

Uso de VMware Horizon Client para Windows 10 UWP

VMware Horizon Client for Windows 10 UWP 4.5



vmware®

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

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

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.

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

VMware, Inc.

Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.: + 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

- 1** **Uso de VMware Horizon Client para Windows 10 UWP** 5
- 2** **Instalación y configuración** 6
 - Requisitos del sistema 6
 - Requisitos de la autenticación de Windows Hello 7
 - Preparar el servidor de conexión para Horizon Client 7
 - Sistemas operativos del escritorio compatibles 8
 - Instalar o actualizar Horizon Client para Windows 10 UWP 8
 - Guardar información sobre los servidores recientes en la ventana de inicio de Horizon Client 9
 - Configurar las opciones de TLS/SSL avanzadas 9
 - Configurar las opciones de VMware Blast 10
 - Mostrar la ayuda de Horizon Client 11
- 3** **Administrar las conexiones de las aplicaciones y los escritorios remotos** 12
 - Configurar el modo de comprobación del certificado en Horizon Client 12
 - Seleccionar un protocolo de visualización 13
 - Conectarse a una aplicación o escritorio remotos 14
 - Deshabilitar Windows Hello en Horizon Client 16
 - Anclar una aplicación o un escritorio remotos a la pantalla Inicio 16
 - Desconectarse de una aplicación o un escritorio remotos 16
 - Cerrar sesión en un escritorio remoto 17
- 4** **Usar una aplicación o un escritorio remotos** 18
 - Matriz de compatibilidad de funciones 18
 - Utilizar el modo de pantalla completa 21
 - Ajustar la resolución de pantalla para aplicaciones y escritorios remotos 21
 - Habilitar la función Zoom local 21
 - Evitar que se bloquee la pantalla 22
 - Utilizar la barra lateral 22
 - Ayudas de navegación y gestos 22
 - Multitarea 23
 - Utilizar Horizon Client con un Microsoft Display Dock 24
 - Copiar y pegar texto e imágenes 24
 - Guardar documentos en una aplicación remota 24
 - Internacionalización 25
- 5** **Solucionar problemas relacionados con Horizon Client** 26
 - Horizon Client deja de responder o el escritorio remoto se bloquea 26

| | |
|---|----|
| Restablecer una aplicación o un escritorio remotos | 27 |
| Desinstalar la aplicación VMware Horizon Client | 27 |
| Conexión a un servidor en el modo Workspace ONE | 27 |
| Recopilar registros para enviarlos al equipo de soporte técnico | 28 |

Uso de VMware Horizon Client para Windows 10 UWP

1

El documento *Uso de VMware Horizon Client para Windows 10 UWP* proporciona información sobre la instalación y el uso del software VMware Horizon[®] Client[™] en un dispositivo con Windows 10 para conectarse a una aplicación o un escritorio remoto del centro de datos.

Esta información está destinada a administradores que deban configurar una implementación de Horizon que incluya dispositivos cliente con Windows 10. Asimismo, está destinada a los administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Instalación y configuración

Configurar una implementación de Horizon para clientes con Windows 10 UWP supone utilizar algunas opciones de configuración del servidor de conexión, cumplir los requisitos del sistema de los servidores de Horizon y los clientes de dispositivo con Windows 10, así como instalar la aplicación VMware Horizon Client para Windows.

Este capítulo cubre los siguientes temas:

- [Requisitos del sistema](#)
- [Requisitos de la autenticación de Windows Hello](#)
- [Preparar el servidor de conexión para Horizon Client](#)
- [Sistemas operativos del escritorio compatibles](#)
- [Instalar o actualizar Horizon Client para Windows 10 UWP](#)
- [Guardar información sobre los servidores recientes en la ventana de inicio de Horizon Client](#)
- [Configurar las opciones de TLS/SSL avanzadas](#)
- [Configurar las opciones de VMware Blast](#)
- [Mostrar la ayuda de Horizon Client](#)

Requisitos del sistema

El dispositivo en el que instala Horizon Client y los periféricos que utilice deben cumplir ciertos requisitos del sistema.

Sistemas operativos

- Rama actual (CB) de Windows 10 versión 1703 (Creators Update)
- Rama actual (CB) de Windows 10 versión 1607 (Actualización de aniversario)
- Rama actual para empresas (CBB) de Windows 10 versión 1607 (Actualización de aniversario)

- Rama de mantenimiento a largo plazo (LTSP) de Windows 10 versión 1607 (Actualización de aniversario)

Autenticación con Windows Hello

Consulte [Requisitos de la autenticación de Windows Hello](#).

Servidor de conexión, servidor de seguridad y Horizon Agent

Versión de mantenimiento más reciente de View 6.x y versiones posteriores.

VMware recomienda que utilice un servidor de seguridad o un dispositivo Unified Access Gateway para que no sea necesaria ninguna conexión VPN.

Protocolo de visualización para aplicaciones y escritorios remotos

- VMware Blast (requiere Horizon Agent 7.0 o una versión posterior)
- PCoIP

Requisitos de la autenticación de Windows Hello

Si desea usar Windows Hello para autenticarse Horizon Client, debe cumplir ciertos requisitos.

Modelos de dispositivos Windows 10

Todos los dispositivos Windows 10 que admitan Windows Hello, como Microsoft Surface Pro 4.

Requisitos de sistema operativo

Configure Windows Hello en **Configuración > Cuentas > Opciones de inicio de sesión**.

Requisitos del servidor de conexión

- Horizon 6 versión 6.2 o una versión posterior.
- Habilitar la autenticación biométrica en el servidor de conexión. Para obtener más información, consulte el apartado sobre cómo configurar la autenticación biométrica en el documento *Administración de View*.

Requisitos de Horizon Client

Habilite Windows Hello tocando **Habilitar Windows Hello** en el cuadro de diálogo de inicio de sesión del servidor. Después de iniciar sesión correctamente, las credenciales de Active Directory se almacenan de forma segura en el dispositivo Windows 10. La opción **Habilitar Windows Hello** aparece la primera vez que inicie sesión y no aparece tras habilitar la autenticación Windows Hello.

