

# Using VMware Horizon Client for Windows 10 UWP

Horizon Client 4.2

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-002237-00

**vmware**<sup>®</sup>

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](mailto:docfeedback@vmware.com)

Beta

Copyright © 2016 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

<b>1</b>	<b>Using VMware Horizon Client for Windows 10 UWP</b>	<b>5</b>
<b>2</b>	<b>Setup and Installation</b>	<b>7</b>
	System Requirements	7
	Preparing Connection Server for Horizon Client	8
	Supported Desktop Operating Systems	8
	Install or Upgrade Horizon Client for Windows 10 UWP	8
	Configure H.264 Decoding in Horizon Client	9
	Save Information About Recent Servers on the Horizon Client Home Window	9
	Configure Screen Lock for Horizon Client	9
	Configure the Local Zoom Feature for Remote Desktops and Applications	10
	Configure Advanced TLS/SSL Options	10
	Displaying Help for Horizon Client	11
<b>3</b>	<b>Managing Remote Desktop and Application Connections</b>	<b>13</b>
	Connect to a Remote Desktop or Application	13
	Setting the Certificate Checking Mode for Horizon Client	14
	Disconnecting From a Remote Desktop or Application	15
	Logging Off From a Remote Desktop	15
	Switch Desktops or Applications	15
<b>4</b>	<b>Using a Remote Desktop or Application</b>	<b>17</b>
	Feature Support Matrix	17
	Using Full-Screen Mode	19
	Adjusting the Screen Resolution for Remote Desktops and Applications	19
	Gestures and Navigation Aids	19
	Multitasking	20
	Using Horizon Client with a Microsoft Display Dock	20
	Saving Documents in a Remote Application	20
	Internationalization and International Keyboards	20
<b>5</b>	<b>Troubleshooting Horizon Client</b>	<b>21</b>
	Horizon Client Stops Responding or the Remote Desktop Freezes	21
	Resetting a Remote Desktop or Application	22
	Uninstall the VMware Horizon Client App	22
	Problem Establishing a Connection When Using a Proxy	22
	Collect Logs to Send to Technical Support	23
	<b>Index</b>	<b>25</b>

Beta

# 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.

Beta

Beta

# 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,”](#) on page 7
- [“Preparing Connection Server for Horizon Client,”](#) on page 8
- [“Supported Desktop Operating Systems,”](#) on page 8
- [“Install or Upgrade Horizon Client for Windows 10 UWP,”](#) on page 8
- [“Configure H.264 Decoding in Horizon Client,”](#) on page 9
- [“Save Information About Recent Servers on the Horizon Client Home Window,”](#) on page 9
- [“Configure Screen Lock for Horizon Client,”](#) on page 9
- [“Configure the Local Zoom Feature for Remote Desktops and Applications,”](#) on page 10
- [“Configure Advanced TLS/SSL Options,”](#) on page 10
- [“Displaying Help for Horizon Client,”](#) on page 11

## System Requirements

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

### Devices

- Microsoft Surface Pro 4
- Microsoft Surface Book
- Microsoft Lumia 950 XL
- Microsoft Lumia 950

You can also install Horizon Client for Windows 10 UWP on a PC that is running a supported Windows 10 operating system.

### Operating systems

- Windows 10 Pro
- Windows 10 LTSC
- Windows 10 Enterprise

**External keyboards and other peripherals**

You can use Horizon Client for Windows 10 UWP with an external keyboard and mouse. You can use a Microsoft Display Dock to connect your Windows 10 smartphone to an external display and mouse and use Horizon Client for Windows UWP just as you would use it on a desktop PC.

For information about the external devices that are supported with your device, see the manufacturer's documentation for your device.

**Connection Server, Security Server, and Horizon Agent**

Horizon 7 version 7.0 and later.

VMware recommends that you use a security server so that your device does not require a VPN connection.

**Display protocol for remote desktops and applications**

VMware Blast

## 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 Access Point, configure Connection Server to work with Access Point. See *Deploying and Configuring Access Point*. Access Point 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 Horizon 7 version 7 or a later release of Connection Server. 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 more information, see the topics about creating desktop and application pools in the *Setting Up Desktop and Application Pools in View* document.

- To use two-factor authentication with Horizon Client, such as RSA SecurID authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in 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.

## Configure H.264 Decoding in Horizon Client

You can configure whether to allow or disable H.264 decoding in Horizon Client for remote desktop and application sessions.

#### Procedure

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

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 Tap to toggle the **Allow H.264 decoding** option to **On** or **Off**.

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

When the option is set to **Off**, H.264 decoding is not allowed, and Horizon Client always uses JPEG/PNG decoding.

