

VMware Horizon Client for Windows 10 UWP Installation and Setup Guide

14 MAR 2019

VMware Horizon Client for Windows 10 UWP 5.0



vmware®

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

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

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

Copyright © 2016–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 VMware Horizon Client for Windows 10 UWP Installation and Setup Guide 5**
- 2 Setup and Installation 6**
 - System Requirements for Windows 10 Devices 6
 - Windows Hello Authentication Requirements 7
 - Preparing Connection Server for Horizon Client 7
 - Supported Desktop Operating Systems 8
 - Install or Upgrade the VMware Horizon Client App 8
 - Save Information About Recent Servers 9
 - Configure Advanced TLS Options 9
 - Configure VMware Blast Options 10
 - Displaying Help for Horizon Client 11
 - Configure Horizon Client Data Sharing 11
 - Horizon Client Data Collected by VMware 11
- 3 Managing Remote Desktop and Published Application Connections 14**
 - Setting the Certificate Checking Mode in Horizon Client 14
 - Connect to a Remote Desktop or Published Application 15
 - Disable Windows Hello Authentication for a Server 17
 - Pinning a Remote Desktop or Published Application to the Start Screen 17
 - Select a Favorite Remote Desktop or Published Application 17
 - Disconnecting from a Remote Desktop or Published Application 18
 - Logging Off from a Remote Desktop 18
 - Disconnecting from a Server 19
- 4 Using a Remote Desktop or Published Application 20**
 - Feature Support Matrix for Windows 10 Clients 20
 - Using Full-Screen Mode 23
 - Using DPI Synchronization 23
 - Adjust the Screen Resolution for Remote Desktops and Published Applications 24
 - Configure the Local Zoom Feature 25
 - Prevent Screen Lock 25
 - Using the Sidebar 25
 - Gestures and Navigation Aids 26
 - Multitasking 27
 - Using Horizon Client with a Microsoft Display Dock 27
 - Copying and Pasting 27
 - Logging Copy and Paste Activity 28

[Saving Documents in a Published Application](#) 28

[Enable Multi-Session Mode for Published Applications](#) 29

[Internationalization](#) 29

5 Troubleshooting Horizon Client 30

[Resetting a Remote Desktop or Application](#) 30

[Uninstall the VMware Horizon Client App](#) 30

[Collect Logs to Send to VMware Technical Support](#) 31

[Horizon Client Stops Responding or the Remote Desktop Freezes](#) 32

[Connecting to a Server in Workspace ONE Mode](#) 32

VMware Horizon Client for Windows 10 UWP Installation and Setup Guide

1

This document, *VMware Horizon Client for Windows 10 UWP Installation and Setup Guide*, provides information about installing, configuring, and using VMware Horizon[®] Client[™] software on a Windows 10 device.

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 data center operations.

If you are an end user, see the *VMware Horizon Client for Windows 10 UWP User Guide* document on [VMware Docs](#), or view the Horizon Client online help.

Setup and Installation

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

This chapter includes the following topics:

- [System Requirements for Windows 10 Devices](#)
- [Windows Hello Authentication Requirements](#)
- [Preparing Connection Server for Horizon Client](#)
- [Supported Desktop Operating Systems](#)
- [Install or Upgrade the VMware Horizon Client App](#)
- [Save Information About Recent Servers](#)
- [Configure Advanced TLS Options](#)
- [Configure VMware Blast Options](#)
- [Displaying Help for Horizon Client](#)
- [Configure Horizon Client Data Sharing](#)

System Requirements for Windows 10 Devices

The Windows 10 device on which you install the VMware Horizon Client app, and the peripherals it uses, must meet certain system requirements.

Operating systems

- Windows 10 1809 SAC
- Windows 10 1803 SAC

Windows Hello authentication

See [Windows Hello Authentication Requirements](#).