Puede utilizar la autenticación Windows Hello como parte de la autenticación en dos fases con la autenticación RADIUS o RSA SecurID.

Preparar el servidor de conexión para Horizon Client

Los administradores deben realizar tareas específicas para permitir que los usuarios finales puedan conectarse a aplicaciones y escritorios remotos.

Antes de que los usuarios finales se puedan conectar al servidor de conexión o a un servidor de seguridad y acceder a una aplicación o un escritorio remotos, debe configurar ciertas opciones de grupo y de seguridad:

- Si tiene pensado usar Unified Access Gateway, configure el servidor de conexión para que funcione con Unified Access Gateway. Consulte el documento *Implementación y configuración de Unified Access Gateway*. Los dispositivos de Unified Access Gateway llevan a cabo la misma función que antes solo realizaban los servidores de seguridad.
- Si utiliza un servidor de seguridad, compruebe que esté utilizando las últimas versiones de mantenimiento del servidor de conexión 5.3.x y del servidor de seguridad 5.3.x o versiones posteriores. Para obtener más información, consulte el documento *Instalación de View*.
- Compruebe que se creó un grupo de aplicaciones o de escritorios y que la cuenta de usuario que tiene pensado utilizar tiene autorización para acceder al grupo. Para obtener más información, consulte el documento *Configurar escritorios virtuales en Horizon 7* o el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*.
- Para utilizar una autenticación en dos fases con Horizon Client, así como la autenticación RSA SecurID o RADIUS, debe habilitar esta característica en el servidor de conexión. Para obtener más información, consulte los temas relacionados con la autenticación de dos fases en el documento *Administración de View*.
- Para usar la autenticación Windows Hello, debe habilitar la autenticación biométrica en el servidor de conexión. La autenticación biométrica es compatible con la versión 6.2 de Horizon 6 y versiones posteriores. Para obtener más información, consulte el documento *Administración de View*.

Sistemas operativos del escritorio compatibles

Los administradores pueden crear máquinas virtuales con sistemas operativos invitados e instalar el software agente en el sistema operativo invitado. Los usuarios finales pueden iniciar sesión en esas máquinas virtuales desde un dispositivo cliente.

Para obtener una lista de los sistemas operativos invitados de Windows admitidos, consulte el tema sobre sistemas operativos compatibles con Horizon Agent en el documento *Instalación de View*.

Instalar o actualizar Horizon Client para Windows 10 UWP

La aplicación VMware Horizon Client es una aplicación de Windows 10 UWP y se instala como otras aplicaciones de Windows 10 UWP.

Prerequisitos

- Compruebe que el dispositivo cliente cumpla los requisitos del sistema de Horizon Client. Consulte [Requisitos del sistema](#).
- Si aún no configuró el dispositivo cliente, hágalo. Consulte la guía del usuario del fabricante del dispositivo.

Procedimiento

- 1 Abra la aplicación Microsoft Store en su dispositivo y utilice su cuenta de Microsoft para iniciar sesión.
- 2 Busque la aplicación VMware Horizon Client.
- 3 Haga clic en **Instalar** o **Gratis** para instalar la aplicación VMware Horizon Client en su dispositivo.

Guardar información sobre los servidores recientes en la ventana de inicio de Horizon Client

Puede configurar Horizon Client para guardar un acceso directo a un servidor en la ventana de inicio después de conectarse a un servidor por primera vez.

Procedimiento

- 1 Toque el menú **Opción** situado en la esquina superior izquierda de la barra de menú de Horizon Client.

Si se conecta a un servidor, puede tocar el menú **Opción** situado en la esquina superior izquierda de la ventana de selección de aplicaciones y escritorios. Si se conecta a una aplicación o un escritorio remotos, puede tocar el botón **Opción**, situado en la ventana de la aplicación o del escritorio, y toque **Configuración**.
- 2 Expande la sección **Avanzado** y **active** la opción **Guardar información sobre servidores recientes**.

Si la opción está **desactivada**, Horizon Client no guardará los servidores recientes en la ventana de inicio.

Configurar las opciones de TLS/SSL avanzadas

Puede seleccionar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar la comunicación entre Horizon Client y los servidores de Horizon y entre Horizon Client y el agente en el escritorio remoto.

De forma predeterminada, TLSv1.0, TLSv1.1, y TLSv1.2 están habilitados. No se admiten SSL v2.0 y 3.0. La cadena de control del cifrado predeterminada es "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".

Si configura un protocolo de seguridad para Horizon Client que no está habilitado en el servidor de Horizon al que el cliente se conecta, se produce un error TLS/SSL y de conexión.

Si desea obtener información sobre la configuración de los protocolos de seguridad aceptados por las instancias del servidor de conexión, consulte el documento *Seguridad de View*.

Procedimiento

- 1 Toque el menú **Opciones** situado en la esquina superior izquierda de la barra de menús de Horizon Client y expanda la sección **Opciones SSL**.

- 2 Para habilitar o deshabilitar un protocolo de seguridad, toque el botón **Activado** o **Desactivado** bajo el nombre del protocolo de seguridad.

Puede habilitar y deshabilitar los protocolos TLSv1.0, TLSv1.1 y TLSv1.2. Los tres protocolos están habilitados de forma predeterminada.

NOTA: Para TLSv1.0 y TLSv1.2, es necesario que se habilite TLSv1.1. No puede deshabilitar TLSv1.1 si TLSv1.0 y TLSv1.2 están habilitados.

- 3 Para cambiar la cadena de control del cifrado, reemplace la cadena predeterminada y toque **Cambiar**.
- 4 (Opcional) Si necesita regresar a la cadena de control del cifrado, toque **Predeterminado**.

Los cambios se aplicarán la próxima vez que se conecte al servidor.

