Using VMware Horizon Client for iOS

VMware Horizon Client for iOS 4.1

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 iOS

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

The information in this document includes system requirements and instructions for installing Horizon Client. This document also provides tips for improving the user experience of navigating and using Windows desktop elements on an iOS device such as an iPad.

This information is intended for administrators who need to set up a View deployment that includes iOS client devices. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

Setup and Installation 1

Setting up a View deployment for iOS clients involves using certain Connection Server configuration settings, meeting the system requirements for View servers and iOS clients, and installing the app for Horizon Client from the Apple App Store. VMware also recommends that you set up a security server so that your iOS clients will not need a VPN connection.

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

You can install Horizon Client on all models of iPad and iPhone.

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

iPad and iPhone models

- iPhone 4, 4s, 5, 5s, 5c, 6, 6 Plus, 6s, 6s Plus, and SE

	■ iPad 2, iPad (3rd generation), iPad (4th generation), iPad mini, iPad mini 3, iPad mini 4, iPad mini with Retina display, iPad Air, iPad Air 2, and iPad Pro Horizon Client includes 64-bit processor support for iPhone 5s, 6, 6 Plus, 6s, 6s Plus, and SE, and iPad Air, iPad Air 2, iPad mini 2, iPad mini 3, iPad mini 4, and iPad Pro.
Operating systems	iOS 8.4.1 and later, including iOS 9.x
External keyboards	(Optional) iPad Keyboard Dock and Apple Wireless Keyboard (Bluetooth)
Smart card authentication	See "Smart Card Authentication Requirements," on page 9.
Touch ID authentication	See "Touch ID Authentication Requirements," on page 10.
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 iOS clients 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)
Network protocol for View	■ IPv4 ■ IPv6 (requires an iOS 9.2 or later client system) For information about using View in an IPv6 environment, see the *View Installation* document.

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard audio devices and with standard conferencing applications such as Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your View deployment must meet certain software and hardware requirements.

Important Only the audio-in feature is supported. The video feature is not supported.

View remote desktop	The desktops must have View Agent 5.3 or later installed. For View Agent 5.3 desktops, the desktops must also have the corresponding Remote Experience Agent installed. For example, if View Agent 5.3 is installed, you must also install the Remote Experience Agent from View 5.3 Feature Pack 1. See the *View Feature Pack Installation and Administration* document for View. If you have View Agent 6.0 or later, or Horizon Agent 7.0 or later, no feature pack is required.

	Real-Time Audio-Video is not supported in RDS desktop sessions or remote applications.
Client access device	Real-Time Audio-Video is supported on all iOS devices that run Horizon Client for iOS. For more information, see "System Requirements," on page 7.

Smart Card Authentication Requirements

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

Horizon Client for iOS supports using smart cards with remote desktops that have Windows 7, Windows Vista, Windows XP, Windows 8.1, Windows 10, and Windows Server 2008 R2 guest operating systems. For Microsoft RDS host-based desktops and applications, the Windows Server 2008 R2 and Windows Server 2012 R2 operating systems are supported. An iOS 8.4.1 or later operating system is required.

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

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

You must also install product-specific application drivers on the remote desktops or Microsoft RDS host.

Users that authenticate with smart cards must have a smart card and each smart card must contain a user certificate.

In addition to meeting these requirements for Horizon Client systems, other View components must meet certain configuration requirements to support smart cards:

- For information about configuring Connection Server to support smart card use, see "Configure Smart Card Authentication" in the *View Administration* document.

  You must add all applicable Certificate Authority (CA) certificates for all trusted user certificates to a server truststore file on the Connection Server host or security server host. These certificates include root certificates and must include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.
- For information about tasks you might need to perform in Active Directory to implement smart card authentication, see the topics about preparing Active Directory for smart card authentication in the *View Installation* document.

Configure Smart Card Authentication

Configuration tasks include connecting and pairing the card reader with the device and setting the smart card removal policy.

Prerequisites

- Verify that you are using the correct version of the client, desktop agent, server, operating system, smart card reader, and smart card. See "Smart Card Authentication Requirements," on page 9.
- If you have not already done so, perform the tasks described in "Prepare Active Directory for Smart Card Authentication," in the *View Installation* document.
- Configure View servers to support smart card use. See the topic "Configure Smart Card Authentication," in the *View Administration* document.

Procedure

1 Pair the device with the smart card reader, according to the documentation provided by the manufacturer of the reader.

If your iOS device has a 30-pin connector, you can plug the smart card reader into the connector. For iPad Air and iPhone 5S, which have Lightning interfaces, you must use a 30-pin adapter to plug the smart card reader into the device's 30-pin connector.

2 Configure the smart card removal policy.

Option	Description
Set the policy on the server	If you use View Administrator to set a policy, the choices are to disconnect users from Connection Server when they remove their smart cards or to keep users connected to Connection Server when they remove their smart cards and let them start new desktop or application sessions without reauthenticating. a In View Administrator, select **View Configuration > Servers**. b On the **Connection Servers** tab, select the Connection Server instance and click **Edit**. c On the **Authentication** tab, select or deselect the **Disconnect user sessions on smart card removal** check box to configure the smart card removal policy. d Click **OK** to save your changes. e Restart the Connection Server service to make your changes take effect. If you select the **Disconnect user sessions on smart card removal** check box, Horizon Client returns to the **Recent** screen when users remove their smart cards.
Set the policy on the desktop	If you use the Group Policy Editor (`gpedit.msc`), you have the following possible settings: no action, lock workstation, force log off, or Disconnect if a Remote Desktop Services session. After you open `gpedit.msc` in the desktop operating system, go to **Windows settings > Security settings > Local policies > Security options > Interactive logon: smart card removal behavior**. Run the `gpupdate /force` command after you change the configuration to force a group policy refresh.

Touch ID Authentication Requirements

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

iPad and iPhone models	Any iPad or iPhone model that supports Touch ID, for example, iPad Air 2 and iPhone 6.
Operating system requirements	■ iOS 8 or later. ■ Add at least one fingerprint in the Touch ID & Passcode setting.
Connection Server requirements	■ Horizon 6 version 6.2 or a later release. ■ Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the *View Administration* document.

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

Horizon Client requirements

- Set the certificate checking mode to **Never connect to untrusted servers** or **Warn before connecting to untrusted servers**. For information about setting the certificate checking mode, see "Certificate Checking Modes for Horizon Client," on page 25.
- Enable Touch ID by tapping **Enable Touch ID** on the View server login screen. After you successfully log in, your Active Directory credentials are stored securely in the iOS device's Keychain. The **Enable Touch ID** option is shown the first time you log in and does not appear after Touch ID is enabled.

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

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.

Some Linux guest operating systems are also supported if you have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later. For information about system requirements, configuring Linux virtual machines for use in Horizon 6 or Horizon 7, and a list of supported features, see *Setting Up Horizon 6 for Linux Desktops*, which is part of the Horizon 6, version 6.1 documentation, or see *Setting Up Horizon 7 for Linux Desktops*.

