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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com
Contents

1 About the Horizon Workspace Administrator's Guide 7

2 Introduction to Horizon Workspace for Administrators 9

3 View Horizon Workspace System and Module Information 13

4 Integrating Horizon Workspace with Active Directory 15
   Single Active Directory Domain Environment 15
   Multi-Domain, Single Forest Active Directory Environment 15
   Multi-Forest Active Directory Environment 16

5 Configuring Horizon Workspace User Authentication 19
   Overview of Horizon Workspace User Authentication 19
   Add or Edit a Network Range 21
   Add or Edit a User Authentication Method 22
   Add and Configure an Identity Provider Instance 23
   Overview of Configuring Horizon Workspace to Use a Third-Party Identity Provider Instance 26
   Editing the Default Access Policy Set 28

6 Managing Access Policy Sets 31
   Overview of Access Policy Settings 31
   Managing Web-Application-Specific Access Policy Sets 32
   Edit an Access Policy Set 34
   Add a Web-Application-Specific Access Policy Set 35
   Apply a Web-Application-Specific Access Policy Set 36

7 Managing Users and Groups 37
   Horizon Workspace User and Group Types 37
   Manage Horizon Workspace Groups 38
   Manage Horizon Workspace Users 43
   Manage Guest Users 49
   Update the Settings That Select Horizon Workspace Users from Active Directory 50

8 Managing the Horizon Workspace Catalog 51
   Overview of Horizon Workspace Resource Types 52
   Overview of Using Resource Categories 54
   View Horizon Workspace Resources 55
   Add Resources to Your Catalog 56

9 Search for Users, Groups, or Catalog Resources 59
10 Configuring Desktop Systems to Use Horizon Workspace
   Command-Line Installer Options for Horizon Workspace for Windows
   Install the Horizon Workspace for Windows Application with Identical Settings to Multiple
   Windows Systems
   Configure the Horizon Workspace for Windows Client to Launch 64-Bit ThinApp Packages on 64-
   Bit Windows Operating Systems

11 Providing Access to the Horizon Workspace File-Sharing Service
   Enable the Horizon Files Module
   Entitling Users and Groups to the File-Sharing Service
   Class of Service

12 Using Mobile Devices with Horizon Workspace
   Enable the Mobile Management Module
   Overview of the Device Enrollment Process for VMware Ready Android Devices
   Configure Your Horizon Workspace to Enroll VMware Ready Android Devices
   Using Mobile Policies and Mobile Policy Sets
   Provide Pre-Defined VPN Configurations to Enrolled VMware Ready Android Devices
   Entitling Users and Groups to Resources Used On Mobile Devices
   Horizon Workspace Server Leasing Process and Enrolled VMware Ready Android Devices

13 Providing Access to Horizon View Desktop Pools
   Enable the View Module to Integrate Horizon View with Horizon Workspace
   View User and Group Entitlements to Horizon View Desktop Pools
   View the Connection Information for a Horizon View Desktop Pool
   Reducing Resource Usage and Increasing Performance of Horizon Workspace for Windows In
   Non-Persistent Horizon View Desktops

14 Providing Access to Web Applications
   Enable the Web Applications Module to Provide Web Application Access
   Establish Secure Single Sign-On to Your Web Applications Through Horizon Workspace
   Adding Web Applications to Your Organization’s Catalog
   Entitle Users and Groups to Web Applications

15 Providing Access to Citrix-Based Applications
   Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix
   Deployment
   View User and Group Entitlements to Citrix-Based Applications
   Editing Horizon Workspace Application Delivery Settings for Citrix-Based Applications
   Managing Categories for Citrix-Based Applications

16 Providing Access to VMware ThinApp Packages
   Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your
   Horizon Workspace System
   Distributing and Managing ThinApp Packages with Horizon Workspace
   Entitle Users and Groups to ThinApp Packages
   Updating Managed ThinApp Packages After Deployment in Horizon Workspace
The Horizon Workspace Administrator’s Guide provides information and instructions about using and maintaining VMware® Horizon Workspace™. With VMware Horizon Workspace, you can customize a catalog of resources for your organization’s applications and data and provide secure, multi-device, managed-user access to those resources. Such resources include Web applications, mobile applications, Windows applications captured as ThinApp packages, Citrix-based applications, and VMware® Horizon View™ desktop pools. Horizon Workspace provides users with a unified experience and offers your IT department unified security and management for all services and applications across multiple devices.

Intended Audience

The Horizon Workspace Administrator’s Guide is intended for enterprise administrators. This information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology, identity management, Kerberos, and directory services. Knowledge of other technologies, such as VMware® ThinApp®, VMware® Horizon View™, Citrix application virtualization, RSA SecurID, and Android app distribution is helpful if you plan to implement those features.

Horizon Workspace Administrator's Guide Overview

Use the Horizon Workspace Administrator’s Guide after you install Horizon Workspace. See Installing and Configuring Horizon Workspace.

To administer Horizon Workspace, you predominantly use the Horizon Workspace Administrator Web interface, logged in as an administrator. You occasionally need to access the Configurator Web interface, the Connector Web interface, and the virtual appliance interfaces. See “Horizon Workspace Web Interface URLs,” on page 11.

The key task you perform as a Horizon Workspace administrator is to entitle users to resources. Other tasks support this key task by providing you with more detailed control over which users or groups are entitled to which resources under which conditions.

The tasks you perform as an administrator vary depending on the resource types you plan to manage. You can manage the file-sharing service, Horizon View desktop pools, Windows applications (ThinApp packages), Citrix-based applications, Web applications, and managed mobile workspaces for VMware Ready Android devices. The actual resource types you manage vary according to the needs of your organization. To entitle a resource type, you must first perform the respective preconfiguration tasks as described in the Installing and Configuring Horizon Workspace.
Horizon Workspace provides you with a centralized Web management console with which you can customize your organization’s catalog, and manage entitlements to resources in that catalog. Your catalog contains your organization’s applications and Horizon View desktops as resources, as well as the Horizon Workspace file-sharing service.

Horizon Workspace detects users’ attributes and enforces policies across the applications, data, and desktops. A user's workspace consists of their set of entitled resources. For each user, you can customize the delivery of Windows, Web, and Software-as-a-Service (SaaS) applications with the ability to access those applications from a single portal, while providing users with self-service access to applications and data from anywhere.

**Horizon Workspace Server Components**

Horizon Workspace server consists of the following virtual appliances. The first five virtual appliances are bundled together in a vApp. The datatemplate-va is generated during configuration of the vApp.

**Table 2-1. Horizon Workspace Server Components**

<table>
<thead>
<tr>
<th>Horizon Workspace Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Workspace Configurator Virtual Appliance (configurator-va)</td>
<td>You start configuring Horizon Workspace with this virtual appliance, using both its console interface and the Configurator Web interface. The configurations you make with the Configurator are distributed to the other virtual appliances in the vApp.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Manager Virtual Appliance (service-va)</td>
<td>This virtual appliance handles ThinApp package synchronization and gives you access to the Administrator Web interface, from which you can manage users, groups, and resources.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Connector Virtual Appliance (connector-va)</td>
<td>The Horizon Workspace Connector provides the following services: user authentication (identity provider), directory synchronization, ThinApp-catalog loading, and View pool synchronization.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Files Virtual Appliance (data-va)</td>
<td>This virtual appliance controls the file storage and sharing service, stores users’ files and folders, and synchronizes them across multiple devices.</td>
</tr>
</tbody>
</table>
Table 2-1. Horizon Workspace Server Components (Continued)

<table>
<thead>
<tr>
<th>Horizon Workspace Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Workspace Gateway Virtual Appliance (gateway-va)</td>
<td>The Horizon Workspace Gateway is the single endpoint for all end user communication. User requests come to the gateway-va virtual machine, which then routes the request to the appropriate virtual appliance.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Data Template Virtual Appliance (datatemplate-va)</td>
<td>This virtual appliance is generated by the Configurator the first time the Horizon Workspace vApp is installed and powered on. It is used for clustering when you create a new data-va virtual machine using the hznAdminTool addvm command.</td>
</tr>
</tbody>
</table>

Horizon Workspace User Client Components

Users can access entitled resources using the Horizon Web-based user portal (an agentless client), a Windows client, a Mac client, an Android client, or an iOS client. Each client provides users with access to resources they are entitled to, but the specific applications, desktops, and data they can access from a particular client varies depending on the client.

Table 2-2. Horizon Workspace User Client Components

<table>
<thead>
<tr>
<th>Horizon Workspace User Client Component</th>
<th>Description</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Workspace User Portal</td>
<td>The Horizon Workspace User Portal is an agentless web-based application. It is the default interface used when users access and use their entitled workspace assets with a browser. Using this portal, users can access their Horizon Workspace files, Horizon View virtual desktops and Horizon Workspace Web applications. If an end user has entitled ThinApp applications and is on a Windows system where the VMware Horizon Workspace for Windows program is installed and active, they can also view and launch their entitled ThinApp packages using this Web client. On iOS devices, users can open this portal in a browser app like Safari and access and use their Horizon View virtual desktops and Horizon Workspace Web applications and Citrix-based applications. They can also launch the Horizon Files for iOS app from this portal, if the app is installed on their device.</td>
<td>Web-based user portal is available on all supported system endpoints, such as Windows systems, Mac systems, iOS devices, Android devices, and VMware Ready devices.</td>
</tr>
<tr>
<td>VMware Horizon Workspace for Windows</td>
<td>When this program is installed on users' Windows systems, they can work with their Horizon Workspace files and virtualized Windows applications captured as ThinApp packages. When this program is installed, a user's personal and shared folders and files are synchronized between their system and Horizon Workspace.</td>
<td>Windows systems</td>
</tr>
<tr>
<td>VMware Horizon Workspace for Mac</td>
<td>When this program is installed on users' Apple Mac OS X systems, they can access their Horizon Workspace files locally. When this program is installed, users' personal and shared folders and files are synchronized between their system and Horizon Workspace.</td>
<td>Mac systems</td>
</tr>
</tbody>
</table>
Table 2-2. Horizon Workspace User Client Components (Continued)

<table>
<thead>
<tr>
<th>Horizon Workspace User Client Component</th>
<th>Description</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Files for iOS</td>
<td>When this app is installed on users' iOS devices and those users are entitled to use your Horizon Workspace system's file-sharing service, they can work with their Horizon Workspace files and synchronize them between their device and Horizon Workspace.</td>
<td>iOS devices</td>
</tr>
<tr>
<td>VMware Horizon Files for Android</td>
<td>When this app is installed on users' Android devices and those users are entitled to use your Horizon Workspace system's file-sharing service, they can work with their files and synchronize them between their device and Horizon Workspace.</td>
<td>Android devices</td>
</tr>
<tr>
<td>VMware Horizon Workspace Switch</td>
<td>When this client is installed on users' VMware® Ready™ Android devices, they can provision and run a preconfigured mobile workspace on those devices. The user's preconfigured mobile workspace is a secure container that consists of a secure Android base and the workspace assets that you entitle to that user. The secure container is managed by Horizon Workspace using policies. When the secure container is provisioned to the user's VMware Ready device, the user can enter the secure container using the Switch app and perform their work tasks using the assets in the policy-managed container, including accessing their files and Web applications.</td>
<td>VMware Ready Android devices</td>
</tr>
</tbody>
</table>

Horizon Workspace Web Interface URLs

Each interface gives you access to different functions. Each Web interface URL listed uses a placeholder, such as HorizonWorkspaceFQDN, ConnectorHostname, and ConfiguratorHostname for the hostname. Replace the placeholder names with the actual values.

Table 2-3. Horizon Workspace URLs

<table>
<thead>
<tr>
<th>URL</th>
<th>User Interface</th>
<th>What you can do here</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/admin">https://HorizonWorkspaceFQDN/admin</a></td>
<td>Administrator Web interface (Active Directory user)</td>
<td>Manage your catalog, users and groups, entitlements, reports, etc. (Log in as the Active Directory user with administrator role.)</td>
</tr>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/SAAS/login/0">https://HorizonWorkspaceFQDN/SAAS/login/0</a></td>
<td>Administrator Web interface (non-Active Directory user)</td>
<td>Use this URL if you cannot login as the Active Directory user with the administrator role. (Log in as an administrator using the username admin and the password you set during configuration.)</td>
</tr>
</tbody>
</table>
### Table 2-3. Horizon Workspace URLs (Continued)

<table>
<thead>
<tr>
<th>URL</th>
<th>User Interface</th>
<th>What you can do here</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/web">https://HorizonWorkspaceFQDN/web</a></td>
<td>Web Client</td>
<td>This URL brings you to the Active Directory user login page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Active Directory Users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>From the Active Directory user login page, log in to Horizon Workspace to manage the resources available to you, such as applications, View pools, and the file-sharing service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Guest Users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the guest user log in page to log in to Horizon Workspace. If you go to the Active Directory user login page first, click <strong>Sign in as a guest user</strong> to go to the guest user login page where you can log in.</td>
</tr>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/auth/login?guest">https://HorizonWorkspaceFQDN/auth/login?guest</a></td>
<td>Web Client (guest user)</td>
<td>This URL brings you to the guest user login page. As a guest user, log in to Horizon Workspace to view and edit shared folders depending on the privileges provided to you by a Horizon Workspace user.</td>
</tr>
<tr>
<td><a href="https://ConnectorHostname/bc/admin/">https://ConnectorHostname/bc/admin/</a></td>
<td>Connector Web interface</td>
<td>Configure additional ThinApp settings, View pool settings, Citrix published application settings, check directory sync status, or alerts. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://ConfiguratorHostname/cfg">https://ConfiguratorHostname/cfg</a></td>
<td>Configurator Web interface</td>
<td>See system information, check modules, set license key, or set admin password. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
</tbody>
</table>
You can view Horizon Workspace system information and information about the Horizon Workspace modules: the Horizon Files module, the Web Applications module, the Mobile Management module, the View module, the ThinApp Packages module, and the Citrix Published Applications module.

Horizon Workspace system information and information about the Horizon Workspace modules is available on the Dashboard page in the Horizon Workspace Administrator Web interface.

**Prerequisites**

Install and configure Horizon Workspace. During the configuration process, enable those modules for the resource types that you want to make available in your users' workspaces. If you do not enable a module during installation, you can configure it later using the Administrator Web interface.

**Procedure**

- **Select** Dashboard > **Modules** to view the module information.
  
  You can view details about each module, including which modules are enabled and how many users are entitled to the resources provided by each module.

- **Select** Dashboard > **System Info** to view Horizon Workspace system information.

**What to do next**

If you want to entitle resource types to your users that are provided by modules that are not enabled in your system, enable those modules. See the appropriate topic.

- “Enable the Horizon Files Module,” on page 71
- “Enable the Web Applications Module to Provide Web Application Access,” on page 101
- “Enable the Mobile Management Module,” on page 82
- “Enable the View Module to Integrate Horizon View with Horizon Workspace,” on page 98
- “Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Horizon Workspace System,” on page 118
- “Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment,” on page 111
Integrating Horizon Workspace with Active Directory

You can integrate Horizon Workspace with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

You can add additional identity provider instances, which are either Connector instances or third-party identity provider instances.

Add additional identity provider instances for the purpose of high availability, to provide additional user authentication methods, and in multi-forest environments to add additional user stores.

If you do not integrate Horizon Workspace with a multi-forest Active Directory environment, your Horizon Workspace deployment contains a single user store named default.

During the proof-of-concept phase of your Horizon Workspace installation, connect Horizon Workspace to a single Active Directory domain or forest. For the production phase of deployment, integrate Horizon Workspace into your existing Active Directory environment.

This chapter includes the following topics:

- “Single Active Directory Domain Environment,” on page 15
- “Multi-Domain, Single Forest Active Directory Environment,” on page 15
- “Multi-Forest Active Directory Environment,” on page 16

Single Active Directory Domain Environment

A single Active Directory deployment allows you to sync users and groups from a single Active Directory domain. By definition, this is a single forest deployment.

To install Horizon Workspace in a single Active Directory domain environment, see instructions for establishing a connection to Active Directory specifically for a single domain in Installing and Configuring Horizon Workspace. For information about configuring Horizon Workspace user authentication, see Chapter 5, “Configuring Horizon Workspace User Authentication,” on page 19.

Multi-Domain, Single Forest Active Directory Environment

A multi-domain, single forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains within a single forest and is based on the Active Directory global catalog instead of LDAP.

To install Horizon Workspace in a multi-domain, single forest Active Directory environment, see the configuring multi-domain, single forest Active Directory instructions in Installing and Configuring Horizon Workspace. For information about configuring Horizon Workspace user authentication, see Chapter 5, “Configuring Horizon Workspace User Authentication,” on page 19.
Multi-Forest Active Directory Environment

A multi-forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains or forests to Horizon Workspace in a multi-forest environment. For a multi-forest Active Directory deployment, you must also add one or more identity provider instances with which to associate user stores.

**Attention** In a multi-forest Active Directory environment, Horizon Workspace does not support VMware View resources or Citrix-based applications. To enable Horizon Workspace users to access these resource types, you must integrate Horizon Workspace with a single Active Directory domain environment or a multi-domain, single forest Active Directory environment.

To configure Horizon Workspace in a multi-forest Active Directory environment, you make configurations for the first forest as necessary, either as a single-domain forest or as a multi-domain forest. The first forest appears as a user store named default. Then you add and configure an identity provider instance for each forest you plan to integrate with your Horizon Workspace deployment. See *Installing and Configuring Horizon Workspace* for instructions about configuring Horizon Workspace in a multi-forest Active Directory environment.

You must add a user store for each forest you plan to integrate with your Horizon Workspace deployment. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16. For information about configuring Horizon Workspace user authentication, see Chapter 5, “Configuring Horizon Workspace User Authentication,” on page 19.

Add a User Store for a Multi-Forest Active Directory Environment

To configure Horizon Workspace in a multi-forest Active Directory environment, you must add a user store for each domain or forest that you plan to integrate with your Horizon Workspace deployment.

The user store is a required construct when you deploy Horizon Workspace in a multi-forest environment. The user store is a collection of users. Associate a user store to an Active Directory forest. This association links one or more identity provider instances, either the Connector or a third-party identity provider, to users and groups in Horizon Workspace.

Horizon Workspace creates a default user store for you during the installation process. You create additional user stores for each additional domain or forest to which you want to integrate Horizon Workspace. Each user store has a sync client, an identity provider that you select for syncing users and groups to Horizon Workspace. Link other identity provider instances, besides the sync client, to a user store to provide high availability or to provide additional authentication methods.

**Prerequisites**

Decide, according to your organization’s needs, the number of user stores required and the best way to associate user stores to your Active Directory deployment, per domain or per forest. For more information about deploying Horizon Workspace in a multi-forest Active Directory environment, see “Multi-Forest Active Directory Environment,” on page 16.

**Procedure**

1. Log in to the Administrator Web interface.
2. Select **Settings > User Stores**.
3. Click **+ User Store**.
4 Provide the user store settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the user store.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Horizon Workspace displays the text in the Name text box in English. You can change the text to a different language.</td>
</tr>
<tr>
<td>Sync Client</td>
<td>This drop-down menu includes all the service clients registered with Horizon Workspace. Select an service client with which the user store syncs users and groups. If you set a Connector instance as the sync client, set an automated sync schedule for that Connector instance.</td>
</tr>
<tr>
<td>Authenticating Identity Providers</td>
<td>This text box lists all identity provider instances registered with Horizon Workspace. Select the identity provider instances that you want to link to this user store. You can associate multiple identity provider instances with a single user store. For example, the identity provider instance selected as the sync client, identity provider instances added for high availability purposes, and identity provider instances added to provide additional methods of authentication.</td>
</tr>
</tbody>
</table>

5 Click Save.

**What to do next**

- Initiate the user and group sync process of the configured sync client (a Connector or a third-party identity provider service client).
- After you sync the user and group information with Active Directory, you can configure the user login screen to present users with user store names instead of domain names. See “Edit a User Store for a Multi-Forest Active Directory Environment,” on page 17
- Associate the user store with one or more authenticating identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.

**Edit a User Store for a Multi-Forest Active Directory Environment**

You can edit an existing user store to change the settings. To configure the user login screen to present users with user store names instead of domain names you must edit the existing user stores.

You might want to edit the settings of a user store, such as the sync client or the authenticating identity providers.

Also, when you add a user store, Horizon Workspace does not give you the option of providing users logging in with the name of the user store instead of a domain name. That option is available when you edit the user store after syncing the service client you selected as the sync client with Active Directory. In a multi-forest Active Directory environment, users logging in must ensure that the correct domain name or user store domain is selected on the login screen. Depending on the complexity of the deployment, using user store names might be simpler to manage than using domain names.

**Prerequisites**

Add user stores to your deployment as necessary. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16.

**Procedure**

1 Log in to the Administrator Web interface.
2 Select Settings > User Stores.
3 Click Edit for the user store you want to configure.
Edit the user store settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>To change the name, replace the name for this user store. Note: Horizon Workspace displays the text in the Name text box in English. You can edit this text, which includes changing the text to a different language.</td>
</tr>
<tr>
<td>Sync Client</td>
<td>To change the sync client, select a different service client with which the user store syncs users and groups. If you set a Connector instance as the sync client, set an automated sync schedule for that Connector instance.</td>
</tr>
<tr>
<td>Authenticating Identity Providers</td>
<td>To change the selected authenticating identity provider instances, select the identity provider instances that you now want to link to this user store. For example, the identity provider instance selected as the sync client, identity provider instances added for high availability purposes, and identity provider instances added to provide additional methods of authentication.</td>
</tr>
<tr>
<td>Display user store name instead of domain name for end user authentication</td>
<td>To provide users logging in with the user store name, as it appears in the Name text box, instead of the domain names, click the checkbox for this option. If you do not select the checkbox, users are presented with the domain names listed in the User Domains section.</td>
</tr>
<tr>
<td>User Domains</td>
<td>This read-only section lists the domain names that Horizon Workspace presents to users on the log-in screen if you do not select the preceding checkbox. Confirm that the domain names listed are correct.</td>
</tr>
</tbody>
</table>

5 Click Save.

What to do next
- If you changed the sync client, initiate the user and group sync process of the newly configured sync client (a Connector or a third-party identity provider service client).
- If you have not already done so, associate the user store with an identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.
Horizon Workspace user authentication requires the use of one or more identity provider instances, which can be Connector instances, third-party identity provider instances, or a combination of both. The identity provider instances authenticate users with Active Directory within the enterprise network.

To configure and add identity provider instances to your Horizon Workspace deployment, you must perform several prerequisites to ensure that Horizon Workspace can properly access your Active Directory deployment.

This chapter includes the following topics:

- “Overview of Horizon Workspace User Authentication,” on page 19
- “Add or Edit a Network Range,” on page 21
- “Add or Edit a User Authentication Method,” on page 22
- “Add and Configure an Identity Provider Instance,” on page 23
- “Overview of Configuring Horizon Workspace to Use a Third-Party Identity Provider Instance,” on page 26
- “Editing the Default Access Policy Set,” on page 28

**Overview of Horizon Workspace User Authentication**

Horizon Workspace attempts to authenticate users based on several configurations you make. For example, when you configure the authentication methods, the default access policy set, network ranges, and the identity provider instances.

The identity provider instances that you use with Horizon Workspace create an in-network federation authority that communicate with Horizon Workspace using SAML 2.0 assertions. The identity provider instances authenticate the user with Active Directory within the enterprise network (using existing network security).

Horizon Workspace supports the following authentication methods with the Connector by default: Active Directory password, Kerberos, and RSA SecurID. However, your third-party identity provider might support additional authentication methods, such as smart-card based authentication, that you can use with your Horizon Workspace deployment.
### Horizon Workspace Authentication Types Supported by Default

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong>  Without any configuration, Horizon Workspace supports Active Directory password authentication. This method authenticates users directly against Active Directory.</td>
</tr>
<tr>
<td><strong>Kerberos</strong>  When properly configured, Kerberos authentication provides domain users with single sign-on access to Horizon Workspace, eliminating the requirement for domain users to log in to Horizon Workspace after they log in to the enterprise network. The identity provider instance validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC).</td>
</tr>
<tr>
<td><strong>RSA SecurID</strong>  RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is the recommended authentication method for users accessing Horizon Workspace from outside the enterprise network.</td>
</tr>
</tbody>
</table>

To implement Kerberos authentication or RSA SecurID authentication, you can use an existing identity provider instance or you can deploy one or more additional identity provider instances, depending on your deployment.

When a user attempts to log in, Horizon Workspace must determine which identity provider instance to authenticate the user against. The identity provider instance can be either a Connector instance or a third-party identity provider instance.

To make the determination, Horizon Workspace evaluates the default access policy set to select which policy in the set to apply. The applied policy dictates the minimum authentication score required for that login event. Horizon Workspace then filters and sorts the available authentication methods based on the minimum authentication score required and the order of the methods, which you can set as necessary to meet your organization's requirements. Horizon Workspace selects the first identity provider instance that meets the authentication method and network range requirements of the policy and forwards the user authentication request to that instance for authentication. If authentication fails, the identity provider selection process continues down the list.

**CAUTION** When you remove or reset an identity provider instance, you must remove the corresponding identity provider name from the Identity Providers page.

You can deploy Horizon Workspace to use the identity provider selection process in a variety of ways, one of which is summarized in the example that follows.

**External RSA SecurID and Internal Password Authentication or Higher Example**

This is one possible way to configure Horizon Workspace to use the Active Directory password or Kerberos authentication method for internal users and RSA SecurID authentication method for external users in the same Horizon Workspace deployment.

- **Internal Policy** - You use the Horizon Workspace Administrator Web interface to create a policy in the default access policy set with a minimum authentication score that accepts Active Directory password as the authentication method. To ensure that Horizon Workspace attempts to authenticate users with Kerberos authentication first, you make the authentication score of the Kerberos method higher than the authentication score of the password method and you place Kerberos at the top of the list on the Authentication Methods page. You also assign a network range for internal users.

- **External Policy** - You use the Horizon Workspace Administrator Web interface to create a policy in the default access policy set with a minimum authentication score that ensures the RSA SecurID authentication method is used to authenticate users. You also assign a network range that includes all possible users, 0.0.0.0 to 255.255.255.255.
The result of this configuration is that users attempting to access Horizon Workspace from inside the enterprise network are directed to an identity provider instance that provides Kerberos authentication or password authentication while users outside the enterprise network are directed to an identity provider instance that provides RSA SecurID authentication. Internal and external users might be sent to the same identity provider instance or to different identity provider instances, depending on how you configure the authentication methods.

**NOTE** Guest users are not prompted for SecurID credentials even when the guest users are external to your enterprise and are redirected to an identity provider instance that can enforce SecurID authentication. See “Horizon Workspace User and Group Types,” on page 37 for a description of guest users.

Add or Edit a Network Range

You can add a network range of IP addresses that you want to direct to a specific identity provider instance. The default network range, called ALL RANGES, includes every IP address available on the Internet, 0.0.0.0 to 255.255.255.255. Even if your Horizon Workspace deployment has a single identity provider instance, you might need to configure the default range and add other ranges to exclude or include specific IP addresses. You must define multiple network ranges if your deployment has multiple identity provider instances with different authentication methods. See “Add and Configure an Identity Provider Instance,” on page 23.

**NOTE** The default network range, ALL RANGES, and its description, "a network for all ranges," are editable. You can edit the name and description, including changing the text to a different language, using the Edit feature on the Network Ranges page.

**Prerequisites**

Perform the necessary network range planning.

- Determine the best way to integrate Horizon Workspace with Active Directory to meet the needs of your organization. Such planning affects the number of identity provider instances in your deployment, which affects the number of network ranges needed. See Chapter 4, “Integrating Horizon Workspace with Active Directory,” on page 15.

- Based on your network topology, define network ranges for your Horizon Workspace deployment.

- To add a network range when the Horizon View module is enabled, take note of the View Client access URL and port number for the network range. See VMware Horizon View documentation for more information.

**Procedure**

1. Log in to the Administrator Web interface.
2. Select Settings > Network Ranges.
3. Edit an existing network range or add a new network range.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit an existing range</td>
<td>Click Edit for the range to edit.</td>
</tr>
<tr>
<td>Add a range</td>
<td>Click + Network Range to add a new range.</td>
</tr>
</tbody>
</table>

4. Complete the form.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network range.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the Network Range.</td>
</tr>
</tbody>
</table>
## Add or Edit a User Authentication Method

You can edit existing user authentication methods. When you add a third-party identity provider, you can configure user authentication methods that Horizon Workspace does not support by default. You can also create access policies to associate authentication methods with specific Web applications.


The minimum authentication score of a method and the order of the method on the Authentication Methods page are significant in the process Horizon Workspace follows to select an identity provider instance for user authentication. To require users to use an authentication method of a specified minimum authentication score to access a Web application, see “Managing Web-Application-Specific Access Policy Sets,” on page 32.

The number of attempts Horizon Workspace makes using a given authentication method varies. Horizon Workspace only makes one Kerberos authentication attempt. If Kerberos is not successful in logging in the user, the next authentication method on the list is attempted. The maximum number of failed login attempts for Password or RSA SecurID authentication is five. When the user has five failed login attempts, Horizon Workspace attempts to log in the user with the next authentication method on the list. When all authentication methods are exhausted, Horizon Workspace issues an error message.

### Prerequisites

- Deploy the authentication systems that you plan to integrate with Horizon Workspace. For example, if you plan to integrate RSA SecurID into your Horizon Workspace deployment, verify that RSA SecurID is installed and configured on your network.

- Use your own criteria to determine the security levels, on a scale from 1, the lowest security, to 5, the highest security, of the authentication methods you plan to use in your Horizon Workspace deployment.

### Procedure

1. Log in to the Administrator Web interface.
2. Select **Settings > Authentication Methods**.
3. Edit an existing authentication method or add a new authentication method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit an Existing Authentication Method</strong></td>
<td>Click <strong>Edit</strong> for the existing authentication method to configure.</td>
</tr>
<tr>
<td><strong>Add a New Authentication Method</strong></td>
<td>Click + <strong>Add Authentication Method</strong> to add a new authentication method. For example, when adding a new third-party identity provider instance to your deployment.</td>
</tr>
</tbody>
</table>

4. Edit the authentication method settings.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for this identity provider instance.</td>
</tr>
<tr>
<td>SAML Context</td>
<td>Select the appropriate SAML context from the drop-down menu. The list includes SAML authentication contexts that are currently supported according to SAML 2.0 specifications.</td>
</tr>
<tr>
<td>Authentication Score</td>
<td>When you create access policies for either the default access policy set or for Web-application-specific policy sets, you configure a minimum authentication score. The policies require users to authenticate using an authentication method with the specified authentication score or higher to access Horizon Workspace, in the case of a default access policy, or a Web application, in the case of a Web-application-specific policy. Apply an authentication score based on your predetermined security levels for authentication methods.</td>
</tr>
<tr>
<td>Default Method</td>
<td>To make the authentication method the default, select <strong>Default Method</strong>. The <strong>Default Method</strong> option is related to the SAML Context option. The following situation provides an example of when Horizon Workspace uses the authentication method you checked as the default method. While adding an authentication method, you select a SAML context. Later, the SAML context that the third-party identity provider instance sends does not match the SAML context you selected for that identity provider instance and Horizon Workspace does not recognize the SAML context sent. Instead of ending the authentication attempt, Horizon Workspace attempts to authenticate the user using the authentication method that you selected as the default method.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

**What to do next**

- Associate each authentication method with the appropriate identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.
- Associate access policies with authentication methods by setting the appropriate minimum authentication score for each access policy.

