VMware Horizon Client for Linux User Guide

Modified on 4 JAN 2018
VMware Horizon Client for Linux 4.7

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

Contents

VMware Horizon Client for Linux User Guide

This document, *VMware Horizon Client for Linux User Guide*, explains how to use VMware Horizon® Client™ for Linux to connect to and use remote desktops and applications.

For information about the software installed on your remote desktops, contact your system administrator.

This document assumes that Horizon Client for Linux is already installed and configured on your client system. For information about installing and configuring Horizon Client for Linux, see the *VMware Horizon Client for Linux Installation and Setup Guide* document.

How Do I Log In?

1

Before you can log in and connect to a remote desktop or application, a system administrator at your company must set up your user account. If your system administrator has not set up your user account, you cannot use Horizon Client or HTML Access.

If Horizon Client prompts you for a server name and domain name, your system administrator must tell you the server name to type and domain to select. At some companies, Horizon Client automatically connects to the correct server and selects the correct domain for you.

If you do not know your user name or password or how to reset your password, contact the system administrator at your company.

When you are ready to log in and get started, see Connect to a Remote Desktop or Application.

Connecting to Remote Desktops and Applications 2

You can use Horizon Client to connect to remote desktops and applications.

This chapter includes the following topics:

Setting the Certificate Checking Mode in Horizon Client

You can determine whether client connections are rejected if any or some server certificate checks fail by configuring a setting in Horizon Client.

Note At some companies, an administrator might set the default certificate verification mode and prevent end users from changing it in Horizon Client.

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

- 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.

In addition to presenting a server certificate, the server also sends a certificate thumbprint to Horizon Client. The thumbprint is a hash of the certificate public key and is used as an abbreviation of the public key. If the server does not send a thumbprint, you see a warning that the connection is untrusted.

If your Horizon administrator has allowed it, you can set the certificate checking mode. To set the certificate checking mode, start Horizon Client and select **File > Preferences** from the menu bar. You have three 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.
- **Warn before connecting to untrusted servers**. If a certificate check fails because the server uses a self-signed certificate, you can click **Continue** to ignore the warning. For self-signed certificates, the certificate name is not required to match the server name you entered in Horizon Client.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

Connect to a Remote Desktop or Application

After logging in to a server, you can connect to the remote desktops and applications that you are authorized to use.

If your administrator has allowed it, you can configure the certificate checking mode for the SSL certificate presented by Connection Server. To determine which mode to use, see Setting the Certificate Checking Mode in Horizon Client.

If you want to use an account configured with unauthenticated access to launch published applications, see Connect to Published Applications Using Unauthenticated Access for information.

Prerequisites

Obtain the following information from your View administrator:

- Instructions about whether to turn on a VPN (virtual private network) connection.
- Server name to use for connecting to the server.
- If the port is not 443, the port number to use for connecting to the server.
- Credentials to log in, such as an Active Directory user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).
- Domain name for logging in.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Either open a terminal window and enter `vmware-view` or search the applications for **VMware Horizon Client**, and double-click the icon.
3. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **OK**.

4 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.

   If the **Domain** drop-down menu is disabled, you must type the user name as **`domain\username`** or **`username@domain`**.

   b (Optional) Select a domain value from the **Domain** drop-down menu.

   c Click **OK**.

5 If the desktop security indicator turns red and a warning message appears, respond to the prompt.

   Usually, this warning means that Connection Server did not send a certificate thumbprint to the client. The thumbprint is a hash of the certificate public key and is used as an abbreviation of the public key.

6 (Optional) To configure display settings for remote desktops, either right-click a desktop icon or select a desktop icon and click the **Settings** (gear-shaped) icon next to the server name in the upper portion of the window.

Option	Description
Display protocol	If the Horizon administrator has allowed it, you can use the **Connect Via** list to select the display protocol. To use VMware Blast, Horizon Agent 7.0 or later must be installed.
Display layout	Use the **Display** list to select a window size or to use multiple monitors.

7 (Optional) To mark the remote desktop or application as a favorite, right-click the desktop or application icon and select **Mark as Favorite** from the context menu that appears.

   A star icon appears in the upper-right corner of the desktop or application name. The next time you log in, you can click the **Show Favorites** button to find this application or desktop quickly.

8 Double-click a remote desktop or application to connect.

   If you are connecting to a session-based remote desktop, which is hosted on a Microsoft RDS host, and if the desktop is already set to use a different display protocol, you will not be able to connect immediately. You will be prompted to either use the protocol that is currently set or have the system log you off of the remote operating system so that a connection can be made with the protocol you selected.

After you are connected, the client window appears.

Connect to Published Applications Using Unauthenticated Access

You can connect to published applications using an unauthenticated access account with Horizon Client.

