VMware Horizon Client for Chrome Installation and Setup Guide

MAR 2020
VMware Horizon Client for Chrome 5.4

vmware®

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

https://docs.vmware.com/

Contents

VMware Horizon Client for Chrome Installation and Setup Guide

This document, *VMware Horizon Client for Chrome Installation and Setup Guide*, provides information about installing, configuring, and using VMware Horizon® Client™ for Chrome on a Chromebook.

This information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

If you are an end user, see the *VMware Horizon Client for Chrome User Guide* document on VMware Docs, or view the Horizon Client for Chrome online help.

Setup and Installation

<div style="text-align: right; font-size: large;">1</div>

Setting up Horizon Client involves installing the Horizon Client for Chrome app on client devices, configuring Connection Server, and opening the required ports.

This chapter includes the following topics:

- System Requirements

- Smart Card Authentication Requirements

- Preparing Connection Server and Security Servers

- Install or Upgrade Horizon Client for Chrome

- Register the VMware Horizon Client for Chrome Extension

- Using the Google Admin Console to Configure Enrolled Chromebook Devices

- Configure HTML Access Agents to Use New TLS Certificates

- Configure HTML Access Agents to Use Specific Cipher Suites

- Using a CA-Signed Certificate with Unified Access Gateway

- Configure Horizon Client Data Sharing

System Requirements

The device on which you use Horizon Client for Chrome must meet certain software requirements.

Device models

Chromebook

Operating systems

Chrome OS 75 or later

CPU architecture

ARM or x86

Connection Server, security server, and View Agent or Horizon Agent

Horizon 6 version 6.2.6 or Horizon 7 version 7.4 and later releases.

To connect to a Horizon 7 version 7.4 server, you must register the Horizon Client for Chrome extension on the server. This change is not required for Horizon 6 version 6.2.6 or Horizon 7 version 7.5 and later servers. For more information see Register the VMware Horizon Client for Chrome Extension.

If client systems connect from outside the corporate firewall, use a security server or a Unified Access Gateway appliance so that client systems do not require a VPN connection.

For more information, see Preparing Connection Server and Security Servers.

Smart card authentication

See Smart Card Authentication Requirements.

Third-party firewalls

Firewalls must allow inbound traffic on certain TCP ports. See Firewall Rules for Client Web Browser Access.

Display protocol

VMware Blast (requires Horizon Agent 7.0 or later)

Smart Card Authentication Requirements

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

Client Hardware and Software Requirements

Users that authenticate with smart cards must have a physical 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 card)

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

- Horizon Client for Chrome
- A compatible smart card reader
- Google Smart Card Connector app

  The connector app provides basic support for smart cards on Chrome OS. You can download the Smart Card Connector app from the Chrome web store. VMware recommends using Google Smartcard Connector App version 1.2.16.1 or later.

- Charismathics CSSI Smart Card Middleware app

Middleware communicates with the smart card and other client certificates. You can download the CSSI Smart Card Middleware app from the Chrome web store.

You might need to install root and intermediate certificates on the Chromebook. For more information, see the Google Chrome OS documentation.

Agent Software Requirements

A Horizon administrator must install the Charismathics CSSI Smart Card Middleware app on the agent machine.

For the supported agent operating systems, see Feature Support Matrix.

Additional Smart Card Authentication Requirements

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

Connection server and security server hosts

Horizon 7 version 7.4 and later.

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

Unified Access Gateway appliances

Unified Access Gateway 3.2 and later.

For information about configuring a Unified Access Gateway appliance to support smart card use, see the *Deploying and Configuring 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 *VMware Horizon Console Administration* document.

Smart Card Authentication Limitations

With smart card authentication, you plug a smart card reader into the Chromebook, insert a smart card, and select a server in Horizon Client. During the authentication step, you enter a PIN instead of a user name and password. After you select a remote desktop or published application, all smart card commands and responses are redirected to the remote desktop or published application.

Smart card authentication has certain limitations when used with Horizon Client for Chrome.

- The Connection Server and Unified Access Gateway smart card user name hints feature is not supported.

- The Connection Server smart card removal policy is not supported.

- Single sign-on is not supported. When you connect to a remote desktop or published application, you must enter the smart card PIN again inside the remote session.

- After you use a smart card to authenticate to a server, you cannot switch to another authentication method, such as Active Directory authentication. To use a different authentication method the next time you connect to a server, you must log out of the Chrome OS or reboot the Chromebook.

- After you select a certificate and enter your PIN, the certificate you selected is cached on the Chromebook and is used the next time you connect to a server. To select a different certificate the next time you connect to a server, you must reboot the Chromebook.

Preparing Connection Server and Security Servers

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must install Connection Server and install security servers, if used.

You can use Unified Access Gateway appliances, rather than security servers, for secure external access. For more information, see the *Deploying and Configuring Unified Access Gateway* document.

Following is a check list of tasks that a Horizon administrator must perform to use Horizon Client for Chrome.

1   Install Connection Server. For installation instructions, see the *Horizon 7 Installation* document.

2   If you use security servers, install Security Server. The version of Security Server must match the version of Connection Server. For installation instructions, see the *Horizon 7 Installation* document.

3   Verify that each Connection Server instance or security server has a TLS certificate that can be fully verified by using the host name that you enter in the Web browser. For more information, see the *Horizon 7 Installation* document.

4   To use two-factor authentication, such as RSA SecurID or RADIUS authentication, verify that this feature is enabled on Connection Server. Beginning with Horizon 7 version 7.11, you can customize the labels on the RADIUS authentication login page. Beginning with Horizon 7 version 7.12, you can configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *VMware Horizon Console Administration* document.

5   To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. This setting is available in Horizon 7 version 7.1 and later. Beginning with Horizon 7 version 7.8, it is enabled by default. For more information, see the *VMware Horizon Console Administration* document.

6   To send the domain list to Horizon Client, enable the **Send domain list** global setting. This setting is available in Horizon 7 version 7.8 and later and is disabled by default. Earlier Horizon 7 versions send the domain list. For more information, see the *VMware Horizon Console Administration* document for Horizon 7 version 7.8 or later.

7   If you use third-party firewalls, configure rules to allow inbound traffic to TCP port 8443 for all security servers and Connection Server hosts in a replicated group, and configure a rule to allow inbound traffic (from servers) to TCP port 22443 on remote desktop virtual machines and RDS hosts in the data center. For more information, see Firewall Rules for Client Web Browser Access.

8   To provide unauthenticated access to published applications, enable this feature in Connection Server. For more information, see the *VMware Horizon Console 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 from Horizon Client.

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*

After the servers are installed, the **Blast Secure Gateway** setting is enabled on the applicable Connection Server instances and security servers in Horizon Console. Also, the **Blast External URL** setting is configured to use the Blast Secure Gateway on the applicable Connection Server instances and security servers. By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach the Connection Server host or security server host. For more information, see "Set the External URLs for a Connection Server Instance," in the *Horizon 7 Installation* document.

Firewall Rules for Client Web Browser Access

To allow client Web browsers to make connections to security servers, Connection Server instances, remote desktops, and published applications, your firewalls must allow inbound traffic on certain TCP ports.