**Add and Configure an Identity Provider Instance**

By adding and configuring identity provider instances to your Horizon Workspace deployment, you can provide high availability, support additional user authentication methods, and add flexibility in the way you manage the user authentication process based on user IP address ranges.

Add additional identity provider instances to your Horizon Workspace deployment for high availability purposes and, when Horizon Workspace is deployed in a multi-forest Active Directory environment, add an additional identity provider instance for each user store you plan add to your deployment.
Prerequisites

- Perform the necessary planning.
- Determine the best way to integrate Horizon Workspace with Active Directory to meet the needs of your organization. You can configure a single domain, a multi-domain forest, or a multi-forest Active Directory deployment. See Chapter 4, “Integrating Horizon Workspace with Active Directory,” on page 15.
- Determine the authentication types required to meet the needs of your organization. For example, you can configure Kerberos authentication for users internal to your organization and RSA SecurID authentication for users external to your organization. You can set up this type of configuration by using a single identity provider instance for both authentication methods or by using a separate identity provider instance for each authentication method.
- Deploy Horizon Workspace with a single Active Directory domain during the proof-of-concept phase of your deployment.
- Prepare additional identity provider instances for your Horizon Workspace deployment.
- To add additional Connector instances, use the `hznAdminTool addvm` command in the configurator-va virtual machine to manually add instances. That command registers the Connector instance and adds its name to the Identity Providers page. See Installing and Configuring Horizon Workspace.

**NOTE** To add Connector instances for a multi-forest deployment, see the `hznAdminTool addvm` instructions that specify the command line options `--useGatewayAsIDP=n` and `--activateOnly=y`. The `--activateOnly=y` option activates the Connector instance without automating the configuration process. Use the Connector Web interface to manually configure each of these instances.

- To add a third-party identity provider instance, perform the following tasks. See “Overview of Configuring Horizon Workspace to Use a Third-Party Identity Provider Instance,” on page 26 for a complete list of tasks related to configuring Horizon Workspace to use a third-party identity provider instance.
  - Verify that the third-party instances are SAML 2.0 compliant and that Horizon Workspace can reach them.
  - Determine how Horizon Workspace obtains the metadata from the third-party instance and copy and save the appropriate metadata information from the third-party instance that you can paste into the Horizon Workspace Administrator Web interface during configuration. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.
  - To enable Horizon Workspace to use additional authentication methods, use the Administrator Web interface to configure the additional authentication methods. See “Add or Edit a User Authentication Method,” on page 22.
- Use the Administrator Web interface to configure network ranges. See “Add or Edit a Network Range,” on page 21.
- To integrate Horizon Workspace into a multi-forest Active Directory deployment, use the Administrator Web interface to add the necessary number of user stores. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16.

Procedure

1. Log in to the Administrator Web interface.
2. Select **Settings > Identity Providers**.
3 Edit an existing Connector instance or add a third-party identity provider instance.

**IMPORTANT** Use the Add Identity Provider option for adding third-party identity provider instances. Do not use the option to add a Connector instance unless VMware technical support instructs you to do so.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector</td>
<td>Click <strong>Edit</strong> for the Connector instance to configure. You add additional Connector instances from the command line as a prerequisite to this task. That command registers the Connector instance and adds its name to the Identity Providers page.</td>
</tr>
<tr>
<td>Third-Party Identity Provider</td>
<td>Click <strong>Add Identity Provider</strong>. This option prompts you for information that enables Horizon Workspace to register an existing third-party identity provider instance.</td>
</tr>
</tbody>
</table>

4 Edit the identity provider instance settings.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The identity provider type drop-down menu is only available when you add an identity provider instance, not when you edit one. Select <strong>Automatic</strong> for Connector instances. Do not select this option unless VMware technical support instructs you to do so. Select <strong>Manual</strong> for third-party identity provider instances.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>Type a name for this identity provider instance.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for this identity provider instance.</td>
</tr>
<tr>
<td>User Store</td>
<td>The User Store text box lists the user stores available in your Horizon Workspace deployment. Select all the user stores you want to associate with this identity provider instance.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>The Authentication Methods text box lists the user authentication methods available in your Horizon Workspace deployment. The list includes the default authentication methods and additional methods you added previously to support third-party identity providers. Adding additional authentication methods is described as a prerequisite to this task. If the authentication method you intend to select is not in the list, add that authentication method as described in the prerequisite. Select the authentication methods for Horizon Workspace to apply when users who are associated with this identity provider instance log in. <strong>NOTE</strong> Verify that selected authentication methods are enabled and properly configured. See <em>Installing and Configuring Horizon Workspace</em>.</td>
</tr>
<tr>
<td>Configure Via</td>
<td>The Configure Via option is only available when you add a third-party identity provider instance and select <strong>Manual</strong> as the identity provider type. Select a URL identifier method. <strong>To enable Horizon Workspace to receive the metadata of the third-party identity provider instance for registration purposes</strong>, type the URL to the metadata in the <strong>Auto-discovery</strong> text box. <strong>Copy the XML metadata from the identity provider instance and paste it in the Meta data XML text box.</strong></td>
</tr>
<tr>
<td>Network Ranges</td>
<td>The network ranges text box lists the existing network ranges in your Horizon Workspace deployment. Select the network ranges of the users, based on their IP addresses, that you want to direct to this identity provider instance for authentication.</td>
</tr>
</tbody>
</table>

5 Click **Save**.
6 If necessary, change the order of the identity provider instances.

   Horizon Workspace searches for an IP address in the list of identity provider instances from top to bottom. If an IP address is assigned to more than one identity provider instance, Horizon Workspace recognizes the first instance, the identity provider instance highest on the list.

   a Click Edit Order of Identity Providers.
   b Use the up and down arrows to move an identity provider instance to the appropriate location.
   c Click Save.

What to do next

- If you are configuring Horizon Workspace for a multi-forest environment, inform your Horizon Workspace users of their respective domains and explain that when they log in, they must select a domain from the drop-down menu. Inform them that they can check the Remember this setting check box to prevent the prompt from being repeated at each login.
- If you added a third-party identity provider instance, copy and save the Horizon Workspace information required to configure a third-party identity provider instance. See “Obtain the Horizon Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance,” on page 27.

Overview of Configuring Horizon Workspace to Use a Third-Party Identity Provider Instance

To configure Horizon Workspace to use a third-party identity provider instance, you must perform several specific steps throughout the configuration.

Pre-Configuration

Complete the following tasks prior to using the Horizon Workspace Administrator Web interface to add the third-party identity provider instance.

1 Verify that the third-party instances are SAML 2.0 compliant and that Horizon Workspace can reach them.

2 Determine how Horizon Workspace obtains the metadata from the third-party instance and copy and save the appropriate metadata information from the third-party instance that you can paste into the Horizon Workspace Administrator Web interface during configuration. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

3 To enable Horizon Workspace to use authentication methods supported by the third-party identity provider, use the Administrator Web interface to configure the additional authentication methods. See “Add or Edit a User Authentication Method,” on page 22

4 Edit an authentication methods by selecting the Default Method checkbox. This action allows Horizon Workspace to use that authentication method in case of an issue with the third-party authentication method. See “Add or Edit a User Authentication Method,” on page 22.

Configuration

When using the Administrator Web interface to add an identity provider instance, perform the following steps specific to third-party identity providers. See “Add and Configure an Identity Provider Instance,” on page 23.

1 Click the + Add Identity Provider button and select Manual from the Type drop-down menu.
2 Select the authentication methods supported by the third-party-identity provider instance that you plan to use with Horizon Workspace.

3 Use the **Configure Via** option to select how to transfer the metadata of the third-party identity provider instance to Horizon Workspace, either by using a URL to the metadata or by copying and pasting the metadata.

**Post Configuration**

Gather the Horizon Workspace SAML information and apply it to the third-party identity provider instance. See “Obtain the Horizon Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance,” on page 27.

1 Use the Horizon Workspace Administrator Web interface to gather the SAML information necessary to configure the third-party identity provider instance.

2 Configure the third-party identity provider instance by applying the SAML information you gathered from Horizon Workspace.

**Obtain the Horizon Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance**

When integrating Horizon Workspace with a third-party identity provider instance, after you perform the configuration on the Horizon Workspace side, you must copy and prepare the SAML certificate information required to perform the configuration on the third-party identity provider side.

**Prerequisites**

Use the Horizon Workspace Web interface to add a third-party identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.

**Procedure**

1 Copy and Save the SAML signing certificate in Horizon Workspace.
   a Log in to the Administrator Web interface.
   b Select **Settings > SAML Certificate**.
   c Copy the certificate information in the Signing Certificate section.
   d Save the certificate information to a text file for later use when you configure the third-party identity provider instance.

2 Make the SAML SP metadata available to the third party identity provider instance.
   a On the Download SAML Certificate page, click **Service Provider (SP) metadata**.
   b Copy and save the appropriate information using the method that best suits your organization.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy the URL of the Page</td>
<td>Copy and save the URL of the Service Provider (SP) metadata page.</td>
</tr>
<tr>
<td>Copy the XML on the Page</td>
<td>Copy and save the content of the page to a text file.</td>
</tr>
</tbody>
</table>

Use this copied information later when you configure the third-party identity provider.
3 Determine the user mapping from the third-party identity provider instance to Horizon Workspace.

When you configure the third-party identity provider, edit the SAML assertion in the third-party identity provider to map Horizon Workspace users.

<table>
<thead>
<tr>
<th>NameID Format</th>
<th>User Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
<td>The NameID value in the SAML assertion is mapped to the email address attribute in Horizon Workspace.</td>
</tr>
<tr>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</td>
<td>The NameID value in the SAML assertion is mapped to the username attribute in Horizon Workspace.</td>
</tr>
</tbody>
</table>

**What to do next**

Apply the information you copied for this task as necessary to configure the third-party identity provider instance.

**Editing the Default Access Policy Set**

Horizon Workspace includes a default access policy set that controls user access to Horizon Workspace User Portal. You can edit the policy set by editing, deleting, or adding policies as necessary.

Each policy in the default access policy set requires that a set of criteria be met in order for Horizon Workspace to allow access to the user portal. See Chapter 6, “Managing Access Policy Sets,” on page 31.

The following access policy set serves as an example of how you can configure the default access policy set to control access to Horizon Workspace User Portal. See “Edit an Access Policy Set,” on page 34 for instructions.

**Example Default Access Policy Set**

This example illustrates how you can edit the default access policy set.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Network</th>
<th>Minimum Authentication Score</th>
<th>TTL (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Internal Range</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>External</td>
<td>All Ranges</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Policies are evaluated in the preceding order. You can drag a policy in a policy set up or down to change the priority for evaluation.

The preceding example policy set applies to the following use case.

**Default Access Policy, Browser Use Case**

1. **Internal.** To access Horizon Workspace from an internal (Internal Range) network, Horizon Workspace presents users with the Active Directory password authentication method. To ensure that Horizon Workspace attempts to authenticate users with Kerberos authentication first, you make the authentication score of the Kerberos method higher than the authentication score of the password method and you place Kerberos at the top of the list on the Authentication Methods page. You also assign a network range for internal users. The user logs in using a browser and now has access to the user portal for an eight-hour session.

2. **External.** To access Horizon Workspace from an external (All Ranges) network, the user is required to login with SecurID, which for this example has an authentication score of 3. The user logs in using a browser and now has access to the user portal for a four-hour session.
When a user attempts to access a resource, except for a Web application covered by a Web-application-specific policy set, the default portal access policy set applies.

For example, the time-to-live (TTL) for such resources matches the TTL of the default portal access policy set. If the TTL for a user who logs in to the user portal is 8 hours according to the default portal access policy set, when the user attempts to launch a resource, the application launches without requiring the user to reauthenticate.
Managing Access Policy Sets

You can configure the default access policy set to specify criteria that must be met for users to access Horizon Workspace User Portal. You can also create Web-application-specific access policy sets to specify criteria that must be met for users to launch specified Web applications.

To apply an access policy, you create the policy as a part of an access policy set. Each policy in an access policy set can specify the following.

- Where users are allowed to log in from, such as inside or outside the enterprise network.
- The minimum authentication score, which defines the authentication methods allowed for that policy.
- The number of hours of access users are provided.

**Note** Horizon Workspace access policies do not control the length of time that a Web application session lasts. They control the amount of time that users have to launch a Web application.

Horizon Workspace has a default access policy set that you can edit. This access policy set controls access to Horizon Workspace as a whole. See “Editing the Default Access Policy Set,” on page 28. To control access to specific Web applications, you can create additional access policy sets. If you do not apply an access policy set to a Web application, the default access policy set applies.

This chapter includes the following topics:

- “Overview of Access Policy Settings,” on page 31
- “Managing Web-Application-Specific Access Policy Sets,” on page 32
- “Edit an Access Policy Set,” on page 34
- “Add a Web-Application-Specific Access Policy Set,” on page 35
- “Apply a Web-Application-Specific Access Policy Set,” on page 36

**Overview of Access Policy Settings**

An access policy set contains one or more access policies. Each access policy consists of settings that you can configure to manage user access to the Horizon Workspace User Portal as a whole or to specified Web applications.

Each access policy links a network range to a minimum authentication score. A user logging in from an IP address within the applied policy’s specified network range is presented with an authentication method that is equal to or higher than the minimum authentication score of the policy. Each identity provider instance in your Horizon Workspace deployment also links network ranges with authentication methods. When you configure an access policy, ensure that the network range and authentication score pairing that you create are covered by an existing identity provider instance.

When you create an access policy, you can configure the following settings.
Network

For each access policy, you determine the user base by specifying a network range. A network range consists of one or more IP ranges. You create network ranges from the Network Ranges page in the Administrator Web interface prior to configuring access policy sets.

Minimum Authentication Score

You assign an authentication score to each authentication method when you configure the Authentication Methods page in the Administrator Web interface prior to configuring access policy sets.

Horizon Workspace supports Active Directory password, Kerberos, and RSA SecurID authentication methods by default. When you integrate third-party identity provider instances into your Horizon Workspace deployment, Horizon Workspace extends support to the additional authentication methods supported by the third-party identity providers.

When a user logs in to Horizon Workspace using an authentication method, Horizon Workspace records time of authentication and the method used for authentication.

When the user then attempts to access a Web application that has an assigned access policy set, Horizon Workspace compares the user’s current authentication score with the authentication score required for access to the Web application. If the user’s current authentication score is lower than the minimum required authentication score for the requested application, Horizon Workspace redirects the user to an identity provider instance that provides the stronger authentication. If the user’s current authentication score is equal to or higher than the minimum required authentication score for the requested application, Horizon Workspace launches the application after verifying the time-to-live value. See the time-to-live explanation that follows. Horizon Workspace denies the request to access the user portal or to launch a Web application under the following conditions.

- No policy is defined for the request.
- No authenticating identity provider instance is defined for the minimum authentication score.
- The user failed to authenticate with all the authentication methods.

Time-To-Live

For each access policy, you assign a time-to-live (TTL) value. The TTL value determines the maximum amount of time users have since their last authentication event to access Horizon Workspace or to launch a specific Web application. For example, a TTL value of 4 in a Web application policy gives users four hours to launch the web application unless they initiate another authentication event that extends the TTL value.

Managing Web-Application-Specific Access Policy Sets

You can create Web-application-specific access policies. For example, you can create an access policy set for a Web application that specifies which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required.

**ATTENTION** As a best practice, configure the minimum authentication score of Web-application-specific policies to be equal to or higher than the minimum authentication score of policies in the default access policy set that have corresponding network ranges.

The following Web-application-specific access policy set provides an example of a policy set you can create to control access to specified Web applications. See Chapter 6, “Managing Access Policy Sets,” on page 31.

Example 1 Web-Application-Specific Policy Set

This example illustrates a policy set you might create and apply to a sensitive application.
### Strict Web-Application-Specific Access Policy Set, Browser Use Case

1. To access Horizon Workspace from outside the enterprise network, the user is required to login with RSA SecurID, which has a minimum authentication score of 3 according to the example. See the External policy example in “Editing the Default Access Policy Set,” on page 28. The user logs in using a browser and now has access to the user portal for a four hour session as provided by the default access policy set.

2. After four hours, the user tries to launch a Web application with the Example 1 Web-application specific policy set applied.

3. Horizon Workspace checks the policies in the Example 1 policy set and applies the External policy with the All Ranges network range since the user request is coming from a Web browser and from the All Ranges network range.

   The user is logged in with a minimum authentication score of 3, an appropriate authentication score to launch the sensitive application, but the TTL of the policy just expired. Therefore, the user is redirected for reauthentication. The reauthentication provides the user with another four hour session and the ability to launch the application. For the next four hours the user can continue to launch the application without having to re-authenticate.

### Example 2 Web-Application-Specific Policy Set

This example illustrates a policy set you might create and apply to an especially sensitive application.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Network</th>
<th>Minimum Authentication Score</th>
<th>TTL (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtraSensitive</td>
<td>All Ranges</td>
<td>Level 3</td>
<td>1</td>
</tr>
</tbody>
</table>

The preceding example policy set applies to the following use case.

### Extra Strict Web-Application-Specific Access Policy Set Use Case

1. User logs in from an inside the enterprise network using the Password authentication method, which is level 1 according to the example. See the Internal policy example in “Editing the Default Access Policy Set,” on page 28.

   Now, the user has access to the user portal for eight hours.

2. The user immediately tries to launch a Web application with the Example 2 policy set applied, which requires level 3 or above authentication.

3. The user is redirected to an identity provider that provides level 3 or higher authentication strength, such as a Connector instance requiring RSA SecurID authentication.

4. After the user successfully logs in, Horizon Workspace launches the application and saves the authentication event.

   The user can continue to launch this application for up to an hour but is asked to reauthenticate after an hour unless the user initiated a level 3 or higher authentication event within an hour of the launch, as dictated by the policy.
Edit an Access Policy Set

You can edit the default access policy set, which is a pre-existing policy set that controls user access to Horizon Workspace as a whole, or you can edit Web-application-specific policy sets that you previously created manually.

You can remove an entire Web-application-specific access policy set at anytime. The default access policy set is permanent. You can edit it, but you cannot remove it.

You can edit an existing policy set, either the default access policy set or a Web-application-specific access policy set, by removing existing policies from the set, editing existing policies in the set, or adding new policies to the set. For an overview of access policy sets, see Chapter 6, “Managing Access Policy Sets,” on page 31.

For information and examples of policy sets, see the appropriate topic.

Prerequisites
- Configure the appropriate identity providers for your deployment. See “Add and Configure an Identity Provider Instance,” on page 23.
- Configure the appropriate network ranges for your Horizon Workspace deployment. See “Add or Edit a Network Range,” on page 21.
- Configure the appropriate authentication methods for your deployment. See “Add or Edit a User Authentication Method,” on page 22.

Procedure
1. Log in to the Administrator Web interface.
3. (Optional) To permanently delete a Web-application-specific access policy set, click Remove for the policy set.
   The Remove option is not available for the default access policy set. The default access policy set cannot be deleted.
4. Click Edit for the existing policy set to configure.
5. (Optional) If appropriate, change the policy set name and description in the respective text boxes.

NOTE Horizon Workspace displays the text in the Policy Set Name and Description text boxes in English. You can edit this text, which includes changing the text to a different language.
6 (Optional) If appropriate, edit an existing policy, remove an existing policy, or add a new policy.

As a best practice, configure the minimum authentication score of Web-application-specific policies to be equal to or higher than the minimum authentication score of policies in the default access policy set that have corresponding network ranges.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Edit an Existing Policy  | a Click the name of the policy to configure.  
                          | b Change policy settings as appropriate.  
                          | c Click Apply. |
| Remove an Existing Policy| a Click the name of the policy to remove.  
                          | b Click Remove. |
| Add a New Policy         | a Click + Access Policy to add a new policy.  
                          | b Configure policy settings as appropriate.  
                          | c Click Add. |

7 Click Save.

The edited access policy set takes effect immediately.

What to do next

If the policy set is a Web-application-specific access policy set that is not yet applied, apply the policy set to one or more Web applications.

Add a Web-Application-Specific Access Policy Set

You can create Web-application-specific policy sets to manage user access to specific Web applications.

For an overview of access policy sets, see Chapter 6, “Managing Access Policy Sets,” on page 31. For information and examples of Web-application-specific access policy sets, see “Managing Web-Application-Specific Access Policy Sets,” on page 32.

Prerequisites

- Configure the appropriate identity providers for your deployment. See “Add and Configure an Identity Provider Instance,” on page 23.
- Configure the appropriate network ranges for your Horizon Workspace deployment. See “Add or Edit a Network Range,” on page 21.
- Configure the appropriate authentication methods for your deployment. See “Add or Edit a User Authentication Method,” on page 22.
- Especially when initially configuring Horizon Workspace, if you plan to edit the default portal access policy set (to control user access to Horizon Workspace as a whole), configure it before creating Web-application-specific policy sets.

Procedure

1 Log in to the Administrator Web interface.
2 Select Policies > Access Policy Sets.
3 Click + Access Policy Set to add a new policy set.
4 Add a policy set name and description in the respective text boxes.
5 Click + Access Policy to add the first policy.
6 Configure policy settings as appropriate.

| ATTENTION | As a best practice, configure the minimum authentication score of Web-application-specific policies to be equal to or higher than the minimum authentication score of policies in the default access policy set that have corresponding network ranges. |

7 Click Add.

8 (Optional) Repeat the steps to add policies until the policy set suits the needs of your organization.

9 Click Save to save the policy set.

**What to do next**

Apply the policy set to one or more Web applications.

**Apply a Web-Application-Specific Access Policy Set**

After you create a Web-application-specific access policy set, you can apply the set to specific Web applications to control user access to those applications.

Horizon Workspace applies the default access policy set to all new Web applications. You must apply a Web-application-specific policy set to a Web application to override the default access policy set.

**Prerequisites**

If not already created, create a Web-application-specific access policy set to control user access to a specific Web application. See “Add a Web-Application-Specific Access Policy Set,” on page 35

**Procedure**

1 Click the Catalog tab.

2 Click Any Application Type > Web Applications.

3 Click the Web application to which to apply a Web-application-specific access policy set.

   The information page for the Web application appears with the Entitlements tab selected by default.

4 Click Access Policies.

5 From the Access Policy Set drop-down menu, select the Web-application-specific access policy set to apply to the application.

6 Click Save.

The access policy set now controls user access to the application.
Managing Users and Groups

You can manage and monitor users and groups, which includes the users and groups imported from Active Directory, guest users, and Horizon Workspace groups.

In the Horizon Workspace Administrator Web interface, the Users & Groups page provides a user-and-group-centric view of Horizon Workspace. For example, from the Entitlements page for a user, you can entitle that user to a resource, and from the Entitlements page of a group, you can entitle that group to a resource. Alternatively, you can take a resource-centric view of Horizon Workspace by using the Catalog page. For example, from the Entitlements page for a resource, you can entitle that resource to a user or group.

This chapter includes the following topics:

- “Horizon Workspace User and Group Types,” on page 37
- “Manage Horizon Workspace Groups,” on page 38
- “Manage Horizon Workspace Users,” on page 43
- “Manage Guest Users,” on page 49
- “Update the Settings That Select Horizon Workspace Users from Active Directory,” on page 50

Horizon Workspace User and Group Types

With the Horizon Workspace Administrator Web interface, you can manage users, guest users, and groups.

Users

Horizon Workspace users are users imported from Active Directory or, if you are deploying Horizon Workspace in evaluation mode, the Demo User Store. The Horizon Workspace user base is updated according to your directory server synchronization schedule.

Groups

The types of groups that can appear in the Administrator Web interface are groups imported from your directory server and Horizon Workspace groups, which are groups you create yourself using Horizon Workspace.
Group Type | Description
---|---
Directory Server Groups | You use the Configurator or Connector Web interface to import groups from your directory server to Horizon Workspace. You cannot use Horizon Workspace to edit the membership of these groups. In the Administrator Web interface, a lock icon next to a group name indicates that the group is a directory server group. You cannot use Horizon Workspace to edit or delete directory server groups. Imported Directory Server groups are updated in Horizon Workspace according to your directory server synchronization schedule.

Horizon Workspace Groups | You use the Administrator Web interface to create Horizon Workspace groups, which are groups you customize to best suit the use of Horizon Workspace within your enterprise. You can create Horizon Workspace groups by adding a combination of users and groups. The groups you add can be either preexisting Horizon Workspace groups, or groups imported from your directory server. In the Administrator Web interface, a check box next to a group name indicates that the group is a Horizon Workspace group. You can use Horizon Workspace to delete a Horizon Workspace group or to modify the users in the group.

You can specify which resources the group’s members are entitled to access and use. Instead of defining entitlements for each individual user, you can entitle a set of users by entitling the group. A user can belong to multiple groups. For example, if you create a Sales group and a Management group, a sales manager can belong to both groups. You can specify which mobile policy settings apply to the group’s members.

Guest Users

The guest users feature is an optional feature that applies solely to the Horizon Workspace file-sharing service. When Horizon Workspace users invite an external user, either a directory server user not synched to Horizon Workspace or someone outside of the enterprise, the invited user is created as a guest user. Guest users access the files and folders they were invited to share by logging in with a user name and password. The password is self managed. You can turn off the guest user attribute in the class of service (COS) that is assigned to the Horizon Workspace users. See “Edit an Existing Class of Service,” on page 75 or “Create a Class of Service,” on page 77 for information about the External Folder Sharing Allowed option.

Manage Horizon Workspace Groups

Creating groups, modifying the membership of groups, and deleting groups are tasks you can perform in Horizon Workspace that only apply to Horizon Workspace groups. Entitling groups to resources and applying mobile policy sets are tasks you can perform for both Horizon Workspace groups and Active Directory groups.

Procedure

- To create a Horizon Workspace group, select **Users & Groups > Groups**, click **Create Group**, and provide the group name and description.
- To delete one or more Horizon Workspace groups, select **Users & Groups > Groups**, select the check boxes that correspond to the Horizon Workspace groups you want to delete, and click **Delete Groups**.

You can only delete Horizon Workspace groups. A lock icon appears next to Active Directory group names, indicating that the group is a Active Directory group and that you cannot use Horizon Workspace to edit or delete the group.

What to do next

After you create a Horizon Workspace group, you can modify the membership of the group. See “Modify Horizon Workspace Group Membership,” on page 39.
Modify Horizon Workspace Group Membership

You can modify Horizon Workspace group membership.

By using a group, you can entitle more than one user to the same resources at the same time, instead of entitling each user individually. You can also apply the same class of service and mobile policy settings to the same set of users by using a group.

You use group rules to define which users are members of a particular Horizon Workspace group. A user can belong to multiple groups. For example, if you create a Sales group and a Management group, a sales manager is a member of both groups.

Procedure

1. Log in to the Administrator Web interface as an administrator.

2. Click the **Users & Groups** tab, and click the **Groups** tab.
   - A check box next to a group name indicates that the group is a Horizon Workspace group.
   - A lock next to a group name indicates that the group is a directory server group. You manage directory server groups directly in the directory server. You cannot use Horizon Workspace to define the membership of directory server groups.

3. Click the name of the Horizon Workspace group whose membership you want to modify.

4. Click the **Users in this Group** tab.
   - The system displays the list of users that are currently members in the group.

5. Click **Modify Users in This Group**.

6. Select an option from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Any of the following</strong></td>
<td>Grants group membership when any of the conditions for group membership are met. This option works like an OR condition. For example, if you select <strong>Any of the following</strong> for the rules Group Is Sales and Group Is Marketing, sales and marketing staff are granted membership to this group.</td>
</tr>
<tr>
<td><strong>All of the following</strong></td>
<td>Grants group membership when all of the conditions for group membership are met. This works like an AND condition. For example, if you select <strong>All of the following</strong> for the rules Group Is Sales and Email Starts With ‘western_region’, only sales staff in the western region are granted membership to this group. Sales staff in other regions are not granted membership.</td>
</tr>
</tbody>
</table>
Configure one or more rules for your Horizon Workspace group. You can nest rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Group             | - Select **Is** to choose a group to associate with this Horizon Workspace group. Type a group name in the text box. As you type, a list of group names appears.  
- Select **Is Not** to choose a group to exclude from this Horizon Workspace group. Type a group name in the text box. As you type, a list of group names appears. |
| Attribute Rules   | The following rules are available for all attributes, including default attributes and any additional custom attributes that your enterprise configured. Examples of attributes are email and phone.  
   **Note**: Rules are not case-sensitive.  
   - Select **Matches** to grant group membership for directory server entries that exactly match the criteria you enter. For example, your organization might have a business travel department that shares the same central phone number. If you want to grant access to a travel booking application for all employees who share that phone number, you can create a rule such as Phone Matches (555) 555-1000.  
   - Select **Does Not Match** to grant group membership to all directory server entries except those that match the criteria you enter. For example, if one of your departments shares a central phone number, you can exclude that department from access to a social networking application by creating a rule such as Phone Does Not Match (555) 555-2000. Directory server entries with other phone numbers have access to the application.  
   - Select **Starts With** to grant group membership for directory server entries that start with the criteria you enter. For example, your organization's email addresses might begin with the departmental name, such as sales_username@example.com. If you want to grant access to an application to everyone on your sales staff, you can create a rule, such as Email Starts With sales_.  
   - Select **Does Not Start With** to grant group membership to all directory server entries except those that start with the criteria you enter. For example, if the email addresses of your human resources department are in the format hr_username@example.com, you can deny access to an application by setting up a rule, such as Email Does Not Start With hr_. Directory server entries with other email addresses have access to the application. |

Any of the following  
Group membership to be granted when any of the conditions for group membership are met for this rule. This is a way to nest rules. For example, you can create a rule that says **All of the following**: Group Is Sales; Group Is California. For Group Is California, Any of the following: Phone Starts With 415; Phone Starts With 510. The group member must belong to your California sales staff and have a phone number that starts with either 415 or 510.

All of the following  
All of the conditions to be met for this rule. This is a way to nest rules. For example, you can create a rule that says **Any of the following**: Group Is Managers; Group Is Customer Service. For Group Is Customer Service, all of the following: Email Starts With cs_; Phone Starts With 555. The group members can be either managers or customer service representatives, but customer service representatives must have an email that starts with cs_ and a phone number that starts with 555.

(Optional) Specify individual users to add to, or exclude from, this Horizon Workspace group by checking the appropriate check box and typing the user names.

Click **Next**, and click **Save**.
View Group Information

You can view detailed information about a group such as its entitled resources, its membership, and its applied mobile policy sets using the Horizon Workspace Administrator Web interface.