Configurar las opciones de VMware Blast

Puede configurar la decodificación H.264 y las opciones de condición de la red para las sesiones de aplicaciones y escritorios remotos que utilizan el protocolo de visualización VMware Blast.

No puede cambiar la opción de condición de la red tras iniciar sesión en un servidor. Puede configurar la decodificación H.264 antes o después de iniciar sesión en un servidor.

Prerequisitos

Esta función requiere la versión 7.0 de Horizon Agent o una versión posterior.

Procedimiento

- 1 Toque el menú **Opción** en la esquina superior izquierda de la barra de menús de Horizon Client y expanda la sección **VMware Blast**.

Si está conectado a un servidor, puede tocar el menú **Opción** en la esquina superior izquierda del escritorio y la ventana de selección de aplicaciones, expandir la sección **Protocolo** y seleccionar **VMware Blast**. No puede cambiar la opción de condición de la red tras iniciar sesión en un servidor.

2 Configure las opciones de descodificación y condición de la red.

| Opción | Acción |
|---|--|
| Permitir la descodificación H.264 | <p>Configure esta opción antes o después de conectarse al servidor de conexión, para permitir la descodificación H.264 en Horizon Client.</p> <p>Cuando está seleccionada esta opción (la opción predeterminada), Horizon Client utiliza la descodificación H.264 si el agente es compatible con la descodificación mediante hardware o software H.264. Si el agente no es compatible con la descodificación mediante hardware o software H.264, Horizon Client usa la descodificación JPG/PNG.</p> <p>Anule la selección de esta opción para usar la descodificación JPG o PNG.</p> |
| Seleccione la condición de su red para disfrutar de la mejor experiencia | <p>Solo puede configurar esta opción antes de conectarse al servidor de conexión. Seleccione una de las siguientes opciones de condición de la red:</p> <ul style="list-style-type: none"> ■ Excelente: Horizon Client utiliza únicamente redes TCP. Esta opción es ideal para un entorno de LAN. ■ Normal (predeterminado): Horizon Client trabaja en modo mixto. En el modo mixto, Horizon Client usa redes TCP al conectarse al servidor y utiliza Blast Extreme Adaptive Transport (BEAT) si el agente y la puerta de enlace de seguridad de Blast (si estuviese habilitada) admiten la conectividad con BEAT. Esta es la opción predeterminada. ■ Deficiente: Horizon Client utiliza únicamente las redes BEAT si el servidor del túnel de BEAT está habilitado en el servidor. De lo contrario, cambia a modo mixto. <p>NOTA: En Horizon 7, versión 7.1 y versiones anteriores, las instancias del servidor de conexión y del servidor de seguridad no son compatibles con el servidor del túnel de BEAT. Unified Access Gateway 2.9 y versiones posteriores son compatibles con el servidor del túnel de BEAT.</p> <p>La puerta de enlace de seguridad de Blast para las instancias del servidor de conexión y del servidor de seguridad no son compatibles con las redes de BEAT.</p> |

Mostrar la ayuda de Horizon Client

Para acceder al sistema de ayuda desde la aplicación Horizon Client, toque el menú **Opción** situado en la esquina superior izquierda de la barra de menús, seleccione el icono de información (!) y toque el vínculo de **Ayuda en línea**. También puede mostrar el sistema de ayuda después de conectarse a un servidor o iniciar sesión en una aplicación o un escritorio remotos.

El sistema de ayuda utiliza las funciones de su navegador web y otras opciones para ayudarle a acceder a la información del producto. Puede buscar contenido en la ayuda con consultas que contengan comillas, caracteres comodín y operadores booleanos.

Administrar las conexiones de las aplicaciones y los escritorios remotos

3

Puede utilizar Horizon Client para conectarse a un servidor e iniciar sesión en aplicaciones y escritorios remotos.

Según el modo en que un administrador configure las directivas para los escritorios remotos, los usuarios finales podrán realizar varias operaciones en los escritorios.

Este capítulo cubre los siguientes temas:

- [Configurar el modo de comprobación del certificado en Horizon Client](#)
- [Seleccionar un protocolo de visualización](#)
- [Conectarse a una aplicación o escritorio remotos](#)
- [Deshabilitar Windows Hello en Horizon Client](#)
- [Anclar una aplicación o un escritorio remotos a la pantalla Inicio](#)
- [Desconectarse de una aplicación o un escritorio remotos](#)
- [Cerrar sesión en un escritorio remoto](#)

Configurar el modo de comprobación del certificado en Horizon Client

Los administradores y, en ocasiones, los usuarios finales pueden configurar si las conexiones de cliente se rechazan en caso de que se produzca un error en una o varias comprobaciones de los certificados del servidor.

La comprobación del certificado se aplica a las conexiones SSL entre el servidor de conexión y Horizon Client. La verificación de los certificados incluye las siguientes comprobaciones:

- ¿Se revocó el certificado?
- ¿El certificado persigue otro objetivo que no sea verificar la identidad del remitente y el cifrado de las comunicaciones del servidor? Es decir, ¿es el tipo de certificado correcto?
- ¿Expiró el certificado o solo será válido en el futuro? Es decir, ¿el certificado es válido según el reloj del equipo?

- ¿El nombre común del certificado coincide con el nombre de host del servidor que lo envía? Se produce un error de coincidencia cuando un equilibrador de carga redirecciona Horizon Client a un servidor que tiene un certificado que no coincide con el nombre de host introducido en Horizon Client. También puede producirse un error de coincidencia si introduce una dirección IP distinta al nombre de host en el cliente.
- ¿El certificado está firmado por una entidad de certificación desconocida o que no es de confianza? Los certificados autofirmados no son certificados de confianza.

Para superar esta comprobación, la cadena de confianza del certificado debe especificar la raíz en el almacén de certificados local del dispositivo.