Prerequisites

Obtain the following information from your Horizon administrator:

- Instructions about whether to turn on a VPN (virtual private network) connection.
- Name of server on which you have unauthenticated access to remote applications.
- If the port is not 443, the port number to use for connecting to the server.
- An Unauthenticated Access user account to use for logging in anonymously, if necessary.
- Instructions about whether to select **Log in anonymously using Unauthenticated Access** in Horizon Client.

If your system administrator instructs you to configure the certificate checking mode, see Setting the Certificate Checking Mode in Horizon Client.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Either open a terminal window and enter `vmware-view` or search the applications for **VMware Horizon Client**, and double-click the icon.
3. In the Horizon Client home screen, select **File > Log in anonymously using Unauthenticated Access** from the menu bar, if it is not already selected.
4. Connect to the Connection Server that is configured for unauthenticated access.
   - If the server that you need has not yet been added, double-click the **+ Add Server** button if no servers have yet been added or click the **+ New Server** button in the menu bar to add a new one, and enter the name of the Connection Server or a security server, and click **Connect**.
   - If the server that you need is displayed in the Horizon Client home screen, right-click the icon for the server and select **Connect** from the context menu.

   You might see a message that you must confirm before the login dialog box appears.
5. In the Server Login dialog box, specify the unauthenticated access account to use.
   a. Select a user account from the drop-down list of existing unauthenticated access accounts.

      The default user account has `(default)` displayed next to it.

   b. (Optional) Click **Always use this account** if you want to bypass the Server Login dialog box the next time you connect to the server.

   c. Click **OK**.

The application selector window appears and displays the published applications that the unauthenticated access account is authorized to use.

Note If you had selected the **Always use this account** option during a previous unauthenticated access login session, you will not be prompted for the account to use for the current unauthenticated access session. To deselect this option, right-click the icon for the server in the Horizon Client home screen, and select **Forget the saved Unauthenticated Access account** from the context menu.

6 To start an application, double-click the application icons to launch it.

The application window appears.

7 Exit the application after you are done using it.

The Disconnect from Session dialog box appears asking if you want to disconnect from the server.

If the session timeout specified by your Horizon administrator is reached, the session is automatically disconnected from the server.

Log Off or Disconnect

With some configurations, if you disconnect from a remote desktop without logging off, applications in the desktop can remain open. You can also disconnect from a server and leave published applications running.

Even if you do not have a remote desktop open, you can log off of the remote desktop operating system. Using this feature has the same result as sending Ctrl+Alt+Del to the desktop and then clicking **Log Off**.

Procedure

- Disconnect without logging off.

Option	Action
Also quit Horizon Client	Click the **Close** button in the corner of the window or select **File > Quit** from the menu bar.
Choose a different remote desktop on the same server	Select **Desktop > Disconnect** from the menu bar.
Choose a remote desktop on a different server	Select **File > Disconnect from server** from the menu bar.

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

- Log off and disconnect from a remote desktop.

Option	Action
From within the desktop OS	Use the Windows **Start** menu to log off.
From the menu bar	Select **Desktop > Disconnect and Log off**. If you use this procedure, files that are open on the remote desktop will be closed without being saved first.

- Log off when you do not have a remote desktop open.
  a From the Home screen with desktop shortcuts, select the desktop and select **Desktop > Log off** from the menu bar.
  b If prompted, supply credentials for accessing the remote desktop.

  If you use this procedure, files that are open on the remote desktop will be closed without being saved first.

Using Remote Desktops and Applications

3

You can use Horizon Client to connect to remote desktops and applications. Horizon Client includes additional features to aid navigation.

This chapter includes the following topics:

Share Access to Local Folders and Drives with Client Drive Redirection

You can use Horizon Client to share folders and drives on the local client system with remote desktops and applications. This feature is called client drive redirection.

Drives can include mapped drives and USB storage devices.

In a Windows remote desktop, shared folders and drives appear in the **This PC** folder or in the **Computer** folder, depending on the Windows operating system version. In a published application, such as Notepad, you can browse to and open a file in a shared folder or drive.

You do not need to be connected to a remote desktop or application to configure client drive redirection settings. The settings apply to all remote desktops and applications. That is, you cannot configure the settings so that local client folders are shared with one remote desktop or application, but not with other remote desktops or applications.

The client drive redirection feature requires that the following library files be installed. On some thin client machines, these library files might not be installed by default.

- `libsigc-2.0.so.0`
- `libglibmm-2.4.so.1`

Prerequisites

To share folders and drives with a remote desktop or application, a Horizon administrator must have enabled the client drive redirection feature.