Procedure

1. Log in to the Administrator Web interface.

2. Select Users & Groups > Groups.

   The page displays a list of all of the groups in your Horizon Workspace deployment with some high-level information about each group.

   - A check box next to a group name indicates that the group is a Horizon Workspace group. You define and manage Horizon Workspace groups within Horizon Workspace.
   
   - A lock next to a group name indicates that the group is a directory server group. You manage directory server groups in your organization's directory server.
   
   - The page displays the following information about each group.

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Users</td>
<td>The number members in the group.</td>
</tr>
<tr>
<td>Number Applications</td>
<td>The number of resources entitled to the group as a whole.</td>
</tr>
<tr>
<td>User Store</td>
<td>The user store with which an Active Directory group is associated. Unless Horizon Workspace is deployed in a multi-forest Active Directory environment, the deployment has a single user store named default.</td>
</tr>
</tbody>
</table>

3. Click a group’s name.

   The group's details page is displayed. The group's name and assigned class of service (COS), if one is assigned to the group, are listed at the top of the page. A COS is assigned if the Horizon Workspace file-sharing service is entitled to the group. You can click the COS name to examine the file sharing and storage settings of the assigned COS.
4 Click the tab that corresponds to the information you want to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlements</td>
<td>The group’s Entitlements page is displayed. In this page, you can:</td>
</tr>
<tr>
<td></td>
<td>- View the list of resources entitled to the users of the group.</td>
</tr>
<tr>
<td></td>
<td>- Click Add entitlement to entitle the group’s users to the individual</td>
</tr>
<tr>
<td></td>
<td>resources that are available in your catalog.</td>
</tr>
<tr>
<td></td>
<td>- Click the name of a listed entitled resource to display that resource’s</td>
</tr>
<tr>
<td></td>
<td>Edit page.</td>
</tr>
<tr>
<td></td>
<td>- For resource types that have an Edit button, you can click the button to</td>
</tr>
<tr>
<td></td>
<td>entitle or unentitle the group’s users to resources of that type, or to</td>
</tr>
<tr>
<td></td>
<td>customize the options for each entitled resource. From the Entitlements</td>
</tr>
<tr>
<td></td>
<td>page, you can make the following changes:</td>
</tr>
<tr>
<td></td>
<td>- For web applications, click Edit to change the group’s entitlements</td>
</tr>
<tr>
<td></td>
<td>to the web applications or the type of deployment for the group’s</td>
</tr>
<tr>
<td></td>
<td>entitled web applications. Select Automatic to have the Web application</td>
</tr>
<tr>
<td></td>
<td>displayed by default in the user portal. Select User-Activated to</td>
</tr>
<tr>
<td></td>
<td>allow the users to add the web application to the user’s My Apps area</td>
</tr>
<tr>
<td></td>
<td>from the App Center collection of applications available to that user.</td>
</tr>
<tr>
<td></td>
<td>- For VMware Ready devices, click Edit to specify the Android workspace</td>
</tr>
<tr>
<td></td>
<td>image and the Android apps for the workspace. The deployment type is</td>
</tr>
<tr>
<td></td>
<td>automatic by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: To make the file-sharing capabilities available in the</td>
</tr>
<tr>
<td></td>
<td>managed mobile workspace on VMware Ready devices used by the group’s</td>
</tr>
<tr>
<td></td>
<td>members, entitle the Horizon Files for Android app, and also use the</td>
</tr>
<tr>
<td></td>
<td>Services area of the Entitlements page to entitle the file-sharing</td>
</tr>
<tr>
<td></td>
<td>service.</td>
</tr>
<tr>
<td></td>
<td>- For configuration profiles, click Edit to change the group’s entitlements to VPN configurations. These VPN configurations are used for managed mobile workspaces on VMware Ready devices only. The deployment type is automatic by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>- For View desktop pools, you can view the group’s existing entitlements to the View desktop pools that are integrated with your Horizon Workspace system. Entitlements to View desktop pools are configured in the Horizon View Connection Server instances that are integrated with your Horizon Workspace system. You cannot change entitlements to View desktop pools using the group’s Entitlements page.</td>
</tr>
<tr>
<td></td>
<td>- For ThinApp packages, click Edit to change the group’s entitlements to the ThinApp packages or the type of deployment for the group’s entitled ThinApp packages. Select Automatic to have the ThinApp package displayed by default in the My Apps area of the user portal. Select User-Activated to allow the users to manually add the ThinApp package from the App Catalog to their My Apps area.</td>
</tr>
<tr>
<td></td>
<td>- For Citrix Published Applications, you can view the group’s existing entitlements to the Citrix-based applications that are integrated with your Horizon Workspace system. Entitlements to Citrix-based applications are configured in the Citrix deployments that are integrated with your Horizon Workspace system. You cannot change entitlements to Citrix-based applications using the group’s Entitlements page.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>For the file-sharing service,</td>
<td>in the Services area, click <strong>Edit</strong> to select</td>
</tr>
<tr>
<td></td>
<td>the class of service (COS) for the user.</td>
</tr>
<tr>
<td>For resources types that have</td>
<td>an <strong>Unentitle</strong> button, you can click the button to remove the group’s</td>
</tr>
<tr>
<td>an <strong>Unentitle</strong> button, you</td>
<td>access to use that specific resource.</td>
</tr>
<tr>
<td>can click the button to</td>
<td><strong>NOTE</strong>: The Provisioning Status column is not used. By default, for the</td>
</tr>
<tr>
<td>remove the group’s access to</td>
<td>table rows that have filled-in entries on this page, the Provisioning Status</td>
</tr>
<tr>
<td>use that specific resource.</td>
<td>columns display Not Enabled, and you cannot change this value.</td>
</tr>
</tbody>
</table>

**Users in this Group**

The group’s membership page is displayed. In this page, you can:

- View the list of users that belong to the group.
- Click a user’s name to display the details page for that user.
- Click **Modify Users in This Group** to view and configure the rules that define membership to the Horizon Workspace group. The **Modify Users in This Group** option is available for Horizon Workspace groups, but not for directory server groups.

**Applied Mobile Policy Sets**

The group’s Applied Mobile Policy Sets page is displayed. In this page, you can:

- View the mobile policy sets that are currently applied to the group’s users.
- Click **Select Mobile Policy Sets** to select which mobile policy sets to apply to the group.

**Manage Horizon Workspace Users**

You can manage Horizon Workspace users, the users imported from Active Directory, using the Administrator Web interface.

Managing users in Horizon Workspace includes tasks such as entitling the users to resources, adding users to the appropriate Horizon Workspace groups as necessary, and managing the state of users’ provisioned workspaces.

**Prerequisites**

Install and configure Horizon Workspace. As part of the installation, import users from Active Directory. See *Installing and Configuring Horizon Workspace*.

**View Horizon Workspace User Information**

You can view detailed information about a user such as the user’s entitled resources, group affiliations, and provisioned desktop systems and mobile devices using the Administrator Web interface. A desktop system or mobile device is considered provisioned if the user has installed one of the appropriate Horizon Workspace clients on the system or device, and used the client to access or deploy entitled resources to that system or device.

User attributes are among the user information you can view, such as the Data Node Hostname attribute and additional attributes that you configured Horizon Workspace to retrieve from your directory server during synchronizations. The usefulness of viewing the additional directory server attributes for an individual user depends on how you use such attributes in your deployment. You can use these additional attributes in the following ways:

- To modify membership of a Horizon Workspace group. For example, if you use the manager attribute in Active Directory, you can map the manager attribute to Horizon Workspace. You can create a group where the group rules restrict membership to users with the manager attribute in their Horizon Workspace user record.
- To enable users to access Web applications with specific attribute requirements. For example, a financial application might restrict access to users with the employee ID attribute in their Horizon Workspace user record.
**Procedure**

1. Log in to the Administrator Web interface.

2. Select **Users & Groups > Users**.
   
   The page displays a list of all your Horizon Workspace users.

3. Click a user's name.
   
   The user's details page is displayed. The user's name, email address, role, and the assigned class of service (COS), if one is assigned to the user, are listed at the top of the page.

4. (Optional) Click the name of the displayed role, **User** or **Administrator**, to change the user's role.

   You can promote users to the administrator role, allowing them access to configure the Horizon Workspace Administrator Web interface. Individuals assigned the Administrator role can still access the Web Client as a user. The URL to access the Administrator Web interface is different than the URL to access the Web Client.

   For the following URLs, replace the `HorizonWorkspaceFQDN` placeholder with the actual value.

<table>
<thead>
<tr>
<th>Web Interface</th>
<th>Required Role</th>
<th>URL Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Web Interface</td>
<td>Administrator</td>
<td><code>https://HorizonWorkspaceFQDN/admin</code></td>
</tr>
<tr>
<td>User Portal</td>
<td>User</td>
<td><code>https://HorizonWorkspaceFQDN/web</code></td>
</tr>
</tbody>
</table>

5. (Optional) Click **Show additional attributes** to see additional attributes assigned to the user, such as directory server attributes and the Data Node Hostname attribute.

   The Data Node Hostname attribute is related to the file-sharing service and can appear as an additional attribute for users. The attribute appears when the user is entitled to the file-sharing service. The value assigned to the attribute is the name of the data-va server to which a user's files and folders are stored. You can use this information for troubleshooting purposes if a user cannot access the file-sharing service. See *Installing and Configuring Horizon Workspace*.

6. If a COS is assigned to the user, click the COS name to view the file storage and sharing policy of the user.

   If the user is entitled to the file-sharing service, either directly or through a group, a COS is assigned to the user. The COS includes information such as the account quota, maximum file size, and share expiration.
Click the tab that corresponds to the information you want to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entitlements</strong></td>
<td>The user’s Entitlements page is displayed. In this page, you can:</td>
</tr>
<tr>
<td></td>
<td>■ View the list of resources entitled to the user.</td>
</tr>
<tr>
<td></td>
<td>■ Click <strong>Add entitlement</strong> to entitle the user to resources that are available in your catalog.</td>
</tr>
<tr>
<td></td>
<td>■ Click the name of a listed entitled resource to display that resource’s Edit page.</td>
</tr>
<tr>
<td></td>
<td>■ For resource types that have an <strong>Edit</strong> button, you can click the button to entitle or unentitle the group’s users to resources of that type, or to customize the options for each entitled resource. From the Entitlements page, you can make the following changes:</td>
</tr>
<tr>
<td></td>
<td>■ For web applications, click <strong>Edit</strong> to change the user’s entitlements to the web applications or the type of deployment for each of the user’s entitled web applications. Select <strong>Automatic</strong> to have the web application displayed by default in the user portal. Select <strong>User-Activated</strong> to allow the user to add the web application to the user’s My Apps area from the App Center collection of applications available to that user.</td>
</tr>
<tr>
<td></td>
<td>■ For VMware Ready devices, click <strong>Edit</strong> to specify the workspace image and the Android apps for the workspace. The deployment type is automatic by default, and you cannot change this setting. <strong>Note</strong>: To make the file-sharing capabilities available in the managed mobile workspace on this user’s VMware Ready device, entitle the Horizon Files for Android app, and also use the Services area of the Entitlements page to entitle the file-sharing service.</td>
</tr>
<tr>
<td></td>
<td>■ For configuration profiles, click <strong>Edit</strong> to change the user’s entitlements to VPN configurations. These VPN configurations are used for managed mobile workspaces on VMware Ready devices only. The deployment type is automatic by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>■ For View desktop pools, you can view the user’s existing entitlements to the View desktop pools that are integrated with your Horizon Workspace system. Entitlements to View desktop pools are configured in the Horizon View Connection Server instances that are integrated with your Horizon Workspace system. You cannot change entitlements to View desktop pools using the user’s Entitlements page.</td>
</tr>
<tr>
<td></td>
<td>■ For ThinApp packages, click <strong>Edit</strong> to change the user’s entitlements to the ThinApp packages or the type of deployment for the user’s entitled ThinApp packages. Select <strong>Automatic</strong> to have the ThinApp package displayed by default in the My Apps area of the user portal. Select <strong>User-Activated</strong> to allow the user to manually add the ThinApp package from the App Catalog to the My Apps area.</td>
</tr>
<tr>
<td></td>
<td>■ For Citrix Published Applications, you can view the user’s existing entitlements to the Citrix-based applications that are integrated with your Horizon Workspace system. Entitlements to Citrix-based applications are configured in the Citrix deployments that are integrated with your Horizon Workspace system. You cannot change entitlements to Citrix-based applications using the user’s Entitlements page.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>- For the file-sharing service, click <strong>Edit</strong> to select the class of service (COS) for the user.</td>
</tr>
<tr>
<td></td>
<td>- For resources types that have an <strong>Unentitle</strong> button, you can click the button to remove the user’s access to use that resource.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Provisioning Status column is not used. By default, for the table rows that have filled-in entries on this page, the Provisioning Status columns display Not Enabled, and you cannot change this value.</td>
</tr>
</tbody>
</table>

**Group Affiliations**

A list of the groups to which the user belongs is displayed. Each group name represents a group to which the user is a member. You can click a group's name to display the details page for that group.

**Workspaces**

The user’s Workspaces page is displayed. In this page, you can:

- View lists of the mobile and desktop workspaces that have been provisioned to the user's mobile devices and desktop systems, including the current status of each workspace.

An item is added to the lists when the user logs in to Horizon Workspace for the first time from a device or system using the appropriate Horizon Workspace client application.

For example, the Desktop Workspaces table lists a Mac desktop workspace when the user installs the Horizon Workspace Client for Mac on a Mac OS X system and uses that client to connect to Horizon Workspace for the first time. The Mobile Workspaces lists an Android secure managed workspace when the user has enrolled a VMware Ready Android device with your Horizon Workspace system, and lists a files workspace when the user has connected with an Android or iOS device using the Files for Android or Files for iOS app.

- For a mobile workspace, you can click its name to perform available actions on that mobile workspace. See “Perform Actions on Desktop Systems and Mobile Devices that Users Have Linked with Your Horizon Workspace System,” on page 47.

**Note** By default, only mobile workspaces that have been recently provisioned to the user are initially displayed. To display the list of all of the mobile workspaces that have been previously provisioned to the user, click **View All**. To toggle back to display only the most recently provisioned mobile workspaces, click **View Latest**.

- For a desktop system, you can click **Delete** to remove the corresponding system from Horizon Workspace. You might want to remove a system from Horizon Workspace because the system is lost, stolen, or no longer in use.
Prevent Users from Accessing Horizon Workspace

You can prevent specific directory server users from accessing Horizon Workspace by deleting or disabling their directory server user accounts or, for directory server accounts that will remain active, by creating filters in Horizon Workspace.

**Procedure**

- Prevent users from accessing Horizon Workspace by implementing the task that best suits your enterprise.

<table>
<thead>
<tr>
<th>Option</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete or Disable Directory Server User Accounts</td>
<td>In your directory server, delete or disable user accounts according to the needs of your enterprise.</td>
</tr>
<tr>
<td></td>
<td>If you disable users already entitled to the file-sharing service and you later re-enable those users, Horizon Workspace retrieves those users’ shared files and folders.</td>
</tr>
<tr>
<td>Create Filters in Horizon Workspace for Active User Accounts in Your Directory Server</td>
<td>Using the Connector Web interface of Horizon Workspace, create filters to exclude user accounts from being transferred from the directory server to Horizon Workspace during synchronizations.</td>
</tr>
<tr>
<td></td>
<td>If you use the create filters method with users already entitled to the file-sharing service, their shared files and folders are deleted and not retrievable if you later add these users back. See <em>Installing and Configuring Horizon Workspace</em> for more information about creating filters to exclude users.</td>
</tr>
</tbody>
</table>

After the next directory sync, the users whose accounts you excluded by filtering, deleting, or disabling can no longer access Horizon Workspace.

Perform Actions on Desktop Systems and Mobile Devices that Users Have Linked with Your Horizon Workspace System

After a user connects to your Horizon Workspace system for the first time using one of the native Horizon Workspace applications installed on a desktop system or using one of the native mobile apps installed on a mobile device, that desktop system or mobile device is said to be linked with your Horizon Workspace system. You can perform actions on such linked desktop systems and mobile devices. The available actions that you can perform depend on the type of connection the user made and the current status of the desktop system or device.

For the managed mobile workspaces, the ones of type Android Secure Managed Workspace, you can perform actions on it such as disabling it, resetting its passcode, and wiping it from the device. You can also review information about the VMware Ready Android device, such as the device’s model number and OS version, see what mobile policies are in effect, see the history of activity on the device, and retrieve log information from the device to help VMware Support diagnose issues.

For initial connections that were made using the native Files for iOS app or Files for Android app on a mobile device, you can delete the workspace, which disables the app’s access to the file-sharing capabilities provided by your Horizon Workspace system.

For initial connections that were made using the native Horizon Workspace application on desktop systems, you can delete the connection, which disables the application’s access to the resources and capabilities provided by your Horizon Workspace system to that user’s desktop system.
Prerequisites

Verify the desktop system or mobile device is linked to your Horizon Workspace system. Linking occurs when a Horizon Workspace user makes an initial connection to your Horizon Workspace system in one of the following ways.

- Enrolls a VMware Ready Android device with your Horizon Workspace system.
- Installs the native Files for iOS app or Files for Android app on a mobile device, configures the app with their Horizon Workspace user account, and uses the app to connect to your Horizon Workspace system. After the Files for iOS app or Files for Android app connects to your Horizon Workspace system, the user's Workspaces page displays a corresponding entry in the Mobile Workspaces table as a files workspace.
- Installs the native Horizon Workspace client application on a Windows or Mac system, configures the application with their Horizon Workspace user account, and uses the application to connect to your Horizon Workspace system. After the client application connects to your Horizon Workspace system, the user's Workspace page displays a corresponding entry in the Desktop Workspaces table.

To verify that the user has a linked desktop system or mobile device, in the Administrator Web interface, open the details page for the user, click Workspaces, and review the displayed information.

<table>
<thead>
<tr>
<th>VMware Ready Android devices that the user enrolled with your Horizon Workspace system are listed in the Mobile Workspaces section of the page with a type set to Android Secure Managed Workspace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial connections that the user made using the native Files for iOS app or Files for Android app on a mobile device are listed in the Mobile Workspaces section of the page with a type set to Files Workspace.</td>
</tr>
</tbody>
</table>

**NOTE**

On a VMware Ready Android device, a connection made from the Files for Android app in the managed mobile workspace is listed as a Files Workspace in the Mobile Workspaces section, in addition to the device's entry with the Android Secure Managed Workspace type.

| Initial connections that the user made using the native Horizon Workspace applications on desktop systems are listed in the Desktop Workspaces section of the page. |

Procedure

1. Log in to the Administrator Web interface.
2. Select Users & Groups > Users
3. Click the user's name.
4. Click Workspaces.
5. Click the name of the linked device on which you want to act.

For entries in the Mobile Workspaces section, clicking the displayed name opens the workspace details page associated with that name.

For entries in the Desktop Workspaces section, the Delete action is the available action. You do not click the displayed name of the desktop system.
6 On the workspace details page, click the button for the action you want to perform.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Workspace</td>
<td>The workspace details page displays the Delete Workspace button for initial connections that were made using the native Files for iOS app or Files for Android app on the mobile device. This action disables access to the file-sharing capabilities that the user previously accessed and used using the app. This action does not prevent the user from reconfiguring the Files for iOS app or Files for Android app on that device to access your Horizon Workspace system using their account information.</td>
</tr>
<tr>
<td>Wipe Workspace</td>
<td>This action removes the managed mobile workspace from the VMware Ready Android device. The secure workspace container, its managed apps and data, and the user's account associated with the Switch app are removed from the device, while the user's personal apps and data on the device are untouched. This action does not prevent the user from using Switch to re-enroll with your Horizon Workspace system.</td>
</tr>
<tr>
<td>Disable Workspace</td>
<td>This action disables the VMware Ready Android device’s access to the managed mobile workspace on the device. The user is locked out of the secure workspace. If the user attempts the enrollment process again, the user is prevented from using the managed mobile workspace until you enable the enrolled device's access using the Enable Workspace button.</td>
</tr>
<tr>
<td>Enable Workspace</td>
<td>Enables access for an enrolled device that was previously disabled with the Disable Workspace action.</td>
</tr>
<tr>
<td>Reset Workspace Passcode</td>
<td>For a VMware Ready Android device, this action resets the user's passcode that is used for accessing the managed mobile workspace.</td>
</tr>
</tbody>
</table>

7 For a VMware Ready Android device, if you want to retrieve log information from the device, open the Activity page by clicking Activity, and then click Retrieve Logs.

If the user consents, the enrolled device sends diagnostic information about the managed mobile workspace to your Horizon Workspace system. The logs are sent at the next lease renewal time. Typically, you use this log information to help VMware Support diagnose issues.

8 For a VMware Ready Android device, if you want to see the policies that are in effect on the device, open the Policies page by clicking Policies.

The information in the Resolved Value column indicates the policy settings that are in effect on the device.

Manage Guest Users

You can view and manage information about guest users. A guest user is either a directory server user not synched to Horizon Workspace or someone outside of the enterprise, whom Horizon Workspace users specifically invite to access selected folders.

As an administrator, you can allow Horizon Workspace users to provide guest users with access to specific files. You can then monitor and manage the guest users. For example, you can see who the guest users are and you can lock out or delete specific guest users.

Procedure

1 Log in to the Administrator Web interface.

2 To view and manage user information, click Users & Groups > Guest Users.

The Guest Users page lists the email address, last login time, and access status of every guest user associated with your Horizon Workspace deployment.
3 Manage guest users as needed.
   - To delete guest users, check the check box for each guest user you want to delete and click **Delete Users**.
     This action removes guest users from Horizon Workspace. Deleted guest users lose access to all files previously shared with them.
   - To prevent guest users from logging in to Horizon Workspace, click **Lock** for each guest user to whom you want to block access.
     You can use this option to temporarily block access to Horizon Workspace.
   - To unblock access to previously blocked guest users, click **Unlock** for each guest user to whom you want to unblock access. When you unlock guest users, they are again able to access the files previously shared with them.

**Update the Settings That Select Horizon Workspace Users from Active Directory**

During the Horizon Workspace setup, you specify the Active Directory, user attributes, and a filter to select those Active Directory users that you want to use with Horizon Workspace. You can update these settings using the Connector Web interface.

**Prerequisites**

Verify that you have the information for the changes that you want to make, for example the new base DN, user attributes to include, exclude filter, and so on.

**Procedure**

1 Log in to the Connector Web interface using the administrative password for Horizon Workspace.
   - The Connector Web interface URL is **https://ConnectorHostname/hc/admin/**.
2 Perform the appropriate action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Change the Active Directory server information, such as the server host, port, base DN, bind DN, bind password, and so on. | a Click Directory.  
b Make your changes.  
c Click Save. |
| Change the mapping of Horizon Workspace user attributes to Active Directory user attributes. | a Click User Attributes.  
b Make your changes.  
c Click Save. |
| Change the user selection rules for the filter that defines which Active Directory users are synced to Horizon Workspace. | a Click Directory Sync.  
b Click Edit Directory Sync Rules.  
c Make your changes on the Select Users page as necessary, and click Next.  
d Make your changes on the Select Groups page as necessary, and click Next.  
e Click Push to Horizon.  
f Click Save and Continue. |
Managing the Horizon Workspace Catalog

Your Horizon Workspace catalog is the repository of all the resources that you can entitle to users. The availability of particular resource types in your catalog is controlled by which modules are enabled in Horizon Workspace.

Display your catalog by clicking the Catalog tab in the Horizon Workspace Administrator Web interface. On the Catalog page, you can perform the following tasks:

- Add new resources to your catalog.
- View the resources to which you can currently entitle users.
- Access information about each resource in your catalog.

Depending on their type, some resources can be added to your catalog directly using the Catalog page. Other resource types require you to take action outside the Administrator Web interface.

<table>
<thead>
<tr>
<th>Resource</th>
<th>How to See the Resource in Your Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web application</td>
<td>Enable the Web Applications module. Using the Administrator Web interface, select the Web Applications application type on the Catalog page.</td>
</tr>
<tr>
<td>Mobile application, uploaded</td>
<td>Enable the Mobile Management module. Using the Administrator Web interface, select the Mobile Applications application type on the Catalog page.</td>
</tr>
<tr>
<td>Secure Android container for VMware® Ready™ Android devices</td>
<td>Enable the Mobile Management module. Using the Administrator Web interface, select the Android Workspace Images application type on the Catalog page.</td>
</tr>
<tr>
<td>Virtualized Windows application captured as a ThinApp package</td>
<td>Enable the ThinApp Packages module. Using the Connector Web interface, sync ThinApp packages to your catalog. Using the Administrator Web interface, select the ThinApp Packages application type on the Catalog page.</td>
</tr>
<tr>
<td>Horizon View desktop pool</td>
<td>Enable the View module. Using the Connector Web interface, synch Horizon View desktop pools to your catalog. Using the Administrator Web interface, select the View desktop Pools application type on the Catalog page.</td>
</tr>
<tr>
<td>Citrix-based application</td>
<td>Enable the Citrix Published Applications module. Using the Connector Web interface, sync Citrix-based applications to your catalog. Using the Administrator Web interface, select the Citrix Published Applications application type on the Catalog page.</td>
</tr>
<tr>
<td>File-sharing service</td>
<td>Enable the Horizon Files module. Using the Administrator Web interface, select the Services application type on the Catalog page.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Overview of Horizon Workspace Resource Types,” on page 52
- “Overview of Using Resource Categories,” on page 54
- “View Horizon Workspace Resources,” on page 55
- “Add Resources to Your Catalog,” on page 56
Overview of Horizon Workspace Resource Types

The types of resources that you can define in your catalog for entitlement and distribution to users are Web applications, Windows applications captured as VMware ThinApp packages, Citrix-based applications, VMware Horizon View desktop pools, and the file-sharing. In your catalog, you can also manage the secure Android container that is provisioned to VMware Ready Android devices as the secure base for the mobile workspace on those devices, and upload Android mobile apps to include those apps in that secure mobile workspace.

Before you can entitle a particular resource to your users, you must populate your catalog with that resource. The method you use to populate your catalog with a resource depends on what type of resource it is.

Horizon Workspace File-Sharing Service

1 You perform the relevant preconfiguration steps during installation of Horizon Workspace, such as adding storage to the data-va virtual appliance and configuring a preview server. See Installing and Configuring Horizon Workspace.

2 You populate your catalog with the file-sharing service by enabling the Horizon Files module. See “Enable the Horizon Files Module,” on page 71.

After you perform these tasks, the file-sharing service is available as a resource in your catalog. You can then entitle users to the resource, allowing them to share their files and folders with other users. See “Entitle Users to the File-Sharing Service,” on page 72.

Web Applications

You populate your catalog with Web applications directly on the Catalog page of the Horizon Workspace Administrator Web interface. When you click a Web application displayed on the Catalog page, information about that application is displayed. From the displayed page, you can configure the Web application, such as by providing the appropriate SAML attributes to configure single sign-on between Horizon Workspace and the target Web application. When the Web application is configured, you can then entitle users and groups to that Web application. See “Add Resources to Your Catalog,” on page 56.

Secure Android Container

The secure Android container is a virtual Android operating system that is the base for the managed mobile workspaces provisioned to VMware Ready Android devices. The secure Android container is implemented in your catalog as a ZIP file also known as a workspace image. By either uploading or removing a workspace image, you determine whether that secure Android container is available as a resource in your catalog. By default, Horizon Workspace provides one secure Android container.

Uploaded Android Mobile Applications

Uploaded mobile applications are Android mobile applications that you upload directly into your catalog. These uploaded Android applications are provisioned to VMware Ready Android devices for the managed mobile workspace on those devices. You populate your catalog with these uploaded mobile applications directly using the Catalog page of the Horizon Workspace Administrator Web interface. When you click the icon for a mobile application that has been uploaded into your catalog, information about the application is displayed. From the displayed page, you can configure settings appropriate to the mobile application, and entitle the uploaded mobile application to users and groups.

Note To entitle uploaded Android mobile apps to users and groups, you must first entitle those users and groups to the secure Android container, also known as the Android workspace image, because the uploaded Android apps are deployed only in the secure Android container.
ThinApp Packages

You populate your catalog with Windows applications captured as ThinApp packages by performing the following tasks.

1. If the ThinApp packages to which you want to provide users access do not already exist, create ThinApp packages that are compatible with Horizon Workspace. See the VMware ThinApp documentation.

2. Create a network share and populate it with the compatible ThinApp packages. See *Installing and Configuring Horizon Workspace* for the requirements on the network share and the directory structure.

3. Configure Horizon Workspace to integrate with the packages on the network share. See *Installing and Configuring Horizon Workspace*.


After you perform these tasks, the virtualized Windows applications, the ThinApp packages that you added to the network share, are now available as resources in your catalog. You can then entitle users to those resources.

To launch and run the ThinApp packages that are distributed and managed by Horizon Workspace, users must have the Horizon Workspace for Windows installed on their Windows systems. See “Distributing and Managing ThinApp Packages with Horizon Workspace,” on page 118.

Citrix-Based Applications

You populate your catalog with Citrix-based applications, by performing the following tasks.

1. If not already deployed, deploy Citrix servers, which includes entitling users to Citrix-based applications. See the appropriate Citrix documentation.

2. Integrate your Horizon Workspace deployment with Citrix servers. See *Installing and Configuring Horizon Workspace*.

3. If not already enabled, enable the Citrix Published Applications module on the Dashboard page of the Administrator Web interface. See “Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment,” on page 111.

After you perform these tasks, the Citrix-based applications you entitled to users with Citrix servers are now available as resources in your catalog.

Horizon View Desktop Pools

You populate your catalog with Horizon View desktop pools, and the corresponding Horizon View desktops, by performing the following tasks.

1. If not already deployed, deploy Horizon View desktop pools in VMware Horizon View, which includes entitling users to desktops. See the VMware Horizon View documentation.

2. Integrate your Horizon Workspace deployment with VMware Horizon View. See *Installing and Configuring Horizon Workspace*.

3. If not already enabled, enable the View module on the Dashboard page of the Administrator Web interface. See “Enable the View Module to Integrate Horizon View with Horizon Workspace,” on page 98.

After you perform these tasks, the Horizon View desktops that you entitled to users with VMware Horizon View are now available as resources in your catalog.
Overview of Using Resource Categories

The default method of searching for catalog resources, is by resource type. You can also search by category.

To enable a search of Horizon Workspace catalog resources by category, create categories and apply them to resources

Create a Resource Category

You can create a Horizon Workspace resource category without immediately applying it or you can create and apply a category at the same time.

