Using VMware Horizon Client for Chrome OS

VMware Horizon Client for Chrome OS 4.2

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

Using VMware Horizon Client for Chrome OS

This guide, *Using VMware Horizon Client for Chrome OS*, provides information about installing and using VMware Horizon® Client™ software on a Chrome OS device to connect to a remote desktop or application in the data center.

The information in this document includes system requirements and instructions for installing and using Horizon Client for Chrome OS.

This information is written for administrators who already have some experience using View and VMware vSphere. If you are a novice user of View, you might occasionally need to refer to the step-by-step instructions for basic procedures in the *View Installation* document and the *View Administration* document.

Setup and Installation 1

Setting up a View deployment for Chrome OS clients involves using certain Connection Server configuration settings, meeting the system requirements for View servers and Chrome OS clients, and downloading and installing Horizon Client for Chrome OS.

Note In Horizon 7 and later, View Administrator is renamed Horizon Administrator. This document uses the name View Administrator to refer to both View Administrator and Horizon Administrator.

This chapter includes the following topics:

System Requirements

The device on which you install Horizon Client must meet certain system requirements.

Device models	Chromebook
Operating systems	Chrome OS, stable channel, ARC version 41.4410.244.13 or later
CPU architecture	■ ARM ■ x86
Connection Server, Security Server, and View Agent or Horizon Agent	Latest maintenance release of View 5.3.x and later releases. VMware recommends that you use a security server so that your device will not require a VPN connection. To use the Unity Touch feature with View 5.3.x desktops, the Remote Experience Agent must be installed on the desktops.

	Remote applications are available on Horizon 6.0 with View and later servers.
Display protocol for View	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later)

Preparing Connection Server for Horizon Client

Administrators must perform specific tasks to enable end users to connect to remote desktops and applications.

Before end users can connect to Connection Server or a security server and access a remote desktop or application, you must configure certain pool settings and security settings:

- If you plan to use Access Point, configure Connection Server to work with Access Point. See *Deploying and Configuring Access Point*. Access Point appliances fulfill the same role that was previously played by only security servers.
- If you are using a security server, verify that you are using the latest maintenance releases of Connection Server 5.3.x and Security Server 5.3.x or later releases. For more information, see the *View Installation* document.
- 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 Connection Server or a security server, verify that the client device can resolve this DNS name.

  To enable or disable the secure tunnel, in View Administrator, go to the Edit View Connection Server Settings dialog box and use the check box called **Use secure tunnel connection to desktop**.
- 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 Connection Server 5.3.x, see the topics about creating desktop pools in the *View Administration* document. For Connection Server 6.0 and later, see the topics about creating desktop and application pools in the *Setting Up Desktop and Application Pools in View* document.
- To use two-factor authentication with Horizon Client, such as RSA SecurID authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in the *View Administration* document.

Using Embedded RSA SecurID Software Tokens

If you create and distribute RSA SecurID software tokens to end users, they need enter only their PIN, rather than PIN and token code, to authenticate.

Setup Requirements

You can use Compressed Token Format (CTF) or dynamic seed provisioning, which is also called CT-KIP (Cryptographic Token Key Initialization Protocol), to set up an easy-to-use RSA authentication system. With this system, you generate a URL to send to end users. To install the token, end users paste this URL directly into Horizon Client on their client devices. The dialog box for pasting this URL appears when end users connect to Connection Server with Horizon Client.

After the software token is installed, end users enter a PIN to authenticate. With external RSA tokens, end users must enter a PIN and the token code generated by a hardware or software authentication token.

The following URL prefixes are supported if end users will be copying and pasting the URL into Horizon Client when Horizon Client is connected to an RSA-enabled Connection Server instance:

- `viewclient-securid://`

- `http://127.0.0.1/securid/`

End users can install the token by tapping the URL. Both prefixes `viewclient-securid://` and `http://127.0.0.1/securid/` are supported. Note that not all browsers support hyperlinks that begin with `http://127.0.0.1`. Also some file browsers, such as the File Manager app on the ASUS Transformer Pad, cannot link the SDTID file with Horizon Client.

For information about using dynamic seed provisioning or file-based (CTF) provisioning, see the Web page *RSA SecurID Software Token for iPhone Devices* at http://www.rsa.com/node.aspx?id=3652 or *RSA SecurID Software Token for Android* at http://www.rsa.com/node.aspx?id=3832.

Instructions to End Users

When you create a CTFString URL or CT-KIP URL to send to end users, you can generate a URL with or without a password or activation code. You send this URL to end users in an email that must include the following information:

- Instructions for navigating to the Install Software Token dialog box.