Puede establecer el modo de comprobación del certificado si su administrador lo ha permitido. En la ventana de inicio de Horizon Client, toque el menú **Opciones** situado en la esquina superior izquierda de la barra de menús y expanda la sección **Modo de comprobación del certificado**. Tiene las siguientes opciones:

- **No conectarse nunca a servidores que no sean de confianza.** Si se produce un error en las comprobaciones de los certificados, el cliente no puede conectarse al servidor. Aparece un mensaje de error con las comprobaciones que han fallado.
- **Intentar conectarme independientemente de los certificados de identidad de los servidores.** Esta opción significa que no se ha llevado a cabo ninguna comprobación del certificado.

Dado que el mecanismo del certificado utilizado en las aplicaciones de Windows 10 UWP está más limitado que para las aplicaciones de escritorio de Windows, es posible que se produzca un error en la comprobación del certificado incluso si el nivel está configurado en **Intentar conectarme independientemente de los certificados de identidad de los servidores**. Por ejemplo, es posible que aparezca un error en la comprobación del certificado debido a los siguientes motivos:

- El certificado firmado por la entidad de certificación raíz fue revocado.
- El certificado firmado por la entidad de certificación intermedia fue revocado.
- El certificado es válido, pero la entidad de certificación intermedia fue revocada.
- El certificado de la cadena incluye una extensión desconocida que está marcada como "crítica".

Seleccionar un protocolo de visualización

Puede seleccionar el protocolo de visualización que utilizará Horizon Client cuando se conecte a una aplicación o un escritorio remotos.

Procedimiento

- 1 En Horizon Client, toque el menú **Opción** situado en la esquina superior izquierda de la barra de menús de Horizon Client.

Si se conecta a un servidor, puede tocar el menú **Opción** situado en la esquina superior izquierda de la ventana de selección de aplicaciones y escritorios.

- 2 Expanda la sección **Protocolo** y seleccione el protocolo de visualización que se va a utilizar.

VMware Blast requiere Horizon Agent 7.0 o una versión posterior.

- 3 (Opcional) Si seleccionó **VMware Blast**, habilite o deshabilite la codificación H.264. Para ello, toque la opción **Permitir la decodificación H.264** y **actívela** o **desactívela**.

Cuando esta opción está **activada**, Horizon Client permite la codificación H.264 si Horizon Agent es compatible con la codificación H.264 para la aplicación o el escritorio remotos. Si Horizon Agent no es compatible con la codificación H.264 para la aplicación o el escritorio remotos, Horizon Client utiliza la codificación JPEG/PNG en su lugar. Cuando esta opción está **desactivada** (esta es la configuración predeterminada), la codificación H.264 no está permitida y Horizon Client siempre utiliza la codificación JPEG/PNG.

La próxima vez que se conecte a una aplicación o un escritorio remotos, Horizon Client utilizará el protocolo de visualización seleccionado. No puede cambiar el protocolo de visualización para una sesión conectada actualmente.

Si se conecta a una aplicación o un escritorio remotos que no sean compatibles con el protocolo de visualización seleccionado, Horizon Client mostrará un mensaje de error.

Conectarse a una aplicación o escritorio remotos

Para conectarse a una aplicación o a un escritorio remotos, debe proporcionar el nombre de un servidor y las credenciales de la cuenta de usuario.

Para usar aplicaciones remotas, debe conectarse a la versión 6.0 o posterior del servidor de conexión.

NOTA: Antes de proporcionar acceso a los usuarios finales a sus escritorios remotos, compruebe que pueda iniciar sesión en un escritorio remoto desde un dispositivo cliente.

Prerequisitos

- 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.
- Realice las tareas administrativas descritas en [Preparar el servidor de conexión para Horizon Client](#).
- Si se encuentra fuera de la red corporativa y no utiliza un servidor de seguridad para acceder a la aplicación o escritorio remoto, compruebe que el dispositivo cliente está configurado para usar una conexión VPN y actívela.

IMPORTANTE: En la mayoría de los casos, utilice un servidor de seguridad en lugar de una VPN.

Si la compañía tiene una red inalámbrica interna para proporcionar acceso enrutable a los escritorios remotos que el dispositivo puede usar, no tiene que configurar ningún servidor de seguridad ni ninguna conexión VPN.

- Compruebe que tiene un nombre de dominio completo (FQDN) del servidor que proporciona acceso a la aplicación o al escritorio remotos. Los nombres de los servidores no admiten guiones bajos (_). Si el puerto no es 443, también necesita el número de puerto.
- Configure el modo de comprobación del certificado para el certificado SSL que presenta el servidor de conexión. Consulte [Configurar el modo de comprobación del certificado en Horizon Client](#).
- Si tiene pensado utilizar Windows Hello como método de autenticación, compruebe que esté configurado en el dispositivo de Windows 10. Para conocer todos los requisitos, consulte [Requisitos de la autenticación de Windows Hello](#).

Procedimiento

- 1 Si se requiere una conexión VPN, active la VPN.
- 2 Toque la aplicación **VMware Horizon Client**.
- 3 Conéctese a un servidor.

| Opción | Descripción |
|------------------------------------|--|
| Conectarse a un servidor nuevo | Toque Agregar servidor , introduzca el nombre de un servidor y, a continuación, toque Conectar . |
| Conectarse a un servidor existente | Toque el icono del servidor en la ventana de inicio. |

Las conexiones entre Horizon Client y los servidores siempre usan SSL. El puerto predeterminado para las conexiones SSL es 443. Si el servidor no está configurado para que utilice el puerto predeterminado, use el formato que se muestra en este ejemplo: **view.company.com:1443**.

- 4 Si se le solicita las credenciales RSA SecurID o las credenciales de la autenticación RADIUS, introduzca el nombre de usuario, el código de acceso y toque **Inicio de sesión**.