Horizon Client for Chrome connections must use HTTPS. HTTP connections are not allowed.

By default, when you install a Connection Server instance or security server, the **VMware Horizon View Connection Server (Blast-In)** rule is enabled in the Windows Firewall and the firewall is configured to allow inbound traffic to TCP port 8443.

Table 1-1. Firewall Rules for Client Browser Access

Source	Default Source Port	Protocol	Target	Default Target Port	Notes
Client Web browser	TCP Any	HTTPS	Security server or Connection Server instance	TCP 443	To make the initial connection, the Web browser on a client device connects to a security server or Connection Server instance on TCP port 443.
Client Web browser	TCP Any	HTTPS	Blast Secure Gateway	TCP 8443	After the initial connection is made, the Web browser on a client device connects to the Blast Secure Gateway on TCP port 8443. The Blast Secure Gateway must be enabled on a security server or Connection Server instance to allow this second connection to take place.
Blast Secure Gateway	TCP Any	HTTPS	HTML Access Agent	TCP 22443	If the Blast Secure Gateway is enabled, after the user selects a remote desktop or published application, the Blast Secure Gateway connects to the HTML Access Agent on TCP port 22443 on the remote desktop virtual machine or RDS host. This agent component is included when you install Horizon Agent.
Client Web browser	TCP Any	HTTPS	HTML Access Agent	TCP 22443	If the Blast Secure Gateway is not enabled, after the user selects a remote desktop or published application, the Web browser on a client device makes a direct connection to the HTML Access Agent on TCP port 22443 on the remote desktop virtual machine or RDS host. This agent component is included when you install Horizon Agent.

Install or Upgrade Horizon Client for Chrome

Horizon Client for Chrome is a Chrome app, and you install it in the same way that you install other Chrome apps.

Prerequisites

Verify that the client device meet the system requirements for Horizon Client for Chrome. See System Requirements.

Procedure

1 Log in to the Chromebook.

2 Download and install VMware Horizon Client for Chrome from the Chrome Web Store.

Register the VMware Horizon Client for Chrome Extension

To enable users to connect to a Horizon 7 version 7.4 server with Horizon Client for Chrome, you must register the VMware Horizon Client for Chrome extension. This procedure is not required to connect to Horizon 6 version 6.2.6 or Horizon 7 version 7.5 and later servers.

Prerequisites

Install VMware Horizon Client for Chrome on the client device. See Install or Upgrade Horizon Client for Chrome.

Procedure

1 On the Connection Server host, navigate to the `install_directory`\VMware\VMware View \Server\sslgateway\conf\settings.properties file.

2 In a text editor, open the `settings.properties` file and add the following line.

`chromeExtension.1=ppkfnjlimknmjoaemnpidmdlfchhehel`

3 Save the `settings.properties` file.

4 To make your changes take effect, restart the VMware Horizon View Security Gateway Component service.

What to do next

Verify that you can use Horizon Client for Chrome to connect to a remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Using the Google Admin Console to Configure Enrolled Chromebook Devices

You can use the Google Admin console to configure Connection Sever settings on enrolled Chromebook devices.

You can configure a list of Connection Server instances, a default Connection Server instance, and certain server and client features.

When you configure a list of servers, the servers appear as shortcuts in Horizon Client. If you configure a default server, Horizon Client connects to that server automatically.

You configure these settings in a JSON configuration file. A Chrome administrator must use the Google Admin console to upload the JSON configuration file for the Horizon Client app. For detailed information about using the Google Admin console, see the G Suite Administrator Help.

Connection Server Instance List

You can use properties in the `server-list` section to configure a server list.

Property	Description
server	IP address or host name of the server.
username	(Optional) Name of a user that is entitled to use the server.
domain	(Optional) Domain of the user specified in the `username` property.
description	(Optional) Description of the server.

The following JSON configuration file example shows a list of servers.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
          "server": "viewserver0.mydomain.com",
          "default": false,
          "description": "View Server 0",
          "username": "User0",
          "desktopId": "RDS2012R2DC",
          "domain": "TestDomain0"
        },{
          "server": "viewserver1.mydomain.com",
          "description": "View Server 1",
          "username": "User1",
          "domain": "TestDomain1",
          "default": false
        }, {
          "server": "123.456.1.2",
          "description": "View Server 2",
          "username": "User2",
          "default": false,
          "domain": "TestDomain2"
        }, {
          "server": "123.456.1.3",
          "description": "View Server 3",
          "username": "User3",
          "default": false,
```

```
            "domain": "TestDomain3"
        }, {
            "server": "viewserver4.mydomain.com",
            "description": "View Server 4",
            "username": "User4",
            "default": false,
            "domain": "TestDomain4"
        }]}
      }
    }
  }
```

Default Connection Server Instance

You can use the `default` property to specify a default server in the `server-list` section. Valid values are `true` and `false`.

The following JSON configuration file example shows a default server.

```
{
  "broker_list": {
    "Value": {
      "settings": {
        "server-list": [{
            "server": "viewserver0.mydomain.com",
            "default": true,
            "description": "View Server 0",
            "username": "User0",
            "desktopId": "RDS2012R2DC",
            "domain": "TestDomain0"
        }]}
      }
    }
  }
}
```

Client Features

You can use settings in the `common-setting` section to configure certain client features.

Setting	Description
enableAnonymousLogin	Configures the Unauthenticated Access feature. The `value` property specifies whether the feature is enabled or disabled. The `editable` property specifies whether users can change the **Log in anonymously using Unauthenticated Access** setting in Horizon Client. Valid values for both properties are `true` and `false`.
allowDataSharing	Configures the Horizon Client data sharing feature. The `value` property specifies whether the feature is enabled or disabled. The `editable` property specifies whether users can change the **Allow data sharing** setting in Horizon Client. Valid values for both properties are `true` and `false`.

The following JSON configuration file example shows the common settings.

```
{
    "broker_list": {
        "settings": {
            "server-list": [{
                "server": "viewserver0.mydomain.com",
                "default": true,
                "description": "View Server 0",
                "username": "User0",
                "domain": "TestDomain0"
            }],
            "common-setting": {
                    "allowDataSharing": false,
                    "enableAnonymousLogin": true,
                    "editable":{
                        "allowDataSharing": true,
                        "enableAnonymousLogin: false
                    }
                }
            }
        }
    }
}
```

Server Features

You can use settings in the `server-list` section to configure certain features for specific servers.

Setting	Description
enableHighResolution	Configures the high resolution mode feature. The `value` property specifies whether the feature is enabled or disabled. The `editable` property specifies whether users can change the **High Resolution Mode** setting in Horizon Client. Valid values for both properties are `true` and `false`.
enableMultiMonitor	Configures the multi-monitor feature. The `value` property specifies whether the feature is enabled or disabled. The `editable` property specifies whether users can change the **Use Multi Monitors if there are two monitors** setting in Horizon Client. Valid values for both properties are `true` and `false`.
enableWindowsKey	Enables or disables the Windows key for remote desktops. The `value` property specifies whether the feature is enabled or disabled. The `editable` property specifies whether users can change the **Enable Windows Key for Desktops** setting in Horizon Client. Valid values for both properties are `true` and `false`.

Setting	Description
timezoneSync	Configures the time zone for remote desktops and published applications. The isSync property specifies whether to set the time zone automatically. The editable property specifies whether users can change the **Set Time Zone Automatically** setting in Horizon Client. Valid values for both properties are true and false. If you set isSync to false, you can set the time zone manually by specifying the timezone property.
resolution	Configures the screen resolution. The width property specifies the screen width and the height property specifies the screen height. Both values should be less than or equal to the Chromebook window's width and height, otherwise Horizon Client uses the default resolution (the Chromebook window's width and height).

The following JSON configuration file example shows the server settings.