  Tell end users to tap **External Token** in the Horizon Client dialog box that prompts them for RSA SecurID credentials when they connect to a Connection Server instance.

- CTFString URL or CT-KIP URL in plain text.

  If the URL has formatting on it, end users will get an error message when they try to use it in Horizon Client.

- Activation code, if the CT-KIP URL that you create does not already include the activation code.

  End users must enter this activation code in a text field of the dialog box.

- If the CT-KIP URL includes an activation code, tell end users that they need not enter anything in the **Password or Activation Code** text box in the Install Software Token dialog box.

Configure Advanced TLS/SSL Options

You can select the security protocols and cryptographic algorithms that are used to encrypt communications between Horizon Client and Horizon servers and between Horizon Client and the agent in the remote desktop.

By default, TLSv1.0, TLSv1.1, and TLSv1.2 are enabled. SSL v2.0 and 3.0 are not supported. The default cipher control string is "!aNULL:kECDH+AESGCM: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 Horizon server to which the client connects, a TLS/SSL error occurs and the connection fails.

For information about configuring the security protocols that are accepted by Connection Server instances, see the *View Security* document.

Procedure

1. Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client screen and tap **Security options**.
2. Tap **Advanced SSL Options**.
3. Make sure that **Use Default Settings** is unchecked.
4. To enable or disable a security protocol, tap the check box next to the security protocol name.
5. To change the cipher control string, replace the default string.
6. (Optional) If you need to revert to the default settings, tap to select the **Use Default Settings** option.

7 Tap **OK** to save your changes.

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

Supported Desktop Operating Systems

Administrators create virtual machines with a guest operating system and install agent software in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported Windows guest operating systems, see the "Supported Operating Systems for View Agent" topic in the View 5.x or 6.x installation documentation. See the "Supported Operating Systems for Horizon Agent" topic in the Horizon 7 installation documentation.

Install or Upgrade Horizon Client for Chrome OS

Horizon Client for Chrome OS is a Chrome OS app, and you install it just as you do other Chrome OS apps.

Prerequisites

If you have not already set up the Chrome OS device, do so. See the manufacturer's user's guide for your device.

Procedure

1 Search for the Horizon Client for Chrome OS app in the Chrome Web Store.

2 Download and install the app.

3 To determine that the installation succeeded, verify that the **Horizon Client for Chrome OS** app icon appears in the Chrome App Launcher.

Selecting a Folder the First Time You Launch Horizon Client

The first time you launch Horizon Client, it prompts you to select and open a folder. You can select an existing folder or create a new folder. You can also select a removable storage device, such as USB thumb drive.

Horizon Client uses the folder you select to share local files with remote desktops and applications. This feature is called client drive redirection.

For complete information about the client drive redirection feature, including system requirements, see "Share Access to Local Storage," on page 18.

You can change the client drive redirection folder at a later time. See "Change the Folder for Client Drive Redirection," on page 18.

Configure Decoding for VMware Blast Sessions

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

Prerequisites

This feature requires Horizon Agent 7.0 or later.

Procedure

1 Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client screen and tap **VMware Blast**.

2 Select the **H.264** check box to allow H.264 decoding, or deselect the **H.264** check box to disable H.264 decoding.

When the check box is selected, Horizon Client uses H.264 decoding if the agent supports H.264 software encoding. If the agent does not support H.264 software encoding, Horizon Client uses JPG/PNG decoding. When the check box is not selected, Horizon Client always use JPG/PNG decoding.

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

Configure the Horizon Client Default View

You can configure whether the Recent screen or the Servers screen appears when you launch Horizon Client.

Procedure

1 Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client screen and tap **Display**.

2 Tap **Default launch view**.

3 Tap an option to select the default view.

Option	Description
Recent	The Recent screen appears when you launch Horizon Client. The Recent screen contains shortcuts to recently used desktops and applications. This is the default setting.
Servers	The Servers screen appears when you launch Horizon Client. The Servers screen contains shortcuts to the servers that you added to Horizon Client.

The default view you selected takes effect immediately.

Horizon Client Data Collected by VMware

If your company participates in the customer experience improvement program, VMware collects data from certain Horizon Client fields. Fields containing sensitive information are made anonymous.

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

The administrator who installs Connection Server can select whether to participate in the VMware customer experience improvement program while running the Connection Server installation wizard, or an administrator can set an option in View Administrator after the installation.

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

Description	Is This Field Made Anonymous?	Example Value
Company that produced the Horizon Client application	No	VMware
Product name	No	VMware Horizon Client
Client product version	No	(The format is *x.x.x-yyyyyy*, where *x.x.x* is the client version number and *yyyyyy* is the build number.)

