Horizon Client for Mac Guide

VMware Horizon Client for Mac 2206

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

https://docs.vmware.com/

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

Contents

Horizon Client for Mac Guide

This guide provides information about installing, configuring, and using VMware Horizon® Client™ software on a Mac.

How to Use This Guide

To get the help that you need from this guide, refer to the chapters that apply to your role and use case.

For administrators - If you are an administrator who needs to set up a Horizon 8 deployment that includes Mac client systems, see the following chapters. These chapters are written for experienced system administrators who are familiar with virtual machine technology and data center operations.

- Chapter 2 System Requirements for Mac Clients
- Chapter 3 Installing and Upgrading Horizon Client on a Mac
- Chapter 4 Configuring Horizon Client on a Mac

For end users and administrators - If you are an end user who needs to use Horizon Client to connect to remote desktops and applicatons and work in remote sessions, see the following chapters. These chapters also contain information relevant to Horizon adminstrators.

- Chapter 5 Connecting to Remote Desktops and Published Applications
- Chapter 6 Using Remote Desktops and Published Applications
- Chapter 7 Using External Devices
- Chapter 8 Troubleshooting Horizon Client

How Do I Log In?

1

Before you can log in and connect to a remote desktop or published application, a system administrator at your company must set up your user account. If Horizon Client prompts you for a server name and domain, your system administrator must tell you the server name to type and the domain to select.

Note 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 Chapter 5 Connecting to Remote Desktops and Published Applications.

System Requirements for Mac Clients

2

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

Mac models

Any 64-bit Intel-based Mac

ARM M1-based Mac running in emulation with Rosetta 2

Memory

At least 4 GB of RAM

Operating systems

- macOS Catalina (10.15)
- macOS Big Sur (11)
- macOS Monterey (12)

Smart card authentication

See Smart Card Authentication Requirements.

Touch ID authentication

See Touch ID Authentication Requirements.

Connection Server and Horizon Agent

Latest maintenance release of Horizon 7 version 7.13 and later releases.

If client systems connect from outside the corporate firewall, use a Unified Access Gateway appliance so that client systems do not require a VPN connection. If your company has an internal wireless network to provide routable access to remote desktops that devices can use, you do not need to set up Unified Access Gateway or a VPN connection.

Display protocols

- PCoIP

- VMware Blast

Network protocols

- IPv4
- IPv6

For information about using Horizon in an IPv6 environment, see the *Horizon Installation and Upgrade* document.

This chapter includes the following topics:

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices. The feature also works with standard conferencing applications. To support Real-Time Audio-Video, your VMware Horizon deployment must meet certain software and hardware requirements.

Virtual desktops

When using Microsoft Teams with Real-Time Audio-Video, virtual desktops must have a minimum of 4 vCPUs and 4 GB of RAM.

Horizon Client computer or client access device

- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. You do not need to install the device drivers on the machine where the agent is installed.

Display protocols

- PCoIP
- VMware Blast

Smart Card Authentication Requirements

Client devices that use a smart card for user authentication must meet certain requirements.

Client Hardware and Software Requirements

Each client machine that uses a smart card for user authentication must have the following hardware and software.

- Horizon Client
- A compatible smart card reader
- Product-specific application drivers

Users must have a smart card, and each smart card must contain a user certificate. The following smart cards are supported.

- U.S. Department of Defense Common Access Card (CAC)
- U.S. Federal Government Personal Identity Verification (PIV) card (also called FIPS-201 smart cards)
- Gemalto .NET card
- Gemalto IDPrime MD card

For CAC and PIV cards, Horizon Client uses the CryptoTokenKit smart card driver by default and you do not need to install any middleware.

For Gemalto .NET cards, install the correct SafeNet Authentication Client version for your macOS version. Gemalto SafeNet Authentication Client supports both CryptoTokenKit and TokenD smart card drivers for Gemalto .NET smart cards.

You can also use the following third-party smart card drivers with CAC and PIV cards.

- PKard for Mac v1.7 and v1.7.1
- Charismathics (CCSI_5.0.3_PIV)
- Centrify Express

To use a third-party smart card driver, you must disable the CryptoTokenKit smart card driver. For more information, see Disabling the CryptoTokenKit Smart Card Driver.

Agent Software Requirements

A Horizon administrator must install product-specific application drivers on the agent machine.

With PIV cards, the operating system installs the related driver when you insert a smart card reader and PIV card for a Windows 7 virtual desktop. The following agent drivers are supported for PIV cards for Windows 7 virtual desktops.

- Charismathics (CSTC PIV 5.2.2)
- Microsoft minidriver
- ActivClient 6.x

The following agent drivers are supported for PIV cards for Windows 10 virtual desktops.

- Charismathics (CSTC PIV 5.2.2)

- ActivClient 7.x

For Gemalto .NET cards, the Gemalto Minidriver for .NET Smart Card driver is supported.

Enabling the Username Hint Field in Horizon Client

In some environments, smart card users can use a single smart card certificate to authenticate to multiple user accounts. Users enter their user name in the **Username hint** text box when they use a smart card to authenticate.

To make the **Username hint** text box appear on the Horizon Client login dialog box, you must enable the smart card user name hints feature for the Connection Server instance in Horizon Console. For information about enabling the smart card user name hints feature, see the *Horizon Administration* document.

If your environment uses a Unified Access Gateway appliance for secure external access, you must configure the Unified Access Gateway appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Unified Access Gateway 2.7.2 and later. For information about enabling the smart card user name hints feature in Unified Access Gateway, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Note Horizon Client supports single-account smart card certificates, even when the smart card user name hints feature is enabled.

Additional Smart Card Authentication Requirements

In addition to meeting the smart card requirements for Horizon Client systems, other VMware Horizon components must meet certain configuration requirements to support smart cards.

Connection Server and security server hosts

A Horizon administrator must add all applicable Certificate Authority (CA) certificates for all trusted user certificates to a server truststore file on the Connection Server or security server host. These certificates include root certificates and must include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

When you generate a certificate for a blank PIV card, enter the path to the server truststore file on the Connection Server or security server host on the **Crypto Provider** tab in the PIV Data Generator tool.

For information about configuring Connection Server to support smart card use, see the *Horizon Administration* document.

Unified Access Gateway

For information about configuring smart card authentication on a Unified Access Gateway appliance, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Active Directory

For information about tasks that an administrator might need to perform in Active Directory to implement smart card authentication, see the *Horizon Administration* document.

Disabling the CryptoTokenKit Smart Card Driver

To use a third-party smart card driver, you must disable the CryptoTokenKit smart card driver on the client system.

To determine which smart card drivers are installed, type the following command on the client system.

```
#system_profiler SPSmartCardsDataType
```

To determine whether a smart card is supported by the CryptoTokenKit smart card driver, type the following command on the client system.

```
#security list-smartcards
```

To disable the CryptoTokenKit smart card driver for CAC and PIV cards, use the following command on the client system.

```
#sudo defaults write /Library/Preferences/com.apple.security.smartcard DisabledTokens -array
com.apple.CryptoTokenKit.pivtoken
```

To disable the CryptoTokenKit smart card driver for Gemalto .NET cards, use the following command on the client system.

```
#sudo defaults write /Library/Preferences/com.apple.security.smartcard DisabledTokens -array
com.gemalto.Gemalto-Smart-Card-Token.PKCS11-Token
```

Touch ID Authentication Requirements

To use Touch ID for user authentication in Horizon Client, you must meet certain requirements.

Mac models

Any Mac model that supports Touch ID, for example, MacBook Pro.

Operating system requirements

Add at least one fingerprint in the Touch ID setting.

Connection Server requirements

- Enable biometric authentication in Connection Server. For information, see the document.

- The Connection Server instance must present a valid root-signed certificate to Horizon Client.

Horizon Client requirements

- Set the certificate checking mode to **Never connect to untrusted servers** or **Warn before connecting to untrusted servers**. For information about setting the certificate checking mode, see Setting the Certificate Checking Mode in Horizon Client.
- Enable Touch ID when you connect to the server. After you successfully log in, your Active Directory credentials are stored securely on the Mac client system. The Touch ID option is shown the first time you log in and does not appear after Touch ID is enabled.

You can use Touch ID with smart card authentication and as part of two-factor authentication with RSA SecurID and RADIUS authentication. If you use Touch ID with smart card authentication, Horizon Client connects to the server after you enter your PIN and the Touch ID login screen does not appear.

OPSWAT Integration Requirements

At some companies, an administrator might integrate Unified Access Gateway with the third-party OPSWAT MetaAccess application. This integration, which is typically used on unmanaged devices in corporate bring-your-own-device (BYOD) environments, enables organizations to define device acceptance policies for Horizon Client devices.

For example, an administrator might define a device acceptance policy that requires client devices to be password protected or have a minimum operating system version. Client devices that comply with the device acceptance policy can access remote desktops and published applications through Unified Access Gateway. Unified Access Gateway denies access to remote resources from client devices that do not comply with the device acceptance policy.

For more information, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Requirements for Using URL Content Redirection

With the URL Content Redirection feature, URL content can be redirected from the client machine to a remote desktop or published application (client-to-agent redirection), or from a remote desktop or published application to the client machine (agent-to-client redirection).

For example, an end user can click a link in the native Microsoft Word application on the client and the link opens in the remote Internet Explorer application, or an end user can click a link in the remote Internet Explorer application and the link opens in a native browser on the client machine. Any number of protocols can be configured for redirection, including HTTP, mailto, and callto.

A Horizon administrator must also configure settings that specify how Horizon Client redirects URL content from the client to a remote desktop or published application, or how Horizon Agent redirects URL content from a remote desktop or published application to the client.

For complete information, see the "Configuring URL Content Redirection" topic in the *Horizon Remote Desktop Features and GPOs* document.

System Requirements for Skype for Business

An end user can run Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network. During Skype audio and video calls, all media processing takes place on the client machine instead of in the virtual desktop.

To use this feature, the VMware Horizon Virtualization Pack for Skype for Business software must be installed on the client machine. This software is installed by default when Horizon Client for Mac is installed.

A Horizon administrator must also install the VMware Virtualization Pack for Skype for Business feature on the virtual desktop when Horizon Agent is installed. For information about installing Horizon Agent, see the *Windows Desktops and Applications in Horizon* document.

For complete requirements, see "Configure Skype for Business" in the *Horizon Remote Desktop Features and GPOs* document.

System Requirements for the Session Collaboration Feature

With the Session Collaboration feature, users can invite other users to join an existing remote desktop session. To support the Session Collaboration feature, your VMware Horizon deployment must meet certain requirements.

Session collaborators

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

Windows remote desktops

The Session Collaboration feature must be enabled at the desktop pool or farm level. For information about enabling the Session Collaboration feature for desktop pools or farms, see the *Windows Desktops and Applications in Horizon* document.

You can use Horizon Agent group policy settings to configure the Session Collaboration feature. For information, see the *Horizon Remote Desktop Features and GPOs* document.

Linux remote desktops

For Linux remote desktop requirements, see the *Linux Desktops and Applications in Horizon* document.

Connection Server

For Horizon 8 deployments, the Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.

Display protocols

VMware Blast

The Session Collaboration feature does not support published application sessions.

Supported Desktop Operating Systems

A Horizon administrator creates virtual machines that have a guest operating system and installs 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 the *Horizon Installation and Upgrade* document.

Some Linux guest operating systems are also supported. For information about system requirements, configuring Linux virtual machines, and a list of supported features, see the *Linux Desktops and Applications in Horizon* document.

Installing and Upgrading Horizon Client on a Mac

3

This topic describes how to install and upgrade Horizon Client on a Mac.

This chapter includes the following topics:

Preparing Connection Server for Horizon Client

Before end users can connect to a server in a Horizon 8 deployment 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 deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring VMware Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.

If your deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 7.13 and Security Server 7.13 or later. For more information, see the installation document for your server version.

Note Security servers are not supported in VMware Horizon 2006 and later.

Secure Tunnel Connection

If you plan to use a secure tunnel connection for client devices, and if the secure connection is configured with a DNS host name for a Connection Server instance or a security server, verify that the client device can resolve this DNS name. .

Desktop and Application Pools

Use the following check list when configuring 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 *Windows Desktops and Applications in Horizon* document.
- If end users have a high-resolution display and use the **High Resolution Mode** client setting while viewing their remote desktops in full-screen mode, verify that sufficient vRAM is allocated for each Windows remote desktop. The amount of vRAM depends on the display resolution and the number of monitors configured for end users.

User Authentication

Use the following check list when setting up user authentication.

- To enable end users to save their passwords with Horizon Client, so that they do not have to supply credentials when they connect to a Connection Server instance, configure Horizon LDAP for this feature in Connection Server.

  Users can save their passwords if Horizon LDAP is configured to allow it, if the Horizon Client certificate verification mode is set to **Warn before connecting to untrusted servers** or **Never connect to untrusted servers**, and if Horizon Client can fully verify the server certificate that Connection Server presents. For more information, see the *Horizon 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. You can customize the labels on the RADIUS authentication login page and configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *Horizon Administration* document.
- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. For more information, see the *Horizon Administration* document.
- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. This setting is enabled by default. For more information, see the *Horizon Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Console. This setting is deactivated by default. For more information, see the *Horizon Administration* document.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ ***domain\username*** ■ ***username@domain.com***

Install Horizon Client on a Mac

You install Horizon Client on Mac client systems from a disk image file.

Prerequisites

- Verify that the client system uses a supported operating system. See Chapter 2 System Requirements for Mac Clients.
- Verify that you can log in as an administrator on the client system.
- Verify that you have the URL for a download page that contains the Horizon Client installer. This URL might be the VMware Downloads page at http://www.vmware.com/go/viewclients, or it might be the URL for a Connection Server instance.

Procedure

1. On the Mac client system, browse to the URL for downloading the Horizon Client installer file.

   The filename format is `VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.dmg`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

2. Double-click the `.dmg` file and click **Agree**.

   The contents of the disk image appear in a Horizon Client Finder window.

3. In the Finder window, drag the **VMware Horizon Client** icon to the **Applications** folder icon.

   If you are not logged in as an administrator user, the Mac client system prompts you for an administrator user name and password.

What to do next

Start Horizon Client and verify that you can connect to a remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Upgrade Horizon Client Online

You can configure Horizon Client to look for and install updates each time it starts. You can also look for and install updates manually.

If Horizon Client detects a new version, you can download and install the new version, have Horizon Client remind you to install the new version the next time it starts, or skip the new version. If you skip a new version when looking for updates manually, the automatic update process also skips that version.

Procedure

- To configure Horizon Client to look for and install updates each time it starts, select **VMware Horizon Client > Preferences** and select the **Automatically check for updates** check box.

  The **Automatically check for updates** check box is selected by default.

- To look manually for and install an update, select **VMware Horizon Client > Check for Updates**.

Configuring Horizon Client on a Mac

4

This section describes how to configure Horizon Client on a Mac.

This chapter includes the following topics:

Using URIs to Configure Horizon Client

You can use uniform resource identifiers (URIs) to create web page or email links that end users can click to start Horizon Client, connect to a server, or open a remote desktop or published application.

You create these links by constructing URIs that provide some or all the following information so that your end users do not need to supply it.

- Server address
- Port number for the server

- Active Directory user name
- Domain name
- Remote desktop or published application display name
- Window size
- Actions including reset, log out, and start session
- Display protocol
- Options for redirecting USB devices

To construct a URI, you use the `vmware-view` URI scheme with Horizon Client specific path and query parts.

To use URIs to start Horizon Client, Horizon Client must already be installed on client computers.

Syntax for Creating vmware-view URIs

URI syntax includes the `vmware-view` URI scheme, a path part to specify the remote desktop or published application, and, optionally, a query to specify remote desktop or published application actions or configuration options.

URI Specification

Use the following syntax to create URIs to start Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

The only required element is the URI scheme, `vmware-view`. Because the scheme name is case-sensitive for some versions of some client operating systems, type `vmware-view`.

Important In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.utf8-chartable.de/.

authority-part

The server address and, optionally, a user name, a non-default port number, or both. Underscores (_) are not supported in server names. Server names must conform to DNS syntax.

To specify a user name, use the following syntax.

```
user1@server-address
```

You cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax.

```
server-address:port-number
```

path-part

The display name of the remote desktop or published application. The display name is specified in Horizon Console when the desktop pool or application pool is created. If the display name contains a space, use the **%20** encoding mechanism to represent the space.