```
{
    "broker_list": {
        "settings": {
            "server-list": [{
                "server": "viewserver0.mydomain.com",
                "default": true,
                "description": "View Server 0",
                "username": "User0",
                "domain": "TestDomain0",
                "settings": {
                    "enableHighResolution": false,
                    "enableMultiMonitor": false,
                    "enableWindowsKey": true,
                    "timezoneSync": {
                        "isSync": false,
                        "timezone": "-00:00"
                    },
                    "resolution": {
                      "width": 600,
                      "height": 800
                    },
                    "editable": {
                        "enableHighResolution": true,
                        "enableMultiMonitor": false,
                        "enableWindowsKey": true,
                        "timezoneSync": false
                    }
                }
            }],
        }
    }
}
```

Configure HTML Access Agents to Use New TLS Certificates

To comply with industry or security regulations, you can replace the default TLS certificates that the HTML Access Agent generates with certificates that a Certificate Authority (CA) signs.

When you install the HTML Access Agent on a remote desktop, the HTML Access Agent service creates default self-signed certificates. The service presents the default certificates to browsers that use Horizon Client for Chrome.

Note In the guest operating system on the desktop virtual machine, this service is called the VMware Blast service.

To replace the default certificates with signed certificates that you obtain from a CA, you must import a certificate into the Windows local computer certificate store on each remote desktop. You must also set a registry value that allows the HTML Access Agent to use the new certificate.

If you replace the default HTML Access Agent certificates with CA-signed certificates, configure a unique certificate on each remote desktop. Do not configure a CA-signed certificate on a parent virtual machine or template that you use to create a desktop pool. That approach results in hundreds or thousands of remote desktops that have identical certificates.

Add the Certificate Snap-In to MMC on a Remote Desktop

Before you can add certificates to the Windows local computer certificate store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the remote desktops where the HTML Access Agent is installed.

Prerequisites

Verify that the MMC and Certificate snap-in are available on the Windows guest operating system where the HTML Access Agent is installed.

Procedure

1   On the remote desktop, click **Start** and type `mmc.exe`.

2   In the **MMC** window, go to **File > Add/Remove Snap-in**.

3   In the **Add or Remove Snap-ins** window, select **Certificates** and click **Add**.

4   In the **Certificates snap-in** window, select **Computer account**, click **Next**, select **Local computer**, and click **Finish**.

5   In the **Add or Remove snap-in** window, click **OK**.

What to do next

Import the SSL certificate into the Windows local computer certificate store. See Import a Certificate for the HTML Access Agent into the Windows Certificate Store.

Import a Certificate for the HTML Access Agent into the Windows Certificate Store

To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Perform this procedure on each remote desktop where the HTML Access Agent is installed.

Prerequisites

- Verify that the HTML Access Agent is installed on the remote desktop.

- Verify that the CA-signed certificate was copied to the remote desktop.

- Verify that the Certificate snap-in was added to MMC. See Add the Certificate Snap-In to MMC on a Remote Desktop.

Procedure

1 In the MMC window on the remote desktop, expand the **Certificates (Local Computer)** node and select the **Personal** folder.

2 In the Actions pane, go to **More Actions > All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the certificate is stored.

4 Select the certificate file and click **Open**.

   To display your certificate file type, you can select its file format from the **File name** drop-down menu.

5 Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extendable properties**.

8 Click **Next** and click **Finish**.

   The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

9 Verify that the new certificate contains a private key.

   a In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

   b In the General tab of the Certificate Information dialog box, verify that the following statement appears: `You have a private key that corresponds to this certificate.`

What to do next

If necessary, import the root certificate and intermediate certificates into the Windows certificate store. See Import Root and Intermediate Certificates for the HTML Access Agent.

Configure the appropriate registry key with the certificate thumbprint. See Set the Certificate Thumbprint in the Windows Registry.

Import Root and Intermediate Certificates for the HTML Access Agent

If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

Procedure

1   In the MMC console on the remote desktop, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

   ▪   If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.

   ▪   If your root certificate is not in this folder, proceed to step 2.

2   Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

3   In the **Certificate Import** wizard, click **Next** and browse to the location where the root CA certificate is stored.

4   Select the root CA certificate file and click **Open**.

5   Click **Next**, click **Next**, and click **Finish**.

6   If an intermediate CA signed your server certificate, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

   a   Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

   b   Repeat steps 3 through 6 for each intermediate certificate that must be imported.

What to do next

Configure the appropriate registry key with the certificate thumbprint. See Set the Certificate Thumbprint in the Windows Registry.

Set the Certificate Thumbprint in the Windows Registry

To allow the HTML Access Agent to use a CA-signed certificate that was imported into the Windows certificate store, you must configure the certificate thumbprint in a Windows registry key. You must take this step on each remote desktop on which you replace the default certificate with a CA-signed certificate.

Prerequisites

Verify that the CA-signed certificate is imported into the Windows certificate store. See Import a Certificate for the HTML Access Agent into the Windows Certificate Store.

Procedure

1   In the MMC window on the remote desktop where the HTML Access Agent is installed, navigate to the **Certificates (Local Computer) > Personal > Certificates** folder.

2   Double-click the CA-signed certificate that you imported into the Windows certificate store.

3   In the Certificates dialog box, click the Details tab, scroll down, and select the **Thumbprint** icon.

4   Copy the selected thumbprint to a text file.

For example: 31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e

Note   When you copy the thumbprint, do not to include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

5   Start the Windows Registry Editor on the desktop where the HTML Access Agent is installed.

6   Navigate to the HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config registry key.

7   Modify the SslHash value and paste the certificate thumbprint into the text box.

8   Reboot Windows.

Results

When a user connects to a remote desktop through Horizon Client for Chrome, the HTML Access Agent presents the CA-signed certificate to the user's browser.

Configure HTML Access Agents to Use Specific Cipher Suites

You can configure the HTML Access Agent to use specific cipher suites instead of the default set of ciphers.

By default, the HTML Access Agent requires incoming TLS connections to use encryption based on certain ciphers that provide strong protection against network eavesdropping and forgery. You can configure an alternative list of ciphers for the HTML Access Agent to use. The set of acceptable ciphers is expressed in the OpenSSL format, which is described at https://www.openssl.org/docs/manmaster/man1/ciphers.html.

Procedure

1 On the desktop where the HTML Access Agent is installed, start the Windows Registry Editor.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.

3 Add a new String (REG_SZ) value, `SslCiphers`, and paste the cipher list in the OpenSSL format into the text box.

4 To make your changes take effect, restart the VMware Blast service.

   In the Windows guest operating system, the service for the HTML Access Agent is called VMware Blast.

Results

To revert to using the default cipher list, delete the `SslCiphers` value and restart the VMware Blast service. Do not simply delete the data part of the value because the HTML Access Agent will then treat all ciphers as unacceptable, in accordance with the OpenSSL cipher list format definition.

When the HTML Access Agent starts, it writes the cipher definition in the VMware Blast service's log file. You can discover the current default cipher list by inspecting the logs when the VMware Blast service starts with no `SslCiphers` value configured in the Windows Registry.