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

- 5 Si se le solicita un nombre de usuario y una contraseña, introduzca las credenciales de Active Directory.
 - a Escriba el nombre y la contraseña de un usuario que tenga autorización para utilizar al menos un grupo de escritorios o de aplicaciones.
 - b Seleccione un dominio.
 - c (Opcional) Si el botón **Habilitar Windows Hello** está disponible, tóquelo para usar el método de autenticación con Windows Hello.

El botón **Habilitar Windows Hello** está habilitado solo si la autenticación biométrica está habilitada en el servidor y no se autenticó previamente con Windows Hello.

- d Toque **Inicio de sesión**.

Si Windows Hello está habilitado e inicia sesión por primera vez, las credenciales de Active Directory se almacenan de forma segura en su dispositivo Windows 10 para que pueda utilizarlas en el futuro.

- 6 Si se le solicita la autenticación con Windows Hello, utilice la huella digital, cara, iris o PIN para autenticarse.

Si no desea utilizar el método de autenticación con Windows Hello, haga clic en **Cancelar** para introducir un nombre de usuario y una contraseña.

- 7 Toque la aplicación o el escritorio al que desee conectarse.

Se iniciará la aplicación o el escritorio remotos.

Deshabilitar Windows Hello en Horizon Client

Puede deshabilitar Windows Hello en un servidor en el que inició sesión anteriormente mediante el proceso de autenticación con Windows Hello.

Prerequisitos

Compruebe que aparezca un acceso directo para el servidor en la ventana de inicio de Horizon Client. Para configurar Horizon Client para que guarde los accesos directos del servidor, consulte [Guardar información sobre los servidores recientes en la ventana de inicio de Horizon Client](#).

Procedimiento

- 1 En la ventana de inicio de Horizon Client, mantenga pulsado el acceso directo del servidor.
- 2 Cuando aparezca el menú contextual, toque **Cerrar la sesión del servidor**.

La próxima vez que se conecte al servidor, puede introducir un nombre de usuario y una contraseña y el botón de **Habilitar Windows Hello** aparecerá en el cuadro de diálogo de inicio de sesión del servidor.

Anclar una aplicación o un escritorio remotos a la pantalla Inicio

Puede anclar una aplicación o un escritorio a la pantalla Inicio al hacer clic con el botón secundario en la aplicación o el escritorio en la ventana de selección de aplicaciones y de escritorios y seleccionar a continuación **Anclar a Inicio** en el menú contextual.

Si no inició sesión en el servidor en el momento en el que toca la aplicación o el escritorio remotos en la pantalla Inicio, Horizon Client le solicita que se autentique en el servidor antes de iniciar la aplicación o el escritorio remotos. Si ya inició sesión en el servidor, la aplicación o el escritorio remotos se inicia y no es necesario que se autentique en el servidor.

Desconectarse de una aplicación o un escritorio remotos

Puede desconectarse de un escritorio remoto sin cerrar sesión, por lo que las aplicaciones seguirán abiertas en el escritorio remoto. También puede desconectarse de una aplicación remota, por lo que dicha aplicación seguirá abierta.

Cuando tiene una sesión iniciada en la aplicación o el escritorio remotos, puede desconectarse tocando el botón **Desconectar** situado en la ventana de la aplicación o del escritorio y, a continuación, tocando **Desconectar**.

NOTA: Horizon Administrator puede configurar el escritorio para cerrar sesión de forma automática cuando se desconecte. En ese caso, se detendrán todos los programas abiertos en el escritorio.

Cerrar sesión en un escritorio remoto

Si está conectado actualmente a un escritorio remoto e inició sesión en él, puede utilizar el menú **Inicio** de Windows para cerrar sesión.

También puede cerrar sesión tocando el botón **Ctrl+Alt+Supr** de la ventana del escritorio o de la aplicación y seleccionado la opción **Cerrar sesión**.

Todos los archivos sin guardar que estén abiertos en el escritorio remoto se cerrarán durante este procedimiento. Si se desconecta de un escritorio remoto sin cerrar sesión, las aplicaciones seguirán abiertas en el escritorio remoto.

Usar una aplicación o un escritorio remotos

4

Horizon Client incluye funciones comunes en otras aplicaciones de Windows 10 UWP, así como funciones específicas de aplicaciones y escritorios remotos.

Este capítulo cubre los siguientes temas:

- [Matriz de compatibilidad de funciones](#)
- [Utilizar el modo de pantalla completa](#)
- [Ajustar la resolución de pantalla para aplicaciones y escritorios remotos](#)
- [Habilitar la función Zoom local](#)
- [Evitar que se bloquee la pantalla](#)
- [Utilizar la barra lateral](#)
- [Ayudas de navegación y gestos](#)
- [Multitarea](#)
- [Utilizar Horizon Client con un Microsoft Display Dock](#)
- [Copiar y pegar texto e imágenes](#)
- [Guardar documentos en una aplicación remota](#)
- [Internacionalización](#)

Matriz de compatibilidad de funciones

Algunas funciones son compatibles con un tipo de cliente, pero no lo son con otros. Por ejemplo, el acceso USB es compatible con Horizon Client para Windows pero no con Horizon Client para Windows 10 UWP.

Tabla 4-1. Funciones compatibles con los escritorios de Windows para Horizon Client para Windows 10 UWP

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

Los escritorios de Windows 10 necesitan la versión de View Agent 6.2 o Horizon Agent 7.0, o una versión posterior de dichos productos. Los escritorios de Windows Server 2012 R2 necesitan View Agent 6.1 o Horizon Agent 7.0, o una versión posterior de dichos productos. Los escritorios de Windows Server 2016 necesitan Horizon Agent 7.0.2 o una versión posterior.

IMPORTANTE: View Agent 6.1 y Horizon Agent 7.0 y las versiones posteriores de ambos productos no son compatibles con los escritorios de Windows XP y Windows Vista. View Agent 6.0.2 es la versión más reciente de View compatible con estos sistemas operativos invitados. Los clientes que tengan un acuerdo de compatibilidad ampliado con Microsoft para Windows XP y Vista y un acuerdo de compatibilidad ampliado con VMware para estos sistemas operativos invitados pueden implementar la versión 6.0.2 de View Agent de sus escritorios de Windows XP y Vista con el servidor de conexión 6.1.