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, which is available with Horizon 6 version 6.2 or later, 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. 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 or RADIUS authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in the *View Administration* document.
- To use Touch ID authentication, you must enable biometric authentication in Connection Server. Biometric authentication is supported in Horizon 6 version 6.2 and later. For more information, see "Configure Biometric Authentication" in the *View Administration* document.
- To enable end users to save their passwords with Horizon Client, so that they do not always need to supply credentials when connecting to a Connection Server instance, configure View LDAP for this feature on the Connection Server host.

  Users can save their passwords if View LDAP is configured to allow it, if the Horizon Client certificate verification mode is set to **Warn before connecting to untrusted servers** or **Never connect to untrusted servers**, and if Horizon Client can fully verify the server certificate that Connection Server presents. For instructions, see "Saving Credentials in Mobile and Mac OS X Horizon Clients" in the *View Administration* document.
- Verify that the desktop or application pool is set to use the VMware Blast display protocol or the PCoIP display protocol. For Connection Server 5.3.x, see the *View Administration* document. For Connection Server 6.0 and later, see the *Setting Up Desktop and Application Pools in View* document.

Install or Upgrade Horizon Client on an iOS Device

You can install Horizon Client from the VMware Downloads page or from the App Store.

Prerequisites

- If you have not already set up the iOS device, do so. See the user guide from Apple.
- Verify that you have the URL for a download page that contains the Horizon Client installer. This URL might be the VMware Downloads page at http://www.vmware.com/go/viewclients, or it might be the URL for a Connection Server instance.

Procedure

1. On your iOS device, Mac, or PC, browse to the URL for downloading the installer file, or search the App Store for the Horizon Client app.
2. Download the app.
3. If you downloaded the app to a Mac or PC, connect your iOS device to the computer and follow the onscreen instructions in iTunes.
4. To determine whether the installation succeeded, verify that the **Horizon** app icon appears on the iOS device.

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://`
- `com.rsa.securid.iphone://`
- `com.rsa.securid://`

For end users who will be installing the token by tapping the URL, only the prefix `viewclient-securid://` is supported.

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+AES:ECDH+AES:RSA+AES:@STRENGTH".

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 **Settings** at the bottom of the Horizon Client screen.

2 Tap **Advanced SSL Options**.

3 Make sure that the **Reset to Default Settings** option is set to off.

4 To enable or disable a security protocol, tap the **On** or **Off** toggle 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 **Reset** in the upper right corner of the screen.

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

Configure VMware Blast Options

You can configure decoding and network protocol options 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 **Settings** at the bottom of the Horizon Client screen.

2 Tap **VMware Blast**.

3 Configure the decoding and network protocol options.

Option	Description
H.264	Select this option to allow H.264 decoding in Horizon Client. When this option is selected (the default setting), 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. Deselect this option to always use JPG/PNG decoding.
UDP	Select this option to allow UDP networking in Horizon Client. When this option is selected (the default setting), Horizon Client uses UDP networking if UDP connectivity is available. If UDP networking is blocked, Horizon Client uses TCP networking. Deselect this option to always use TCP networking. **Note** UDP is disabled by default on a Horizon remote desktop. For UDP to work, it must be enabled on the desktop, the client, and the Blast Secure Gateway (BSG).

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 **Settings** at the bottom of the Horizon Client screen.

2 Tap **Default 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.

Configure AirWatch to Deliver Horizon Client to Mobile Devices

You can configure AirWatch to deliver Horizon Client to mobile device users. You can optionally specify a default list of Connection Server instances. The Connection Server instances that you specify appear as shortcuts in Horizon Client.

Prerequisites

- Install and deploy AirWatch. See http://www.air-watch.com.
- Become familiar with the AirWatch console. This procedure assumes you know how to use the AirWatch console. For more information, see the AirWatch documentation or online help.

Procedure

1 Log in to the AirWatch console as an administrator.

2 Select **Accounts > Users > List View**, click **Add User**, and add user accounts for the users who will run Horizon Client on their mobile devices.

3 Select **Accounts > Users > User Groups**, click **Add**, and create a user group for the user accounts that you created.

4 Upload and add the Horizon Client application to AirWatch.

   a Select **Apps & Books > Applications > List View** and click **Add Application** on the **Public** tab.

   b Search for and select VMware Horizon Client for Apple iOS in the App Store.

   c On the **Info** tab, type an application name and specify the supported mobile device models.

   d On the **Assignment** tab, assign the Horizon Client application to the user group that you created.

   e (Optional) To configure a default Connection Server instance, on the **Deployment** tab, select the **Send Application Configuration** check box, type `servers` in the **Configuration Key** text box, select **String** from the **Value Type** drop-down menu, and type an IP address or host name in the **Configuration Value** text box.

   `servers` is case sensitive. To specify a list of Connection Server instances, type multiple IP addresses or host names, separated by commas, in the **Configuration Value** text box.

   For example: `123.456.1.1, viewserver4.mydomain.com, 123.456.1.2`

   Note This feature is supported only for iOS 7 and later devices. You cannot push a default Connection Server list to an iOS 6 device.

   f Publish the Horizon Client application.

5 Install and set up the AirWatch MDM Agent on each iOS device.

   You can download the AirWatch MDM Agent from iTunes.

6 Use the AirWatch console to install the Horizon Client application on the mobile devices.

   You cannot install the Horizon Client application before the effective date on the **Deployment** tab.

AirWatch delivers Horizon Client to the mobile devices in the user group that you associated with the Horizon Client application.

When a user launches Horizon Client, Horizon Client communicates with the AirWatch MDM Agent on the device. If you configured a default list of Connection Server instances, AirWatch pushes the server information to the AirWatch MDM Agent on the device and shortcuts for those servers appear in Horizon Client.

What to do next

You can use the AirWatch console to edit the Horizon Client application and push those changes to mobile devices. For example, you can add a default Connection Server instance to the server list for the Horizon Client application.

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.

Although the information is encrypted while in transit to Connection Server, the information on the client system is logged unencrypted in a user-specific directory. The logs do not contain any personally identifiable information.

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.)
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

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

Description	Is This Field Made Anonymous ?	Example Value
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.)
Maximum concurrent USB device connections	No	2
USB device vendor ID	No	Examples include the following: ■ Kingston ■ NEC ■ Nokia ■ Wacom

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

Description	Is This Field Made Anonymous ?	Example Value
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)

Using URIs to Configure Horizon Client

2

Using uniform resource identifiers (URIs), you can create a Web page or an email with links that end users click to launch Horizon Client, connect to Connection Server, and launch a specific desktop or application with specific configuration options.

