VMware Horizon Client for Android Installation and Setup Guide

VMware Horizon Client for Android 2103

vmware®

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

https://docs.vmware.com/

Contents

VMware Horizon Client for Android Installation and Setup Guide

This guide provides information about installing, configuring, and using VMware Horizon® Client™ software on an Android or Chromebook device.

This information is intended for administrators who must set up a VMware Horizon deployment that includes Android and Chromebook client devices. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

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

Setup and Installation

<div style="text-align: right; font-size: 3em; color: #999;">1</div>

Setting up a Horizon deployment for Android and Chromebook client devices involves using certain Connection Server configuration settings, meeting the system requirements for Horizon servers and client devices, and installing the Horizon Client app.

This chapter includes the following topics:

- System Requirements
- Preparing Connection Server for Horizon Client
- Installing Horizon Client
- Using Embedded RSA SecurID Software Tokens
- Create a Virtual Smart Card
- Pair a Virtual Smart Card with Smart Card Middleware
- Configure Device ID Sharing with OPSWAT
- Configure Advanced TLS Options
- Configure VMware Blast Options
- Configure Seamless Window Mode on a Chromebook Device
- Configure Horizon Client in Thin Client Mode
- Using the Google Admin Console to Configure Enrolled Chromebook Devices
- Configure the Horizon Client Default View
- Configure Horizon Client Data Sharing

System Requirements

Android, thin client, and Chromebook devices that run Horizon Client must meet certain hardware and software requirements.

System Requirements for Android Devices

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

Android operating systems

- Android 5.0 (Lollipop)

- Android 6.0 (Marshmallow)

- Android 7.0 and 7.1 (Nougat)

- Android 8.0 and 8.1 (Oreo)

- Android 9.0 (Pie)

- Android 10.0 (Q)

- Android 11.0 (R)

CPU architecture

- ARM

- ARM64

- x86

- x86_64

Note Non-NEON devices are not supported.

External keyboards

(Optional) Bluetooth and docked keyboard devices. For information about the external devices that your specific device supports, see the documentation from the device manufacturer.

Smart cards

See Smart Card Authentication Requirements.

Connection Server and Horizon Agent

Latest maintenance release of Horizon 7 version 7.5 and later releases.

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

Display protocols

- PCoIP

- VMware Blast

Network protocols

- IPv4

- IPv6

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

System Requirements for Thin Clients

You can install Horizon Client on certain thin clients.

The thin client on which you install Horizon Client, and the external input devices it uses, must meet certain system requirements.

Thin client models and Android operating systems

- Remix Mini with Android 5.1 (RemixOS 2.0.205 or later)

- NVIDIA SHIELD Android TV with Android 6.0

- Amazon Fire TV (1st Generation) with Android 5.1

External input devices

Horizon Client generally works with any external input device, including keyboards and controllers, that works with the thin client. For information about the devices that a specific thin client supports, see the documentation from the device manufacturer.

Horizon Client requirements

Enable the **Thin Client mode** setting in Horizon Client. See Configure Horizon Client in Thin Client Mode.

System Requirements for Chromebooks

You can install Horizon Client on certain Chromebook models. You install Horizon Client on a Chromebook from Google Play.

Chromebook models that support Android apps

Google is continuing to evaluate Chromebook models that support Android apps. For the latest information, go to https://sites.google.com/a/chromium.org/dev/chromium-os/chrome-os-systems-supporting-android-apps?visit_id=0-636124384717258228-2661029306&rd=1.

Horizon Client feature limitations

Because of device and operating system limitations, certain Horizon Client features work only on an Android device, and certain features work only on a Chromebook device. These limitations are mentioned where the features are described in this document.

System Requirements for Real-Time Audio-Video

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

Remote desktops and published applications

Remote desktops and RDS hosts must have Horizon Agent 7.5 or later installed.

Client access device

Real-Time Audio Video is supported on all devices that run Horizon Client. For more information, see System Requirements.

Smart Card Authentication Requirements

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

Using the Derived Credentials Feature

To use the derived credentials feature, a Horizon administrator must install smart card middleware on the virtual desktops or RDS host that hosts published desktops. No other middleware for PIV cards must be installed on the same virtual desktops or RDS host. VMware has tested Charismathics CSSI/CSTC 5.2.2 and ActivClient 7.1. The Windows Inbox Smart Card Minidriver is not supported.

On the client device, you must create a virtual smart card and pair it with the smart card middleware installed on the remote desktop. For information, see Create a Virtual Smart Card and Pair a Virtual Smart Card with Smart Card Middleware.

Enabling the User Name Hint Text Box in Horizon Client

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

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

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

Horizon Client continues to support single-account smart card certificates even when the smart card user name hints feature is enabled.

Additional Smart Card Authentication Requirements

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

Connection Server and security server hosts

An administrator must add all applicable Certificate Authority (CA) certificate chains for all trusted user certificates to a server truststore file on the Connection Server host or, if a security server is used, on the security server host. These certificate chains include root certificates and, if an intermediate certificate authority issues the user's smart card certificate, must also include intermediate certificates.

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

Unified Access Gateway appliances

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

Active Directory

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

Fingerprint Authentication Requirements

To use fingerprint authentication in Horizon Client, the client device on which you install Horizon Client must meet certain requirements.

Android device models

Any Android device model that has a fingerprint sensor and native fingerprint reader functionality.

Fingerprint authentication is not supported on a Chromebook device.

Operating system requirements

- Android 6 (Marshmallow) and later

- The **Fingerprint Authentication** option must be enabled and at least one fingerprint must be enrolled.

Connection Server requirements

- Horizon 7 version 7.5 or a later release.

- Enable biometric authentication in Connection Server. For information, see "Configure Biometric Authentication" in the *Horizon 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 Setting the Certificate Checking Mode in Horizon Client.

- Enable fingerprint authentication by tapping **Enable Fingerprint** on the server login window. After you successfully log in, your Active Directory credentials are stored securely in your Android device. The **Enable Fingerprint** option is shown the first time you log in and does not appear after fingerprint authentication is enabled.

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

OPSWAT Integration Requirements

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

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

To use OPSWAT integration, the following requirements must be met.

- An administrator must configure the Endpoint Compliance Checks feature in Unified Access Gateway. Unified Access Gateway 3.8 or later is required. For information, see the *Deploying and Configuring VMware Unified Access Gateway* document.

- You must install OPSWAT Mobile App on the client device. You can download OPSWAT Mobile App from the App Store.

Horizon Client generates a device ID that is unique to the client device. When you start Horizon Client, and OPSWAT Mobile App is installed, Horizon Client prompts you to share the device ID with OPWSAT Mobile App. To share the device ID, tap **Share**. If you tap **Never ask again**, Horizon Client does not share the device ID and you are not prompted again. To close the dialog box, tap **Cancel**.

If you tap **Share**, OPSWAT verifies the client device's security status and sends a compliance report to the MetaAccess server. If the client device is already registered with OPSWAT, it is enrolled successfully. If the device is not registered with OPSWAT, an error message appears and the device is not enrolled. To return to Horizon Client, tap **Return**.

You can configure device ID sharing by enabling or disabling a setting in Horizon Client. For more information, see Configure Device ID Sharing with OPSWAT.

Supported Desktop Operating Systems

A Horizon administrator creates virtual machines that have a guest operating system and installs agent software in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported Windows guest operating systems, see the *Horizon Installation* document.

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

Preparing Connection Server for Horizon Client

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must configure certain Connection Server settings.

Unified Access Gateway and Security Servers

If your VMware Horizon deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring VMware Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.

If your VMware Horizon deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 7.5 and Security Server 7.5 or later releases. For more information, see the installation document for your Horizon version.

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

Secure Tunnel Connection

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

Desktop and Application Pools

Use the following check list when configuring desktop and application pools.

- Verify that a desktop or application pool has been created and that the user account that you plan to use is entitled to access the pool. For more information, see the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.

- Verify that the desktop or application pool is set to use the VMware Blast display protocol or the PCoIP display protocol. For information, see the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.

User Authentication

Use the following check list when setting up user authentication.

- To use Fingerprint authentication with Horizon Client, you must enable biometric authentication in Connection Server. For more information, see the *Horizon Administration* document.

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

  Users can save their passwords if Horizon LDAP is configured to allow it, if the Horizon Client certificate verification mode is set to **Warn before connecting to untrusted servers** or **Never connect to untrusted servers**, and if Horizon Client can fully verify the server certificate that Connection Server presents. For more information, see the *Horizon Administration* document.

- To provide end users with unauthenticated access to published applications in Horizon Client, you must enable this feature in the Connection Server instance. For more information, see the topics about unauthenticated access in the *Horizon Administration* document.

- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature for the Connection Server instance. Beginning with Horizon 7 version 7.11, you can customize the labels on the RADIUS authentication login page. Beginning with Horizon 7 version 7.12, you can configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *Horizon Administration* document.

- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. For more information, see the *Horizon Administration* document.

- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. Beginning with Horizon 7 version 7.8, this setting is enabled by default. For more information, see the *Horizon Administration* document.

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

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

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

Installing Horizon Client

You install Horizon Client in the same way that you install other Android apps. You can also use VMware Workspace ONE UEM to deliver Horizon Client to Android device users.

Install or Upgrade Horizon Client

Horizon Client is an Android app, and you install it in the same way that you install other Android apps.

Prerequisites

- Set up the client device. See the manufacturer's user's guide for the client device.

- Verify that the client device meets the system requirements for Horizon Client. See System Requirements.

- 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.

- Become familiar with the client device's procedure for installing apps.

  Devices from different manufacturers use different methods for installing Android apps. See the manufacturer's user's guide for the client device. Depending on the device, you might need to install a particular driver or file browser before you can install an app.

Procedure

1 Download the Horizon Client app to the device.

   - For a Chromebook device, download Horizon Client from Google Play.

   - For an Android device, download Horizon Client from the Amazon Appstore for Android.

   - For all types of devices, download Horizon Client from the VMware Downloads page at http://www.vmware.com/go/viewclients.

   Note   For some devices, you must download the file to a PC or USB device.

2 If necessary, copy the app (.apk file) to your client device.

3 Install the app according to the client device's customary procedure for installing Android apps.

   For example, on some devices, you must tap the file to install it.

4 Verify that the Horizon app appears on the client device.

What to do next

The first time you start Horizon Client on an Android 6.0 Marshmallow device, the app prompts you to allow Horizon Client to make and manage phone calls, access photos, media, and files, and record audio on your device.

If you installed Horizon Client on a thin client, see Configure Horizon Client in Thin Client Mode.

Configure Workspace ONE UEM to Deliver Horizon Client to Android Devices

You can configure Workspace ONE UEM to deliver Horizon Client to Android device users.

You can optionally configure a list of Connection Server instances, a default Connection Server instance, or application properties. If you configure a list of servers, the servers appear as shortcuts in Horizon Client. If you specify a default server, Horizon Client connects to that server automatically.