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

Description	Is This Field Made Anonymous ?	Example Value
Client binary architecture	No	Examples include the following: ■ i386 ■ x86_64 ■ arm
Client build name	No	Examples include the following: ■ VMware-Horizon-Client-Win32-Windows ■ VMware-Horizon-Client-Linux ■ VMware-Horizon-Client-iOS ■ VMware-Horizon-Client-Mac ■ VMware-Horizon-Client-Android ■ VMware-Horizon-Client-WinStore
Host operating system	No	Examples include the following: ■ Windows 8.1 ■ Windows 7, 64-bit Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host operating system kernel	No	Examples include the following: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unknown (for Windows Store)
Host operating system architecture	No	Examples include the following: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Host system model	No	Examples include the following: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision WorkStation T3400 (A04 03/21/2008)
Host system CPU	No	Examples include the following: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (for iPad)
Number of cores in the host system's processor	No	For example: 4
MB of memory on the host system	No	Examples include the following: ■ 4096 ■ unknown (for Windows Store)
Number of USB devices connected	No	2 (USB device redirection is supported only for Linux, Windows, and Mac OS X clients.)

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

Description	Is This Field Made Anonymous?	Example Value
Maximum concurrent USB device connections	No	2
USB device vendor ID	No	Examples include the following: ■ Kingston ■ NEC ■ Nokia ■ Wacom
USB device product ID	No	Examples include the following: ■ DataTraveler ■ Gamepad ■ Storage Drive ■ Wireless Mouse
USB device family	No	Examples include the following: ■ Security ■ Human Interface Device ■ Imaging
USB device usage count	No	(Number of times the device was shared)

Managing Remote Desktop and Application Connections 2

Use Horizon Client to connect to a server, edit the list of servers you connect to, log in to or off of remote desktops, and use remote applications. For troubleshooting purposes, you can also reset remote desktops and applications.

Depending on how the administrator configures policies for remote desktops, end users might be able to perform many operations on their desktops.

This chapter includes the following topics:

Connect to a Remote Desktop or Application

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

Prerequisites

- Obtain credentials to log in, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- Perform the administrative tasks described in "Preparing Connection Server for Horizon Client," on page 8.
- If you are outside the corporate network and are not using a security server to access the remote desktop, verify that your client device is set up to use a VPN connection and turn on that connection.

  Important VMware recommends using a security server rather than a VPN.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or application. Underscores (_) are not supported in server names. You also need the port number if the port is not 443.

- If you plan to use embedded RSA SecurID software, verify that you have the correct CT-KIP URL and activation code. See "Using Embedded RSA SecurID Software Tokens," on page 8.
- Configure the certificate checking mode for the SSL certificate presented by View Connection Server. See "Setting the Certificate Checking Mode for Horizon Client," on page 17.

Procedure

1 On your Chrome OS device, tap the **Chrome App Launcher** icon in the taskbar and tap the **Horizon Client for Chrome OS** app.

The Horizon Client window opens.

2 Connect to a server.

Option	Action
Connect to a new server	Type the name of a server, type a description (optional), and tap **Connect**. For example: `view.company.com` The default port for SSL connections is 443. If the sever is not configured to use the default port, use the format shown in this example: `view.company.com:1443`.
Connect to a existing server	Tap the server shortcut on the **Servers** tab.

Connections between Horizon Client and a View server always use SSL.

3 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, either type your credentials or, if you plan to use an embedded RSA SecurID token, install an embedded token.

Option	Action
Existing token	If you use a hardware authentication token or software authentication token on a smart phone, enter your user name and passcode. The passcode might include both a PIN and the generated number on the token.
Install software token	Click **External Token**. In the Install Software Token dialog box, paste the CT-KIP URL or CTFString URL that your administrator sent to you in email. If the URL contains an activation code, you do not need to enter anything in the **Password or Activation Code** text box.

4 If you are prompted a second time for RSA SecurID credentials 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 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.

5 In the login dialog box, type your user name and password, select a domain, and tap **Connect**.

6 (Optional) Tap the display protocol settings icon in the upper-right corner of the screen to select the display protocol to use.

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

7 Tap a remote desktop or application icon to connect to it.

After you connect to a remote desktop or application for the first time, a shortcut for the desktop or application is saved to the **Recent** tab. The next time you want to connect to the remote desktop or application, you can tap this shortcut.