## Save Information About Recent Servers on the Horizon Client Home Window

You can configure whether Horizon Client saves recent servers on the Horizon Client home window.

#### Procedure

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

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 Tap to toggle the **Save information about recent servers** option to **On** or **Off**.

When the option is set to **On** (the default setting), Horizon Client saves a server shortcut on the home window after you connect to a server for the first time.

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

## Configure Screen Lock for Horizon Client

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 or allow screen lock for the Horizon Client app.

---

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

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 Tap to toggle the **Prevent screen lock** option to **On** or **Off**.

When the option is set to **On** (the default setting), screen lock does not occur in the Horizon Client app. When the option is set to **off**, screen lock may occur in the Horizon Client app.

## Configure the Local Zoom Feature for Remote Desktops and Applications

You can configure whether the zoom feature on your Windows 10 device is available in remote desktops and applications.

With the zoom feature, you can pinch your fingers together or apart on your touchscreen to zoom in and out. 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 Tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.

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 Tap to toggle the **Local zoom** option to **On** or **Off**.

When the option is set to **On**, you can pinch your fingers together or apart on your touchscreen to zoom in and out in a remote desktop or application.

When the option is set to **Off** (the default setting), you cannot use the local zoom feature in remote desktops and applications.

## 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:EC DH+AESGCM:RSA+AESGCM:kECDH+AES:EC DH+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.

The security options appear under **Advanced SSL Options**.

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 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.

## 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**.

If you are connected to a remote desktop or application, you can tap the **Option** button in the desktop or application window, tap **Settings**, tap the information icon (!), and tap the link under **Online Help**.

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.

Beta

# 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:

- [“Connect to a Remote Desktop or Application,”](#) on page 13
- [“Setting the Certificate Checking Mode for Horizon Client,”](#) on page 14
- [“Disconnecting From a Remote Desktop or Application,”](#) on page 15
- [“Logging Off From a Remote Desktop,”](#) on page 15
- [“Switch Desktops or Applications,”](#) on page 15

## 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 credentials to log in, such as an Active Directory username and password or RSA SecurID 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, verify that your client device is set up to use a VPN connection and turn on that connection.

---

**IMPORTANT** VMware recommends using 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 View 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. You also need the port number if the port is not 443.
- Configure the certificate checking mode for the SSL certificate presented by Connection Server. See [“Setting the Certificate Checking Mode for Horizon Client,”](#) on page 14.

### 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
<b>Connect to a new server</b>	Tap <b>+New Server</b> , enter the name of a server, and tap <b>Connect</b> .
<b>Connect to an existing server</b>	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, 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 Tap **Login**.
- 6 Tap a desktop or application to connect to it.

The remote desktop or application starts.

## 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. 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".

## 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 **Power** button in the desktop or application window and tapping **Disconnect**.

---

**NOTE** A View 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 **Disconnect** button in the desktop or application window and tapping **Logoff**, or by tapping the **Ctrl+Alt+Del** button in of 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.

## Switch Desktops or Applications

If you are connected to a remote desktop or application, you can switch to another remote desktop or application.

### Prerequisites

To switch to a remote desktop or application on a different server, obtain the credentials to log in.

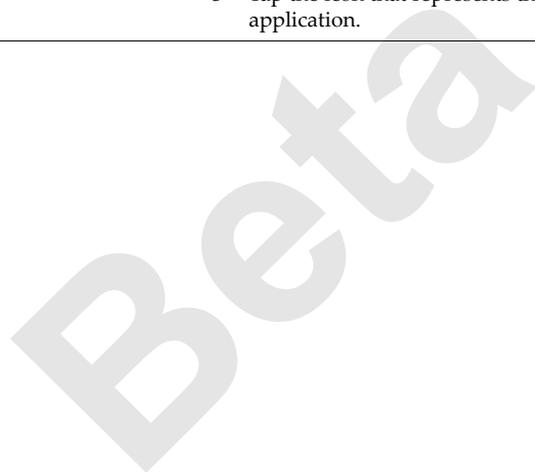
**Procedure**

- 1 From within the remote desktop or application, tap the **Disconnect** button at the top of the window and tap **Disconnect**.

The desktop and application selector window appears.

- 2 Select a different remote desktop or application.

