Using VMware Horizon Client for Windows 10 UWP

Horizon Client 4.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002509-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

Using VMware Horizon Client for Windows 10 UWP

1

Using VMware Horizon Client for Windows 10 UWP provides information about installing and using VMware Horizon® Client™ software on a Windows 10 device to connect to a remote desktop or application in the data center.

This information is intended for administrators who must set up a Horizon deployment that includes Windows 10 client devices. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

Setup and Installation 2

Setting up a Horizon deployment for Windows 10 UWP clients involves using certain Connection Server settings, meeting the system requirements for Horizon servers and Windows 10 device clients, and installing the VMware Horizon Client Windows app.

This chapter includes the following topics:

System Requirements

The device on which you install Horizon Client, and the peripherals it uses, must meet certain system requirements.

Operating systems

- Windows 10 Current Branch (CB) version 1703 (Creators Update)
- Windows 10 Current Branch (CB) version 1607 (Anniversary Update)
- Windows 10 Current Branch for Business (CBB) version 1607 (Anniversary Update)
- Windows 10 Long-Term Servicing Branch (LTSB) version 1607 (Anniversary Update)

Windows Hello authentication

See "Windows Hello Authentication Requirements," on page 8.

Connection Server, Security Server, and Horizon Agent	Latest maintenance release of View 6.x and later releases. VMware recommends that you use a security server or Unified Access Gateway appliance so that your device does not require a VPN connection.
Display protocol for remote desktops and applications	■ VMware Blast (requires Horizon Agent 7.0 or later) ■ PCoIP

Windows Hello Authentication Requirements

To use Windows Hello to authenticate in Horizon Client, you must meet certain requirements.

Windows 10 device models	Any Windows 10 device that supports Windows Hello, such as Microsoft Surface Pro 4.
Operating system requirements	Set up Windows Hello in **Settings > Accounts > Sign-in options**.
Connection Server requirements	■ Horizon 6 version 6.2 or a later release. ■ Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the *View Administration* document.
Horizon Client requirements	Enable Windows Hello by tapping **Enable Windows Hello** on the server login dialog box. After you successfully log in, your Active Directory credentials are stored securely on the Windows 10 device. **Enable Windows Hello** is shown the first time you log in and does not appear after Windows Hello authentication is enabled.

You can use Windows Hello authentication as part of two-factor authentication with RSA SecurID and RADIUS authentication.

Preparing Connection Server for Horizon Client

Administrators must perform specific tasks to enable end users to connect to remote desktops and applications.

Before end users can connect to Connection Server or a security server and access a remote desktop or application, you must configure certain pool settings and security settings:

- If you plan to use Unified Access Gateway, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring Unified Access Gateway* document. Unified Access Gateway appliances fulfill the same role that was previously played by only security servers.
- If you are using a security server, verify that you are using the latest maintenance releases of Connection Server 5.3.x and Security Server 5.3.x or later releases. For more information, see the *View Installation* document.
- Verify that a desktop or application pool has been created and that the user account that you plan to use is entitled to access the pool. For information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.
- To use two-factor authentication with Horizon Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in the *View Administration* document.

- To use Windows Hello authentication, you must enable biometric authentication in Connection Server. Biometric authentication is supported in Horizon 6 version 6.2 and later. For more information, see the *View Administration* document.

Supported Desktop Operating Systems

Administrators create virtual machines with a guest operating system and install agent software in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported Windows guest operating systems, see "Supported Operating Systems for Horizon Agent" in the *View Installation* document.

Install or Upgrade Horizon Client for Windows 10 UWP

The VMware Horizon Client app is a Windows 10 UWP app, and you install just as you do other Windows 10 UWP apps.

Prerequisites

- Verify that your client device meets the system requirements for Horizon Client. See "System Requirements," on page 7.
- If you have not already set up the client device, do so. See the manufacturer's user's guide for your device.

Procedure

1. Open the Microsoft Store app on your device and use your Microsoft account to log in.
2. Search for the VMware Horizon Client app.
3. Click **Install** or **Free** to install the VMware Horizon Client app on your device.