If your environment is set up for Android for Work, do not follow this procedure. Instead, see Configure Workspace ONE UEM to Deliver Horizon Client to Android for Work Devices.

Prerequisites

- Install and deploy VMware Workspace ONE UEM. See https://my.workspaceone.com/products/Workspace-ONE-UEM.

- Download the Horizon Client app from the VMware Downloads page at http://www.vmware.com/go/viewclients, from Google Play, or from the Amazon Appstore for Android.

- Become familiar with the Workspace ONE UEM console. For information, see the Workspace ONE UEM product documentation at https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

- Decide which version of Horizon Client to deploy with Workspace ONE UEM. You cannot deploy both the ARM and the x86 version at the same time.

- If you plan to configure application settings, become familiar with the settings and their valid values. See the table in Application Settings.

Procedure

1 Log in to the Workspace ONE UEM console as an administrator.

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

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

4 Create an application profile for Horizon Client.

    a   Select **Apps & Books > Applications > Application Settings > Profiles** and click **Add Profile**.

    b   Select the **SDK Profile** configuration type.

c   Select the **Android** profile type.

d   (Optional) Click **Custom Settings** to configure a list of servers, a default server, or application settings.

To configure a list of servers, specify properties in the `server-list` section. Use the `server` property to specify the IP address or host name of the server, the `username` and `domain` properties to specify the name and domain of a user that is entitled to use the server, and the `description` property to specify a description of the server. The `username`, `domain`, and `description` properties are optional. To configure a default server, specify the `default` property in the `server-list` section. Valid values are `true` or `false`. To configure application settings, specify application properties in the `setting-list` section.

For example:

```
{
  "settings": {
    "server-list":
    [
       {"server":"123.456.1.1","username":"User1","domain":"TestDomain1","description":"View
server 1","default":true},
       {"server":"123.456.1.2","username":"User2","domain":"TestDomain2","description":"View
server 2"},
       {"server":"123.456.1.3","username":"User3","domain":"TestDomain3","description":"View
server 3"},

{"server":"viewserver4.mydomain.com","username":"User4","domain":"TestDomain4","description":"
View server 4"}
    ] ,
    "setting-list":
       {"screen_resolution":"1024*768",
        "send_log_email":"testuser@mail.com",
        "enable_h264":"true",
        "all_monitor":"true",
        "default_startscreen":"recent",
        "ssl_cipher_string":"!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA
+AES",
        "ssl_tls":"tlsv1.1,tlsv1.2",
        "security_mode":"verify",
        "camera":"front",
        "enable_dpi_sync":"true",
        "enable_log":"false"
      }
  }
}
```

5   Upload and add the Horizon Client application.

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

    b   Browse to the Horizon Client app that you downloaded and click **Save** to upload the application.

    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   On the **Deployment** tab, set **Application uses Workspace ONE SDK** to **Yes** and select the SDK profile that you created from the **SDK Profile** drop-down menu.

    f   Publish the Horizon Client application.

6   Install and set up the Workspace ONE UEM Agent on each device.

You can download the Workspace ONE UEM Agent from Google Play or the Amazon Appstore for Android.

7   Use the Workspace ONE UEM console to install the Horizon Client application on the devices.

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

Results

Workspace ONE UEM delivers Horizon Client to the devices in the user group that you associated with the Horizon Client application.

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

What to do next

You can use the Workspace ONE UEM console to edit the Horizon Client application and push those changes to devices.

Configure Workspace ONE UEM to Deliver Horizon Client to Android for Work Devices

You can configure Workspace ONE UEM to deliver Horizon Client to Android for Work device users.

You can optionally configure a list of Connection Server instances, a default Connection Server instance, or application properties. If you configure a list of servers, the servers appear as shortcuts in Horizon Client. If you configure a default server, Horizon Client connects to that server automatically.

Use this procedure only if your environment is set up for Android for Work. If your environment is not set up for Android for Work, see Configure Workspace ONE UEM to Deliver Horizon Client to Android Devices.

Prerequisites

- Verify that your Workspace ONE UEM environment is integrated with Android for Work.

- Install and deploy Workspace ONE UEM. You must install AirWatch Server v8.0 FP02 or later and AirWatch Agent v4.2 or later. See https://my.workspaceone.com/products/Workspace-ONE-UEM. You can download the Workspace ONE UEM Agent from Google Play or the Amazon Appstore for Android.

- Become familiar with the Workspace ONE UEM console. For information, see the Workspace ONE UEM product documentation at https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/index.html.

- Verify that you have a corporate Google account. You must have a corporate Google account to enroll Android for Work devices. For information about the enrollment process, see the Workspace ONE UEM product documentation.

- If you plan to configure application settings, become familiar with the settings and their valid values. See the table in Application Settings.

Procedure

1 Log in to the Workspace ONE UEM Console as an administrator.

2 Create and configure a smart group for your Horizon Client users.

    a Select **Groups and Settings > Groups > Assignment Groups**.

    b Click **Add Smart Group**.

    c Enter the smart group name, select the smart group type, and configure the smart group properties.

    d Click **Save**.

3 Add the Horizon Client application.

    a Select **Apps & Books > Applications > List View**.

    b On the **Public** tab, click **Add Application**.

    c Select **Android** from the **Platform** drop-down menu, click **Search App Store**, enter `com.vmware.view.client.android` in the **Name** text box, and click **Next**.

    d Click **Select** next to the Horizon Client application.

    e Click **Save & Publish**.

4 Assign the Horizon Client application to users and configure the deployment details.

    a Select **Apps & Books > Applications > List View**.

    b On the **Public** tab, click the **Edit** icon next to the Horizon Client application.

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

d   (Optional) On the **Deployment** tab, select a push mode, select the **Send Application Configuration** check box, enter `broker_list` in the **Configuration Key** text box, select **String** from the **Value Type** drop-down menu, and enter a list of servers in the **Configuration Value** text box in JSON format.

To configure a list of servers, specify properties in the `server-list` section. Use the `server` property to specify the IP address or host name of the server, the `username` and `domain` properties to specify the name and domain of a user that is entitled to use the server, and the `description` property to specify a description of the server. The `username`, `domain`, and `description` properties are optional. To configure a default server, specify the `default` property in the `server-list` section. Valid values are `true` or `false`. To configure application settings, specify application properties in the `setting-list` section.

For example:

```
{
  "settings": {
    "server-list":
    [
       {"server":"123.456.1.1","username":"User1","domain":"TestDomain1","description":"View
server 1","default":true},
       {"server":"123.456.1.2","username":"User2","domain":"TestDomain2","description":"View
server 2"},
       {"server":"123.456.1.3","username":"User3","domain":"TestDomain3","description":"View
server 3"},

{"server":"viewserver4.mydomain.com","username":"User4","domain":"TestDomain4","description":"
View server 4"}
    ] ,
    "setting-list":
      {"screen_resolution":"1024*768",
       "send_log_email":"testuser@mail.com",
       "enable_h264":"true",
       "all_monitor":"true",
       "default_startscreen":"recent",
       "ssl_cipher_string":"!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA
+AES",
       "ssl_tls":"tlsv1.1,tlsv1.2",
       "security_mode":"verify",
       "camera":"front",
       "enable_dpi_sync":"true",
       "enable_log":"false"
      }
  }
}
```

e   Click **Save & Publish** to make the Horizon Client application available to end users.

5 Enroll Android for Work devices.

   You use your corporate Google account to enroll the devices.

6 In the Workspace ONE UEM Console, install the Horizon Client application on each device.

Results

Workspace ONE UEM delivers Horizon Client to the Android devices in the smart group that you created.

When a user starts Horizon Client, Horizon Client communicates with the Workspace ONE UEM Agent on the Android device.

If you configured a list of Connection Server instances or a default Connection Server instance, Workspace ONE UEM pushes the server information to the Workspace ONE UEM Agent on the Android devices.

What to do next

You can use the Workspace ONE UEM 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.

Using Embedded RSA SecurID Software Tokens

If you create and distribute RSA SecurID software tokens to end users, users need enter only their PIN, rather than their PIN and a 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 a Connection Server instance with Horizon Client.

Horizon Client also supports file-based provisioning. When a file-based software token is issued to a user, the authentication server generates an XML-format token file called an SDTID file. Horizon Client can import the SDTID file directly. Users can also start Horizon Client by tapping the SDTID file in a file browser.

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 for end users that copy and paste the URL into Horizon Client when Horizon Client is connected to an RSA-enabled Connection Server instance:

- `viewclient-securid://`

- `http://127.0.0.1/securid/`

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

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

Instructions to End Users

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

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

  Instruct 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 receive 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 box of the dialog box.

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

Create a Virtual Smart Card

To use the derived credentials feature, you must create a virtual smart card to use when you log in to a server and connect to a remote desktop. One virtual smart card can hold multiple certificates.

Prerequisites

- Verify that the client device, remote desktops, RDS hosts, Connection Server host, and other Horizon components meet the smart card authentication requirements. See Smart Card Authentication Requirements.

- Import a certificate. You can use a third-party application, such as Purebred, to deliver the certificate to the client device. For an Android device, you can copy a certificate file to the Android device and then import it into the Android system settings.

- For an Android device, verify that the device has a passcode. A passcode is not required to create a virtual smart card on a Chromebook.

Procedure

1 Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2 Tap **Derived Credentials** and then tap **Create new virtual smart card**.

3 (Android device only) Perform device authentication.

4 Enter and confirm a PIN for the virtual smart card.

5 Tap **Continue to import derived credentials** and import the derived credential.

   a Tap **PIV Authentication Certificate**.

   b Select a certificate.

   c Tap **Select**.

6 (Optional) To import a digital signature certificate or encryption certificate after you import the PIV authentication certificate, tap **Digital Signature Certificate** or **Encryption Certificate** and follow the prompts.

7 To create the virtual smart card, tap **Done**.

   The derived credential appears in the **Settings** window. The **Use Derived Credentials** setting is set to on.

8 To create another virtual smart card for a different Horizon environment, tap **Create new virtual smartcard** and repeat these steps.

What to do next

Pair a Virtual Smart Card with Smart Card Middleware.

Pair a Virtual Smart Card with Smart Card Middleware

To use the derived credentials feature, you must create a group policy object (GPO) in Active Directory that pairs a virtual smart card with the smart card middleware installed on the remote desktop. You then apply the GPO to the organizational unit (OU) that contains the remote desktop.

Prerequisites

- Verify that the system requirements for using derived credentials are met. See Smart Card Authentication Requirements.

- Create a Virtual Smart Card.

- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.

- Verify that the MMC and Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1 On the Active Directory server, open the Group Policy Management Console (`gpmc.msc`).

2 Right-click **Group Policy Objects** and select **New**.

3 In the **Name** text box, type a name for the group policy object, for example, `Derived Credentials`, and click **OK**.

4 Right-click the group policy object that you created and select **Edit**.

5 Expand **Computer Configuration > Preferences > Windows Settings** .

6 Right-click **Registry** and select **New > Collection Item**.

7 Change the collection item name from `Collection` to a meaningful name, for example, the middleware name `Charismathics`.