The HTML Access Agent default cipher definition might change from one release to the next to provide improved security.

Using a CA-Signed Certificate with Unified Access Gateway

If you use a Unified Access Gateway appliance instead of a Connection Server or security server, you must install a CA-signed certificate that has a Subject Alternative Name (SAN) configured.

If you use a CA-signed certificate that does not have a SAN configured, or a self-signed certificate, users receive a "Your connection is not private" error and cannot connect with Horizon Client for Chrome.

Note If you use a Connection Server instance or security server, users can still connect by clicking the `Proceed to ip-address (unsafe)` link.

For information about installing and configuring certificates for Horizon 7, see the *Horizon 7 Installation* document. For information about installing certificates in Chrome, see the Google Chrome documentation.

Configure Horizon 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 to join the CEIP, see the *VMware Horizon Console 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.

Procedure

1   Click **Settings** (gear icon) on the server selection page.

2   Tap to toggle the **Allow data sharing** option to on or off.

Data Collected by VMware

If your company participates in the VMware Customer Experience Improvement Program (CEIP), and data sharing is enabled on the client, VMware collects data about the client system.

VMware collects data on the clients to prioritize hardware and software compatibility. If a Horizon administrator has opted to participate in the CEIP, VMware collects anonymous data about your deployment to improve the response to customer requirements. No data that identifies your organization is collected. Client information is sent first to Connection Server and then on to VMware, along with data from servers, desktop pools, and remote desktops.

To participate in the CEIP, the administrator who installs Connection Server can opt in while running the Connection Server installation wizard, or an administrator can set an option in Horizon Console after the installation.

Table 1-2. Client Data Collected for the CEIP

Description	Field name	Is This Field Made Anonymous?	Example Value
Company that produced the application	`<client_vendor>`	No	VMware
Product name	`<client_product>`	No	VMware Horizon Client for Chrome
Client product version	`<client_version>`	No	5.4.0-*build_number*
Client binary architecture	`<client_arch>`	No	browser
Native architecture of the browser	`<browser_arch>`	No	ChromeOS
Browser user agent string	`<browser_user_agent>`	No	Chrome/3.0.1750
Browser's internal version string	`<browser_version>`	No	3.0.1750 (for Chrome)
Browser's core implementation	`<browser_core>`	No	Chrome
Whether the browser is running on a handheld device	`<browser_is_handheld>`	No	true

Managing Remote Desktop and Published Application Connections

2

End users can use HTML Access to connect to a server and use remote desktops and published applications. For troubleshooting purposes, end users can reset remote desktops and published applications.

This chapter includes the following topics:

- Connect to a Remote Desktop or Published Application
- Use Unauthenticated Access to Connect to Published Applications
- Trust a Self-Signed Root Certificate
- Setting the Time Zone
- Manage Server Shortcuts
- Log Off or Disconnect

Connect to a Remote Desktop or Published Application

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

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

Prerequisites

- 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.

- If you are using smart card authentication, make sure that all smart card authentication requirements are met and that you are familiar with the limitations. For information, see Smart Card Authentication Requirements and Smart Card Authentication Limitations.

- 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.

Procedure

1 Log in to the Chromebook.

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

3 Open the VMware Horizon Client app.

4 If you are prompted to grant access to the Smart Card Connector, click **Allow**.

   This prompt appears the first time you start Horizon Client if smart card authentication is configured on the Chromebook.

5 Connect to a server.

Option	Action
Connect to a new server	Click the plus sign (+), enter the name of the server, enter a description of the server (optional), and click **Connect**.
Connect to an existing server	Click the server shortcut.

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

6 If a smart card is required or optional, select the smart card certificate to use and enter your PIN.

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

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

8 If you are prompted a second time for RSA SecurID or RADIUS authentication credentials, enter the next generated number on the token.

   Do not enter your PIN, and do not enter the same generated number that entered previously. If necessary, wait until a new number is generated. If this step is required, it is required only when you mistype the first passcode or when configuration settings in the RSA server change.

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

   a   Enter 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 you cannot select a domain, you must enter the user name in the format `username@domain` or `domain\username`.

   c   Tap **Login**.

10   (Optional) To mark a remote desktop or published application as a favorite, click the gray star inside the icon for the remote desktop or published application.

   The star icon turns from gray to yellow. The next time you log in, you can click the star icon in the upper-right part of the browser window to show only favorite items.

11   To connect to remote desktop or published application, click its icon in the desktop and application selector window.

12   If you are using smart card authentication, enter the smart card PIN again inside the remote session.

Results

If, soon after connecting to a remote desktop or published application, you are disconnected and see a prompt that asks you to click a link to accept the security certificate, select whether to trust the certificate. See Trust a Self-Signed Root Certificate.

If the time zone in the remote desktop or published application does not use the time zone set in the client device, set the time zone manually. See Setting the Time Zone.

What to do next

Horizon Client provides navigation aids to help you use remote desktops and published applications. For information, see Using Remote Desktops and Using Published Applications.

Use Unauthenticated Access to Connect to Published Applications

If you have an Unauthenticated Access user account, you can log in to a server anonymously and connect to your published applications.

Prerequisites

- Perform the administrative tasks described in Preparing Connection Server and Security Servers.

- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *VMware Horizon Console Administration* document.

Procedure

1 Click the **Settings** toolbar button in the upper-right corner of the server selection page and toggle the **Log in anonymously using Unathenticated Access** option to on.

2 Connect to a server, enter an Unauthenticated Access user account, and click **Login**.

The application selection window appears.

3 Click the icon for the published application that you want to access.

Trust a Self-Signed Root Certificate

Sometimes, when connecting to a remote desktop or published application for the first time, the browser might prompt you to accept the self-signed certificate that the remote machine uses. You must trust the certificate before you can connect to the remote desktop or published application.

Chrome gives you the option to trust the self-signed certificate permanently. If you do not trust the certificate permanently, you must verify the certificate every time you restart your browser.

Procedure

1 If the browser presents an untrusted certificate warning, or a warning appears stating that your connection is not private, examine the certificate to verify that it matches the certificate that your company uses.

You might need to contact your system administrator for assistance. For example, in Chrome, you might use the following procedure.

   a Click the lock icon in the address bar.

   b Click the **Certificate information** link.

   c Verify that the certificate matches the certificate that your company uses.

      You might need to contact your system administrator for assistance.

2 Accept the security certificate.

In Chrome, you can click the **Advanced** link on the browser page, and click **Proceed to** *server-name* **(unsafe)**.

Results

The remote desktop or published application starts.

Setting the Time Zone

The time zone that a remote desktop or published application uses is set to the time zone in your local system automatically.

When you use Horizon Client, if the time zone cannot be correctly determined due to certain daylight saving policies, you might need to set the time zone manually.