You can simplify the process of connecting to a remote desktop or application by creating Web or email links for end users. You create these links by constructing URIs that provide some or all of the following information, so that your end users do not need to supply it:

- Connection Server address
- Port number for Connection Server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from Active Directory user name
- Domain name
- Desktop or application display name
- Actions including reset, log off, and start session

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

NOTE You can use URIs to launch Horizon Client only if the client software is already installed on end users' client computers.

This chapter includes the following topics:

Syntax for Creating vmware-view URIs

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

URI Specification

Use the following syntax to create URIs for launching Horizon Client:

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

The only required element is the URI scheme, `vmware-view`. For some versions of some client operating systems, the scheme name is case-sensitive. Therefore, use `vmware-view`.

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

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

authority-part

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

To specify a user name, use the following syntax:

`user1@`*`server-address`*

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

To specify a port number, use the following syntax:

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

path-part

Specifies the desktop or application. Use the desktop display name or application display name. This name is the one specified in View Administrator when the desktop or application pool was created. If the display name has a space in it, use the **`%20`** encoding mechanism to represent the space.

query-part

Specifies the configuration options to use or the desktop or application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If queries conflict with each other, the last query in the list is used. Use the following syntax:

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

Supported Queries

This topic lists the queries that are supported for this type of Horizon Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the *Using VMware Horizon Client* guide for each type of client system.

action

Table 2-1. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available desktops and applications hosted on the specified server. You are not required to specify a desktop or application when using this action. If you use the `browse` action and specify a desktop or application, the desktop or application is highlighted in the list of available items.
`start-session`	Launches the specified desktop or application. If no action query is provided and the desktop or application name is provided, `start-session` is the default action.

Table 2-1. Values That Can Be Used with the action Query (Continued)

Value	Description
`reset`	Shuts down and restarts the specified desktop or remote application. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify an application, the action will be ignored or the end user will see the warning message "Invalid URI action."

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

defaultLaunchView Sets the default launch view for Horizon Client. Valid values are **`recent`** and **`servers`**.

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

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

tokenUserName Specifies the RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, the Windows user name is used. The syntax is **`tokenUserName=`*`name`***.

Examples of vmware-view URIs

You can create hypertext links or buttons with the `vmware-view` URI scheme and include these links in email or on a Web page. Your end users can click these links to, for example, launch a particular remote desktop with the startup options you specify.

URI Syntax Examples

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

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

Horizon Client is launched and connects to the `view.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the desktop whose display name is displayed as **Primary Desktop**, and the user is logged in to the guest operating system.

Note The default display protocol and window size are used. The default display protocol is PCoIP. The default window size is full screen.

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

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

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

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

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

Horizon Client is launched and connects to the `view.mycompany.com` server. In the login box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the application whose display name is displayed as **Calculator**. The connection uses the VMware Blast display protocol.

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

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

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

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

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

Horizon Client is launched and connects to the `view.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client displays a dialog box that prompts the user to confirm the reset operation for Primary Desktop. After the reset occurs, depending on the type of client, the user might see a message indicating whether the reset was successful.

Note This action is available only if the View administrator has enabled this feature for end users.

8 `vmware-view://`

If the client is already running, the Horizon Client app comes to the foreground. If the client is not already running, Horizon Client is launched.

9 `vmware-view://?defaultlaunchview=recent`

The Horizon Client is launched and the user sees the Recent screen.

HTML Code Examples

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

```
<html>
<body>

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

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

</body>
</html>
```

Managing Remote Desktop and Application Connections 3

Use Horizon Client to connect to Connection Server or a security 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.

To use remote applications, you must connect to Connection Server 6.0 or later.

NOTE Before you have end users access their remote desktops, test that you can log in to a remote desktop from a client device.

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.
- Obtain the NETBIOS domain name for logging in. For example, you would use `mycompany` rather than `mycompany.com`.

- Perform the administrative tasks described in "Preparing Connection Server for Horizon Client," on page 11.
- 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 that connection on.

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

  If your company has an internal wireless network to provide routable access to remote desktops that your device can use, you do not have to set up a View security server or VPN connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or application. Note that 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 12.
- Configure the certificate checking mode for the SSL certificate presented by Connection Server. See "Certificate Checking Modes for Horizon Client," on page 25.
- If you plan to use Touch ID to authenticate, add at least one fingerprint in the Touch ID & Passcode setting on your iOS device. For complete Touch ID authentication requirements, see "Touch ID Authentication Requirements," on page 10.

Procedure

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

2 Tap the **Horizon** app icon on the Home screen.

3 Connect to a server.

Option	Action
Connect to a new server	Type the name of a server, type a description (optional), and tap **Add Server**.
Connect to an existing server	Tap the server icon on the Servers screen.

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

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

If your smart card has only one certificate, that certificate is already selected. If there are many certificates, you can scroll through them if necessary.

5 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.

6 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.

7 (Optional) If the **Enable Touch ID** setting is available, turn the setting on to use Touch ID to authenticate.

The **Enable Touch ID** setting is available only if biometric authentication is enabled on the server and you have not previously authenticated with Touch ID.

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

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

b Select a domain.

c (Optional) Tap to toggle the **Remember this Password** option to on if your administrator has enabled this feature and if the server certificate can be fully verified.

d Tap **Login**.

If Touch ID is enabled and you are logging in for the first time, your Active Directory credentials are stored securely in the iOS devices's Keychain for future use.

9 If you are prompted for Touch ID authentication, place your finger on the **Home** button.

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

PCoIP provides an optimized PC experience for delivery of images, audio, and video content on the LAN or across the WAN. **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**.

11 Tap a desktop or application to connect to it.

If you are using smart card authentication, you are not prompted to supply your PIN again, but the login process takes longer than if you use Active Directory authentication.

If you are connecting to a session-based remote desktop, which is hosted on a Microsoft RDS host, and if the desktop is already set to use the Microsoft RDP display protocol, you will not be able to connect immediately. You will be prompted to have the system log you off of the remote operating system so that a connection can be made with the PCoIP display protocol or the VMware Blast display protocol. VMware Blast requires Horizon Agent 7.0 or later.

After you connect to a desktop or application for the first time, a shortcut for the desktop or application is saved to the Recent screen. The next time you want to connect to the remote desktop or application, you can tap the shortcut instead of typing the server's name.

Certificate Checking Modes 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.

Important For instructions about distributing a self-signed root certificate that users can install on their iOS devices, see the instructions on the Apple Web site. For example, for iPads, see http://www.apple.com/ipad/business/docs/iPad_Certificates.pdf.

To set the certificate checking mode, tap **Settings** at the bottom of the Horizon Client screen and tap **Server Certificates Verification 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.

Manage Saved Servers

When you connect to a View server, Horizon Client saves the server to the Servers screen. You can edit and remove saved servers.

Horizon Client saves the server, even if you mistype the name or type the wrong IP address. You can delete or change this information.

Important You tap a server name to connect to the server.