8 To create registry items that pair a virtual smart card with the smart card middleware installed in the remote desktop, right-click the collection item that you created and select **New > Registry Item**.

    To pair a virtual smart card with Charismathics middleware, use the following values.

    - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]`

    - `"ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31`

    - `"Crypto Provider"="Charismathics Smart Security Interface CSP"`

    To pair a virtual smart card with ActivClient middleware, use the following values.

    - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\VMware Remote Smart Card]`

    - `"80000001"="C:\\Program Files\\HID Global\\ActivClient\\ac.scapi.scmd.dll"`

    - `"ATR"=hex:3b,1c,96,56,4d,57,61,72,65,43,61,72,64,23,31`

    - `"ATRMask"=hex:ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff`

    - `"Crypto Provider"="Microsoft Base Smart Card Crypto Provider"`

    - `"Smart Card Key Storage Provider"="Microsoft Smart Card Key Storage Provider"`

9 Open the Group Policy Management Editor and link the new GPO to the OU that contains the remote desktop.

    For a virtual desktop, link the GPO to the OU that contains the virtual desktop. For a published desktop, link the GPO to the OU that contains the RDS host.

10 To verify the registry settings in the remote desktop, restart the remote desktop or open the remote desktop and run `cmd gpudate /force`.

What to do next

Log in to the server and connect to the remote desktop. The process is the same as when you use a physical smart card.

Note If you enter the wrong PIN more than five times when using a virtual smart card to authenticate, the virtual smart card is removed and you must create a new virtual smart card.

Configure Device ID Sharing with OPSWAT

If OPSWAT Mobile App is installed on the client device, you are prompted to share the client device ID when you start Horizon Client. You can also enable or disable device ID sharing by configuring a setting in Horizon Client.

Prerequisites

Configure OPSWAT integration. See OPSWAT Integration Requirements.

Procedure

1   Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window and tap **Share Device ID with OPSWAT**.

2   Tap to toggle the **Share Device ID with OPSWAT** option to on or off.

If you toggle the setting to off, the setting is disabled and Horizon Client prompts you to share the device ID the next time you start Horizon Client.

If you toggle the setting to on, you must select one of the following options.

Option	Description
Share	Horizon Client shares the device ID with OPSWAT. OPSWAT verifies the client device's security status and sends a compliance report to the MetaAccess server. If the client device is already registered with OPSWAT, it is enrolled successfully. If the device is not registered with OPSWAT, an error message appears and the device is not enrolled. To return to Horizon Client, tap **Return**.
Never ask again	Horizon Client does not share the device ID with OPSWAT and it does not prompt you to share the device ID again.
Cancel	Horizon Client prompts you to share the device ID the next time you start Horizon Client.

Configure Advanced TLS Options

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

By default, TLS v1.1 and TLS v1.2 are enabled. SSL v2.0, SSL v3.0, and TLS v1.0 are not supported. The default cipher control string is "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".

If you configure a security protocol for Horizon Client that is not enabled on the server to which the client system connects, a TLS error occurs and the connection fails.

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

Procedure

1   Open **Settings** and tap **Security options**.

- If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon to access **Settings**.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar.

- If you are not connected to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2   Tap **Advanced SSL Options**.

3   Verify that **Use Default Settings** is deselected.

4   To enable or disable a security protocol, tap the check box next to the security protocol name.

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

6   (Optional) To revert to the default settings, tap to select the **Use Default Settings** option.

7   To save your changes, tap **OK**.

Results

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

Configure VMware Blast Options

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

You cannot configure VMware Blast settings after you connect to a server.

JPG/PNG encoding is always used in multi-monitor mode, even when H.264 decoding is enabled.

Prerequisites

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

Procedure

1   Start Horizon Client.

2   Before you log in to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window and tap **VMware Blast**.

    You cannot configure VMware Blast settings after you log in to a server.

3   To allow H.264 decoding in Horizon Client, tap and toggle the **H.264** option to on.

    When this option is selected (the default setting), Horizon Client uses H.264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. When this option is deselected, Horizon Client uses JPG/PNG decoding.

Results

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

Configure Seamless Window Mode on a Chromebook Device

When Horizon Client for Android is installed on a Chromebook device, you can enable or disable seamless window mode. Seamless window mode is enabled by default. This feature requires Chrome OS M64 or later.

When you start a published application in seamless window mode, only the published application's window is visible and you interact with the application as if it were running on your local client device. When seamless window mode is disabled, both the published application and its desktop are visible.

Seamless window mode has the following limitations.

■   Only one external display is supported.

■   You can have a maximum of four published applications open at the same time.

■   USB redirection is not supported.

■   H.264 decoding is not supported in VMware Blast sessions.

■   The session prelaunch feature is not supported.

Procedure

1   Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2   Tap **Seamless window** and select or deselect **Seamless window**.

Configure Horizon Client in Thin Client Mode

You can configure Horizon Client to work on a thin client.

Prerequisites

Install Horizon Client on the thin client. For thin client requirements, see System Requirements for Thin Clients.

Procedure

1   Start Horizon Client on the thin client.

2   Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

3   Tap **Thin Client mode** and enable **Thin Client mode**.

What to do next

See Using Horizon Client on a Thin Client.

Using Horizon Client on a Thin Client

Some features are different or unavailable when you use Horizon Client in thin client mode.

- The Horizon Client window resolution is set to **Auto-fit** by default. The auto-fit resolution is the same as the thin client's HDMI output. For example, if the thin client supports HDMI 4K output, the auto-fit resolution is 4K. If the thin client supports HDMI 1080p output, the auto-fit resolution is 1920x1080. You can downscale the resolution by modifying the Horizon Client **Resolution** setting.

- The Horizon Client **Presentation Mode** and **Stay Awake** display settings are not available.

- You cannot modify the Horizon Client **Keyboard** settings.

- The Horizon Client Tools radial menu is not available in remote desktops and published applications.

- In general, the gestures you use in Horizon Client depend on the thin client model and the type of external input device that you use with the thin client. For example, you might have a keyboard, mouse, remote control, or game controller. See the documentation for the external input device for more information.

- The Unity Touch sidebar contains **Keyboard**, **Settings**, and **Disconnect** icons. For more information, see Using the Unity Touch Sidebar with a Remote Desktop and Using the Unity Touch Sidebar with a Published Application.

- The Unity Touch sidebar is supported on Remix Mini and NVIDIA SHIELD Android TV devices. The Unity Touch sidebar is not supported on Amazon Fire TV.

- If you are connected to a remote desktop or published application from an Amazon Fire TV device, you must use a pop-up menu to display Horizon Client Settings and to disconnect from the remote desktop or published application. On a remote control or external keyboard, press the **Menu** button to display the pop-up menu.

Using the Google Admin Console to Configure Enrolled Chromebook Devices

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

You can configure a list of Connection Server instances, a default Connection Server instance, and certain application settings.

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

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

You can install Horizon Client only on certain Chromebook models. For information, see System Requirements for Chromebooks.

Connection Server Instance List

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

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

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

```
{
  "broker_list": "{\"settings\": {\"server-list\": [{\"server\": \"123.456.1.1\",\"description
\":\"View Server 1\",\"username\": \"User1\",\"domain\": \"TestDomain1\"},{\"server
\":\"123.456.1.2\",\"description\": \"View Server 2\",\"username\": \"User2\",\"domain\":
\"TestDomain2\"}, {\"server\": \"123.456.1.3\",\"description\": \"View Server 3\",\"username\":
\"User3\",\"domain\": \"TestDomain3\"}, {\"server\": \"viewserver4.mydomain.com\",\"description\":
\"View Server 4\",\"username\": \"User4\",\"domain\": \"TestDomain4\"}]}}"
}
```

Default Connection Server Instance

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

The following JSON configuration file example shows a default server.

```
{
 "broker_list": "{\"settings\": {\"server-list\": [{\"server\": \"123.456.1.1\",\"description\":
\"View Server 1\",\"default\": true,\"username\": \"User1\",\"domain\": \"TestDomain1\"}]}}"
 }
```

Application Settings

You can use properties in the `setting-list` section to configure application settings. All the properties are optional.

Property	Description
`screen_scaling`	Configures display scaling. Valid values are "1/2", "2/3", "3/4", "Auto-fit", or "No Scaling".
`screen_resolution`	Configures the screen resolution. Valid values are "1024*768", "1280*1024", "1600*1200", "Auto-fit", or "No Scaling".
`enable_log`	Enables or disables the log collection feature. Valid values are "true" or "false".
`send_log_email`	The email address, for example, "`testuser@mail.com`", to send log files. This email address appears in the **To:** field by default when a user uses the log collection feature. See Manually Retrieve and Send Horizon Client Log Files.
`all_monitor`	Enables or disables multiple-monitor mode. Valid values are "`true`" or "`false`".
`default_startscreen`	Configures the Horizon Client default view. Valid values are "`recent`" or "`servers`".
`ssl_tls`	Configures the security protocol, or protocols, that Horizon Client uses. Valid values are "`tlsv1.1`", "`tlsv1.2`", or "`tlsv1.1,tlsv1.2`". If you specify this property without a valid value, "`tlsv1.1,tlsv1.2`" is used.
`ssl_cipher_string`	Specifies the default TLS cipher control string.
`security_mode`	Configures the certificate checking mode. Valid values are "`verify`", "`warn`", or "`don't verify`".
`enable_h264`	Enables or disables H.264 decoding. Valid values are "`true`" or "`false`".
`enable_dpi_sync`	Enables or disables the DPI synchronization feature. Valid values are "`true`" or "`false`".

Property	Description
camera	Specifies whether to use the front or back camera on the device. Valid values are "front" or "rear".
enable_unauthenticated_access	Enables or disables the Unauthenticated Access feature. Valid values are "true" or "false".

The following JSON configuration file example includes application properties in the setting-list section.

```
{
  "broker_list": "{\"settings\": {\"server-list\": [{\"server\": \"123.456.1.1\",\"description
\":\"View Server 1\",\"username\": \"User1\",\"domain\": \"TestDomain1\"}, {\"server
\":\"123.456.1.2\",\"description\": \"View Server 2\",\"username\": \"User2\",\"domain\":
\"TestDomain2\"}, {\"server\": \"123.456.1.3\",\"description\": \"View Server 3\", \"username\":
\"User3\",\"domain\": \"TestDomain3\"}, {\"server\": \"viewserver4.mydomain.com\",\"description\":
\"View Server 4\",\"username\": \"User4\",\"domain\": \"TestDomain4\"}],\"setting-list\":
{\"screen_resolution\":\"1024*768\",\"send_log_email\":\"testuser@mail.com\",\"enable_h264\":\"true
\",\"all_monitor\":\"true\",\"default_startscreen\":\"recent\", \"ssl_cipher_string\":\"!aNULL:kECDH
+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES\",\"ssl_tls
\":\"tlsv1.1,tlsv1.2\",\"security_mode\":\"verify\",\"camera\":\"front\",\"enable_dpi_sync\":\"true
\",\"enable_log\":\"false\", \"enable_unauthenticated_access\":\"true\"}}}"
}
```

Configure the Horizon Client Default View

You can configure whether recently used remote desktops and published applications shortcuts, or server shortcuts, appear when you start Horizon Client.