To set the correct time zone manually before you are connected to a remote desktop or published application, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window. Turn off the **Set Time Zone Automatically** option in the **Settings** window and select one of the time zones from the drop-down menu. The value you select is saved as your preferred time zone to use when connecting to a remote desktop or published application.

To set the correct time zone manually after you are connected to a remote desktop or published application, return to the desktop and application selector window and change the current time zone setting.

Manage Server Shortcuts

After you connect to a server, Horizon Client creates a server shortcut. You can edit and remove server shortcuts.

Horizon Client saves the server name or IP address in a shortcut, even if you mistype the server name or type the wrong IP address. You can delete or change this information by editing the server name or IP address. If you do not type a server description, the server name or IP address becomes the server description.

Procedure

1   Right-click the server shortcut.

    A context menu appears.

2   Use the context menu to delete the server shortcut or edit the server name or server description.

3   If you edited the server shortcut, click **Complete** to save your changes.

Log Off or Disconnect

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

Procedure

◆ Disconnect from a remote desktop.

Option	Description
From within the remote desktop	Point your mouse at the top of the remote desktop window until the menu bar appears and then click the **Disconnect** button. Alternatively, click the **X** (Close) button in the upper-right corner of the remote desktop window.
From the Session Management Center	Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, open the Session Management Center, select the remote desktop session, and click **Disconnect**. You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

◆ Log off from a remote desktop.

Option	Description
From within the remote desktop	Point your mouse at the top of the remote desktop window until the menu bar appears and then click the **Log out** button.
From the Session Management Center	Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, open the Session Management Center, select the remote desktop session, and click **Log off**. You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

◆ Close a published application.

Option	Description
From within the published application	Click the **X** (Close) button in the corner of the published application window.
From the shelf	Right-click the published application icon in the shelf and click **Close**.

◆ To log off from a server, click the **Log Out** button in the upper-right corner of the desktop and application selector window.

Using a Remote Desktop or Published Application

3

Horizon Client provides a familiar, personalized desktop and application environment.

This chapter includes the following topics:

- Feature Support Matrix
- Gestures
- Using Multiple Monitors
- Setting the Screen Resolution
- Use Full-Screen Mode
- Using DPI Synchronization
- Using the Real-Time Audio-Video Feature for Webcams and Microphones
- Using Remote Desktops
- Using Published Applications
- Using Published Applications in Kiosk Mode
- Copying and Pasting Text and Images
- Transferring Files Between the Client and a Remote Desktop or Published Application
- Share Access to Local Folders and Drives with Client Drive Redirection
- Printing From a Remote Desktop or Published Application
- Use Multiple Sessions of a Published Application From Different Client Devices
- Adjusting the Sound in Remote Desktops and Published Applications
- Shortcut Key Combinations
- Internationalization

Feature Support Matrix

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

Table 3-1. Features Supported for Windows Virtual Desktops

Feature	Windows 7 Desktop	Windows 8.x Desktop	Windows 10 Desktop	Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Desktop
RSA SecurID or RADIUS	X	X	X	X
Single sign-on	X	X	X	X
RDP display protocol				
PCoIP display protocol				
VMware Blast display protocol	X	X	X	X
USB redirection				
Real-Time Audio-Video (RTAV)	X	X	X	X
Windows Media MMR				
Virtual printing				
VMware Integrated Printing			X	Windows Server 2016/2019 only
Location-based printing	X	X	X	X
Smart cards	X	X	X	X
Multiple monitors	X	X	X	X

For descriptions of these features and their limitations, see the *Horizon 7 Architecture Planning* document.

Features Supported for Published Desktops on RDS Hosts

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

Note The following table contains rows only for the features that are available from RDS hosts if you use Horizon Client for Chrome. Additional features are available if you use an installed version of Horizon Client, such as Horizon Client for Windows.

Table 3-2. Features Supported for RDS Hosts with View Agent 6.2.6 or Later, or Horizon Agent 7.0 or Later, Installed

Feature	Windows Server 2012 R2 RDS Host	Windows Server 2016 RDS Host	Windows Server 2019 RDS Host
RSA SecurID or RADIUS	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Single sign-on	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
VMware Blast display protocol	X	Horizon AgentHorizon Agent 7.0.2 and later	Horizon Agent 7.7 and later

Table 3-2. Features Supported for RDS Hosts with View Agent 6.2.6 or Later, or Horizon Agent 7.0 or Later, Installed (continued)

Feature	Windows Server 2012 R2 RDS Host	Windows Server 2016 RDS Host	Windows Server 2019 RDS Host
VMware Integrated Printing		Horizon Agent 7.12 and later	Horizon Agent 7.12 and later
Location-based printing	View Agent 6.2.6 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.0.2 through 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.7 and later
Real-Time Audio-Video (RTAV)	Horizon Agent 7.0.2 and later	Horizon Agent 7.0.3 and later	Horizon Agent 7.7 and later
Multiple monitors	X	X	Horizon Agent 7.7 and later
Smart cards	X	X	Horizon Agent 7.7 and later

For information about which editions of each guest operating system are supported, see the *Horizon 7 Installation* document.

Gestures

VMware has created user interaction aids to help you navigate conventional Windows user interface elements on a non-Windows device.

Clicking

As in other apps, you can tap your touchpad to click a user interface element. If the Chromebook has a touch screen, you can touch to click a user interface element. You can also use an external mouse.

Right-Clicking

The following options are available for right-clicking:

- Tap with two fingers on the touchpad.

- Hold down the Alt key on the keyboard and tap the touchpad with a single finger.

- Use an external mouse to right-click.

- If the Chromebook has a touch screen, tap with two fingers to right-click.

Scrolling and Scrollbars

The following options are available for vertical scrolling.

- Tap and hold with your thumb and then scroll down with one finger on the touchpad. You can also scroll with two fingers.

- Use an external mouse to scroll.

- If the Chromebook has a touch screen, tap with two fingers and then drag to scroll. The text under your fingers moves in the same direction as your fingers.

Zooming In and Out

Zooming in and out is not supported.

Window Resizing

To use the touchpad to resize a window, touch and hold one finger at the corner or side of the window and drag to resize.

If the Chromebook has an external mouse, place your cursor on the edge of the window and drag the border of the window to make it wider or narrower.

If the Chromebook has a touch screen, place one finger at the corner or side of the window and drag to resize.

Sound, Music, and Video

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

Multiple Monitor Feature Limitation

Touch gestures are disabled when the multiple monitor feature is enabled. For more information, see Using Multiple Monitors.

Using Multiple Monitors

You can use up to two monitors with remote desktops.

If you are not connected to a remote desktop, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and turn on the **Use Multi Monitors if there are two monitors** option in the **Settings** window. If you have two monitors and you connect to a remote desktop, the multiple-monitor feature is used. If you have only a single monitor, or more than two monitors, single-monitor mode is used. If you switch to another remote desktop, it opens in multiple-monitor mode and the previous remote desktop reverts back to single-monitor mode.

If you are already connected to a remote desktop, you can enable the multiple-monitor feature by turning on the **Use Multi Monitors if there are two monitors** option in the **Settings** window.

The multiple-monitor feature has the following limitations.

- It is not supported for published applications.

- It is not supported if Unified Desktop mode is enabled for the client device.

For information about how to disable Unified Desktop mode, see the Google Chrome documentation.

An administrator can disable the multiple-monitor feature. For information, see Using the Google Admin Console to Configure Enrolled Chromebook Devices.

Setting the Screen Resolution

Horizon Client can resize the remote desktop to match the size of the browser window. To use this feature, a Horizon administrator must configure the remote desktop to have the correct amount of video RAM (VRAM). The default VRAM configuration is 36 MB. If you are not using 3D applications, the minimum VRAM requirement is 16 MB.