Alternatively, you can specify a desktop or application ID, which is a path string that includes the desktop or application pool ID. To find a desktop or application ID, open ADSI Edit on the Connection Server host, navigate to `DC=vdi,dc=vmware,dc=int`, and select the `OU=Applications` node. All the desktop and application pools are listed. The `distinguishedName` attribute specifies the ID value. You must encode the ID value before you specify it in a URI, for example, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Note More than one remote desktop or published application can have the same display name, but the desktop and application ID is unique. To specify a particular remote desktop or published application, use the desktop or application ID rather than the display name.

query-part

The configuration options to use, or the remote desktop or published application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If the queries conflict, Horizon Client uses the last query in the list. Use the following syntax.

```
query1=value1[&query2=value2...]
```

Supported Queries

The following queries are supported for this type of Horizon Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the guide document for each type of client system for the list of supported queries.

action

Table 4-1. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when using this action. If you use the `browse` action and specify a remote desktop or published application, the remote desktop or published application is highlighted in the list of available items.
`start-session`	Opens the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified remote desktop or published application. Unsaved data is lost. Resetting a remote desktop is the same as pressing the Reset button on a physical PC.
`restart`	Shuts down and restarts the specified remote desktop. Restarting a remote desktop is the same as the Windows operating system restart command. The operating system usually prompts the user to save any unsaved data before it restarts.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify a published application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add when the published application starts. Use the syntax `args=`*value*, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**
- For a double quotation mark ("), use **`%22`**

For example, to specify the filename "`My new file.txt`" for the Notepad++ application, use **`%22My%20new%20file.txt%22`**.

appProtocol

For published applications, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Connects a USB device to the foreground remote desktop or published application when you plug in the device. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redirects all USB devices that are currently connected to the client system to the remote desktop or published application. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnStartup=true`**.

desktopLayout

Sets the size of the window that displays a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query.

Table 4-2. Valid Values for the desktopLayout Query

Value	Description
`fullscreen`	Full screen on all connected external monitors. This value is the default.
`windowLarge`	Large window.
`windowSmall`	Small window.
*W*x*H*	Custom resolution, where you specify the width by height, in pixels. An example of the syntax is **`desktopLayout=1280x800`**.

desktopProtocol

For remote desktops, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`desktopProtocol=PCOIP`**.

domainName

Specifies the NETBIOS domain name associated with the user who is connecting to the remote desktop or published application. For example, you might use `mycompany` rather than `mycompany.com`.

filePath

Specifies the path to the file on the local system that you want to open with the published application. You can specify the full path or a relative path, for example, `~/username/test%20file.txt`. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**

For example, to represent file path `/Users/username/test file.txt`, use **`/User/username/test%20file.txt`**.

Examples of vmware-view URIs

You can use the `vmware-view` URI scheme to create hypertext links or buttons and include these links in email or on a Web page. For example, an end user can click a URI link to start a remote desktop with the startup options that you specify.

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name `Primary Desktop`, and the user is logged in to the guest operating system.

Note In this example, the default display protocol and window size are used. The default display protocol is PCoIP and the default window size is full screen.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the desktop ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (encoded value `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for the Connection Server instance. (The default port is 443.) Because a remote desktop identifier is provided, the remote desktop opens, even though the `start-session` action is not included in the URI.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`. The user must supply the domain name and password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the published application that has the display name `Calculator`. The connection uses the VMware Blast display protocol.

6
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany
```

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`, and the **Domain** text box is populated with `mycompany`. The user must supply only a password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system.

7
```
vmware-view://view.mycompany.com/
```

Horizon Client starts and the user is taken to the login prompt for connecting to the `view.mycompany.com` server.

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client resets the specified desktop.

Note This action is available only if a Horizon administrator has enabled the reset feature for the remote desktop.

9
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client restarts the specified desktop.

Note This action is available only if a Horizon administrator has enabled the restart feature for the remote desktop.

10
```
vmware-view://
```

Horizon Client starts and the user is taken to the page for entering the address of a server.

11
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Starts My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the published application start command. The filename is enclosed in double quotes because it contains spaces.

12
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Starts Notepad++ 12 on server 10.10.10.10 and passes the argument `a.text b.txt` in the published application start command. Because the argument is not enclosed in quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Published applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code the hypertext link labeled **Test Link** and a button labeled **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</
a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Syntax for Creating vmware-view URIs

URI syntax includes the `vmware-view` URI scheme, a path part to specify the remote desktop or published application, and, optionally, a query to specify remote desktop or published application actions or configuration options.

URI Specification

Use the following syntax to create URIs to start Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

The only required element is the URI scheme, `vmware-view`. Because the scheme name is case-sensitive for some versions of some client operating systems, type `vmware-view`.

Important In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.utf8-chartable.de/.

authority-part

The server address and, optionally, a user name, a non-default port number, or both. Underscores (_) are not supported in server names. Server names must conform to DNS syntax.

To specify a user name, use the following syntax.

```
user1@server-address
```

You cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax.

```
server-address:port-number
```

path-part

The display name of the remote desktop or published application. The display name is specified in Horizon Console when the desktop pool or application pool is created. If the display name contains a space, use the **%20** encoding mechanism to represent the space.

Alternatively, you can specify a desktop or application ID, which is a path string that includes the desktop or application pool ID. To find a desktop or application ID, open ADSI Edit on the Connection Server host, navigate to `DC=vdi,dc=vmware,dc=int`, and select the `OU=Applications` node. All the desktop and application pools are listed. The `distinguishedName` attribute specifies the ID value. You must encode the ID value before you specify it in a URI, for example, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Note More than one remote desktop or published application can have the same display name, but the desktop and application ID is unique. To specify a particular remote desktop or published application, use the desktop or application ID rather than the display name.

query-part

The configuration options to use, or the remote desktop or published application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If the queries conflict, Horizon Client uses the last query in the list. Use the following syntax.

```
query1=value1[&query2=value2...]
```

Supported Queries

The following queries are supported for this type of Horizon Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the installation and setup guide for each type of client system for the list of supported queries.

action

Table 4-3. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when using this action. If you use the `browse` action and specify a remote desktop or published application, the remote desktop or published application is highlighted in the list of available items.
`start-session`	Opens the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified remote desktop or published application. Unsaved data is lost. Resetting a remote desktop is the same as pressing the Reset button on a physical PC.
`restart`	Shuts down and restarts the specified remote desktop. Restarting a remote desktop is the same as the Windows operating system restart command. The operating system usually prompts the user to save any unsaved data before it restarts.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify a published application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add when the published application starts. Use the syntax `args=`*value*, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**
- For a double quotation mark ("), use **`%22`**

For example, to specify the filename "`My new file.txt`" for the Notepad++ application, use **`%22My%20new%20file.txt%22`**.

appProtocol

For published applications, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Connects a USB device to the foreground remote desktop or published application when you plug in the device. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redirects all USB devices that are currently connected to the client system to the remote desktop or published application. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnStartup=true`**.

desktopLayout

Sets the size of the window that displays a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query.

Table 4-4. Valid Values for the desktopLayout Query

Value	Description
`fullscreen`	Full screen on all connected external monitors. This value is the default.
`windowLarge`	Large window.
`windowSmall`	Small window.
*W*x*H*	Custom resolution, where you specify the width by height, in pixels. An example of the syntax is **`desktopLayout=1280x800`**.

desktopProtocol

For remote desktops, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`desktopProtocol=PCOIP`**.

domainName

Specifies the NETBIOS domain name associated with the user who is connecting to the remote desktop or published application. For example, you might use `mycompany` rather than `mycompany.com`.

filePath

Specifies the path to the file on the local system that you want to open with the published application. You can specify the full path or a relative path, for example, `~/username/test%20file.txt`. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**

For example, to represent file path `/Users/username/test file.txt`, use **`/User/username/test%20file.txt`**.

Examples of vmware-view URIs

You can use the `vmware-view` URI scheme to create hypertext links or buttons and include these links in email or on a Web page. For example, an end user can click a URI link to start a remote desktop with the startup options that you specify.

URI Syntax Examples

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name `Primary Desktop`, and the user is logged in to the guest operating system.

Note In this example, the default display protocol and window size are used. The default display protocol is PCoIP and the default window size is full screen.

2
```
vmware-view://view.mycompany.com/
cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the desktop ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (encoded value `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3
```
vmware-view://view.mycompany.com:7555/Primary%20Desktop
```

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for the Connection Server instance. (The default port is 443.) Because a remote desktop identifier is provided, the remote desktop opens, even though the `start-session` action is not included in the URI.

4
```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP
```

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`. The user must supply the domain name and password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

5
```
vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST
```

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the published application that has the display name `Calculator`. The connection uses the VMware Blast display protocol.

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`, and the **Domain** text box is populated with `mycompany`. The user must supply only a password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system.

7 `vmware-view://view.mycompany.com/`

Horizon Client starts and the user is taken to the login prompt for connecting to the `view.mycompany.com` server.

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the reset operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the reset feature for the remote desktop.

9 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the restart operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the restart feature for the remote desktop.

10 `vmware-view://`

Horizon Client starts and the user is taken to the page for entering the address of a server.

11 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

Starts My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the published application start command. The filename is enclosed in double quotes because it contains spaces.

12 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

Starts Notepad++ 12 on server 10.10.10.10 and passes the argument `a.text b.txt` in the published application start command. Because the argument is not enclosed in quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Published applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code the hypertext link labeled **Test Link** and a button labeled **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</
a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Configuring E911 Services for Microsoft Teams

To allow E911 services for the Media Optimization for Microsoft Teams feature, you must manually enable macOS location services for Horizon Client. These services provide the client's geolocation information to Microsoft Teams running in a remote desktop for location-based routing during emergency calls.

Note E911 services require Horizon Agent 2111 or later.

In addition to having macOS location services enabled for Horizon Client, E911 services require certain configurations in the Horizon Agent GPO and on the client system. By default, these configurations are set to allow E911 services and may be changed by an administrator.

- Configure the Horizon Agent GPO. For more information about enabling these services on the agent, see Configuring Media Optimization for Microsoft Teams in the *Horizon Remote Desktop Features and GPOs* document.

With the services configured on the agent, you can configure the local system and the client to share location information.

Share Location Information

To enable location services on the local machine, open **System Preferences**, select **Security & Privacy**, click the **Privacy** tab, and select **Location Services**. Unlock and use the controls to select **Enable Location Services** for the **VMware Horizon Client** app.

Enable Location Sharing in Horizon Client

To enable location sharing in Horizon Client, open the client and select **Settings > Geolocation**.

Configure E911 Services

The `configure.ini` file on the Mac client system includes the **html5mmr.webrtc.supportE911** option which enables or deactivates E911 services. By default, this option is set to the value **1** to enable E911 services.

To deactivate E911 services for the client, set the value to **0**.

The `configure.ini` file on the Mac client system includes the **html5mmr.webrtc.supportE911** option which enables or deactivates E911 services. By default, this option is set to the value **1** to enable E911 services.

To deactivate E911 services for the client, set the value to **0**.

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.

About Certificate Checking

Server certificate checking 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.

For information about distributing a self-signed root certificate and installing it on Mac client systems, see the *Advanced Server Administration* document for the Mac Server that you are using, which is available from the Apple website.

How to Set the Certificate Checking Mode

A system administrator might ask end users to set the certificate checking mode in Horizon Client to make sure that they can successfully connect to a server. At some companies, an administrator might set the certificate checking mode and prevent end users from changing it in Horizon Client.

To set the certificate checking mode, start Horizon Client and select **VMware Horizon Client > Preferences** from the menu bar. You can select one of the following options.

- **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.
- **Warn before connecting to untrusted servers**. This setting means that you can click **Continue** to ignore the warning if a certificate check fails because the server uses a self-signed certificate. For self-signed certificates, the certificate name is not required to match the server name that you entered in Horizon Client. You can also receive a warning if the certificate has expired.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

If an administrator later installs a security certificate from a trusted certificate authority and all certificate checks pass when you connect, this trusted connection is remembered for that specific server. In the future, if that server ever presents a self-signed certificate again, the connection fails. After a particular server presents a fully verifiable certificate, it must always do so.

You can configure the default certificate checking mode and prevent end users from changing it in Horizon Client. For more information, see Configuring the Certificate Checking Mode for End Users.

Using an SSL Proxy Server

If you use an SSL proxy server to inspect traffic sent from the client environment to the Internet, enable the **Allow connection via an SSL Proxy** setting. This setting allows certificate checking for secondary connections through an SSL proxy server and applies to both Blast Secure Gateway and secure tunnel connections. If you use an SSL proxy server and enable certificate checking, but you do not enable the **Allow connection via an SSL Proxy** setting, connections fail because of mismatched thumbprints. The **Allow connection via an SSL Proxy** setting is not available if you enable the **Do not verify server identity certificates** option. When the **Do not verify server identity certificates** option is enabled, Horizon Client does not verify the certificate or thumbprint and an SSL proxy is always allowed.

To allow VMware Blast connections through a proxy server, see Configure VMware Blast Options.

Configuring the Certificate Checking Mode for End Users

You can configure the certificate checking mode for end users. For example, you can configure that full verification is always performed. Certificate checking occurs for TLS connections between a server and Horizon Client.

You can configure one of the following certificate verification strategies for end users.

- End users are allowed to select the certificate checking mode in Horizon Client.
- (No verification) No certificate checks are performed.
- (Warn) If the server presents a self-signed certificate, end users are warned. Users can determine whether to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

If you use an SSL proxy server to inspect traffic sent from the client environment to the Internet, you can configure certificate checking for secondary connections through the SSL proxy server. This feature applies to both Blast Secure Gateway and secure tunnel connections. You can also allow proxy server use for VMware Blast connections.

For information about the types of certificate checks that can be performed, see Setting the Certificate Checking Mode in Horizon Client.

You can configure the certificate checking mode and proxy server settings so that end users cannot change them by setting keys in the `/Library/Preferences/com.vmware.horizon.plist` file on the Mac client.

To configure the certificate checking mode, set the **`Security Mode`** key to one of the following values.

- **1** implements `Never connect to untrusted servers.`
- **2** implements `Warn before connecting to untrusted servers.`
- **3** implements `Do not verify server identity certificates.`

To allow connections through an SSL proxy server, set the **`SSL Proxy Mode`** key to one of the following values.

- **1** enables **Allow connection via an SSL Proxy**
- **0** deactivates **Allow connection via an SSL Proxy**

To allow VMware Blast connections through a proxy server, see #unique_30.

Configure Horizon Client to Select a Smart Card Certificate

You can configure a Horizon Client setting to select a local certificate, or the certificate on a smart card, when you connect to a server. If you do not configure this setting, you must manually select a certificate.

Prerequisites

For your setting to take effect, a Horizon administrator must configure smart card authentication on the server and only one certificate must be available on your client system or smart card.

If you have multiple certificates, Horizon Client always prompts you to select a certificate, regardless of how you configure this setting.

Procedure

1 In the **Applications** folder, double-click **VMware Horizon Client**.

2 Select **VMware Horizon Client > Preferences** from the menu bar.

3 Click **General** in the Preferences dialog box.

4 Select **Automatically select certificate**.

5 Close the Preferences dialog box.

Your changes take effect when the dialog box is closed.

Configure Advanced TLS Options

You can select the security protocols and cryptographic algorithms that VMware Horizon 8 uses to encrypt communications between Horizon Client and servers, and between Horizon Client and Horizon Agent.

Horizon also uses the security options to encrypt the USB channel (communication between the USB plugin 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.

Important At least one of the protocol versions that you enable in Horizon Client must also be enabled in the remote desktop for USB devices to be redirected to the remote desktop.

For information about configuring the security protocols that Connection Server can accept, see the *Horizon Security* document.

Procedure

1 Select **VMware Horizon Client > Preferences** from the menu bar, click **Security**, and click **Advanced**.

2 To enable or disable a security protocol, select the check box next to the security protocol name.

3 To change the cipher control string, replace the default string.

4 (Optional) To revert to the default settings, click **Restore Defaults**.

5 To save your changes, click **Confirm**.

Results

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

Configuring Log File Collection Values

Horizon Client generates log files in the `~/Library/Logs/VMware Horizon Client` directory on the Mac client. An administrator can configure the maximum number of log files, and the maximum number of days to keep log files, by setting keys in the `/Library/Preferences/com.vmware.horizon.plist` file on the Mac client.

Table 4-5. PLIST Keys for Log File Collection

Key	Description
`MaxDebugLogs`	Maximum number of log files. The maximum value is 100.
`MaxDaysToKeepLogs`	Maximum number of days to keep log files. This value has no limit.

Files that do not match these criteria are deleted when you start Horizon Client.

If the `MaxDebugLogs` or `MaxDaysToKeepLogs` keys are not set in the `com.vmware.horizon.plist` file, the default number of log files is five and the default number of days to keep log files is seven.

Configure VMware Blast Options

You can configure VMware Blast options for remote desktop and published application sessions that use the VMware Blast display protocol.

You can allow H.264 decoding and High Efficiency Video Coding (HEVC). H.264 is an industry standard for video compression, which is the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. When H.264 decoding is allowed, you can also allow increased color fidelity.