Procedure

1 Open **Settings** and tap **Display**.

- If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon to access **Settings**.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper right corner of the Horizon Client toolbar.

- If you are not connected to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2 Tap **Default launch view**.

3   To select the default view, tap an option.

Option	Description
Recent	The **Recent** tab appears when you start Horizon Client. The Recent tab contains shortcuts to recently used remote desktops and published applications. This is the default setting.
Servers	The **Servers** tab appears when you start Horizon Client. The Servers tab contains shortcuts to the servers that you added to Horizon Client.

Results

The default view that you selected takes effect immediately.

Configure Horizon Client Data Sharing

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

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

Data sharing is enabled by default in Horizon Client. You must configure the data sharing setting before you connect to a server. The setting is applied to all servers. You cannot change the Horizon Client data sharing setting after you connect to a server.

Procedure

1   Tap the **Settings** (gear icon) in the upper-right corner of the Horizon Client window and tap **Allow data sharing**.

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

Horizon Client Data Collected by VMware

If a Horizon administrator has opted to participate in the customer experience improvement program, and data sharing is enabled on the client system, VMware collects data about the client system.

VMware collects data about client systems to prioritize hardware and software compatibility. If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to respond better to customer requirements. VMware does not collect data that identifies your organization. Horizon Client information is sent first to the Connection Server instance and then to VMware, along with data about Connection Server, desktop pools, and remote desktops.

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

A Horizon administrator can select whether to participate in the VMware customer experience improvement program when installing Connection Server or by setting an option in Horizon Console after the installation.

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

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

Using URIs to Configure Horizon Client

<div style="text-align: right; font-size: 3em; color: gray;">2</div>

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

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

- Server address

- Port number for the server

- Active Directory user name

- RADIUS or RSA SecurID user name, if different from the Active Directory user name

- Domain name

- Remote desktop or published application display name

- Actions including reset, log out, and start session

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

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

This chapter includes the following topics:

- Syntax for Creating vmware-view URIs

- Examples of vmware-view URIs

Syntax for Creating vmware-view URIs

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

URI Specification

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

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

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

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

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

authority-part

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

To specify a user name, use the following syntax.

```
user1@server-address
```

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

To specify a port number, use the following syntax.

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

path-part

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

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

If you specify a desktop or application ID, you must use only lowercase letters, even if the desktop or application ID contains uppercase letters in ADSI Edit.

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

query-part

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

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

Supported Queries

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

action

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

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

args

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

- For a colon (:), use **%3A**

- For a back slash (\), use **%5C**

- For a space ( ), use **%20**

- For a double quotation mark ("), use **%22**

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

appProtocol

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

defaultLaunchView

Sets the default view for when Horizon Client starts. 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

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

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, Horizon Client uses the Windows user name. The syntax is **tokenUserName=***name*.

unauthenticatedAccessEnabled

If this option is set to **true**, the Unauthenticated Access feature is enabled by default. If this option is set to **false**, the Unauthenticated Access feature is disabled. When this option is set to **""**, the Unauthenticated Access feature is disabled. The **Log in anonymously using Unauthenticated Access** option is available in the Horizon Client settings. An example of the syntax is **unauthenticatedAccessEnabled=true**.

unauthenticatedAccessAccount

If the Unauthenticated Access feature is enabled, sets the account to use. If Unauthenticated Access is disabled, then this query is ignored. An example of the syntax using the **anonymous1** user account is **unauthenticatedAccessAccount=anonymous1**.

Examples of vmware-view URIs

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

URI Syntax Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10   `vmware-view://view.mycompany.com?action=reset`

Horizon Client starts 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 shows a dialog box that prompts the user to confirm the reset operation for all remote applications.

11   `vmware-view://`

If Horizon Client is already running, it comes to the foreground. If Horizon Client is not running, it starts.

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

Horizon Client starts and the user sees the **Recent** tab.

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

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

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

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

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

15   `vmware-view://view.mycompany.com/Notepad?`
       `unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1`

Horizon Client starts and connects to the `view.mycompany.com` server using the `anonymous1` user account. The Notepad application starts without prompting the user to provide login credentials.