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

- Determine whether Connection Server is configured not to use SSL. Horizon Client requires SSL connections. Check whether the global setting in View Administrator for the **Use SSL for client connections** check box is deselected. If so, you must either select the check box, so that SSL is used, or set up your environment so that clients can connect to an HTTPS enabled load balancer or other intermediate device that is configured to make an HTTP connection to Connection Server.
- Verify that the security certificate for Connection Server is working properly. If it is not, in View Administrator, you might also see that the agent on desktops is unreachable.
- Verify that the tags set on the Connection Server instance allow connections from this user. See the *View Administration* document.
- Verify that the user is entitled to access the desktop or application. See the *Setting Up Desktop and Application Pools in View* document.

Setting the Certificate Checking Mode for Horizon Client

Administrators and sometimes end users can configure whether client connections are rejected if any or some server certificate checks fail.

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

- 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.

Note For information about distributing a self-signed root certificate that users can install on their Chrome OS devices, as well as instructions for installing a certificate on a Chrome OS device, see the documentation on the Google Web site.

To set the security mode, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client screen, tap **Security options**, and tap **Security mode**. You have three choices:

- **Never connect to untrusted servers**. If any of the certificate checks fails, the client cannot connect to the server. An error message lists the checks that failed.
- **Warn before connecting to untrusted servers**. If a certificate check fails because the server uses a self-signed certificate, you can click **Continue** to ignore the warning. For self-signed certificates, the certificate name is not required to match the server name you entered in Horizon Client.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

If the certificate checking mode is set to **Warn**, you can still connect to a Connection Server instance that uses a self-signed certificate.

If an administrator later installs a security certificate from a trusted certificate authority, so that 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.

Share Access to Local Storage

You can configure Horizon Client to share local storage with a remote desktop or application. This feature is called client drive redirection.

In a Windows remote desktop or remote application, local storage appears as **sdcard on HorizonClient** in the **Devices and drives** section in the **This PC** folder or in the **Other** section in the **Computer** folder.

The first time you launch Horizon Client, it prompts you to select a folder to use with the client drive redirection feature. You can change this folder at a later time. See "Change the Folder for Client Drive Redirection," on page 18.

Prerequisites

- Enable the client drive redirection feature. This task includes installing View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, and enabling the agent **Client Drive Redirection** option. It can also include setting policies or registry settings to control client drive redirection behavior. For more information, see *Setting Up Desktop and Application Pools in View*.
- Connect to the remote desktop or application with which you want to share local storage. If you have not logged in at least once, become familiar with the procedure "Connect to a Remote Desktop or Application," on page 15.

Procedure

1 Open the Unity Touch sidebar, tap the **Settings** (gear) icon, and tap **Local storage redirection**.

2 Select the **Local Storage Redirection** check box to share local storage with the remote desktop or application, or deselect the **Local Storage Redirection** check box to stop sharing local storage with the remote desktop or application.

What to do next

Verify your changes from within the remote desktop or application.

- From within a Windows remote desktop, open the **This PC** folder and look in the **Devices and drives** section, or open the **Computer** folder and look in the **Other** section. If you enabled the **Local Storage Redirection** setting, you should see **sdcard on HorizonClient**.
- From a remote application, select **File > Open** or **File > Save As**, if applicable. If you enabled the **Local Storage Redirection** setting, you should be able to navigate to **sdcard on HorizonClient**.

Change the Folder for Client Drive Redirection

The first time you launch Horizon Client, Horizon Client prompts you to select a folder to use with the client drive redirection feature. You can change this folder in Horizon Client.

NOTE Horizon Client creates a folder named `Android` in the folder you select to use with the client drive redirection feature.

Procedure

1 Tap the folder icon in the upper-left corner of the Horizon Client screen.

2 When the Select a folder to open dialog box appears, select a folder and tap **Open**.

You can select an existing folder or create a new folder. You can also select a removable storage device, such as a USB thumb drive.

What to do next

Connect to a remote desktop or application and verify your changes from within the remote desktop or application.

- From within a Windows remote desktop, open the **This PC** folder and look in the **Devices and drives** section, or open the **Computer** folder and look in the **Other** section. The folder you selected is named **sdcard on HorizonClient**.
- From within a remote application, select **File > Open** or **File > Save As**, if applicable. You should be able to navigate to **sdcard on HorizonClient**.

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 On the **Servers** tab, tap and hold the server shortcut until the context menu appears.

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

3 If you edited the server shortcut, tap **Done** to save your changes.

Select a Favorite Remote Desktop or Application

You can select remote desktops and applications as favorites. Favorites are identified by a star. The star helps you quickly find your favorite desktops and applications. Your favorite selections are saved, even after you log off from the server.