The maximum resolution that is supported, and whether HEVC is supported, depends on the capability of the graphical processing unit (GPU) on the client. A GPU that can support 4K resolution for JPEG/PNG might not support 4K resolution for H.264. If a resolution for H.264 is not supported, Horizon Client uses JPEG/PNG instead.

If your environment uses a proxy server, you can specify whether to allow VMware Blast connections to an operating system proxy server.

For an SSL proxy server, you also need to configure certificate checking for secondary connections through the SSL proxy server. For more information, see Setting the Certificate Checking Mode in Horizon Client.

You can configure the default HEVC and proxy server options and prevent end users from changing them in Horizon Client. For more information, see #unique_30.

You can configure VMware Blast options before or after you connect to a server.

For administrators - You can configure the VMware Blast HEVC and proxy server options so that end users cannot change them by setting keys in the `/Library/Preferences/com.vmware.horizon.plist` file on the Mac client. To configure the HEVC option, set the **`Allow HEVC`** key to one of the following values.

- **`1`** enables **High Efficiency Video Decoding (HEVC)**
- **`0`** disables **High Efficiency Video Decoding (HEVC)**

To configure the proxy server option, set the **`Blast via Proxy Mode`** key to one of the following values.

- **`1`** enables **Allow Blast connections to use operating system proxy settings**
- **`0`** disables **Allow Blast connections to use operating system proxy settings**

Prerequisites

To use High Efficiency Video Coding (HEVC), your environment must meet the following requirements:

- Horizon Agent 7.13 or later must be installed.
- For increased color accuracy with YUV 4:4:4, Horizon Agent 7.13 or later must be installed.
- Client system must have a GPU that supports HEVC decoding.
- For full-range color and improved color fidelity, Horizon Agent 2203 or later and Horizon Client for Mac 2203 or later must be installed. These features apply only if YUV 4:4:4 is being used.

Depending on the Horizon Agent version that is installed, a Horizon administrator can use agent-side group policy settings to enable or deactivate VMware Blast features, including H.264 and HEVC high color accuracy. For information, see "VMware Blast Policy Settings" in the *Horizon Remote Desktop Features and GPOs* document.

Procedure

1. Start Horizon Client.
2. Select **VMware Horizon Client > Preferences** from the menu bar and click **VMware Blast**.
3. Beginning with Horizon Client for Mac version 2206, both **Allow H.264 Decoding** and **Allow BlastCodec Decoding** options are on by default for Intel-based Mac. If you leave both options selected, BlastCodec is used for receiving remote screen content. If you de-select Allow BlastCodec Decoding, H.264 is used.

   For M1-based Macs, the **Allow H.264 decoding** check box is selected by default. With this setting, Horizon Client uses H.264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. When this option is deselected, Horizon Client uses JPG/PNG decoding.

4 (Optional) To allow increased color fidelity when H.264 decoding is allowed in Horizon Client, select the **Allow high color accuracy (reduces battery life and performance)** check box.

   When this option is selected, Horizon Client uses high color accuracy, but only if the agent supports high color accuracy. Selecting this option might reduce battery life and performance. This feature is deactivated by default.

5 To allow HEVC, select the **Allow High Efficiency Video Decoding (HEVC)** check box.

   When this option is selected, performance and image quality are improved if the client machine has a GPU that supports HEVC decoding. This feature is enabled by default.

   If this option is selected but the client machine does not have a GPU that supports HEVC decoding, or the agent does not support HEVC encoding, Horizon Client uses H.264 decoding instead if H.264 is selected. Horizon Client uses Blast Codec decoding if H.264 is not selected.

6 To allow VMware Blast connections through a proxy server, select the **Allow Blast connections to use operating system proxy settings** check box.

Results

Changes 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.

Configuring Cursor Event Handling

You can optimize cursor event handling by configuring settings in the `~/Library/Preferences/VMware Horizon View/config` file on the Mac client system.

Note To use cursor event handling, Horizon Agent 2006 or later must be installed on the remote desktop.

Setting	Description
`RemoteDisplay.mouseMoveMaxLatencyMsec`	Sets the maximum latency allowed, in milliseconds, when coalescing mouse movement events. Coalescing mouse movement events can reduce client-to-agent bandwidth use, but it can potentially add minor latency to mouse movement. Valid values are 0 through 50. A value of 0 disables the feature. The default value is 0.
`RemoteDisplay.allowCursorWarping`	Enables or disables the cursor warping feature. When this feature is enabled and the mouse is in absolute mode, the remote agent detects sudden cursor movements and reflects them to the client by moving the local cursor. When this feature is disabled, the client ignores sudden cursor movements in the remote agent. Valid values are TRUE or FALSE. The default value is TRUE.
`RemoteDisplay.allowCursorEventsOnLowLatencyChannel`	Determines whether the low-latency channel is used for cursor updates. Valid values are TRUE or FALSE. The default value is TRUE.

You can also configure cursor event handling on the agent machine. For example, you can use the agent-side **Cursor Warping** group policy setting to configure cursor warping, and you can modify Windows registry settings on the agent machine to enable or disable coalescing mouse movement events and the low-latency channel. The settings on both the client and agent must match for the feature to be enabled. For information about the agent-side settings, see the *Horizon Remote Desktop Features and GPOs* document.

Configure Horizon 8 Client Data Sharing

If a Horizon administrator has opted to participate in the VMware Customer Experience Improvement Program (CEIP), VMware collects and receives anonymous data from client systems through Connection Server. You can configure whether to share this client data with Connection Server.

For information about configuring Horizon 8 to join the CEIP, see the *Horizon Administration* document.

Data sharing is enabled by default in Horizon Client. 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.

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.

The information is encrypted when it is in transit to the Connection Server instance. The information on the client system is logged unencrypted in a user-specific directory. The logs do not contain personally identifiable information.

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 Console after the installation.

Table 4-6. Data Collected from Horizon Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous?
Company that produced the Horizon Client application	No
Product name	No
Client product version	No
Client binary architecture	No
Client build name	No
Host operating system	No
Host operating system kernel	No
Host operating system architecture	No
Host system model	No
Host system CPU	No
Number of cores in the host system's processor	No
MB of memory on the host system	No
Number of USB devices connected	No
Maximum concurrent USB device connections	No
USB device vendor ID	No
USB device product ID	No
USB device family	No
USB device use count	No

Procedure

1. Start Horizon Client.
2. Select **VMware Horizon Client > Preferences** from the menu bar and click **General**.
3. Select or deselect the **Allow data sharing** check box.

Configuring Sleep Mode Options

To control sleep mode behavior during remote sessions, you can set keys in the `/Library/Preferences/com.vmware.horizon.plist` file on the Mac client.

Key	Description
`kPreventSystemSleepWhenBeingSessions`	If the value is `true`, Horizon Client prevents the system from going to sleep if remote sessions are connected. If the value is `false`, Horizon Client does not prevent the system from going to sleep. The default value is `true`.
`kPreventSystemSleepBatteryPercentage`	If the battery status is **Not Charging**, and one or more remote sessions are connected, Horizon Client prevents the system from going to sleep if the remaining battery power percentage is not less than the value specified in this key. The default value is 50. If no remote sessions are connected, the client sleeps according to the system settings. This option works only when the `kPreventSystemSleepWhenBeingSessions` is `true`.

MAC Address Deny List

Horizon Client reports the MAC address of the user's local hardware instead of the MAC address of the VPN by using a hard-coded deny list of MAC addresses.

The following MAC addresses are included in the deny list.

```
000000000000
00059a3c7800
00059a3c7a00
00090faa0001
00090ffe0001
001c42000008
001c42000009
005056c00001
005056c00008
00ff091cb893
00ff10404c08
00ff39c549ca
00ff5ab2e94a
00ff5d79fab3
00ffa43eb222
00ffc7cd3234
02004c4f4f50
0205857feb80
025041000001
080027000443
080027000c04
0800270014be
080027002049
08002700281e
```

```
080027003494
0800270034f0
080027004816
08002700509c
0800270074bd
08002700802d
08002700ac25
08002700c4be
08002700c84c
08002700c84e
08002700d49e
08002700e41d
08002700e4a0
08002700e843
08002700e865
08002700e8d3
08002700f061
08002700f091
08002700f4eb
0a0027000000
0a0027000002
0a0027000003
0a002700000d
1e85de8f5e73
2e85de8f5e73
```

In addition, the following MAC address is used for the Touch Bar on many MacBook laptops.

```
acde48001122
```

Configuring Real-Time Audio-Video on a Mac Client

You can configure Real-Time Audio-Video settings at the command line by using the Mac defaults system. With the defaults system, you can read, write, and delete Mac user defaults by using Terminal (`/Applications/Utilities/Terminal.app`).

Mac defaults belong to domains, and domains typically correspond to individual applications. The domain for the Real-Time Audio-Video feature is com.vmware.rtav.

Syntax for Configuring Real-Time Audio-Video

You can use the following commands to configure the Real-Time Audio-Video feature.

Table 4-7. Command Syntax for Real-Time Audio-Video Configuration

Command	Description
`defaults write com.vmware.rtav srcWCamId "`*webcam-userid*`"`	Sets the preferred webcam to use on remote desktops. When this value is not set, the webcam is selected by system enumeration automatically. You can specify any webcam connected to (or built into) the client system.
`defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"`	Sets the preferred microphone (audio-in device) to use on remote desktops. When this value is not set, remote desktops use the default recording device set on the client system. You can specify any microphone connected to (or built into) the client system.
`defaults write com.vmware.rtav srcWCamFrameWidth` *pixels*	Sets the image width. The value defaults to a hardcoded value of 320 pixels. You can change the image width to any pixel value.
`defaults write com.vmware.rtav srcWCamFrameHeight` *pixels*	Sets the image height. The value defaults to a hardcoded value of 240 pixels. You can change the image height to any pixel value.
`defaults write com.vmware.rtav srcWCamFrameRate` *fps*	Sets the frame rate. The value defaults to 15 fps. You can change the frame rate to any value.
`defaults write com.vmware.rtav LogLevel "`*level*`"`	Sets the logging level for the Real-Time Audio-Video log file (`~/Library/Logs/VMware/vmware-RTAV-`*pid*`.log`). You can set the logging level to trace or debug.
`defaults write com.vmware.rtav IsDisabled` *value*	Determines whether Real-Time Audio-Video is enabled or disabled. Real-Time Audio-Video is enabled by default. (This value is not in effect.) To disable Real-Time Audio-Video on the client, set the value to true.
`defaults read com.vmware.rtav`	Displays Real-Time Audio-Video configuration settings.
`defaults delete com.vmware.rtav` *setting*	Deletes a Real-Time Audio-Video configuration setting, for example: `defaults delete com.vmware.rtav srcWCamFrameWidth`

Note You can adjust frame rates from 1 fps up to a maximum of 25 fps and resolution up to a maximum of 1920x1080. A high resolution at a fast frame rate might not be supported on all devices or in all environments.

Working with Shortcut Mappings

This section describes how to set up shortcut mappings for Horizon Client on a Mac.

Considerations for Mapping Operating System Keyboard Shortcuts

Mac and Windows both include default keyboard shortcuts. For example, Command-Tab and Command-Space bar are common keyboard shortcuts on Mac systems and Ctrl+Esc and Alt+Enter are common keyboard shortcuts on Windows systems. If you attempt to map one of these

operating system keyboard shortcuts in Horizon Client, the behavior of the shortcut on the Mac client system and in the remote desktop or published application can be unpredictable.

- If you map a keyboard shortcut, how the shortcut behaves on the Mac client system depends on how the operating system manages the shortcut. For example, the keyboard shortcut might trigger an action in the operating system and Horizon Client might not respond to the shortcut. Alternatively, the keyboard shortcut might trigger an action in both the operating system and Horizon Client.
- Before you map a Mac keyboard shortcut in Horizon Client, you must disable the shortcut in System Preferences on the Mac client system. Not all Mac keyboard shortcuts can be disabled.
- If you map a Windows keyboard shortcut in Horizon Client, the mapped action occurs when you use the shortcut in the remote desktop or published application.
- For published applications, Windows shortcuts that include the Windows key are disabled by default and do not appear on the Horizon Client Keyboard Preferences dialog box. If you create a mapping for one of these disabled keyboard shortcuts, the shortcut appears in the Keyboard Preferences dialog box.

For a list of the default Mac keyboard shortcuts, go to the Apple support website (http://support.apple.com). For a list of the default Windows shortcuts, go to the Microsoft Windows website (http://windows.microsoft.com).

Create Keyboard Shortcut Mappings

You can customize how remote desktops and published applications interpret Apple keyboard shortcuts by creating keyboard shortcut mappings.

When you create a keyboard shortcut mapping, you map an Apple keyboard shortcut to a Windows keyboard shortcut. A keyboard shortcut consists of one or more key modifiers, such as Control and Shift, and a key code. A key code can be any key on your keyboard, except for a modifier key. When you press a mapped keyboard shortcut on your Apple keyboard, the corresponding Windows keyboard shortcut or action occurs in the remote desktop or application.

If you attempt to map an operating system keyboard shortcut, the results can be unpredictable. For more information, see Considerations for Mapping Operating System Keyboard Shortcuts.

Procedure

1. Select **VMware Horizon Client > Preferences** and click **Keyboard & Mouse**.
2. Select the **Key Mappings** tab.

3 Configure the keyboard shortcut mappings.

Option	Action
Delete a keyboard shortcut mapping	Select the mapping to delete and click the minus (-) button.
Add a keyboard shortcut mapping	a Click the plus (+) button. b Specify the Apple keyboard shortcut sequence by clicking one or more keyboard modifiers and typing a key code in the text box. You can also select a key from the drop-down menu. The **From:** field shows the keyboard shortcut that you created. c Specify the corresponding Windows keyboard shortcut sequence by clicking one or more keyboard modifiers and typing a key code in the text box. You can also select a key from the drop-down menu. The **To:** field shows the keyboard shortcut that you created. d To save your changes, click **OK**. The keyboard shortcut mapping is enabled by default (the **On** check box next to the keyboard shortcut mapping is selected).
Modify a keyboard shortcut mapping	Double-click the mapping and make your changes. ■ To modify the Apple keyboard shortcut sequence, click one or more keyboard modifiers and type a key code in the text box. You can also select a key from the drop-down menu. ■ To modify the corresponding Windows keyboard shortcut sequence, click one or more keyboard modifiers and type a key code in the text box. You can also select a key from the drop-down menu. To save your changes, click **OK**.
Disable a keyboard shortcut mapping	Deselect the **On** check box next to the keyboard shortcut mapping. When you disable a keyboard shortcut mapping, Horizon Client does not send the Apple keyboard shortcut to the remote desktop or application.
Enable or disable language-specific key mappings	Select or deselect the **Enable Language Specific Key Mappings** check box. The check box is selected by default.
Restore the default mappings	Click **Restore Defaults**. Any changes that you made to the default keyboard shortcut mappings are deleted and the default mappings are restored.

4 Close the Preferences dialog box.

Your keyboard shortcut mapping changes take effect immediately. You do not need to restart open remote desktops or published applications to make the changes take effect.

Modify the Horizon Client Mouse Shortcut Mappings

You can configure a single-button Apple mouse to send a right-click and a middle-click to remote desktops and published applications. You can modify, enable, or disable the default mouse shortcut mappings. You cannot create mouse shortcut mappings, or delete the default mouse shortcut mappings.

Procedure

1 Select **VMware Horizon Client > Preferences** and click **Keyboard & Mouse**.

2 Select the **Mouse Shortcuts** tab.

3 Modify the mouse shortcut mappings.

Option	Action
Modify a mouse shortcut mapping	Double-click the mapping and make your changes. To save your changes, click **OK** .
Disable a mouse shortcut mapping	Deselect the **On** check box next to the mouse shortcut mapping. When you disable a mouse shortcut mapping, Horizon Client does not send the mouse shortcut to the remote desktop or published application.
Enable a mouse shortcut mapping	Select the **On** check box next to the mouse shortcut mapping. When you enable a mouse shortcut mapping, Horizon Client sends the mouse shortcut to the remote desktop or published application.
Restore the default settings	Click **Restore Defaults**. Any changes that you made to the default mouse shortcut mappings are deleted and the default mappings are restored.

4 Close the Preferences dialog box.

Your mouse shortcut mapping changes take effect immediately. You do not need to restart open remote desktops or published applications to make the changes take effect.

Modify the Horizon Client Shortcuts for Windows Actions

Horizon Client includes preconfigured shortcut mappings for common Windows actions, including Toggle Full Screen, Quit, Hide Application, Cycle Through Windows, and Cycle Through Windows in Reverse. It also includes a preconfigured shortcut mapping for Toggle Exclusive Mode. You can enable or disable the default shortcuts. You cannot create shortcuts or delete the default shortcuts.