Procedure

1 Open the Settings dialog box with the Sharing panel displayed.

Option	Description
From the desktop and application selection window	Right-click a desktop or application icon, select **Settings**, and click **Sharing**. Alternatively, select **Connection > Settings** from the menu bar and click **Sharing**.
From the Sharing dialog box when you connect to a desktop or application	Click **Allow** to share, or **Deny** to not share, your home directory.
From within a desktop OS	Select **Connection > Settings** from the menu bar and click **Sharing**.

2 Configure the client drive redirection settings.

Option	Action
Share a specific folder or drive with remote desktops and applications	Click the **Add** button, browse to and select the folder or drive to share, and click **OK**. **Note** You cannot share a folder on a USB device if the device is already connected to a remote desktop or application with the USB redirection feature.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the **Remove** button.
Allow remote desktops and applications access to files in your home directory	Select the **Share your home folder:** *home-directory* check box.
Share USB storage devices with remote desktops and applications	Select the **Allow access to removable storage** check box. The client drive redirection feature automatically shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives. You do not need to select a specific device to share. **Note** USB storage devices already connected to a remote desktop or application with the USB redirection feature are not shared. If this check box is deselected, you can use the USB redirection feature to connect USB storage devices to remote desktops and applications.
Do not show the Sharing dialog box when you connect to a remote desktop or application	Select the **Do not show dialog when connecting to a desktop or application** check box. If this check box is deselected, the Sharing dialog box appears the first time you connect to a desktop or application after you connect to a server. For example, if you log in to a server and connect to a desktop, you see the Sharing dialog box. If you then connect to another desktop or application, you do not see the dialog box again. To see the dialog box again, you must disconnect from the server and then log in again.

What to do next

Verify that you can see the shared folders from within the remote desktop or application:

- From within a Windows remote desktop, open File Explorer and look in the **This PC** folder, or open Windows Explorer and look in the **Computer** folder, depending on the Windows operating system version.
- From within a published application, if applicable, select **File > Open** or **File > Save As** and navigate to the folder or drive.

The folders and drives that you selected for sharing might use one or more of the following naming conventions:

- ***name* on *MACHINE-NAME***. For example, **jsmith on JSMITH-W03**.
- ***N* on *MACHINE-NAME***. For example, **Z on JSMITH-W03**.
- ***name* (*N*:)**. For example, **jsmith (Z:)**.

A redirected folder can have two entrances, such as **Z on JSMITH-W03** and **jsmith (Z:)**, and both entrances can appear at the same time. If all the volume labels (from A: through Z:) are already in use, the redirected folder has only one entrance, such as **Z on JSMITH-W03**.

Internationalization

The user interface and documentation are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, and Spanish.

If you are using a Ubuntu 10.4 Linux client system and you want to display the client user interface in a language other than English, you must set the client system to use a locale that uses UTF-8 encoding.

Copying and Pasting Text

It is possible to copy text to and from remote desktops and applications. Your View 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.

This feature is available if you use the VMware Blast display protocol or the PCoIP display protocol. Remote applications are supported with Horizon 6.0 or later.

You can copy text from Horizon Client to a remote desktop or application, or the reverse, but the pasted text is plain text.

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

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.

Contact your system administrator to find out where documents created in published applications are saved in your environment.

Switch Remote Desktops or Published Applications

If you are connected to a remote desktop, you can switch to another desktop. You can also connect to published applications while you are connected to a remote desktop.

Procedure

- Select a remote desktop or application from the same server or a different server.

Option	Action
Choose a different desktop or application on the same server	Perform one of the following actions: ■ If you are logged in to a remote desktop and you want to switch to another remote desktop or application that is already running on your client, select the desktop or application from the **View** menu. ■ If you are logged in to a remote desktop or application and you want to switch to another desktop or application that is not running, select **File > Return to Desktop and Applications List** from the menu bar and then launch the desktop or application from the selector window. ■ From the desktop and application selector window, double-click the icon for the other desktop or application. That desktop or application opens in a new window so that you have multiple windows open, and you can switch between them.
Choose a different desktop or application on a different server	Perform either of the following actions: ■ If you want to keep the current desktop or application open and also connect to a remote desktop or application on another server, start a new instance of Horizon Client and connect to the other desktop or application. ■ If you want to close the current desktop and connect to a desktop on another server, go to the desktop selector window, click the **Disconnect** icon in the upper-left corner of the window, and confirm that you want to log off of the server. You will be disconnected from the current server and any open desktop or application sessions. You can then connect to a different server.

Using the Seamless Window Feature

With the Seamless Window feature, you can interact with an application that is running on a remote desktop as if it was a locally running application.

This feature is available only on Ubuntu 14.04 and Ubuntu 16.04 systems.