HTML Code Examples

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

```
<html>
<body>

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

<form><input type="button" value="TestButton" onClick="window.location.href=
```

```
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Managing Remote Desktop and Published Application Connections

3

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

Depending on how you configure policies for remote desktops, end users might be able to perform many operations on their remote desktops.

This chapter includes the following topics:

- Setting the Certificate Checking Mode in Horizon Client

- Connect to a Remote Desktop or Published Application

- Use Unauthenticated Access to Connect to Published Applications

- Share Access to Local Storage with Client Drive Redirection

- Add a Shortcut to the Android Home Screen or Chrome App Launcher

- Manage Server Shortcuts

- Select a Favorite Remote Desktop or Published Application

- Switch Remote Desktops or Published Applications

- Reconnecting to a Remote Desktop or Published Application

- Disconnecting From a Remote Desktop or Published Application

- Log Off From a Remote Desktop

- Disconnecting From a Server

- Manage Remote Desktop and Published Application Shortcuts

- Using Android 7.0 Nougat Multi-Window Modes with Horizon Client

- Using Horizon Client with Samsung DeX

Setting the Certificate Checking Mode in Horizon Client

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license.

Server certificate checking includes the following checks:

- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?

- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?

- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.

- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA. To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

For information about distributing a self-signed root certificate that users can install on their client devices, and instructions for installing a certificate on an Android or Chromebook device, see the documentation for the device.

To set the certificate checking mode, start Horizon Client, tap the Settings (gear) icon in the upper-right corner of the Horizon Client window, tap **Security options**, and tap **Security mode**. You can select one of the following options.

- **Never connect to untrusted servers**. This setting means that you cannot connect to the server if any of the certificate checks fail. An error message lists the checks that failed.

- **Warn before connecting to untrusted servers**. This setting means that you can click **Continue** to ignore the warning if a certificate check fails because the server uses a self-signed certificate. For self-signed certificates, the certificate name is not required to match the server name that you entered in Horizon Client. You can also receive a warning if the certificate has expired.

- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

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

Connect to a Remote Desktop or Published Application

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

Before you have end users access their remote desktops and published applications, test that you can connect to a remote desktop or published application from a client device. You might need to specify a server and supply credentials for your user account.

Prerequisites

- Obtain credentials for logging in, such as an Active Directory user name and password, RSA SecurID user name and passcode, RADIUS authentication credentials, or smart card personal identification number (PIN).

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

- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.

- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.

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

- 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.

- Configure the certificate checking mode for the certificate presented by the server. See Setting the Certificate Checking Mode in Horizon Client.

- If you plan to use fingerprint authentication, verify that the Fingerprint Authentication option is enabled and at least one fingerprint is enrolled on the client device. For complete fingerprint authentication requirements, see Fingerprint Authentication Requirements.

Procedure

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

2 Open the **Horizon** app.

3 Connect to a server.

Option	Action
Connect to a new server	Enter the name of a server, enter a description (optional), and tap **Connect**. If a server has already been added, tap the plus sign (**+**) icon in the upper-right corner of the window instead.
Connect to an existing server	Tap the server shortcut on the **Servers** tab.

Connections between Horizon Client and servers always use TLS. The default port for TLS connections is 443. If the server is not configured to use the default port, use the format *servername*:*port*, for 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 the smart card has only one certificate, that certificate is already selected. If there are many certificates, you can scroll through the certificates.

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

Option	Action
Use an 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 a software token	a Tap **External Token**. b In the Install Software Token dialog box, paste the CT-KIP URL or CTFString URL that your system administrator sent to you in email. If the URL contains an activation code, you do not need to enter a value 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 that you entered before. 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   If you are prompted for a user name and password, supply your Active Directory credentials.

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

b   Select a domain.

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

c   (Optional) If the **Enable Fingerprint** check box is available, select it to use fingerprint authentication.

The **Enable Fingerprint** check box is available only if biometric authentication is enabled on the server and you have not previously authenticated with fingerprint authentication.

d   (Optional) Select the **Save Password** check box if your system administrator has enabled this feature and if the server certificate can be fully verified.

If you are saving a password for the first time, you are prompted to activate the device administrator, which is required to save a password on client devices.

e   Tap **Login**.

If fingerprint authentication is enabled and you are logging in for the first time, your Active Directory credentials are stored securely in the client device's database for future use.

8   If you are prompted for fingerprint authentication, place your finger on the fingerprint sensor.

If you do not want to use fingerprint authentication, tap **Cancel**. You can connect to the server again and tap **Use password** to enter a user name and password.

9   (Optional) To select the display protocol to use, tap the **Switch Protocol** icon in the upper-right corner of the desktop and application selector window.

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

10   Tap a remote desktop or published application to connect to it.

If you are connecting to a published desktop, and if the desktop is already set to use the Microsoft RDP display protocol, you cannot connect immediately. You are prompted to have the system log you off the remote operating system so that a connection can be made with the PCoIP display protocol or the VMware Blast display protocol.

Results

If you are using Horizon Client on a Chromebook, or on an Android device in DeX desktop mode, the remote desktop or published application starts in a new window instead of in the original window. The desktop and application selector window remains open so that you can connect to multiple remote desktops and published applications. If you open a new published application, Horizon Client opens all previous published application sessions. You can have a maximum of four remote sessions open at the same time.

After you connect to a remote desktop or published application for the first time, Horizon Client saves a shortcut for the remote desktop or published application on the **Recent** tab. The next time you connect to the remote desktop or published application, you can tap the shortcut instead of tapping the server shortcut.

Use Unauthenticated Access to Connect to Published Applications

A Horizon administrator can create Unauthenticated Access users and entitle those users to published applications on a particular server. Unauthenticated Access users can log in to the server anonymously to connect to their published applications.

Before you have end users access a published application with the Unauthenticated Access feature, test that you can connect to the published application from a client device. You might need to specify a server and supply credentials for the user account.

Prerequisites

- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.

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

- Configure the certificate checking mode for the certificate presented by the server. See Setting the Certificate Checking Mode in Horizon Client.

- If you are accessing published applications outside of the corporate network, verify that the client device is set up to use a VPN connection and turn on that connection.

Procedure

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

2 Open the **Horizon** app.

3 Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window, tap **Unauthenticated access**, and tap to toggle the **Unauthenticated access** option to on.

4 Connect to the server on which you have unauthenticated access to published applications.

Option	Description
Connect to a new server	Enter the name of a server, enter a description (optional), and tap **Connect**. If a server has already been added, tap the plus sign (+) icon in the upper-right corner of the window instead.
Connect to an existing server	Tap the server shortcut on the **Servers** tab.

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

5 When the login window appears, select a user account from the **User account** drop-down menu, if required.

If only one user account is available, that account is automatically selected.

6 (Optional) Select **Always use this account** to bypass the login window the next time you connect to the server.

To deselect this setting before you connect to the server the next time, touch and hold the server shortcut until the context menu appears, tap **Edit**, tap **Forget the saved Unauthenticated Access account (*name*)**, and tap **Done**.

7 Tap **Login** to log in to the server.

The application selection window appears.

8 Tap a published application icon to start the published application.

Results

After you connect to a published application for the first time, Horizon Client saves a shortcut for the published application on the **Recent** tab. The next time you connect to the published application, you can tap the shortcut instead of tapping the server icon.

Share Access to Local Storage with Client Drive Redirection

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

In a Windows remote desktop or published application, local storage appears in the **Devices and drives** section in the **This PC** folder, or in the **Other** section in the **Computer** folder. The folders and storage devices that you select for sharing use the naming format *name* **on HorizonClient**.

Prerequisites

- Enable the client drive redirection feature. This task involves enabling the agent **Client Drive Redirection** option. It can also include setting policies or registry settings to control client drive redirection behavior. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

- Connect to the remote desktop or published application with which you want to share local storage. If you have not logged in at least once, become familiar with the procedure Connect to a Remote Desktop or Published Application .

Procedure

1 Open **Settings** and tap **Local storage redirection**.

- If you are connected to the remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar.

2 Tap **Local Storage Redirection** and configure the local storage redirection options.

Option	Action
Share all removable storage devices automatically	Select **Enable auto direct for mounted storage**. All removable storage devices mounted to your device are shared with the remote desktop or published application automatically. This option is selected by default.
Do not share all removable storage devices automatically	Deselect **Enable auto direct for mounted storage**. The next time you connect to the remote desktop or published application, removable storage devices mounted to your device are not shared with the remote desktop or published application automatically. **Note** Deselecting **Enable auto direct for mounted storage** does not stop sharing a removable storage device that is already shared with the remote desktop or published application.
Share a specific folder or removable storage device	Select the name of the local folder or removable storage device in the list. The device becomes available in the remote desktop or published application. When you connect a removable storage device, its name appears in the list. When you disconnect a removable storage device, its name is removed from the list.
Stop sharing a specific folder or removable storage device	Deselect the name of the local folder or removable storage device in the list. The device is no longer available in the remote desktop or published application.

3 Tap **OK** to save your settings.

What to do next

Verify your changes in the remote desktop or published application.

- In a Windows remote desktop, open the **This PC** folder and look in the **Devices and drives** section, or open the **Computer** folder and look in the **Other** section. If you shared a folder or storage device, you should see the folder or device. Shared folders and storage devices use the naming format *name* **on HorizonClient**.

- In a published application, select **File > Open** or **File > Save As**, if applicable. If you shared a folder or storage device, you should be able to navigate to the folder or device. Shared folders and storage devices use the naming format *name* **on HorizonClient**.

Add a Shortcut to the Android Home Screen or Chrome App Launcher

When Horizon Client is installed on an Android device, you can add a shortcut for a remote desktop or published application to the Android home screen and then tap the shortcut to open the remote desktop or published application. When Horizon Client is installed on a Chromebook device, Horizon Client adds the remote desktop or published application shortcut to the Chrome App Launcher.

VMware Horizon Client for Android Installation and Setup Guide

On Android 5, 6, and 7 devices, Horizon Client adds the remote desktop or published application shortcut to the Android home screen.

On Android 8 devices, remote desktop and published application shortcuts appear as entries above the **Horizon** app icon when you touch and hold the app icon. You can drag an entry from the app icon to the Android home screen to create a shortcut directly on the Android home screen.

This feature is not available on Amazon devices, on Android devices that Workspace ONE UEM manages, or when you use the Unauthenticated Access feature to connect to the server anonymously.

Procedure

1   You can add a remote desktop or published application shortcut before or after you connect to a server.

    If you are not connected to a server, you must have connected to the remote desktop or published application at least once from the device so that a shortcut for the remote desktop or published application appears on the **Recent** tab.

Option	Action
You are not connected to a server	On the **Recent** tab, touch and hold the shortcut until **Add To Home** appears at the bottom of the window and then drag the shortcut to **Add To Home**.
You are connected to a server	On the **All** or **Favorites** tab, touch and hold the remote desktop or published application shortcut until the context menu appears and tap **Add To Home**.

2   Type a name for the shortcut and tap **OK**.

    If the name is longer than 12 characters, the extra characters do not appear in the shortcut.

3   In the Add to Home screen dialog box, tap **Add automatically**, or touch and hold the shortcut to place it manually.

Manage Server Shortcuts

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

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

Server shortcuts can appear on multiple pages and you can swipe across pages to see more shortcuts. Horizon Client creates pages, as needed, to accommodate all your server shortcuts.

Procedure

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

2   Use the context menu to delete or modify the server shortcut.

You can edit the server name, server description, and user name. You can also remove a credential that was saved for fingerprint authentication by tapping **Remove Credential**.

Select a Favorite Remote Desktop or Published Application

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

Prerequisites

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

Procedure

1   On the **Servers** tab, tap the server shortcut 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   To select or deselect a favorite remote desktop or published application, perform these steps.

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

4   (Optional) To see only favorite remote desktops or published applications, tap the **Favorites** tab.

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

Switch Remote Desktops or Published Applications

If you use a Chromebook device, or an Android device in DeX desktop mode, you can have multiple remote desktops and published applications open at the same time, and you can switch between them.

Procedure

◆ To select a different remote desktop or published application on the same server, tap the new remote desktop or published application shortcut in the desktop and application selector window.

The remote desktop or published application opens in a new window. You now have multiple windows open and you can switch between them.