Procedure

1. Log in to the Administrator Web interface.
2. Click the Catalog tab.
3. Click the checkbox of one or more resources.
   - A checked resource activates the Apply Categories button, which is a requirement for creating a category. To create and apply categories at the same time, click the checkboxes of all the resources to which to apply the new category. If you want to create a category without immediately applying it, the resource selected is not meaningful. In that situation, you can click the checkbox of any resource in the catalog.
4. Click Apply Categories.
5. Type a new category name in the Search categories text box.
6. Click Add category....
   - Horizon Workspace creates the new category, but does not apply it.
7. (Optional) To apply the category to the selected resources, click the checkbox for the new category name.
   - Horizon Workspace applies the category to the selected resources.

What to do next

If appropriate, apply the category to resources. See “Apply a Category to Resources,” on page 54.

Apply a Category to Resources

After you create a category, you can apply that category to any of the resources in the catalog

Prerequisites

Create a resource category.

Procedure

1. Log in to the Administrator Web interface.
2. Click the Catalog tab.
3. Click the checkboxes of all the resources to which to apply the category.
4. Click Apply Categories and select the name of the category to apply.
   - The category is applied to the selected resources.
Remove or Delete a Category

After you create and apply categories to resources, you can disassociate a category from a resource and you can permanently remove a category from the catalog.

you can later remove the category label to disassociate the category from the resource. You can also delete the category permanently from the catalog. When you permanently delete a category, the category disappears from catalog. It no longer appears in the Any Category drop-down menu or as a label to any resource to which you previously applied it.

Procedure
1 Log in to the Administrator Web interface.
2 Click the Catalog tab.
3 Click the checkbox of one or more resources.
   A checked resource activates the Apply Categories button, which is a requirement for removing and deleting a category. To remove a category label from one or more resources, click the checkboxes of all the resources from which to remove the category label. If you want to permanently delete a category, the resource selected is not meaningful. In that situation, you can click the checkbox of any resource in the catalog.
4 Click Apply Categories.

Option | Description
--- | ---
Remove Category from Resources | The checkbox of the label is selected. Click that check box to remove the category label from the selected resource.
Delete Category Permanently | Hover over the category. An x appears. Click the x to permanently remove the category from the catalog.

View Horizon Workspace Resources

Access your catalog to view information about the resources to which you can entitle users, such as Horizon Workspace Web applications, ThinApp packages, Citrix-based applications, Horizon View desktop pools, and the file-sharing service. You can view resources by application type or by category.

Prerequisites
- Enable the resource modules that correspond to the resource types to which you want to entitle users. The Horizon Files module, Web Applications module, Mobile Management module, View module, ThinApp Packages module, and Citrix Published Applications module are available.
- Add resources to the catalog to meet the needs of your enterprise. See Chapter 8, “Managing the Horizon Workspace Catalog,” on page 51.
- To view resources by category, create and apply categories. See “Overview of Using Resource Categories,” on page 54.

Procedure
1 Log in to the Horizon Workspace Administrator Web interface.
2 Click the Catalog tab.
   Horizon Workspace lists all the resources in the catalog.
3 (Optional) To change the sort method click Application or Application type.
4. (Optional) To view resources by a specific type, select a resource type from the **Any Application Type** drop-down menu.

Application types that you have not added to Horizon Workspace do not appear in the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Any Application Type</strong></td>
<td>Lists all of the resources in your catalog.</td>
</tr>
<tr>
<td><strong>Web Applications</strong></td>
<td>Lists only Web applications in your catalog. Web applications include SaaS applications and Web applications managed internally by your enterprise.</td>
</tr>
<tr>
<td><strong>Mobile Applications</strong></td>
<td>Lists only uploaded Android mobile applications in the catalog. These mobile applications are Android applications used in the managed mobile workspace on VMware Ready Android devices.</td>
</tr>
<tr>
<td><strong>Android Workspace Images</strong></td>
<td>Lists the secure Android containers available in your catalog. The secure Android container, also known as a workspace image, is a version of the Android operating system that is installed as the base operating system for secure managed mobile workspaces on VMware Ready Android devices. In addition to the base operating system, a workspace image includes some default applications that one would typically find in a base Android operating system distribution, such as the Calculator and Browser applications.</td>
</tr>
<tr>
<td><strong>ThinApp Packages</strong></td>
<td>Lists only Windows applications captured as ThinApp packages. ThinApp packages appear in your catalog if you add ThinApp packages to your deployment while configuring Horizon Workspace prior to accessing the Administrator Web interface.</td>
</tr>
<tr>
<td><strong>View Desktop Pools</strong></td>
<td>Lists only the Horizon View desktop pools. Horizon View desktop pools appear in your catalog if you integrate Horizon Workspace with VMware Horizon View prior to accessing the Administrator Web interface.</td>
</tr>
<tr>
<td><strong>Citrix Published Applications</strong></td>
<td>Lists only Citrix-based applications. Citrix-based applications appear in your catalog if you integrate Horizon Workspace with your Citrix deployment prior to accessing the Administrator Web interface.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Lists only services in your catalog. The filing-sharing service is the only service available for Horizon Workspace.</td>
</tr>
</tbody>
</table>

5. (Optional) To view resources by a specific category, select one or more category names from the **Any Category** drop-down menu.

Horizon Workspace lists all the resources that meet the criteria you selected.

- If you select one category, Horizon Workspace lists all the resources marked with that category label.
- If you select more than one category, Horizon Workspace only lists resources that marked with all of those category labels.

6. Click the icon for a specific resource to view the details of that resource.

### Add Resources to Your Catalog

You can add Web applications and upload Android mobile applications to your catalog directly using the Catalog page of the Horizon Workspace Administrator Web interface.

See the appropriate topic for detailed instructions about adding a Web application or mobile application to your catalog:

- “Add a Web Application to Your Catalog from the Cloud Application Catalog,” on page 105
- “Add a Web Application to Your Catalog by Creating a New Application Record,” on page 107
- “Add a Web Application to Your Catalog by Importing a ZIP or JAR File,” on page 108
The following instructions provide an overview of the steps involved in adding these types of resources to your catalog.

**Procedure**

1. Log in to the Horizon Workspace Administrator Web interface.
2. Click the **Catalog** tab.
3. Click **+ Add Application**.
4. Click an option depending on the resource type, and the location of the application. When importing an Android workspace image, you do not have to click an option in this step.

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Resource Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application ...from the cloud application catalog</td>
<td>Web application</td>
<td>Horizon Workspace includes access to several default Web applications, available in the cloud application catalog, that you can add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... create a new one</td>
<td>Web application</td>
<td>By filling out the appropriate form, you can create an application record for the Web applications you want to add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... import a ZIP or JAR file</td>
<td>Web application</td>
<td>You can import a Web application that you previously configured in Horizon Workspace. You might want to use this method to roll a Horizon Workspace deployment from staging to production. In such a situation, you export a Web application from the staging deployment as a ZIP file. You then import the ZIP file into the production deployment.</td>
</tr>
<tr>
<td>Mobile Application ... upload an APK file</td>
<td>Mobile application</td>
<td>You can upload an Android app to make it available to provision to entitled users. These uploaded Android apps are used in the managed mobile workspace on VMware Ready Android devices.</td>
</tr>
<tr>
<td>Android Workspace Image ... from a ZIP file</td>
<td>Android workspace image</td>
<td>You can upload an Android workspace image to make it available to provision to entitled users. These resources are the secure Android container for the managed mobile workspace on VMware Ready Android devices.</td>
</tr>
</tbody>
</table>

5. Follow the prompts to finish adding resources to the catalog.
Search for Users, Groups, or Catalog Resources

Use the search text box in the Administrator Web interface to search for Horizon Workspace users, groups, or resources in your catalog.

Procedure

1. Log in to the Administrator Web interface.
2. Enter a string into the search text box.
   
   For example, to search for all users that have an email address mycompany.com, enter *mycompany.com*.

The Search Results page displays with the returned results listed on three tabs, according to the following rules.

- **Users tab**
  
  The typed-in string matches the starting characters of any word within the Horizon Workspace user’s first name, last name, or user principal name.

- **Groups tab**
  
  The typed-in string matches the starting characters of any word within the group’s name or description.

- **Catalog tab**
  
  The typed-in string matches the starting characters of any word within the catalog resource’s name or description.

**Note**  
Up to 100 results are returned for each record type. For example, if the string appears in the records of more than 100 users, a maximum of 100 results is listed on the *Users* tab. You cannot change this maximum.
IT departments often create system images to replicate the enterprise’s desired software configuration on enterprise-owned systems. When you create system images for systems or devices that will be issued to your Horizon Workspace users, or otherwise set up a user’s system, you usually install the appropriate Horizon Workspace application.

Before a user can use a particular system or device to access and use certain resource types that your Horizon Workspace system provides for them, the Horizon Workspace application that can deliver that resource type must be installed to that system or device. Each type of system or device from which your Horizon Workspace users access their entitled resources has a corresponding appropriate Horizon Workspace application that provides access to the resource from that system or device.

The Horizon Workspace system uses the term desktop to refer to a system that is running either the Windows operating system or the Mac operating system. For a Windows desktop, you install the Horizon Workspace for Windows program when you want the user on that system to use the following resource types provided by your Horizon Workspace system.

- The files and folders syncing and sharing service. You must entitle the user to the Horizon Workspace file-sharing service.
- ThinApp packages. You must entitle the user to those packages that you want that user to use.

For a Mac desktop, install the Horizon Workspace for Mac program when you want the user on that system to access the files and folders syncing and sharing service. You must entitle the user to the Horizon Workspace file-sharing service.

**Note** If you do not want to install a Horizon Workspace application on your users’ enterprise-owned desktop systems, the users can use the browser-based user portal from those systems to access the types of resources that are available through the user portal. From a desktop system, users can point a browser to your Horizon Workspace system’s fully qualified domain name (FQDN) and log in. Once logged in to the browser-based user portal, those users can access and use their entitled Web apps and the Web interface to the Horizon Workspace file-sharing service without having to install another application to their desktop system.

Installing the Horizon Workspace for Windows application requires administrator privileges on the Windows system to which the client is being installed.

**Note** If any browser windows are open during installation of the Horizon Workspace for Windows application, problems might occur with launching ThinApp packages from the user portal. Either close all browser windows before installing the application, or immediately after installing the application, restart your browsers. See “ThinApp Packages Fail to Launch from the User Portal,” on page 148.
This chapter includes the following topics:

- “Command-Line Installer Options for Horizon Workspace for Windows,” on page 62
- “Install the Horizon Workspace for Windows Application with Identical Settings to Multiple Windows Systems,” on page 68
- “Configure the Horizon Workspace for Windows Client to Launch 64-Bit ThinApp Packages on 64-Bit Windows Operating Systems,” on page 69

Command-Line Installer Options for Horizon Workspace for Windows

You can set various options for the Horizon Workspace for Windows client application when you run its installer program using the command line or a deployment script. Because this client application provides features related to the use of the file-sharing and ThinApp package capabilities, you typically use these installer options to set runtime options associated with those features.

Available Command-Line Options for the Horizon Workspace for Windows Installer

After you download the EXE file for the client application’s installer to a Windows system, you can see a list of the installation options by running the following command,

```
VMware-Horizon-Workspace-n.n.n-nnnnnnn /?
```

where `n.n.n-nnnnnnn` represents the file’s version and build number. A dialog box appears that lists the available installation options that you can pass to the installer when installing the client application using the command line or a deployment script.

Table 10-1. Installer Command-Line Options

<table>
<thead>
<tr>
<th>Installer Option</th>
<th>Value</th>
<th>Description</th>
<th>Long Form Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>/c</td>
<td>path to configuration file/filename</td>
<td>Provides a configuration file to use in the installation process.</td>
<td>/cfgfile</td>
</tr>
<tr>
<td>/T</td>
<td>path to temporary directory</td>
<td>Provides a directory to use as a temporary extraction location during the installation process.</td>
<td>/Temp</td>
</tr>
<tr>
<td>/S</td>
<td>path to search for files</td>
<td>Provides a set of paths for the installer to search for files, in addition to the installer package file.</td>
<td>/SearchPaths</td>
</tr>
<tr>
<td>/P</td>
<td>path to package file/filename</td>
<td>Provides a package file to use in the installation process.</td>
<td>/Package</td>
</tr>
<tr>
<td>/s</td>
<td>No values</td>
<td>Runs the installation silently. A silent installation does not display messages or windows during deployment. You typically use this option when using a deployment script to run the installer program in an unattended install process, and you want to suppress the display of interactive messages and windows. You can use this option with the /x or /uninst option to silently uninstall the application.</td>
<td>/silent</td>
</tr>
<tr>
<td>/nsr</td>
<td>No values</td>
<td>Suppresses an automatic reboot after a successful silent installation process.</td>
<td>/noSilentReboot</td>
</tr>
<tr>
<td>/f2</td>
<td>path to log file</td>
<td>Provides the location of the installation log file.</td>
<td>/log</td>
</tr>
<tr>
<td>/d</td>
<td>No values</td>
<td>Write debugging information to the installation log file.</td>
<td>/debug</td>
</tr>
<tr>
<td>/V</td>
<td>No values</td>
<td>Sets verbose logging.</td>
<td>/verbose</td>
</tr>
</tbody>
</table>
Table 10-1. Installer Command-Line Options (Continued)

<table>
<thead>
<tr>
<th>Installer Option</th>
<th>Value</th>
<th>Description</th>
<th>Long Form Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>/L</td>
<td>English language name or localized language name or three-letter language abbreviation or language identifier</td>
<td>Runs the installer in the named language, for example, VMware-Horizon-Workspace-n.n.n-nnnnnn /lang French where n.n.n-nnnnnn is the file version and build number for your downloaded installer program.</td>
<td>/lang</td>
</tr>
<tr>
<td>/v</td>
<td>key-value pairs</td>
<td>Provides a set of arguments to use in the installation process as a key-value pair, provided in the format key=value. These arguments are passed to the MSI file and configure runtime for the file sharing and ThinApp packages capabilities provided by the Windows application.</td>
<td>/msi_args</td>
</tr>
<tr>
<td>/x</td>
<td>No values</td>
<td>Uninstalls the application.</td>
<td>/uninst</td>
</tr>
<tr>
<td>/clean</td>
<td>No values</td>
<td>Cleans out the installation registration information.</td>
<td>No long form alternative</td>
</tr>
</tbody>
</table>

**Key-Value Pairs for the /v Option**

The following table describes the available key-value pairs used for the /v installer option.

Table 10-2. Keys for the /v Installer Command-Line Option

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HORIZONURL</td>
<td>URL</td>
<td>Provides the URL to your Horizon Workspace system, where HTTPS is the required protocol, to allow the Windows application to communicate with your Horizon Workspace system, for example HORIZONURL=<a href="https://HorizonWorkspaceFQDN">https://HorizonWorkspaceFQDN</a>. Note The value must include the full URL, including the protocol portion, such as https://.</td>
</tr>
<tr>
<td>PROMPTFORAUTH</td>
<td>0 or 1</td>
<td>Presents users with a login window if Kerberos authentication fails. Set the value of this variable to 1 to enable the client application to respond to a Kerberos failure by prompting users to log in from a browser window. VMware-Horizon-Workspace-n.n.n-nnnnnn /v PROMPTFORAUTH=1 Setting the value of this variable to 0 is the same as not including the variable in the command. The result is that upon a Kerberos failure the client application does not automatically open the login in a browser window. However, the user receives an indication in the Windows system tray that the client is not authenticated to the server yet and can start the process manually.</td>
</tr>
</tbody>
</table>
Table 10-2. Keys for the /v Installer Command-Line Option (Continued)

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA_SYNC_FOLDER</td>
<td>file path</td>
<td>Provides the named location for the Horizon sync folder that is used by the Windows system on which the client application is being installed. By default, the installer creates a folder at %userprofile%/Horizon, where %userprofile% is the user's folder in the standard Windows Users folder. In the typical interactive install of the client application, where the logged-in user double-clicks the EXE file and completes the installation screens, the installer creates the Horizon sync folder as C:\Users\username\Horizon by default. In a command-line install of the client application, you can use the DATA_SYNC_FOLDER key to set the location of the Horizon sync folder. You can use environment variables to set the location for every user account on that Windows system. To set the path so that it is appropriately created and mapped for each user, escape the environment variables in the key-value pair used in the installation command. VMware-Horizon-Workspace-n.n.n-nnnnnnnn /v DATA_SYNC_FOLDER = #:%username%\Horizon The # can be a mapped network drive or a UNC path. Note The DATA_SYNC_FOLDER option is usually used for Horizon View non-persistent desktops, also known as Horizon View floating desktops or Horizon View stateless desktops.</td>
</tr>
</tbody>
</table>
### Table 10-2. Keys for the /v Installer Command-Line Option (Continued)

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALL_MODE</td>
<td>COPY_TO_LOCAL</td>
<td>Sets the deployment mode for how the client application obtains ThinApp packages at runtime. ThinApp packages are virtualized Windows applications. The ThinApp packages reside on a network share that is integrated with your Horizon Workspace system using the Connector.</td>
</tr>
<tr>
<td></td>
<td>HTTP_DOWNLOAD</td>
<td>With COPY_TO_LOCAL, the user's entitled packages are downloaded to the client Windows system using a file copy. When the user launches a ThinApp package, the virtualized application runs locally on that system. Before the user's first download and use of an entitled ThinApp package and to continue synchronizing the packages to the client Windows system, the client Windows system must join the same Active Directory domain to which the ThinApp packages' network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and copy files from the network share.</td>
</tr>
<tr>
<td></td>
<td>RUN_FROM_SHARE</td>
<td>With HTTP_DOWNLOAD, the user's entitled packages are downloaded to the client Windows system using the HTTP protocol. When the user launches a ThinApp package, the virtualized application runs locally on that system. The Horizon Workspace client uses the user's Horizon Workspace system account to authenticate to your Horizon Workspace Server to obtain the list of the user's entitled packages to download. The share user account provided in the Connector Web interface for enabling account-based access to the ThinApp packages' network share is the account used by the Horizon Workspace Connector to access the ThinApp packages from the repository. That share user account for the Connector needs read permission on the network share. The account that the user used to log in to the client Windows system and the user's Horizon Workspace system account do not need to have any permissions on the network share. The client Windows system does not have to join the same domain to which the ThinApp packages' network share is joined. This download method is typically slower than using the other modes. The benefit to this mode is that the client Windows system does not have to join the Active Directory domain to obtain and run the virtualized application. <strong>IMPORTANT</strong> For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in the Horizon Workspace Connector must be configured for account-based access. See <em>Installing and Configuring Horizon Workspace</em>.</td>
</tr>
<tr>
<td></td>
<td>RUN_FROM_SHARE</td>
<td>With RUN_FROM_SHARE, the virtualized application is streamed to the client Windows system from the network share when the user launches the ThinApp package. The RUN_FROM_SHARE option is best suited for Windows systems that will always have connectivity to the network share where the ThinApp packages reside, because the ThinApp packages are not present on the Windows system and the virtualized applications only run if the Windows system can connect to the network share. The client Windows system must join the same Active Directory domain to which the ThinApp packages...</td>
</tr>
</tbody>
</table>
### Table 10-2. Keys for the /v Installer Command-Line Option (Continued)

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packages' network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and execute files on the network share. For all of the modes, the network share must have the appropriate file and sharing permissions configured. See Installing and Configuring Horizon Workspace. IMPORTANT When installing Horizon Workspace for Windows in floating Horizon View desktops, you best use the RUN_FROM_SHARE option to avoid copying the ThinApp packages into those stateless Horizon View desktop systems. When the client application is installed with one of these configurations, the user account that logs into the Windows system must have the appropriate file and sharing permissions on the network share to be able to obtain the ThinApp packages:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLLINGINTERVAL frequency</td>
<td>Enables you to set the frequency, measured in seconds, of synchronizations between the installed client application and your Horizon Workspace system to check for new ThinApp packages or entitlements. If unspecified, the default value of 300 seconds (5 minutes) applies.</td>
<td></td>
</tr>
<tr>
<td>ENABLE_DATA 0 or 1</td>
<td>Enables you to disable the file-sharing features in the client application that is being installed. Set the value of this variable to 0 to disable the file-sharing features. If unspecified, the default value of 1 applies.</td>
<td></td>
</tr>
<tr>
<td>ENABLE_AUToupdate 0 or 1</td>
<td>Enables you to disable the automatic update check and download activity. If enabled, the installed Horizon Workspace for Windows application automatically checks if a newer application is available for downloading in your Horizon Workspace system. If there is a newer version available, the Horizon Workspace for Windows application automatically downloads and updates itself to the newer version. This option is enabled by default. Set the value of this variable to 0 to disable automatic update. If unspecified, the default value of 1 applies. <strong>NOTE</strong> An updated Horizon Workspace for Windows application is not installed if the logged-in user account does not have administrator privileges.</td>
<td></td>
</tr>
<tr>
<td>ENABLE_THINAPP 0 or 1</td>
<td>Enables you to disable syncing of ThinApp packages by the client application. Set the value of this variable to 0 to disable the syncing of ThinApp packages. If unspecified, the default value of 1 applies.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10-2. Keys for the /v Installer Command-Line Option (Continued)

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHARED_CACHE</td>
<td>0 or 1</td>
<td>Determines whether the ThinApp package cache is located in a common folder in the Windows system to which the client application is being installed. Set the value of this variable to 1 to specify that all user accounts on the Windows system share a common cache location. By default, the common folder is <code>C:\Program Data\VMware\Horizon ThinApp</code>. If unspecified, the default value of 0 applies, and each Windows user account gets its own cache, and its default location is <code>%LOCALAPPDATA%\VMware\Horizon ThinApp\PackageCache</code>. <strong>Note</strong> If you specify a shared cache, the Horizon Workspace for Windows application does not automatically delete ThinApp packages from this shared cache. Because SHARED_CACHE=1 indicates that all user accounts on the Windows system share the same location, the packages must remain in the shared location so that entitled users can use them, even when you unentitle one user. When you unentitle a user from a ThinApp package, the Horizon Workspace for Windows application unregisters that package for that user. Other entitled users on that Windows system can continue to use the ThinApp package. You can delete the common cache manually to reclaim the space if no user accounts on that Windows system are entitled to use the ThinApp packages. Each ThinApp package has its own folder under the cache location.</td>
</tr>
<tr>
<td>AUTO_TRY_HTTP</td>
<td>0 or 1</td>
<td>When the Horizon Workspace for Windows application is installed with the COPY_TO_LOCAL option and account-based access is configured for the Horizon Workspace Connector, the AUTO_TRY_HTTP option determines whether the client should automatically try downloading the user's entitled ThinApp packages using the HTTP protocol, as for the HTTP_DOWNLOAD option, if the first attempt to download fails. This option is enabled by default. Set the value of this option to 0 to disable automatically trying the HTTP protocol for the download. If unspecified, the default value of 1 applies. <strong>Important</strong> For the AUTO_TRY_HTTP option to work, the ThinApp packages integration in the Horizon Workspace Connector must be configured for account-based access. See <em>Installing and Configuring Horizon Workspace</em>.</td>
</tr>
</tbody>
</table>

Example: Example of Using the Horizon Workspace for Windows Command-Line Installer Options

If your Horizon Workspace instance has a URL of `https://HorizonWorkspaceFQDN`, and your Connector is configured for account-based access to your ThinApp packages’ network share, and you want to silently install the Horizon Workspace for Windows application to multiple desktops of that Horizon Workspace instance with these options:

- The ThinApp install option set to HTTP_DOWNLOAD, because you expect these Windows systems will not be likely to join the domain. The Connector is appropriately configured for account-based access to the ThinApp packages’ network share.
- The clients check for new packages and entitlements with the Horizon Workspace system every 60 seconds.

You would create a script that invokes the following command:

```
VMware-Horizon-Workspace-n.n.n-nnnnnnn.exe /s
/v HORIZONURL=https://HorizonWorkspaceFQDN INSTALL_MODE=HTTP_DOWNLOAD POLLINGINTERVAL=60
```

where you replace the `n.n.n-nnnnnnn` portion of the file name to match the name of your downloaded Horizon Workspace for Windows installer.
 Deprecated Command-Line Options

The following options were used in previous Horizon Workspace releases and are no longer used in the current release.

- The `/z SSLBYPASS` option is ignored if provided on the command line.
- The `/z HORIZONSERVER` option is superseded by the `/v HORIZONURL` option.
- The `/v DOWNLOAD` option is superseded by the `/v INSTALL_MODE` option.

Install the Horizon Workspace for Windows Application with Identical Settings to Multiple Windows Systems

To deploy the Horizon Workspace for Windows application to multiple Windows systems and have the same configuration settings applied to all of those systems, you can implement a script that installs the Horizon Workspace for Windows application using the command-line installation options.

**IMPORTANT** Error messages do not appear on screen when you deploy Horizon Workspace for Windows silently. To check for errors during a silent installation, monitor the `%TEMP%` folder, checking for new `vminst.XXXXXX.log` files. The error messages for a failed silent installation appear in these files.

Typically, this deployment scenario is used for Windows systems that are Horizon View desktops. For a description of settings to use for non-persistent, also known as floating or stateless, Horizon View desktops, see “Reducing Resource Usage and Increasing Performance of Horizon Workspace for Windows In Non-Persistent Horizon View Desktops,” on page 99.

Prerequisites

- Verify that the Windows systems are running Windows operating systems that are supported for the version of the Horizon Workspace for Windows application you are installing. See the Horizon Workspace User Guide or the release notes that apply for that Horizon Workspace for Windows application.
- Verify that the Windows systems have installed browsers that are supported by the Windows application you are installing.
- If you want the ability to run a command to familiarize yourself with the available options before you create the deployment script, verify that you have a Windows system on which you can run that command. The command to list the options is only available on a Windows system. See “Command-Line Installer Options for Horizon Workspace for Windows,” on page 62.

Procedure

1. Obtain the Horizon Workspace for Windows installer’s executable file and locate that executable file on the system from which you want to silently run the installer.

One method for obtaining the executable file is to download it using the your Horizon Workspace system’s download page. If you have set up your Horizon Workspace system to provide the Windows application installer from the download page, you can download the executable file by opening the download page’s URL in a browser. The download page’s URL is `https://HorizonWorkspaceFQDN/download`, where `HorizonWorkspaceFQDN` is the fully qualified domain name for your Horizon Workspace system.
Using the installer's command-line options, create a deployment script that fits the needs of your organization.

Examples of scripts you can use are Active Directory group policy scripts, login scripts, VB scripts, batch files, SCCM, and so on.

For example, if your Horizon Workspace instance has a URL of https://HorizonWorkspaceFQDN, and you want to silently install the Windows client to Windows systems that you expect will be used off the domain, with the ThinApp deployment mode set to download mode and have the Horizon Workspace for Windows application sync with the server every 60 seconds, you would create a script that invokes the following command:

```
VMware-Horizon-Workspace-n.n.n-nnnnnnn.exe /s
/v HORIZONURL=https://HorizonWorkspaceFQDN INSTALL_MODE=HTTP_DOWNLOAD POLLINGINTERVAL=60
```

where you replace the n.n.n-nnnnnnn portion of the file name to match that of your downloaded file.

3 Run the deployment script against the Windows systems.

If the silent installation is successful, the Horizon Workspace for Windows application is deployed to the Windows systems. Users logged in to those Windows systems can access their entitled assets from those systems.

**NOTE** A user's entitled ThinApp package is streamed or downloaded and cached to the user's Windows system after the polling interval elapses. As a result, users might see the ThinApp package displayed when they log in to the Horizon Workspace browser-based user portal. The ThinApp package does not start until the client syncs the application on the next polling interval.

**What to do next**

Verify that Horizon Workspace for Windows is properly installed on the Windows systems by trying some of the typical user tasks. See the Horizon Workspace User Guide.

### Configure the Horizon Workspace for Windows Client to Launch 64-Bit ThinApp Packages on 64-Bit Windows Operating Systems

When you plan on having your Horizon Workspace users run 64-bit ThinApp packages on 64-bit Windows operating systems, you must first perform some configuration steps on the Horizon Workspace for Windows client application that is installed on the 64-bit Windows systems.

To enable the Horizon Workspace for Windows client on 64-bit Windows operating systems to launch 64-bit ThinApp packages, you must download the 64-bit HorizonPlugin.dll file from the connector-va virtual machine's filesystem and manually install that DLL file on the 64-bit Windows systems. If you do not follow these steps and you sync 64-bit ThinApp packages with your Horizon Workspace system, when users on those Windows systems try to launch their entitled 64-bit ThinApp packages, an error message "Unable to load notification module HorizonPlugin.dll" is displayed.

Launching 64-bit ThinApp packages is supported on 64-bit Windows operating systems only. The Horizon Workspace for Windows client does not support launching 64-bit ThinApp packages on 32-bit Windows operating systems.

**Prerequisites**

- Verify that you can use ssh and the sshuser account to log in to the service-va. You must be able to download a file from the connector-va's filesystem using ssh.
For the steps on how to connect to the service-va using ssh, see the VMware knowledge base article at http://kb.vmware.com/kb/2061672.

To set a password for the sshuser account on the connector-va, log in to the connector-va as the root user using the vSphere client console and the connector-va's command-line interface console. Run the command `passwd sshuser` to set the password.

**Procedure**

1. On the 64-bit Windows system on which the Horizon Workspace for Windows client is installed, move the existing HorizonPlugin.dll file from its existing location in `C:\Windows` to `C:\Windows\SysWOW64`.

2. Download the 64-bit HorizonPlugin.dll file from the connector-va virtual machine's filesystem to a local system from which you can copy it to the 64-bit Windows system.
   a. Launch an SSH client session and connect to the connector-va.
   b. Log in as the sshuser.
   c. Copy the file `/opt/vmware/thinapp-plugin-x64/HorizonPlugin.dll` to a local system so that it is available for copying to the 64-bit Windows system.

3. Copy the 64-bit HorizonPlugin.dll file into the `C:\windows\System32` directory on the 64-bit Windows system.

4. Restart the Horizon Workspace for Windows client with the updated configuration.

On the client 64-bit Windows system, the original HorizonPlugin.dll file is installed in `C:\Windows\SysWOW64` directory and the 64-bit HorizonPlugin.dll file that is from the connector-va's filesystem is installed in `C:\windows\System32` directory. The Horizon Workspace for Windows client installed on that 64-bit Windows system can launch 64-bit ThinApp packages that are provided to that system by your Horizon Workspace system.
You can entitle Horizon Workspace users to the file-sharing service. The file sharing service allows Horizon Workspace users to share files and folders with other Horizon Workspace users and with guest users.

Guest users are users external to Horizon Workspace whom Horizon Workspace users specifically invite to access selected folders.

The file-sharing service allows Horizon Workspace users to synchronize access to their files across multiple devices ensuring that they get up-to-date and always-on access to their files of choice.

If you enable the Horizon Files module, you can then use the Administrator Web interface to configure the file-sharing service in your catalog and to entitle the service as a resource to users and groups.

A class of service (COS) is a defined set of file storage and sharing attributes, such as account quota, maximum file size allowed, file types disallowed, and so on. When you entitle the file-sharing service to a user or group, you also assign a COS to that entitlement, and the defined settings are applied to those users. Horizon Workspace includes a default COS. To customize the attributes for different users and groups in your organization, you can edit the default COS and create new ones. You can assign different classes of service to specific users or groups.