After you install the client, you must manually configure this feature by setting the following environment variable before starting a Horizon Client session.

```
export ENABLE_SEAMLESS_WINDOW=1
```

Using the Session Collaboration Feature

You can use the Session Collaboration feature to invite other users to join an existing remote desktop session.

Invite a User to Join a Remote Desktop Session

When the Session Collaboration feature is enabled for a remote desktop, you can invite other users to join an existing remote desktop session.

By default, you can send Session Collaboration invitations by email, in an instant message (IM), or by copying a link to the clipboard and forwarding the link to users. To use the email invitation method, an email application must be installed. To use the IM invitation method, Skype for Business must be installed and configured. You can invite only users that belong to a domain that the server allows for authentication. You can invite up to five users by default.

A Horizon administrator can disable the email and IM invitation methods, change the maximum number of collaborators, and disable the Session Collaboration feature. For information about how the Session Collaboration feature behaves at your company, contact your system administrator.

The Session Collaboration feature has the following limitations.

- If you have multiple monitors, only the primary monitor is shown to session collaborators.
- The Session Collaboration feature does not support PCoIP or RDP sessions. You must select the VMware Blast display protocol when you create a remote desktop session.
- H.264 hardware encoding is not supported. If the session owner is using hardware encoding and a collaborator joins the session, both fall back to software encoding.
- Anonymous collaboration is not supported. Session collaborators must be identifiable through Horizon-supported authentication mechanisms.
- Session collaborators must have Horizon Client 4.7 for Windows, Mac, or Linux installed, or they must use HTML Access 4.7. If a session collaborator has an unsupported version of Horizon Client, an error message appears when the user clicks a collaboration link.
- You cannot use the Session Collaboration feature to share Linux remote desktop sessions or published application sessions.

Prerequisites

To invite users to join a remote desktop session, a Horizon administrator must enable the Session Collaboration feature.

Procedure

1 Connect to a remote desktop for which the session collaboration feature is enabled.

You must use the VMware Blast display protocol.

2 In the system tray in the remote desktop, click the VMware Horizon Collaboration icon, for example,  .

The collaboration icon looks different depending on the Windows operating system version.

3 When the VMware Horizon Collaboration dialog box opens, enter the user name (for example, **`testuser`** or **`domain\testuser`**) or the email address of the user that you want to join the remote desktop session.

The first time you enter the user name or email address of a particular user, you must click **Look up "*user*"**, enter a comma (,), or press the **Enter** key to validate the user. The session collaboration feature remembers the user the next time you enter the user's user name or email address.

You can invite up to five users by default. A Horizon administrator can change the maximum number of users that you can invite.

4 Select an invitation method.

The following invitation methods are available by default. A Horizon administrator can disable the email and IM invitation methods.

Option	Action
Email	Copies the collaboration invitation to the clipboard and opens a new email message in the default email application. An email application must be installed to use this invitation method.
IM	Copies the collaboration invitation to the clipboard and opens a new window in Skype for Business. Press Ctrl+V to paste the link into the Skype for Business window. Skype for Business must be installed and configured to use this invitation method.
Copy Link	Copies the collaboration invitation to the clipboard. You must manually open another application, such as Notepad, and press Ctrl+V to paste the invitation.

After you send an invitation, the VMware Horizon Collaboration icon also appears on the desktop and the session collaboration user interface turns into a dashboard that shows the current state of the collaboration session and enables you to take certain actions.

When a session collaborator accepts your invitation and joins the session, the session collaboration feature notifies you and a red dot appears on the VMware Horizon Collaboration icon in the system tray.

What to do next

Manage the collaborative session in the VMware Horizon Collaboration dialog box. See Manage a Collaborative Session.

Manage a Collaborative Session

After you send a session collaboration invitation, the Session Collaboration user interface turns into a dashboard that shows the current state of the collaborative session and enables you to take certain actions.

Prerequisites

Start a collaborative session. See Invite a User to Join a Remote Desktop Session.

Procedure

1. In the remote desktop, click the VMware Horizon Collaboration icon in the system tray, or double-click the VMware Horizon Collaboration icon on the desktop.

   The names of all session collaborators appear in the Name column and their status appears in the Status column.

2. Use the VMware Horizon Session Collaboration dashboard to manage the collaboration session.

Option	Action
Revoke an invitation or remove a collaborator	Click **Remove** in the Status column.
Hand off control to a session collaborator	After the session collaborator joins the session, toggle the switch in the Control column to **On**. To resume control of the session, double-click or press any key. The session collaborator can also give back control by toggling the switch in the Control column to **Off**, or by clicking the **Give Back Control** button.
Add a collaborator	Click **Add Collaborators**.
End the collaborative session	Click **End Collaboration**. All active collaborators are disconnected. You can also end the collaborative session by clicking the VMware Horizon Session Collaboration icon on the desktop and clicking the **Stop** button.