Note If the new published application is in the same farm as the current application, the new published application opens in the same window.

◆ To select a different remote desktop or published application on a different server, tap the **Disconnect** icon in the upper-right corner of the desktop and application selector window and tap **Log Out** to disconnect from the server.

You can now connect to a different server and open a new remote desktop or published application.

Reconnecting to a Remote Desktop or Published Application

For security purposes, a Horizon administrator can set timeouts that log you off a server and lock a published application after some period of inactivity.

By default, you must log in again if you have Horizon Client open and are connected to a particular server for more than 10 hours. This timeout applies to both remote desktop and published application connections.

You receive a warning prompt 30 seconds before a published application is locked automatically. If you do not respond, the published application is locked. By default, the timeout occurs after 15 minutes of inactivity, but a Horizon administrator can change the timeout period.

For example, if you have one or more published applications open and you walk away from your computer, the published application windows might no longer be open when you return an hour later. Instead, you might see a dialog box that prompts you to click **OK** so that the published application windows appear again.

To configure these timeout settings in Horizon Console, select **Settings > Global Settings**, click the **General Settings** tab, and click **Edit**.

On a Chromebook or an Android device in DeX desktop mode, if you navigate to the desktop and application selector window and one or more published application sessions are disconnected, Horizon Client prompts you to reconnect to the sessions. You can click **Reconnect to applications** to open the published application sessions, or click **Not now** to close the message. You can also select a check box not to show the message again.

Disconnecting From a Remote Desktop or Published Application

When you are logged in to a remote desktop, you can disconnect without logging off so that applications remain open in the remote desktop. You can also disconnect from a published application so that the published application remains open.

To disconnect from a remote desktop or published application that is in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the **Disconnect** icon. The Horizon Client Tools radial menu icon appears at the right edge of the window when you are connected to a remote desktop or published application. For more information, see Using the Horizon Client Tools on a Mobile Device.

If you are not using full-screen mode, tap **Disconnect** in the menu in the upper-right corner of the Horizon Client toolbar.

On a thin client, disconnect by clicking the **Disconnect** icon in the Unity Touch sidebar or in a pop-up menu, depending on your thin client model. For more information, see Using Horizon Client on a Thin Client.

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

Log Off From a Remote Desktop

You can log off from a remote desktop, even if the remote desktop is not open in Horizon Client. If the remote desktop is open in Horizon Client, you can use the Windows **Start** menu to log off.

Prerequisites

Obtain credentials for logging in, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.

Procedure

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

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

3   Touch and hold the remote desktop shortcut until the context menu appears.

    You can perform this step from either the **All** or **Favorites** tab.

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

Results

The remote desktop is disconnected after you are logged off. Any unsaved files that are open on the remote desktop are closed during the log out operation.

What to do next

Disconnect from the server. See Disconnecting From a Server.

Disconnecting From a Server

After you have finished using a remote desktop or published application, you can disconnect from the server.

To disconnect from a server, tap the Back button. Alternatively, tap the **Log Out** icon in the upper-right corner of the desktop and application selector window and tap **Log Out**.

Manage Remote Desktop and Published Application Shortcuts

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

If you have many remote desktop and published application shortcuts, the shortcuts might appear on multiple pages. You can swipe across the pages to see more shortcuts. Horizon Client creates pages, as needed, to accommodate all your shortcuts.

Procedure

◆ To remove a remote desktop or published application shortcut from the **Recent** tab, perform these steps.

  a Touch and hold the shortcut until **Remove Shortcut** appears at the bottom of the window.

  b Drag the shortcut to **Remove Shortcut**.

◆ To move a remote desktop or published application shortcut, touch and hold the shortcut and drag it to the new location.

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

Using Android 7.0 Nougat Multi-Window Modes with Horizon Client

Android 7.0 Nougat allows several apps to share the screen at the same time. You can use split-screen mode with Horizon Client on an Android 7.0 Nougat device. Horizon Client does not support picture-in-picture mode.

With split-screen mode, you can run Horizon Client and another app side by side, or one above the other. A dividing line separates the two apps, and you can make one app larger and the other app smaller.

Using Horizon Client with Samsung DeX

If the Android device supports Samsung DeX, you can use Horizon Client in DeX desktop mode.

When the device is in DeX desktop mode, Horizon Client treats the device as a thin client and **Thin Client mode** is enabled. For more information, see Using Horizon Client on a Thin Client.

The following features are supported when you use Horizon Client in Horizon DeX desktop mode.

- You can configure Horizon Client to start automatically when you switch to DeX desktop mode. See Enable the DeX Mode Auto Launch Feature.

- Remote desktop and published application sessions continue to run after you enter or exit DeX desktop mode.

- If Horizon Client is maximized, remote desktops enter full-screen mode after you switch to DeX desktop mode.

- To switch the language input method in a remote desktop, you can use the language switch key on a Samsung physical keyboard.

- You can connect to multiple remote desktops and published applications at the same time. Smart card authentication is not supported for multiple sessions.

Enable the DeX Mode Auto Launch Feature

You can configure Horizon Client to start automatically when you switch the Android device to DeX desktop mode. The DeX mode auto launch feature is disabled by default.

Prerequisites

- Verify that the Android device supports Samsung DeX.

- Verify that a default server is not configured for Horizon Client. You cannot enable the DeX mode auto launch feature if a default server is configured.

Procedure

1 Before you log in to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2 Tap **Display**, tap **Dex Mode Auto Launch**, and tap to toggle the **Dex Mode Auto Launch** option to on.

Results

If you added a remote desktop or published application shortcut to the Android home screen, Horizon Client connects to the most recent shortcut after Horizon Client starts. For information about adding shortcuts to the Android home screen, see Add a Shortcut to the Android Home Screen or Chrome App Launcher.

Using a Microsoft Windows Desktop or Application

4

Horizon Client includes additional features to aid in navigation on Android devices, thin clients, and Chromebook devices. Users can use external devices with remote desktops and published applications, copy text and images from client devices to remote desktops and published applications, and save documents in published applications.

This chapter includes the following topics:

- Feature Support for Horizon Client for Android Clients
- Input Devices, Keyboards, and Keyboard Settings
- Using the Real-Time Audio-Video Feature
- Using Native Operating System Gestures with Touch Redirection
- Using the Unity Touch Sidebar with a Remote Desktop
- Using the Unity Touch Sidebar with a Published Application
- Using the Horizon Client Tools on a Mobile Device
- Gestures
- Multitasking
- Copying and Pasting Text and Images
- Dragging Text and Image Files
- Printing From a Remote Desktop or Published Application
- Use USB Devices in a Remote Desktop or Published Application
- Saving Documents in a Published Application
- Use Multiple Sessions of a Published Application From Different Client Devices
- Screen Resolutions and Using External Displays
- Using DPI Synchronization
- PCoIP Client-Side Image Cache
- Using International Keyboards

Feature Support for Horizon Client for Android Clients

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

Supported Windows Virtual Desktops

Windows virtual desktops are single-session virtual machines.

This version of Horizon Client works with Windows virtual desktops that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows 7, Windows 8.x, and Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 virtual desktops require Horizon Agent 7.7 or later.

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

Supported Published Desktops on RDS Hosts

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

This version of Horizon Client works with RDS hosts that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 RDS hosts require Horizon Agent 7.7 or later.

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

Requirements for Specific Remote Desktop Features

Some remote desktop features have specific requirements or limitations.

- The VMware Integrated Printing feature requires Horizon Agent 2006 or later.

- The VMware Integrated Printing feature is supported only with Windows 10, Windows Server 2016, and Windows Server 2019 remote desktops. Windows 7, Windows 8.x, and Windows Server 2012 R2 remote desktops cannot use this feature.

- Because of device and operating system limitations, certain Horizon Client features work only on an Android device, and certain features work only on a Chromebook device. These limitations are mentioned where the features are described in this document.

Supported Linux Desktops

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

Input Devices, Keyboards, and Keyboard Settings

You can use Bluetooth and docked keyboard devices and keyboards with remote desktops and published applications. You can also set preferences for settings, such as auto-capitalization and text correction.

Using External Keyboards and Input Devices

For information about the devices that a specific tablet supports, see the documentation from the tablet manufacturer.

For some external keyboards, Horizon Client detects the keyboard automatically. For other external keyboards, you must either tap the tablet screen with three fingers at the same time, or tap the **Keyboard** icon, to detect the keyboard. If you are using a remote desktop or published application in full-screen mode, the **Keyboard** icon is in the Horizon Client Tools radial menu. If you are not using full-screen mode, the **Keyboard** icon is on the Horizon Client toolbar.

Note On Kindle Fire tablets, tapping with three fingers does not display the onscreen keyboard. You can instead use the **Keyboard** icon to show the onscreen keyboard.

After Horizon Client detects the external keyboard, you might not be able to use the Horizon Client Tools or three-finger tap to show the onscreen keyboard. You might first need to deactivate the external keyboard by pressing its **Eject** key.

Using International Onscreen Keyboards

With the correct input methods installed, you can input characters for English-United States, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, and Spanish.

To select a language for the keyboard or voice, tap the Keyboard Settings key on the onscreen keyboard. The Keyboard Settings key is the left-most key on the bottom row of the onscreen keyboard. After you finish selecting settings, tap the **Back** button to close the dialog box.

Using a Stylus

For all Android devices that support a stylus, you can use a stylus in remote desktops and published applications. For example, you can use a stylus in remote desktops and published applications on a Samsung Galaxy S4. For full functionality, use the VMware Blast display protocol when you connect to the remote desktop or published application. If you use the PCoIP display protocol, the stylus behaves the same way as finger touch.

Using the Real-Time Audio-Video Feature

With the Real-Time Audio-Video feature, you can use the client device's built-in cameras and microphones in a remote desktop or published application. Real-Time Audio-Video is compatible 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 the client device.

For information about setting up the Real-Time Audio-Video feature for remote desktops and published applications, see the *Configuring Remote Desktop Features in Horizon* document.

When you install Horizon Client on an Android 6 or later device, Horizon Client prompts you for permission to access the camera and microphone. You must grant permission for the camera and microphone to work with the remote desktop or published application. You can enable or disable access to the camera or microphone in the Android Settings app. For Android devices earlier than Android 6, permission to the camera and microphone is opened by default.

When the camera is being used by another app, the remote desktop or published application cannot use the camera simultaneously. Also, when the remote desktop or published application is using the camera, the client device cannot use the camera at the same time.

If the client device has both a front and a back camera, you can select which camera to use in the remote desktop or published application. If you are using full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, tap **Camera**, tap **Select a camera**, and tap the camera to use. If you are not using full-screen mode, tap **Settings** in the upper-right corner of the Horizon Client toolbar. The **Camera** setting is available only when the camera is started.

Using Native Operating System Gestures with Touch Redirection

With the touch redirection feature, you can use native operating system gestures from a touch-based mobile device in a remote desktop or published application. For example, you can touch, hold, and release an item on a Windows 8.1 remote desktop to display the item's context menu.

When touch redirection is enabled, 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 most remote desktops.

To disable touch redirection, open **Settings**, tap **Touch**, and toggle the **Windows native touch gestures** setting to off. If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon. If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar. If you are not connected to a remote desktop or published application, tap the gear icon in the upper right corner of the Horizon Client window.

Using the Unity Touch Sidebar with a Remote Desktop

You can quickly navigate to an application or file in a remote desktop from the 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.

The Unity Touch feature is available only if a Horizon administrator has enabled it. If users have a floating desktop, users' favorite applications and files can be saved only if Windows roaming user profiles are configured for the remote desktop. A Horizon administrator can also create a default **Favorite Applications** list that end users see the first time the sidebar appears. For more information, see "Configuring Unity Touch" in the *Configuring Remote Desktop Features in Horizon* document.

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

If the Unity Touch sidebar is closed, a tab appears on the left side of the window. You can swipe this tab to the right to open the sidebar. You can also slide the tab up or down.

From the Unity Touch sidebar, you can perform many actions in a remote desktop.

Table 4-1. Unity Touch Sidebar Actions for a Remote Desktop

Action	Procedure
Show or hide the onscreen keyboard	(Thin client only) Select the **Keyboard** icon.
Change the Horizon Client settings	(Thin client only) Select the **Settings** icon.
Disconnect from the remote desktop	(Thin client only) Select the **Disconnect** icon.
Show the sidebar	Swipe the tab to the right. When the sidebar is open, you cannot perform actions on the remote desktop window 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 remote desktop window or the Horizon Client Tools radial menu.
Navigate to an application	Tap **All Programs** and navigate to the application just as you would from the Windows Start menu.
Navigate to a file	Tap **My Files** to access the User folder, and navigate to the file. **My Files** includes folders such as My Pictures, My Documents, and Downloads. **My Files** includes the folders in the user profile (%USERPROFILE% directory). If you relocate the system folder in the %USERPROFILE% directory, the **My Files** menu can also display content from the relocated folder, whether it is a local relocated folder or a network share folder.
Search for an application or file	- Tap in the **Search** box and type the name of the application or file. - To use voice dictation, tap the microphone on the keyboard. - To launch an application or file, tap the name of the application or file in the search results. - To return to the home view of the sidebar, tap the **X** to close the **Search** box.
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	Touch and hold the application name under **Running Applications** until the context menu appears. Tap **Minimize**.

Table 4-1. Unity Touch Sidebar Actions for a Remote Desktop (continued)

Action	Procedure
Maximize a running application or window	Touch and hold the application name under **Running Applications** until the context menu appears. Tap **Maximize**.
Close a running application or window	Touch and hold the application name under **Running Applications** until the context menu appears. Tap **Close**.