Procedure

1 Select **VMware Horizon Client > Preferences** and click **Keyboard & Mouse**.

2 Select the **Horizon Shortcuts** tab.

3 Modify the default shortcuts.

Option	Action
Enable a shortcut	Select the **On** check box next to the shortcut. When you enable a shortcut, Horizon Client does not send the shortcut to the remote desktop or published application.
Disable a shortcut	Deselect the **On** check box next to the shortcut. When you disable a shortcut, Horizon Client sends the shortcut to the remote desktop or published application. **Note** The behavior of the shortcut on the remote desktop or published application can be unpredictable.
Restore the default settings	Click **Restore Defaults**. Any changes that you made are deleted and the default settings are restored.

4 Close the Preferences dialog box.

Your changes take effect immediately. You do not need to restart open remote desktops or published applications to make the changes take effect.

Connecting to Remote Desktops and Published Applications

5

Horizon Client communicates with a server, which acts as a broker between the client device and remote desktops and published applications. You enter credentials into Horizon Client, the server authenticates your credentials, and then the server finds the remote desktops and published applications that you are entitled to use.

This chapter includes the following topics:

Allowing Access to macOS Accessibility Features

You must grant Horizon Client access to the system's accessibility features for optimal performance of the keyboard and mouse inside remote desktops and published applications.

When you first start Horizon Client, Horizon Client prompts you to grant access to the system's accessibility features. If you do not grant access at that time, you can grant access later by going to System Preferences, selecting **Security & Privacy**, clicking the **Privacy** tab, and selecting **Accessibility**.

Connect to a Remote Desktop or Published Application

The procedure for connecting to a remote desktop or published application is slightly different for administrators and end users, so refer to the section that applies to you. See

Procedure for Administrators

Verify that you have completed the following tasks:

- Obtain login credentials, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication credentials, or smart card personal identification number (PIN).
- 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 that the server presents. See Setting the Certificate Checking Mode in Horizon Client.
- If you are using smart card authentication, configure Horizon Client to use a local certificate or the certificate on your smart card automatically. See Configure Horizon Client to Select a Smart Card Certificate.
- If you plan to use Touch ID to authenticate, add at least one fingerprint in the Touch setting on your Mac. Touch ID authentication is available only if biometric authentication is enabled on the server. For complete Touch ID authentication requirements, see Touch ID Authentication Requirements.

Before you have end users access remote desktops and published applications, test that you can connect to a remote desktop or published application from the client system.

1. If a VPN connection is required, turn on the VPN.
2. In the **Applications** folder, double-click **VMware Horizon Client**.
3. Click **Continue** to start the remote USB services, or click **Cancel** to use Horizon Client without the remote USB services. If you click **Continue**, you must provide system credentials. If you click **Cancel**, you can enable the remote USB services later.

   Note The prompt to start the remote USB services appears the first time you start Horizon Client. It does not appear again, regardless of whether you click **Cancel** or **Continue**.

4

Option	Description
Connect to a new server	Click the **New Server** icon on the Horizon Client Home window, enter the server name and port number (if necessary), and click **Connect**. An example of using a non-default port is **`view.company.com:1443`**.
Connect to an existing server	Double-click the server shortcut on the Horizon Client Home window.

5 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the credentials and click **Login**.

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

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

b Select a domain.

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

c (Optional) Select the **Remember this password** check box if this feature is enabled and if the server certificate can be fully verified.

d (Optional) Select the **Enable Touch ID** check box to enable Touch ID authentication.

If Touch ID is enabled and you are logging in for the first time, your Active Directory credentials are stored securely on your Mac for future use.

e Click **Login**.

You might see a message that you must confirm before the login dialog box appears.

7 If you are prompted for Touch ID authentication, place your finger on the Touch ID sensor.

8 If multiple display protocols are configured for a remote desktop, select the protocol to use.

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

Option	Description
Select a display protocol for a remote desktop	Select the remote desktop name, press Control-click, and select the display protocol from the context menu. Alternatively, you can select **Settings** from the context menu and select the display protocol from the **Connect Via** drop-down menu in the Settings dialog box.
Select a display protocol for a published application	Select the published application name, press Control-click, select **Settings** from the context menu, and select the display protocol from the **Preferred protocol** drop-down menu in the Settings dialog box.

9 Double-click a remote desktop or published application to connect to it.

If you are connecting to a published desktop, and if the published desktop is already set to use a different display protocol, you are prompted to either use the protocol that is set or have the system log you off the remote operating system so that a connection can be made with the protocol that you selected.

Note If you are entitled to only one remote desktop on the server, Horizon Client connects to that remote desktop automatically.

If a Horizon administrator has enabled the client drive redirection feature, the Sharing dialog box might appear. From the Sharing dialog box, you can allow or deny access to files on your local system. For more information, see Share Local Folders and Drives.

After you connect to a server for the first time, Horizon Client connects to that server automatically the next time you start Horizon Client. To disable this feature, see Connecting to a Server When Horizon Client Starts.

If Horizon Client cannot connect to the remote desktop or published application, perform the following tasks:

- Verify that the certificate for the server is working properly. If it is not, in Horizon Console, you might also see that Horizon Agent on remote desktops is unreachable.
- Verify that the tags set on the Connection Server instance allow connections from this user. See the *Horizon Administration* document.
- Verify that the user is entitled to access the remote desktop or published application. For information about entitling users, see the *Windows Desktops and Applications in Horizon* document.

Procedure for End Users

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

Obtain the following information from your system 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 for logging in, such as an Active Directory user name and password, RSA SecurID user name and passcode, RADIUS authentication credentials, or smart card personal identification number (PIN).
- Domain name for logging in.
- Instructions about whether you can use Touch ID authentication.

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

If you use smart card authentication, you can configure Horizon Client to use a local certificate automatically, or to use the certificate on your smart card. See Configure Horizon Client to Select a Smart Card Certificate.

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

2 In the **Applications** folder, double-click **VMware Horizon Client**.

3 Click **Continue** to start the remote USB services, or click **Cancel** to use Horizon Client without the remote USB services. If you click **Continue**, you must provide system credentials. If you click **Cancel**, you can enable the remote USB services later.

Note The prompt to start the remote USB services appears the first time you start Horizon Client. It does not appear again, regardless of whether you click **Cancel** or **Continue**.

4

Option	Description
Connect to a new server	Click the **New Server** icon on the Horizon Client Home window, enter the server name and port number (if necessary), and click **Connect**. An example of using a non-default port is **`view.company.com:1443`**.
Connect to an existing server	Double-click the server shortcut on the Horizon Client Home window.

5 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the credentials and click **Login**.

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

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

   b Select a domain.

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

   c (Optional) Select the **Remember this password** check box if this feature is enabled and if the server certificate can be fully verified.

   d (Optional) Select the **Enable Touch ID** check box to enable Touch ID authentication.

   If Touch ID is enabled and you are logging in for the first time, your Active Directory credentials are stored securely on your Mac for future use.

   e Click **Login**.

   You might see a message that you must confirm before the login dialog box appears.

7 If you are prompted for Touch ID authentication, place your finger on the Touch ID sensor.

8 (Optional) If multiple display protocols are configured for a remote desktop, select the protocol to use.

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

Option	Description
Select a display protocol for a remote desktop	Select the remote desktop name, press Control-click, and select the display protocol from the context menu. Alternatively, you can select **Settings** from the context menu and select the display protocol from the **Connect Via** drop-down menu in the Settings dialog box.
Select a display protocol for a published application	Select the published application name, press Control-click, select **Settings** from the context menu, and select the display protocol from the **Preferred protocol** drop-down menu in the Settings dialog box.

9 Double-click a remote desktop or published application to connect to it.

If you are connecting to a published desktop, and if the published desktop is already set to use a different display protocol, you are prompted to either use the protocol that is set or have the system log you off the remote operating system so that a connection can be made with the protocol that you selected.

Note If you are entitled to only one remote desktop on the server, Horizon Client connects to that remote desktop automatically.

If a Horizon administrator has enabled the client drive redirection feature, the Sharing dialog box might appear. From the Sharing dialog box, you can allow or deny access to files on your local system. For more information, see Share Local Folders and Drives.

After you connect to a server for the first time, Horizon Client connects to that server automatically the next time you start Horizon Client. To disable this feature, see Connecting to a Server When Horizon Client Starts.

Connecting to a Server When Horizon Client Starts

After you connect to a server for the first time, Horizon Client connects automatically to that server the next time you start Horizon Client.

To disable this feature, select the server shortcut on the Horizon Client Home window, press Control-click, and deselect the **Always connect at launch** setting.

If there are other server shortcuts on the Horizon Client Home window, you can enable the **Always connect at launch** setting for a different server. You can enable the **Always connect at launch** setting for only one server at a time.

Configure Reconnect Behavior for Published Applications

If you disconnect from a server without closing a published application, Horizon Client prompts you to reopen that published application the next time you connect to the server. You can change this behavior by modifying the Reconnect Behavior setting in Horizon Client.

Prerequisites

Obtain credentials for connecting to the server, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

Procedure

1. On the Horizon Client **Home** window, double-click the server icon.
2. If prompted, supply your credentials.
3. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window.
4. Select **Applications** in the left pane of the Settings dialog box.
5. Select an application reconnect behavior option.

   These options determine how Horizon Client behaves when a user connects to the server and published applications are still running.

Option	Description
Ask to reconnect to open applications	Horizon Client shows the message **You have one or more remote applications running. Would you like to open them now?** You can respond by clicking **Reconnect to Applications** or **Not Now**. You can also select the **Don't show this message again** check box to suppress the message in the future. This setting is enabled by default.
Reconnect automatically to open applications	Horizon Client reopens any running published applications immediately.
Do not ask to reconnect and do not automatically reconnect	Horizon Client does not prompt you to reopen running published applications, nor does it reopen running published applications. This setting has the same effect as the **Don't show this message again** check box.

Results

The new setting takes effect the next time you connect to the server.

Add Horizon Client to the Dock

You can add Horizon Client to the Dock on the Mac client system.

Procedure

1. In the **Applications** folder, select **VMware Horizon Client**.
2. Drag the **VMware Horizon Client** icon to the Dock.
3. To configure the Dock icon to open Horizon Client at login or to show the icon in the Finder, right-click the icon on the Dock, select **Options**, and select the appropriate command from the context menu.

Results

When you quit Horizon Client, the application shortcut remains in the Dock.

Log Out or Disconnect

If you disconnect from a remote desktop without logging out, applications in the remote desktop might remain open. You can also disconnect from a server and leave published applications running.

You can log out from a remote desktop even if you do not have the remote desktop open. This feature has the same result as sending Ctrl+Alt+Del to the remote desktop and then clicking **Log Off**.

Note The Windows key combination Ctrl+Alt+Del is not supported in remote desktops. Instead, select **Connection > Send Ctrl-Alt-Del** from the menu bar. Alternatively, press Fn-Control-Option-Delete on an Apple keyboard.

Procedure

- Disconnect from a remote desktop without logging off.

Option	Action
Disconnect and quit Horizon Client	a Click the **Close** button in the corner of the window, or select **File > Close** from the menu bar. b Select **VMware Horizon Client > Quit VMware Horizon Client** from the menu bar.
Disconnect and remain in Horizon Client	Click the **Disconnect** button in the toolbar, or select **Connection > Disconnect** from the menu bar.

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

- Log out and disconnect from a remote desktop.

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

- Disconnect from a published application.

Option	Action
Disconnect from the server and leave the published application running	Perform one of the following actions: ■ Click the **Disconnect from Server** button in the left side of the toolbar in the desktop and application selection window. ■ Select **File > Disconnect from Server** from the menu bar.
Close the published application and disconnect from the server	a Quit the published application in the usual manner, for example, click the **Close** button in the corner of the application window. b Click the **Disconnect from Server** button in the left side of the toolbar in the desktop and application selection window, or select **File > Disconnect from Server** from the menu bar.

- Log out when you do not have a remote desktop open.

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

Option	Action
From the Home window	a Double-click the server shortcut and supply credentials. b Select the remote desktop and select **Connection > Log Off** from the menu bar.
From the desktop and application selection window	Select the remote desktop and select **Connection > Log Off** from the menu bar.

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, click the **Disconnect from Server** icon in the upper-left corner of the Horizon Client menu bar.

Using Remote Desktops and Published Applications

6

Horizon Client includes additional features to help you use remote desktops and published applications on your local client device.

This chapter includes the following topics:

Feature Support for Mac Clients

Certain guest operating systems and remote desktop features require specific Horizon Agent versions. Use this information when planning which features to make available to your end users.

Supported Windows Virtual Desktops

Windows virtual desktops are single-session virtual machines.

This version of Horizon Client works with Windows virtual desktops that have Horizon Agent 7.13 or later installed. Supported guest operating systems include Windows 7, Windows 8.x, and Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows 7 and Windows 8.x virtual desktops are not supported with Horizon Agent 2006 and later.

Supported Published Desktops on RDS Hosts

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

This version of Horizon Client works with RDS hosts that have Horizon Agent 7.13 or later installed. Supported guest operating systems include Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Window Server 2012 RDS hosts are not supported with Horizon Agent 2006 and later.

Requirements for Specific Features

Most remote desktop features work with Horizon Agent 7.5, but some features require later Horizon Agent versions.

Feature	Requirements
Dragging files and folders	Horizon Agent 7.9 or later
VMware Integrated Printing and location-based printing	Horizon Agent 7.9 or later

This version of Horizon Client for Mac does not support Virtual Printing (also known as ThinPrint).

Supported Linux Desktops

For a list of supported Linux guest operating systems and information about supported features, see the *Linux Desktops and Applications in Horizon* document.

Keyboard Input Source Language Synchronization

When you connect to a remote desktop, the keyboard input source language on the client system is synchronized in the remote desktop.

For example, if the keyboard input source language on a Mac client system (**System Preferences > Keyboard > Input Sources**) is Japanese, Japanese appears in the language bar in the remote desktop.

This feature supports the following keyboard input source languages on the client system.

- English
- French
- German
- Japanese
- Korean
- Spanish
- Simplified Chinese
- Traditional Chinese

Synchronization does not occur if the keyboard input source language is not supported.

Keyboard input source language synchronization is controlled by the agent-side **Keyboard locale synchronization** group policy setting. For more information, see "VMware Blast Group Policy Settings" in the *Horizon Remote Desktop Features and GPOs* document.

Sharing Remote Desktop Sessions

With the Session Collaboration feature, you can invite other users to join an existing remote desktop session. A remote desktop session that is shared in this way is called a collaborative session. The user that shares a session with another user is called the session owner, and the user that joins a shared session is called a session collaborator.

Information for End Users

A Horizon administrator must enable the Session Collaboration feature. Contact your administrator to learn about how the Session Collaboration feature behaves at your company.

Information for Administrators

Enabling the Session Collaboration feature for Windows desktops includes enabling the Session Collaboration feature at the desktop pool or farm level. It can also include using group policies to configure Session Collaboration features, such as the available invitation methods. For complete requirements, see System Requirements for the Session Collaboration Feature.

For information about enabling the Session Collaboration feature for Windows desktops and farms, see the *Windows Desktops and Applications in Horizon* document. For information about using group policy settings to configure the Session Collaboration feature, see the *Horizon Remote Desktop Features and GPOs* document.

For information about enabling the Session Collaboration feature for Linux desktops, see the *Linux Desktops and Applications in Horizon* document.

Invite a User to Join a Remote Desktop Session

With the Session Collaboration feature, you can invite users to join a remote desktop session by sending collaboration invitations by email, in an instant message (Windows remote desktops only), or by copying a link to the clipboard and forwarding the link to users.

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 change the maximum number of users that you can invite.

The Session Collaboration feature has the following limitations.

- If you have multiple monitors, only the primary monitor is shown to session collaborators.
- You must select the VMware Blast display protocol when you create a remote desktop session to share. The Session Collaboration feature does not support PCoIP or RDP sessions.
- 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 for Windows, Mac, or Linux installed, or they must use HTML Access.
- 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 published application sessions.

Prerequisites

- A Horizon administrator must enable and configure the Session Collaboration feature.
- To use the email invitation method, an email application must be installed.
- To use the IM invitation method for a Windows remote desktop, Skype for Business must be installed and configured.

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 might look different, depending on the 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. For Windows remote desktops, the Session Collaboration feature remembers the user the next time you enter the user's user name or email address.

4 Select an invitation method.

   Not all invitation methods might be available.

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	(Windows remote desktops only) 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.

Results

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 to join a Windows remote desktop session, the Session Collaboration feature notifies you and a red dot appears on the VMware Horizon Collaboration icon in the system tray. When a session collaborator accepts your invitation to join a Linux remote desktop session, a notification appears in the primary session desktop.

What to do next

Manage the remote desktop session in the VMware Horizon Collaboration dialog box. See Manage a Shared Remote Desktop Session.

Manage a Shared Remote Desktop Session

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

For administrators - You can prevent the hand-off of control to a session collaborator. For Windows remote desktops, see the **Allow control passing to collaborators** group policy setting in the *Horizon Remote Desktop Features and GPOs* document. For Linux remote desktops, see the `collaboration.enableControlPassing` parameter in the *Linux Desktops and Applications in Horizon* document.