Procedure

1 Tap **Servers** (cloud icon) at the bottom of the screen to display the saved servers.

2 To manage a saved server, touch and hold the server icon until the context menu appears.

Option	Action
Change the user name, domain, server name, or description	a Tap **Edit Server** in the context menu. b Make your changes on the Edit Server screen. c Tap **Update** to save your changes.
Remove a server	Tap **Delete Server** in the context menu. The desktop and application shortcuts associated with the server are also deleted.

Option	Action
Forget a saved password	Tap **Forget Password** in the context menu. This option is available only if you previously saved your password.
Disable Touch ID	Tap **Sign Out**. This option is available only if you previously enabled Touch ID.

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 Tap **Servers** (cloud icon) at the bottom of the screen and tap the server icon to connect to the server.

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	Action
Select a favorite	Touch 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 page.
Deselect a favorite	Touch 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 page.

4 (Optional) Tap **Favorites** (star icon) at the bottom of the screen to display only favorite desktops or applications.

You can tap **All** (cloud icon) at the bottom of the screen 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 logged in to the remote desktop or application, you can disconnect by tapping the Horizon Client Tools radial menu icon and tapping the **Disconnect** icon.

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 23.

Procedure

1. Tap **Servers** (cloud icon) at the bottom of the screen and tap the server icon.
2. If prompted, supply your RSA user name and passcode, your Active Directory user name and password, or both.
3. Touch and hold the desktop name until the context menu appears.
4. Tap **Log Off** in the context menu.

What to do next

Tap the **Logout** button in the upper-left corner of the screen 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.

Desktop and application shortcuts can appear on multiple pages and you can swipe across pages to see more shortcuts. Horizon Client creates new pages, as needed, to accommodate all of your shortcuts.

Procedure

- Perform these steps to remove a desktop or application shortcut from the Recent screen.
  a. Touch and hold the shortcut.
  b. Tap the **X** button.
- To move a desktop or application shortcut, touch and hold the shortcut, drag it to the new location, and tap **Done**.

  You cannot drag a shortcut to another page unless that page already exists.

Using 3D Touch with Horizon Client

You can use Peek and Pop gestures to interact with Horizon Client on a 3D Touch-enabled iPhone 6s or iPhone 6s Plus.

Using Peek and Pop with the Horizon app on Your Home Screen

You can Peek at the **Horizon** app on your Home screen to show a quick action menu. On the quick action menu, you can tap the **Connect to Most Recent Server** item to quickly connect to the most recently used server. If a recent server does not exist, you can tap the **Connect to Most Recent Server** item to add a new server.

After you connect to a remote desktop or application, Horizon Client adds a shortcut to the desktop or application to the quick action menu. For example, if you connect to a remote desktop named Win7, Horizon Client adds **Connect to Win7**. You can tap a shortcut to quickly connect a remote desktop or application. The **Horizon** icon quick action menu can contain up to three shortcuts.

Using Peek and Pop Inside Horizon Client

On the desktop and application selection screen, you can Peek at a remote desktop or application to show a quick action menu. You can tap items in the quick action menu to connect, log off, mark a favorite, and perform other actions, depending on the remote desktop or application. You can also Pop into a remote desktop or application to connect to it.

Quick action menus are also available on the Servers, Recent, and Favorites screens. For example, on the Servers screen, you can Peek at a saved server and tap items in the quick action menu to edit, remove, or connect to the server. On the Recent screen, you can Peek at a remote desktop or application shortcut and tap items in the quick action menu to remove the shortcut or connect to the desktop or application. You can also Pop into a saved server or remote desktop or application shortcut to connect to it.

Enabling Peek for the Horizon Client Tools

By default, the Horizon Client Tools radial menu icon appears in the middle of the screen when you are connected to a remote desktop or application. You tap the radial menu icon to expand the menu and display icons for each tool, which you tap to select. For pictures of the radial menu icon and tools icons, see Table 4-6.

If you enable Peek for the Horizon Client Tools, the Horizon Client Tools radial menu icon does not appear. To display the icons for each tool, press deeply on any place on the screen.

To enable Peek for the Horizon Client Tools, tap **Settings** at the bottom of the Horizon Client screen, tap **Touch**, and toggle the **Peek for the menu** setting to on. If you are connected to a remote desktop or application, you can access settings by tapping the **Settings** (gear) icon in the Horizon Client Tools radial menu.

Using Spotlight Search with Horizon Client

You can use Spotlight search on iOS 9.x devices to search for and connect to remote desktops and applications.

When you log in to a server in Horizon Client, the remote desktops and applications on the server are added to the Spotlight index. Only the remote desktops and applications on the last server to which you logged in are indexed.

To use Spotlight search to search for a particular remote desktop or application, type its name or a partial name in the Spotlight search field. For example, to find a remote desktop named Win 2008 RDS Desktop, you might type **`Win`** or **`RDS`**.

To use Spotlight search to find your favorite remote desktops and applications, type **favorite** in the Spotlight search field. To search for any remote desktop or application, type **vmware** or **horizon** in the Spotlight search field. The search results can contain up to 10 items.

To connect to a remote desktop or application, tap its name in the search results. If you are not currently connected to the server, the Horizon Client login screen appears and you can log in.

Using Split View and Slide Over with Horizon Client

You can use Split View and Slide Over with Horizon Client on any iPad model that supports Split View and Slide Over and is running iOS 9.x.

With Split View and Slide Over, you can open Horizon Client and another app at the same time. You can run Horizon Client as either the primary app or the secondary app.

If you rotate your device or slide the vertical divider that separates the primary and secondary apps, Horizon Client automatically adjusts to fit the size of the window. If you are connected to a remote desktop, the remote desktop automatically adjusts to fit the size of the window if the **Resolution** setting is set to **Auto - Fit**. For information about setting the resolution for a remote desktop, see "Changing the Display Resolution Setting," on page 44.

NOTE Horizon Client does not support Picture in Picture.

Using a Microsoft Windows Desktop or Application

4

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

This chapter includes the following topics:

Feature Support Matrix for iOS

Some features are supported on one type of Horizon Client but not on another.

Table 4-1. Features Supported on Windows Desktops for iOS Horizon Clients

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008/2012 R2 Desktop
RSA SecurID or RADIUS	X	X	X	Limited	Limited	X
Single sign-on	X	X	X	Limited	Limited	X
RDP display protocol						

Table 4-1. Features Supported on Windows Desktops for iOS Horizon Clients (Continued)

Feature	Windows 10 Desktop	Windows 8.x Desktop	Windows 7 Desktop	Windows Vista Desktop	Windows XP Desktop	Windows Server 2008/2012 R2 Desktop
PCoIP display protocol	X	X	X	Limited	Limited	X
VMware Blast display protocol	X	X	X			X
USB access						
Real-Time Audio-Video (audio-in only)	X	X	X			X
Wyse MMR						
Windows 7 MMR						
Virtual printing						
Location-based printing	X	X	X	Limited	Limited	X
Smart cards	X	X	X	Limited	Limited	X
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 or Horizon Agent 7.0 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 Connection Server 6.1.