Option	Action
<b>Choose a different remote desktop or application on the same server</b>	From the desktop and application selector window, tap the icon that represents the different remote desktop or application. If you connect to multiple remote applications in the same farm, you can switch between the applications by clicking or tapping the application windows.
<b>Choose a different remote desktop or application on a different server</b>	<ol style="list-style-type: none"> <li>a From the desktop and application selector window, tap the <b>Disconnect</b> button in the upper-left corner of the menu bar to disconnect from the server.</li> <li>b Tap another server, enter your credentials, and tap <b>Login</b> to connect to the new server.</li> <li>c Tap the icon that represents the different remote desktop or application.</li> </ol>



# 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,”](#) on page 17
- [“Using Full-Screen Mode,”](#) on page 19
- [“Adjusting the Screen Resolution for Remote Desktops and Applications,”](#) on page 19
- [“Gestures and Navigation Aids,”](#) on page 19
- [“Multitasking,”](#) on page 20
- [“Using Horizon Client with a Microsoft Display Dock,”](#) on page 20
- [“Saving Documents in a Remote Application,”](#) on page 20
- [“Internationalization and International Keyboards,”](#) on page 20

## 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 for Single-User Remote Desktops with Horizon Agent 7.0 or Later Installed

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

**Table 4-1.** Features Supported for Single-User Remote Desktops with Horizon Agent 7.0 or Later Installed (Continued)

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

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

## Feature Support for Session-Based 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 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	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	X	X	Horizon Agent 7.0.2 and later
Location-based printing	X (virtual machine only)	X (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, see "Supported Operating Systems for Horizon Agent" in the *View Installation* document.

## 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 select one of the options in the Resolution section.

You can also change the screen resolution after you log in to a remote desktop or application by tapping the **Option** button in the remote desktop or application window and tapping **Settings**.

## 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:

- Tap with two fingers on the touchpad.
- Use an external mouse to right-click.
- Tap and hold on the touch screen until the right-click menu appears.

### Zooming In and Out

As in other apps, pinch your fingers together or apart to zoom on the touch screen.

### Scrolling and Scroll Bars

The following options are available for vertical scrolling:

- Tap and hold with your thumb and then scroll down with one finger on the touchpad. You can also scroll with two fingers.
- Use an external mouse to scroll.
- Tap with one or two fingers and then drag to scroll on the touch screen. 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 selector screen 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.

## 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 "RDS Profiles Settings" topic in the *Setting Up Desktop and Application Pools in View* document.

## Internationalization and International Keyboards

Both the Horizon Client user interface and the documentation are available only in English. International keyboards are not supported in this release.

# Troubleshooting Horizon Client

---

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,”](#) on page 21
- [“Resetting a Remote Desktop or Application,”](#) on page 22
- [“Uninstall the VMware Horizon Client App,”](#) on page 22
- [“Problem Establishing a Connection When Using a Proxy,”](#) on page 22
- [“Collect Logs to Send to Technical Support,”](#) on page 23

## Horizon Client Stops Responding or the Remote Desktop Freezes

When the screen 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 View 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 View 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 View 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 8.

## Problem Establishing a Connection When Using a Proxy

Sometimes if you attempt to connect to Connection Server using a proxy while on the LAN, an error occurs.

### Problem

If the View environment is set up to use a secure connection from the remote desktop to Connection Server, and if the client device is configured to use an HTTP proxy, you might not be able to connect.

### Cause

Unlike Windows Internet Explorer, the client device does not have an Internet option to bypass the proxy for local addresses. When an HTTP proxy is used for browsing external addresses, and you try to connect to Connection Server using an internal address, you might see the error message `Could not establish connection`.

### Solution

- ◆ Remove the proxy settings so that the device no longer uses a proxy.

## 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 remote desktop or application, you can tap the **Option** button in the desktop or application window and tap **Settings**.

- 2 In the Logging section, 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.

A folder called `vmware-view-logs-timestamp` is created in the location 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.

Beta

# Index

## C

certificates, ignoring problems **14**  
Connection Server **8**  
connection problems **22**

## D

disconnecting from a remote desktop **15**

## F

feature support matrix **17**  
full-screen mode **19**

## G

gestures **19**

## H

H.264 encoding **9**  
help system **11**  
Horizon Client  
    disconnect from a desktop **15**  
    logging in **13**  
    troubleshooting **21**  
Horizon Client for Windows 10 UWP **5**

## I

installing **8**  
internationalization **20**

## L

local zoom **10**  
logging **23**  
logging in  
    to a desktop **13**  
    to a server **13**  
logging off **15**

## M

managing desktops **13**  
multitasking **20**

## O

operating systems **8**

## P

prerequisites for client devices **8**  
proxy connections **22**

## R

remote desktops and applications **17**  
resetting a desktop **22**

## S

save server information **9**  
saving documents in a remote application **20**  
screen lock **9**  
screen resolution **19**  
security servers **8**  
setup for Windows Surface Pro **7**  
SSL options **10**  
switching desktops and applications **15**  
system requirements **7**

## T

troubleshooting, connection problems **22**

## U

uninstalling **22**

## W

Windows Display Dock **20**

Beta