Save Information About Recent Servers on the Horizon Client Home Window

You can configure Horizon Client to save a server shortcut on the home window after you connect to a server for the first time.

Procedure

1. Tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.

   If you are connected to a server, you can tap the **Option** menu in the upper-left corner of the desktop and application selection window. If you are connected to a remote desktop or application, you can tap the **Option** button in the desktop or application window and tap **Settings**.
2. Expand the **Advanced** section and tap to toggle the **Save information about recent servers** option to **On**.

   If the option is set to **Off**, Horizon Client does not save recent servers on the home window.

Configure Advanced TLS/SSL Options

You can select the security protocols and cryptographic algorithms that are used to encrypt communications between Horizon Client and Horizon servers and between Horizon Client and the agent in the remote desktop.

By default, TLSv1.0, TLSv1.1, and TLSv1.2 are enabled. SSL v2.0 and 3.0 are not supported. The default cipher control string is "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".

If you configure a security protocol for Horizon Client that is not enabled on the Horizon server to which the client connects, a TLS/SSL error occurs and the connection fails.

For information about configuring the security protocols that are accepted by Connection Server instances, see the *View Security* document.

Procedure

1 Tap the **Option** menu in the upper-left corner of the Horizon Client menu bar and expand the **SSL Options** section.

2 To enable or disable a security protocol, tap the **On** or **Off** toggle under the security protocol name.

You can enable and disable the TLSv1.0, TLSv1.1, and TLSv1.2 protocols. All three protocols are enabled by default.

Note TLSv1.0 and TLSv1.2 require TLSv1.1 to be enabled. You cannot disable TLSv1.1 if TLSv1.0 and TLSv1.2 are enabled.

3 To change the cipher control string, replace the default string and tap **Change**.

4 (Optional) If you need to revert to the default cipher control string, tap **Default**.

Your changes take effect the next time you connect to the server.

Configure VMware Blast Options

You can configure H.264 decoding and network condition options for remote desktop and application sessions that use the VMware Blast display protocol.

You cannot change the network condition option after you log in to a server. You can configure H.264 decoding before or after you log in to a server.

Prerequisites

This feature requires Horizon Agent 7.0 or later.

Procedure

1 Tap the **Option** menu in the upper-left corner of the Horizon Client menu bar and expand the **VMware Blast** section.

If you are connected to a server, you can tap the **Option** menu in the upper-left corner of the desktop and application selection window, expand the **Protocol** section, and select **VMware Blast**. You cannot change the network condition option after you log in to a server.

2 Configure the decoding and network condition options.

Option	Action
Allow H.264 decoding	Configure this option, before or after connecting to Connection Server, to allow H.264 decoding in Horizon Client. When this option is selected (the default setting), Horizon Client uses H. 264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. Deselect this option to use JPG/PNG decoding.
Select your network condition for the best experience	You can only configure this option before connecting to Connection Server. Select one of the following network condition options: ■ **Excellent** - Horizon Client uses only TCP networking. This option is ideal for a LAN environment. ■ **Typical (default)** - Horizon Client works in mixed mode. In mixed mode, Horizon Client uses TCP networking when connecting to the server and uses Blast Extreme Adaptive Transport (BEAT) if the agent and Blast Security Gateway (if enabled) support BEAT connectivity. This option is the default setting. ■ **Poor** - Horizon Client uses only BEAT networking if the BEAT Tunnel Server is enabled on the server, otherwise it switches to mixed mode. **Note** In Horizon 7 version 7.1 and earlier, Connection Server and Security Server instances do not support the BEAT Tunnel Server. Unified Access Gateway 2.9 and later supports the BEAT Tunnel Server. Blast Security Gateway for Connection Server and Security Server instances do not support BEAT networking.

Displaying Help for Horizon Client

To access the help system from within the Horizon Client app, tap the **Option** menu in the upper-left corner of the menu bar, tap the information icon (**!**), and tap the link under **Online Help**. You can also display the help system after you connect to a server or log in to a remote desktop or application.