If you use a Chromebook device that has a high pixel density resolution, such as a Google Chromebook Pixel, you can set the remote desktop or published application to use that resolution. Turn on the **High Resolution Mode** option in the **Settings** window. This option appears in the **Settings** window only if you are using a high-resolution display, or a normal display that uses a scale that is greater than 100 percent, and an administrator has not disabled the feature.

For information about disabling the High Resolution Mode feature, see Using the Google Admin Console to Configure Enrolled Chromebook Devices .

The High Resolution Mode feature cannot change the resolution for an active remote session. You must log out and log in again to make the feature take effect.

To use the 3D rendering feature, you must allocate sufficient VRAM for each remote desktop.

- The software-accelerated graphics feature, which is available with vSphere 5.0 or later, enables you to use 3D applications, such as Windows Aero themes or Google Earth. This feature requires from 64 MB to 128 MB of VRAM.

- The shared hardware-accelerated graphics feature (vSGA), which is available with vSphere 5.1 or later, enables you to use 3D applications for design, modeling, and multimedia. This feature requires from 64 MB to 512 MB of VRAM. The default is 96 MB.

- The dedicated hardware-accelerated graphics feature (vDGA), which is available with vSphere 5.5 or later, dedicates a single physical GPU (graphical processing unit on an ESXi host to a single virtual machine. Use this feature if you require high-end hardware-accelerated workstation graphics. This feature requires from 64 MB to 512 MB of VRAM. The default is 96 MB.

When 3D rendering is enabled, the maximum number of monitors is one and the maximum resolution is 3840 x 2160.

Similarly, if you use a Chromebook that has a high pixel density resolution, such as a Google Chromebook Pixel, you must allocate sufficient VRAM for each remote desktop.

Important Estimating the amount of VRAM that you need for the VMware Blast display protocol is similar to estimating how much VRAM is required for the PCoIP display protocol. For guidelines, see "Estimating Memory Requirements for Virtual Desktops" in the *Horizon 7 Architecture Planning* document.

Use Full-Screen Mode

You can display a remote desktop in full-screen mode.

Prerequisites

Connect to the remote desktop.

Procedure

◆ To display the remote desktop in full-screen mode, point to the top of the remote desktop window until the menu bar appears and click the **Fullscreen** button.

◆ To exit from full-screen mode, point to the top of the remote desktop window until the menu bar appears and click the **Quit fullscreen** button.

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.

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

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

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

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

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

- 32-bit or 64-bit Windows 7

- 32-bit or 64-bit Windows 8.x

- 32-bit or 64-bit Windows 10

- Windows Server 2012 R2 configured as a desktop

- Windows Server 2016 configured as a desktop

- Windows Server 2019 configured as a desktop

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

- Windows Server 2012 R2

- Windows Server 2016

- Windows Server 2019

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

- Windows 10 version 1607 and later

- Windows Server 2016 and later configured as a desktop

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

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, but the DPI setting does not change in the remote desktop, you might need to log out and log in again to make Horizon Client aware of the new DPI setting on the client system.

- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you might need to log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.

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

With the Real-Time Audio-Video feature, you can use the client machine'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, and it supports standard webcams, audio USB devices, and analog audio input.

The default video resolution is 320 x 240 pixels. The default Real-Time Audio-Video settings work well with most webcam and audio applications.

For information about changing the Real-Time Audio-Video settings, see "Configuring Real-Time Audio-Video Group Policy Settings" in the *Configuring Remote Desktop Features in Horizon 7* document.

When a remote desktop or published application is connected to the client machine's webcam or microphone, before the remote desktop or published application can use to the webcam or microphone, Chrome asks for permission the first time. If you allow the device to be used, Chrome does not ask for permission again.

If Real-Time Audio-Video is being used in a remote desktop or published application session and you open a connection to a second remote desktop or published application, and if a security warning appears (for example, if a valid certificate was not installed), ignoring the warning and continuing to connect to the second remote desktop or published application causes Real-Time Audio-Video to stop working in the first session.

Select a Preferred Webcam or Microphone on a Chromebook

With the Real-Time Audio-Video feature, if multiple webcams or microphones are connected to the local client system, only one of the devices is used in the remote desktop or published application. To specify which webcam or microphone is preferred, you can configure Real-Time Audio-Video settings in Horizon Client for Chrome.

If it is available, the preferred webcam or microphone is used in the remote desktop or published application. If the preferred webcam or microphone is not available, another webcam or microphone is used.

Prerequisites

- Verify that a USB webcam or USB microphone, or other type of microphone, is installed and operational on the local client system.

- Connect to a server.

Procedure

1   Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and scroll down to the Real-Time Audio-Video settings.

2   From the **Preferred microphone** drop-down menu, select a preferred microphone.

3   From the **Preferred webcam** drop-down menu, select a preferred webcam.

Results

The next time you start a remote desktop or published application, the preferred webcam or microphone that you selected is redirected to the remote session.

Using Remote Desktops

You can use the top menu bar in a remote desktop window to perform common tasks in a remote desktop.

- To open the top menu bar in a remote desktop, move your mouse to the top of the remote desktop window until the top menu bar appears.

- To use the Ctrl+Alt+Delete keyboard shortcut inside a remote desktop, click **Send Ctrl+Alt +Delete to the to current work area** in the top menu bar.

- To enter full screen mode, click **Fullscreen** in the top menu bar. To exit full screen mode, click **Quit Fullscreen** in the top menu bar.

- To use the Esc key in a remote desktop when the remote desktop is in full screen mode, click **Send ESC** in the top menu bar.

- To disconnect from a remote desktop, click **Disconnect** in the top menu bar, or click the **X** (Close) button in the upper-right corner of the remote desktop window.

- To view information about Horizon Client, click **About** in the top menu bar.

To switch to another open remote desktop, click that remote desktop window. You can also browse through all the open remote desktops (including local and published applications) on the client device by pressing Alt+Tab. To focus on a selected remote desktop, release the Alt key.

For information about logging off from a remote desktop, see Log Off or Disconnect. For information about restarting a remote desktop, see Restart a Remote Desktop. For information about resetting a remote desktop, see Reset Remote Desktops or Published Applications.

Using Published Applications

Horizon Client provides navigation aids to help you use published applications.

- To maximize and minimize a published application, click the **Maximize** and **Minimize** buttons in the same way that you do in any application.

- To restore a minimized published application, click its shelf icon on the client device or select the published application session and click the **Restore** button in the Session Management Center window. In Kiosk mode, you must use the Session Management Center to restore a minimized published application. For more information, see Using Published Applications in Kiosk Mode.

- To reset a published application, see Reset Remote Desktops or Published Applications.

To switch to another open published application, click the published application window. You can also browse through all open published applications (including local applications and remote desktops) on the client device by pressing Alt+Tab. To focus on a selected published application, release the Alt key.

Using Published Applications in Kiosk Mode

When you are using published applications in Kiosk mode, you must use the Session Management Center to perform certain tasks.