Connection Server, security server, and View Agent or Horizon Agent	<p>Latest maintenance release of Horizon 6 version 6.2.x and later releases.</p> <p>VMware recommends that you use a security server or Unified Access Gateway appliance so that client devices do not require a VPN connection.</p>
Display protocols	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Horizon 6 version 6.2 or a later release. ■ Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the <i>Horizon 7 Administration</i> document.
Horizon Client requirements	<p>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.</p>

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

Preparing Connection Server for Horizon Client

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must configure certain Connection Server settings.

Unified Access Gateway and Security Servers

- If your Horizon deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.
- If your Horizon deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 6.x and Security Server 6.x or later releases. For more information, see the installation document for your Horizon version.

Desktop and Application Pools

- 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 *Setting Up Virtual Desktops in Horizon 7* and *Setting Up Published Desktops and Applications in Horizon 7* documents.

User Authentication

- To use Windows Hello authentication with Horizon Client, 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 *Horizon 7 Administration* document.
- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature for the Connection Server instance. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Administrator. This setting is available in Horizon 7 version 7.8 and later and is disabled by default. Earlier Horizon 7 versions send the domain list. For more information, see the *Horizon 7 Administration* document.

When users log in to a server, and **Send domain list** is disabled, the **Domain** drop-down menu in Horizon Client shows *DefaultDomain* and users might need to enter a domain, for example, username@domain.com, in the **User name** text box. If users do not enter the domain manually, and if more than one domain is configured, they might fail to log in to the server.

Supported Desktop Operating Systems

Horizon 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 *Horizon 7 Installation* document.

Install or Upgrade the VMware Horizon Client App

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

Prerequisites

- Verify that the client device meets the system requirements for Horizon Client. See [System Requirements for Windows 10 Devices](#).
- Set up the Windows 10 client device. See the manufacturer's user's guide for the device.

Procedure

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

Save Information About Recent Servers

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

Procedure

- 1 Open the **Option** menu.
 - If you are not connected to a server, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.
 - If you are connected to a server, but not yet connected to a remote desktop or published application, 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 published application, tap the **Option** button in the floating menu in the remote desktop or published application window and tap **Setting**.
- 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 Options

You can select the security protocols and cryptographic algorithms that Horizon uses to encrypt communications between Horizon Client and servers, and between Horizon Client and Horizon Agent.

By default, TLS v1.1 and TLS v1.2 are enabled. SSL v2.0, SSL v3.0, and TLS v1.0 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 server to which the client system connects, a TLS error occurs and the connection fails.

For information about configuring the security protocols that Connection Server can accept, see the *Horizon 7 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 TLS v1.1 and TLS v1.2 protocols. Both protocols are enabled by default.
- 3 To change the cipher control string, replace the default string and tap **Change**.
- 4 (Optional) 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 for remote desktop and published application sessions that use the VMware Blast display protocol.

You can configure H.264 decoding before or after you connect to a server.

Note In earlier Horizon Client versions, you had to select a network condition option to provide the best user experience with VMware Blast. In this release, Horizon Client senses current network conditions and chooses a transport to provide the best user experience automatically.

Prerequisites

To use this feature, Horizon Agent 7.0 or later must be installed.

Procedure

- 1 Open the **Option** menu.
 - If you are not connected to a server, 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, tap the **Option** menu in the upper-left corner of the desktop and application selection window, expand the **Protocol** section, and select **VMware Blast**.
- 2 To enable or disable H.264 encoding, tap and toggle the **Allow H.264 decoding** option to **On** or **Off**.

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

Changes for H.264 take effect the next time a user connects to a remote desktop or published application and selects the VMware Blast display protocol. Your changes do not affect existing VMware Blast sessions.

Displaying Help for Horizon Client

To access the Horizon Client help from within the VMware Horizon Client app, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar, tap the information (!) icon, and tap the link under **Online Help**.

Configure Horizon Client Data Sharing

If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects and receives anonymous data on client systems to prioritize hardware and software compatibility. You can configure whether to share information on your client system by enabling or disabling a setting in Horizon Client.

Horizon Client data sharing is enabled by default. You must configure the data sharing setting before you connect to a server. The setting is applied to all servers. You cannot change the Horizon Client data sharing setting after you connect to a server.