Para ver las descripciones de estas funciones y sus limitaciones, consulte el documento *Planificación de arquitectura de View*.

Compatibilidad de funciones para escritorios publicados 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 simultáneas en un host RDS. Un host RDS puede ser un equipo físico o una máquina virtual.

En la tabla siguiente se incluyen solo filas con las funciones que son compatibles. Algunas funciones son compatibles con hosts RDS de máquinas virtuales, pero no lo son no con hosts RDS de máquinas físicas.

Tabla 4-2. Funciones compatibles con hosts RDS con View Agent 6.0.x o versiones posteriores, o bien Horizon Agent 7.0 o versiones posteriores instalados

| Función | Host RDS con Windows Server 2008 R2 | Host RDS con Windows Server 2012 | Host RDS con Windows Server 2016 |
|--|--|--|---|
| RSA SecurID o RADIUS | X | X | Horizon Agent 7.0.2 y posterior |
| Single Sign-On | X | X | Horizon Agent 7.0.2 y posterior |
| Protocolo de visualización de VMware Blast | Horizon Agent 7.0 y posterior | Horizon Agent 7.0 y posterior | Horizon Agent 7.0.2 y posterior |
| Protocolo de visualización PCoIP | X | X | Horizon Agent 7.0.2 y posterior |
| Impresión según ubicación | View Agent 6.0.1 y posterior (solo máquinas virtuales) | View Agent 6.0.1 y posterior (solo máquinas virtuales) | Horizon Agent 7.0.2 y posterior (solo máquinas virtuales) |

Para obtener información sobre qué service pack o qué ediciones de cada sistema operativo invitado son compatibles, consulte el tema sobre sistemas operativos compatibles con View Agent en el documento de instalación de View 5.x o 6.x. Consulte el tema sobre sistemas operativos compatibles con Horizon Agent en el documento de instalación de Horizon 7.

Utilizar el modo de pantalla completa

Puede mostrar aplicaciones y escritorios remotos en pantalla completa o con el modo de ventana en un dispositivo Surface Pro 4 o Surface Book. El modo de pantalla completa está habilitado de forma predeterminada.

Para activar o desactivar el modo de pantalla completa, toque el botón **Opción** de la ventana de la aplicación o el escritorio remotos y seleccione **Pantalla completa** después de iniciar sesión en una aplicación o un escritorio remotos.

Ajustar la resolución de pantalla para aplicaciones y escritorios remotos

Si su tablet tiene una pantalla de alta resolución, es posible que tenga problemas para leer los iconos y el texto en una aplicación o un escritorio remotos. Puede reducir la resolución de pantalla para mejorar la legibilidad.

Para modificar la resolución de pantalla antes de iniciar sesión en una aplicación o un escritorio remotos, toque el menú **Opción** situado en la esquina superior izquierda de la barra de menús de Horizon Client, expanda la sección **Modo de resolución** y seleccione una de las opciones de resolución.

También puede cambiar la resolución de pantalla después de conectarse a un servidor o iniciar sesión en una aplicación o un escritorio remotos.

Habilitar la función Zoom local

Al habilitar la función Zoom local, puede juntar los dedos o separarlos en la pantalla táctil para ampliar o reducir el zoom en la aplicación o el escritorio remotos.

En los escritorios de máquinas virtuales con Windows 8 y Windows 10, y en aplicaciones y escritorios con Windows Server 2012 R2 y Windows Server 2016 RDS no puede juntar los dedos y separarlos para ampliar o reducir el zoom, a menos que habilite la función Zoom local.

Procedimiento

- 1 Conéctese a una aplicación o un escritorio remotos.
- 2 Toque el botón **Opción** de la ventana de la aplicación o el escritorio y seleccione **Configuración**.
- 3 Expande la sección **Avanzado** y **active** la opción **Zoom local**.

Si la opción está **desactivada**, no podrá utilizar esta función en la aplicación ni el escritorio remotos. Esta opción está **activada** de forma predeterminada.

Evitar que se bloquee la pantalla

Cuando un dispositivo con Windows 10 permanece inactivo durante cierto tiempo, es posible que la pantalla se atenúe, se active el bloqueo de pantalla o esta se apague para ahorrar batería. Puede establecer una opción con el fin de evitar que la pantalla se bloquee para una aplicación o un escritorio remotos.

NOTA: El tiempo que los dispositivos con Windows 10 reproducen contenido de audio o de vídeo se registra como tiempo de inactividad. La cantidad de tiempo de inactividad necesaria para que se bloquee la pantalla varía en función de la configuración de usuario del dispositivo.

Procedimiento

- 1 Conéctese a una aplicación o un escritorio remotos.
- 2 Toque el botón **Opción** de la ventana de la aplicación o el escritorio y seleccione **Configuración**.
- 3 Expanda la sección **Avanzado** y active la opción **Pantalla siempre activa**.

Si la opción está **desactivada**, es posible que la pantalla se bloquee.

Utilizar la barra lateral

Después de conectarse a una aplicación o un escritorio remotos, puede utilizar la barra lateral para abrir aplicaciones y escritorios diferentes.

Tabla 4-3. Acciones de la barra lateral

| Acción | Descripción |
|---|--|
| Mostrar la barra lateral | Toque el botón Opción de la ventana de la aplicación o el escritorio remotos y seleccione Barra lateral . |
| Ocultar la barra lateral | Toque cualquier parte dentro de la ventana de la aplicación o el escritorio remotos. |
| Abrir una aplicación o un escritorio remotos | Toque el nombre de la aplicación o el escritorio remotos en la barra lateral. |
| Buscar una aplicación o un escritorio remotos | Escriba el nombre de la aplicación o el escritorio remotos en el cuadro Buscar . Para abrir la aplicación o el escritorio remotos, toque su nombre en los resultados de búsqueda. |

Ayudas de navegación y gestos

VMware creó ayudas de interacción de usuario para mejorar la navegación convencional por los elementos de la interfaz de usuario de Windows.