If you delete a COS that is assigned to users or groups, the users are automatically reassigned to the default COS. You cannot delete the default COS.

This chapter includes the following topics:
- “Enable the Horizon Files Module,” on page 71
- “Entitling Users and Groups to the File-Sharing Service,” on page 72
- “Class of Service,” on page 74

**Enable the Horizon Files Module**

To provide the capability in your Horizon Workspace deployment to entitle Horizon Workspace users to share files and folders, you must enable the Horizon Files module. As a result, the file-sharing service is available in your catalog as an available resource.

**Prerequisites**

Install Horizon Workspace. As part of the installation, implement the Horizon Files module preconfiguration steps, such as adding storage and configuring a document preview application. See *Installing and Configuring Horizon Workspace.*
Procedure

1. Log in to the Configurator Web interface.
   
   See “Horizon Workspace Web Interface URLs,” on page 11 for the URL for the Configurator Web interface.

2. Click the Module Configuration tab.

3. Click Enable this module in the Horizon Files module.

The Horizon Files module is now enabled, and the file-sharing service is available in your catalog as a resource that can be entitled to users or groups.

What to do next

- If needed, edit the default class of service (COS), create a COS, or both. See “Class of Service,” on page 74
- Entitle users or groups to the file-sharing service.
- Verify the distribution of the appropriate Horizon Workspace applications to users’ desktops and mobile devices.

For Mac and Windows systems, users can use a browser to access their files and folders. For a native experience, users can use the Horizon Workspace native applications on iOS, Android, Windows, and Mac OS X operating systems. For example, using Horizon Workspace for Windows, the user can modify files and add folders using Windows Explorer. VMware Horizon Files for iOS is the native application for iOS devices.

**NOTE** On Windows and Mac systems, the best practice for users is to install the respective application, VMware Horizon Workspace for Windows or VMware Horizon Workspace for Mac. These applications automatically sync the changes a user makes to the folder named Horizon that has been shared to all the shared instances. Users can download and install these applications manually. See Horizon Workspace User Guide.

To install on multiple Windows systems at once, the Horizon Workspace administrator can silently install Horizon Workspace for Windows. See “Install the Horizon Workspace for Windows Application with Identical Settings to Multiple Windows Systems,” on page 68.

**Entitling Users and Groups to the File-Sharing Service**

To give users or groups the capability to share files and folders, you must entitle them to the file-sharing service. Entitling a user or group includes assigning a class of service (COS) to that user or group.

After you configure one or more classes of service in a manner that best suits your enterprise, you can entitle users and groups to the file-sharing service as an entitled resource, and assign the appropriate class of service. See “Class of Service,” on page 74. You assign a class of service to a user by adding either a new user entitlement or a new group entitlement to the group to which the user belongs.

**Entitle Users to the File-Sharing Service**

You can entitle individual users to the Horizon Workspace file-sharing service, which includes assigning a class of service (COS).

In many cases, the most effective way to entitle users to the file-sharing service is to add a group entitlement for the file-sharing service to a group, and add the users to that group. In certain situations, entitling individual users to the file-sharing service is more appropriate.
Prerequisites

- Enable the Horizon Files module. Enabling this module makes the file-sharing service available as a resource in your catalog.
- Configure one or more classes of service as appropriate for the file storage and sharing needs of your enterprise.
- Review “Criteria for Class of Service Precedence,” on page 74.

Procedure

1. Log in to the Administrator Web interface.
2. Select Users & Groups > Users.
3. Click the name of the user to whom you want to entitle the file-sharing service.
4. Click Add Entitlement.
5. Click the check box for the resource that corresponds to the file-sharing service.
6. From the COS drop-down menu, select the COS that you want to assign to the user.
7. Click Save.

The selected user is now governed by the file storage and sharing policy of the newly assigned class of service.

Entitle Groups to the File-Sharing Service

You can entitle a group’s users to the file-sharing service by entitling the group to that resource, which includes assigning a class of service (COS).

In many cases, the most effective way to entitle users to the file-sharing service is to add a group entitlement for the file-sharing service to a group, and add the users to that group.

Prerequisites

- Enable the Horizon Files module. Enabling this module makes the file-sharing service available as a resource in your catalog.
- Configure one or more classes of service as appropriate for the file storage and sharing needs of your enterprise.
- Review “Criteria for Class of Service Precedence,” on page 74.

Procedure

1. Log in to the Administrator Web interface.
2. Select Users & Groups > Groups.
3. Click the name of the group to which you want to entitle the file-sharing service.
4. Click Add Entitlement.
5. Click the check box for the resource that corresponds to the file-sharing service.
6. From the COS drop-down menu, select the COS that you want to assign to the group.
7. Click Save.
The result of which file storage and sharing settings are applied to the group’s users might vary from one user to another, according to the resolution of precedence for the classes of service to which they are currently assigned. Their COS assignment might or might not change. See “Criteria for Class of Service Precedence,” on page 74.

Class of Service

When you entitle users or groups to the file-sharing service, you assign a class of service (COS) to them. You can create multiple classes of service to provide different users with different file storage and sharing policies. A user’s assigned COS defines the file storage and sharing policy for that user.

Horizon Workspace includes a default COS with preconfigured settings. After you enable the Horizon Files module, you can edit the default class of service to fit your organization’s needs. You can also create one or more additional classes of service.

CAUTION As a best practice, when you edit a COS or change a COS assignment, wait 15 minutes before you entitle users to the file-sharing service. Fifteen minutes is the duration user entries are cached in data servers.

Criteria for Class of Service Precedence

A Horizon Workspace user can be entitled to the file-sharing service multiple times, which can result in the assignment of several different classes of service to that user. The file storage and sharing policy for each user is determined by the COS that takes precedence for that user.

You can entitle users to the file-sharing service by adding user entitlements or group entitlements. Through this process, and because a user can belong to multiple groups, a user might be entitled to the file-sharing service multiple times with a different class of service assigned through each entitlement. A given user has only one assigned COS at a time. The assigned COS determines the file storage and sharing policy of that user. In the Administrator Web interface, you can see the name of the user’s assigned COS by displaying the user’s details page. To display the user’s details page, click User & Groups > Users, and click the user’s name.

User Entitlement Takes Precedence

A COS assigned to a user through a user entitlement takes precedence over a COS assigned to the user through a group entitlement. A user can only have one user entitlement to the file-sharing service, but can be a member of an unlimited number of groups that each have a group entitlement to the file-sharing service. In such a situation, these several different entitlements might assign several different classes of service to the same user. Horizon Workspace enforces the file storage and sharing policy as determined by the COS assigned to the user as a user entitlement.

Top-Level Group Entitlement Takes Precedence

If a user does not have a COS assigned through a user entitlement, but has multiple classes of service assigned through group entitlements, Horizon Workspace applies a COS to that user according to the order of groups as listed in the Group Entitlements section of the resource page for the file-sharing service. To access the service’s resource page, in the Administrator Web interface, click the Catalog tab, click Any Application Type > Services, and click Horizon Files. The Group Entitlements section lists all the groups entitled to the file-sharing service. Some of the groups might have a named COS while some might have the default COS. The group highest on the list that has a named COS and to which the user is a member takes precedence.

Changing the COS that Takes Precedence

You can change the COS assignment for users by taking the steps to entitle the user to the file-sharing service again.
If a user has a user entitlement to the file-sharing service, you can change the COS for the user by following the steps to entitle the user to the file-sharing service, and selecting the COS you want as the assigned COS for that new entitlement.

If a user is entitled to the file-sharing service through a group entitlement, you can change the COS for the group by following the steps to add another group entitlement to the file-sharing service, and selecting the COS you want as the assigned COS for that new group entitlement. This action might change the COS assignment of the other members of the group.

**Edit an Existing Class of Service**

You can edit an existing class of service (COS) whether it is assigned to users or not. If the COS is assigned to users, this action changes the policy that governs their file storage and sharing behavior.

Horizon Workspace includes a default COS. You can use the default COS as is, or edit the settings to customize the COS for your organization's needs. You can also create different classes of service and apply them to different users and groups, depending on your organization's needs.

The Administrator Web interface is the main tool for configuring the Horizon Workspace file-sharing service, but some file-sharing functionality can only be configured using the CLI utility. See Horizon Workspace Files Command Line Interface.

**CAUTION** If you assign a COS to users, and then configure an existing setting in the COS to a lower value, users lose the higher value previously assigned to them. The reconfiguration might cause users to receive warning messages about approaching or exceeding the limit. For example, if you lower the Account Quota setting, users whose accounts are over the new limit might receive warning messages, even when they did not change the files in their account.

**Prerequisites**

Enable the Horizon Files module.

**Procedure**

1. Log in to the Horizon Workspace Administrator Web interface.
2. Click the Catalog tab.
3. Click Any Application Type > Services.
4. Click Horizon Files.
5. Click Class of Service.
6. Click Edit for the COS you want to edit.
7. Edit the settings in the form as appropriate.

**NOTE** The default content for the COS Name, Description, and Quota Warning Msg text boxes is editable. You can edit these text boxes, including changing the text to a different language, while creating or editing the class of service form.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS Name</td>
<td>The name for the class of service. After you create a COS, you cannot edit the COS name.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A description for the class of service.</td>
</tr>
<tr>
<td>Account Quota (MB)</td>
<td>The amount of disk space in megabytes that users are allowed on the server. When a user's account reaches the assigned limit, new files cannot be added and an error message appears on the user's screen. A value of 0 provides users with an unlimited amount of disk space for files and folders.</td>
</tr>
<tr>
<td>Form Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Quota Warning Msg</td>
<td>The email message sent to users when the amount of disk space they are allowed on the server reaches the threshold percentage. To edit the message, use the default formatting and replace text only.</td>
</tr>
<tr>
<td>Threshold (%)</td>
<td>The threshold that triggers the quota warning email message. The threshold refers specifically to the amount of disk space used as a percentage of the account quota. When the disk space used reaches the threshold, users receive a warning email message.</td>
</tr>
<tr>
<td>Required Period Before Trigger Causes Warning</td>
<td>The minimum amount of time that must lapse once the threshold percentage is crossed for a trigger event, an activity that increases the users use of disk space, to cause Horizon Workspace to issue the quota warning message. For example, the interval is set to three days and after a user receives the first warning, the user uploads another file after two days, Horizon Workspace does not issue a warning message.</td>
</tr>
<tr>
<td>Max File size (MB)</td>
<td>The maximum size of a file that users can upload to Horizon Workspace.</td>
</tr>
<tr>
<td>File Types Disallowed</td>
<td>Extensions for file types you want to block. Users cannot upload files with these extensions to Horizon Workspace.</td>
</tr>
<tr>
<td>Trashed File Lifetime Value</td>
<td>The period of time a file can still be retrieved (undeleted) in the file's History after it has been deleted, before it is automatically purged.</td>
</tr>
<tr>
<td>Internal Expiration</td>
<td>The amount of time shared files and folders can be accessed by your enterprise's Horizon Workspace users. A value of 0 indicates that shares never expire.</td>
</tr>
<tr>
<td>External Folder Sharing Allowed</td>
<td>When this box is checked, Horizon Workspace users can invite external users to access folders. These external users are also referred to as guest users.</td>
</tr>
<tr>
<td>Public Files Sharing Allowed</td>
<td>When this box is checked, Horizon Workspace users can make files available on the Internet.</td>
</tr>
<tr>
<td>External Expiration</td>
<td>The amount of time shared folders can be accessed by guest users. A value of 0 indicates that shares never expire.</td>
</tr>
<tr>
<td>Public Expiration</td>
<td>The amount of time files are accessible on the Internet. A value of 0 indicates that shares never expire.</td>
</tr>
</tbody>
</table>
| Domains Allowed or Not Allowed | This option enables you to restrict or allow guest-user access to shared folders based on the guest user's domain. When you check a radio button for this option, you select one of the following external folder sharing controls:  
  - **No Domain Policy**: to allow all external domains potential access to folders shared by Horizon Workspace users.  
  - **Allowed**: to specify domains from which guest users can access shared folders. When this choice is selected, type the allowed domain names in the **Allowed domains for external sharing** text box.  
  - **Restricted**: to specify domains from which guest users are prevented from accessing shared folders. When this choice is selected, type the restricted domain names in the **Restricted domains for external sharing** text box. |
| Host Pool | This option is applicable when your Horizon Workspace deployment contains two or more data-va servers. When you add a new data-va server to your deployment, it appears in the Host Pool list. You can select the data-va server to which newly provisioned users are assigned. The user's data is then stored in the assigned server. When neither no server is selected or all servers are selected, the file-sharing service assigns new users evenly among all servers in the list. When you select more than one server, the file-sharing service assigns new users evenly among the selected servers.  
Horizon Workspace uses the Host Pool setting to assign users to specific servers. After users are assigned to a server, you cannot change the assigned server, unless you manually move users’ data. Editing the COS to change the selected servers in the Host Pool list will not change the assigned server.  
The server to which a user's data is stored is provided as the value to the Data Node Hostname attribute. You can use the Administrator Web interface to find the Data Node Hostname attribute and value on the user’s details page. Click **Users & Groups > Users**, and click the user’s name. |
Form Item | Description
---|---
Pin/Passcode Required | When this box is checked, mobile-device users must use a passcode to access the file-sharing application on their mobile device. Users are prompted to create a passcode the first time they provision their mobile workspace on the mobile device.
Open/Edit with | This box is checked by default. When this box is checked, users can use third-party applications on their mobile devices to edit files that are managed by the file-sharing service.

8 Click **Save**.

**What to do next**
After you configure one or more classes of service for the file storage and sharing needs of your enterprise, you can apply the classes of service to specific users and groups. See "Entitling Users and Groups to the File-Sharing Service," on page 72.

**Create a Class of Service**
You can create a class of service (COS) that you assign to a user or group when you entitle the file-sharing service to that user or group.

Horizon Workspace includes a default COS. You can use the default COS as is, edit the settings to customize the COS for your organization’s needs, or copy it and save it as a COS with a new name. You also can create different classes of service and apply them to different users and groups, depending on your organization’s needs.

The Administrator Web interface is the main tool for configuring the file-sharing service, but some of the functionality of the file-sharing service can only be configured using the CLI utility. See *Horizon Workspace Files Command Line Interface*.

**CAUTION** If you assign a COS to users, and then configure an existing setting in the COS to a lower value, users lose the higher value previously assigned to them. The reconfiguration might cause users to receive warning messages about approaching or exceeding the limit. For example, if you lower the Account Quota setting, users whose accounts are over the new limit might receive warning messages, even when they did not change the files in their account.

**Prerequisites**
Enable the Horizon Files module.

**Procedure**
1 Log in to the Administrator Web interface.
2 Click the **Catalog** tab.
3 Click **Any Application Type > Services**.
4 Click **Horizon Files**.
5 Click **Class of Service**.
6 Create a COS using one of two methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new COS</td>
<td>Click <strong>Add a new COS</strong>.</td>
</tr>
<tr>
<td>Copy an existing COS as a starting point, and customize the settings.</td>
<td>Click <strong>Copy</strong> in the row of the existing COS.</td>
</tr>
</tbody>
</table>
Complete the form for the COS.

**Note** The default content for the COS Name, Description, and Quota Warning Msg text boxes is editable. You can edit these text boxes, including changing the text to a different language, while creating or editing the class of service form.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS Name</td>
<td>The name for the class of service. After you create a COS, you cannot edit the COS name.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A description for the class of service.</td>
</tr>
<tr>
<td>Account Quota (MB)</td>
<td>The amount of disk space in megabytes that users are allowed on the server. When a user’s account reaches the assigned limit, new files cannot be added and an error message appears on the user’s screen. A value of 0 provides users with an unlimited amount of disk space for files and folders.</td>
</tr>
<tr>
<td>Quota Warning Msg</td>
<td>The email message sent to users when the amount of disk space they are allowed on the server reaches the threshold percentage. To edit the message, use the default formatting and replace text only.</td>
</tr>
<tr>
<td>Threshold (%)</td>
<td>The threshold that triggers the quota warning email message. The threshold refers specifically to the amount of disk space used as a percentage of the account quota. When the disk space used reaches the threshold, users receive a warning email message.</td>
</tr>
<tr>
<td>Required Period</td>
<td>The minimum amount of time that must lapse once the threshold percentage is crossed for a trigger event, an activity that increases the users use of disk space, to cause Horizon Workspace to issue the quota warning message. For example, the interval is set to three days and after a user receives the first warning, the user uploads another file after two days, Horizon Workspace does not issue a warning message.</td>
</tr>
<tr>
<td>Before Trigger</td>
<td></td>
</tr>
<tr>
<td>Causes Warning</td>
<td></td>
</tr>
<tr>
<td>Max File size (MB)</td>
<td>The maximum size of a file that users can upload to Horizon Workspace.</td>
</tr>
<tr>
<td>File Types Disallowed</td>
<td>Extensions for file types you want to block. Users cannot upload files with these extensions to Horizon Workspace.</td>
</tr>
<tr>
<td>Trashed File</td>
<td>The period of time a file can still be retrieved (undeleted) in the file’s History after it has been deleted, before it is automatically purged.</td>
</tr>
<tr>
<td>Lifetime Value</td>
<td></td>
</tr>
<tr>
<td>Internal Expiration</td>
<td>The amount of time shared files and folders can be accessed by your enterprise’s Horizon Workspace users. A value of 0 indicates that shares never expire.</td>
</tr>
<tr>
<td>External Folder</td>
<td>When this box is checked, Horizon Workspace users can invite external users to access folders. These external users are also referred to as guest users.</td>
</tr>
<tr>
<td>Sharing Allowed</td>
<td></td>
</tr>
<tr>
<td>Public Files</td>
<td>When this box is checked, Horizon Workspace users can make files available on the Internet.</td>
</tr>
<tr>
<td>Sharing Allowed</td>
<td></td>
</tr>
<tr>
<td>External Expiration</td>
<td>The amount of time shared folders can be accessed by guest users. A value of 0 indicates that shares never expire.</td>
</tr>
<tr>
<td>Public Expiration</td>
<td>The amount of time files are accessible on the Internet. A value of 0 indicates that shares never expire.</td>
</tr>
<tr>
<td>Domains Allowed</td>
<td>This option enables you to restrict or allow guest-user access to shared folders based on the guest user's domain.</td>
</tr>
<tr>
<td>or Not Allowed</td>
<td>When you check a radio button for this option, you select one of the following external folder sharing controls:</td>
</tr>
<tr>
<td></td>
<td>■ No Domain Policy to allow all external domains potential access to folders shared by Horizon Workspace users.</td>
</tr>
<tr>
<td></td>
<td>■ Allowed to specify domains from which guest users can access shared folders. When this choice is selected, type the allowed domain names in the Allowed domains for external sharing text box.</td>
</tr>
<tr>
<td></td>
<td>■ Restricted to specify domains from which guest users are prevented from accessing shared folders. When this choice is selected, type the restricted domain names in the Restricted domains for external sharing text box.</td>
</tr>
</tbody>
</table>
Table

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Pool</td>
<td>This option is applicable when your Horizon Workspace deployment contains two or more data-va servers. When you add a new data-va server to your deployment, it appears in the Host Pool list. You can select the data-va server to which newly provisioned users are assigned. The user's data is then stored in the assigned server. When either no server is selected or all servers are selected, the file-sharing service assigns new users evenly among all servers in the list. When you select more than one server, the file-sharing service assigns new users evenly among the selected servers. Horizon Workspace uses the Host Pool setting to assign users to specific servers. After users are assigned to a server, you cannot change the assigned server, unless you manually move users' data. Editing the COS to change the selected servers in the Host Pool list will not change the assigned server. The server to which a user's data is stored is provided as the value to the Data Node Hostname attribute. You can use the Administrator Web interface to find the Data Node Hostname attribute and value on the user's details page. Click Users &amp; Groups &gt; Users, and click the user's name.</td>
</tr>
<tr>
<td>Pin/Passcode Required</td>
<td>When this box is checked, mobile-device users must use a passcode to access the file-sharing application on their mobile device. Users are prompted to create a passcode the first time they provision their mobile workspace on the mobile device.</td>
</tr>
<tr>
<td>Open/Edit with</td>
<td>This box is checked by default. When this box is checked, users can use third-party applications on their mobile devices to edit files that are managed by the file-sharing service.</td>
</tr>
</tbody>
</table>

8 Click Save.

What to do next

After you configure one or more classes of service for the file storage and sharing needs of your enterprise, you can apply the classes of service to specific users and groups. See “Entitling Users and Groups to the File-Sharing Service,” on page 72.

View the Class of Service Associated with a User or Group

You can view a class of service (COS) that is associated with a particular user or group.

After you entitle users or groups to the file-sharing service, you can use the Horizon Workspace Administrator Web interface to view which COS is associated with those users and groups.

Prerequisites

- Enable the Horizon Files module. See “Enable the Horizon Files Module,” on page 71.
- Configure one or more classes of service. See “Edit an Existing Class of Service,” on page 75 or “Create a Class of Service,” on page 77.

Procedure

1 Log in to the Administrator Web interface.
2 View the classes of service that are associated with users and groups.

Two methods are available for listing COS names. To open a COS specifically for viewing use the user and group method.

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
</table>
| List all entitlements to the file-sharing service. | a Click the Catalog tab.  
b Click Any Application Type > Services.  
c Click Horizon Files.  
The Entitlements tab is selected by default. The group entitlements and user entitlements are listed in separate tables. The COS associated with each user or group is listed. |
| Search for a specific user or group, and display the Entitlements page for that user or group. | a Click the Users & Groups tab.  
b Click the Users tab or the Groups tab.  
c Click the name of an individual user or group.  
The Entitlements tab for that user or group is displayed. If the user or group has an associated COS, the name of the COS appears at the top of the page. You can click the COS name to see the settings that are defined for that COS. |

Delete a Class of Service

You can delete a class of service.

Prerequisites

Consider the ramifications of deleting a COS. When you delete a COS, if users are associated with it, the deleted COS is replaced with the default COS. When settings in the deleted COS, such as Account Quota or Max File Size, are replaced with lower values, users lose the higher value previously assigned to them. The reconfiguration might cause users to receive warning messages about approaching or exceeding the limit.

Procedure

1 Log in to the Administrator Web interface.
2 Click the Catalog tab.
3 Click Any Application Type > Services .
4 Click Horizon Files.
5 Click Class of Service.
6 Click Delete for the COS you want to remove.

The COS is deleted. When you delete a COS that is associated with users or groups, those users and groups do not lose the ability to share files and folders. In such a case, the default COS is applied to those users and groups.
Your Horizon Workspace users can use their mobile devices to access and use their entitled resources. The Horizon Workspace capabilities that are delivered to and available on a user’s mobile device are determined by the type of mobile device, the client app that is available for and installed on the device, and the user’s entitlements.

<table>
<thead>
<tr>
<th>Mobile Device Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| iOS device         | Users use the Horizon Workspace browser-based user portal, loaded into a browser app, to use their entitled Web applications, and they use the Horizon Files for iOS app to use their entitled file-sharing features.  
**Note** To have your users use the Horizon Workspace file-sharing features on their iOS devices, you must entitle those users to the Horizon Workspace file-sharing service, and tell the users to install the Horizon Files for iOS app on the devices. Users install the Horizon Files for iOS app from the Apple App Store. |
| Android device     | Users use the Horizon Workspace browser-based user portal, loaded into a browser app, to use their entitled Web applications, and they use the Files for Android app to use their entitled file-sharing features.  
**Note** To have your users use the Horizon Workspace file-sharing features on their Android devices, you must entitle those users to the Horizon Workspace file-sharing service, and tell the users to install the Files for Android app onto their devices. Users install the Files for Android app from Google Play. |
| VMware Ready Android device | A user enrolls a VMware Ready Android device with your Horizon Workspace system by installing the VMware Horizon Workspace Switch app on the device, starting the app, and following the on-screen instructions. After the device is enrolled, your Horizon Workspace system provisions a secure workspace consisting of a secure workspace container, mobile apps, and policy enforcement information to the device. After the provisioning activity completes, the user can use the secure workspace on the VMware Ready device, and your Horizon Workspace system can control the access and behavior of the secure workspace container and its mobile apps. In the secure workspace, the user loads the browser-based user portal into the browser app to use the user’s entitled Web applications, and uses the Files for Android app to use the entitled file-sharing features.  
**Note** To have your users use the Horizon Workspace file-sharing features in the secure workspace, you must:  
1. Entitle those users to the Horizon Workspace file-sharing service.  
2. Entitle those users to the Horizon Files for Android app that is located in your catalog. The app is provisioned to the secure workspace container on the enrolled device so the user can use the Files for Android app from within the secure workspace. |

This chapter includes the following topics:

- “Enable the Mobile Management Module,” on page 82
- “Overview of the Device Enrollment Process for VMware Ready Android Devices,” on page 82
- “Configure Your Horizon Workspace to Enroll VMware Ready Android Devices,” on page 83
- “Using Mobile Policies and Mobile Policy Sets,” on page 87
Enable the Mobile Management Module

Enable this module to enable the capabilities of your Horizon Workspace system for providing managed mobile workspaces on VMware Ready Android devices.

Prerequisites

Install Horizon Workspace. See Installing and Configuring Horizon Workspace.

Procedure

1. Log in to the Configurator Web interface.
   
   See “Horizon Workspace Web Interface URLs,” on page 11 for the URL for the Configurator Web interface.

2. Click the Module Configuration tab.

3. Click Enable this module in the Mobile Management module.

The Mobile Management module is now enabled.

What to do next

Configure the settings, according to your organization's needs, that correspond to enrolling and using VMware Ready Android devices with your Horizon Workspace system.

Overview of the Device Enrollment Process for VMware Ready Android Devices

Before your Horizon Workspace system can provision a secure mobile workspace, consisting of the secure workspace container and its contained mobile apps, to a VMware Ready Android device, and manage that workspace, the user must enroll the device with your Horizon Workspace system.

After a VMware Ready Android device is enrolled, your Horizon Workspace system provisions a secure workspace consisting of the secure workspace container, mobile apps, and policy enforcement information to the device. After the provisioning activity completes, the user can use the secure workspace on the VMware Ready Android device, and your Horizon Workspace system can control the access and behavior of the secure workspace container and its mobile apps. This combination of the secure workspace container, its mobile apps, and related data is the user’s managed workspace.

To enroll a VMware Ready Android device, a user must install the VMware Horizon Workspace Switch app from Google Play on the VMware Ready Android device. When using an Android device to browse the list of available apps at Google Play, the list displays the Switch app if the device is a VMware Ready Android device. To enroll the device after installing the Switch app, the user launches the app, and enters the hostname for your Horizon Workspace system (the HostnameFQDN), username, and password. Then the Switch app downloads and installs both the secure Android container that contains the managed workspace on the device and any imported Android applications in your catalog that you have entitled to that user.

After the secure Android container is installed on the device, the user touches the Switch icon to access the managed workspace. On the initial access, the user accepts your end user terms, if you have specified an end user license agreement using the Mobile > Workspace EULA setting, and creates a passcode. This passcode is used to securely access the managed workspace.
After the passcode is created, the device switches to the managed workspace and displays the Home screen for the managed workspace. The user can touch the icon for the applications list to see the mobile apps that you have entitled to that user for use in the managed workspace.

To switch back to the personal side of the device, the user touches the Switch icon that is visible in the managed workspace. To switch from the personal side to the managed workspace, the user touches the Switch icon on the personal side of the device.

**IMPORTANT** The VMware Ready Android device must be set to automatically sync data. The auto-sync data setting must be enabled for Switch and the managed mobile workspace to work properly. Because devices from different manufacturers might have different ways to enable the auto-sync data setting, users must consult their device manufacturer’s documentation to locate the auto-sync data setting on their devices.

---

**Configure Your Horizon Workspace to Enroll VMware Ready Android Devices**

When a VMware Ready device is enrolled with your Horizon Workspace system, Horizon Workspace can provision a secure workspace to that device, and manage and control the behavior of that secure workspace. The provisioned workspace is also called the user’s managed mobile workspace.

Setting up the elements that are necessary to use your Horizon Workspace system to provision secure workspaces to VMware Ready Android devices involves several steps.

**Prerequisites**

Verify that the appropriate resources for provisioning workspaces to VMware Ready Android devices have been added to your catalog. To provide managed mobile workspaces for users’ VMware Ready Android devices, you must have at least one Android workspace image in your catalog. To provide mobile apps in the provisioned workspace, you import Android applications into your catalog as resources.

Horizon Workspace includes a standard Android workspace image by default. Horizon Workspace also includes some Android applications in your catalog by default.

If you want require the users to accept an end user license agreement during device enrollment, perform the steps in “Configure an End User License Agreement for VMware Ready Android Device Enrollment,” on page 84.

Some of the default policy settings apply to enrolled VMware Ready Android devices. If you want to use policy settings for the users other than the ones in the standard policy sets, verify the users are members of a named group. Mobile policy settings are applied to users by associating mobile policy sets with the group that the users belong to. If necessary, create a new Horizon Workspace group and add the users to it. See “Manage Horizon Workspace Groups,” on page 38.

**Procedure**

1. **Configure an End User License Agreement for VMware Ready Android Device Enrollment** on page 84
   
   You can configure text for an end user license agreement (EULA) to which your organization wants users’ confirmation and agreement as they are enrolling their VMware Ready Android devices with your Horizon Workspace system.

2. **Import an Android Workspace Image into Your Catalog** on page 84
   
   An Android workspace image is a version of the Android operating system that is installed as the secure Android container for a managed mobile workspace on VMware Ready devices. By importing an Android workspace image, you make it available for entitling to users and groups to provide for their managed mobile workspaces on such devices.
3 **Upload a Mobile Android Application into Your Catalog** on page 85

To make an Android app available for inclusion in mobile workspaces provisioned to enrolled VMware Ready Android devices, you must first upload the app into your catalog as a resource.

4 **Entitle Users and Groups to Required Resources for VMware Ready Devices** on page 86

Before a user can enroll a VMware Ready device with your Horizon Workspace system, you must entitle that user to the appropriate resources. At a minimum, you must entitle the user to an Android workspace image.

After a workspace is provisioned to an enrolled VMware Ready Android device, you can perform actions on the provisioned workspace, such as disabling it, resetting the password, and wiping it. See “Perform Actions on Desktop Systems and Mobile Devices that Users Have Linked with Your Horizon Workspace System,” on page 47.

**What to do next**

Certain policies are applied to provisioned workspaces on VMware Ready Android devices by default. If you want to apply policies to the provisioned workspaces that are different than the default policies, see “Apply Mobile Policy Sets to a Group,” on page 92.

**Configure an End User License Agreement for VMware Ready Android Device Enrollment**

You can configure text for an end user license agreement (EULA) to which your organization wants users' confirmation and agreement as they are enrolling their VMware Ready Android devices with your Horizon Workspace system.

**Prerequisites**

Verify that you have the text of your enterprise's terms and conditions to which you want your users to agree for enrolling their devices with your system and using the devices with their entitled resources. The text can be 50,000 characters or less. If you provide this text, when a user enrolls a VMware Ready Android device with your Horizon Workspace system, this text is displayed and the user must accept the terms and conditions before completing the enrollment process.