For descriptions of these features, see the *View 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 and later.

Table 4-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0 or Later, Installed

Feature	Windows Server 2008 R2 RDS Host on a Physical Machine	Windows Server 2008 R2 RDS Host on a Virtual Machine	Windows Server 2012 RDS Host on a Physical Machine	Windows Server 2012 RDS Host on a Virtual Machine
RSA SecurID or RADIUS	X	X	X	X
Smart card	View Agent 6.1 and later	View Agent 6.1 and later	View Agent 6.1 and later	View Agent 6.1 and later
Single sign-on	X	X	X	X
RDP display protocol (for desktop clients)	X	X	X	X

Table 4-2. Features Supported for RDS Hosts with View Agent 6.0.x or Later, or Horizon Agent 7.0 or Later, Installed (Continued)

Feature	Windows Server 2008 R2 RDS Host on a Physical Machine	Windows Server 2008 R2 RDS Host on a Virtual Machine	Windows Server 2012 RDS Host on a Physical Machine	Windows Server 2012 RDS Host on a Virtual Machine
PCoIP display protocol	X	X	X	X
VMware Blast display protocol	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later
HTML Access		View Agent 6.0.2 and later		View Agent 6.0.2 and later
Virtual printing (for desktop clients)		View Agent 6.0.1 and later		View Agent 6.0.1 and later
Location-based printing		View Agent 6.0.1 and later		View Agent 6.0.1 and later
Multiple monitors (for desktop clients)	X	X	X	X
Unity Touch (for mobile and Chrome OS clients)	X	X	X	X

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.

Limitations for Specific Features

Specific features that are supported on Windows desktops for Horizon Client for iOS have certain restrictions.

Table 4-3. Requirements for Specific Features

Feature	Requirements
Left Handed Mode	This feature is iOS specific. If your remote desktop is configured so that the primary and secondary mouse buttons are switched, use the Left Handed Mode feature. See "Configure Horizon Client to Support Reversed Mouse Buttons," on page 43.
Location-based printing for Windows Server 2008 R2 desktops, RDS desktops (on virtual machine RDS hosts), and remote applications	Horizon 6.0.1 with View and later servers.

Table 4-3. Requirements for Specific Features (Continued)

Feature	Requirements
Smart cards for RDS desktops	View Agent 6.1 and later.
Real-Time Audio-Video (audio-in only)	See "System Requirements for Real-Time Audio-Video," on page 8

Note You can also use Horizon Client to securely access remote Windows-based applications, in addition to remote desktops. Selecting an application in Horizon Client opens a window for that application on the local client device, and the application looks and behaves as if it were locally installed.

You can use remote applications only if you are connected to Connection Server 6.0 or later. For information about which operating systems are supported for the RDS (Remote Desktop Sessions) host, which provides remote applications and session-based desktops, see "Supported Operating Systems for Horizon 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.

Feature Support for Linux Desktops

Some Linux guest operating systems are supported if you have View Agent 6.1.1 or later or Horizon Agent 7.0 or later. For a list of supported Linux operating systems and information about supported features, see *Setting Up Horizon 6 for Linux Desktops*, which is part of the Horizon 6 version 6.1 documentation, or see *Setting Up Horizon 7 for Linux Desktops*, which is part of the Horizon 7 version 7 documentation.

External Keyboards and Input Devices

Horizon Client supports the iPad Keyboard Dock and Apple Wireless Keyboard (Bluetooth) external keyboards. Horizon Client supports Apple Pencil as a pointer device on iPad Pro.

Horizon Client automatically detects the iPad Keyboard Dock external keyboard. To use the Apple Wireless Keyboard (Bluetooth) with a remote desktop, you must first pair the keyboard with the client device.

After you pair the keyboard with the iPad, make sure that you do not have the onscreen keyboard in split keyboard mode when you attempt to make the iPad detect the Bluetooth keyboard. To make the client device detect the wireless keyboard, tap the screen with three fingers at the same time, or tap the **Keyboard** button in the Horizon Client Tools.

Also with the Apple Wireless Keyboard (Bluetooth), after the external keyboard is detected, you cannot use the Horizon Client Tools or three-finger tap to display the onscreen keyboard. You must first deactivate the external keyboard by pressing its Eject key.

The Apple Wireless Keyboard (Bluetooth) does not input the Japanese full-width tilde correctly in remote desktops.

International Keyboards

You can input characters for English, Japanese, French, German, Simplified Chinese, Traditional Chinese, and Korean.

Use an English keyboard on your iOS device with a remote desktop that uses a Korean or Japanese input method editor (IME). If you use a Korean or Japanese keyboard on your iOS device and you connect to a remote desktop that uses a Korean or Japanese IME, the remote desktop Windows IME English/Korean or English/Japanese mode is not synchronized with the iOS keyboard locale.

Enable the Japanese 106/109 Keyboard Layout

If you are connected to a Windows XP desktop, you can configure Horizon Client to use the Japanese 106/109 keyboard layout.

Prerequisites

Use Horizon Client to connect to a Windows XP desktop that has the Japanese keyboard layout enabled.

Procedure

1 Use the Horizon Client Tools to display the Options dialog box.

2 Tap to toggle the **Japanese 106/109 Keyboard** option to on.

This setting is disabled if the keyboard layout on the Windows XP desktop is not set to Japanese. This setting is hidden if the desktop is not running Windows XP.

3 Tap **Done**.

Using the Real-Time Audio-Video Feature for Microphones

With the Real-Time Audio-Video feature, you can use a microphone connected to your mobile device on your remote desktop. Real-Time Audio-Video is compatible with standard audio devices and with standard conferencing applications such as Skype, WebEx, and Google Hangouts.

Real-Time Audio-Video is enabled by default when you install Horizon Client on your device.

Note Only the audio-in feature is supported. The video feature is not supported.

For information about setting up the Real-Time Audio-Video feature on a remote desktop, see the *Setting Up Desktop and Application Pools in View* document.

The first time you use the microphone, Horizon Client prompts you for permission to access it. You must grant permission for the microphone to work with your remote desktop. You can enable and disable access to the microphone by changing the Microphone permission for Horizon Client in the iOS Settings app.

Using Native Operating System Gestures with Touch Redirection

You can use native operating system gestures from your touch-based mobile device when you are connected to a Windows 8, Windows 10, or Windows Server 2012 remote desktop, or to a remote application that is hosted on Windows Server 2012. For example, you can touch, hold, and release an item on a Windows 8 desktop to display the item's context menu.

When touch redirection is enabled, you can use only native operating system touch gestures. Horizon Client local gestures, such as double-click and pinch, no longer work. You must drag the Unity Touch tab button to display the Unity Touch sidebar.