- To open the Session Management Center window, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and click **Open** next to **Session Management Center**. If you have a remote desktop session open, you must close the remote desktop session before you can access the desktop and application selector window.

- To restore a minimized published application in Kiosk mode, select the published application session and click the **Restore** button in the Session Management Center window.

- To switch published applications in Kiosk mode, select the published application session and click the **Restore** button in the Session Management Center window.

- To close the Session Management Center window in Kiosk mode, click the close (**X**) button in the upper-right corner of the Session Management Center window.

Copying and Pasting Text and Images

By default, you can copy and paste plain text and HTML-format rich text from the client device to a remote desktop or published application.

You can also copy and paste plain text and HTML-format rich text from a remote desktop or published application to the client device if a Horizon administrator enables this feature.

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

When you copy and paste images and rich text, the following restrictions apply.

- If the clipboard source is a Google app, such as Google Docs, you can copy and paste images only when the client device can access the Google website.

- If you copy an image and rich text (or plain text) together from the client device, and the destination is an application that supports only rich text, such as WordPad, the image is discarded and only the text is copied and pasted. If the destination application supports HTML/XML-format rich text, such as Microsoft Word, this restriction does not apply.

- A Horizon administrator can use group policies to restrict clipboard formats during copy and paste operations. The clipboard format filter policies for Microsoft Office Chart and Smart Art data and Microsoft Text Effects data is not supported. For information about clipboard format filter policies, see the *Configuring Remote Desktop Features in Horizon 7* document. Using Smart Policies to control the copy and paste behavior in remote desktops is not supported.

You can copy a maximum of 1 MB of data from a remote desktop or published application to the client device. Plain text that exceeds this limit is truncated. Rich text is converted to plain text.

The clipboard can accommodate a maximum of 1 MB of data for all types of copy and paste operations. If the plain text and rich text data together use less than maximum clipboard size, the formatted text is pasted. Often the rich text cannot be truncated, so that if the text and formatting use more than the maximum clipboard size amount, the rich text is discarded, and plain text is pasted. If you are unable to paste all the formatted text you selected in one operation, you might need to copy and paste smaller amounts in each operation.

Logging Copy and Paste Activity

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

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

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

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

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

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

Transferring Files Between the Client and a Remote Desktop or Published Application

You can transfer files from the client device to a remote desktop or published application. You might also be able to transfer files from a remote desktop or published application to the client system.

To upload a file, drag the file from the client system to the remote desktop or published application window. When the upload is finished, the file appears in the `C:\Users\`*username*`\Documents` folder.

To download a file, select the file in the remote desktop or published application by pressing Ctrl +C. After you confirm the file transfer, the file appears in the `Downloads` directory on the client device.

A Horizon administrator can configure the ability to allow, disallow, or allow in one direction only, the transfer of files by modifying the **Configure file transfer** group policy setting for VMware Blast. This group policy setting has the following values.

- If the **Disabled both upload and download** value is selected, you cannot transfer files in either direction.

- If the **Enabled file upload only** value is selected (the default setting), you can only transfer files from the client system to a remote desktop or published application.

- If the **Enabled file download only** value is selected, you can only transfer files from a remote desktop or published application to the client system.

If the **Configure clipboard redirection** group policy setting is disabled from the server to the client, file download is also disabled.

For more information about these group policy settings, see the *Configuring Remote Desktop Features in Horizon 7* document.

This feature has the following limitations.

- You can download files up to 500 MB and upload files up to 2 GB.

- You cannot download or upload folders or files that have a size of zero.

- If a file transfer is in progress in a remote session and you open a connection to a second remote session, and if a security warning appears, if you ignore the warning and continue to connect to the second remote session the file transfer in the first session aborts.

Share Access to Local Folders and Drives with Client Drive Redirection

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

Shared drives can include mapped drives and USB storage devices.

The client drive redirection feature has the following limitations.

- Using the Windows registry key settings `ForcedByAdmin`, `default shares`, and `permissions` to configure client drive redirection are not supported.

- The TCP and UDP side channels are not supported. If the agent machine is configured to use either of these side channels, you cannot use the client drive redirection feature.

- Dynamic Environment Manager policies are not supported.

- Network recovery is not supported. You cannot use client drive redirection after network reconnection unless you disconnect the session and connect again.

- You can use the client drive redirection feature with only one remote session at a time. Multiple remote sessions are not supported.

- You cannot change properties for shared folders or files in the remote desktop.

Prerequisites

To share folders and drives with a remote desktop or published application, a Horizon administrator must enable the client drive redirection feature. This task involves installing Horizon Agent 7.4 or later and enabling the agent **Client Drive Redirection** option. It can also include setting policies to control the client drive redirection behavior. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

1 Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and turn on the **Enable Folder Sharing** option in the Settings window.

2 To select a specific folder or drive to share, click **Select**, click **Add**, browse to and select the folder or drive, and click **OK**.

You can add multiple folders and drives, but you can select only one item at a time. You can remove a folder or drive by clicking the **X** next to its name in the Folder Sharing dialog box.

3 To save the settings, click **OK**.

The folder sharing settings apply to all remote desktops and published applications.

Results

In a remote desktop, a network location appears for each folder and drive that you shared. For example, if you shared a folder named `test1`, the `test1(Z:)` network location might appear in the remote desktop. A device also appears for each shared folder and drive. The device name format is *folder* `on Horizon`, for example, `test1 on Horizon`.

In a published application, you can select **File > Open** or **File > Save As**, if applicable, and navigate to the shared folder or drive.

Printing From a Remote Desktop or Published Application

You can print to a network printer or a locally attached printer from a remote desktop or published application.

To use this feature, Horizon Agent 7.12 or later must be installed on the virtual machine or RDS host, and the VMware Integrated Printing option must be enabled during the installation. For more information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Desktop and Application Pools in Horizon 7* document.

You can disable the VMware Integrated Printing feature for Horizon Client for Chrome users by enabling the **Disable printer redirection for non-desktop client** group policy setting. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

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. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and other settings.

Prerequisites

To use VMware Integrated Printing, a Horizon administrator must enable the VMware Integrated Printing feature in the remote desktop. This task involves enabling the **VMware Integrated Printing** option in the Horizon Agent installer and setting policies that control virtual printing behavior. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document. For information about configuring policies, see the *Configuring Remote Desktop Features in Horizon 7* 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.