**Procedure**

1. Select Mobile > Workspace EULA.
2. In the Workspace EULA area, type the text of your enterprise's terms and conditions into the field.
   - You can also copy and paste the text into the field.
3. Click Save.

**Import an Android Workspace Image into Your Catalog**

An Android workspace image is a version of the Android operating system that is installed as the secure Android container for a managed mobile workspace on VMware Ready devices. By importing an Android workspace image, you make it available for entitling to users and groups to provide for their managed mobile workspaces on such devices.

**Prerequisites**

Verify that you have the file for the Android workspace image you want to import. Android workspace images are provided in a ZIP file format from VMware. Only Android workspace images provided by VMware are supported. Horizon Workspace includes at least one standard Android workspace image that is installed when you enable the Mobile Management module for your Horizon Workspace system.
Procedure
1  Log into the Administrator Web interface as an administrator.
2  Click the Catalog tab.
3  Click + Add Application > Android Workspace Image ...from a zip file.
   A window opens in which you choose ZIP file to upload.
4  Browse to locate and select the Android workspace image's ZIP file.
5  (Optional) Specify a description.
6  Click Upload.
   The upload might take some time.

The Android workspace image is imported into your catalog, and you can entitle it to groups and users.

Upload a Mobile Android Application into Your Catalog

To make an Android app available for inclusion in mobile workspaces provisioned to enrolled VMware Ready Android devices, you must first upload the app into your catalog as a resource.

Android apps that you directly upload into your catalog are used in the workspaces deployed to enrolled VMware Ready Android devices only. When these uploaded Android apps are deployed to the secure workspace container that is provisioned on an enrolled VMware Ready Android device, they are managed by your Horizon Workspace system as part of the secure workspace on that device.

IMPORTANT Horizon Workspace uploads some Android applications into your catalog by default when you enable the Mobile Management module for your Horizon Workspace system. Make sure that you have the most up-to-date versions of these applications so that any bug fixes included in the recent versions are deployed to the users' mobile workspaces on VMware Ready Android devices. The version number of the application is provided on its resources page. See “View Horizon Workspace Resources,” on page 55.

To update an uploaded Android application, upload the APK of the higher version into your catalog.

Prerequisites
Verify that you have the APK file.

NOTE Android applications that use the following features do not work in the mobile workspace provisioned to VMware Ready Android devices:

- The Google Maps API.
- Android Cloud to Device Messaging (C2DM).

Android applications that specify the external SD card as their installation destination are not supported for installation into the mobile workspace. Such APKs have android:installLocation="preferExternal" set in their AndroidManifest.xml file.

Procedure
1  Log in to the Administrator Web interface as an administrator.
2  Click the Catalog tab.
3  Click + Add Application > Mobile Application ... upload an apk file.
   A window opens in which you choose the mobile application's file.
4  Browse to locate and select the file to upload.
5 (Optional) Specify a description for the mobile application. The description appears on the mobile application's resource page in your catalog.

6 Click Upload.

The mobile application is available in your catalog as a resource that you can entitle to users and groups.

**Entitle Users and Groups to Required Resources for VMware Ready Devices**

Before a user can enroll a VMware Ready device with your Horizon Workspace system, you must entitle that user to the appropriate resources. At a minimum, you must entitle the user to an Android workspace image.

In many cases, the most effective way to entitle users to managed mobile applications, and the Android workspace images for VMware Ready devices, is to add the entitlements to a group of users. However, in certain situations entitling individual users to the mobile applications and Android workspace images is more appropriate.

The Administrator Web interface has two available methods for entitling users and groups to a resource: from the user’s or group’s details page or from the resource’s page. Usually entitling imported Android applications using the details page for the user or group is more efficient because the available imported Android applications are visibly grouped together and you can pick out the ones you can entitle for use in the secure Android workspace image.

**Prerequisites**

Use the Dashboard page to verify the Mobile Management module is enabled for your Horizon Workspace system.

**Procedure**

1 Log in to the Administrator Web interface.
2 Use one of the available methods to entitle a user or group.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access the details page for the user or group, and entitle the Android workspace image and mobile applications from that page.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Click the Users &amp; Groups tab.</td>
</tr>
<tr>
<td>2</td>
<td>Click the appropriate tab: Users or Groups.</td>
</tr>
<tr>
<td>3</td>
<td>Click the name of an individual user or group.</td>
</tr>
<tr>
<td>On the user’s or group’s page, the Entitlements tab is selected by default.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>On the Entitlements page, in the section for managed mobile workspaces, click Edit to specify the workspace image and the Android apps for the workspace. The deployment type is automatic by default, and you cannot change this setting. When you entitle a workspace image, the VMware Horizon Email app is entitled by default, and you cannot change this setting.</td>
</tr>
<tr>
<td>5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Access the resource pages for the workspace image and imported Android applications, and entitle users or groups to those resources. |
| 1 | Click the Catalog tab. |
| 2 | Click Any Application Type > Android Workspace Images |
| 3 | Click the workspace image. |
| On the Android workspace image’s resource page, the Entitlements tab is selected by default. Group entitlements are listed in one area of the page, while user entitlements are listed in another. |
| 4 | Click Add group entitlement or Add user entitlement as appropriate. |
| 5 | Enter the names of the groups or users as appropriate. |
| You can search for users or groups by starting to type a search string and allowing the autocomplete feature to list the options, or you can click browse to view the entire list. |
| 6 | Click Save. |
| 7 | Click Done on the Entitlements page. |
| 8 | Click the Catalog tab. |
| 9 | Click Any Application Type > Mobile Applications |
| 10 | In the Mobile Applications section, click the icon for the imported Android application to which you want to entitle users and groups. |
| Note: Only those Android applications that you have imported directly into your catalog, or which are imported by default when the Mobile Management module is enabled, can be used in the managed workspace on VMware Ready devices. |
| On the application’s resource page, the Entitlements tab is selected by default. Group entitlements are listed in one area of the page, while user entitlements are listed in another. |
| 11 | Click Add group entitlement or Add user entitlement as appropriate. |
| 12 | Enter the names of the groups or users as appropriate. |
| You can search for users or groups by starting to type a search string and allowing the autocomplete feature to list the options, or you can click browse to view the entire list. |
| 13 | Click Save. |
| 14 | Click Done on the Entitlements page. |
| Repeat the steps for entitling an application for each Android application you want to entitle to users or groups. |

Using Mobile Policies and Mobile Policy Sets

Use policies to control the required behavior of the managed mobile workspace on provisioned VMware Ready Android devices.

Policies determine capability-related settings for users’ managed mobile workspaces on VMware Ready Android devices. A policy set is a collection of those policies that control behaviors related to a particular category of features. For example, a passcode policy set contains policies that set passcode-related requirements such as passcode strength.
The policies that you can set in Horizon Workspace are grouped into three categories:

- Data containment policies
- Workspace lifetime policies
- Passcode policies

Each group’s Applied Policy Sets page displays the name of the policy sets, by category, that are associated with the group’s users. The actual policy settings in each of the listed policy sets that are pushed to a user’s managed mobile workspace depends on the outcome of the policy resolution if the user belongs to multiple groups.

Horizon Workspace includes standard policy sets, and associates policy settings in these standard policy sets to every group by default. For each policy category, these settings are defined in a standard policy set named Base. See “Standard Mobile Policy Sets Included In Horizon Workspace,” on page 88. You can customize the settings in the standard policy sets by editing them, or you can create your own policy sets and apply them to groups to override the standard settings.

A group is the smallest object to which you can apply a policy set. You cannot apply a policy set to a user. To apply a policy set to multiple users, create a Horizon Workspace group, add the users to that group, and then apply the policy set to that group.

**Policy Resolution**

Because a user can belong to multiple groups, and each group can have different policy settings, the system uses a policy resolution algorithm to determine the specific policy settings to apply to that user’s mobile workspace. The system performs policy resolution for each policy category. To preview the result of the policy resolution for groups and users for a policy category, on the Policies page, click **Preview Policy Resolution for Groups and Users** for that category. On the Policies page, you can raise or lower the priority of a policy set with respect to the other policy sets in that category by using the links in the category’s Reorder Priority column.

**Standard Mobile Policy Sets Included In Horizon Workspace**

Horizon Workspace includes several standard policy sets by default. You can customize these policy sets to meet your organization’s needs.

For each policy category, Horizon Workspace includes a standard policy set named Base. For the passcode category, Horizon Workspace also includes two standard policy sets named Very Strong and Strong.

By default, Horizon Workspace applies the policy settings defined in each category’s Base policy set to every group, and therefore to every user. If a user enrolls a mobile device and you have not created or applied any custom policy sets to the user’s group, the policy settings in the Base policy sets that are relevant for that user’s type of mobile device are used.

If the policy settings in these standard policy sets do not meet your organization’s needs, or if you want to customize their names, you can edit them on the Policies page. For example, if you want to localize the Strong name to a more appropriate name in your language, locate it in the Passcode Policy Sets table on the Policies page, click **Edit**, and enter the new name.

**NOTE** You cannot change the name of the standard policy sets named Base.
**Data Containment Policies**

Data containment policies control the access and flow of data for the managed mobile workspaces provisioned on VMware Ready Android devices.

### Table 12-1. Policies that control behaviors related to data containment on enrolled devices

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of camera</td>
<td>Determines whether users can use the on-device camera on the device. When set to No, the normal camera functionality is rendered ineffective on the device. The camera application and icon remain in the managed workspace and the shutter icon is visible when the user launches the camera. However, when the user launches the camera in the managed workspace, a static default image is displayed instead of the normal camera view, and if the user touches the shutter icon, an image file of that static default image is saved.</td>
</tr>
<tr>
<td>Allow copy &amp; paste</td>
<td>Determines whether users can copy and paste between their personal applications and the managed applications in the secure workspace on the device.</td>
</tr>
<tr>
<td>Location services</td>
<td>Determines whether location services are required. If required, users cannot access the managed mobile workspace unless they turn on location services on the personal side of the device.</td>
</tr>
</tbody>
</table>
| Location accuracy          | Controls the accuracy to which applications in the managed workspace can track the device's location.  
1 Using Low accuracy sets the policy to require the device's location services are set to use at least one of the following location accuracy settings on the device: Wi-Fi network or mobile network.  
2 Using High accuracy sets the policy to require the device's location services are set to use the GPS network for accuracy. A policy violation does not occur if the device is set to use a higher location accuracy than the policy setting requires. If the device's is set to use a higher location accuracy such as GPS network, and you set this policy to Low accuracy, a policy violation does not occur because the device is within the location accuracy set by the policy setting. |

**Workspace Lifetime Policies**

Workspace lifetime policies control what happens to the managed mobile workspace on an enrolled VMware Ready Android device when the mobile device has not appropriately communicated with the Horizon Workspace server.

These policies control the interval at which the lease on the enrolled mobile device is renewed with the Horizon Workspace server, and when an automatic disable or automatic wipe is performed after lease renewal failures. These policies protect the administrator's ability to control the managed resources on the enrolled mobile device by automatically restricting access if the client on the device has not communicated with the server.
### Table 12-2. Policies that control behaviors related to workspace lifetime on enrolled mobile devices

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease interval</td>
<td>The amount of time between lease renewals attempts. The lease interval sets how frequently the client on the device attempts to renew its lease with the server. See “Horizon Workspace Server Leasing Process and Enrolled VMware Ready Android Devices,” on page 95. A value of less than 15 minutes can cause noticeable battery consumption.</td>
</tr>
<tr>
<td>Auto disable</td>
<td>The amount of time after which the managed mobile workspace on the device will be automatically disabled if the device has not contacted the management server. A value of at least three to four days is recommended, unless your company has a requirement for stricter settings. If this time period is exceeded, access to the managed mobile workspace is disabled. The underlying client services on the device continue the standard attempts to contact the server. Access is automatically restored the next time that contact is successful and the lease is renewed.</td>
</tr>
<tr>
<td>Auto wipe</td>
<td>The amount of time after which the managed mobile workspace will be automatically wiped if the underlying client services have not contacted the management server. A value of at least seven days is recommended, unless your company has a requirement for stricter settings. If this time period is exceeded, the automatic wipe deletes the managed mobile workspace from the device.</td>
</tr>
</tbody>
</table>

**Note**: The timer for performing the automatic disable and wipe starts at the first lease renewal failure. For example, if the automatic disable time is 3 days and the lease interval is 1 day, the automatic disable happens after 4 days (1 + 3).

### Passcode Policies

Passcode policies determine passcode-related requirements, such as whether the user must set a passcode to access the managed mobile workspace on the enrolled VMware Ready Android device, passcode strength, frequency of expiration, and the circumstances for which the user’s access is automatically locked if the correct passcode is not entered.

The default passcode policy set, named Base, is applied by default to all groups. This Base policy set enforces having a passcode on enrolled devices. According to your organization’s needs, you can edit the Base policy set to remove enforcement of the passcode.

The passcode protection policy set also applies to the VMware Horizon Mail for Android app when the app is provisioned in the managed mobile workspace to entitled users. Therefore, you should set the passcode protection policy to the same strength and expiration settings as your email server’s policy settings.

### Table 12-3. Policies that control behaviors related to passcodes on the enrolled devices

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcode</td>
<td>Determines whether the user is required to set a passcode. This passcode applies to the managed mobile workspace, consisting of the secure workspace container and the managed apps and data that are contained within the secure workspace container. When this policy setting is set to Yes, the user must enter the passcode to access the managed mobile workspace. When this policy setting is set to Yes, you can set the other passcode-related settings for the policy set.</td>
</tr>
<tr>
<td>Min length</td>
<td>Sets the minimum length of the passcode.</td>
</tr>
<tr>
<td>Min digits</td>
<td>Sets the minimum number of digits the passcode must have.</td>
</tr>
<tr>
<td>Min letters</td>
<td>Sets the minimum number of letters the passcode must have.</td>
</tr>
<tr>
<td>Min uppercase letters</td>
<td>Sets the minimum number of uppercase letters the passcode must have.</td>
</tr>
<tr>
<td>Min lowercase letters</td>
<td>Sets the minimum number of lowercase letters the passcode must have.</td>
</tr>
</tbody>
</table>
### Table 12-3. Policies that control behaviors related to passcodes on the enrolled devices (Continued)

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min special characters</td>
<td>Sets the minimum number of non-alphanumeric characters the passcode must have.</td>
</tr>
<tr>
<td>Passcode timeout</td>
<td>Sets the amount of time for which a user can re-access the managed mobile workspace without having to re-enter the passcode.</td>
</tr>
<tr>
<td>Attempts before lockout</td>
<td>Sets the number of times that a user can enter an incorrect passcode before being locked out of the managed mobile workspace for five minutes. After the five minutes has elapsed, the user can again enter an incorrect passcode up to the number of times specified by the <strong>Attempts before lockout</strong> setting before being locked out for a second five minute period. If the user enters a third set of incorrect attempts, up to the number set by the <strong>Attempts before lockout</strong> setting, the managed mobile workspace is wiped from the device. For example, when <strong>Attempts before lockout</strong> is set to 8, and the user enters an incorrect passcode 8 times, the workspace automatically locks for five minutes. After five minutes, if the user again enters an incorrect passcode another 8 times, the workspace automatically locks for five minutes. After five minutes, if the user yet again enters an incorrect passcode another 8 times (for a total of 24 incorrect passcode entries), the workspace is automatically wiped from the device. The lockout period for each set of attempts is five minutes. The number of sets of allowed attempts before the automatic wipe is three. You cannot change those defaults.</td>
</tr>
<tr>
<td>Passcode expiration</td>
<td>Sets the amount of time after which the passcode expires and must be changed.</td>
</tr>
</tbody>
</table>

### Create Mobile Policy Sets

Create a new policy set for a policy category when there is no existing policy set that meets your organization’s needs.

By default, the settings in each policy category’s standard policy set, named Base, are applied to all groups, which applies the settings to every Horizon Workspace user. The actual policy settings in each of the listed policy sets that are pushed to a user’s mobile device depends on the outcome of the policy resolution algorithm.

If the policy settings in the standard policy set do not meet your organization’s needs, you can create a policy set for that category, and associate your policy set with the All Users group. If you have a named group of users, such as Finance or Sales, and you want to apply specific policy settings to those users, create a policy set for that category, and associate your policy set with that group.

**Procedure**

1. Log in to the Administrator Web interface.
2. Click **Policies > Mobile Policy Sets**.
3. For each category for which you want to specify policies, click the corresponding button.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Containment Policy Set</td>
<td>Policies that control the access and flow of data on enrolled devices. See “Data Containment Policies,” on page 89.</td>
</tr>
<tr>
<td>Workspace Lifetime Policy Set</td>
<td>Policies that determine how the managed resources on an enrolled device are protected when it has not communicated with your Horizon Workspace system over a period of time. See “Workspace Lifetime Policies,” on page 89.</td>
</tr>
<tr>
<td>Passcode Policy Set</td>
<td>Policies that determine passcode-related requirements, such as passcode strength, frequency of expiration, and the circumstances for which the managed resources on the enrolled device are automatically locked or wiped if the correct passcode is not entered. See “Passcode Policies,” on page 90.</td>
</tr>
</tbody>
</table>

4. In the **Policy Set Name** text box, type a name for the new policy set.
5   (Optional) In the **Description** text box, type a meaningful description.

6   Select the check box for the policy that you want to set, and then select the desired policy setting.

   For example, to prevent use of the camera in the managed mobile workspace, select **No** for the **Allow camera** setting in a data containment type of policy set.

7   Click **Save** to create the policy set.

**What to do next**

You can now apply this policy set to one or more groups. See “Apply Mobile Policy Sets to a Group,” on page 92.

**Apply Mobile Policy Sets to a Group**

You can apply policy sets to a group. Depending on the type of mobile device and which policy settings are applicable for that device type, the policy settings are applied to the users’ enrolled devices for the users that belong to that group. When a user belongs to multiple groups, a policy resolution algorithm determines the combination of policy settings that are applied to that user.

**Prerequisites**

Verify that the group of users to which you want to apply policy settings is available in the system. If not, create the group using the steps in Chapter 7, “Managing Users and Groups,” on page 37.

Create the policy sets that you want to associate with the group. See “Create Mobile Policy Sets,” on page 91.

**Procedure**

1   Select **Users & Groups > Groups**.

2   Click the group name to which you want to apply policy sets.

3   Click **Applied Mobile Policy Sets**.

   The mobile policy sets currently applied to the group are listed according to the policy category.

4   Click **Select Mobile Policy Sets**.

5   For each policy category, select the mobile policy set that you want to apply to this group’s users.

   By default, Horizon Workspace includes a default policy set for each policy category. Each of these default sets is applied to every group by default unless you apply a different policy set from that category to the group.

   **Note** The names of the **Strong** and **Very Strong** policy sets are defined by the Horizon Workspace administrator. You can customize these names, including using a name in a different language, using the Edit feature on the Mobile Policy Sets page. See “Standard Mobile Policy Sets Included In Horizon Workspace,” on page 88.

6   Click **Save**.
Provide Pre-Defined VPN Configurations to Enrolled VMware Ready Android Devices

Create a VPN configuration to provide pre-set VPN settings to enrolled VMware Ready Android devices. Using a configuration is a way to provide convenience to your users because they do not have to manually configure the VPN settings on their mobile devices before they can connect the enrolled devices to your enterprise’s VPN system.

When configured and the configuration is entitled to users, Horizon Workspace system installs the VPN information to entitled users’ managed mobile workspaces on the VMware Ready devices. When installed, those managed mobile workspaces use the pre-set values to access your organization’s VPN system, and the managed mobile workspaces use VPN for network access to your corporate network.

NOTE The users to which you entitle a VPN configuration must install the VPN client application that is appropriate for your VPN system provider on the personal side of their VMware Ready Android devices before they enroll their VMware Ready Android devices with your system. If the user attempts to provision the workspace before configuring the VPN client, a policy violation occurs and the user cannot open the workspace. You must provide the users with the name of the appropriate VPN client so they can install that VPN client app from Google Play on the personal side of their devices.

Prerequisites

Verify that you have the relevant VPN information, such as the VPN connection name, VPN server, type of VPN connection, and so on.

Procedure

1. Log in to the Administrator Web interface.
2. Select Mobile > VPN Settings
3. In the Configuration Name field, type a name for this configuration.
   This name is used to identify this configuration and distinguish it from other configurations, for example, when you want one group of users to use one set of values and another group to use a different set.
4. In the Connection Name field, type a name for this VPN connection. This name is used to identify this VPN connection on the enrolled mobile device.
5. In the Server field, type the address of the VPN server to use for this configuration.
   Use either a symbolic name format, such as vpn.mycompany.com, or a dotted IP address, such as 127.0.0.1.
6. Select the VPN system provider that you are using.
   NOTE When you use the Juniper VPN provider, the workspace cannot activate a VPN connection unless the user first launches the Juniper Junos Pulse VPN client on the personal phone side and accept that VPN client's End User License Agreement (EULA).
7. (Optional) If you want to use a proxy server for the VPN connection, click Enable, type a proxy server name, and select a port number.
   The proxy server name can be a symbolic name format, such as myproxy.mycompany.com, or a dotted IP address, such as 127.0.0.1.
8. Click Save.

The VPN configuration is available for entitling to users and groups.
What to do next

Entitle the VPN configuration profile to users and groups by clicking Entitlements.

Entitling Users and Groups to Resources Used On Mobile Devices

To use resources and services provided by Horizon Workspace on their mobile devices, users must be entitled to the appropriate set of resources in your catalog. When they connect to Horizon Workspace for the first time, Horizon Workspace sends the relevant information about their entitlements to the device.

For iOS devices and Android devices that are not VMware Ready Android devices provisioned with a managed mobile workspace, the mobile device can access the following resource types if the user is entitled to them.

- Web applications. The user can launch their entitled Web applications after logging in to the user portal using a browser app on the device.
- The Horizon Workspace file-sharing service, using the native Files for Android or Files for iOS app on the device. Users can install the native apps from the Apple App Store or Google Play.
- Citrix-based applications. The Citrix Receiver mobile app must be installed on the mobile device to use the entitled Citrix-based applications.
- Horizon View desktops. If the native Horizon View client app is installed on the mobile device, the user can open the Horizon View desktop from the user portal into the Horizon View client app. Alternatively, the user can set a preference in the user portal to open Horizon View desktops in a Web browser.

When a VMware Ready Android device is enrolled with your Horizon Workspace system and the secure workspace is provisioned to the device, the secure workspace can access the following resource types if the user is entitled to them.

- Web applications. The user can launch their entitled Web applications after logging in to the user portal using the browser app in the secure workspace.
- Android applications that you uploaded into your catalog. On enrolled VMware Ready Android devices, your Horizon Workspace system manages the behavior of these mobile applications after the secure workspace is provisioned to the enrolled device. You must also entitle users to the secure workspace container, known as the Android workspace.
- The Horizon Workspace file-sharing service and the Files for Android app. Entitle users to the Files for Android app that is located in your catalog and to the file-sharing service. This app is imported into your catalog by default when you enable the Mobile Management module.
- Citrix-based applications. The Citrix Receiver mobile app must be available in the managed mobile workspace for the user to use the entitled Citrix-based applications. To make the Citrix Receiver mobile app available for the managed mobile workspaces on VMware Ready Android devices, you need to obtain the Citrix Receiver for Android app from the Citrix Web site, upload the app to your catalog, and then entitle the app to the appropriate users.
- Horizon View desktops. If the native Horizon View client app is available in the managed mobile workspace, the user can open the Horizon View desktop from the user portal into the Horizon View client app. Alternatively, the user can set a preference in the user portal to open Horizon View desktops in a Web browser. The Horizon View client app is loaded into your catalog by default. To make the native Horizon View client app available in the users’ managed mobile workspaces, entitle users to the Horizon View Android app in your catalog.

In many cases, the most effective way to entitle users to the resources for use with their mobile workspaces is to add the entitlements to a group of users. However, in certain situations entitling individual users to the resources is more appropriate. See the following topics for the applicable steps for each resource type.

- “Entitle Users and Groups to Web Applications,” on page 109
Horizon Workspace Server Leasing Process and Enrolled VMware Ready Android Devices

On VMware Ready Android devices that are enrolled with your Horizon Workspace system, the system uses a leasing process to remotely manage the lifecycles of the managed mobile workspaces on those devices. Using this leasing process, the Horizon Workspace client app that is installed and running on the device, the Switch app, communicates with your Horizon Workspace system to receive updates of policies and entitlements, and to respond to administrative commands that you issue using the Administrator Web interface, such as wiping a managed mobile workspace from the device.

Switch polls the Horizon Workspace server to obtain a lease from the server. The lease brings information to the about policies, entitlements, and any administrative commands that have been issued to the device's managed mobile workspace. Each time Switch renews its lease with the Horizon Workspace server, it receives any updated policies, updated entitlements, or administrative commands that were issued since the previous lease renewal. A successful lease renewal grants Switch permission to continue operating until the automatic disable period expires. Each successful lease renewal resets the countdown.

**Note** Network latency can affect the length of time between when the server sends the lease and Switch receives it.

### Lease Renewal Attempts

Switch attempts to renew its lease in the following situations.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device's display times out.</td>
<td>When the user reawakens the display, if Switch is running, it polls the server to renew the lease.</td>
</tr>
<tr>
<td>The user presses the power button, turning off the display.</td>
<td>When the user reawakens the display, if Switch is running, it polls the server to renew the lease.</td>
</tr>
<tr>
<td>The managed passcode times out.</td>
<td>The user must enter the passcode that is used to access the managed workspace assets, and the client polls the server to renew the lease. The passcode timeout is set by the <a href="#">Passcode timeout policy setting</a>. See “Passcode Policies,” on page 90.</td>
</tr>
<tr>
<td>The user manually forces the client to poll the server by syncing the account associated with the client app on the device.</td>
<td>Typically, the user can view the account in the accounts list on the device, and touch <strong>Sync now</strong> to sync the client app with the Horizon Workspace server.</td>
</tr>
<tr>
<td>The time elapsed since the last successful lease renewal exceeds the lease interval.</td>
<td>The lease interval is set in the <strong>Lease interval</strong> policy setting, and it determines how frequently Switch attempts to renew the lease. When the amount of time that has elapsed since the last lease renewal exceeds the lease interval, Switch polls the server. See “Workspace Lifetime Policies,” on page 89.</td>
</tr>
</tbody>
</table>

### Failing to Renew a Lease

The lease renewal process can fail, such as when there is no network connectivity between Switch and the server or Switch cannot reach the server for some reason. The **Auto disable** and **Auto wipe** policy settings determine what happens if the lease fails to be renewed within the time intervals set in those policy settings. See “Workspace Lifetime Policies,” on page 89. When the user launches the client app, the time periods for **Auto disable** and **Auto wipe** are checked.
### Time Period  Result

**Auto disable**  If there is no successful lease renewal before this time period elapses, Switch is automatically disabled. The disabled Switch continues its attempts to contact the server, according to the frequency set by the lease interval. Access is automatically restored the next time the client successfully renews the lease.

**Auto wipe**  If there is no successful lease renewal before this time period elapses, the managed mobile workspace is automatically wiped. Switch remains installed on the device. To reprovision a managed mobile workspace on the device, the user must launch Switch and repeat the setup process.

**NOTE**  If either Switch or the device has been powered off, and has failed to renew its lease past the time interval set by the **Auto wipe** policy setting, the next time Switch starts up or is launched, it makes a final attempt to renew the lease. If that attempt fails to renew the lease, the managed mobile workspace is automatically wiped from the device.
Providing Access to Horizon View Desktop Pools

By integrating your organization's VMware® Horizon View™ Connection Server instance with your Horizon Workspace system, you give your Horizon Workspace users the ability to use the Horizon Workspace client to access their entitled VMware Horizon View desktop pools. Additionally, when the View module is enabled, you can use the Horizon Workspace Administrator Web interface to see the associations between Horizon Workspace users and groups and their entitled Horizon View desktop pools.

**Note:** You use the View Connection Server instance and its associated View Administrator management Web interface to entitle users and groups to Horizon View desktop pools. See the VMware View documentation.

Typically, you integrate Horizon View with your Horizon Workspace system as part of the process of installing and configuring your Horizon Workspace system. To complete the integration of Horizon View with your Horizon Workspace system, you enable the View module. Enabling the View module provides the following capabilities:

- You can use the Horizon Workspace Administrator Web interface to monitor user and group entitlements to Horizon View desktop pools.
- Your Horizon Workspace users can use the Horizon Workspace User Portal to access their entitled Horizon View desktop pools.

  To ensure the best user experience on iPads, users should install the Horizon View Client for iOS on their devices.

If the View module was not enabled during the installation and configuration of your Horizon Workspace system, you can enable the module after integrating your organization's VMware® Horizon View™ Connection Server instance with your Horizon Workspace system. See “Enable the View Module to Integrate Horizon View with Horizon Workspace,” on page 98.

This chapter includes the following topics:

- “Enable the View Module to Integrate Horizon View with Horizon Workspace,” on page 98
- “View User and Group Entitlements to Horizon View Desktop Pools,” on page 98
- “View the Connection Information for a Horizon View Desktop Pool,” on page 99
- “Reducing Resource Usage and Increasing Performance of Horizon Workspace for Windows In Non-Persistent Horizon View Desktops,” on page 99
Enable the View Module to Integrate Horizon View with Horizon Workspace

If you did not enable the View module in the Configurator Web interface when you installed and configured Horizon Workspace, you can enable it later starting from the Modules tab on the Dashboard page of the Administrator Web interface.

See Installing and Configuring Horizon Workspace for detailed instructions about the configurations required on VMware View and on Horizon Workspace, such as in the Connector Web interface.

Prerequisites

Procedure

1. Log in to the Administrator Web interface.
2. Select Dashboard > Modules, if not already selected.
3. In the View module, click Enable this module.
4. Perform the configurations required to complete the Integration of VMware View with Horizon Workspace.

The View module is enabled.

If a message displays telling you to go to the Connector, then the integration is not fully in place. Ensure that your Horizon Workspace system is integrated with your Horizon View system according to the steps in Installing and Configuring Horizon Workspace before enabling the View module.

What to do next

Monitor user and group entitlements to Horizon View desktop pools. See “View User and Group Entitlements to Horizon View Desktop Pools,” on page 98.

View User and Group Entitlements to Horizon View Desktop Pools

You can see the Horizon View desktop pools to which your Horizon Workspace users and groups are entitled.

**IMPORTANT** You cannot use Horizon Workspace to make changes to Horizon View desktop pools. If a Horizon View administrator makes any changes to Horizon View desktop pools, such as entitling and unentitling users or changing the supported client types, you must force a sync to propagate the changes to your Horizon Workspace system. Use the Horizon Workspace Connector Web interface to force a sync.