Touch redirection is enabled by default when you connect to a Windows 8, Windows 10, or Windows Server 2012 remote desktop, or to a remote application that is hosted on Windows Server 2012.

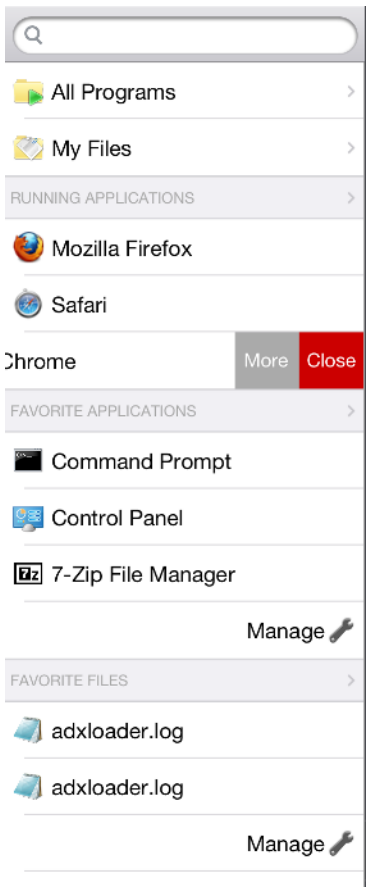
To disable touch redirection, tap **Settings** at the bottom of the Horizon Client screen, tap **Touch**, and toggle the **Windows Native Touch Gestures** setting to off. If you are connected to a remote desktop or application, you can access settings by tapping the **Settings** (gear) icon in the Horizon Client Tools radial menu.

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.

If the Unity Touch feature is enabled, the sidebar appears on the left side of the screen when you first access a remote desktop.

Figure 4-1. Unity Touch Sidebar



If you access a desktop that has Unity Touch enabled but the sidebar is not displayed, you can see a tab on the left side of the screen. Besides swiping this tab to the right to open the sidebar, you can slide the tab up or down.

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

Table 4-4. Unity Touch Sidebar Actions for a Remote Desktop

Action	Procedure
Show the sidebar	Swipe the tab to the right. When the sidebar is open, you cannot perform actions on the desktop screen or the Horizon Client Tools radial menu.
Hide the sidebar	Swipe the tab to the left to close the sidebar. When the sidebar is open, you cannot perform actions on the desktop screen or the Horizon Client Tools radial menu. You can also touch the desktop screen, including the Horizon Client Tools radial menu, to hide the sidebar.
Navigate to an application	Tap **All Programs** and navigate to the application just as you would from the Windows Start menu.

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

Action	Procedure
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.
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	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Minimize**.
Maximize a running application or window	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Maximize**.
Close a running application or window	Touch the application name under **Running Applications** and swipe from right to left. Tap the **Close** button that appears.
Restore a running application or window to its previous size and position	1 Touch the application name under **Running Applications** and swipe from right to left. 2 Tap the **More** button that appears. 3 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. Your favorites are remembered across all of your mobile devices so that, for example, you have the same list whether using your smart phone or your tablet.
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.

Note To use the Unity Touch feature with View 5.3.x desktops, the Remote Experience Agent must be installed on the desktops. If you have the Remote Experience Agent installed but want to turn off this feature, you can set a registry value on the remote desktop.

If users have a floating desktop, users' favorite applications and files can be saved only if Windows roaming user profiles are configured for the desktop. Administrators can create a default **Favorite Applications** list that end users see the first time the sidebar appears.

For Connection Server 5.3.x servers, see the *View Feature Pack Installation and Administration* document. For Connection Server 6.0 and later servers, see the *Setting Up Desktop and Application Pools in View* document.

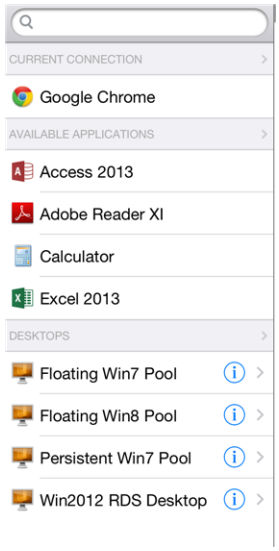
Using the Unity Touch Sidebar with a Remote Application

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.

When you access a remote application, the Unity Touch sidebar appears on the left side of the screen. If the Unity Touch sidebar is closed, a tab appears on the left side of the screen. You can swipe this tab to the right to reopen the sidebar. You can also slide the tab up or down.

Note You can use remote applications only if you are connected to Connection Server 6.0 or later.

Figure 4-2. Unity Touch Sidebar for a Remote Application



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

Table 4-5. Unity Touch Sidebar Actions for a Remote Application

Action	Procedure
Show the sidebar	Swipe the tab to the right to open the sidebar. When the sidebar is open, you cannot perform actions on the application screen.
Hide the sidebar	Swipe the tab to the left to close the sidebar. When the sidebar is open, you cannot perform actions on the application screen. In Horizon Client 3.1 and later, you can also touch the application screen, including the Horizon Client Tools radial menu, to hide the sidebar.
Switch between running applications	Tap the application under **Current Connection**.
Open an application	Tap the name of the application under **Available Applications** in the sidebar. The application starts and the sidebar closes.

Table 4-5. Unity Touch Sidebar Actions for a Remote Application (Continued)

Action	Procedure
Close a running application	1 Touch the application name under **Current Connection** and swipe from right to left. 2 Tap the **Close** button that appears.
Minimize a running application	1 Touch the application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Minimize**.
Maximize a running application	1 Touch the application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Maximize**.
Restore a running application	1 Touch the application name under **Current Connection** and swipe from right to left. 2 Tap the **More** button that appears. 3 Tap **Restore**.
Switch to a remote desktop	Tap the desktop name under **Desktops**.

Horizon Client Tools on a Mobile Device

On a mobile device, the Horizon Client Tools include buttons for displaying the onscreen keyboard, virtual touchpad, configuration settings, and a virtual keypad for arrow keys and function keys.

The Horizon Client radial menu icon appears in the middle of the screen when you are connected to a remote desktop or application. Tap to expand the radial menu and display icons for each tool, which you can tap to select. Tap outside the tool icons to collapse the icons back into the radial menu icon.

The radial menu includes several tools.

Table 4-6. Radial Menu Icons

Icon	Description
	Horizon Client Tools radial menu
	Disconnect
	Onscreen keyboard (toggles to show or hide)
	Settings
	Navigation keys

Table 4-6. Radial Menu Icons (Continued)

Icon	Description
	Virtual touchpad
	Gesture help

Onscreen Keyboard

The onscreen keyboard has more keys than the standard onscreen keyboard, for example, Control keys and function keys are available. To display the onscreen keyboard, tap the screen with three fingers at the same time or tap the **Keyboard** icon.

You can also use the feature that displays the onscreen keyboard whenever you tap a text field, such as in a note or new contact. If you then tap in an area that is not a text field, the keyboard is dismissed.