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.

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 collaborative 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. In Windows remote desktops, you can also end the collaborative session by clicking the **Stop** button next to the **VMware Horizon Session Collaboration** icon. The **Stop** button is not available in Linux remote desktops.

Join a Remote Desktop Session

With the Session Collaboration feature, you can click the link in a collaboration invitation to join a remote desktop session. 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 session in the remote desktop and application selector window.

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

Note In a Cloud Pod Architecture environment, you cannot join a collaborative session by logging in to the server unless you log in to the session owner's pod.

When you join a remote desktop session with the Session Collaboration feature, you cannot use the following features in the remote desktop session.

- USB redirection
- Real-Time Audio-Video (RTAV)
- Multimedia redirection
- Client drive redirection
- Smart card redirection
- Microsoft Lync redirection
- File redirection and Keep in Dock functionality
- Clipboard redirection

You also cannot change the remote desktop resolution in the remote desktop session.

Prerequisites

To join a remote desktop session with the Session Collaboration feature, you must have Horizon Client for Windows, Mac, or Linux installed on the client system, or you must use HTML Access.

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 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**.

Searching for Remote Desktops and Published Applications

After you connect to a server, the available remote desktops and published applications on that server appear in the desktop and application selection window. You can search for a particular remote desktop or published application by typing in the window.

When you begin to type, Horizon Client highlights the first matching remote desktop or published application name. To connect to a highlighted remote desktop or published application, press the Enter key. If you continue to type after the first match is found, Horizon Client continues to search for matching remote desktops and published applications. If Horizon Client finds multiple matching remote desktops or published applications, you can press the Tab key to switch to the next match. If you stop typing for two seconds and then begin to type again, Horizon Client assumes that you are starting a new search.

Autoconnect to a Remote Desktop

You can configure a server to open a particular remote desktop when you connect to that server. You cannot configure a server to open a published application.

If you are entitled to only one remote desktop on the server, Horizon Client always opens that remote desktop when you connect to the server.

Prerequisites

Obtain credentials for connecting to the server, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

Procedure

1. On the Horizon Client Home window, double-click the server icon.
2. If prompted, supply your credentials.
3. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window.
4. Select the remote desktop in the left pane of the Settings dialog box.
5. Select **Autoconnect to this desktop**.

Open a Recent Remote Desktop or Published Application

You can open recent remote desktops and published applications in Horizon Client.

Recent remote desktops and published applications appear in the order in which they were opened. If you are not already connected to the server when you open a recent remote desktop or published application, the server login screen appears and you must provide your credentials.

Prerequisites

To use this feature, you must have previously opened a remote desktop or published application. If you plan to open a recent desktop or published application from the Dock, VMware Horizon Client must be in the Dock. See Add Horizon Client to the Dock.

Procedure

- To open a remote desktop or published application from the Dock, Ctrl-click **VMware Horizon Client** in the Dock and select the remote desktop or published application from the menu.
- To open a remote desktop or published application from the **File** menu, start Horizon Client, select **File > Open Recent**, and select the remote desktop or published application from the menu.

Open Local Files in Published Applications

You can turn on the ability to open local files in published applications directly from the local file system.

If you select a local file and press Control-click, the **Open With** menu lists the available published applications. You can also open a local file by dragging it into the published application window or Dock icon.

If you set a published application as the default application for files that have a certain file extension, all files on your local file system that have that file extension are registered with the server. You can also turn on the ability to run published applications from the Applications folder.

Note If a file name contains characters that are invalid in the Windows file system, you cannot open the file in a published application. For example, you cannot open a file named `test2<.txt` in Notepad.

Prerequisites

For administrators - to open local files in published applications, a Horizon administrator must install the client drive redirection feature in Horizon Agent. The client drive redirection feature is installed by default. For more information, see the *Horizon Remote Desktop Features and GPOs* document.

For end users - to open local files in published applications, a Horizon administrator must install the client drive redirection feature.

Procedure

1. Connect to a server.
2. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selector window and select **Applications** in the left pane.
3. To turn on the ability to open local files with published applications from the local file system, select **Open local files in hosted applications**.
4. To turn on the ability to run published applications from the `Applications` folder on the client system, select **Run hosted applications from your local Applications folder**.

Select a Favorite Remote Desktop or Published Application

You can select favorite remote desktops and published applications. Shortcuts for favorite items are identified by a star and appear on the **Favorites** tab. Favorite items are saved after you log off from the server.

Prerequisites

Obtain the credentials for connecting to the server, such as a user name and password or RSA SecurID and passcode.

Procedure

1. On the Horizon Client Home window, double-click the server icon.
2. If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.
3. To select or deselect a favorite remote desktop or published application, perform these steps.

Option	Action
Select a favorite	Select the remote desktop or published application shortcut, press Control-click, and select **Mark as Favorite** from the context menu. A star appears in the upper-right corner of the remote desktop or published application shortcut.
Deselect a favorite	Select the remote desktop or published application shortcut, press Control-click, and deselect **Mark as Favorite** from the context menu. A star no longer appears in the upper-right corner of the remote desktop or published application shortcut.

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

   You can click the **Favorites** button again to display all the available remote desktops and published applications.

Configure Reconnect Behavior for Published Applications

If you disconnect from a server without closing a published application, Horizon Client prompts you to reopen that published application the next time you connect to the server. You can change this behavior by modifying the Reconnect Behavior setting in Horizon Client.

Prerequisites

Obtain credentials for connecting to the server, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

Procedure

1 On the Horizon Client **Home** window, double-click the server icon.

2 If prompted, supply your credentials.

3 Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window.

4 Select **Applications** in the left pane of the Settings dialog box.

5 Select an application reconnect behavior option.

These options determine how Horizon Client behaves when a user connects to the server and published applications are still running.

Option	Description
Ask to reconnect to open applications	Horizon Client shows the message **You have one or more remote applications running. Would you like to open them now?** You can respond by clicking **Reconnect to Applications** or **Not Now**. You can also select the **Don't show this message again** check box to suppress the message in the future. This setting is enabled by default.
Reconnect automatically to open applications	Horizon Client reopens any running published applications immediately.
Do not ask to reconnect and do not automatically reconnect	Horizon Client does not prompt you to reopen running published applications, nor does it reopen running published applications. This setting has the same effect as the **Don't show this message again** check box.

Results

The new setting takes effect the next time you connect to the server.

Switch Remote Desktops or Published Applications

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

Procedure

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

Option	Action
Choose a different remote desktop or published application on the same server	Perform one of the following actions: ■ To keep the current remote desktop and also connect to another remote desktop, select **Window > VMware Horizon Client** from the menu bar and double-click the shortcut for the other remote desktop. That remote desktop opens in a new window so that you have multiple remote desktops open. You can switch between remote desktops from the **Window** menu on the menu bar. ■ To close the current remote desktop and connect to another remote desktop, select **Connection > Disconnect** from the menu bar and double-click the shortcut for the other remote desktop. ■ To open another published application, double-click the shortcut for the other published application. That published application opens in a new window. You now have multiple published applications open, and you can switch between them by clicking in an application window.
Choose a different remote desktop or published application on a different server	If you are entitled to multiple remote desktops or published applications, so that the desktop and application selection window is open, click the **Disconnect from Server** button in the left side of the toolbar in the desktop and application selection window and disconnect from the server. If you are entitled to only one remote desktop or published application, and the desktop and application selection window is not open, you can select **File > Disconnect from Server** from the menu bar and then connect to a different server.

Using Published Applications

You can use many Mac functions with published applications.

- When you run a published application, its icon appears in the Dock. You can maximize a minimized published application by clicking its icon in the Dock.
- You can keep, open, and quit a published application from its context menu in the Dock. If you select **Keep in Dock**, the published application icon remains in the Dock, even after you close all application windows.
- You can open a published application by clicking its icon in the Dock.
- You can open local files in published applications and run published applications from the Applications folder on the client system. To enable these features, see Share Local Folders and Drives.
- Flashing Windows taskbar items are forwarded to Horizon Client. For example, if the published application is an IM client and you receive a new message, a flashing red dot appears on the IM client icon in the Dock.
- You can start voice dictation, minimize, and zoom a published application from the menu bar.

- You can use the Exposé feature to see open published applications, and you can press Command-Tab to switch between open published applications.
- You can use standard Mac keyboard shortcuts to interact with published applications. For example, you can press Command-W to close an individual application window and Command-S to save the current file. You can also use standard Mac keyboard shortcuts to copy, cut, and paste text between applications on the Mac and published applications. You can customize keyboard shortcut mappings. See Create Keyboard Shortcut Mappings.
- If a published application creates a Windows System Tray item, that item appears in the notification area on the menu bar on the Mac client system. You can interact with this item from the notification area on the Mac in the same way that you interact with it from the System Tray on a Windows system.

  Note When you reclick a redirected System Tray item in the notification area on the Mac, the context menu does not disappear.

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.

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

For administrators - You 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 *Horizon Remote Desktop Features and GPOs* document.

Use Multiple Sessions of a Published Application From Different Client Devices

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log in 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.

- If the Mac client system goes to sleep while you are connected to a published application in multi-session mode, the published application session is not resumed.
- You cannot use the same published application in both single-session mode and multi-session mode. For example, if you are using a published application in single-session mode, you must quit the application before you can change it to multi-session mode.

Prerequisites

A Horizon administrator must enable multi-session mode for the application pool. End users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Windows Desktops and Applications in Horizon*.

Procedure

1. Connect to a server.
2. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selector window and select **Multi-Launch**.

   If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.
3. 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.

Run Published Applications from the Applications Folder

You can configure Horizon Client so that published applications appear in the `Applications` folder on the client system.

If a Horizon administrator has configured one or more category folders for a published application, you can optionally configure Horizon Client to show the published application in those folders in the `Applications` folder on the client system.

For information about configuring shortcuts and category folders for published applications, see the *Windows Desktops and Applications in Horizon* document.

Prerequisites

Connect to a server.

Procedure

1. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selector window and select **Applications** in the left pane.
2. To turn on the ability to run published applications from the `Applications` folder on the client system, select **Run hosted applications from your local Applications folder**.

3 (Optional) To show the category folders that are configured for published applications in the `Applications` folder, select **Allow automatic shortcuts from the server**.

Use a Local IME with Published Applications

If you use non-English keyboards and locales, you can use an IME (input method editor) that is installed in the local client system to send non-English characters to published applications.

You can use the **Input** menu in the menu bar on the Mac or keyboard shortcuts to switch to a different IME. You do not need to install an IME on the server that hosts the published application.

Note On a Mac, an IME is called an input source.

When this feature is enabled, the local IME is used. If an IME is installed and configured on the server that hosts the published application, that remote IME is ignored.

Prerequisites

- Verify that one or more IMEs are installed in the client system.

Procedure

1 Start Horizon Client and connect to a server.

2 In the desktop and application selection window, Control-click a published application and select **Settings**.

3 In the Remote Applications pane, select the **Extend the local IME to hosted applications** check box.

4 Use the local IME as you might use it with locally installed applications.

Results

The **Input** menu appears in the menu bar on the Mac client. When you use a published application, you can switch to a different language or IME by using the **Input** menu or keyboard shortcuts. Key combinations that perform certain actions, such as Command-C to copy and Command-V to paste, work correctly.

Using a Touch Bar with Server, Desktop, and Application Connections

If the Mac has a Touch Bar, you can use the Touch Bar to add a server, disconnect from a server, or connect to a recent remote desktop or published application.

Before you connect to a server, you can touch the plus (**+**) icon to add a server. After you connect to a server, you can touch the **Disconnect** icon to disconnect from the server.

If you previously connected to a remote desktop or published application, its name appears on the Touch Bar before you connect to a server. You can touch the remote desktop or application name to log in to the server and start the remote desktop or published application.

You can add, remove, and reorder the items in the Horizon Client app Touch Bar by selecting **VMware Horizon Client > Customize Touch Bar**.

For information about using the Touch Bar after you connect to a remote desktop or published application, see Using a Touch Bar with Remote Desktops and Published Applications.

Using a Touch Bar with Remote Desktops and Published Applications

You can use a Touch Bar to interact with remote desktops and published applications.

Interacting with Remote Desktops

After you connect to a remote desktop, you can use icons on the Touch Bar to perform the following tasks.

- Disconnect, log out, restart or reset, and send Ctrl+Alt+Delete to the remote desktop.
- Enter or exit full-screen mode.
- Bring the desktop and application selection window to the foreground.
- View a list of all the currently open remote desktops and published applications.
- Switch to another open remote desktop or published application.

You can add, remove, and reorder the items in the Horizon Client app Touch Bar by selecting **VMware Horizon Client > Customize Touch Bar**.

Note The log out, reset, and restart features are available only if a Horizon administrator has enabled them. If the remote desktop is in exclusive mode, you cannot use the Touch Bar to enter or exit full-screen mode or bring the desktop and application selection window to the foreground.

Interacting with Published Applications

After you connect to a published application, the following icons appear on the Touch Bar.

From left to right, you can use these icons to perform the following tasks:

- Display a list of function keys.
- View the list of open windows for the current published application. You can click a window title to switch to that window.
- Zoom (toggles between maximize and restore).
- Hide all windows of the current published application.
- Minimize the current published application window.
- Bring the application selection window to the foreground.

- View a list of all currently open remote desktops and published applications. You can click the remote desktop or published application to bring it to the foreground.

You can add, remove, and reorder the items in the Published Application Touch Bar by selecting **Window > Customize Touch Bar** from the menu bar.

Configure Horizon Client to Forget the Server User Name and Domain

By default, Horizon Client stores the user name and domain that you enter when you log in to a server. For increased security, you can configure Horizon Client so that it never remembers the server user name and domain.

Procedure

1. Select **VMware Horizon Client > Preferences** from the menu bar.
2. Click **General** in the Preferences dialog box.
3. Deselect **Remember username and domain**.
4. Close the Preferences dialog box.

   Your changes take effect when the dialog box is closed.

Share Local Folders and Drives

With the client drive redirection feature, you can share folders and drives on the local client system with remote desktops and published applications.

Shared drives can include mapped drives and USB storage devices.

When using the client drive redirection feature to share a USB drive with a remote desktop, you cannot unplug the device and plug it back in during the remote desktop session.

The client drive redirection feature does not support sharing Microsoft OneDrive, Google Drive, and enterprise file storage.

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.

The client drive redirection settings apply to all remote desktops and published applications.

Prerequisites

For end users - To share folders and drives with a remote desktop or published application, a Horizon administrator must enable the client drive redirection feature.

For administrators - To enable and configure the client drive redirection feature, verify that you have completed the following tasks:

- Verify that the client drive redirection feature is installed in Horizon Agent. The client drive redirection feature is installed by default.
- You can include or exclude folders on devices that have specified vendor and product IDs from being redirected by using the **Include Vid/Pid Device** and **Exclude Vid/Pid Device** group policy settings. For more information, see the *Horizon Remote Desktop Features and GPOs* document.

Procedure

1 Open the Preferences dialog box and display the Sharing panel.

Option	Description
From the desktop and application selection window	Select **VMware Horizon Client > Preferences** and click **Sharing**.
From the Sharing dialog box that appears when you connect to a remote desktop or published application	Click the **Preferences > Sharing** link in the dialog box.
From within a remote desktop operating system	Select **VMware Horizon Client > Preferences** 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 published applications	Click the plus (+) button, browse to and select the folder or drive to share, and click **Add**. **Note** If a USB device is already connected to a remote desktop or published application with the USB redirection feature, you cannot share a folder on the USB device.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the minus (-) button.
Give remote desktops and published applications access to files in your home directory	Select the **Allow access to *home-directory*** check box.

Option	Action
Share USB storage devices with remote desktops and published applications	Toggle the **Allow auto access to removable storage** option to on. The client drive redirection feature shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives automatically. Selecting a specific device to share is not necessary. **Note** USB storage devices already connected to a remote desktop or published application with the USB redirection feature are not shared. If this option is toggled off, you can use the USB redirection feature to connect USB storage devices to remote desktops and published applications.
Do not show the Sharing dialog box when you connect to a remote desktop or published 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 remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Sharing dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box. To see the dialog box again, you must disconnect from the server and log in again.

What to do next

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

- In 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.
- In a published application, 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.

Naming Convention	Example
folder-name on *desktop-name*	jsmith on JSMITH-W03
folder-name (*drive-number*:)	jsmith (Z:)
folder-name on *desktoptop-name* (*drive-number*:)	jsmith on JSMITH-W03 (Z:)

For remote desktops running certain Horizon Agent versions, a redirected folder can have two entrances, such as under **Devices and drives** and **Network locations** in Windows 10, 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.