This feature requires Horizon Agent 7.12 or later.

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.

    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>*).

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**.

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 on to the server from different client devices.

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

The multi-session mode feature has the following limitations.

- Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.

- If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

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

Procedure

1 Connect to a server.

2 Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, scroll down to the **Multi-Launch** setting, and click **Set**.

   Alternatively, if you previously started a remote desktop or published application, you can click the **Open Menu** button in the sidebar, click **Settings**, and scroll down to the **Multi-Launch** setting. If no published applications are available to use in multi-session mode, the **Multi-Launch** setting is dimmed.

3 Select the published applications that you want to use in multi-session mode and click **OK**.

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

Adjusting the Sound in Remote Desktops and Published Applications

By default, sound playback is enabled for remote desktops and published applications. A Horizon administrator can set a policy to disable sound playback. Some limitations apply to sound playback in remote desktops and published applications.

- To turn up the volume, use the sound control on the client system, not the sound control in the remote desktop.

- Occasionally, the sound might go out of sync with the video.

- In conditions of heavy network traffic, or if the browser is performing many tasks, sound quality might be reduced.

Shortcut Key Combinations

Some key combinations cannot be sent to a remote desktop or published application, regardless of the language that you use.

Chrome allows some key presses and key combinations to be sent to both the client system and the destination system. For other keys and key combinations, the input is processed only locally and is not sent to the destination system.

The following keys and keyboard combinations often do not work in remote desktops.

- Ctrl+T

- Ctrl+W

- Ctrl+N

- Command key

- Alt+Enter

- Ctrl+Alt+*any_key*

  Important   To input Ctrl+Alt+Del, use the **Send Ctrl+Alt+Delete** toolbar button at the top of the sidebar.

- Caps Lock+*modifier_key* (such as Alt or Shift)

- Function keys on a Chromebook

- Windows key combinations

If you enable the Windows key for remote desktops, the following Windows key combinations work in remote desktops. To enable this key, click the **Open Settings Window** toolbar button in the sidebar and turn on **Enable Windows Key for Desktops**.

After you turn on the **Enable Windows Key for Desktops**, you must press Ctrl+Search to simulate pressing the Windows key.

These key combinations do not work for published applications. These key combinations do work for Windows Server 2012 R2 and Windows Server 2016 remote desktops and published desktops.

Some key combinations that work in remote desktops that have a Windows 8.x or Windows Server 2012 R2 operating system do not work in remote desktops that have a Windows 7 or Windows 10 operating system.

Table 3-3. Windows Key Shortcuts for Windows 10 Remote Desktops and Windows Server 2016 Remote Desktops

Keys	Action	Limitations
Win	Open or close Start.	
Win+A	Open Action center.	
Win+E	Open File Explorer.	
Win+G	Open game bar when a game is open.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	

Table 3-3. Windows Key Shortcuts for Windows 10 Remote Desktops and Windows Server 2016 Remote Desktops (continued)

Keys	Action	Limitations
Win+K	Open the Connection quick action.	
Win+M	Minimize all windows.	
Win+R	Open the Run dialog box.	
Win+S	Open Search.	
Win+X	Open the **Quick Link** menu.	
Win+, (comma)	Temporarily peek at the remote desktop.	
Win+Shift+M	Restore minimized windows on the remote desktop.	
Win+Enter	Open Narrator.	

Table 3-4. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops

Keys	Action	Limitations
Win+F1	Open Windows Help and Support.	
Win	Show or hide the Start window.	
Win+B	Set focus on the notification area.	
Win+C	Open the Charms panel.	
Win+D	Show and hide the remote desktop.	
Win+E	Open File Explorer.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	
Win+K	Open the Devices charm.	
Win+M	Minimize all windows.	
Win+Q	To search everywhere or within the open app, if the app supports app search, open the Search charm.	
Win+R	Open the Run dialog box.	
Win+S	To search Windows and the Web, open the Search charm.	
Win+X	Open the **Quick Link** menu.	
Win+Z	Show the commands available in the app.	
Win+, (comma)	Temporarily show the remote desktop, as long as you continue pressing the keys.	Does not work on Windows 2012 R2 operating systems.
Win+Shift+M	Restore minimized windows on the remote desktop.	
Win+Home	Minimize all but the active remote desktop window (restores all windows when you press Win+Home a second time).	
Win+Enter	Open Narrator.	

Table 3-5. Windows Key Shortcuts for Windows 7 Remote Desktops

Keys	Action	Limitations
Win	Open or close the **Start** menu.	
Win+D	Show and hide the remote desktop.	
Win+M	Minimize all windows.	
Win+E	Open the `Computer` folder.	
Win+R	Open the Run dialog box.	
Win+Home	Minimize all but the active remote desktop window.	
Win+G	Cycle through running remote desktop gadgets.	
Win+U	Open the Ease of Access Center.	

Internationalization

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

Troubleshooting Horizon Client

4

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

This chapter includes the following topics:

- Restart a Remote Desktop
- Reset Remote Desktops or Published Applications
- Uninstall Horizon Client for Chrome
- Enable Log Collection

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.

For information about enabling the desktop restart feature, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

◆ Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the remote desktop session, and click **Restart**.

You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

Note A remote desktop session does not appear in the Session Management Center unless you connect to and then disconnect from the remote desktop.

Results

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

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 a published application quits the application without saving any unsaved data. You can reset all running published applications, or you can reset specific published application sessions.

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

For information about enabling the desktop reset feature, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

1   To reset all running published applications, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, scroll down to **Reset all your running applications**, and click **Reset**.

2   To reset a published application session, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the **Remote Apps** button for the application session, and click **Terminate**.

    You can also open the Session Management Center by right-clicking the published application icon in the shelf and clicking **Session Management Center**.

3   To reset a remote desktop, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the remote desktop session, and click **Reset**.

    You can also open the Session Management Center by right-clicking the published application icon in the shelf and clicking **Session Management Center**.

Results

When you reset a remote desktop, the operating system in the remote desktop restarts and Horizon Client disconnects and logs off 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.

Uninstall Horizon Client for Chrome

To uninstall the VMware Horizon Client for Chrome app, you remove it in the same way that you remove other Chromebook apps.

Procedure

1   Log in to the Chromebook.

2   Right-click the VMware Horizon Client app and select **Uninstall**.

What to do next

To reinstall the VMware Horizon Client for Chrome app, see Install or Upgrade Horizon Client for Chrome.

Enable Log Collection

When you enable log collection, Horizon Client collects log information that can help VMware troubleshoot problems with Horizon Client.

You cannot enable log collection after you connect to a remote desktop or published application.

Prerequisites

Connect to a server.

Procedure

1   Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window.

2   To enable log collection, turn on the **Enable Collect Log** option in the **Settings** window and select the **Basic**, **Debug**, or **Trace** log level.

The path to the log file appears under the **Enable Collect Log** option in the **Settings** window.

3   To change the log file path, click the default path, browse to and select a folder in which to save the log file, and click **Save**.

The new path appears under the **Enable Collect Log** option in the **Settings** window.

4   To close the **Settings** window, click **Close**.

Results

Horizon Client collects and saves logging information continuously until you quit Horizon Client.