Important To use the three-finger tap, make sure the iOS accessibility feature for zooming is turned off. When the zoom accessibility feature is turned on, you zoom by double-tapping with three fingers, and tapping once with three fingers does nothing.

Even if you use an external keyboard, a one-row onscreen keyboard might still appear, which contains function keys, and the Ctrl, Alt, Win, and arrow keys. Some external keyboards do not have all these keys.

Sending a String of Characters

From the onscreen keyboard, 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.**

Use this feature if you have a poor network connection. That is, use this feature if, when you type a character, the character does not immediately appear in the application. With this feature, you can quickly type up to 1,000 characters and then either tap **Send** or tap **Return** to have all 1,000 characters appear at once in the application.

Navigation Keys

Tap the **Ctrl/Page** icon in the Horizon Client Tools or onscreen keyboard to display the navigation keys. These keys include Page Up, Page Down, arrow keys, function keys, and other keys that you often use in Windows environments, such as Alt, Del, Shift, Ctrl, Win, and Esc. You can press and hold arrow keys for continuous key strokes. For a picture of the Ctrl/Page icon, see the table at the beginning of this topic.

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+Del, 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 Del key.

Onscreen Touchpad and Full Screen Touchpad

The virtual touchpad can be either regular-size, to resemble a touchpad on a laptop computer, or full screen, so that the entire device screen is a touchpad.

By default, when you tap the touchpad icon, you can touch anywhere on the screen to move the mouse pointer. The screen becomes a full-screen touchpad.

- Moving your finger around the touchpad creates a mouse pointer that moves around the remote desktop or application.
- You can use the regular-size and full screen virtual touchpad for single-clicking and double-clicking.
- The regular touchpad also contains left-click and right-click buttons.
- To simulate holding down the left-click button while dragging, double-tap with one finger and then drag.

  To enable this feature, use the Horizon Client Tools to display the Options dialog box, and click to toggle the **Touchpad Tap & Drag** option to on.
- You can tap with two fingers and then drag to scroll vertically.

You can drag the regular-size virtual touchpad to the side of the device so that you can use your thumb to operate the touchpad while you are holding the device.

You can make the virtual touchpad resemble the touchpad on a laptop, including right-click and left-click buttons. Tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, tap **Touch**, and toggle the **Full Screen Touchpad Mode** setting to off.

To adjust how quickly the pointer moves when you use the touchpad, tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, tap **Touch**, and drag the slider in the **Touchpad Sensitivity** option.

You can also set the **Full Screen Touchpad Mode** and **Touchpad Sensitivity** settings from the Horizon Client Settings screen. Tap **Settings** at the bottom of the Horizon Client screen and tap **Touch** to display the touchpad settings.

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 applications, you tap to click a user interface element.

In a remote desktop, if you tap and hold for a second, a magnifying glass appears, along with a mouse pointer, for precise placement. This feature is especially helpful when you want to resize a window.

Note If your remote desktop is configured for a left-handed user, see "Configure Horizon Client to Support Reversed Mouse Buttons," on page 43.

Right-Clicking

The following options are available for right-clicking:

- Use the Horizon Client Tools to display the regular virtual touchpad and use the touchpad's right-click button.
- On 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.

- On 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.

  Important Scrolling with one finger has the following limitations: It does not work if you have zoomed in, or when the onscreen keyboard is displayed, or when you are using the full screen touchpad.

- Use the Horizon Client Tools to display the touchpad, tap the touchpad with two fingers, and then drag to scroll.
- Use the onscreen touchpad to move the mouse pointer and click scroll bars.

Zooming In and Out

As in other applications, pinch your fingers together or apart to zoom on a touch screen.

Window Resizing

If you use the full screen touchpad to resize a window, touch and hold one finger at the corner or side of the window and drag to resize, or double-tap with one finger and then drag.

If you use the regular-size virtual touchpad, to simulate holding down the left-click button while dragging the corner or side of a window, double-tap with one finger and then drag.

If you are not using either type of virtual touchpad, tap and hold until the magnifying glass appears at the corner or side of the window. Move your finger around until the resizing arrows appear. Lift your finger off the screen. The magnifying glass is replaced by a resizing circle. Tap this resizing circle and drag it to resize the window.

Sound, Music, and Video

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

Multitasking

You can switch between Horizon Client and other apps without losing a remote desktop or application connection.

In a WiFi network, by default Horizon Client runs in the background for up to three minutes on iOS 7.0 and later devices. In a 3G network, Horizon Client suspends data transmission when you switch to another app. Data transmission resumes when you switch back to Horizon Client.

You can copy and paste plain text between an iOS app and a remote desktop or between two remote desktops. Formatting information is not copied.

- Text that you copy to the clipboard is automatically copied to your remote desktop's clipboard when you log in to the remote desktop.
- If you are logged in to a remote desktop, text that you copy to the remote desktop's clipboard is copied to your iOS device's clipboard when you press the **Home** button or switch to the background.

By default, you can copy and paste plain text between an iOS device application and a remote application. The clipboard can accommodate 1 MB of data for copy and paste operations. To enable users to copy plain text between a remote application and an iOS device application, you must modify the PCoIP session group policy setting called **Configure clipboard redirection** on the RDS host that hosts the remote application pool. For information about configuring this group policy setting, see the *Setting Up Desktop and Application Pools in View* document.

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.

Configure Horizon Client to Support Reversed Mouse Buttons

You can use the **Left Handed Mode** option if the primary and secondary mouse buttons are switched in your remote desktop.

If you set the mouse properties inside your remote desktop so that the primary mouse button is the one on the right side, as many left-handed people do, you must turn on the **Left Handed Mode** option in Horizon Client. If you do not turn on this option when mouse buttons are reversed, a single tap acts as a click of the secondary mouse button. For example, a single tap might display a context menu rather than selecting something or inserting a cursor.

Procedure

- If you are already connected to the remote desktop, perform these steps.
  a. Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings screen.
  b. Tap **Touch** on the Settings screen.
  c. Tap **Left Handed Mode** to toggle the option to on.
  d. Tap **Done** to close the Settings screen.
- If you are not connected to the remote desktop, perform these steps.
  a. Tap **Settings** at the bottom of the Horizon Client screen.
  b. Tap **Touch** on the Settings screen.
  c. Tap **Left Handed Mode** to toggle the option to on.

A single tap now acts as a click with the primary mouse button.

Screen Resolutions and Using External Displays

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

When you connect your device to an external display or projector, Horizon Client supports certain maximum display resolutions. You can change the screen resolution used on your device to allow scrolling a larger screen resolution.

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.

You can pinch your fingers apart to zoom in and make the desktop larger than the device screen. You can then tap and drag to access the edges of the desktop.

Changing the Display Resolution Setting

To change the resolution from a remote desktop or application, tap to expand the Horizon Client Tools radial menu icon, tap the **Settings** (gear) icon, and tap **Resolution**. You can also change the resolution from the Horizon Client Settings screen. Tap **Settings** at the bottom of the Horizon Client screen and tap **Resolution**.