Prerequisites

Obtain the credentials you need to connect to the server, such as a user name and password or RSA SecurID and passcode.

Procedure

1 On the **Servers** tab, tap the server shortcut.

2 If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 Perform these steps to select or deselect a desktop or application as a favorite.

Option	Description
Select a favorite	On the **All** tab, tap and hold the desktop or application name until the context menu appears and tap **Mark as Favorite**. A star appears in the upper right corner of the name and the name appears on the **Favorites** tab.
Deselect a favorite	On the **All** or **Favorites** tab, tap and hold the desktop or application name until the context menu appears and tap **Unmark Favorite**. A star no longer appears in the upper right corner of the name and the name disappears from the **Favorites** tab.

4 To display only favorite desktops or applications, tap the **Favorites** tab.

You can tap the **All** tab to display all the available desktops and applications.

Disconnecting From a Remote Desktop or Application

You can disconnect from a remote desktop without logging off, so that applications remain open on the remote desktop. You can also disconnect from a remote application so that the remote application remains open.

When you are connected to the remote desktop or application, you can disconnect by tapping the **Disconnect** icon in the Unity Touch sidebar.

NOTE A View administrator can configure your desktop to automatically log off when disconnected. In that case, any open programs in your desktop are stopped.

Log Off from a Remote Desktop

You can log off from a remote desktop operating system, even if you do not have a desktop open in Horizon Client.

If you are currently connected to and logged in to a remote desktop, you can use the Windows **Start** menu to log off. After Windows logs you off, the desktop is disconnected.

NOTE Any unsaved files that are open on the remote desktop are closed during the logoff operation.

Prerequisites

- Obtain the credentials that you need to log in, such as Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- If you have not logged in at least once, become familiar with the procedure "Connect to a Remote Desktop or Application," on page 15.

Procedure

1 On the **Servers** tab, tap the server shortcut.

2 If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.

3 On the **All** tab, tap and hold the desktop shortcut until the context menu appears.

If the desktop is a favorite, you can also perform this step on the **Favorites** tab.

4 Tap **Log Off** in the context menu.

What to do next

Tap the back arrow in the upper-left corner of the Horizon Client screen, or the **Disconnect** icon in the upper-right corner of the Horizon Client screen, and tap **Log Out** to disconnect from the server.

Manage Desktop and Application Shortcuts

After you connect to a remote desktop or application, Horizon Client saves a shortcut for the recently used desktop or application. You can rearrange and remove these shortcuts.

Procedure

- Perform these steps to remove a desktop or application shortcut from the **Recent** tab.
  a Tap and hold the shortcut until **Remove Shortcut** appears at the bottom of the screen.
  b Drag the shortcut to **Remove Shortcut**.
- To move a desktop or application shortcut, drag and drop it to the new location.

Using a Remote Desktop or Application on a Chrome OS Device

3

On Chrome OS devices, Horizon Client includes additional features to aid in navigation.

This chapter includes the following topics:

Feature Support Matrix

When you access a remote desktop from Horizon Client for Chrome OS, some features are not available.

Table 3-1. Features Supported on Windows Desktops for Chrome OS Horizon Clients

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows XP Desktop	Windows Vista Desktop	Windows Server 2008/2012 R2 or Windows Server 2016 Desktop
RSA SecurID or RADIUS	X	X	X	Limited	Limited	X
Single sign-on	X	X	X	Limited	Limited	X
RDP display protocol						
PCoIP display protocol	X	X	X	Limited	Limited	X
VMware Blast display protocol	X	X	X			X
USB access						
Real-time audio-video (RTAV)						
Wyse MMR						

Table 3-1. Features Supported on Windows Desktops for Chrome OS Horizon Clients (Continued)

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows XP Desktop	Windows Vista Desktop	Windows Server 2008/2012 R2 or Windows Server 2016 Desktop
Windows 7 MMR						
Virtual printing						
Location-based printing	X	X	X	Limited	Limited	X
Smart cards						
Multiple monitors						

Windows 10 desktops require View Agent 6.2 or later or Horizon Agent 7.0 or later. Windows Server 2012 R2 desktops require View Agent 6.1 or later. Windows Server 2016 desktops require Horizon Agent 7.0.2 or later.

Important View Agent 6.1 and later and Horizon Agent 7.0 and later releases do not support Windows XP and Windows Vista desktops. View Agent 6.0.2 is the last View release that supports these guest operating systems. Customers who have an extended support agreement with Microsoft for Windows XP and Vista, and an extended support agreement with VMware for these guest operating systems, can deploy the View Agent 6.0.2 version of their Windows XP and Vista desktops with View Connection Server 6.1.