Using the URL Content Redirection Feature

A Horizon administrator can configure URL links that you click inside a remote desktop or published application to open in the default browser on the local client system. The URL link

might be to a web page, a phone number, an email address, or another type of link. This feature is called URL Content Redirection.

A Horizon administrator can also configure URL links that you click inside a browser or application on the local client system to open in a remote desktop or published application. If Horizon Client is not already open you click the URL link, it starts and prompts you to log in.

A Horizon administrator might set up the URL Content Redirection feature for security purposes. For example, if you are at work and click a link that points to a URL outside your company network, the link might be more safely opened in a published application. An administrator can configure which published application opens the link.

Each company configures its own URL Content Redirection policies. If you are an end user and have questions about how the URL Content Redirection feature behaves at your company, contact your system administrator.

Responding to URL Content Redirection Prompts

The first time you start Horizon Client and connect to a server on which the URL Content Redirection feature is configured, Horizon Client prompts you to open the VMware Horizon URL Filter application when you click a link for redirection. Click **Open** to allow the URL to be redirected.

Depending on how the URL Content Redirection feature is configured, Horizon Client might display an alert message that asks you to change your default web browser to VMware Horizon URL Filter. If you see this prompt, click the **Use "VMware Horizon URL Filter"** button to allow VMware Horizon URL Filter to become the default browser. This prompt appears only once, unless you change your default browser after clicking **Use "VMware Horizon URL Filter"**.

Horizon Client might also display an alert message that asks you to select an application when you click a URL. If you see this prompt, you can click **Choose Application** to search for an application on the local client system, or click **Search App Store** to search for and install a new application. If you click **Cancel**, the URL is not opened.

Using URL Content Redirection with Chrome

If the Chrome browser prompts you to enable the VMware Horizon URL Content Redirection Helper extension, click **Enable Extension** to use the URL Content Redirection feature with the Chrome browser. If you click **Remove from Chrome**, the extension is removed and URLs clicked in Chrome are not redirected. You can still install the extension manually from the Chrome Web Store.

The first time a URL is redirected from the Chrome browser on the client system, you are prompted to open the URL in Horizon Client. If you select the **Remember my choice for VMware Horizon Client links** check box (recommended) and then click **Open VMware Horizon Client**, this prompt does not appear again.

Using URL Content Redirection with Microsoft Edge (Chromium)

To use the Microsoft Edge (Chromium) browser for URL Content Redirection, you must install the helper extension for the browser on the client. See "Install the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on Linux" in the *Horizon Remote Desktop Features and GPOs* document.

Hide the Horizon Client Window

You can hide the VMware Horizon Client window after you open a remote desktop or published application.

Procedure

1. To hide the VMware Horizon Client window after you open a remote desktop or published application, click the **Close** button in the corner of the VMware Horizon Client window.

   The VMware Horizon Client icon remains in the Dock.
2. To configure a setting that always hides the Horizon Client window after you open a remote desktop or published application, perform these steps before you connect to a server.
   a. Select **VMware Horizon Client > Preferences** from the menu bar and click **General** in the Preferences dialog box.
   b. Select **Hide client window after desktop/application launched**.
   c. Close the Preferences dialog box.

      Your changes take effect when the dialog box is closed.
3. To show the Horizon Client window after it has been hidden, select **Window > Open Selection Window** from the menu bar, or right-click the VMware Horizon Client icon in the Dock and select **Show All Windows**.

Dragging Shortcuts and URIs

You can drag server, remote desktop, and published application shortcuts and Uniform Resource Identifiers (URIs).

You can drag a server shortcut from the Horizon Client Home window into another app, such as Notes. The server shortcut appears as a URI in the other app, for example, `vmware-view://server-address`. You can also drag a server address or URI from another app into the Home window.

After you connect to a server, you can drag a remote desktop or published application shortcut from the Horizon Client desktop and application selection window into another app, such as Notes. The shortcut appears as a URI in the other app, for example, `vmware-view://server-name/item-name`.

If you drag a server, remote desktop, or published application shortcut from Horizon Client into a folder on the Mac, Horizon Client creates a shortcut file in the folder. You can double-click this shortcut file to start Horizon Client and connect to the server, remote desktop, or published application.

For information about URI syntax, see Using URIs to Configure Horizon Client.

Dragging and Dropping

The drag and drop feature works differently depending on the Horizon Agent version and how it is configured.

With Horizon Agent 7.9 and later, you can drag and drop files, folders, text, rich text, and images between the client system and remote desktops and published applications. With earlier Horizon Agent versions, you can drag and drop text, rich text, and images from the client system to a remote desktop through clipboard redirection, and you can drag and drop files from the client system to a published application through file association.

Depending on the Horizon Agent version, a Horizon administrator can use certain group policy settings or Smart Policies to configure drag and drop behavior. For complete information about configuring the drag and drop feature, see the *Horizon Remote Desktop Features and GPOs* document for your VMware Horizon version.

Dragging Text and Images

You can drag text and images from the client system to an open application in a remote desktop or a published application. For example, you can drag text from a browser on the client system and drop it into the WordPad application in a remote desktop. Depending on how the drag and drop feature is configured, you might also be able to drag text and images from an open application in a remote desktop or a published application to the client system.

The following data formats are supported.

- Plain Text (NSPasteboardTypeString)
- Rich Text (NSPasteboardTypeRTF)
- Image (kUTTypeImage)

For administrators - a Horizon administrator can configure drag and drop behavior by configuring group policy settings. The settings to configure depend on the Horizon Agent version. For complete information, see the *Horizon Remote Desktop Features and GPOs* document for your Horizon version.

For end users - a Horizon administrator can configure drag and drop behavior. A Horizon administrator can also disable this feature.

Dragging Files and Folders

For administrators - with Horizon Agent 7.9 and later, you can drag and drop files and folders between the Mac client system and remote desktops and published applications. You can drag

and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation. **For end users** - depending on how a Horizon administrator has configured the drag and drop feature, you might be able to drag and drop files and folders between the Mac client system and remote desktops and published applications. You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.. With Horizon Agent 7.9 and later, you can drag and drop files and folders between the Mac client system and remote desktops and published applications. You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.

If you drag a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.

By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled. A Horizon administrator can control the drag and drop direction by configuring group policy settings.

Dragging and dropping files, folders, and file contents requires that the client drive redirection feature is installed in Horizon Agent. The client drive redirection feature is installed by default. For complete information about configuring the drag and drop feature, including feature requirements, see the *Horizon Remote Desktop Features and GPOs* document for your VMware Horizon version.

Tips for Using the Drag and Drop Feature

When using the drag and drop feature, follow these tips.

For administrators - Depending on the Horizon Agent version, some tips might not apply to your environment.

For end users - Depending on how a Horizon administrator configures the drag and drop feature, some tips might not apply to your environment.

- You must use the VMware Blast or PCoIP display protocol.
- When a drag and drop operation is in progress, you cannot start a new drag and drop operation until after the first drag and drop operation has finished.
- You cannot drag and drop between remote desktops.
- **For administrators** - You cannot drag and drop between published applications from different farms.
- **For administrators** - You cannot drag and drop between published applications.

- If you drag and drop a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.
- You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.
- By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled.
- When you drag a file from the client system and drop it into a published application, you cannot click **Save as** to copy the file back to a different file on the client system. You can click **Save** to copy the file back to the same file on the client system.
- If you drag a file from the client system to an application in a remote desktop, the file is copied to the remote desktop and you can only edit the copy of the file.
- If you are dragging formatted text, some of the data is text and some of the data is formatting information. If you drag a large amount of formatted text, or text and an image, when you attempt to drop the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.
- If you are dragging both plain text and RTF data, and the total data size is less than the drag and drop size threshold, the formatted text is copied. Because RTF data cannot be truncated, if the total data size is greater than the drag and drop size threshold, the RTF data is discarded and only the plain text (or part of the plain text) is copied.
- If you are unable to drag all the formatted text and images in one operation, you might need to drag smaller amounts in each operation.
- A built-in timeout mechanism exists for fault tolerance.
- When you drag and drop a file or folder between different operating systems, the file or folder name must be accepted by both operating systems.

Copying and Pasting Text and Images

By default, you can copy and paste from the 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 text and images, including Rich Text Format (RTF).

For example, to copy text on the client system, select the text and press Command-C. To paste the text into a remote desktop, press Command-V in the remote desktop.

For administrators - 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 *Horizon Remote Desktop Features and GPOs* document.

This feature has the following limitations.

- You cannot copy and paste files between a remote desktop and the file system on the local client computer.
- If you are copying formatted text, some of the data is text and some of the data is formatting information. If you copy a large amount of formatted text or text and an image, when you attempt to paste the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.
- If the text and RTF data together use less than the maximum clipboard size, the formatted text is pasted. Often, the RTF data cannot be truncated, so that if the text and formatting use more than the maximum clipboard size amount, the RTF data is discarded, and the plain text is pasted.
- If you are unable to paste all the formatted text and images that you selected in one operation, you might need to copy and paste smaller amounts in each operation.

Configuring the Client Clipboard Memory Size

You can configure the client clipboard memory size by creating a file named `config` in the `%HomeDir%/Library/Preferences/VMware Horizon View/` directory on the Mac client.

To set the client clipboard memory size, add the following parameter to the `config` file.

```
mksvchan.clipboardSize=value
```

value is the client clipboard memory size in kilobytes. If you specify 0, or do not specify a value, the default client clipboard memory size is 16384 kilobytes (16 MB).

A large clipboard memory size can negatively affect performance, depending on your network. Do not set the clipboard memory size to a value greater than 16 MB.

Logging Copy and Paste Activity

When a Horizon administrator enables the clipboard audit feature, Horizon Agent records information about copy and paste activity in an event log in the agent machine. The clipboard audit feature is deactivated by default.

To enable the clipboard audit feature, you must configure the **Configure clipboard audit** group policy setting.

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

For more information about the group policy settings for clipboard redirection, see the *Horizon Remote Desktop Features and GPOs* document.

The event log where information about copy and paste activity is recorded is named VMware Horizon RX Audit. To view the event log in 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.

PCoIP Client-Side Image Cache

PCoIP client-side image caching stores image content on the client to avoid retransmitting data. This feature reduces bandwidth use.

The PCoIP image cache captures spatial and temporal redundancy. For example, when you scroll through a PDF document, new content appears from the bottom of the window and the oldest content disappears from the top of the window. The remaining content is constant and moves upward. The PCoIP image cache can detect this spatial and temporal redundancy.

During scrolling, because the display information sent to the client is primarily a sequence of cache indexes, using the image cache saves a significant amount of bandwidth. This efficient scrolling has benefits both on the LAN and over the WAN.

- On the LAN, where the bandwidth is relatively unconstrained, using client-side image caching delivers significant bandwidth savings.
- Over the WAN, to stay within the available bandwidth constraints, scrolling performance is degraded without client-side caching. Over the WAN, client-side caching saves bandwidth and ensures a smooth, highly responsive scrolling experience.

With client-side caching, the client stores portions of the display that were previously transmitted. The cache size is 250 MB.

Improve Mouse Performance in a Remote Desktop

If you use the VMware Blast display protocol or the PCoIP display protocol when using 3D applications in a remote desktop, mouse performance improves when you enable the relative mouse feature.

In most circumstances, if you are using applications that do not require 3D rendering, Horizon Client transmits information about mouse pointer movements by using absolute coordinates. Using absolute coordinates, the client renders the mouse movements locally, which improves performance, especially if you are outside the corporate network.

For work that requires using graphics-intensive applications, such as AutoCAD, or for playing 3D video games, you can improve mouse performance by enabling the relative mouse feature, which uses relative, rather than absolute, coordinates.

When the relative mouse feature is enabled, performance might be slow if you are outside the corporate network, on a WAN.

Prerequisites

A Horizon administrator must turn on 3D rendering for the desktop pool. For information about pool settings and the options available for 3D rendering, see the *Windows Desktops and Applications in Horizon* document.

Procedure

1. Start Horizon Client and log in to the server.
2. Right-click the remote desktop and select **VMware Blast** or **PCoIP**.
3. Connect to the remote desktop.
4. Select **Connection > Enable Relative Mouse** from the menu bar.

   The option is a toggle. To deactivate the relative mouse feature, select **Connection > Enable Relative Mouse** again.

   Note If you use Horizon Client in windowed mode rather than full-screen mode and the relative mouse feature is enabled, you might not be able to move the mouse pointer to the Horizon Client menu options or move the pointer outside of the Horizon Client window. To resolve this situation, press Control+Option.

Using Server, Remote Desktop, and Published Application Shortcuts

You can reorder and drag and drop server, remote desktop, and published application shortcuts. You can also select favorite remote desktop and published application shortcuts and remove server shortcuts from the Horizon Client Home window.

Reordering Shortcuts

You can reorder server, remote desktop, and published application shortcuts.

Each time you connect to a server, Horizon Client saves a server shortcut to the Home window. You can reorder these server shortcuts by selecting a shortcut and dragging it to a new position on the Home window.

After you connect to a server, the available remote desktops and published applications on that server appear in the desktop and application selection window. Remote desktop shortcuts appear first, followed by published application shortcuts. Remote desktop shortcuts and published application shortcuts are arranged alphabetically and cannot be rearranged.

When you are in the Favorites view (you clicked the **Favorites** button in the upper-right corner of the desktop and application selection window), you can reorder remote desktop and published application shortcuts by selecting a shortcut and dragging it to a new position on the window.

Dragging Shortcuts and URIs

You can drag server, remote desktop, and published application shortcuts and Uniform Resource Identifiers (URIs).

You can drag a server shortcut from the Horizon Client Home window into another app, such as Notes. The server shortcut appears as a URI in the other app, for example, `vmware-view://server-address`. You can also drag a server address or URI from another app into the Home window.

After you connect to a server, you can drag a remote desktop or published application shortcut from the Horizon Client desktop and application selection window into another app, such as Notes. The shortcut appears as a URI in the other app, for example, `vmware-view://server-name/item-name`.

If you drag a server, remote desktop, or published application shortcut from Horizon Client into a folder on the Mac, Horizon Client creates a shortcut file in the folder. You can double-click this shortcut file to start Horizon Client and connect to the server, remote desktop, or published application.

For information about URI syntax, see Using URIs to Configure Horizon Client.

Select a Favorite Remote Desktop or Published Application

You can select favorite remote desktops and published applications. Shortcuts for favorite items are identified by a star and appear on the **Favorites** tab. Favorite items are saved after you log off from the server.

Prerequisites

Obtain the credentials for connecting to the server, such as a user name and password or RSA SecurID and passcode.

Procedure

1. On the Horizon Client Home window, double-click the server icon.
2. If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 To select or deselect a favorite remote desktop or published application, perform these steps.

Option	Action
Select a favorite	Select the remote desktop or published application shortcut, press Control-click, and select **Mark as Favorite** from the context menu. A star appears in the upper-right corner of the remote desktop or published application shortcut.
Deselect a favorite	Select the remote desktop or published application shortcut, press Control-click, and deselect **Mark as Favorite** from the context menu. A star no longer appears in the upper-right corner of the remote desktop or published application shortcut.

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

You can click the **Favorites** button again to display all the available remote desktops and published applications.

Removing a Server Shortcut from the Home Window

After you connect to a server, Horizon Client saves a server shortcut to the Home window.

You can remove a server shortcut by selecting the shortcut and pressing the **Delete** key. Alternatively, you can Control-click or right-click the shortcut on the Horizon Client Home window and select **Delete.**

You cannot remove remote desktop or published application shortcuts that appear after you connect to a server.

Using External Devices 7

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

This chapter includes the following topics:

Printing From a Remote Desktop or Published Application

With the VMware Integrated Printing feature, you can print to a network printer or a locally attached printer from a remote desktop or published application.

For administrators - refer to the following documents for more information.

- For information about installing the VMware Integrated Printing feature, see the *Windows Desktops and Applications in Horizon* document.
- For information about configuring the VMware Integrated Printing feature, see the *Horizon Remote Desktop Features and GPOs* document.
- For information about the types of remote desktops that support the VMware Integrated Printing feature, see Feature Support for Mac Clients.

Set Printing Preferences for the VMware Integrated Printing Feature

You can set printing preferences in a remote desktop for the VMware Integrated Printing feature. With the VMware Integrated Printing feature, you can use local or network printers from a remote desktop without having to install additional printer drivers in the Windows remote desktop. You can also select the preferred printer on the Horizon Client for Windows to use in remote sessions. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and other settings.

In a single-user virtual machine desktop, each virtual printer appears as *<printer_name>*(*vdi*) by default. In a published desktop or published application, each virtual printer appears as *<printer_name>*(v*<session_ID>*) by default.

A Horizon administrator can use a group policy to modify the printer naming convention for client printers that are redirected. For information, see the *Horizon Remote Desktop Features and GPOs* document for your Horizon Agent version.