Join a Collaborative Session

To join a collaborative session, you can click the link in a collaboration invitation. The link might be in an email or instant message, or in a document that the session owner forwards to you. Alternatively, you can log in to the server and double-click the icon for the collaborative session in the remote desktop and application selector window.

This procedure describes how to join a collaborative session from a collaboration invitation.

You cannot use the following remote desktop features in a collaborative session.

- USB redirection
- Real-Time Audio-Video (RTAV)
- Multimedia redirection
- Client drive redirection

- Smart card redirection
- Virtual printing
- Clipboard redirection

You cannot change the remote desktop resolution in a collaborative session.

Prerequisites

To join a collaborative session, you must have Horizon Client 4.7 for Windows, Mac, or Linux installed on the client system, or you must use HTML Access 4.7 or later.

Procedure

1. Click the link in the collaboration invitation.

   Horizon Client opens on the client system.

2. Enter your credentials to log in to Horizon Client.

   After you are successfully authenticated, the collaborative session begins and you can see the session owner's remote desktop. If the session owner transfers mouse and keyboard control to you, you can use the remote desktop.

3. To return mouse and keyboard control to the session owner, click the VMware Horizon Session Collaboration icon in the system tray and toggle the switch in the Control column to **Off**, or click the **Give Back Control** button.

4. To leave the collaborative session, click **Options > Disconnect**.

Using External Devices

4

You can use external keyboards, external displays, microphones, and other external devices with remote desktops and applications in Horizon Client.

This chapter includes the following topics:

Keyboards and Monitors

You can use multiple monitors and all types of keyboards with a remote desktop. Certain settings ensure the best possible user experience.

Best Practices for Using Multiple Monitors

Following are recommendations for successfully using multiple monitors with a remote desktop:

- Define the primary monitor as the bottom-left-most monitor.
- Enable Xinerama. If you do not enable Xinerama, the primary display might be identified incorrectly.
- The menu bar will appear on the top-left-most monitor. For example, if you have two monitors side by side and the top of the left monitor is lower than the top of the right monitor, the menu bar will appear on the right monitor because the right monitor is still the top-left-most monitor.
- You can use up to 4 monitors if you have enough video RAM.

  To use more than 2 monitors to display your remote desktop on a Ubuntu client system, you must configure the `kernel.shmmax` setting correctly. Use the following formula:

  max horizontal resolution X *max vertical resolution* X *max number of monitors* X 4

  For example, manually setting `kernel.shmmax` to 65536000 allows you to use four monitors with a screen resolution of 2560x1600.

- Horizon Client uses the monitor configuration that is in use when Horizon Client starts. If you change a monitor from landscape to portrait mode or if you plug an additional monitor in to the client system while Horizon Client is running, you must restart Horizon Client in order to use the new monitor configuration.

Horizon Client supports the following monitor configurations:

- If you use 2 monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.
- If you have a version of Horizon Client that is earlier than 4.0, and you use more than 2 monitors, the monitors must be in the same mode and have the same screen resolution. That is, if you use 3 monitors, all 3 monitors must be in either portrait mode or landscape mode and must use the same screen resolution.
- Monitors can be placed side by side, stacked 2 by 2, or vertically stacked only if you are using 2 monitors.
- If you specify that you want to use all monitors, and if you are using the VMware Blast or PCoIP display protocol, you can specify a subset of adjacent monitors to use by right-clicking the desktop in the desktop selector window, selecting **Full Screen - All Monitors** from the **Display** drop-down list, and clicking to select the monitors you want to use.

  Note If you have a Ubuntu client system, you must select the top-left-most monitor as one of the monitors. For example, if you have 4 monitors stacked 2 X 2, you must select either the 2 monitors on top or the 2 left-most monitors.

Screen Resolution

Consider the following guidelines when setting screen resolutions:

- If you open a remote desktop on a secondary monitor and then change the screen resolution on that monitor, the remote desktop moves to the primary monitor.
- With PCoIP, if you use 2 monitors, you can adjust the resolution for each monitor separately, with a resolution of up to 2560 x 1600 per display. If you use more than 2 monitors, the monitors must use the same screen resolution.
- With the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Hardware Version	Windows Version	Number of 4K Displays Supported
10 (ESXi 5.5.x compatible)	7, 8, 8.x, 10	1
11 (ESXi 6.0 compatible)	7 (3D rendering feature disabled and Windows Aero disabled)	3

Hardware Version	Windows Version	Number of 4K Displays Supported
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1

Note When the remote desktop screen resolution is set to 3840 x 2160 (4K), items on the screen might appear smaller, and you might not be able to use the Screen Resolution dialog box in the remote desktop to make text and other items larger.