Hacer clic

Como en otras aplicaciones, puede tocar para hacer clic en un elemento de la interfaz de usuario. También puede utilizar un mouse externo.

Hacer clic con el botón secundario

Las siguientes opciones están disponibles para hacer clic con el botón secundario:

- Utilice un mouse externo para hacer clic con el botón secundario.
- En un panel táctil, toque con dos dedos.
- Mantenga pulsada una pantalla táctil hasta que aparezca el menú del botón secundario.

Ampliar o reducir el zoom

En una pantalla táctil, junte los dedos o sepárelos para ampliar o reducir el zoom.

En los sistemas operativos compatibles con la entrada táctil, la opción de ampliar o reducir el zoom en una pantalla táctil solo funciona si habilita la función Zoom local. Consulte [Habilitar la función Zoom local](#). Windows 8, Windows 8.1, Windows 10, Windows Server 2012 y Windows Server 2016 son compatibles con la entrada táctil.

Desplazamiento y barras de desplazamiento

Las siguientes opciones están disponibles para el desplazamiento vertical:

- Utilice un mouse externo para desplazarse.
- Mantenga pulsado un panel táctil con el pulgar y, a continuación, desplácese hacia abajo con dos dedos.
- Toque una pantalla táctil con dos dedos, y a continuación, arrastre los dedos para desplazarse o utilice un dedo para arrastrar la barra de desplazamiento. El texto que tiene pulsado se mueve en la misma dirección que los dedos.

Sonido, música y vídeo

Si el sonido está activado en el dispositivo, puede reproducir audio y vídeo en un escritorio remoto.

Ctrl+Alt+Supr

Como la combinación de teclas de Windows Ctrl+Alt+Supr no se admite en aplicaciones y escritorios remotos, deberá tocar el botón **Ctrl+Alt+Supr** de la ventana de la aplicación o el escritorio remotos en su lugar.

Multitarea

Puede cambiar entre Horizon Client y otras aplicaciones sin perder la conexión a la aplicación o al escritorio remotos.

Puede cambiar el tamaño de la aplicación Horizon Client para que se muestre en una parte de la pantalla junto a otra aplicación.

Si una sesión permanece inactiva durante un tiempo, aparecerá un mensaje antes de que se agote el tiempo de espera de la sesión que le preguntará si desea mantener la sesión activa. Toque cualquier parte o haga clic en cualquier lugar de la pantalla, o bien pulse una tecla del teclado para que la sesión permanezca activa. Si transcurrió suficiente tiempo como para que la conexión a la aplicación o el escritorio remotos se pierda, Horizon Client vuelve a la ventana de selección de aplicaciones y escritorios, y le indica que vuelva a establecer conexión.

Utilizar Horizon Client con un Microsoft Display Dock

La aplicación VMware Horizon Client funciona con Continuum para Windows 10 Mobile. Puede utilizar un Microsoft Display Dock para conectar su smartphone con Windows 10 a una pantalla y un mouse externos. Esta función le permite utilizar Horizon Client tal y como lo haría en un equipo de escritorio.

Copiar y pegar texto e imágenes

De forma predeterminada, puede copiar y pegar texto desde su sistema cliente a una aplicación o escritorio remotos. Si un administrador de Horizon habilita la función, también puede copiar y pegar texto desde una aplicación o escritorio remotos a su sistema cliente o entre dos aplicaciones o escritorios remotos.

Solo puede copiar y pegar texto sin formato. No se admiten imágenes y RTF (formato de texto enriquecido).

Horizon Administrator puede establecer esta función para que sea posible realizar estas operaciones desde su sistema cliente a una aplicación o un escritorio remotos, así como desde una aplicación o un escritorio remotos a su sistema cliente, o ninguna o ambas posibilidades.

Los administradores de Horizon pueden configurar la capacidad de copiar y pegar; para ello, configuran una directiva de grupo que pertenece a Horizon Agent. En función de la versión del agente y del Horizon Server, los administradores también pueden usar directivas de grupo para restringir los formatos del portapapeles durante las operaciones de copiar y pegar, o bien usar directivas inteligentes para controlar el comportamiento de estas operaciones en escritorios remotos. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

El portapapeles puede acumular hasta 64 K de datos para operaciones de copiado y pegado. Si intenta copiar un tamaño mayor que el máximo permitido para el portapapeles, el texto aparecerá truncado.

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

Guardar documentos en una aplicación remota

Con determinadas aplicaciones remotas como, por ejemplo, Microsoft Word o WordPad, puede crear y guardar documentos. La ubicación en la que se guardan estos documentos depende del entorno de red de su empresa. Por ejemplo, los documentos se pueden guardar en un recurso compartido principal en su equipo local.

Los administradores pueden utilizar un archivo de plantilla ADMX para establecer una directiva de grupo que especifique la ubicación en la que se guardarán los documentos. Esta directiva se denomina **Establecer directorio principal de usuario de Servicios de Escritorio remoto**. Para obtener más información, consulte el documento *Configurar funciones de escritorios remotos en Horizon 7*.

Internacionalización

La interfaz de usuario y la documentación están disponibles en inglés, japonés, francés, alemán, chino simplificado, chino tradicional, coreano y español. También es posible introducir caracteres de esos idiomas.

Solucionar problemas relacionados con Horizon Client

5

Puede solucionar la mayoría de los problemas relacionados con Horizon Client restableciendo el escritorio o volviendo a instalar la aplicación.

También puede habilitar la recopilación de registros y enviar archivos de registro a VMware para solucionar problemas.