The help system uses features of your Web browser, as well as some additional capabilities, to help you access product information. You can search the help using queries that contain quotation marks, wildcards, and Boolean operators.

Managing Remote Desktop and Application Connections 3

You can use Horizon Client to connect to a server and log in to remote desktops and applications.

Depending on how an administrator configures policies for remote desktops, end users might be able to perform many operations on their desktops.

This chapter includes the following topics:

Setting the Certificate Checking Mode for Horizon Client

Administrators and sometimes end users can configure whether client connections are rejected if any or some server certificate checks fail.

Certificate checking occurs for SSL connections between Connection Server and Horizon Client. Certificate verification includes the following checks:

- Has the certificate been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

  To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

If your administrator has allowed it, you can set the certificate checking mode. On the Horizon Client home window, tap the **Option** menu in the upper-left corner of the menu bar and expand the **Certificate Checking Mode** section. You have the following choices:

- **Never connect to untrusted servers**. If any of the certificate checks fails, the client cannot connect to the server. An error message lists the checks that failed.
- **Attempt to connect regardless of server identity certificates**. This setting means that no certificate checking occurs.

Because the certificate mechanism used in Windows 10 UWP apps is more limited than for Windows desktop applications, the certification check can fail even if the level is set to **Attempt to connect regardless of server identity certificates**. For example, the certification check can fail for the following reasons:

- The certificate signed by the root CA has been revoked.
- The certificate signed by the intermediate CA has been revoked.
- The certificate is valid but the intermediate CA has been revoked.
- The certificate in the chain contains an unknown extension that is marked "critical".

Select a Display Protocol

You can select the display protocol that Horizon Client uses when you connect to a remote desktop or application.

Procedure

1 In Horizon Client, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.

  If you are connected to a server, you can tap the **Option** menu in the upper-left corner of the desktop and application selection window.

2 Expand the **Protocol** section and select the display protocol to use.

  VMware Blast requires Horizon Agent 7.0 or later.

3 (Optional) If you selected **VMware Blast**, enable or disable H.264 encoding by tapping and toggling the **Allow H.264 decoding** option to **On** or **Off**.

  When this option is set to **On**, Horizon Client allows H.264 encoding if Horizon Agent for the remote desktop or application supports H.264 encoding. If Horizon Agent for the remote desktop or application does not support H.264 encoding, Horizon Client uses JPEG/PNG encoding instead. When this option is set to **Off** (the default setting), H.264 encoding is not allowed and Horizon Client always using JPEG/PNG encoding.

The next time you connect to a remote desktop or application, Horizon Client uses the display protocol that you selected. You cannot change the display protocol for a currently connected session.

If you connect to a remote desktop or application that does not support the display protocol that you selected, Horizon Client displays an error message.

Connect to a Remote Desktop or Application

To connect to a remote desktop or application, you must provide the name of a server and supply credentials for your user account.

To use remote applications, you must connect to Connection Server 6.0 or later.

Note Before you have end users access their remote desktops, test that you can log in to a remote desktop from a client device.

Prerequisites

- Obtain login credentials, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- Obtain the NETBIOS domain name for logging in. For example, you might use `mycompany` rather than `mycompany.com`.
- Perform the administrative tasks described in "Preparing Connection Server for Horizon Client," on page 8.
- If you are outside the corporate network and are not using a security server to access the remote desktop or application, verify that your client device is set up to use a VPN connection and turn on that connection.

  IMPORTANT In most cases, use a security server rather than a VPN.

  If your company has an internal wireless network to provide routable access to remote desktops that your device can use, you do not have to set up a security server or VPN connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- Configure the certificate checking mode for the SSL certificate presented by Connection Server. See "Setting the Certificate Checking Mode for Horizon Client," on page 13.
- If you plan to use Windows Hello to authenticate, verify that Windows Hello is set up on your Windows 10 device. For complete requirements, see "Windows Hello Authentication Requirements," on page 8.