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

Feature Support for Session-Based Desktops on RDS Hosts

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

Note The following table contains rows only for the features that are supported. Where the text specifies a minimum version of View Agent, the text "and later" is meant to include Horizon Agent 7.0.x and later.

Table 3-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0.x or Later, Installed

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 RDS Host	Windows Server 2016 RDS Host
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later
PCoIP display protocol	X	X	Horizon Agent 7.0.2 and later
VMware Blast display protocol	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0.2 and later
HTML Access	View Agent 6.0.2 and later (virtual machine only)	View Agent 6.0.2 and later (virtual machine only)	Horizon Agent 7.0.2 and later
Client drive redirection	View Agent 6.1.1 and later	View Agent 6.1.1 and later	Horizon Agent 7.0.2 and later
Virtual printing (for desktop clients)	View Agent 6.0.1 and later (virtual machine only)	View Agent 6.0.1 and later (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)

Table 3-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0.x or Later, Installed (Continued)

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 RDS Host	Windows Server 2016 RDS Host
Location-based printing	View Agent 6.0.1 and later (virtual machine only)	View Agent 6.0.1 and later (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)
Multiple monitors (for desktop clients)	X	X	Horizon Agent 7.0.2 and later
Unity Touch (for mobile and Chrome OS clients)	X	X	Horizon Agent 7.0.2 and later

For information about which editions of each guest operating system are supported, or which service packs, see the "Supported Operating Systems for View Agent" topic in the View 5.x or 6.x installation documentation. See the "Supported Operating Systems for Horizon Agent" topic in the Horizon 7 installation documentation.

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 your Chrome OS device 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 your Chrome OS device has a touch screen, tap with two fingers at nearly the same time. The right-click occurs where the first finger tapped.

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 your Chrome OS device has a touch screen, tap with one or two fingers and then drag to scroll. The text under your fingers moves in the same direction as your fingers. Scrolling with one finger does not work if you have zoomed in or when the onscreen keyboard is displayed.

Zooming In and Out

As in other apps, use your keyboard and press Ctrl and + to zoom in and Ctrl and - to zoom out. If your Chrome OS device has a touch screen, you can pinch your fingers apart to zoom out and pinch your fingers together to zoom in.

Window Resizing

To use your touchpad to resize a window, touch and hold one finger at the corner or side of the window and drag to resize. If your Chrome OS device 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. You cannot resize the window if it is maximized.

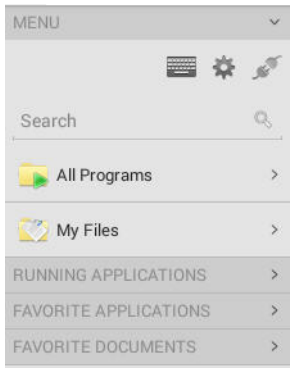
Sound, Music, and Video

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

Using the Unity Touch Sidebar with a Remote Desktop

You can quickly navigate to a remote desktop application or file from a Unity Touch sidebar. From this sidebar, you can open files and applications, switch between running applications, and minimize, maximize, restore, or close windows and applications in a remote desktop.

Figure 3-1. Unity Touch Sidebar for a Remote Desktop



From this sidebar, you can perform many actions on a file or application.

Table 3-3. Unity Touch Sidebar Actions for a Remote Desktop

Action	Procedure
Show or hide the onscreen keyboard	Tap the **Keyboard** icon.
Change Horizon Client settings	Tap the **Settings** icon.
Disconnect from the desktop	Tap the **Disconnect** icon.
Show the sidebar	Drag the sidebar to the right or tap the sidebar tab.
Hide the sidebar	Drag the sidebar to the left or tap in the desktop area.
Navigate to an application	Tap **All Programs** and navigate to the application just as you would from the Windows Start menu.
Navigate to a file	Tap **My Files** to access the `User` folder, and navigate to the file. **My Files** includes folders such as `My Pictures`, `My Documents`, and `Downloads`. **My Files** includes the folders in the user profile (`%USERPROFILE%` directory). If you relocate the `system` folder in the `%USERPROFILE%` directory, the **My Files** menu can also display content from the relocated folder, whether it is a local relocated folder or a network share folder.
Search for an application or file	■ Tap in the **Search** box and type the name of the application or file. ■ To use voice dictation, tap the microphone on the keyboard. ■ To launch an application or file, tap the name of the application or file in the search results. ■ To return to the home view of the sidebar, tap the **X** to close the **Search** box.