Este capítulo cubre los siguientes temas:

- [Horizon Client deja de responder o el escritorio remoto se bloquea](#)
- [Restablecer una aplicación o un escritorio remotos](#)
- [Desinstalar la aplicación VMware Horizon Client](#)
- [Conexión a un servidor en el modo Workspace ONE](#)
- [Recopilar registros para enviarlos al equipo de soporte técnico](#)

Horizon Client deja de responder o el escritorio remoto se bloquea

Si la ventana se bloquea, en primer lugar, intente restablecer el sistema operativo del escritorio remoto.

Problema

Horizon Client no funciona o se cierra de forma inesperada repetidas veces o el escritorio remoto se bloquea.

Origen

Asumiendo que los servidores de Horizon están configurados correctamente y que los firewalls adyacentes tienen los puertos correctos abiertos, normalmente se producen otros problemas que están relacionados con Horizon Client en el dispositivo o con el sistema operativo invitado en el escritorio remoto.

Solución

- Si el sistema operativo del escritorio remoto se bloquea, use Horizon Client en el dispositivo para restablecer el escritorio.

Esta opción está disponible solo si Horizon Administrator habilitó esta función.

- Desinstale y vuelva a instalar la aplicación en el dispositivo.
- Si se encuentra con un error de conexión cuando intenta conectarse al servidor, es posible que necesite cambiar la configuración del proxy.

Restablecer una aplicación o un escritorio remotos

Si se conectó a una aplicación o un escritorio remotos e inició sesión en uno de ellos, puede tocar el botón **Desconectar** de la ventana de la aplicación o el escritorio y seleccionar **Restablecer** para restablecer la aplicación o el escritorio remotos.

El comando **Restablecer** solo está disponible si Horizon Administrator lo permitió y si el estado de la aplicación o el escritorio remotos permiten que se realice la acción.

Es posible que necesite restablecer una aplicación o un escritorio remotos si el sistema operativo del escritorio o de la aplicación dejan de responder.

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 una aplicación remota, se cierran todas las aplicaciones remotas, así como todas las sesiones de las aplicaciones remotas. Los cambios que no se hayan guardado en las aplicaciones remotas se perderán.

Desinstalar la aplicación VMware Horizon Client

Puede desinstalar y volver a instalar la aplicación VMware Horizon Client del dispositivo con Windows 10 UWP para solucionar problemas relacionados con Horizon Client.

La desinstalación de Horizon Client se realiza tal y como desinstalaría cualquier aplicación de Windows 10 UWP.

Procedimiento

- 1 En su dispositivo, busque la aplicación VMware Horizon Client.
- 2 Haga clic con el botón secundario en el icono **VMware Horizon Client** y toque **Desinstalar**.

Qué hacer a continuación

Vuelva a instalar la aplicación VMware Horizon Client. Consulte [Instalar o actualizar Horizon Client para Windows 10 UWP](#).

Conexión a un servidor en el modo Workspace ONE

Si no puede conectarse a un servidor directamente a través de Horizon Client si las autorizaciones de aplicaciones y escritorios no están visibles en Horizon Client, es posible que el modo Workspace ONE esté habilitado en el servidor.

Problema

- Cuando intente conectarse al servidor directamente a través de Horizon Client, Horizon Client le redireccionará al portal de Workspace ONE.
- Al abrir un escritorio o aplicación mediante un URI o un acceso directo o al abrir un archivo local a través de la asociación de archivos, la solicitud le redireccionará al portal de Workspace ONE para autenticarse.
- Después de que abra un escritorio o una aplicación a través de Workspace ONE y se inicie Horizon Client, no podrá ver ni abrir otros escritorios o aplicaciones remotos autorizados en Horizon Client.

Origen

A partir de la versión 7.2 de Horizon 7, un administrador podrá habilitar el modo Workspace ONE en una instancia del servidor de conexión. Este comportamiento es normal cuando se habilita el modo Workspace ONE en una instancia del servidor de conexión.

Solución

Utilice Workspace ONE para conectarse a un servidor habilitado de Workspace ONE y acceder a sus aplicaciones y escritorios remotos.

Recopilar registros para enviarlos al equipo de soporte técnico

Puede habilitar el registro y recopilar un paquete de registros para enviarlo al equipo de soporte técnico.

Para solucionar algunos problemas, es posible que se le solicite que recopile registros para enviarlos al equipo de soporte técnico. El registro afectará al rendimiento de Horizon Client si se utiliza una sesión de túnel segura para conectarse al escritorio remoto. No olvide desactivar la función de registro avanzado cuando no se necesite el registro.

Prerequisitos

Póngase en contacto con el equipo de soporte técnico de VMware para determinar el lugar al que se enviarán los archivos de registro que recopile.

Procedimiento

- 1 En Horizon Client, toque el menú **Opción** situado en la esquina superior izquierda de la barra de menús.

Si se conecta a un servidor, puede tocar el menú **Opción** situado en la esquina superior izquierda de la ventana de selección de aplicaciones y escritorios. Si se conecta a una aplicación o un escritorio remotos, puede tocar el botón **Opción**, situado en la ventana de la aplicación o del escritorio, y toque **Configuración**.

- 2 Expande la sección **Registro** y active la opción **Habilitar registro avanzado**.

- 3 Toque **Recopilar información de soporte técnico**, desplácese hasta la ubicación del dispositivo en la que se almacenarán los archivos de registro, seleccione el directorio y toque **Seleccionar carpeta**.

Por ejemplo, para una mayor comodidad, es posible que seleccione el elemento **Escritorio** para guardar los registros en una carpeta de su escritorio local.

Horizon Client crea una carpeta con el nombre *vmware-view-logs-marca de hora* en la ubicación especificada.

- 4 (Opcional) Para crear un archivo `.zip` de la carpeta de registros antes de enviarla al equipo de soporte técnico, haga clic con el botón secundario en la carpeta y seleccione **Enviar a > Carpeta comprimida (en zip)**.

Qué hacer a continuación

Envíe los registros al equipo de soporte técnico de VMware.