Procedure

- 1 Start Horizon Client.
- 2 Tap the **Option** menu in the upper-left corner of the Horizon Client menu bar and expand the **Advanced** section.
- 3 Expand the **Allow Data Sharing** section and tap to toggle the **Allow Data Sharing** option to on or off.

Horizon Client Data Collected by VMware

If a Horizon administrator has opted to participate in the customer experience improvement program, and data sharing is enabled on the client system, VMware collects data about the client system.

VMware collects data about client systems to prioritize hardware and software compatibility. If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to respond better to customer requirements. VMware does not collect data that identifies your organization. Horizon Client information is sent first to the Connection Server instance and then to VMware, along with data about Connection Server, desktop pools, and remote desktops.

A Horizon administrator can select whether to participate in the VMware customer experience improvement program when installing Connection Server or by setting an option in Horizon Administrator after the installation.

Table 2-1. Data Collected from Horizon Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous?	Example Value
Company that produced the Horizon Client application	No	VMware
Product name	No	VMware Horizon Client
Client product version	No	(The format is x.x.x-yyyyyy, where x.x.x is the client version number and yyyyyy is the build number.)
Client binary architecture	No	Examples include the following: <ul style="list-style-type: none"> ■ i386 ■ x86_64 ■ arm
Client build name	No	Examples include the following: <ul style="list-style-type: none"> ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Host operating system	No	Examples include the following: <ul style="list-style-type: none"> ■ Windows 8.1 ■ Windows 7, 64-bit Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host operating system kernel	No	Examples include the following: <ul style="list-style-type: none"> ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unknown (for Windows Store)
Host operating system architecture	No	Examples include the following: <ul style="list-style-type: none"> ■ x86_64 ■ i386 ■ armv71 ■ ARM
Host system model	No	Examples include the following: <ul style="list-style-type: none"> ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision Workstation T3400 (A04 03/21/2008)

Table 2-1. Data Collected from Horizon Clients for the Customer Experience Improvement Program (Continued)

Description	Is This Field Made Anonymous?	Example Value
Host system CPU	No	Examples include the following: <ul style="list-style-type: none"> ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (for iPad)
Number of cores in the host system's processor	No	For example: 4
MB of memory on the host system	No	Examples include the following: <ul style="list-style-type: none"> ■ 4096 ■ unknown (for Windows Store)
Number of USB devices connected	No	2 (USB device redirection is supported only for Linux, Windows, and Mac clients.)
Maximum concurrent USB device connections	No	2
USB device vendor ID	No	Examples include the following: <ul style="list-style-type: none"> ■ Kingston ■ NEC ■ Nokia ■ Wacom
USB device product ID	No	Examples include the following: <ul style="list-style-type: none"> ■ DataTraveler ■ Gamepad ■ Storage Drive ■ Wireless Mouse
USB device family	No	Examples include the following: <ul style="list-style-type: none"> ■ Security ■ Human Interface Device ■ Imaging
USB device use count	No	(Number of times the device was shared)

Managing Remote Desktop and Published Application Connections

3

End users can use Horizon Client to connect to a server, log in to or off of remote desktops, and use published applications. For troubleshooting purposes, end users can also reset remote desktops and published applications.

End users might be able to perform many operations in remote desktops, depending on how a Horizon administrator configures policies.

This chapter includes the following topics:

- [Setting the Certificate Checking Mode in Horizon Client](#)
- [Connect to a Remote Desktop or Published Application](#)
- [Disable Windows Hello Authentication for a Server](#)
- [Pinning a Remote Desktop or Published Application to the Start Screen](#)
- [Select a Favorite Remote Desktop or Published Application](#)
- [Disconnecting from a Remote Desktop or Published Application](#)
- [Logging Off from a Remote Desktop](#)
- [Disconnecting from a Server](#)

Setting the Certificate Checking Mode in Horizon Client

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license.

End users can configure a setting in Horizon Client to determine whether Horizon Client connections are rejected if server certificate checking fails.

Server certificate checking 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.