Procedure

1 If a VPN connection is required, turn on the VPN.

2 Tap the **VMware Horizon Client** app.

3 Connect to a server.

Option	Description
Connect to a new server	Tap **Add Server**, enter the name of a server, and tap **Connect**.
Connect to an existing server	Tap the server icon the home window.

Connections between Horizon Client and servers always use SSL. The default port for SSL connections is 443. If the server is not configured to use the default port, use the format shown in this example: **`view.company.com:1443`**.

4 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and tap **Login**.

The passcode might include both a PIN and the generated number on the token.

5 If you are prompted for a user name and password, supply Active Directory credentials.

a Type the user name and password of a user who is entitled to use at least one desktop or application pool.

b Select a domain.

c (Optional) If the **Enable Windows Hello** button is available, tap it to use Windows Hello authentication.

The **Enable Windows Hello** button is available only if biometric authentication is enabled on the server and you have not previously authenticated with Windows Hello.

d Tap **Login**.

If Windows Hello is enabled and you are logging in for the first time, your Active Directory credentials are stored securely on your Windows 10 device for future use.

6 If you are prompted for Windows Hello authentication, use your fingerprint, face, iris, or PIN to authenticate.

If you do not want to use Windows Hello authentication, click **Cancel** to enter a user name and password.

7 Tap a desktop or application to connect to it.

The remote desktop or application starts.

Disable Windows Hello in Horizon Client

You can disable Windows Hello for a server that you previously logged in to with Windows Hello authentication.

Prerequisites

Verify that a shortcut for the server appears on the Horizon Client home window. To configure Horizon Client to save server shortcuts, see "Save Information About Recent Servers on the Horizon Client Home Window," on page 9.

Procedure

1 Tap and hold the server shortcut on the Horizon Client home window.

2 When the context menu appears, tap **Sign out server**.

The next time you connect to the server, you can enter a user name and password and the **Enable Windows Hello** button appears on the server login dialog box.

Pinning a Remote Desktop or Application to the Start Screen

You can pin a remote desktop or application to the Start screen by right-clicking the desktop or application on the desktop and application selection window and selecting **Pin to Start** from the context menu.

If you are not logged in to the server when you tap the remote desktop or application on the Start screen, Horizon Client prompts you to authenticate to the server before it starts the remote desktop or application. If you are already logged in to the server, the remote desktop or application starts and you do not need to authenticate to the server.

Disconnecting From a Remote Desktop or Application

You can disconnect from a remote desktop without logging off, so that applications remain open on the remote desktop. You can also disconnect from a remote application so that the remote application remains open.

When you are logged in to the remote desktop or application, you can disconnect by tapping the **Disconnect** button in the desktop or application window and tapping **Disconnect**.

Note A Horizon administrator can configure your desktop to automatically log off when disconnected. In that case, any open programs in your desktop are stopped.

Logging Off From a Remote Desktop

If you are currently connected to and logged in to a remote desktop, you can use the Windows **Start** menu to log off.

You can also log off by tapping the **Ctrl+Alt+Del** button in the desktop or application window and tapping **Log off**.

Any unsaved files that are open on the remote desktop are closed during the logoff operation. If you disconnect from a remote desktop without logging off, applications remain open on the remote desktop.

Using a Remote Desktop or Application

4

Horizon Client includes features that are common to other Windows 10 UWP apps, as well as features that are specific to remote desktops and applications.

This chapter includes the following topics:

Feature Support Matrix

Some features are supported on one type of client but not on another. For example, USB access is supported with Horizon Client for Windows but not with Horizon Client for Windows 10 UWP.

Table 4-1. Features Supported on Windows Desktops for Windows 10 UWP Horizon Clients

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008/2012 R2 and Windows Server 2016 Desktops
USB redirection						
Real-Time Audio-Video (RTAV)						
Serial port redirection						

Table 4-1. Features Supported on Windows Desktops for Windows 10 UWP Horizon Clients (Continued)

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008/2012 R2 and Windows Server 2016 Desktops
VMware Blast display protocol	X	X	X			X
RDP display protocol						
PCoIP display protocol	X	X	X	Limited	Limited	X
Persona Management						
Wyse MMR						
Windows Media MMR						
Location-based printing	X	X	X	Limited	Limited	X
Virtual printing						
Smart cards						
RSA SecurID or RADIUS	X	X	X	Limited	Limited	X
Single sign-on	X	X	X	Limited	Limited	X
Multiple monitors						

Windows 10 desktops require View Agent 6.2 or later or Horizon Agent 7.0 or later. Windows Server 2012 R2 desktops require View Agent 6.1 or later or Horizon Agent 7.0 or later. Windows Server 2016 desktops require Horizon Agent 7.0.2 or later.