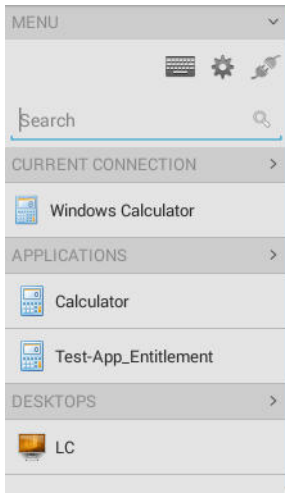
Table 3-3. Unity Touch Sidebar Actions for a Remote Desktop (Continued)

Action	Procedure
Open an application or file	Tap the name of the file or application in the sidebar. The application starts and the sidebar closes.
Switch between running applications or open windows	Tap the application name under **Running Applications**. If more than one file is open for one application, tap the chevron (>) next to the application to expand the list.
Minimize a running application or window	Tap and hold the application name under **Running Applications** until the context menu appears. Tap **Minimize**.
Maximize a running application or window	Tap and hold the application name under **Running Applications** until the context menu appears. Tap **Maximize**.
Close a running application or window	Tap and hold the application name under **Running Applications** until the context menu appears. Tap **Close**.
Restore a running application or window to its previous size and position	Tap and hold the application name under **Running Applications** until the context menu appears. Tap **Restore**.
Create a list of favorite applications or files	1 Search for the application or file, or tap **Manage** under the **Favorite Applications** or **Favorite Documents** list. If the **Manage** bar is not visible, tap the chevron (>) next to **Favorite Applications** or **Favorite Files**. 2 Tap the check box next to the names of your favorites in the search results or in the list of available applications or files. The favorite that you add last appears at the top of your favorites list.
Remove an application or file from the favorites list	1 Search for the application or file, or tap **Manage** under the **Favorite Applications** or **Favorite Dcuments** list. If the **Manage** bar is not visible, tap the chevron (>) next to **Favorite Applications** or **Favorite Documents**. 2 Tap to remove the check mark next to the name of the application or file in the favorites list.
Reorder an application or file in the favorites list	1 Tap **Manage** under the **Favorite Applications** or **Favorite Documents** list. If the **Manage** bar is not visible, tap the chevron (>) next to **Favorite Applications** or **Favorite Documents**. 2 In the favorites list, touch and hold the handle on the left side of the application or file name and drag the favorite up or down the list.

Using the Unity Touch Sidebar with a Remote Application

You can quickly navigate to a remote application from a Unity Touch sidebar. From this sidebar, you can launch applications, switch between running applications, and minimize, maximize, restore, or close remote applications. You can also switch to a remote desktop.

Figure 3-2. Unity Touch Sidebar for a Remote Application



From the Unity Touch sidebar, you can perform many actions on a remote application.

Table 3-4. Unity Touch Sidebar Actions for a Remote Application

Action	Procedure
Show or hide the onscreen keyboard	Tap the **Keyboard** icon.
Modify Horizon Client settings	Tap the **Settings** icon.
Disconnect from the application	Tap the **Disconnect** icon.
Show the sidebar	Drag the sidebar to the right or tap the sidebar tab. When the sidebar is open, you cannot perform actions on the application screen.
Hide the sidebar	Drag the sidebar to the left or tap in the application area. When the sidebar is open, you cannot perform actions on the application screen.
Switch between running applications	Tap the application under **Current Connection**.
Open an application	Tap the name of the application under **Applications** in the sidebar. The application starts and the sidebar closes.
Close a running application	1 Tap and hold the application name under **Current Connection** until the context menu appears. 2 Tap **Close**.
Minimize a running application	1 Tap and hold the application name under **Current Connection** until the context menu appears. 2 Tap **Minimize**.
Maximize a running application	1 Tap and hold the application name under **Current Connection** until the context menu appears. 2 Tap **Maximize**.

Table 3-4. Unity Touch Sidebar Actions for a Remote Application (Continued)

Action	Procedure
Restore a running application	1 Tap and hold the application name under **Current Connection** until the context menu appears. 2 Tap **Restore**.
Switch to a remote desktop	Tap the desktop name under **Desktops**.

Using the Onscreen Keyboard

You can use an onscreen keyboard in a remote desktop or application. To display the onscreen keyboard, tap the **Keyboard** icon in the Unity Touch sidebar. To hide the onscreen keyboard, tap the **Keyboard** icon again.