To set the certificate checking mode, start Horizon Client, 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.** This setting means that you cannot connect to the server if any of the certificate checks fail. 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 by Windows 10 apps is more limited than the certificate mechanism used by Windows desktop applications, the certificate check can fail even if the level is set to **Attempt to connect regardless of server identity certificates**. For example, the certificate 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".

Connect to a Remote Desktop or Published Application

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

Before you have end users access their remote desktops and published applications, test that you can connect to a remote desktop or published application from a client device. You might need to specify a server and supply credentials for your user account.

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](#).
- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or published 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 certificate presented by the server. See [Setting the Certificate Checking Mode in Horizon Client](#).
- If you plan to use Windows Hello to authenticate, verify that Windows Hello is set up on the Windows 10 device. For complete requirements, see [Windows Hello Authentication Requirements](#).

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 in the home window.

Connections between Horizon Client and servers always use TLS. The default port for TLS 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 your 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 the 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 (Optional) To select the display protocol to use, tap the **Option** menu in the upper-left corner of the desktop and application selection window and expand the **Protocol** section.

VMware Blast provides better battery life and is the best protocol for high-end 3D and mobile device users.

- 8 Tap a remote desktop or published application to connect to it.

The remote desktop or published application starts.

Disable Windows Hello Authentication for a Server

If you previously logged in to a server with Windows Hello authentication, and you no longer want to use Windows Hello authentication to authenticate, you must disable Windows Hello authentication for the server.

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](#).

Procedure

- 1 Tap and hold the server shortcut on the Horizon Client home window.
- 2 To disable Windows Hello authentication for the server, tap **Sign out server** in the context menu.

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 Published Application to the Start Screen

To add a tile for a remote desktop or published application to the Start screen on the client device, right-click the remote desktop or published application on the desktop and application selection window and tap **Pin to Start** in the context menu.

To start the remote desktop or published application from the Start screen, tap its tile. If you are already logged in to the server, the remote desktop or published application starts immediately. If you are not logged in to the server, Horizon Client starts and prompts you to authenticate to the server before it starts the remote desktop or published application.

Select a Favorite Remote Desktop or Published Application

You can select favorite remote desktops and published applications. A star identifies favorite items on the desktop and application selection window. Favorite items are saved after you log out from the server.

Prerequisites

Connect to the server.

Procedure

- To select or deselect a favorite item, right-click a remote desktop or published application on the desktop and application selection window until the context menu appears and tap **Mark as Favorite**.

A star appears in the upper-right corner of the remote desktop or published application on the desktop and application selection window.

- To deselect a favorite item, right-click a remote desktop or published application on the desktop and application selection window until the context menu appears and tap **Unmark Favorite**.

A star no longer appears in the upper-right corner of the remote desktop or published application on the desktop and application selection window.

- To display only favorite remote desktops or published applications, tap the **Show Favorites** button (star icon) in the upper-right corner of the desktop and application selection window.

The favorites window appears. To return to the desktop and application selection window, tap the **Show All** button in the upper-right corner of the favorites window.

Disconnecting from a Remote Desktop or Published Application

When you are logged in to a remote desktop, you can disconnect without logging off so that applications remain open in the remote desktop. You can also disconnect from a published application so that the published application remains open.

To disconnect from a remote desktop or published application, tap the **Disconnect** button in the floating menu in the remote desktop or published application window and tap **Disconnect**.

Note A Horizon administrator can configure a remote desktop to log off when it is disconnected. In that case, any open applications in the remote desktop are closed.

Logging Off from a Remote Desktop

If you are 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 floating menu in the remote desktop window and tapping **Log Off**.

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

Disconnecting from a Server

After you have finished using a remote desktop or published application, you can disconnect from the server.

To disconnect from a server, tap the **Disconnect** icon in the upper-left corner of the desktop and application selection window and tap **Log Off**.