Important View Agent 6.1 and later and Horizon Agent 7.0 and later releases do not support Windows XP and Windows Vista desktops. View Agent 6.0.2 is the last View release that supports these guest operating systems. Customers who have an extended support agreement with Microsoft for Windows XP and Vista, and an extended support agreement with VMware for these guest operating systems, can deploy the View Agent 6.0.2 version of their Windows XP and Vista desktops with Connection Server 6.1.

For descriptions of these features and their limitations, see the *View Architecture Planning* document.

Feature Support for Published Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. Multiple users can have desktop sessions on an RDS host simultaneously. An RDS host can be either a physical machine or a virtual machine.

The following table contains rows only for the features that are supported. Certain features are supported on virtual machine RDS hosts and not on physical machine RDS hosts.

Table 4-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0 or Later, Installed

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 RDS Host	Windows Server 2016 RDS Host
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later
VMware Blast display protocol	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0.2 and later
PCoIP display protocol	X	X	Horizon Agent 7.0.2 and later
Location-based printing	View Agent 6.0.1 and later (virtual machine only)	View Agent 6.0.1 and later (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)

For information about which editions of each guest operating system are supported, or which service packs, see the "Supported Operating Systems for View Agent" topic in the View 5.x or 6.x installation documentation. See "Supported Operating Systems for Horizon Agent" in the Horizon 7 installation documentation.

Using Full-Screen Mode

You can display remote desktops and applications in full-screen or windowed mode on a Surface Pro 4 or Surface Book. Full-screen mode is enabled by default.

To toggle full-screen mode on and off, after you log in to a remote desktop or application, tap the **Option** button in the remote desktop or application window and tap **Full Screen**.

Adjusting the Screen Resolution for Remote Desktops and Applications

If your tablet has a high-resolution screen, you might have some difficulty reading the icons and text in a remote desktop or application. You can lower the screen resolution to improve readability.

To change the screen resolution before you log in to a remote desktop or application, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar, expand the **Resolution Mode** section, and select one of the resolution options.

You can also change the screen resolution after you connect to a server or log in to a remote desktop or application.

Enable the Local Zoom Feature

When you enable the local zoom feature, you can pinch your fingers together or apart on your touchscreen to zoom in and out in the remote desktop or application.

For Windows 8 and Windows 10 virtual machine desktops, and for Windows Server 2012 R2 and Windows Server 2016 RDS desktops and applications, you cannot pinch your fingers together and apart to zoom in and out unless you enable the local zoom feature.

Procedure

1 Connect to a remote desktop or application.

2 Tap the **Option** button in the desktop or application window and tap **Settings**.

3 Expand the **Advanced** section and tap to toggle the **Local Zoom** option to **On**.

If the option is set to **Off**, you cannot use the local zoom feature in the remote desktop or application. The option is set to **On** by default.

Prevent Screen Lock

After a certain amount of idle time, your Windows 10 device might dim the display, activate the lock screen, or power down the display to conserve power. You can set an option to prevent screen lock for a remote desktop or application.

Note Windows 10 devices register watching and listening as user idle time. The amount of idle time required before screen lock occurs depends on your device's user settings.

Procedure

1 Connect to a remote desktop or application.

2 Tap the **Option** button in the desktop or application window and tap **Settings**.

3 Expand the **Advanced** section and tap to toggle the **Screen always on** option to **On**.

If the option is set to **Off**, screen lock may occur.

Using the Sidebar

After you connect to a remote desktop or application, you can use the sidebar to open other desktops and applications.