Prerequisites

- Verify that your Horizon Workspace system is integrated with your Horizon View system according to the steps in Installing and Configuring Horizon Workspace.
- Synchronize information and the respective entitlements from the Horizon View Connection Server instances with your Horizon Workspace system. You can force a sync using the following steps:

  1. Open the Connector Web interface in your browser. The Connector Web interface URL is https://ConnectorHostname/hc/admin/, where ConnectorHostname is the hostname for your Horizon Workspace Connector.
  2. Log in to the Connector Web interface using the administrative password for your Horizon Workspace system.
  3. Click View pools and click Sync Now.
Procedure
1. Log in to the Administrator Web interface.
2. View user and group entitlements to Horizon View desktop pools.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| View the list of users and groups entitled to a specific Horizon View desktop pool. | a. Click the Catalog tab.  
b. Click Any Application Type > View Desktop Pools.  
c. Click the icon for the Horizon View desktop pool for which you want to list entitlements.  
The Entitlements tab is selected by default. Group entitlements and user entitlements are listed in separate tables. |
| View the list of Horizon View desktop pool entitlements for a specific user or group. | a. Click the Users & Groups tab.  
b. Click the Users tab or the Groups tab.  
c. Click the name of an individual user or group.  
The Entitlements tab is selected by default. Entitled Horizon View desktop pools, if any, are listed in the View Pools table on the Entitlements page. |

View the Connection Information for a Horizon View Desktop Pool
You can view the information about the connection between Horizon Workspace and a Horizon View desktop pool.

Procedure
1. Log in to the Administrator Web interface.
2. Click the Catalog tab.
3. Click Any Application Type > View Desktop Pool.
4. Click the name of a Horizon View desktop pool.
5. Click the Details tab.
6. View the connection information, which consists of attributes retrieved from the Horizon View Connection Server instance.

See the VMware Horizon View documentation for details about these attributes.

Reducing Resource Usage and Increasing Performance of Horizon Workspace for Windows In Non-Persistent Horizon View Desktops
To reduce resource usage and increase performance when using the Horizon Workspace for Windows client in non-persistent desktops, also known as stateless desktops, you can configure the client with settings optimized for using it in a non-persistent Horizon View desktop.

Problem
When a non-persistent Horizon View desktop has the Horizon Workspace for Windows application installed in the Horizon View desktop, each time a user starts a session, an increased amount of resources are used, such as storage I/Os.
Cause

Non-persistent Horizon View desktops are inherently stateless. Such Horizon View desktops are also known as floating desktops, and new sessions can be created when the floating desktops are recomposed or the user is given a new desktop from the pool. Unless the Horizon Workspace for Windows application used in the non-persistent desktops is configured with settings that are optimized for this scenario, the users might experience degraded performance when using the file-sharing features or ThinApp packages.


Solution

- Install the Horizon Workspace for Windows application in the template that is used for the non-persistent Horizon View desktops using the recommended command-line installer options.

<table>
<thead>
<tr>
<th>/v Installer Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_AUTOUPDATE = 0</td>
<td>Prevents the automatic update of the Horizon Workspace for Windows application to a newer version. Typically, your Horizon View administrator updates the application in the template.</td>
</tr>
<tr>
<td>DATA_SYNC_FOLDER = #:%username%\Horizon, where # is a mapped network drive or UNC path</td>
<td>If you plan to have the users use the file-sharing service in these Horizon View desktops, redirect the files to a network share that can be accessed from these desktops. To set the path so that it is appropriately created and mapped for each user, escape the environment variables using the ^ escape characters when you use this installer option.</td>
</tr>
<tr>
<td>ENABLE_DATA = 0</td>
<td>If you do not plan to have the users use the file-sharing service in these Horizon View desktops, use this option to disable the file-sharing service.</td>
</tr>
<tr>
<td>INSTALL_MODE = RUN_FROM_SHARE</td>
<td>If you plan to have the users use ThinApp packages in these Horizon View desktops, use this option to have the ThinApp packages streamed from the server instead of downloaded to the Windows system.</td>
</tr>
</tbody>
</table>

**Note**  Users must be entitled to the file-sharing service in the Horizon Workspace server to have the capability to sync files using Horizon Workspace for Windows, and must be entitled to ThinApp packages to use them.

This code sample is an example of installing the Horizon Workspace for Windows application with an optimal configuration for non-persistent Horizon View desktops where the users are expected to use both the file-sharing service and ThinApp packages. The HORIZONURL option specifies the Horizon Workspace server for this installation.

```
VMware-Horizon-Workspace-n.n.n-nnnnnnn.exe /v HORIZONURL=https://server.company.com
ENABLE_AUTOUPDATE=0 DATA_SYNC_FOLDER=#:\%username\%\Horizon INSTALL_MODE=RUN_FROM_SHARE
```
Providing Access to Web Applications

You can entitle Horizon Workspace users to your organization’s external Web applications.

To enable users to access a Web application through Horizon Workspace, verify that the following requirements are met:

- If you configure the Web application to use a federation protocol, use SAML 1.1, SAML 2.0, or WS-Federation 1.2. However, you have the option of configuring the Web application to not use a federation protocol at all.
- The users you plan to entitle to the Web application are registered users of that application.
- If the Web application is a multitenant application, Horizon Workspace points to your instance of the application.

This chapter includes the following topics:

- “Enable the Web Applications Module to Provide Web Application Access,” on page 101
- “Establish Secure Single Sign-On to Your Web Applications Through Horizon Workspace,” on page 102
- “Adding Web Applications to Your Organization’s Catalog,” on page 105
- “Entitle Users and Groups to Web Applications,” on page 109

Enable the Web Applications Module to Provide Web Application Access

To allow Horizon Workspace users to access Web applications using the appropriate Horizon Workspace clients, you must enable the Web Applications module.

Prerequisites

Install Horizon Workspace. See the Installing and Configuring Horizon Workspace.

Procedure

1. Log in to the Configurator Web interface.
   See “Horizon Workspace Web Interface URLs,” on page 11 for the URL for the Configurator Web interface.
2. Click the Module Configuration tab.
3. Click Enable this module in the Web Applications module.

The Web Applications module is now enabled.
What to do next

Add Web applications to the catalog. Configure Web applications as necessary, which might include configuring license tracking and provisioning for applications. See “Adding Web Applications to Your Organization’s Catalog,” on page 105.

Establish Secure Single Sign-On to Your Web Applications Through Horizon Workspace

You can provide single sign-on through Horizon Workspace to your Web applications that are configured with either SAML or WS-Federation protocol for authentication.

Your users that are registered to use the application sign in through Horizon Workspace to access these Web applications.

Configuring Web Applications that Use SAML Protocol

Many of the applications in the cloud application catalog use SecurityAssertion Markup Language (SAML1 or SAML 2) to exchange authentication and authorization data to verify that users can access a Web application.

The configuration form for adding Web applications to your catalog is partially configured. You can complete some SAML configurations in the Administrator Web interface, but you might also need to work with your Web application account representatives to complete other required setup.

Configuring Horizon Workspace for Single-Sign on to Microsoft Office 365 Applications

Office 365 SharePoint and Office 365 Outlook Web applications can be configured for single sign-on through Horizon Workspace. To use single sign-on to access these Office 365 applications, the Microsoft Office 365 domain must be changed from managed to federated, and Office 365 domain parameters settings changed to authenticate through Horizon Workspace.

To set up single-sign on Horizon Workspace, you

- Make changes to the domain attribute mapping in Horizon Workspace
- Synchronize Active Directory to Horizon Workspace
- Convert Your Microsoft Office 365 domain from managed to federated
- Update the settings for the Office 365 account to Horizon Workspace settings

End User Authentication to Office 365 from Native Clients

Office 365 does not support single sign on for desktop or mobile native clients, such as Outlook. To authenticate a native client in Office 365, users must configure a password in the Office 365 app. Users right-click on the Office 365 app in their Horizon Workspace user portal and click Set Password. They then configure their native client with this password.

Table 14-1. Supported Native Clients

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Native Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows computers</td>
<td>Microsoft Outlook Client</td>
</tr>
<tr>
<td>Apple Mac computers</td>
<td>Microsoft Outlook Client, Mac Outlook Web App</td>
</tr>
<tr>
<td>iPhone and iPad devices</td>
<td>iOS Email, Outlook Web App</td>
</tr>
<tr>
<td>Android devices</td>
<td>Android Email</td>
</tr>
</tbody>
</table>
A forgotten password cannot be retrieved. If users forget their passwords, they go back to the Office 365 app and enter a new password. They also must change this password on the native client.

Office 365 Requirements

Work with your Microsoft service provider to make sure that your managed Office 365 environment is correctly set up before you configure Horizon Workspace for single sign-on. The Office 365 directory synchronization tool must have synchronized your Active Directory to the Office 365 account, and the Windows PowerShell must be installed on the Windows server.

Mapping Attributes in the Horizon Workspace Connector

To enable Horizon Workspace to interact with Office 365, you must map the following Horizon Workspace user attributes to the Active Directory user attributes.

Procedure

1. Log in to the Connector Web interface using the administrative password for your Horizon Workspace server.

   The Connector Web interface URL is https://ConnectorHostname/hc/admin/.

2. Verify that the Horizon userPrincipalName attribute is mapped to the Directory userPrincipalName attribute.

3. Click Add and add the Horizon attribute objectGUID and map it to the Directory attribute objectGUID.

4. Click Save.

5. To sync your changes to Active Directory immediately, select Directory Sync and click Edit Directory Sync Rules to run the Horizon Connector Sync wizard, otherwise your changes are synced to Active Directory at your next scheduled sync interval.

6. Exit the Connector.

What to do next

Convert your Office 365 managed domain to a federated domain for single sign-on and update the settings for the Office 365 account to Horizon Workspace settings.

Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Horizon Workspace

You must convert your Office 365 managed domain to a federated domain for single sign-on and update the settings for the Office 365 account to Horizon Workspace settings.

Prepare your Office 365 domain to use Horizon Workspace for authentication.

Prerequisites

Run the Microsoft PowerShell Convert-MsoDomainToFederated cmdlet to convert the Office 365 domain from standard authentication to single sign-on. Refer to your Microsoft Windows 365 documentation for information about how to run the cmdlet.
Procedure

1. Run the `Set-MsolDomainAuthentication` cmdlet to change the following variables to the Horizon Workspace settings.

<table>
<thead>
<tr>
<th>Table 14-2: Replacing the Cmdlet Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line of cmdlet</strong></td>
</tr>
<tr>
<td>-DomainName</td>
</tr>
<tr>
<td>-IssuerUri</td>
</tr>
<tr>
<td>-FederationBrandName</td>
</tr>
<tr>
<td>-PassiveLogOnUri</td>
</tr>
<tr>
<td>-ActiveLogOnUri</td>
</tr>
<tr>
<td>-LogOffUri</td>
</tr>
<tr>
<td>-MetadataExchangeUri</td>
</tr>
<tr>
<td>-SigningCertificate</td>
</tr>
</tbody>
</table>

2. Verify the federation settings. Type `Get-MsolDomainFederationSettings -DomainName <YOUR DOMAIN>`

Example: Example of Output From Powershell Cmdlet

```
Set-MsolDomainAuthentication
-DomainName example.mycompanydomain_name.com
-Authentication Federated
-IssuerUri example
-FederationBrandName Mycompany, Inc.
-PassiveLogOnUri https://host/port/SAAS/API/1.0/POST/sso
-LogOffUri https://login.microsoftonline.com/logout.srf
-ActiveLogOnUri https://host/port/SAAS/auth/wsfed/active/logon
-MetadataExchangeUri https://host/port/SAAS/auth/wsfed/services/mex
```
Adding Web Applications to Your Organization's Catalog

After the Web Applications module is enabled, you can add your organization's Web applications to your catalog and make these applications accessible to your Horizon Workspace users and groups.

When you add an entry for a Web application to the catalog, you create an application record and configure the address of the Web application. Horizon Workspace uses the application record as a template to establish a secure connection with the Web application.

The following methods can be used to add application records of Web applications to your catalog from the Catalog page.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the cloud application catalog</td>
<td>Popular enterprise Web application types are listed in the Horizon Workspace cloud application catalog. These applications are partially configured to work in Horizon Workspace. You must complete the rest of the application record form.</td>
</tr>
<tr>
<td>Create a new one</td>
<td>You can add Web applications to your catalog that are not listed in the cloud application catalog. The application record for Web applications that Horizon Workspace does not include are more generic than that of cloud application catalog applications. You enter the application description and configuration information to create the application record.</td>
</tr>
<tr>
<td>Import a ZIP or JAR file</td>
<td>You can import a Web application that you previously configured in Horizon Workspace. You might want to use this method to move a Horizon Workspace deployment from staging to production. In such a situation, you export a Web application from the staging deployment as a ZIP file. Then you import the ZIP file to the production deployment.</td>
</tr>
</tbody>
</table>

After you add Web applications to the catalog, you can configure entitlements, access policies, licensing, and provisioning information.

Add a Web Application to Your Catalog from the Cloud Application Catalog

The cloud application catalog is populated with Web applications. These applications include some information in their application records. When you add a Web application to your catalog from the cloud application catalog, you must provide additional information to complete the application record.

When you add a Web application to the catalog, you are creating an entry that points indirectly to the Web application. The entry is defined by the application record, which is a form that includes a URL to the Web application.

Prerequisites

Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 101.

When you add a Web application to the catalog, you can apply a Web-application-specific access policy set to control user access to the application. If such a Web-application-specific access policy set does not already exist and you intend to apply one to this Web application, create the access policy set now. See “Managing Web-Application-Specific Access Policy Sets,” on page 32.
Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Click the Catalog tab.
3. Click + Add Application > Web Application ...from the cloud application catalog.
4. Click the icon of the Web application to add to your organization's catalog.

   The application record is added to your catalog, and record's Details page displays with the name and authentication profile already specified in the form.
5. (Optional) Customize the information on the Details page for your organization's needs.

   Items on the page are populated with information specific to the Web application.

   For example, you might choose an icon that best represents this Web application to your Horizon Workspace users when they see the application listed in their Horizon Workspace client.

   You can edit some of the populated items, depending on the application.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>If necessary, change the name of the application.</td>
</tr>
<tr>
<td>Description</td>
<td>Change the description of the application.</td>
</tr>
<tr>
<td>Icon</td>
<td>Click Choose File to upload an icon for the application. Horizon Workspace supports PNG, JPEG, and ICON file formats up to 4MB. Horizon Workspace resizes uploaded icons to 80px X 80px. To prevent distortion, upload icons where the height and width are equal to each other and as close as possible to the 80px X 80px resize dimensions.</td>
</tr>
<tr>
<td>Categories</td>
<td>To allow the application to appear in a category search of catalog resources, select the respective category from the drop-down menu.</td>
</tr>
</tbody>
</table>

6. Click Save.

7. Click Configuration, edit the application record's configuration details, and click Save.

   Some of the items on the form are prepopulated with information specific to the Web application. Some of the prepopulated items are editable, while others are not. The information requested varies from application to application.

   For some applications, the form has an Application Parameters section. If the section exists for an application and a parameter in the section does not have a default value, provide a value to allow the application to launch. If a default value is provided, you can edit the value.

   When you use Office 365 SharePoint or Office 365 Outlook applications, you must edit the Application Parameters section. For Office 365 SharePoint, enter your domain as mycompany. For Office 365 Outlook, enter your domain as mycompany.com.

8. Select the Entitlements, Licensing, and Provisioning tabs and customize the information as appropriate.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlements</td>
<td>Entitle users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future.</td>
</tr>
<tr>
<td>Access Policies</td>
<td>Apply a Web-application-specific access policy set to control user access to the application.</td>
</tr>
</tbody>
</table>
Tab Description

Licensing Configure license tracking. Add license information for the application to track license use in reports.

Provisioning Select a provisioning adapter. Horizon Workspace ships with the provisioning adapters for Google Apps and Mozy. If you are configuring either of these Web applications, you can select the appropriate provisioning adapter. Provisioning provides automatic application user management from a single location. Provisioning adapters allow the Web application to retrieve specific information from Horizon Workspace as required. For example, to enable automatic user provisioning to Google Apps, user account information, such as user ID, first name, and last name must exist in the Google Apps database. An application might require other information, such as group-membership and authorization-role information.

What to do next
For details about adding user and group entitlements for Web applications, see “Entitle Users and Groups to Web Applications,” on page 109.

Add a Web Application to Your Catalog by Creating a New Application Record
You create an application record when the Web application to add to your catalog is not available in the cloud application catalog.

When you successfully complete the application record for a Web application, an entry is created in your catalog that points indirectly to the Web application, and the Web application and Horizon Workspace can use SAML to communicate with each other.

Prerequisites
Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 101.

When you add a Web application to the catalog, you can apply a Web-application-specific access policy set to control user access to the application. If such a Web-application-specific access policy set does not already exist and you intend to apply one to this Web application, create the access policy set now. See “Managing Web-Application-Specific Access Policy Sets,” on page 32

Procedure
1. Log in to the Horizon Workspace Administrator Web interface.
2. Click the Catalog tab.
3. Click + Add Application > Web Application...create a new one.
   The application record is added to your catalog, and the system displays the record’s Details page.
4. Complete the information on the Details page, and click Next.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Provide the name of the application.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Provide a description of the application.</td>
</tr>
<tr>
<td>Icon</td>
<td>(Optional) Click Choose File to upload an icon for the application. Horizon Workspace supports PNG, JPG, and ICON file formats up to 4MB. Horizon Workspace resizes uploaded icons to 80px X 80px. To prevent distortion, upload icons where the height and width are equal to each other and as close as possible to the 80px X 80px resize dimensions.</td>
</tr>
</tbody>
</table>

Authentication Profile: Specify the appropriate federation protocol, if any.

After clicking Next, the Configuration page appears.
5 Edit the application record’s configuration details as necessary, and click **Save**.

Some of the items on the form are prepopulated.

When the **SAML 2.0 POST Profile** is selected on the Details page, the Configuration page includes the Configure Via section. Use the options in the Configure Via section to specify how the application metadata is retrieved. You can select retrieval by auto-discovery URL, meta-data XML, or manual configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-discovery (meta-data) URL</td>
<td>If the XML metadata is accessible on the Internet, provide the URL.</td>
</tr>
<tr>
<td>Meta-data XML</td>
<td>If the XML metadata is not accessible on the Internet, but is available to you, paste the XML in the text box.</td>
</tr>
<tr>
<td>Manual configuration</td>
<td>If the XML metadata is not available to you, complete the XML manual configuration items.</td>
</tr>
</tbody>
</table>

6 Select the **Entitlements**, **Licensing**, and **Provisioning** tabs and customize the information as appropriate.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlements</td>
<td>Entitle users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future.</td>
</tr>
<tr>
<td>Access Policies</td>
<td>Apply a Web-application-specific access policy set to control user access to the application.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Configure license tracking. Add license information for the application to track license usage in reports.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Select a provisioning adapter. Horizon Workspace ships with the provisioning adapters for the Google Apps and Mozy Web applications. If you are configuring either of these applications, you can select the appropriate provisioning adapter. Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from Horizon Workspace as required. For example, to enable automatic user provisioning to Google Apps, user account information, such as user ID, first name, and last name must exist in the Google Apps database. Other information, such as group-membership and authorization-role information might be required by an application.</td>
</tr>
</tbody>
</table>

**What to do next**

See “Entitle Users and Groups to Web Applications,” on page 109 for details about adding user and group entitlements for Web applications.

**Add a Web Application to Your Catalog by Importing a ZIP or JAR File**

You can import to your catalog a Web application that was previously configured in another Horizon Workspace instance, for example when moving from a staging system to a production system.

This process involves exporting the application bundle of a Web application from a Horizon Workspace instance and importing the bundle to another Horizon Workspace instance. Because you import the Web application from a Horizon Workspace deployment, the application might not require further configuration, especially if you thoroughly tested the configuration values in the original deployment. To further configure the Web application after importing it, see “Add a Web Application to Your Catalog from the Cloud Application Catalog,” on page 105 or “Add a Web Application to Your Catalog by Creating a New Application Record,” on page 107.
Prerequisites
Verify the following items:

- The Web Applications module is enabled. See “Enable the Web Applications Module to Provide Web Application Access,” on page 101.
- You can log in as an administrator to the Horizon Workspace instance that has the Web application to add to your catalog.

Procedure
1. Log in to the Horizon Workspace Administrator Web interface of the Horizon Workspace instance from which to export a Web application.
2. Click the Catalog tab.
3. Click Any Application Type > Web Applications.
4. Click the icon of the Web application to export.
5. Click Export this Application.
6. Click Export.
7. Save the zipped application bundle to your local system.
8. Log in to the Horizon Workspace Administrator Web interface of the Horizon Workspace instance to which to import the Web application.
9. Click the Catalog tab.
10. Click + Add Application > Web Application ...import a zip or jar file..
11. Browse to the location on your local system where you saved the compressed application bundle as a ZIP file, select the file, and click Submit.

What to do next
For details about adding user and group entitlements for Web applications, see “Entitle Users and Groups to Web Applications,” on page 109.

Entitle Users and Groups to Web Applications
You can entitle users and groups to Web applications.

You can only entitle Horizon Workspace users, users who are imported from your directory server, to Web applications. When you entitle a user to a Web application, the user sees the application and can launch it from their Horizon Workspace client. If you remove the entitlement, the user cannot see or launch the application from the client.

In many cases, the most effective way to entitle users to Web applications is to add a Web application entitlement to a group of users. However, in certain situations entitling individual users to a Web application is more appropriate.

Prerequisites
- Add one or more Web applications to your catalog. See “Adding Web Applications to Your Organization’s Catalog,” on page 105.
Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Entitle users to a Web application.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Access a Web application and entitle users or groups to it.           | a. Click the Catalog tab.  
 b. Click Any Application Type > Web Applications.  
 c. Click the Web application to which to entitle users and groups.  
 The information page for the Web application appears with the Entitlements tab selected by default. Group entitlements are listed in one table, user entitlements are listed in another table.  
 d. Click Add group entitlement or Add user entitlement.  
 e. Type the names of the groups or users.  
 You can search for users or groups by starting to type a search string and allowing the autocomplete feature to list the options, or you can click browse to view the entire list.  
 f. Use the drop-down menu to select how to activate each selected Web application.  
   - Automatic displays the application by default in an entitled user's list of Web applications the next time that user logs in using their Horizon Workspace client.  
   - User-Activated requires that an entitled user must add the Web application to their list of Web applications using their Horizon Workspace client before the user can use the application.  
 g. Click Save. |
| Access a user or group and add Web application entitlements to that user or group. | a. Click the Users & Groups tab.  
 b. Click the Users or Groups tab.  
 c. Click the name of a user or group.  
 d. Click Add Entitlement.  
 e. Select the check boxes next to the Web applications to which you want to entitle the user or group.  
 f. Use the drop-down menu to select how to activate each selected Web application.  
   - Automatic displays the application by default in an entitled user's list of Web applications the next time that user logs in using their Horizon Workspace client.  
   - User-Activated requires that an entitled user must add the Web application to their list of Web applications using their Horizon Workspace client before the user can use the application.  
 g. Click Save. |

The selected user or group is now entitled to use the Web application.
You can provide Horizon Workspace users access to Citrix-based applications.

When you integrate a Citrix deployment with Horizon Workspace, Horizon Workspace users can use Citrix Receiver on their systems and devices to access their entitled Citrix-based applications.

**NOTE** After you integrate Horizon Workspace with your Citrix deployment, you use the Citrix deployment to manage Citrix-based applications and to entitle users to the applications. You can then use the Horizon Workspace Administrator Web interface to view the Citrix-based applications and their entitlements.

Typically, you integrate your Citrix deployment with Horizon Workspace while deploying Horizon Workspace. To complete the integration, you can enable the Citrix Published Applications module using the Administrator Web interface.

Horizon Workspace provides default global application delivery settings for Citrix-based applications. For example, you can edit the settings that control application streaming and application security. You can configure the delivery settings globally, for all the Citrix-based applications in the Horizon Workspace catalog, or for individual Citrix-based applications.

This chapter includes the following topics:

- “Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment,” on page 111
- “View User and Group Entitlements to Citrix-Based Applications,” on page 112
- “Editing Horizon Workspace Application Delivery Settings for Citrix-Based Applications,” on page 113
- “Managing Categories for Citrix-Based Applications,” on page 115

**Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment**

If you did not enable the Citrix Published Applications module when you installed and configured Horizon Workspace, you can enable it later from the Modules tab on the Dashboard page of the Administrator Web interface.

See *Installing and Configuring Horizon Workspace* for detailed instructions about the configurations required on your Citrix deployment and on Horizon Workspace, such as in the Connector Web interface.

**Procedure**

1. Log in to the Administrator Web interface.
2. Select Dashboard > Modules.

3. In the Citrix Published Applications module, click Enable this module.

4. Perform the configurations required to complete the Integration of your Citrix deployment with Horizon Workspace.

The Citrix Published Applications module is enabled. The Citrix-based applications available in the respective server farm are visible in your catalog.

What to do next

To edit the delivery settings of Citrix-based applications, such as the settings for streaming or security, use the Horizon Workspace Administrator Web interface. See “Editing Horizon Workspace Application Delivery Settings for Citrix-Based Applications,” on page 113.

View User and Group Entitlements to Citrix-Based Applications

You can see the Citrix-based applications to which your Horizon Workspace users and groups are entitled.

IMPORTANT You cannot use Horizon Workspace to make changes to your Citrix deployment or Citrix-based applications. If a Citrix administrator makes any changes, such as entitled new users to an application, or adding a new server farm, you must force a sync to propagate the changes to Horizon Workspace. Use the Horizon Workspace Connector Web interface to force a sync.

Prerequisites

Verify that Horizon Workspace is integrated with Citrix deployment. See Installing and Configuring Horizon Workspace.

Synchronize information, including entitlements, from your Citrix deployment to Horizon Workspace. You can force a sync with the following steps:

1. Open the Connector Web interface in your browser. The Connector Web interface URL is https://ConnectorHostname/hc/admin/, where ConnectorHostname is the hostname for your Horizon Workspace Connector.

2. Log in to the Connector Web interface using the administrative password for Horizon Workspace.

3. Click Published Apps - Citrix and click Sync Now.

Procedure

1. Log in to the Administrator Web interface.
2 View user and group entitlements to Citrix-based applications.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| View the list of users and groups entitled to a specific Citrix-based application. | a Click the Catalog tab.  
b Click Any Application Type > Citrix Published Applications.  
c Click the name of the Citrix-based application for which you want to list entitlements.  
The Entitlements tab is selected by default. Group entitlements and user entitlements are listed in separate tables. |

| View the list of Citrix-based application entitlements for a specific user or group. | a Click the Users & Groups tab.  
b Click the Users tab or the Groups tab.  
c Click the name of an individual user or group.  
The Entitlements tab is selected by default. Entitled Citrix-based applications are listed in the Citrix Published Applications table on the Entitlements page. |

Editing Horizon Workspace Application Delivery Settings for Citrix-Based Applications

You can use the Horizon Workspace Administrator Web interface to edit the delivery settings of Citrix-based applications.

Using the Administrator Web interface, you can edit the delivery settings globally for all of the Citrix-based applications available from your Horizon Workspace deployment, or individually for specific Citrix-based applications.

You configure the delivery settings by editing Independent Computing Architecture (ICA) properties. ICA is a Citrix proprietary protocol. A wide range of ICA properties are available, controlling areas such as security, display, and compression. For more information about configuring ICA properties, see Citrix documentation.

Horizon Workspace includes default global settings that define how the configured Citrix deployment delivers Citrix-based applications to users. You can use the Horizon Workspace Administrator Web interface to configure the default Horizon Workspace settings and to add new settings.

You can also use the Horizon Workspace Administrator Web interface to specify delivery settings for individual applications. Settings for individual applications take precedence over global settings. When you provide ICA properties for the delivery of a specific application, list all the properties necessary for the Citrix deployment to deliver the application in the manner you expect. When delivery settings exist in Horizon Workspace for an individual application, Horizon Workspace applies only those settings and ignores all global application delivery settings.

Edit the Horizon Workspace Application Delivery Settings Globally for All Citrix-Based Applications

You can use the Horizon Workspace Administrator Web interface to edit the global settings for the Citrix-based applications in your Horizon Workspace deployment.

The ICA properties text boxes for the global application delivery settings are populated with default settings until you edit them.

Prerequisites
Enable the Citrix Published Applications module. See “Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment,” on page 111
Procedure

1. Log in to the Administrator Web interface as an administrator.
2. Select **Settings > Citrix Published Applications**.
3. Edit the ICA properties according to Citrix guidelines.

   The ICA Client Properties and the ICA Launch Properties text boxes work together. They must both have content or they must both be empty.
4. Click **Save**.

Unless individual applications have their own application delivery settings, your Citrix deployment applies the global ICA properties when it delivers Citrix-based applications available through Horizon Workspace to users.

**Edit the Horizon Workspace Application Delivery Settings for a Single Citrix-Based Application**

You can use the Horizon Workspace Administrator Web interface to edit the settings for individual Citrix-based applications in your Horizon Workspace deployment.

The ICA properties text boxes for individual applications are empty until you manually add properties.

When you edit the application delivery settings, the ICA properties, of an individual Citrix-based application, those settings take precedence over the global settings. You can configure the global ICA property settings from the Citrix Published Applications page by selecting **Settings > Citrix Published Application**.

**Prerequisites**

Enable the Citrix Published Applications module. See “Enable the Citrix Published Applications Module to Integrate Horizon Workspace with Your Citrix Deployment,” on page 111

**Procedure**

1. Log in to the Administrator Web interface as an administrator.
2. Click the **Catalog** tab.
3. Click **Any Application Type > Citrix Published Applications**.
4. Click the name of the Citrix-based application to edit.
5. Click **Configuration**.
6. View the information about the application as carried forward from your Citrix deployment.
   
   The page provides several details about the application, such as the application name, application ID, server name, and so on. Also, the page displays information about the application's enablement. If the **Enabled** check box is not selected, the application is disabled in your Citrix deployment.
7. If the **Enabled** check box is not selected and you want to hide the application from users, select the **Hide When Disabled** check box.
8. In the ICA properties text boxes, add properties or edit existing properties according to Citrix guidelines.

   The ICA Client Properties and the ICA Launch Properties text boxes work together. They must both have content or they must both be empty.
9. Click **Save**.
Your Citrix deployment applies the ICA properties listed on the Horizon Workspace Configuration page of an application when it delivers the Citrix-based application to users.

Managing Categories for Citrix-Based Applications

You can use the Horizon Workspace Administrator Web interface and your Citrix deployment to manage Citrix-based application categories.

In your Citrix deployment, you give an application a category name by editing the **Client application folder** text box in the application’s properties. When you integrate your Citrix deployment with Horizon Workspace, existing category names for Citrix-based applications are carried over to Horizon Workspace.

After the integration, you can continue to create categories in your Citrix deployment. Those categories are carried over to Horizon Workspace during the next sync. You can also create categories directly in Horizon Workspace. See “Overview of Using Resource Categories,” on page 54.