Using a Remote Desktop or Published Application

4

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

This chapter includes the following topics:

- [Feature Support Matrix for Windows 10 Clients](#)
- [Using Full-Screen Mode](#)
- [Using DPI Synchronization](#)
- [Adjust the Screen Resolution for Remote Desktops and Published Applications](#)
- [Configure the Local Zoom Feature](#)
- [Prevent Screen Lock](#)
- [Using the Sidebar](#)
- [Gestures and Navigation Aids](#)
- [Multitasking](#)
- [Using Horizon Client with a Microsoft Display Dock](#)
- [Copying and Pasting](#)
- [Saving Documents in a Published Application](#)
- [Enable Multi-Session Mode for Published Applications](#)
- [Internationalization](#)

Feature Support Matrix for Windows 10 Clients

When planning which display protocols and features to make available to your end users, use the following information to determine which guest operating systems support the feature.

Table 4-1. Features Supported for Windows Virtual Desktops

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008/2012 R2, Windows Server 2016, or Windows Server 2019 Desktop
USB redirection						
Real-Time Audio-Video (RTAV)						
Serial port redirection						
VMware Blast display protocol	X	X	X			X
RDP display protocol						
PCoIP display protocol	X	X	X	Limited	Limited	X
Persona Management						
Windows Media MMR						
Location-based printing	X	X	X	Limited	Limited	X
Virtual printing						
VMware Virtual Print Redirection						
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 remote desktops require View Agent 6.2 or later or Horizon Agent 7.0 or later. Windows Server 2012 R2 remote desktops require View Agent 6.1 or later or Horizon Agent 7.0 or later. Windows Server 2016 remote desktops require Horizon Agent 7.0.2 or later. Windows Server 2019 remote desktops require Horizon Agent 7.7 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 remote 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 remote desktops with Connection Server 6.1.

For descriptions of these features and their limitations, see the *Horizon 7 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 remote 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 R2 RDS Host	Windows Server 2016 RDS Host	Windows Server 2019 RDS host
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 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	Horizon Agent 7.7 and later
PCoIP display protocol	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Location-based printing	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.0.2 through 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.7 and later

For information about which editions of each guest operating system are supported, see "Supported Operating Systems for Horizon Agent" in the *Horizon 7 Installation* document.

Using Full-Screen Mode

If you are using a Surface Pro 4 or Surface Book, you can display remote desktops and published applications in full-screen or windowed mode. Full-screen mode is enabled by default.

After you log in to a remote desktop or published application, you can toggle full-screen mode on or off by tapping **Fullscreen** in the **Option** menu in the remote desktop or published application window.

Using DPI Synchronization

The DPI Synchronization feature ensures that the DPI (dots per inch) setting in a remote desktop or published application matches the client machine's DPI setting.

If you want to adjust the resolution manually, you can turn off the **Allow display scaling** option in Horizon Client and select a resolution. For more information, see [Adjust the Screen Resolution for Remote Desktops and Published Applications](#).

If DPI synchronization is disabled, display scaling is used. The Display Scaling feature scales the remote desktop or published application appropriately.

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default. With DPI Synchronization, the DPI value in the remote session changes to match the DPI value of the client machine when you connect to a remote desktop or published application. The DPI Synchronization feature requires Horizon Agent 7.0.2 or later.

If the **DPI Synchronization Per Connection** agent group policy setting is enabled in addition to the **DPI Synchronization** group policy setting, DPI Synchronization is supported when you reconnect to a remote desktop. This feature is disabled by default. The DPI Synchronization Per Connection feature requires Horizon Agent 7.8 or later.

For more information about the **DPI Synchronization** and **DPI Synchronization Per Connection** group policy settings, see the *Configuring Remote Desktop Features in Horizon 7* document.

For virtual desktops, the DPI Synchronization feature is supported on the following guest operating systems:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop
- Windows Server 2019 configured as a desktop

For published desktops and published applications, the DPI Synchronization feature is supported on the following RDS hosts:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

For virtual desktops, the DPI Synchronization Per Connection feature is supported on the following guest operating systems:

- Windows 10 version 1607 and later
- Windows Server 2016 and later configured as a desktop

The DPI Synchronization Per Connection feature is not supported for published desktops or published applications.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, but the DPI setting does not change in the remote desktop, you might need to log out and log in again to make Horizon Client aware of the new DPI setting on the client system.
- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you might need to log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.
- If a Horizon administrator changes the **DPI Synchronization** group policy setting value for Horizon Agent, you must log out and log in again to make the new setting take effect.