Restore a running application or window to its previous size and position	Touch and hold the application name under **Running Applications** until the context menu appears. Tap **Restore**.
Create a list of favorite applications or files	1 Search for the application or file, or tap **Manage** under the **Favorite Applications** or **Favorite Documents** list. If the **Manage** bar is not visible, tap the chevron (**>**) next to **Favorite Applications** or **Favorite Files**. 2 Tap the check box next to the names of your favorites in the search results or in the list of available applications or files. The favorite that you add last appears at the top of your favorites list. 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.

Using the Unity Touch Sidebar with a Published Application

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

The Unity Touch feature is available only if a Horizon administrator has enabled it.

If the Unity Touch feature is enabled, the Unity Touch sidebar appears on the left side of the window when you first connect to a published application. If the Unity Touch sidebar is closed, a tab appears on the left side of the window. You can swipe this tab to the right to reopen the sidebar. You can also slide the tab up or down.

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

Table 4-2. Unity Touch Sidebar Actions for a Published Application

Action	Procedure
Show or hide the onscreen keyboard	(Thin client only) Select the **Keyboard** icon.
Modify Horizon Client settings	(Thin client only) Select the **Settings** icon.
Disconnect from the published application	(Thin client only) Select the **Disconnect** icon.
Show the sidebar	Swipe the tab to the right to open the sidebar. When the sidebar is open, you cannot perform actions on the published application window.
Hide the sidebar	Swipe the tab to the left to close the sidebar. When the sidebar is open, you cannot perform actions on the published application window.
Switch between running published applications	Tap the application under **Current Connection**. **Note** To avoid losing data, save your data before switching from a published application that is in multi-session mode.
Open a published application	Tap the name of the published application under **Applications** in the sidebar. The published application starts and the sidebar closes.
Close a running published application	1 Touch and hold the published application name under **Current Connection** until the context menu appears. 2 Tap **Close**.
Minimize a running published application	1 Touch and hold the published application name under **Current Connection** until the context menu appears. 2 Tap **Minimize**.
Maximize a running published application	1 Touch and hold the published application name under **Current Connection** until the context menu appears. 2 Tap **Maximize**.
Restore a running published application	1 Touch and hold the published application name under **Current Connection** until the context menu appears. 2 Tap **Restore**.
Switch to a remote desktop	Tap the remote desktop name under **Desktops**.

Using the 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.

When you use a remote desktop or published application in full-screen mode, the Horizon Client Tools radial menu icon appears at the right edge of the window. You can drag the radial menu icon to relocate it. 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.

If the remote desktop or published application is not in full-screen mode, a toolbar appears on the right side of the menu bar at the top of the window. You can tap the **Full Screen** icon on the toolbar to enter full-screen mode. When you are in full-screen mode, you can tap a similar icon in the radial menu to exit full-screen mode.

The radial menu includes several tools.

Table 4-3. Radial Menu Icons

Icon	Description
	Horizon Client Tools radial menu
	Disconnect
	Onscreen keyboard (toggles to show or hide)
	Settings
	Navigation keys
	Virtual touchpad
	Gesture help
	Exit full-screen mode

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.

If you are using a remote desktop or published application in full-screen mode, tap **Keyboard** icon in the Horizon Client Tools radial menu. If you are not using full-screen mode, tap the **Keyboard** icon on the Horizon Client toolbar.

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.

To turn this feature on or off, use the **Keyboard popup** and **Keyboard dismiss** options. To display these options when you are using a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, and tap **Keyboard**. If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar. If you are not connected to a remote desktop or published application, tap the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window.

Note On Kindle Fire tablets, tapping with three fingers does not display the onscreen keyboard. You can instead tap the **Keyboard** icon on the Horizon Client toolbar to display the onscreen keyboard.

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+Shift, first tap the onscreen Ctrl key. After the Ctrl key turns blue, tap the onscreen Alt key. After the Alt key turns blue, tap the onscreen Shift key. A single onscreen key is provided for the key combination Ctrl+Alt+Del.

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 published 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.

- 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, by setting the **Full screen touchpad** setting to off. If you are using the remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, tap **Touch**, and deselect the **Full screen touchpad** setting.

To adjust how quickly the pointer moves when you use the touchpad, adjust the **Touchpad sensitivity** option. If you are using the remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, tap **Touch**, tap **Touchpad sensitivity**, and drag the slider.

If you are not using full-screen mode, **Settings** is in the menu in the upper-right corner of the Horizon Client toolbar. If you are not connected to a remote desktop or published application, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

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.

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.

- On some devices, you can use an external mouse, such as a USB or Bluetooth mouse, to right-click.

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 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.

If you use the regular-size virtual touchpad, touch and hold the left-click button while dragging the corner or side of a window.

Sound, Music, and Video

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

Using a Thin Client

How you interact with Windows user interface elements when Horizon Client is installed on a thin client depends on the thin client model and the external input device you are using with the thin client. For more information, see Using Horizon Client on a Thin Client.

Multitasking

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

In a WiFi network, by default Horizon Client runs in the background indefinitely. 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.

The Horizon Client icon appears in the status bar when the app is running in the background and there is a connection to a remote desktop or published application. To switch back to Horizon Client, tap the icon in the status bar.

Copying and Pasting Text and Images

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

You can also copy and paste plain text and HTML-format rich text from a remote desktop or published application to the client device, or between remote sessions, if a Horizon administrator enables these features. For example, you can copy and paste an image from one remote desktop to another remote desktop.

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

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

- You cannot copy and paste images from a remote desktop or published application to the client device.

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

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

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

You can copy a maximum of 64 KB of data from a remote desktop or published application to the client device. Plain text that exceeds this limit is truncated. Rich text is converted to plain text.

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

When copying images between different remote sessions, the maximum clipboard size is 1 MB.

Logging Copy and Paste Activity

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

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

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

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

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

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

Dragging Text and Image Files

You can drag a text or image file from local storage on the client device to a published application or open application in a remote desktop and drop the file's content into the application. To use this feature, you must have an Android 7.0 or later device, or a Chromebook that is running Chrome OS M63 or later.

For example, if you are using an Android phone, you can select **Settings > Storage > Explore** or open the MyFiles app, select a folder, and drag a text file to the WordPad application in a remote desktop. If you are using a Chromebook device, you can drag files from the `Downloads` folder or from a USB device attached to the Chromebook device.

This feature has the following limitations.

- You can drag a maximum of 1 MB of data.

- You cannot drag Rich Text Format (RTF) text.

- If you select multiple files, only the content of the first file is dropped into the application.

- You cannot drag text files and image files from a remote desktop or published application to the client device.

A Horizon administrator can use the **Configure clipboard redirection** group policy settings to disable this feature. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Printing From a Remote Desktop or Published Application

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

To use this feature, Horizon Agent must be installed on the virtual machine or RDS host with the VMware Integrated Printing option enabled. For more information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Printing from a remote desktop or published application is a two-step procedure. For example, first you select **File > Print** in a Windows application, select the virtual printer that belongs to the mobile device, and tap **Print**. Next, the device's print dialog box appears. From the device's print dialog box, you click **Print** again. You can optionally select local print options, such as number of copies, paper size, and so on.

A Horizon administrator can disable the VMware Integrated Printing feature by using the **Disable printer redirection for non-desktop client** group policy setting. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Use USB Devices in a Remote Desktop or Published Application

With the USB redirection feature, you can use locally attached USB devices, such as thumb flash drives, in a remote desktop or published application.

When you use the USB redirection feature, most USB devices that are attached to the client device become available from a menu in Horizon Client. You use this menu to connect and disconnect the USB devices.

For information about USB device requirements and limitations for USB redirection, see "Using USB Devices with Remote Desktops and Applications" in the *Configuring Remote Desktop Features in Horizon* document.

Prerequisites

- To redirect USB devices to a remote desktop or published application, a Horizon administrator must enable the USB redirection feature.

  This task includes installing the USB Redirection component of Horizon Agent, and can include setting policies regarding USB redirection. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

- Verify that the USB over Session Enhancement SDK feature is enabled on the remote desktop. For information, see "Enabling the USB Over Session Enhancement SDK Feature" in the *Configuring Remote Desktop Features in Horizon* document.

- Become familiar with USB Redirection Limitations.

Procedure

1 Connect to the server.

2 Tap the **Switch Protocol** icon in the upper-right corner of the desktop and application selector window and tap **VMware Blast**.

You must use the VMware Blast protocol to use the USB redirection feature.

3 Connect to the remote desktop or published application.

4 Open **Settings** and tap **USB redirection**.

- If you are connected to the remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar.

The available USB devices appear in the USB redirection list. If no USB devices are available, `No suitable devices available` appears.

5 Select the check box next to the USB device that you want to redirect to the remote desktop or published application.

A system dialog prompts you to give Horizon Client access to the USB device.

6 To give Horizon Client access to the USB device, click **OK**.

You can give Horizon Client access to the USB device by default by selecting the **Use by default for this USB device** check box. The permission to access the device remains valid only until the device is disconnected.

Results

The redirected USB device appears in the remote desktop or published application. A USB device might take up to 20 seconds to appear in a remote desktop or published application.

What to do next

To disconnect a USB device from the remote desktop or published application, repeat the steps in this procedure, but deselect the check box for the USB device in the USB redirection list.

USB Redirection Limitations

The USB redirection feature has certain limitations.

- When you access a USB device from a menu in Horizon Client and use the device in a remote desktop or published application, you cannot access the USB device on the local device.

- USB devices that do not appear in the menu, but are available in a remote desktop or published application, include human interface devices such as keyboards and pointing devices. The remote desktop or published application, and the local device, use these devices at the same time. Interaction with these USB devices can sometimes be slow because of network latency.

- Large USB disk drives can take several minutes to appear in the remote desktop or published application.

- Some USB devices require specific drivers. If a required driver is not already installed, you might be prompted to install it when you connect the USB device to the remote desktop or published application.

- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.

- You cannot format a redirected USB drive in a published desktop unless you connect as an administrator user.

- Auto-connection of USB devices to remote desktops and published applications is not supported.

- USB device filtering is not supported.

- USB device splitting is not supported.

- On a Chromebook, USB redirection for published applications is not supported.

Saving Documents in a Published Application

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

A Horizon administrator can use the RDS Profiles group policy setting called **Set Remote Desktop Services User Home Directory** to specify where documents are saved. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Use Multiple Sessions of a Published Application From Different Client Devices

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log on to the server from different client devices.

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

The multi-session mode feature has the following limitations.

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

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

Prerequisites

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

Procedure

1 Connect to a server.

2 Tap the application icon in the upper-right corner of the Horizon Client toolbar and tap **Multi-Launch**.

If the application icon does not appear on the toolbar, tap the three vertical dots. If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.

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

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

Screen Resolutions and Using External Displays

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

When you connect a client device to an external display or projector, Horizon Client supports certain maximum display resolutions. You can change the screen resolution that the client device uses 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 remote desktop fits inside the client device, and the remote desktop icons and task bar icons are a certain size. If you use a larger resolution, the remote desktop still fits inside the client device, but the remote desktop and taskbar icons become smaller.

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

Changing the Display Resolution Setting

You can use the **Resolution** setting to set the display resolution to a larger value. If you are using a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, tap **Display**, and tap **Resolution**. If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar. If you are not connected to a remote desktop or published application, tap the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window.

Using High Quality Mode

You can use the High Quality Mode feature to obtain the best display quality in remote desktops and published applications.

To enable High Quality Mode, before you connect to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window, tap **Display**, and then tap **High Quality Mode**. You cannot enable the **High Quality Mode** setting after you connect to a remote desktop or published application.

The High Quality Mode feature has the following requirements and limitations.

- You cannot use the High Quality Mode feature for existing sessions. You must log out and log in to a new session for the feature to take effect.

- If the client device has less than an extra-high density (xhdpi) screen, the **High Quality Mode** setting is not available.

High Quality Mode is disabled by default.

Using External Displays

You can use the **Enable External display** setting to configure settings for external displays, such as projectors and attached monitors.