Note Certain options, including 3/4 Scaling and No Scaling, are not available on iPhone 6 when the device is in zoomed mode. To display these options, you must exit zoomed mode.

Screen Resolutions for Using Projectors

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

To display the keyboard and an expanded onscreen touchpad on the device while displaying the remote desktop on the projector or attached monitor, enable the **Presentation Mode** setting. The expanded touchpad and keyboard appear when you plug the device into the external monitor. The device detects the maximum resolution provided by the external display.

You can mirror the entire device display on a projector or attached monitor, including the Unity Touch sidebar, by turning off the **Presentation mode** setting. If you are connected to a remote desktop and the **Presentation Mode** setting is enabled, you can click **Done** to switch to mirror mode.

You can use the **Keep the screen alive during Presentation** setting to keep the display from turning off after a period of inactivity while in presentation mode.

You can configure these setting from a remote desktop or application by tapping to expand the Horizon Client Tools radial menu icon and tapping the **Settings** (gear) icon. You can also configure these setting by tapping the **Settings** (gear) icon at the bottom of the Horizon Client screen.

PCoIP Client-Side Image Cache

PCoIP client-side image caching stores image content on the client to avoid retransmission. This feature reduces bandwidth usage.

The PCoIP image cache captures spatial, as well as temporal, redundancy. For example, when you scroll down through a PDF document, new content appears from the bottom of the window and the oldest content disappears from the top of the window. All the other content remains constant and moves upward. The PCoIP image cache is capable of detecting this spatial and temporal redundancy.

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

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

With client-side caching, the client stores portions of the display that were previously transmitted. The cache size is one-half of the available RAM. If that amount of RAM is less than 50 MB, the cache size is 50 MB.

Suppress the Cellular Data Warning Message

When Horizon Client detects that you are using a cellular data connection, the Network Usage dialog box appears to notify you that your remote desktop or application connection might use a substantial portion of your data plan.

The Network Usage dialog box appears after you connect to a server and try to launch a remote desktop or application, after you tap a recent desktop or application shortcut, and after you connect to a remote application and try to launch another application or remote desktop from the Unity Touch sidebar. The Network Usage dialog box appears only when you launch Horizon Client.

You can suppress the Network Usage dialog box after it appears. You can also set an option to always suppress the Network Usage dialog box.

Procedure

- To suppress the Network Usage dialog box after it appears in Horizon Client, tap **Never Remind** in the Network Usage dialog box.
- To set an option to always suppress the Network Usage dialog box, tap **Settings** at the bottom of the Horizon Client screen and toggle the **Cellular Data Warning** option to off.

Internationalization

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

Troubleshooting Horizon Client 5

You can solve most Horizon Client problems by resetting the desktop or reinstalling the app.

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

This chapter includes the following topics:

Collecting and Sending Logging Information

You can configure Horizon Client to collect log information and send log files to VMware for troubleshooting.

If Horizon Client quits unexpectedly while log collection is enabled, Horizon Client prompts you to send log files to VMware when you relaunch Horizon Client.

If you choose to send log files to VMware, Horizon Client sends a message from the email account configured on your device and attaches a GZ file that contains the last five log files. The file name contains a time stamp, for example, `Horizon_View_Client_logs_timestamp.log.gz`.

You can also manually retrieve and send log files at any time.

Enable Horizon Client Log Collection

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

Because log collection affects the performance of Horizon Client, enable log collection only if you are experiencing a problem.

Prerequisites

Verify that an email account is configured on your device. Horizon Client uses this email account to send log files.

Procedure

1 If you are already connected to a remote desktop or application, perform these steps:

   a Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings screen.

   b Tap **Log Collection** on the Settings screen.

   c Tap to toggle the **Logging** option to on.

   d Tap **Done** to close the Settings screen.

2 If you are not connected to a remote desktop or application, perform these steps:

   a Tap **Settings** at the bottom of the Horizon Client screen to open the Settings screen.

   b Tap **Log Collection** on the Settings screen.

   c Tap to toggle the **Logging** option to on.

After log collection is enabled, Horizon Client generates several log files. When Horizon Client quits unexpectedly or is exited and relaunched, the log files are merged and compressed into a single GZ file. If you choose to send the log, Horizon Client attaches the GZ file to an email message.

If you switch from a running desktop to settings, enable log collection, and switch back to the desktop, you must reconnect to the desktop to collect a complete log file.

Manually Retrieve and Send Horizon Client Log Files

When Horizon Client log collection is enabled on your device, you can manually retrieve and send log files at any time.

This procedure shows you how to retrieve and send log files through Horizon Client. If your device is connected to a PC or Mac, you can also use iTunes to retrieve log files.

Prerequisites

- Verify that an email account is configured on your device. Horizon Client sends log files from this email account.
- Enable Horizon Client log collection. See "Enable Horizon Client Log Collection," on page 47.

Procedure

1 In Horizon Client, tap the email icon at the top of the screen.

2 Type the address of the email recipient in the **To:** line and click **Send** to send the message.

   The email account configured on your device appears in the **From:** line.

   The existing GZ log file is attached to the message. Horizon Client saves a maximum of five GZ log files. It deletes the oldest files when the GZ log file count is greater then five.

Disable Horizon Client Log Collection

Because log collection affects the performance of Horizon Client, disable log collection if you are not troubleshooting a problem.

Procedure

1 If you are already connected to a remote desktop or application, perform these steps.

   a Tap to expand the Horizon Client Tools radial menu icon and tap the **Settings** (gear) icon to open the Settings screen.

   b Tap **Log Collection** on the Settings screen.

   c Tap to toggle the **Logging** option to off.

   d Tap **Done** to close the Settings screen.

2 If you are not connected to a remote desktop or application, perform these steps.

   a Tap **Settings** at the bottom of the Horizon Client screen to open the Settings screen.

   b Tap **Log Collection** on the Settings screen.

   c Tap to toggle the **Logging** option to off.

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 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 23.

Procedure

1 Tap **Servers** (cloud icon) at the bottom of the screen and tap the server icon to connect to the server.

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

3 Touch and hold the desktop or application name until the context menu appears.

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.

Procedure

1 If you have Horizon Client in iTunes on your Mac or PC, browse or search the Apps Library for the Horizon Client app and remove it.

   Use the same procedure that you would use to remove any iTunes app.

2 Connect your device to your computer and allow the device to synchronize with iTunes on your Mac or PC.

3 If the Horizon Client app is not removed from your device, touch and hold the **Horizon** app icon until it wiggles and tap the **X** icon to delete the app.

What to do next

Reinstall Horizon Client.

See "Install or Upgrade Horizon Client on an iOS Device," on page 12.

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 mobile 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 iOS device, as described in the device user guide from Apple.
- 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