Adjust the Screen Resolution for Remote Desktops and Published Applications

You can adjust the screen resolution manually for remote desktops and published applications.

Procedure

- 1 Open the **Option** menu.
 - If you are not connected to a server, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.
 - If you are connected to a server, but you are not yet connected to a remote desktop or published application, 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 published application, tap the **Option** button in the floating menu and tap **Setting**.
- 2 Toggle the **Allow display scaling** option to **Off**.
- 3 Select a resolution mode.

Configure the Local Zoom Feature

With the local zoom feature, you can pinch your fingers together and apart on a touchscreen to zoom in and out inside a remote desktop or published application.

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. Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2016 support touch input.

Procedure

- 1 Connect to a remote desktop or published application.
- 2 Tap the **Option** button in the floating menu in the remote desktop or published application window and tap **Setting**.
- 3 Expand the **Advanced** section and tap to toggle the **Local Zoom** option to **On** or **Off**.

Prevent Screen Lock

After a certain amount of idle time, the client 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 published 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 the device's user settings.

Procedure

- 1 Connect to the remote desktop or published application.
- 2 Tap the **Option** button in the floating menu in the remote desktop or published application window and tap **Setting**.
- 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 published application, you can use the sidebar to open other remote desktops and published applications.

Table 4-3. Sidebar Actions

Action	Description
Show the sidebar	Tap the Option button in the remote desktop or published application window and tap Sidebar .
Hide the sidebar	Tap anywhere inside the remote desktop or published application window.

Table 4-3. Sidebar Actions (Continued)

Action	Description
Open a remote desktop or published application	Tap the name of the remote desktop or published application in the sidebar.
	Note To avoid losing data, save your data before switching from a published application that is in multi-session mode.
Search for a remote desktop or published application	Type the name of the remote desktop or published application in the Search box. To open the remote desktop or published 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 [Configure the Local Zoom Feature](#). 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.

Using Windows Key Combinations

After you log in to a remote desktop or application, you can tap the **Combination Key** button in the floating menu to use the following Windows key combinations:

- Ctrl+Alt+Del
- Win+R
- Alt+F4
- Alt

Note Win+R is available only in remote desktop sessions.

Sound, Music, and Video

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

Multitasking

You can switch between Horizon Client and other apps without losing a remote desktop or published application connection, and 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, you receive a prompt before the session times out, asking if you want to keep the session alive. To keep the session alive, tap or click anywhere on the screen, or press a key on your keyboard. If enough time has passed so that the connection to the remote desktop or published application is 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

By default, you can copy and paste from the local client system to a remote desktop or published application. You can also copy and paste from a remote desktop or published application to the client system, or between two remote desktops or published applications, if a Horizon administrator enables these features.

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

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

A Horizon administrator configures the ability to copy and paste by setting agent group policies. Depending on the Horizon server and agent version, a Horizon administrator 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 copy and paste feature has the following limitations.

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

Logging Copy and Paste Activity

When you enable the clipboard audit feature, Horizon Agent records information about copy and paste activity in an event log on the agent machine. The clipboard audit feature is disabled by default.

To enable the clipboard audit feature, you must configure the **Configure clipboard audit** group policy setting for VMware Blast or PCoIP.

You can optionally configure the **Whether block clipboard redirection to client side when client doesn't support audit** group policy setting for VMware Blast or PCoIP to specify whether to block clipboard redirection to clients that do not support the clipboard audit feature.

For information about configuring these group policy settings, see the "VMware Blast Policy Settings" and "PCoIP Clipboard Settings" topics in the *Configuring Remote Desktop Features in Horizon 7* document.

This feature requires Horizon Agent 7.7 or later on the agent machine.