Table 4-3. Sidebar Actions

Action	Description
Show the sidebar	Tap the **Option** button in the remote desktop or application window and tap **Side Bar**.
Hide the sidebar	Tap anywhere inside the remote desktop or application window.
Open a remote desktop or application	Tap the name of the remote desktop or application in the sidebar.
Search for a remote desktop or application	Type the name of the remote desktop or application in the **Search** box. To open the remote desktop or application, tap its name in the search results.

Gestures and Navigation Aids

VMware has created user interaction aids to help you navigate conventional Windows user interface elements.

Clicking

As in other apps, you can tap to click a user interface element. You can also use an external mouse.

Right-Clicking

The following options are available for right-clicking:

- Use an external mouse to right-click.
- On a touchpad, tap with two fingers.

- On a touch screen, tap and hold until the right-click menu appears.

Zooming In and Out

On a touch screen, pinch your fingers together or apart to zoom.

On operating systems that support touch input, zoom in and zoom out on a touch screen work only if you enable the local zoom feature. See "Enable the Local Zoom Feature," on page 21. Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2016 support touch input.

Scrolling and Scroll Bars

The following options are available for vertical scrolling:

- Use an external mouse to scroll.
- On a touchpad, tap and hold with your thumb and then scroll down with two fingers.
- On a touch screen, tap with two fingers and then drag to scroll, or use one finger to drag the scroll bar. The text under your fingers moves in the same direction as your fingers.

Sound, Music, and Video

If sound is turned on for your device, you can play audio and video in a remote desktop.

Ctrl+Alt+Del

Because the Windows key combination Ctrl+Alt+Del is not supported in remote desktops and applications, tap the **Ctrl+Alt+Del** button in the remote desktop or application window instead.

Multitasking

You can switch between Horizon Client and other apps without losing a remote desktop or application connection.

You can resize the Horizon Client app so that it takes up part of the screen alongside another app.

If you leave a session idle for some amount of time, before the session times out, you receive a prompt, asking if you want to keep the session alive. Tap or click anywhere on the screen or press a key on your keyboard to keep the session alive. If enough time has passed so that the connection to the remote desktop or application was lost, Horizon Client returns to the desktop and application selection window and prompts you to reconnect.

Using Horizon Client with a Microsoft Display Dock

The VMware Horizon Client app works with Continuum for Windows 10 Mobile. You can use a Microsoft Display Dock to connect your Windows 10 smartphone to an external display and mouse. With this feature, you can use Horizon Client just as you would use it on a desktop PC.

Copying and Pasting Text and Images

By default, you can copy and paste text from your client system to a remote desktop or application. If a Horizon administrator enables the feature, you can also copy and paste text from a remote desktop or application to your client system or between two remote desktops or applications.

You can copy and paste plain text only. Images and RTF (Rich Text Format) are not supported.

A Horizon administrator can set this feature so that copy and paste operations are allowed only from your client system to a remote desktop or application, or only from a remote desktop or application to your client system, or both, or neither.

Horizon administrators configure the ability to copy and paste by configuring group policy settings that pertain to Horizon Agent. Depending on the Horizon server and agent version, administrators might also be able to use group policies to restrict clipboard formats during copy and paste operations or use Smart Policies to control the copy and paste behavior in remote desktops. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

The clipboard can accommodate 64 K of data for copy and paste operations. If you try to copy more than the maximum clipboard size, the text is truncated.

You cannot copy and paste files between a remote desktop and the file system on your client computer.

Saving Documents in a Remote Application

With certain remote applications, such as Microsoft Word or WordPad, you can create and save documents. Where these documents are saved depends on your company's network environment. For example, your documents might be saved to a home share mounted on your local computer.

Administrators can use an ADMX template file to set a group policy that specifies where documents are saved. This policy is called **Set Remote Desktop Services User Home Directory**. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Internationalization

Both the user interface and the documentation are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, and Spanish. You can also input characters for these languages.

Troubleshooting Horizon Client 5

You can solve most Horizon Client problems by resetting the desktop or reinstalling the app.