Prerequisites

To use VMware Integrated Printing, a Horizon administrator must install the VMware Integrated Printing feature in the remote desktop. This task involves enabling the **VMware Integrated Printing** option in the Horizon Agent installer. For information about installing Horizon Agent, see the *Windows Desktops and Applications in Horizon* document. For information about configuring the VMware Integrated Printing feature, see the *Horizon Remote Desktop Features and GPOs* document.

To determine whether the VMware Integrated Printing feature is installed in a remote desktop, verify that the `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` and `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` files exist in the remote desktop file system.

Procedure

1. In the Windows remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**.
2. In the **Devices and Printers** window, right-click the virtual printer and select **Printer properties** from the context menu.
3. On the **General** tab, click **Preferences**.
4. In the Printing Preferences dialog box, select the different tabs and specify which settings to use.
5. To save your changes, click **OK**.

Printing From a Remote Desktop to a Local USB Printer

A USB printer is a printer that is attached to a USB port on the local client system. You can send print jobs to a USB printer attached to the local client system from a remote desktop.

You can use either the USB redirection feature or the VMware Integrated Printing feature to print to a USB printer from a remote desktop. Redirected USB printers and virtual printers can work together without conflict.

Using the USB Redirection Feature

To use the USB redirection feature to attach a USB printer to a virtual USB port in a remote desktop, the required printer drivers must be installed in the remote desktop and on the client system.

When you use the USB redirection feature to redirect a USB printer, the USB printer is no longer logically attached to the physical USB port on the local client system and it does not appear in the list of local printers on the local client system. You can print to the USB printer from the remote desktop, but you can no longer print to the USB printer from the local client system.

In a remote desktop, redirected USB printers appear as *<printer_name>*.

For more information, see Use USB Devices.

Using the VMware Integrated Printing Feature

When you use the VMware Integrated Printing feature to send print jobs to a USB printer, you can print to the USB printer from both the remote desktop and the local client system and you do not need to install printer drivers in the remote desktop.

To use the VMware Integrated Printing feature, the feature must be enabled when a Horizon administrator installs Horizon Agent. For installation information, see the *Windows Desktops and Applications in Horizon* document.

For more information, see Set Printing Preferences for the VMware Integrated Printing Feature.

Use USB Devices

As a user, you can connect the VMware Horizon Client on your local device to attached USB devices, such as headphones, for use in a remote desktop or published application.

When you use the USB redirection feature, most USB devices attached to the local device become available from menus in Horizon Client. You use these menus to connect and disconnect the USB devices. The menus also offer settings to connect automatically.

For administrators - For information about USB device requirements and limitations, see the *Horizon Remote Desktop Features and GPOs* document.

For end users - The types of USB devices that you can redirect depend on settings made by Horizon system administrator.

Note The client can detect but cannot use USB storage devices that are in use by the local device. These devices appear on the menu as shared and unavailable.

You can connect USB devices to a remote desktop or published application manually or automatically. You can configure auto-connect settings for all devices, or for specific devices.

The following table describes the auto-connect settings that apply to all devices. You can set these before connecting to a server or desktop application.

Setting	Description
Auto-connect all devices at startup	Connects all USB devices automatically when the remote desktop or published application starts.
Auto-connect all devices when inserted	Connects all USB devices automatically when you insert the device in the local operating system.

The following table describes the auto-connect settings that apply to specific devices.

Setting	Description
Auto-connect device at startup or **On startup**	Connects the USB device automatically when the remote desktop or published application starts.
Auto-connect device when inserted or **On insert**	Connects the USB device automatically when you insert the device in the local opertaing system.

Prerequisites

- System settings: A Horizon system administrator must have activated the USB redirection feature on the server hosting the remote desktop or published applications.

  For administrators - This administrator task may include installing the USB Redirection component of Horizon Agent, and setting policies regarding USB redirection.

- Local privileges: To start the services, you need administrator privileges on the local device.

  The first time you start Horizon Client, a prompt offers you the option to start the services. You can also start the services from the menu bar. Click **Connection > USB > Start remote USB services** and provide the Administrator password.

  The first time you connect a USB device, you must provide the administrator password for the local device. Horizon Client prompts you for the password.

- Review the USB Redirection Limitations.

Procedure

1. Connect the USB device to the local operating system. If the USB requires drivers, the first time you connect the device to a remote desktop, prompts appear.
2. Start Horizon Client and on the menu bar, click **Connection > USB**.
   a. If the USB services are not running, click **Start remote USB services**.
   b. Have the administrator password for the local device ready, and then click **Continue**.
   c. Enter the password and click **OK**.
   d. To configure the default USB connection behavior for the client, click the auto-connection settings you want to activate for all devices. This option applies to the USB connections in general. You can apply different behavior for each device after connecting to a remote desktop or published application.
3. Connect to a server and start a remote desktop or published application.

   A new screen opens specific to your selection. Certain remote desktops or published application require sign-in depending on the settings made by the system administrator.
4. To connect a USB device, return to the main window of Horizon Client and then click **Connection**, **USB**.
5. Click the USB device on the list, and click **Continue**.

Results

While in the remote desktop or published application, you can use the USB device as you typically do on the local device. For exceptions, see USB Redirection Limitations

After connecting, USB device can take up to 20 seconds to appear in a remote desktop or published application. If a USB device is not in the list for the remote desktop or published application after several minutes, physically disconnect the USB device from the local device and then reconnect to the local device.

What to do next

For administrators - If you encounter problems with USB redirection, see the topic about troubleshooting USB redirection problems in the *Horizon Remote Desktop Features and GPOs* document.

USB Redirection Limitations

The USB redirection feature has certain limitations.

- When you access a USB device from a menu in Horizon Client and use the device in a remote desktop or published application, you cannot access the USB device on the local device.
- USB devices that do not appear in the menu, but are available in a remote desktop or published application, include human interface devices such as keyboards and pointing devices. The remote desktop or published application, and the local device, use these devices at the same time. Interaction with these USB devices can sometimes be slow because of network latency.
- Large USB disk drives can take several minutes to appear in the remote desktop or published application.
- Some USB devices require specific drivers. If a required driver is not already installed, you might be prompted to install it when you connect the USB device to the remote desktop or published application.
- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, configure Horizon Client so that it connects USB devices to the remote desktop or published application automatically. Otherwise, if you try to manually redirect the USB device by using a menu item, the device is not redirected unless you unplug the device and then plug it in again.
- Webcams are not supported for USB redirection.
- 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 unless you connect as an administrator user.

Note Do not redirect USB Ethernet devices to a remote desktop. The remote desktop can connect to the network if the local system is connected. If you set the remote desktop to autoconnect USB devices, you can add an exception to exclude the Ethernet connection. See Configuring USB Redirection on a Mac Client .

Configuring USB Redirection on a Mac Client

You can configure which USB devices are redirected to a remote desktop.

You can configure USB policies for View Agent or Horizon Agent on the remote desktop, and for Horizon Client on the Mac client system, to achieve the following goals.

- Restrict the types of USB devices that Horizon Client makes available for redirection.
- Make View Agent or Horizon Agent prevent certain USB devices from being forwarded from a client computer.
- Specify whether Horizon Client splits composite USB devices into separate components for redirection.

  Composite USB devices consist of a combination of two or more devices, such as a video input device and a storage device.

Configuration settings on the client might be merged with or overridden by corresponding policies set for View Agent or Horizon Agent on the remote desktop. For information about how USB settings on the client work together with View Agent or Horizon Agent USB policies, see the topics about using policies to control USB redirection in the *Horizon Remote Desktop Features and GPOs* document.

Using Rules from a Previous Horizon Client Release

In previous Horizon Client releases, you had to use `sudo` to configure USB filtering and splitting rules. You can use the following procedure to move rules that use `sudo` to new rules that do not use sudo.

1 On the Mac client, open Terminal (`/Applications/Utilities/Terminal.app`) and run the following command:

```
sudo defaults export com.vmware.viewusb /tmp/usb.plist
```

2 Open a Terminal window (press command+N) and run the following command:

```
defaults import com.vmware.viewusb /tmp/usb.plist
```

3 In the first Terminal window, run the following command:

```
sudo rm -rf /tmp/usb.plist
```

4 Close both Terminal windows.

You can now use `defaults write com.vmware.viewusb property value` to update the rules.

Syntax for Configuring USB Redirection

You can configure filtering and splitting rules to include USB devices, or to exclude USB devices from being redirected. On a Mac client, you configure USB functionality by using Terminal (`/Applications/Utilities/Terminal.app`) and running a command as root.

- To list the rules:

  ```
  # defaults read domain
  ```

  For example:

  ```
  # defaults read com.vmware.viewusb
  ```

- To remove a rule:

  ```
  # defaults delete domain property
  ```

  For example:

  ```
  # defaults delete com.vmware.viewusb ExcludeVidPid
  ```

- To set or replace a filter rule:

  ```
  # defaults write domain property value
  ```

  For example:

  ```
  # defaults write com.vmware.viewusb ExcludeVidPid vid-1234_pid-5678
  ```

  Important Some configuration parameters require the VID (vendor ID) and PID (product ID) for a USB device. To find the VID and PID, you can search on the Internet for the product name combined with `vid` and `pid`. Alternatively, you can look in the USB Log file after you plug in the USB device to the Mac client when Horizon Client is running. For more information, see Turn on Logging for USB Redirection.

- To set or replace a splitting rule for a composite device:

  ```
  # defaults write domain property value
  ```

  For example:

  ```
  # defaults write com.vmware.viewusb AllowAutoDeviceSplitting true
  # defaults write com.vmware.viewusb SplitExcludeVidPid vid-03f0_Pid-2a12
  # defaults write com.vmware.viewusb SplitVidPid "'vid-0911_Pid-149a(exintf:03)'"
  # defaults write com.vmware.viewusb IncludeVidPid vid-0911_Pid-149a
  ```

Composite USB devices consist of a combination of two or more devices, such as a video input device and a storage device. The first line in this example turns on automatic splitting of composite devices. The second line excludes the specified composite USB device (`Vid-03f0_Pid-2a12`) from splitting.

The third line instructs Horizon Client to treat the components of a different composite device (`Vid-0911_Pid-149a`) as separate devices, but to exclude the component that has interface number 03 from being redirected. This component is kept local.

Because this composite device includes a component that is ordinarily excluded by default, such as a mouse or keyboard, the fourth line is necessary so that the other components of the composite device `Vid-0911_Pid-149a` can be redirected to the remote desktop.

The first three properties are splitting properties. The last property is a filtering property. Filtering properties are processed before splitting properties.

- To exclude devices that have specific vendor and product IDs from being forwarded automatically:

  ```
  # defaults write com.vmware.viewusb ExAutoRedirectVidPid vid-xxxx_pid-xxxx
  ```

  For example:

  ```
  # defaults write com.vmware.viewusb ExAutoRedirectVidPid vid-1234_pid-5678
  ```

- To exclude families of devices from being forwarded automatically:

  ```
  # defaults write com.vmware.viewusb ExAutoRedirectFamily "family-name;family-name"
  ```

  For example:

  ```
  # defaults write com.vmware.viewusb ExAutoRedirectFamily "storage;hid"
  ```

Example: Excluding a USB Ethernet Device

You might want to exclude a USB Ethernet device from redirection. For example, if the Mac client uses a USB Ethernet device to connect the network for the Mac client to a remote desktop, and you redirect that USB Ethernet device, the Mac client loses its connection to both the network and the remote desktop.

To hide a device from the USB connection menu permanently, or if you have set the remote desktop to autoconnect USB devices, you can add an exception to exclude the Ethernet connection as follows.

```
defaults write com.vmware.viewusb ExcludeVidPid vid-xxxx_pid-yyyy
```

In this example, *xxxx* is the vendor ID and *yyyy* is the product ID of the USB Ethernet adapter.

USB Redirection Properties

When creating filtering rules, you can use the USB redirection properties.

Table 7-1. Configuration Properties for USB Redirection

Policy Name and Property	Description
Allow Auto Device Splitting Property: `AllowAutoDeviceSplitting`	Allow the automatic splitting of composite USB devices. The default value is undefined, which equates to **`false`**.
Exclude Vid/Pid Device From Split Property: `SplitExcludeVidPid`	Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is as follows: `vid-`*`xxx1`*`_pid-`*`yyy1`*`[;vid-`*`xxx2`*`_pid-`*`yyy2`*`]...` You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-55**`** The default value is undefined.
Split Vid/Pid Device Property: `SplitVidPid`	Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is as follows: `vid-`*`xxxx`*`_pid-`*`yyyy`*`([exintf:`*`zz`*`[;exintf:`*`ww`*`]])[;...]` You can use the `exintf` keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Note** If the composite device includes components that are automatically excluded, such as mouse and keyboard components, then Horizon does not include the components that you have not explicitly excluded automatically. You must specify a filter policy such as `Include Vid/Pid Device` to include those components. The default value is undefined.
Allow Audio Input Devices Property: `AllowAudioIn`	Allows audio input devices to be redirected. The default value is undefined, which equates to **`true`**.
Allow Audio Output Devices Property: `AllowAudioOut`	Allows audio output devices to be redirected. The default value is undefined, which equates to **`false`**.
Allow HID Property: `AllowHID`	Allows input devices other than keyboards or mice to be redirected. The default value is undefined, which equates to **`true`**.
Allow HIDBootable Property: `AllowHIDBootable`	Allows input devices other than keyboards or mice that are available at startup time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to **`true`**.
Allow Device Descriptor Failsafe Property: `AllowDevDescFailsafe`	Allows devices to be redirected even if the Horizon Client fails to get the config/device descriptors. To allow a device even if it fails the config/desc, include it in the Include filters, such `IncludeVidPid` or `IncludePath`. The default value is undefined, which equates to **`false`**.

Table 7-1. Configuration Properties for USB Redirection (continued)

Policy Name and Property	Description
Allow Keyboard and Mouse Devices Property: `AllowKeyboardMouse`	Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be redirected. The default value is undefined, which equates to **`false`**.
Allow Smart Cards Property: `AllowSmartcard`	Allows smart-card devices to be redirected. The default value is undefined, which equates to **`false`**.
Allow Video Devices Property: `AllowVideo`	Allows video devices to be redirected. The default value is undefined, which equates to **`true`**.
Disable Remote Configuration Download Property: `DisableRemoteConfig`	Disables the use of View Agent or Horizon Agent settings when performing USB device filtering. The default value is undefined, which equates to **`false`**.
Exclude All Devices Property: `ExcludeAllDevices`	Excludes all USB devices from being redirected. If set to **`true`**, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to **`false`**, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of `Exclude All Devices` to **`true`** on View Agent or Horizon Agent, and this setting is passed to Horizon Client, the View Agent or Horizon Agent setting overrides the Horizon Client setting. The default value is undefined, which equates to **`false`**.
Exclude Device Family Property: `ExcludeFamily`	Excludes families of devices from being redirected. The format of the setting is *family_name_1*[**`;`***family_name_2*]... For example: **`bluetooth;smart-card`** The default value is undefined. **Note** If you have enabled automatic device splitting, Horizon examines the device family of each interface of a composite USB device to decide which interfaces to exclude. If you have disabled automatic device splitting, Horizon examines the device family of the whole composite USB device.
Exclude Vid/Pid Device Property: `ExcludeVidPid`	Excludes devices with specified vendor and product IDs from being redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0781_pid-****;vid-0561_pid-554c`** The default value is undefined.
Exclude Path Property: `ExcludePath`	Exclude devices at specified hub or port paths from being redirected. The format of the setting is `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** The default value is undefined.

Table 7-1. Configuration Properties for USB Redirection (continued)

Policy Name and Property	Description
Include Device Family Property: `IncludeFamily`	Includes families of devices that can be redirected. The format of the setting is *family_name_1*[`;` *family_name_2*]... For example: **`storage`** The default value is undefined.
Include Path Property: `IncludePath`	Include devices at a specified hub or port paths that can be redirected. The format of the setting is `bus-`*x1*[`/`*y1*]...`_port-`*z1*[`;bus-`*x2*[`/`*y2*]...`_port-`*z2*]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** The default value is undefined.
Include Vid/Pid Device Property: `IncludeVidPid`	Includes devices with specified vendor and product IDs that can be redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy1*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0561_pid-554c`** The default value is undefined.

USB Device Families

You can specify a USB device family when you create USB filtering rules for Horizon Client or Horizon Agent.

Note Some devices do not report a device family.

Table 7-2. USB Device Families

Device Family Name	Description
`audio`	Any audio-input or audio-output device.
`audio-in`	Audio-input devices such as microphones.
`audio-out`	Audio-output devices such as loudspeakers and headphones.
`bluetooth`	Bluetooth-connected devices.
`comm`	Communications devices such as modems and wired networking adapters.
`hid`	Human interface devices excluding keyboards and pointing devices.
`hid-bootable`	Human interface devices that are available at startup time, excluding keyboards and pointing devices.
`imaging`	Imaging devices such as scanners.
`keyboard`	Keyboard device.
`mouse`	Pointing device such as a mouse.

