interfaz de usuario y la documentación están disponibles en inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español.

Para obtener más información sobre qué paquetes de idioma debe usar en el sistema cliente, el navegador y el escritorio remoto, consulte [Teclados internacionales](#).

Teclados internacionales

Cuando utilice configuraciones regionales y teclados que no sean en idioma inglés, debe usar cierta configuración en el sistema cliente, el navegador y el escritorio remoto. Algunos idiomas necesitan que use un IME (editor de métodos de entrada) en el escritorio remoto.

Al tener instalados las configuraciones locales y los métodos de entrada correctos, puede introducir caracteres de los siguientes idiomas: inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español.

Tabla 4-7. Configuración del idioma de entrada necesaria

Idioma	Idioma de entrada en el sistema cliente local	¿IME necesario en el sistema cliente local?	Idioma de entrada y del explorador en el escritorio remoto	¿IME necesario en el escritorio remoto?
Inglés	Inglés	No	Inglés	No
Francés	Francés	No	Francés	No
Alemán	Alemán	No	Alemán	No
Chino (simplificado)	Chino (simplificado)	Modo de entrada inglés	Chino (simplificado)	Sí
Chino (tradicional)	Chino (tradicional)	Modo de entrada inglés	Chino (tradicional)	Sí
Japonés	Japonés	Modo de entrada inglés	Japonés	Sí
Coreano	Coreano	Modo de entrada inglés	Coreano	Sí
Español	Español	No	Español	No

Solucionar problemas relacionados con Horizon Client

5

Puede solucionar la mayoría de los problemas de Horizon Client reiniciando o restableciendo los escritorios remotos o las aplicaciones publicadas, o bien reinstalando Horizon Client.

Este capítulo incluye los siguientes temas:

- [Reiniciar un escritorio remoto](#)
- [Restablecer un escritorio remoto o una aplicación publicada](#)

Reiniciar un escritorio remoto

Si el sistema operativo del escritorio remoto deja de responder, es posible que tenga que reiniciar un escritorio remoto. Reiniciar un escritorio remoto es similar a usar el comando de reinicio del sistema operativo Windows. El sistema operativo del escritorio remoto le suele pedir que guarde los datos que no guardó antes de reiniciar.

Solo puede reiniciar un escritorio remoto si un administrador de Horizon habilitó la función de reinicio para dicho escritorio.

Para obtener información sobre cómo habilitar la función de reinicio de escritorio, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Requisitos previos

Obtenga las credenciales de inicio de sesión, como el nombre de usuario y la contraseña de Active Directory, el nombre de usuario y la contraseña de RSA SecurID o el nombre de usuario y la contraseña de la autenticación RADIUS.

Procedimiento

- ◆ Utilice el comando **Reiniciar**.

Opción	Acción
En la barra lateral	Cuando esté conectado a un escritorio remoto, haga clic en la barra de herramientas Abrir menú que se encuentra junto al nombre del escritorio remoto en la lista En ejecución de la barra lateral y seleccione Reiniciar .
Usar un URI	Para reiniciar un escritorio, utilice el URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=restart</code> .

Se reinicia el sistema operativo del escritorio remoto, Horizon Client se desconecta y cierra la sesión del escritorio remoto.

Pasos siguientes

Espere un periodo de tiempo apropiado para que se reinicie el sistema antes de intentar volver a conectarse al escritorio remoto.

Si no se soluciona el problema reiniciando el escritorio remoto, puede que tenga que restablecer el escritorio remoto. Consulte [Restablecer un escritorio remoto o una aplicación publicada](#).

Restablecer un escritorio remoto o una aplicación publicada

Puede que tenga que restablecer un escritorio remoto si el sistema operativo del escritorio deja de responder y no se soluciona el problema reiniciando el escritorio remoto. Al restablecer las aplicaciones publicadas, saldrá de todas las aplicaciones abiertas.

La acción de restablecer un escritorio remoto es equivalente a pulsar el botón Restablecer en un equipo físico para forzar su restablecimiento. Los archivos que estén abiertos en el escritorio remoto se cerrarán sin guardarse.

Al restablecer las aplicaciones publicadas, se cierran las aplicaciones sin guardar los datos que no se guardaran. Se cierran todas las aplicaciones publicadas abiertas, incluso las de diferentes granjas de servidores RDS.

Solo puede restablecer un escritorio remoto si un administrador de Horizon habilitó la función de restablecimiento para dicho escritorio.

Para obtener información sobre cómo habilitar la función de restablecimiento de escritorios, consulte el documento *Configurar escritorios virtuales en Horizon 7* o *Configurar aplicaciones y escritorios publicados en Horizon 7*.

Procedimiento

- ◆ Utilizar el comando **Restablecer**.

Opción	Acción
Restablecer aplicaciones publicadas desde la ventana de selección de aplicaciones	En la ventana para seleccionar la aplicación y el escritorio, antes de conectarse a un escritorio remoto o una aplicación publicada, haga clic en el botón de la barra de herramientas Configuración , situado en la esquina superior derecha de la pantalla y, a continuación, en Restablecer para restablecer todas las aplicaciones publicadas que se estén ejecutando.
Restablecer un escritorio remoto desde la barra lateral	Si se conecta a un escritorio remoto, haga clic en el botón Abrir menú de la barra de herramientas situado junto al nombre del escritorio en la lista En ejecución de la barra lateral y seleccione Restablecer .

Opción	Acción
Restablecer aplicaciones publicadas desde la barra lateral	Para restablecer todas las aplicaciones en ejecución, haga clic en el botón Abrir ventana Configuración de la barra de herramientas, situado en la parte superior de la barra lateral y, a continuación, en Restablecer .
Restablecer un escritorio remoto utilizando un URI	Para restablecer un escritorio remoto, utilice el URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&action=reset</code> .

Cuando restablezca un escritorio remoto, el sistema operativo del escritorio remoto se reinicia y Horizon Client desconecta y cierra la sesión del escritorio remoto. Al restablecer aplicaciones publicadas, se cerrarán dichas aplicaciones.

Pasos siguientes

Espere un periodo de tiempo apropiado para reiniciar el sistema antes de intentar volver a conectarse al escritorio remoto o la aplicación publicada.