You can also enable log collection and send log files to VMware for troubleshooting.

This chapter includes the following topics:

Horizon Client Stops Responding or the Remote Desktop Freezes

When the window freezes, first, try resetting the remote desktop operating system.

Problem

Horizon Client does not work or repeatedly exits unexpectedly or the remote desktop freezes.

Cause

Assuming that Horizon servers are configured properly and that firewalls surrounding them have the correct ports open, other issues usually relate to Horizon Client on the device or to the guest operating system on the remote desktop.

Solution

- If the operating system in the remote desktop freezes, use Horizon Client on the device to reset the desktop.

  This option is available only if the Horizon administrator has enabled this feature.
- Uninstall and reinstall the app on the device.
- If you get a connection error when you attempt to connect to the server, you might need to change your proxy settings.

Resetting a Remote Desktop or Application

If you are currently connected to and logged in to a remote desktop or application, you can tap the **Disconnect** button in the desktop or application window and tap **Reset** to reset the remote desktop or application.

The **Reset** command is available only if the Horizon administrator has allowed it and only if the status of the remote desktop or application is such that the action can be taken.

You might need to restart a remote desktop or application if the desktop operating system or application stops responding.

Resetting a remote desktop is the equivalent of pressing the **Reset** button on a physical PC to force the PC to restart. Any files that are open on the remote desktop are closed without being saved.

Resetting a remote application quits all remote applications and logs off all of your remote application sessions. Unsaved changes in remote applications might be lost.

Uninstall the VMware Horizon Client App

You can sometimes resolve problems with Horizon Client by uninstalling and reinstalling the VMware Horizon Client app from the Windows 10 UWP device.

You uninstall Horizon Client just as you would uninstall any Windows 10 UWP app.

Procedure

1 On your device, locate the VMware Horizon Client app.

2 Right-click the **VMware Horizon Client** tile or icon and tap **Uninstall**.

What to do next

Reinstall the VMware Horizon Client app. See "Install or Upgrade Horizon Client for Windows 10 UWP," on page 9.

Connecting to a Server in Workspace ONE Mode

If you cannot connect to a server directly through Horizon Client, or if your desktop and application entitlements are not visible in Horizon Client, Workspace ONE mode might be enabled on the server.

Problem

- When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.
- When you open a desktop or application through a URI or shortcut, or when you open a local file through file association, the request redirects you to the Workspace ONE portal for authentication.
- After you open a desktop or application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or applications in Horizon Client.

Cause

Beginning with Horizon 7 version 7.2, an administrator can enable Workspace ONE mode on a Connection Server instance. This behavior is normal when Workspace ONE mode is enabled on a Connection Server instance.

Solution

Use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops and applications.

Collect Logs to Send to Technical Support

You can enable logging and collect a log bundle to send to technical support.

To troubleshoot some issues, you might be directed to collect logs to send to technical support. Logging will affect the performance of Horizon Client if a secure tunnel session is being used to connect to the remote desktop. Be sure to turn the advanced logging feature off when logging is no longer necessary.

Prerequisites

Contact VMware technical support so that you can determine where to send the log files you collect.

Procedure

1 In Horizon Client, tap the **Option** menu in the upper-left corner of the menu bar.

   If you are connected to a server, you can tap the **Option** menu in the upper-left corner of the desktop and application selection window. If you are connected to a remote desktop or application, you can tap the **Option** button in the desktop or application window and tap **Settings**.

2 Expand the **Logging** section and tap to toggle the **Enable advanced logging** option to on.

3 Tap **Collect support information**, navigate to the location on your device to store the log files, select the directory, and tap **Select folder**.

   For example, for convenience you might tap the **Desktop** item to save the logs in a folder on your local desktop.

   Horizon Client creates a folder named `vmware-view-logs-`*`timestamp`* in the location that you specified.

4 (Optional) To create a `.zip` file of the log folder before sending it to technical support, right-click the folder and select **Send to > Compressed (zipped) folder**.

What to do next

Send the logs to VMware technical support.

Index