- With RDP, if you have multiple monitors, you cannot adjust the resolution for each monitor separately.

Keyboard Limitations

For the most part, keyboards work as well with a remote desktop as they do with a physical computer. Following is a list of the limitations you might encounter, depending on the type of peripherals and software on your client system:

- If you use the PCoIP display protocol and want the remote desktop to detect which keyboard map your client system uses, such as, for example, a Japanese keyboard or a German keyboard, you must set a GPO in the View agent. Use the **Turn on PCOIP user default input language synchronization** policy, available as part of the View PCoIP Session Variables ADM template file. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.
- Some multimedia keys on a multimedia keyboard might not work. For example, the Music key and My Computer key might not work.
- If you connect to a desktop using RDP and if you have the Fluxbox window manager, if a screen saver is running in the remote desktop, after a period of inactivity, the keyboard might stop working.

  Regardless of which window manager you use, VMware recommends turning off the screen saver in a remote desktop and not specifying a sleep timer.

Connect USB Devices

You can access locally attached USB devices, such as thumb flash drives, cameras, and printers, from a remote desktop. This feature is called USB redirection.

With this feature, most USB devices that are attached to the local client system are available from a menu in Horizon Client. You can use the menu to connect and disconnect the devices.

Using USB devices with remote desktops has the following limitations:

- When you access a USB device from a menu in Horizon Client and use the device in a remote desktop, you cannot access the device on the local computer.
- USB devices that do not appear in the menu, but are available in a remote desktop, include human interface devices such as keyboards and pointing devices. The remote desktop and the local computer use these devices at the same time. Interaction with these devices can sometimes be slow because of network latency.

- Large USB disk drives can take several minutes to appear in the desktop.
- Some USB devices require specific drivers. If a required driver is not already installed on a remote desktop, you might be prompted to install it when you connect the USB device to the remote desktop.
- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, you must set Horizon Client to automatically connect USB devices to your remote desktop. Otherwise, if you try to manually redirect the USB device by using a menu item, the device will not be redirected unless you unplug the device and then plug it in again.
- Webcams are not supported for USB redirection using the **Connect USB Device** menu. See Using the Real-Time Audio-Video Feature for Webcams and Microphones.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.
- You cannot format a redirected USB drive in a published desktop on an RDS host unless you connect to the remote desktop as an administrator user.

You can connect USB devices to a remote desktop either manually or automatically.

Note Do not redirect USB devices such as USB Ethernet devices and touch screen devices to the remote desktop. If you redirect a USB Ethernet device, your client system will lose network connectivity. If you redirect a touch screen device, the remote desktop will receive touch input but not keyboard input. If you have set your virtual desktop to autoconnect USB devices, you can configure a policy to exclude specific devices. See "Configuring Filter Policy Settings for USB Devices" in the *Configuring Remote Desktop Features in Horizon 7* document.

Prerequisites

- To use USB devices with a remote desktop, the View administrator must have enabled the USB feature for the remote desktop.
- When Horizon Client was installed, the **USB Redirection** component must have been installed. If you did not include this component in the installation, uninstall the client and run the installer again to include the **USB Redirection** component.

Procedure

- Manually connect a USB device to a remote desktop.
  a Connect the USB device to your local client system.
  b From the Horizon Client menu bar, click **Connect USB Device**.
  c Select the USB device.

  The device is manually redirected from the local system to the remote desktop.

- Connect the USB device to a remote hosted application.
  a In the desktop and application selector window, open the remote application.

    The name of the application is the name that your administrator has configured for the application.

  b In the desktop and application selector window, right-click the application icon and select **Settings**.

  c In the left pane, select **USB Devices**.

  d In the right pane, select the USB device and click **Connect**.

  e Select the application, and click **OK**.

    Note The name of the application in the list comes from the application itself and might not match the application name that your administrator configured to appear in the desktop and application selector window.

    You can now use the USB device with the remote application. After you close the application, the USB device is not released right away.

  f When you are finished using the application, to release the USB device so that you can access it from your local system, in the desktop and application selector window, open the Settings window again, select **USB Devices**, and select **Disconnect**.

- Configure Horizon Client to connect USB devices automatically to the remote desktop when Horizon Client starts.

  This option is selected by default.

  a Before you plug in the USB device, start Horizon Client and connect to a remote desktop.

  b From the Horizon Client menu bar, click **Connect USB Device**.

  c Select **Automatically Connect at Startup**.

  d Plug in the USB device and restart Horizon Client.

  USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop. USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop.

- Configure Horizon Client to connect USB devices automatically to the remote desktop when you plug them in to the local system.

  Enable this option if you plan to connect devices that use MTP drivers, such as Android-based Samsung smart phones and tablets. This option is selected by default.

  a Before you plug in the USB device, start Horizon Client and connect to a remote desktop.

  b From the Horizon Client menu bar, click **Connect USB Device**.

c Select **Automatically Connect when Inserted**.

d Plug in the USB device.

USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop.

If the USB device does not appear in the desktop after several minutes, disconnect and reconnect the device to the client computer.

Using the Real-Time Audio-Video Feature for Webcams and Microphones

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone on a remote desktop. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications, and supports standard webcams, audio USB devices, and analog audio input.

Note This feature is available only with the version of Horizon Client for Linux provided by third-party vendors or with the Horizon Client software available from the VMware Product Downloads Web site.

When You Can Use a Webcam

If a Horizon administrator has configured the Real-Time Audio-Video feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, a webcam that is built-in or connected to the local client computer can be used on a remote desktop. You can use the webcam in conferencing applications such as Skype, Webex, or Google Hangouts.

During the setup of an application such as Skype, Webex, or Google Hangouts on the remote desktop, you can choose input and output devices from menus in the application. For virtual machine desktops, you can choose VMware Virtual Microphone and VMware Virtual Webcam. For published desktops, you can choose Remote Audio Device and VMware Virtual Webcam.

With many applications, however, this feature will just work, and selecting an input device is not necessary.

If the webcam is currently being used by the local client computer it cannot be used by the remote desktop simultaneously. Also, if the webcam is being used by the remote desktop it cannot be used by the local client computer at the same time.

If more than one webcam is connected to the local client computer, you can configure a preferred webcam to use on remote desktops.

Select a Default Microphone on a Linux Client System

If you have multiple microphones on your client system, only one of them is used on your Horizon 7 desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

1. In the Ubuntu graphical user interface, select **System > Preferences > Sound**.

   You can alternatively click the **Sound** icon on the right side of the toolbar at the top of the screen.
2. Click the **Input** tab in the Sound Preferences dialog box.
3. Select the preferred device and click **Close**.

Set Printing Preferences for a Virtual Printer Feature on a Remote Desktop

With the virtual printing feature, you can use local or network printers from a remote desktop without having to install additional print drivers in the remote desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and other settings.

Important The virtual printing feature is available only with Horizon Client 3.2 or a later release that is available from the VMware Product Downloads Web site, or with the version of Horizon Client for Linux that is provided by third-party vendors.

This feature also has the following requirements:

- The remote desktop must have View Agent 6.0.2 or later, or Horizon Agent 7.0 or later, installed.
- You must be using the VMware Blast or PCoIP display protocol.

For more information about VMware thin-client and zero-client partners, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=vdm. For client software provided by third-party vendors, you must be using the VMware Blast, PCoIP, or FreeRDP display protocol. This feature does not work with rdesktop.

After a printer is added on the local client computer, Horizon Client adds that printer to the list of available printers on the remote desktop. No further configuration is required. If you have administrator privileges, you can still install printer drivers on the remote desktop without creating a conflict with the virtual printer component.

Important This feature is not available for the following types of printers:

- USB printers that are using the USB redirection feature to connect to a virtual USB port in the remote desktop.

  You must disconnect the USB printer from the remote desktop in order to use the virtual printing feature with it.

- The Windows feature for printing to a file.

  Selecting the **Print to file** check box in a Print dialog box does not work. Using a printer driver that creates a file does work. For example, you can use a PDF writer to print to a PDF file.

This procedure applies to remote desktops that have a Windows 7 or Windows 8.x (desktop) operating system. The procedure is similar, but not exactly the same, for Windows Server 2008 and Windows Server 2012.

Procedure

1. In the Windows 7 or Windows 8.x remote desktop, click **Start > Devices and Printers**.
2. In the Devices and Printers window, right-click the default printer, select **Printer Properties** from the context menu, and select the printer.

   Virtual printers appear as *<printer_name>* in single-user virtual machine desktops and as *<printer_name>(s<session_ID>)* in published desktops on RDS hosts if View Agent 6.2 or later, or Horizon Agent 7.0 or later, is installed. If View Agent 6.1 or earlier is installed in the remote desktop, virtual printers appear as *<printer_name>#:<number>*.
3. In the Printer Properties window, click the **Device Setup** tab and specify which settings to use.
4. On the **General** tab, click **Preferences** and specify which settings to use.
5. In the Printing Preferences dialog box, select the different tabs and specify which settings to use.