When the **Enable External display** setting is selected, you can use the following settings.

Presentation mode

When you enable this setting, a keyboard and expanded onscreen touchpad appear on the device when you display a remote desktop on an external display. The expanded touchpad and keyboard appear when you plug the device into the external display. The device detects the maximum resolution provided by the external display.

Multi-Monitor mode

When you enable this setting on an Android device, Horizon Client extends a secondary desktop on an external display. The Unity Touch sidebar is supported only on the client's internal monitor. You cannot change the orientation and full-screen mode. You can interact with remote desktops and published applications on the external display with the onscreen touchpad and full-screen touchpad. You cannot use the physical mouse on the external display.

Keep screen on when external display is connected

> This setting keeps the display from turning off after a period of inactivity.

Zoom

> Drag this slider to set the resolution for the external display.

If you are connected to a remote desktop or published application, pressing the **Back** button quits presentation mode or multi-monitor mode and the **Enable External display** setting is deselected. When the **Enable External display** setting is deselected, all the external display settings are disabled.

To configure external display settings if you are using a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon, tap the gear icon, tap **Display**, and then tap **External Display Options**. If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar. If you are not connected to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

Do not use an external mouse, such as a Bluetooth mouse, when you use the **Presentation Mode** setting. Instead, use the large onscreen touchpad on the client device.

Using Multi-Monitor Mode on a Chromebook

To enter multi-monitor mode when Horizon Client for Android is installed on a Chromebook, maximize the remote session window. After you maximize a remote desktop window on the Chromebook display, it appears on the external display, or displays, automatically. After you maximize a published application window, you can drag it to an external display. To quit multi-monitor mode, restore the remote session window from the maximized state.

The multi-monitor mode feature has the following requirements and limitations.

- Chrome OS M64 or later is required.

- Two external displays are supported.

- The display topology in the remote session is similar to, but might not be exactly the same as, the display topology that is configured on the Chromebook device.

- Unified desktop mode must not be enabled on the Chromebook device.

Changing the Display Zoom Level on a Chromebook Device

When Horizon Client for Android is installed on a Chromebook device and seamless window mode is enabled, you can change the display zoom level for published applications.

To change the display zoom level for published applications, tap the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window and tap **Remote Applications**. In the Remote Applications dialog box, you can set the device display zoom level to 100, 110, 125, 150, 175, or 200 percent. You can set the external display zoom level to 100, 150, 200, 250, or 300 percent. The default display zoom level is 100 percent for both the device display and the external display.

This feature has the following requirements and limitations:

- Chrome OS M64 or later is required.

- You can change the display zoom level for only one external display.

- Seamless window mode must be enabled. For more information, see Configure Seamless Window Mode on a Chromebook Device.

You can also enable or disable local storage redirection for published applications from the Remote Applications dialog box. This feature is enabled by default. For more information about this feature, see Share Access to Local Storage with Client Drive Redirection.

Using DPI Synchronization

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

Like the Display Scaling feature, the DPI Synchronization feature can improve the readability of text and icons on high-DPI displays. Unlike the Display Scaling feature, which increases the size of fonts and images and can make them blurry, the DPI Synchronization feature increases the size of fonts and images, keeping them sharp. For this reason, the DPI Synchronization feature is generally preferred for an optimal user experience.

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

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default.

Behavior of DPI Synchronization

The default DPI synchronization behavior depends on the Horizon Agent version that is installed in the agent machine.

Beginning with Horizon Agent 2012, the client's per-monitor DPI setting is synchronized to the agent and changes take effect immediately during a remote session by default. This feature is controlled by the DPI Synchronization Per Monitor agent group policy setting. The DPI Synchronization Per Monitor feature is supported by default for virtual desktops and physical desktops. It is not supported for published desktops.

With earlier Horizon Agent versions, the client supports synchronization only to the system DPI setting. DPI Synchronization happens during the initial connection, and Display Scaling works in case of reconnection, if necessary. When DPI Synchronization works and the client system's DPI setting matches the remote desktop's DPI setting, Display Scaling cannot take effect, even if you select the Allow Display Scaling option in the user interface. Windows does not allow users to change the system-level DPI setting for the current user session, and DPI synchronization occurs only when they log in and start a remote session. If users change the DPI setting during a remote session, they must log out and log in again to make the remote desktop's DPI setting match the client system's new DPI setting.

The agent DPI setting is located in the Windows registry at `Computer\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Note The system DPI setting might not be the same as the main monitor's DPI setting. For example, if you close the main monitor and the system switches to an external display that has a different DPI setting than the main monitor, the system DPI setting is still the same as the DPI setting of the previously closed main monitor.

This version of the client does not support the DPI Synchronization Per Connection agent group policy setting, which is provided with Horizon Agent versions 7.8 through 2006.

For more information about the DPI synchronization group policy settings, see the *Configuring Remote Desktop Features in Horizon* document for your Horizon Agent version.

Supported Guest Operating Systems for Virtual Desktops

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

- 32-bit or 64-bit Windows 7

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

- 32-bit or 64-bit Windows 10

- Windows Server 2012 R2 configured as a desktop

- Windows Server 2016 configured as a desktop

- Windows Server 2019 configured as a desktop

Note For Windows server machines that are configured as a desktop, the DPI Synchronization Per Monitor feature is not supported.

Supported RDS Hosts for Published Desktops and Published Applications

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

- Windows Server 2012 R2

- Windows Server 2016

- Windows Server 2019

Note For RDS hosts, the DPI Synchronization Per Monitor feature is not supported. This limitation does not apply to published applications that run on desktop pools with the VM Hosted Applications feature

PCoIP Client-Side Image Cache

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

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

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

- On the LAN, where the bandwidth is relatively unconstrained, using client-side image caching delivers significant bandwidth savings.

- Over the WAN, to stay within the available bandwidth constraints, scrolling performance is degraded without client-side caching. Over the WAN, client-side caching saves bandwidth and ensures a smooth, highly responsive scrolling experience.

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

Using International Keyboards

To select a language for the keyboard or voice, tap the Keyboard Settings key on the onscreen keyboard. The Keyboard Settings key is the left-most key on the bottom row of the onscreen keyboard.

Troubleshooting

5

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

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

This chapter includes the following topics:

- Restart a Remote Desktop
- Reset a Remote Desktop or Published Applications
- Uninstall Horizon Client
- Collecting and Sending Logging Information to VMware
- Report Horizon Client Crash Data to VMware
- Horizon Client Stops Responding or the Remote Desktop Freezes
- Problem Establishing a Connection When Using a Proxy
- Connecting to a Server in Workspace ONE Mode

Restart a Remote Desktop

If the remote desktop operating system stops responding, you might need to restart a remote desktop. Restarting a remote desktop is similar to using the Windows operating system restart command. The remote desktop operating system usually prompts you to save any unsaved data before it restarts.

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

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

Procedure

1 On the **Servers** tab, tap the server shortcut 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 remote desktop shortcut until the context menu appears.

You can perform this step from either the **All** or **Favorites** tab.

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

Results

The operating system in the remote desktop restarts and the client disconnects and logs off from the remote desktop.

What to do next

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

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

Reset a Remote Desktop or Published Applications

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

Resetting a remote desktop is similar to pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop are closed and are not saved.

Resetting published applications quits the applications without saving any unsaved data. All open published applications are closed, including applications that come from different RDS server farms.

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

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

Prerequisites

Obtain login credentials, such as a user name and password, RSA SecurID user name and password, RADIUS authentication user name and password, or smart card personal identification number (PIN).

Procedure

1   On the **Servers** tab, tap the server shortcut 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 remote desktop or published application shortcut until the context menu appears.

You can perform this step from either the **All** or **Favorites** tab.

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

Results

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

What to do next

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

Uninstall Horizon Client

You can sometimes resolve problems with Horizon Client by uninstalling and reinstalling Horizon Client app. You uninstall Horizon Client just as you would any Android app.

Procedure

1   On the client device, go to the **Horizon** app.

2   Touch and hold the app icon until the **Uninstall** (trash can) icon appears on the client device.

3   Drag the app to the **Uninstall** (trash can) icon.

Alternatively, you can go to **Apps > Settings** and select **Applications > Manage Applications** to uninstall Horizon Client.

What to do next

Reinstall Horizon Client.

See Install or Upgrade Horizon Client.

Collecting and Sending Logging Information to VMware

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

If Horizon Client quits unexpectedly, it immediately prompts you to send log files to VMware. If log collection is enabled, the crash log file contains detailed debug information. If log collection is disabled, only certain exception information is included in the crash log file.

Horizon Client generates the following log files and keeps the last five files of each log file type.

- `Horizon_View_Client_logs_timestamp.txt`

- `libcdk_timestamp.txt`

- `pcoip_client_`*`timestamp`*`.txt`

If you send log files to VMware, Horizon Client uses the available email client on the client device to create a message. If the email client can send multiple attachments, Horizon Client attaches the last five files of each log file type to the message. If the email client cannot send multiple attachments, Horizon Client compresses the last five files of each log file type and attaches a ZIP file to the message. The ZIP file name contains a time stamp, for example, `Horizon_View_Client_logs_`*`timestamp`*`.zip`.

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 client is available on the device. Horizon Client requires an email client to send log files.

Procedure

1 Open **Settings** and tap **Log collection**.

- If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar.

- If you are not connected to a remote desktop or published application, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2 Tap to toggle the **Enable log** option to on and tap **OK** to confirm your choice.

Results

After log collection is enabled, Horizon Client generates a log file it quits unexpectedly or when it is exited and restarted.

Manually Retrieve and Send Horizon Client Log Files

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

This procedure explains how retrieve and send log files through Horizon Client. You can also retrieve log files by using tools that can access app storage space. Horizon Client saves log files in the `Android/data/com.vmware.view.client.android/files` directory.

Prerequisites

- Verify that an email client is available on the client device. Horizon Client requires an email client to send log files.

- Enable Horizon Client log collection. See Enable Horizon Client Log Collection.

Procedure

1   Open **Settings** and tap **Log collection**.

- If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper right corner of the Horizon Client toolbar.

- If you are not connected to a remote desktop or published application, tap the gear icon in the upper right corner of the Horizon Client window.

2   Tap **Send the log**.

Horizon Client uses the email client on the client device to create a message. The body of the message contains information about the client device. If the email client can send multiple attachments, Horizon Client attaches the last five log files of each type to the message. If the email client cannot send multiple attachments, Horizon Client compresses the last five log files of each type and attaches a ZIP file to the message.

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   Open **Settings** and tap **Log collection**.

- If you are connected to a remote desktop or published application in full-screen mode, tap the Horizon Client Tools radial menu icon and tap the gear icon.

- If you are not using full-screen mode, tap **Settings** in the menu in the upper-right corner of the Horizon Client toolbar.

- If you are not connected to a server, tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2   Tap to toggle the **Enable log** option to off.

Report Horizon Client Crash Data to VMware

You can configure Horizon Client to report crash data to VMware.

Procedure

1 Tap the **Settings** (gear) icon in the upper-right corner of the Horizon Client window.

2 Tap **Crash Reporting**.

3 Tap to toggle the **Crash Reporting** option to on or off.

   The setting is enabled by default.

Results

If Horizon Client stops responding, a crash log file is uploaded to the server the next time Horizon Client starts.

Horizon Client Stops Responding or the Remote Desktop Freezes

Horizon Client stops responding or a remote desktop freezes.

Problem

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

Cause

If the server is configured properly and the correct firewall ports are open, the cause of the problem usually relates to Horizon Client on the device or to the remote desktop operating system.

Solution

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

   This option is available only if a Horizon administrator has enabled the desktop reset feature.

◆ Uninstall and reinstall the Horizon Client app on the client device.

◆ If resetting the remote desktop and reinstalling Horizon Client do not help, you can reset the client device, as described in the user guide for the client device.

◆ If you receive 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

When you attempt to connect to a server by using a proxy while on the LAN, an error sometimes occurs.

Problem

If your Horizon environment is set up to use a secure connection from a remote desktop to a server, and if the client device is configured to use an HTTP proxy, you might not 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 a server by using an internal address, you might see the error message `Could not establish connection`.

Solution

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

Connecting to a Server in Workspace ONE Mode

You cannot connect to a server directly through Horizon Client, or your remote desktop and published application entitlements are not visible in Horizon Client.

Problem

■ When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.

■ When you open a remote desktop or published application through a URI or shortcut, or when you open a local file through file association, the request redirects you to the Workspace ONE portal for authentication.

■ After you open a remote desktop or published application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or published applications in Horizon Client.

Cause

A Horizon administrator can enable Workspace ONE mode on a Connection Server instance. This behavior is normal when Workspace ONE mode is enabled on a Connection Server instance.

Solution

Use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops and published applications.