The event log where information about copy and paste activity is recorded is named VMware Horizon RX Audit. To view the event log on the agent machine, use the Windows event viewer. To view the event log from a centralized location, configure VMware Log Insight or Windows Event Collector. For information about Log Insight, go to <https://docs.vmware.com/en/vRealize-Log-Insight/index.html>. For information about Windows Event Collector, see the Microsoft documentation.

Saving Documents in a Published Application

With certain published 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.

A Horizon administrator can use the RDS Profiles group policy setting called **Set Remote Desktop Services User Home Directory** to specify where documents are saved. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Enable Multi-Session Mode for Published Applications

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log on to the server from different client devices.

For example, if you open a published application in multi-session mode on client A, and then open the same published application on client B, the published application remains open on client A and a new session of the published application opens on client B. By comparison, when multi-session mode is disabled (single-session mode), the published application session on client A disconnects and reconnects on client B.

The multi-session mode feature has the following limitations.

- Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.
- If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

A Horizon administrator must enable multi-session mode for the application pool. Users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Setting Up Published Desktops and Applications in Horizon 7*. This feature requires Horizon 7 version 7.7 or later.

Procedure

- 1 Connect to a server.
- 2 Tap the **Option** menu in the upper-left corner of the desktop and application selection window.
- 3 Expand the **Advanced** section and then expand the **Multi-Launch** section.

If no published applications are available to use in multi-session mode, the **Multi-Launch** option does not appear.

- 4 Select the published applications that you want to use in multi-session mode.

If a Horizon administrator has enforced multi-session mode for a published application, you cannot change this setting.

Internationalization

The Horizon Client user interface and 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

You can solve most Horizon Client problems by restarting or resetting remote desktops or published applications, or by reinstalling Horizon Client.

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

This chapter includes the following topics:

- [Resetting a Remote Desktop or Application](#)
- [Uninstall the VMware Horizon Client App](#)
- [Collect Logs to Send to VMware Technical Support](#)
- [Horizon Client Stops Responding or the Remote Desktop Freezes](#)
- [Connecting to a Server in Workspace ONE Mode](#)

Resetting a Remote Desktop or Application

If a remote desktop or published application stops responding, you might need to reset it.

Resetting a remote desktop is the same as 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 published application quits all published applications and logs off all published application sessions. Unsaved changes in published applications might be lost.

To reset a remote desktop or published application, tap the **Disconnect** button in the remote desktop or published application window and tap **Reset**.

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

Uninstall the VMware Horizon Client App

You can sometimes resolve problems with Horizon Client by uninstalling and reinstalling the VMware Horizon Client app.

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

Procedure

- 1 On the client 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 the VMware Horizon Client App](#).

Collect Logs to Send to VMware Technical Support

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

To troubleshoot some issues, you might be directed to collect log files to send to VMware technical support. Because logging can affect the performance of Horizon Client, turn off the advanced logging feature when logging is no longer necessary.

Prerequisites

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

Procedure

- 1 Open the **Option** menu.
 - If you are not connected to a server, tap the **Option** menu in the upper-left corner of the Horizon Client menu bar.
 - If you are connected to a server, but not yet connected to a remote desktop or published application, 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 published application, tap the **Option** button in the floating menu in the remote desktop or application window and tap **Setting**.
- 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 VMware technical support, right-click the folder and select **Send to > Compressed (zipped) folder**.

What to do next

Send the logs to VMware technical support.

Horizon Client Stops Responding or the Remote Desktop Freezes

Horizon Client stops responding or a remote desktop freezes.

Problem

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

Cause

If the server is configured properly and the correct firewall ports are open, the cause of the problem usually relates to Horizon Client on the device or to the remote desktop operating system.

Solution

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

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

Connecting to a Server in Workspace ONE Mode

You cannot connect to a server directly through Horizon Client, or your remote desktop and published application entitlements are not visible in Horizon Client.

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 remote desktop or published 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 remote desktop or published application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or published applications in Horizon Client.

Cause

Beginning with Horizon 7 version 7.2, a Horizon 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 published applications.