Table 7-2. USB Device Families (continued)

Device Family Name	Description
other	Family not specified.
pda	Personal digital assistants.
physical	Force feedback devices such as force feedback joysticks.
printer	Printing devices.
security	Security devices such as fingerprint readers.
smart-card	Smart-card devices.
storage	Mass storage devices such as flash drives and external hard disk drives.
unknown	Family not known.
vendor	Devices with vendor-specific functions.
video	Video-input devices.
wireless	Wireless networking adapters.
wusb	Wireless USB devices.

Turn on Logging for USB Redirection

You can use USB logs to troubleshoot and to determine the product ID and vendor ID of various devices that you plug in to the Mac client.

Procedure

1. On the Mac client, use a text editor to open the `config` file in the `~/Library/Preferences/VMware Horizon View/` directory.
2. To set the log level for USB redirection, add the `view-usbd.logLevel` parameter to the `config` file.

   For example:

   ```
   #[or info, debug, error]. Info level by default.
   view-usbd.logLevel=trace
   ```

Using Webcams and Microphones

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

For information about setting up the Real-Time Audio-Video feature on the agent machine, including configuring the frame rate and image resolution, see the *Horizon Remote Desktop Features and GPOs* document.

When You Can Use a Webcam with the Real-Time Audio-Video Feature

If a Horizon administrator has configured the Real-Time Audio-Video feature, you can use a webcam that is built in or connected to the client computer in a remote desktop or published application. 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 a remote desktop, you can select input and output devices from menus in the application.

For remote desktops and published applications, a redirected webcam is named VMware Virtual Webcam in the application.

For many applications, you do not need to select an input device.

When the client computer uses the webcam, the remote session can use it at the same time. Also, if the remote session uses the webcam, the client computer can use it at the same time.

Note If you use a USB webcam, do not connect it from the **Connection > USB** menu in Horizon Client. Doing so routes the device through USB redirection and the performance is not usable for video chat.

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

Select a Default Microphone on the Mac Client

If you have multiple microphones on the Mac client, the remote desktop uses only one microphone. You can use the System Preferences on the Mac client to specify the default microphone in the remote desktop.

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

For administrators - This procedure describes how to select a microphone from the user interface of the Mac client. You can also configure a preferred microphone by using the Mac defaults system. See Configure a Preferred Webcam or Microphone on a Mac Client.

For end users - This procedure describes how to select a microphone from the user interface of the Mac client. You can also configure a preferred microphone by using the Mac defaults system.

Important When you use a USB microphone, do not connect it from the **Connection > USB** menu in Horizon Client. Doing so routes the device through USB redirection and the device cannot use the Real-Time Audio-Video feature.

Prerequisites

- Verify that you have a USB microphone, or another type of microphone, installed and operational on the Mac client.
- Use the VMware Blast display protocol or the PCoIP display protocol for the remote desktop.

Procedure

1. On the Mac client, select **Apple menu > System Preferences** and click **Sound**.
2. Open the Input pane of Sound preferences.
3. Select the microphone that you prefer to use.

Results

The next time that you connect to a remote desktop and start a call, the remote desktop uses the default microphone that you selected on the Mac client.

Configure a Preferred Webcam or Microphone on a Mac Client

If you connect multiple webcams or microphones to the Mac client, you can use one specific webcam and one microphone in a remote desktop with the Real-Time Audio-Video feature. You specify the preferred webcam and microphone at the command line by using the Mac defaults system.

With the Real-Time Audio-Video feature, webcams, audio input devices, and audio output devices do not require USB redirection to work and the required network bandwidth is reduced. Analog audio input devices are also supported.

In most environments, you do not need to configure a preferred microphone or webcam. If you do not set a preferred microphone, remote desktops use the default audio device set in the System Preferences of the local operating system. See Select a Default Microphone on the Mac Client. If you do not configure a preferred webcam, the remote desktop uses the webcam by enumeration.

Prerequisites

- If you are configuring a preferred USB webcam, verify that the webcam is installed and operational on the client system.
- If you are configuring a preferred USB microphone or another type of microphone, verify that the microphone is installed and operational on the Mac client.
- Use the VMware Blast display protocol or the PCoIP display protocol for the remote desktop.

Procedure

1 On the Mac client, start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the Real-Time Audio-Video log file.

   a Attach the webcam or audio device.

   b In the **Applications** folder, double-click **VMware Horizon Client** to start Horizon Client.

   c Start a call and then stop the call.

2 Find log entries for the webcam or microphone in the Real-Time Audio-Video log file.

   a In a text editor, open the Real-Time Audio-Video log file.

   The Real-Time Audio-Video log file is named `~/Library/Logs/VMware/vmware-RTAV-pid.log`, where *pid* is the process ID of the current session.

   b Search the Real-Time Audio-Video log file for entries that identify the attached webcams or microphones.

   The following example shows how webcam entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum()
- 1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum()
- Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509   SystemId=0xfa20000005ac8509
```

   The following example shows how microphone entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void
AudioCaptureBase::LogDevEnum() - 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void
AudioCaptureBase::LogDevEnum() - Index=255   Name=Built-in Microphone   UserId=Built-in
Microphone#AppleHDAEngineInput:1B,0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void
AudioCaptureBase::LogDevEnum() - Index=255   Name=Built-in Input   UserId=Built-in
Input#AppleHDAEngineInput:1B,0,1,1:2   SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 Find the webcam or microphone that you prefer in the Real-Time Audio-Video log file and make a note of its user ID.

   The user ID appears after the string UserId= in the log file. For example, the user ID of the internal face time camera is FaceTime HD Camera (Built-in) and the user ID of the internal microphone is Built-in Microphone.

4 In Terminal (`/Applications/Utilities/Terminal.app`), use the `defaults write` command to set the preferred webcam or microphone.

Option	Action
Set the preferred webcam	Type **`defaults write com.vmware.rtav srcWCamId "webcam-userid"`**, where *webcam-userid* is the user ID of the preferred webcam, which you obtained from the Real-Time Audio-Video log file. For example: `defaults write com.vmware.rtav srcWCamId "HD Webcam C525"`
Set the preferred microphone	Type **`defaults write com.vmware.rtav srcAudioInId "audio-device-userid"`**, where *audio-device-userid* is the user ID of the preferred microphone, which you obtained from the Real-Time Audio-Video log file. For example: `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"`

5 (Optional) Use the `defaults read` command to verify your changes to the Real-Time Audio-Video feature.

For example: **`defaults read com.vmware.rtav`**

A list of Real-Time Audio-Video settings appears.

Results

The next time you connect to a remote desktop and start a new call, the remote desktop uses the preferred webcam or microphone, if it is available. If the preferred webcam or microphone is not available, the remote desktop uses another available webcam or microphone.

Allowing Access to Webcams and Microphones

When you first use a webcam or microphone in a remote session, you are prompted to grant access to the system's camera and microphone features.

If you do not grant access at that time, you can grant access later by going to System Preferences, selecting **Security & Privacy**, clicking the **Privacy** tab, and selecting **Camera** or **Microphone**.

Monitors and Screen Resolution

When you use the VMware Blast display protocol or the PCoIP display protocol, you can extend a remote desktop to multiple monitors. If you have a Mac with Retina Display, you can see the remote desktop in full 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
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1
13 or 14	7, 8, 8.x, 10 (3D rendering feature enabled)	1
13 or 14	7, 8, 8.x, 10	4

For administrators - For the best performance, the virtual machine should have at least 2 GB of RAM and 2 vCPUs. This feature might require good network conditions, such as a bandwidth of 1000 Mbps with low network latency and a low package loss rate.

Using Full-Screen Mode with Multiple Monitors

When a remote desktop window is open, to extend the remote desktop across multiple monitors, select **Window > Enter Full Screen** from the menu bar or from the expander arrows in the upper-right corner of the remote desktop window. To make the remote desktop fill only one monitor, select **Window > Use Single Display in Full Screen** from the menu bar.

The monitors do not have to be in the same mode. For example, if you are using a laptop that is connected to an external monitor, the external monitor can be in portrait mode or landscape mode.

You can select a full-screen option from the Settings dialog box after you connect to a server and before you open a remote desktop. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window, select the remote desktop, and select a full-screen option from the **Full Screen** drop-down menu.

You can use the selective multiple-monitor feature to display a remote desktop window on a subset of your monitors. For more information, see Select Specific Monitors to Display a Remote Desktop.

Using Remote Desktops with Split View

With Split View, which is supported in El Capitan (10.11) and later, you can fill your Mac screen with two applications without manually moving and resizing windows. You can use Split View with remote desktops in full-screen mode (**Full Screen** or **Use Single Display in Full Screen** option).

Using a High-Resolution Mac with Retina Display

If you use the VMware Blast display protocol or the PCoIP display protocol, Horizon Client supports high resolutions for client systems that support Retina Display.

To enable high-resolution mode for a remote desktop, connect to the remote desktop and select **Connection > Use Full Resolution for Retina Display** from the menu bar.

To enable high-resolution mode for published applications, click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selector window, click **Applications** in the left pane, click the **Display** tab, and select the **Use Full Resolution for Retina Display** check box.

In high-resolution mode, the DPI Synchronization feature ensures that the remote desktop's DPI setting matches the client system's DPI setting.

Allow Display Scaling

With the Display Scaling feature, remote desktops and published applications support the client system's scaling setting and appear normal-sized rather than very small.

Horizon Client saves the display scaling setting for each remote desktop separately. For published applications, the display scaling setting applies to all published applications that are available to the currently logged-in user.

Procedure

1. Start Horizon Client and connect to a server.
2. To allow display scaling for a remote desktop, connect to the remote desktop and select **Connection > Allow Display Scaling** from the menu bar.
3. To allow display scaling for published applications, click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window, select **Applications** in the left pane, click the **Display** tab, and select the **Allow Display Scaling** check box.

Using DPI Synchronization

The DPI Synchronization feature ensures that the DPI setting in a remote desktop or published application matches the client system's DPI setting.

The DPI Synchronization feature has the following requirements.

- The client system must support Retina Display.
- Full-resolution mode must be selected for the remote desktop or published applications. See Using a High-Resolution Mac with Retina Display.
- If you use multiple monitors, the Retina Display must be the primary window in system preferences. You cannot have more than one display in full-screen mode.

A Horizon administrator can disable the DPI synchronization feature.

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

Customize the Display Resolution and Display Scaling for a Remote Desktop

You can use Horizon Client to customize the display resolution and display scaling for a remote desktop. The display resolution determines the clarity of the text and images. At higher resolutions, such as 1600 x 1200 pixels, items appear sharper. Display scaling, which is represented as a percentage, increases or decreases the size of text, icons, and navigation elements.

Feature Limitations and Considerations

This feature has the following limitations and considerations.

- Custom display resolution and display scaling settings are stored only on the local client system. If you log in to the remote desktop from a different system, the settings are not applied.
- Customizing the display resolution for a remote desktop is not supported in multiple-monitor mode.
- If you select a custom resolution that is higher than the client resolution, Horizon Client resizes the remote desktop window to fit the client window. If you select a custom resolution that is lower than the client resolution, black bars appear in the remote desktop window.
- If you customize the display resolution during a remote desktop session, your changes take effect immediately. If you customize display scaling during a remote desktop session, you must log out and log back in to make your changes take effect.

Customize the Display Resolution and Display Scaling for a Remote Desktop

1 Start Horizon Client and connect to a server.

2 In the desktop and application selector window, right-click the remote desktop and select **Settings**.

3 Click the **Display** tab.

4 To customize the display resolution, select a resolution from the **Resolution** drop-down menu.

If you select **Automatic** (the default setting), Horizon Client fits the remote desktop to the client window size. If the remote desktop does not support the display resolution that you select, it uses the default setting.

5 To customize display scaling, select a scaling size from the **Scaling** drop-down menu.

If you select **Automatic** (the default setting), Horizon Client sets the display scaling percentage based on the display resolution that you select.

Select Specific Monitors to Display a Remote Desktop

If you have two or more monitors, you can select the monitors on which to display a remote desktop window. For example, if you have two monitors, you can specify that the remote desktop window appears on only one of those monitors.

You can select up to four adjacent monitors.

Prerequisites

You must have two or more monitors.

Procedure

1. Start Horizon Client and connect to a server.
2. In the desktop and application selector window, right-click the remote desktop and select **Settings**.
3. On the **General** tab, select **PCoIP** or **VMware Blast** from the **Connect Via** drop-down menu.
4. On the **Display** tab, select **Use Selected Displays** from the **Full Screen** drop-down menu.

   Thumbnails of the monitors that are currently connected to the client system appear under Display arrangement. The display topology matches the display settings on the client system.
5. To select or deselect a monitor on which to display the remote desktop window, click a thumbnail.

   When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.
6. Connect to the remote desktop.

   Your changes are applied immediately when you connect to the remote desktop. The remote desktop enters full-screen mode on the displays that you selected.

Select Specific Monitors to Display Published Applications

If you have two or more monitors, you can select the monitors on which to display published application windows. For example, if you have three monitors, you can specify that published application windows appear on only two of those monitors.

You can select up to four adjacent monitors. The monitors can be side by side, or stacked vertically. For example, you might configure two rows of two monitors each.

Prerequisites

You must have two or more monitors.

Procedure

1. Start Horizon Client and connect to a server.
2. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window.
3. Select **Applications** in the left pane of the Settings dialog box.

4 Click the **Display** tab.

Thumbnails of the monitors that are currently connected to the client system appear under Display Arrangement. The display topology matches the display settings on the client system.

5 To select or deselect a monitor on which to display published applications, click a thumbnail.

When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.

Using Exclusive Mode

Exclusive mode is similar to full-screen mode in that the remote desktop fills the screen. With exclusive mode, unlike full-screen mode, the VMware Horizon Client menu bar and Dock do not appear when you move your pointer to the edges of the screen.

To enter exclusive mode, open a remote desktop in windowed mode, press and hold down the Option key, and select **Window > Enter Exclusive Mode**.

When a remote desktop is in windowed mode, you can also press Command-Control-Option-F to enter exclusive mode. To exit exclusive mode, press Command-Control-Option-F again.

Note If you do not press and hold down the Option key, the **Enter Full Screen** menu item appears instead of the **Enter Exclusive Mode** menu item. If the remote desktop is in full-screen mode, you cannot select the **Enter Excusive Mode** menu item.

To use exclusive mode with two monitors, before you open the remote desktop, select **Use All Displays** from the Settings dialog box, and then open the desktop and enter exclusive mode. To use exclusive mode with a single monitor, before you open the remote desktop, select **Use Single Display** from the Settings dialog box, and then connect to the remote desktop and enter exclusive mode.

To open the Settings dialog box, click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selection window, select the remote desktop, and select an option from the **Full Screen** drop-down menu.

Troubleshooting Horizon Client

8

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

This chapter includes the following topics:

Restart a Remote Desktop

If the remote desktop operating system stops responding, you might need to restart a remote desktop. Restarting a remote desktop is similar to using the Windows operating system restart command. The remote 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 restart feature for the remote desktop and the remote desktop is powered on. You can restart only one remote desktop at a time.

For information about enabling the desktop restart feature, see the *Windows Desktops and Applications in Horizon* document.

Procedure

- In the desktop and application selection window, select the remote desktop shortcut, press Control-click, and select **Restart** from the context menu.

Results

The operating system in the remote desktop restarts and the client disconnects and logs out from the remote desktop.

What to do next

Wait an appropriate amount of time for the system to restart 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 Remote Desktops or Published Applications.

Reset Remote Desktops 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 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 and are not saved.

Resetting published applications quits all open applications.

Resetting published applications quits 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 reset feature for the remote desktop and the remote desktop is powered on. You can reset only one remote desktop at a time.

Procedure

- Use the **Reset** command.

Option	Action
Reset a remote desktop from the desktop and application selection window	Select the remote desktop name, press Control-click, and select **Reset** from the context menu.
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**.

Results

When you reset a remote desktop, the operating system in the remote desktop restarts and the client disconnects and logs out from the remote desktop. When you reset published applications, the published applications quit.

What to do next

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

Uninstalling Horizon Client

Sometimes you can resolve problems with Horizon Client by uninstalling and reinstalling Horizon Client.

To uninstall Horizon Client, use the same method that you use to uninstall any application.

Drag the **VMware Horizon Client** application from the **Applications** folder to the **Trash** and empty the trash.

After Horizon Client is uninstalled, you can reinstall it.

See Install Horizon Client on a Mac.

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

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.

Collecting Support Data

The log collection feature creates log files that contain support data that can help VMware troubleshoot problems with Horizon Client.

To collect support data, select **VMware Horizon Client > About VMware Horizon Client** and click **Collect Support Data**. Horizon Client saves log files in a ZIP file in the `Desktop` folder.