The onscreen keyboard includes the PageUp and PageDn navigation keys, function keys, and other keys that you often use in Windows environments, including Ctrl, Alt, Del, Shift, Win, Caps, Esc, and Del. Use the Shift key on this keypad when you need to use key combinations that include the Shift key, such as Ctrl +Shift. To tap a combination of these keys, such as Ctrl+Alt+Shift, first tap the onscreen Ctrl key. After the Ctrl key turns blue, tap the onscreen Alt key. After the Alt key turns blue, tap the onscreen Shift key. A single onscreen key is provided for the key combination Ctrl+Alt+Del.

You can tap the pen icon on the left side of the Ctrl key to display the local input buffer. Text that you type into this text box is not sent to an application until you tap **Send.** For example, if you open an application such as Notepad and tap the pen icon, the text that you type does not appear in the Notepad application until you tap **Send**. This feature is useful if you have a poor network connection and characters do not immediately appear when you type them. With this feature, you can quickly type up to 1,000 characters and then either tap **Send** or **Return** to have all 1,000 characters appear at once in the application.

Screen Resolutions and Using External Displays

You can use Horizon Client with external displays and you can change screen resolutions.

When you connect your Chrome OS device to an external display or projector, you can display Horizon Client in full-screen mode by pressing the full screen key on your device's keyboard.

Enlarging the Screen Resolution for a Remote Desktop

By default, the display resolution is set so that the entire Windows desktop fits inside your device, and the desktop icons and task bar icons are a certain size. If you change the default to a higher resolution, the desktop still fits inside the device, but the desktop and taskbar icons become smaller.

Changing the Display Resolution Setting

To change the resolution setting, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client screen, tap **Display**, and tap **Resolution**.

Using Projectors

You can use the **Resolution** setting to set a larger resolution for projectors.

Saving Documents in a Remote Application

With certain remote applications, such as Microsoft Word or WordPad, you can create and save documents. Where these documents are saved depends on your company's network environment. For example, your documents might be saved to a home share mounted on your local computer.

Administrators can use an ADMX template file to set a group policy that specifies where documents are saved. This policy is called "Set Remote Desktop Services User Home Directory." For more information, see the "RDS Profiles Settings" topic in the *Setting Up Desktop and Application Pools in View* document.

Internationalization

Both the user interface and the 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 resetting the desktop or reinstalling the app.

This chapter includes the following topics:

Reset a Remote Desktop or Application

Resetting a remote desktop shuts down and restarts the desktop. Resetting a remote application quits the application. You might need to reset a desktop or application if the desktop operating system or application stops responding.

Resetting a remote desktop is the equivalent of pressing the **Reset** button on a physical PC to force the PC to restart. Any files that are open on the remote desktop will be closed without being saved first.

Resetting a remote application quits all remote applications and logs off all of your remote application sessions. Unsaved changes in remote applications might be lost.

NOTE A View administrator can disable the reset feature for certain types of desktops. For more information, see the *View Administration* document.

Prerequisites

- Obtain credentials to log in, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- If you have not logged in at least once, become familiar with the procedure "Connect to a Remote Desktop or Application," on page 15.

Procedure

1. On the **Servers** tab, tap the server shortcut.
2. If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.
3. On the **All** tab, tap and hold the desktop or application shortcut until the context menu appears.

   If the desktop or application is a favorite, you can also perform this step on the **Favorites** tab.

4 Tap **Reset** in the context menu.

Reset is available only if the status of the desktop or application is such that the action can be taken.

Uninstall Horizon Client

You can sometimes resolve problems with Horizon Client by uninstalling and reinstalling Horizon Client for Chrome OS.

You uninstall Horizon Client for Chrome OS just as you would any Chrome OS app.

Procedure

- On your Chrome OS device, tap the App Launcher icon in the taskbar, right-click the **Horizon Client for Chrome OS** app icon, and select **Uninstall**.

What to do next

Reinstall Horizon Client.

See "Install or Upgrade Horizon Client for Chrome OS," on page 10.

Horizon Client Stops Responding or the Remote Desktop Freezes

When the screen freezes, first, try resetting the remote desktop operating system.

Problem

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

Cause

Assuming that View servers are configured properly and that firewalls surrounding them have the correct ports open, other issues usually relate to Horizon Client on the device or to the guest operating system on the remote desktop.

Solution

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

  This option is available only if the View administrator has enabled this feature.
- Uninstall and reinstall the app on the device.
- If resetting the remote desktop and reinstalling Horizon Client do not help, you can reset the Chrome OS device, as described in the device user guide.
- If you get a connection error when you attempt to connect to the server, you might need to change your proxy settings.

Problem Establishing a Connection When Using a Proxy

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

Problem

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

Cause

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

Solution

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

Index

U