   For the **Page Adjustment** advanced setting, VMware recommends that you retain the default settings.
6. Click **OK**.

Troubleshooting Horizon Client 5

You can solve most problems with Horizon Client by restarting or resetting the desktop, or by reinstalling the VMware Horizon Client application.

This chapter includes the following topics:

Restart a Remote Desktop

You might need to restart a remote desktop if the desktop operating system stops responding. Restarting a remote desktop is the equivalent of the Windows operating system restart command. The desktop operating system usually prompts you to save any unsaved data before it restarts.

You can restart a remote desktop only if a Horizon administrator has enabled the desktop restart feature for the desktop.

Procedure

- Use the **Restart** command.

Option	Action
From within the desktop	Select **Connection > Restart Desktop** from the menu bar.
From the desktop selection window	Select the remote desktop and select **Connection > Restart Desktop** from the menu bar.

  Horizon Client prompts you to confirm the restart action.

The operating system in the remote desktop reboots and Horizon Client disconnects and logs off from the desktop.

What to do next

Wait an appropriate amount of time for system startup before you attempt to reconnect to the remote desktop.

If restarting the remote desktop does not solve the problem, you might need to reset the remote desktop. See Reset a Remote Desktop or Published Applications.

Reset a Remote Desktop or Published Applications

You might need to reset a remote desktop if the desktop operating system stops responding and restarting the remote desktop does not solve the problem. Resetting published applications quits all open applications.

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 and are not saved.

Resetting published applications is the equivalent of quitting the applications without saving any unsaved data. All open published applications are closed, even applications that come from different RDS server farms.

You can reset a remote desktop only if a Horizon administrator has enabled the desktop reset feature for the desktop.

Procedure

- Use the **Reset** command.

Option	Action
Reset a remote desktop from within the desktop	Select **Connection > Reset** from the menu bar.
Reset a remote desktop from the desktop and application selection window	Select the remote desktop and select **Connection > Reset** from the menu bar.
Reset published applications from the desktop and application selection window	Click the **Settings** button (gear icon) in the upper right corner of the window, select **Applications** in the left pane, click **Reset**, and click **Continue**.

When you reset a remote desktop, the operating system in the remote desktop reboots and Horizon Client disconnects and logs off from the desktop. When you reset published applications, the applications quit.

What to do next

Wait an appropriate amount of time for system startup before attempting to reconnect to the remote desktop or published application.

Uninstall Horizon Client for Linux

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

The method you use for uninstalling Horizon Client for Linux depends on the version and the method you used for installing the client software.

Prerequisites

Verify that you have root access on the Linux client system.

Procedure

- If you have Horizon Client 3.1 or earlier, or if you installed the client from the Ubuntu Software Center, select **Applications > Ubuntu Software Center**, and in the **Installed Software** section, select **vmware-view-client** and click **Remove.**
- If you have Horizon Client 3.2 or later, which you installed from the VMware Product Downloads Web site, open a Terminal window, change directories to the directory that contains the installer file, and run the installer command with the –u option.

  ```
  sudo env VMWARE_KEEP_CONFIG=yes \

  ./VMware-Horizon-Client-x.x.x-yyyyyyy.arch.bundle -u vmware-horizon-client
  ```

  In the file name, *x.x.x* is the version number, *yyyyyyy* is the build number, and *arch* is either `x86` or `x64`. Using the `VMWARE_KEEP_CONFIG=yes` setting means retain the configuration settings when the client is uninstalled. If this environment variable is not set, you are prompted to specify whether to save the configuration settings.

Problems with Keyboard Input

If, when you type in a remote desktop or application, none of the keystrokes seem to work, the issue might be with security software on your local client system.

Problem

While connected to a remote desktop or application, no characters appear when you type. Another symptom might be that a single key keeps repeating itself.

Cause

Some security software, such as Norton 360 Total Security, includes a feature that detects keylogger programs and blocks keystroke logging. This security feature is meant to protect the system against unwanted spyware that, for example, steals passwords and credit card numbers. Unfortunately, this security software might block Horizon Client from sending keystrokes to the remote desktop or application.

Solution

- On the client system, turn off the keylogger detection feature of your antivirus or security software.

What to Do If Horizon Client Exits Unexpectedly

Horizon Client might exit even if you do not close it.

Problem

Horizon Client might exit unexpectedly. Depending on your Connection Server configuration, you might see a message such as `There is no secure connection to the View Connection Server`. In some cases, no message is displayed.

Cause

This problem occurs when the connection to Connection Server is lost.

Solution

- Restart Horizon Client. You can connect successfully as soon as Connection Server is running again. If you continue to have connection problems, contact your Horizon administrator.

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, 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 applications.