In the Horizon Workspace Administrator Web interface, you can create and view categories of all Citrix-based applications by clicking the **Catalog** tab and clicking **Any Application type > Citrix Published Applications**. You can view and edit the categories of a specific Citrix-based application by clicking the name of the application and selecting **Details**.

When you create a category in Horizon Workspace, the category never appears in your Citrix deployment.

When you create a category in your Citrix deployment, the category appears in Horizon Workspace at the next sync. When you update a category name in your Citrix deployment, the updated category name appears in Horizon Workspace while the original category name remains. If you want to remove the original category name from Horizon Workspace, you must remove it manually.
With Horizon Workspace, you can centrally distribute and manage ThinApp packages. ThinApp packages are virtualized Windows applications, and are used on Windows systems. Entitled users who have the Horizon Workspace Client for Windows installed on their Windows systems can launch and use their entitled ThinApp packages on those Windows systems.

In the ThinApp capture and build processes, you create a virtual application from a Windows application. That virtualized Windows application can run on a Windows system without that system having the original Windows application installed. The ThinApp package is the set of virtual application files generated by running the ThinApp capture and build processes on a Windows application. The package includes the primary data container file and entry point files to access the Windows application.

Not every ThinApp package is compatible with Horizon Workspace. When you capture a Windows application, the default settings in the ThinApp capture-and-build process create a package that Horizon Workspace cannot distribute and manage. You create a ThinApp package that Horizon Workspace can distribute and manage by setting the appropriate parameters during the capture and build processes. See the VMware ThinApp documentation for detailed information on ThinApp features and the appropriate parameters to use to create a package compatible with Horizon Workspace.

After you integrate your Horizon Workspace system with your ThinApp repository according to the steps in Installing and Configuring Horizon Workspace, you can see in your catalog those ThinApp packages from the repository that Horizon Workspace can distribute and manage. After you see the ThinApp packages in your catalog, you can then entitle users and groups to those ThinApp packages, and optionally configure license tracking information for each package.

This chapter includes the following topics:

- “Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Horizon Workspace System,” on page 118
- “Distributing and Managing ThinApp Packages with Horizon Workspace,” on page 118
- “Entitle Users and Groups to ThinApp Packages,” on page 123
- “Updating Managed ThinApp Packages After Deployment in Horizon Workspace,” on page 125
- “Delete ThinApp Packages from Horizon Workspace,” on page 130
- “Make Existing ThinApp Packages Compatible with Horizon Workspace,” on page 131
Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Horizon Workspace System

If you did not enable the ThinApp Packages module when you installed and configured your Horizon Workspace system, you can enable it later from the Modules tab on the Dashboard page of the Administrator Web interface.

Typically, after you complete the steps to integrate the source of your ThinApp packages with your Horizon Workspace system, the Dashboard page automatically indicates that the ThinApp Packages module is enabled. Sometimes, the module might not appear enabled, and you can use these steps to complete the enablement.

Prerequisites

Verify that your Horizon Workspace system is integrated with the source of the ThinApp packages, according to the steps in Installing and Configuring Horizon Workspace.

Procedure

1. Log in to the Administrator Web interface.
2. Select Dashboard > Modules.
3. In the ThinApp Packages module, click Enable this module.

The ThinApp Packages module is enabled. The ThinApp packages that are available at the source location are visible in your catalog.

If a message tells you to go to all connector instances, then the prerequisite integration is not fully in place. Ensure that your Horizon Workspace system is integrated with the source of the ThinApp packages according to the steps in Installing and Configuring Horizon Workspace before you enable the ThinApp Packages module.

What to do next

As appropriate, distribute the Horizon Workspace Client for Windows to users’ Windows systems for those users to whom you want to entitle ThinApp packages. See “Deploying the Horizon Workspace for Windows Application To Use ThinApp Packages,” on page 119.

Distributing and Managing ThinApp Packages with Horizon Workspace

Before your Horizon Workspace users can run their ThinApp packages that are registered to them using Horizon Workspace, those users must have the Horizon Workspace for Windows client application installed and running on their Windows systems.

ThinApp packages are virtualized Windows applications. The ThinApp packages are distributed to Windows systems, and a user logged into the Windows system can launch and run those ThinApp packages that are registered on that Windows system. Horizon Workspace can distribute and manage ThinApp packages that are compatible with Horizon Workspace. See Installing and Configuring Horizon Workspace for a description of the requirements on ThinApp packages for use with Horizon Workspace.

To successfully launch and run one of these virtualized applications in the user’s logged-in Windows session, the following elements are required:

- The virtualized application’s ThinApp package is registered for that user’s use by the Horizon Workspace server.
- A particular DLL is available on that Windows system.
The HorizonThinAppClient.exe process is running.

When a compatible ThinApp package is created, it is configured to load a particular DLL when the logged-in user launches the virtualized application in their logged-in Windows session. At that time, the virtualized application attempts to load the DLL. When the DLL is loaded, it attempts to verify with the locally installed Horizon Workspace ThinApp client whether that ThinApp package is registered on that Windows desktop for that user. The locally installed ThinApp client determines whether that application is registered for that user without communicating with the Horizon Workspace server. If the application is registered on that Windows desktop for that user, the ThinApp client checks to see if it last synched with the Horizon Workspace server. If the ThinApp client confirms that the time from the last synch is within the offline grace period configured for the installed client, the client allows the application to run.

Because that DLL is available on the Windows system only if the Horizon Workspace for Windows application is installed on that Windows system, and because the HorizonThinAppClient.exe process is running if the Horizon Workspace for Windows application is running on that system, the Horizon Workspace for Windows application must be installed on the Windows system to run ThinApp packages that are distributed and managed by your Horizon Workspace server.

The Horizon Workspace for Windows client application is used by the Horizon Workspace file-sharing service and for ThinApp packages. To use the file-sharing features, as opposed to the file-storage features, of the Horizon Workspace file-sharing service, the user is not required to have the client application installed. Many of the file-sharing features can be accessed using the Horizon Workspace browser-based user portal. The client application enhances the user experience of the file-sharing features beyond the experience available in the Horizon Workspace user portal. However, to use ThinApp packages that are distributed and managed by Horizon Workspace, the Horizon Workspace for Windows application must be installed and running.

Deploying the Horizon Workspace for Windows Application To Use ThinApp Packages

The Horizon Workspace for Windows application can be installed by either double-clicking its installer EXE file, running the executable file using the command-line options, or running a script that uses the command-line options. Local administrator privileges are required to install the application. For information about installing the Horizon Workspace for Windows application by double-clicking its installer EXE file, see the Horizon Workspace User Guide.

The configuration of the installed application determines how a ThinApp package that is distributed by Horizon Workspace is deployed to that Windows system. By default, when the Horizon Workspace for Windows application is installed by double-clicking its installer EXE file, the client is configured to deploy ThinApp packages using the COPY_TO_LOCAL deployment mode, with the AUTO_TRY_HTTP option enabled. Those default installer options result is what is called a download deployment mode. With the COPY_TO_LOCAL and AUTO_TRY_HTTP default settings, the client application first tries to download the ThinApp packages by copying them to the Windows system endpoint, and if the first attempt fails, the client application tries to download the ThinApp packages using HTTP. If your Horizon Workspace Connector is configured for account-based access to your ThinApp repository, the client application can download the ThinApp packages using HTTP. After the ThinApp packages are downloaded to the local Windows system, the user runs the virtualized applications on the local system.

To avoid having the virtualized applications downloaded to the local Windows system and using space on the Windows system, you can have users run the ThinApp packages from the network share by using what is called a streaming deployment mode. To have your users run the ThinApp packages using streaming mode, you must install the Horizon Workspace for Windows application on the Windows systems using a command-line installation process. The installer has command-line options that you can use to set the runtime deployment mode for the ThinApp packages. To set the runtime deployment mode to stream the ThinApp packages, use the RUN_FROM_SHARE installer option.
One method for installing the Horizon Workspace for Windows application to multiple Windows systems is to use a script to install the application silently to the Windows systems. You can install the client silently to multiple Windows systems at the same time.

**NOTE**  A silent installation does not display messages or windows during the install process.

You set a value in the script to indicate whether the clients installed by that script deploy ThinApp packages using the ThinApp streaming mode, or RUN_FROM_SHARE option, or one of the ThinApp download modes, such as the COPY_TO_LOCAL or HTTP_DOWNLOAD option. See “Install the Horizon Workspace for Windows Application with Identical Settings to Multiple Windows Systems,” on page 68.

### Determining the Appropriate Deployment Mode for ThinApp Packages on Windows Endpoints

The configuration of the Horizon Workspace for Windows application on the Windows endpoint determines whether a ThinApp package that is distributed using Horizon Workspace is deployed using ThinApp streaming mode, RUN_FROM_SHARE, or one of the ThinApp download modes, COPY_TO_LOCAL or HTTP_DOWNLOAD. When you create the script to silently install Horizon Workspace for Windows to Windows endpoints, such as desktop and laptop computers, you set the options that set the ThinApp package deployment mode. Choose the deployment mode that best fits the network environment for the selected endpoints, considering details such as network latency.

With streaming mode, when the Horizon Workspace for Windows application synchronizes with Horizon Workspace, the client downloads application shortcuts for the ThinApp packages’ virtualized Windows applications to the Windows desktop, and when the user launches the ThinApp packages, the virtualized Windows applications run from the file share on which the ThinApp packages reside. Therefore, streaming mode is best appropriate for systems that will always be connected to the network share, such as Horizon View desktops. With download mode, at the first use or update of a ThinApp package, the user must wait for the ThinApp package to download to the Windows system first, and shortcuts are created. After the initial download, the user launches and runs the virtualized Windows application on the local Windows system.

**IMPORTANT**  For non-persistent Horizon View desktops, also known as floating or stateless Horizon View desktops, you are expected to set the client to use ThinApp streaming mode by using the command-line installer option `/v INSTALL_MODE=RUN_FROM_SHARE` when installing the client. The RUN_FROM_SHARE option provides the most optimal runtime experience for using ThinApp packages in floating Horizon View desktops. See “Command-Line Installer Options for Horizon Workspace for Windows,” on page 62.
Table 16-1. ThinApp Deployment Mode for the Virtualized Applications Captured as ThinApp Packages

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| ThinApp streaming mode | In ThinApp streaming mode, the virtualized applications are streamed each time they are started. This method avoids using disk space in the desktop that would be used when copying the virtualized applications to the desktop. The desktop must be connected to the ThinApp packages' network share for the applications to run. The following environments might provide the consistency and stability required:  
  * Horizon View desktops, either stateless or persistent, with excellent connectivity to the file share on which the ThinApp packages reside.  
  * Users with Windows desktops that are not Horizon View desktops, that are shared by multiple users. This situation avoids the accumulation on disk of downloaded user-specific applications and also provides quick access to applications without causing a delay for downloads specific to a user.  
  The account that the user uses to log in to the Windows system is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and execute files on the network share. |
| ThinApp download mode | In ThinApp download mode, applications are downloaded to the Windows endpoint. The user runs the virtualized application locally on the endpoint. You might prefer ThinApp download mode for the following situations:  
  * Persistent Horizon View desktops  
  * LAN-connected desktops that are periodically offline  
  * A LAN with poor network latency  
  Horizon Workspace provides two flavors of the ThinApp download mode: COPY_TO_LOCAL and HTTP_DOWNLOAD. If the client is configured for COPY_TO_LOCAL, the Windows endpoint must be joined to the same domain as the file share unless the AUTO_TRY_HTTP option is enabled and the Connector is configured for account-based access to the ThinApp packages' network share. When the AUTO_TRY_HTTP option is enabled and the Connector is configured for account-based access, if the Windows endpoint is not joined to the same domain and the first attempt to download the ThinApp packages fails, the Horizon Workspace for Windows client application will automatically try to download the ThinApp packages using the HTTP protocol as for the HTTP_DOWNLOAD mode. With HTTP_DOWNLOAD, the Windows endpoint does not have to be joined to the same domain as the file share. However, the copy and sync times when using HTTP_DOWNLOAD are significantly longer than when using COPY_TO_LOCAL.  
  **IMPORTANT** If the Connector is not enabled for account-based access, downloading using the HTTP protocol does not work, even if AUTO_TRY_HTTP is enabled or the client is configured with the HTTP_DOWNLOAD option.  
  When using COPY_TO_LOCAL, the account that the user uses to log in to the Windows system is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and copy files from the network share. When using HTTP_DOWNLOAD, the share user account that is entered in the Connector Web interface when you configure your Horizon Workspace system's access to the ThinApp packages' network share is the account that is used to download the ThinApp packages. That share user account needs to have read permission on the ThinApp packages' network share to copy the files from the network share. |

The ThinApp packages' network share must meet the appropriate requirements for the deployment mode that you set for the Windows endpoints. See Installing and Configuring Horizon Workspace.

**Offline Grace Period and ThinApp Packages**

The offline grace period is the period of time for which a virtualized application is allowed to launch and run on a Windows system without syncing with the Horizon Workspace server.

ThinApp packages are virtualized Windows applications, and Horizon Workspace can distribute these applications to Windows systems. When Horizon Workspace distributes a ThinApp package to the Windows system for the first time for the user logged in to that system, the package’s virtualized applications are registered on that Windows system for that user’s use. The appropriate shortcuts are added to the Windows desktop, and the user can launch the virtualized applications using the shortcuts as for standard Windows applications installed to that system.
When a user launches one of the virtualized applications that was deployed to the Windows system by Horizon Workspace, the ThinApp package requests permission to run from the ThinApp agent running on the system. The ThinApp agent verifies the following conditions.

- Verifies whether the application is registered on this Windows desktop for the logged-in user.
- Verifies whether the Windows system has synced with the Horizon Workspace server within the configured offline grace period.

If both of those conditions are true, the ThinApp agent allows the virtualized application to run.

The frequency of how often the Horizon Workspace for Windows application syncs with the Horizon Workspace server is set by the POLLINGINTERVAL installer option. By default, the frequency is every 5 minutes. The offline grace period is set to 30 days by default. If a Windows system has had network connectivity to connect to the Horizon Workspace server at any time within a 30-day timespan, the application can sync with the server and virtualized applications can run.

However, if the Windows system has no network connectivity to connect to the Horizon Workspace server, the application cannot sync with the server. Virtualized applications registered on that Windows system can run on the disconnected system up to the time set by the offline grace period.

**Set the Offline Grace Period for ThinApp Packages**

Setting the offline grace period for the ThinApp agent on a Windows system requires modifying the registry. The default offline grace period is 30 days, and is a system-wide setting.

**Prerequisites**

- Verify that Horizon Workspace for Windows is installed on the Windows system.
- Verify that you have local administrative permissions to modify the Windows system's registry.

**Procedure**

1. Open the Windows system's registry in the Registry Editor.
2. Locate the OfflineGracePeriod registry key.

   Windows System | Registry Key
   ---------------|-----------------|
   Windows 32-bit  | HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\Horizon ThinApp\OfflineGracePeriod
   Windows 64-bit  | HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\Horizon ThinApp\OfflineGracePeriod

   The OfflineGracePeriod key has type REG_DWORD. The default settings is 720 (30 days).
3. Update the OfflineGracePeriod value to a timespan in hours.
4. Exit the Registry Editor.

**Using the Command-Line HorizonThinAppCtrl.exe Application**

The Horizon Workspace for Windows client application includes a command-line application, HorizonThinAppCtrl.exe, that you can use to perform operations related to using ThinApp packages on the client's Windows system.

The installation process for Horizon Workspace for Windows installs HorizonThinAppCtrl.exe in the HorizonThinApp folder in the Windows directory location where the Horizon Workspace for Windows is installed.
To use the HorizonThinAppCtrl.exe application to perform one of its supported commands, provide the command as the first argument, followed by the command’s available options, as appropriate.

**HorizonThinAppCtrl.exe command options**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HorizonThinAppCtrl.exe recheck</td>
<td>This command immediately does an entitlement check of the ThinApp packages that are associated with the user account that is logged into the Horizon Workspace for Windows client. Any newly entitled or updated ThinApp packages are synced.</td>
</tr>
</tbody>
</table>
| HorizonThinAppCtrl.exe set                   | This command changes the ThinApp deployment mode used for ThinApp packages on this Windows system. Because this command changes the registry keys associated with the ThinApp deployment mode, only administrators with the appropriate registry permissions are able to change the install mode using this command. Available values for install_mode are:  
  - CopyToLocal  
  - RunFromShare  
  - HttpDownload  |
| HorizonThinAppCtrl.exe authorize             | This command verifies whether a ThinApp package can be launched. This command does not actually launch the ThinApp package. Provide the ThinApp package's GUID and the path to the package’s executable file. If ThinApp download mode is used for the packages on the Windows client system, the path is relative to the local cache folder, which is the same as the path relative to the repository root. An example is HorizonThinAppCtrl.exe authorize guid= 436E1D7D-552C-4F70-8197-DB1B05D30394 path="FileZilla Client 3.3.2/FileZilla.exe" You can see the ThinApp package's GUID, application path, and executable file name on its resources page in the Administrator Web interface. |
| HorizonThinAppCtrl.exe quit                  | This command tells the Horizon Workspace for Windows to exit cleanly.                                                                       |
| HorizonThinAppCtrl.exe launch app=package_path| This command is used to manually launch a ThinApp package, where package_path is the path to the package’s executable file, and launch_url is the Horizon Workspace protocol URL for that package, in the form horizon://package_path. An example is HorizonThinAppCtrl.exe launch app="FileZilla Client 3.3.2/FileZilla.exe" url="horizon://FileZilla Client 3.3.2/FileZilla.exe" This command is not typically used by end users, who can launch their entitled ThinApp packages from their My Apps area in the user portal. This command is typically used for debugging. |

**Entitle Users and Groups to ThinApp Packages**

You can entitle users and groups to Windows applications that are captured as ThinApp packages.

You can only entitle Horizon Workspace users, users who are imported from your directory server, to ThinApp packages. When you entitle a user to a ThinApp package, the user sees the application and can start it from the appropriate Horizon Workspace client on their system. If you remove the entitlement, the user cannot see or start the application.

Often, the most effective way to entitle users to ThinApp packages is to add a ThinApp package entitlement to a group of users. In certain situations entitling individual users to a ThinApp package is more appropriate.

**Prerequisites**

Configure Horizon Workspace to sync ThinApp packages to your Horizon Workspace catalog. When the ThinApp packages are synced to your catalog, you can entitle them to your users and groups.

Use the Configurator Web Interface or the Connector Web Interface to sync ThinApp packages to your catalog. You cannot add ThinApp packages directly to your catalog with the Administrator Web interface.
### Procedure

1. Log in to the Horizon Workspace Administrator Web interface.

2. Entitle users to a ThinApp package.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Access a ThinApp package and entitle users or groups to it.** | | a | Click the Catalog tab.  
| | b | Click Any Application Type > ThinApp Packages.  
| | c | Click the ThinApp package to which to entitle users and groups.  
| | d | Click Add group entitlement or Add user entitlement.  
| | e | Type the names of the groups or users.  
| | f | From the drop-down menu, select the activation method for the ThinApp package.  
| | g | Click Save.  
| **Access a user or group and add ThinApp package entitlements to that user or group.** | | a | Click the Users & Groups tab.  
| | b | Click the Users or Groups tab.  
| | c | Click the name of an individual user or group.  
| | d | Click Add entitlement.  
| | e | Click the check boxes next to the ThinApp packages to which to entitle the user or group.  
| | f | From the drop-down menu, select the activation method for the ThinApp package.  
| | g | Click Save.  

The selected users or groups are now entitled to use the ThinApp package.

**What to do next**

Verify that the Horizon Workspace for Windows client application is installed on users’ Windows systems.
Updating Managed ThinApp Packages After Deployment in Horizon Workspace

After adding a ThinApp package to your organization’s catalog and entitling your Horizon Workspace users to that ThinApp package, your organization might want to update that package and have the users use a newer, or rebuilt, version of the ThinApp package, without having to unentitle the users from the current package and then entitling them to the newer package.

An updated ThinApp package might be made available because a newer version of the Windows application for that package is released, or because the packager of the application has changed the values of parameters used by the package.

ThinApp 4.7.2 and newer versions provide an update mechanism for ThinApp packages used in a Horizon Workspace system. This ThinApp update mechanism is different from other update mechanisms for ThinApp packages used outside of a Horizon Workspace environment. The updated ThinApp package must have been updated with this mechanism for you to be able to deploy the updated package in Horizon Workspace and have users automatically see the newer version.

For ThinApp packages that are managed in a Horizon Workspace system, two Package.ini parameters are used by Horizon Workspace to determine that a package is an updated version of another package.

**AppID**

The unique identifier for the ThinApp package in Horizon Workspace. All entry points (executables) for the package’s application are assigned the same AppID. After a ThinApp package is synced to your organization’s Horizon Workspace catalog, the package’s AppID is displayed in the GUID column in the ThinApp package’s resource page. This value consists of alphanumeric characters in a pattern of character sets, each set separated by dashes, such as in the following example:

```
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

Horizon Workspace considers any ThinApp package with the same AppID to be versions of the same application.

**VersionID**

The version number of the ThinApp package. Horizon Workspace uses the VersionID to keep track of different versions of the managed ThinApp package. You increment the VersionID value by one (1) to mark that ThinApp package as an update of another package, retaining the same AppID.

You place the updated package in a new folder in the network share folder configured for the managed ThinApp packages. See *Installing and Configuring Horizon Workspace*. When Horizon Workspace performs the scheduled sync with the network share folder and it encounters an application that has the same AppID as another application, it compares the VersionID values. The ThinApp package with the highest VersionID is used as the most recent update. Horizon Workspace automatically incorporates the previous user entitlements to the ThinApp package with the highest VersionID, and shortcuts on the users’ systems are synced to point to the updated package.

**IMPORTANT** The standard ThinApp **InventoryName** parameter is important to successful updates of managed ThinApp packages. Both the previous and updated ThinApp packages must have the same value for the InventoryName parameter. If the person creating the ThinApp package changes the InventoryName in a package, and then creates an updated package, you must make sure the InventoryName values match for the updates to work properly in your Horizon Workspace system.

See the *ThinApp Package.ini Parameters Reference Guide* for details about the various parameters that are used in a ThinApp package’s Package.ini file.
Update a Managed ThinApp Package

Updating a ThinApp package that is already managed by Horizon Workspace and in your organization’s catalog involves multiple steps. The updated ThinApp package might be provided to you by another group in your organization. To ensure that your Horizon Workspace system can automatically use the updated package in place of the existing one for the entitled users, you must ensure the updated package was created using the same AppID as the current package, has a VersionID value that is higher than the existing package’s VersionID value, and is enabled for management by Horizon Workspace.

Prerequisites

Verify that you have access to the location where your managed ThinApp packages reside and can create subfolders at that location.

Procedure

1. **Obtain the AppID and VersionID values of a Managed ThinApp Package** on page 126

   To ensure that Horizon Workspace automatically uses the updated ThinApp package in place of the current one, the updated ThinApp package must be created using the AppID of the currently managed ThinApp package and a higher VersionID value than the current version.

2. **Create the Updated ThinApp Package** on page 127

   The AppID and VersionID values of the currently managed ThinApp package are used for creating the updated package. The updated package uses the same AppID value and a higher VersionID value.

3. **Copy an Updated ThinApp Package to the Network Share** on page 129

   After you create the updated ThinApp package, you copy the appropriate files to a new subfolder at the same level as the existing subfolder on the network share.

What to do next

Your Horizon Workspace catalog displays the new version of the updated ThinApp package after the next sync of your Horizon Workspace system with your ThinApp package location. If you want to see the new version reflected in the ThinApp package’s resources page, you can manually sync using the ThinApp Packages page of the Connector Web interface. See *Installing and Configuring Horizon Workspace*.

Obtain the AppID and VersionID values of a Managed ThinApp Package

To ensure that Horizon Workspace automatically uses the updated ThinApp package in place of the current one, the updated ThinApp package must be created using the AppID of the currently managed ThinApp package and a higher VersionID value than the current version.

When the Setup Capture process is used to create an updated ThinApp package, the AppID value is automatically retrieved by the Setup Capture program from the existing ThinApp package’s executables, and the VersionID value is automatically incremented. However, the person who is creating the updated ThinApp package might use a different method for creating the updated package. When the Setup Capture process is not used to create the updated ThinApp package, the person creating the package must obtain the AppID and VersionID values for the ThinApp package that is currently managed by your Horizon Workspace system. The AppID and VersionID values are displayed on pages in the ThinApp package’s resource page in the Horizon Workspace Administrator Web interface.

Procedure

1. Click the Catalog tab.

2. Click Any Application Type > ThinApp Packages.

3. Click the ThinApp package to open its resource page.

4. Click Details.
5 Make note of the value listed in the **Version** field on the Details page.

6 Click **ThinApp Package** to display the ThinApp Package page.

7 Make note of the **AppID** value listed in the GUID column.

   The value listed in the GUID column is the value that Horizon Workspace uses to identify this ThinApp package.

**What to do next**

The person who is creating the updated ThinApp package should complete the steps in “Create the Updated ThinApp Package,” on page 127.

**Create the Updated ThinApp Package**

The **AppID** and **VersionID** values of the currently managed ThinApp package are used for creating the updated package. The updated package uses the same **AppID** value and a higher **VersionID** value.

Sometimes the updated ThinApp package is provided to you by another team in your organization. The person who creates the updated ThinApp package can use one of the described methods.

**Prerequisites**

Verify that you have the **AppID** and **VersionID** values of the current ThinApp package by completing the steps in “Obtain the AppID and VersionID values of a Managed ThinApp Package,” on page 126.

Verify that you have a version of the ThinApp program that is compatible with your version of Horizon Workspace. For information about specific ThinApp versions, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
## Procedure

- Using a version of the ThinApp program that is supported by Horizon Workspace, create the updated ThinApp package using one of the available methods.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Recapture using Setup Capture.**          | Use this method when the project folder for the existing ThinApp package managed by Horizon Workspace is unavailable. To create an updated package with Setup Capture, you need only the following items:  
  - The application executables from the existing ThinApp package  
  - The application installer  
  - Setup Capture and the ThinApp program at a version supported by Horizon Workspace.  
  
  During the capture process, select to manage the package with Horizon Workspace and that the package is an update of an existing base ThinApp package. Browse to the folder that contains the executables for the currently managed ThinApp package. Point to the folder, and not to specific executables.  
  
  With this method, you do not need to obtain the AppID or VersionID values in advance of creating the updated package. After you designate the package as an update and point to the prior version in Setup Capture, the capture process reads the AppID of the prior package and reuses it for the updated package. The process also provides an incremented VersionID for the updated package, and assigns the same InventoryName. |
| **Update the Package.ini file manually and then rebuild the package.** | Use this method when you do not have the application installer for the recapture process, or when you need to update the package to a newer ThinApp version and want to update more than what the relink command would handle. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new Package.ini parameter that you want to set.  
  
  To mark the new package as an update, edit the following Horizon Workspace parameters in the [Build Options] section of the Package.ini file:  
  - Set the AppID parameter to match the AppID value of the currently managed ThinApp application. You cannot reuse a value of genid for AppID, because then a new AppID value will be generated for the updated package and your Horizon Workspace system will not recognize the new package as an update to the existing one.  
  - Increment the value of the VersionID parameter to a higher integer than the currently managed ThinApp package. If there is no VersionID parameter set for the currently managed package, its value is 1 by default, and you would add a line for the VersionID parameter to Package.ini and set it to a value of 2 (VersionID = 2)  
  - Make sure the InventoryName parameter value matches the InventoryName value of the currently managed package. The InventoryName values for the current package and the updated package must be identical. |
| **Use the relink –h command with the AppID and VersionID options.** | Use this method in one of the following situations:  
  - You do not have the project folder for the application.  
  - You have already captured, built, and tested the package in a test environment that was not a Horizon Workspace system, and the only remaining steps are to enable the updated package for Horizon Workspace and place it in the network share used by the Horizon Workspace system.  
  - You are updating the package only to update the ThinApp runtime for the package to incorporate bug fixes available in that new ThinApp version. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For example, if you have changed the project directory, including the Package.ini file, for a virtual application, rebuilt the package, and tested the package, the test environment might not have been Horizon Workspace. The final stage of updating the application is to enable it for Horizon Workspace. At that point, the easiest route is to use the <code>relink -h</code> command, instead of recapturing or rebuilding. <strong>Note</strong>: The ThinApp runtime is always updated when you run the <code>relink -h</code> command on a ThinApp package. You can run the relink command from the ThinApp Program Files directory to get help on the command’s syntax. When the existing ThinApp package is already enabled for use by Horizon Workspace, you can run the following command to reuse the package’s existing AppID and increment the VersionID: <code>relink -h -VersionID + executable-folder/*.</code> Where <code>executable-folder</code> is a folder containing the executables of the ThinApp package you want to update. <strong>Important</strong>: When you use the <code>relink</code> command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Horizon Workspace environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point relink to a copy of the folder of executables. Other use cases for the <code>relink</code> command, including enabling a ThinApp package for use in a Horizon Workspace environment, are covered in the VMware knowledge base article at <a href="http://kb.vmware.com/kb/2021928">http://kb.vmware.com/kb/2021928</a>.</td>
<td></td>
</tr>
</tbody>
</table>

You have a set of files (EXE files, and optionally DAT files) for the updated ThinApp package.

**What to do next**

Copy the files to a new subfolder on the network share, by completing the steps in “Copy an Updated ThinApp Package to the Network Share,” on page 129.

**Copy an Updated ThinApp Package to the Network Share**

After you create the updated ThinApp package, you copy the appropriate files to a new subfolder at the same level as the existing subfolder on the network share.

**Prerequisites**

Verify that you have the files for the updated ThinApp package, as a result of completing the steps in “Create the Updated ThinApp Package,” on page 127 and incrementing the VersionID value. Verify that you have access to the network share and can make subfolders and copy files to it.

**Procedure**

1. In the network share folder, create a new subfolder for the updated ThinApp package.

   Retain the existing subfolder for the ThinApp package that you are updating, and do not alter its contents.

   After the next scheduled sync, Horizon Workspace ignores the older package, when it recognizes the new package has the same AppID value and a higher VersionID value.
Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named appshare on a host named server, and the application is called abceditor, the subfolder for theThinApp package is \\server\appshare\abceditor.

**NOTE** Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Horizon Workspace. Non-ASCII characters are not supported.

2 Copy the EXE and DAT files for the updated ThinApp package into that new subfolder.

3 (Optional) If you do not want to wait for the next scheduled sync time, you can manually sync your Horizon Workspace system with the network share using the ThinApp Packages page of the Connector Web interface.

When Horizon Workspace performs the scheduled sync with the network share folder and it encounters an application that has the same AppID as another application, it compares the VersionID values. The ThinApp package with the highest VersionID is used as the most recent update. Horizon Workspace automatically incorporates the previous user entitlements to the ThinApp package with the highest VersionID, and shortcuts on the users’ systems are synced to point to the updated package.

### Delete ThinApp Packages from Horizon Workspace

You can permanently remove a ThinApp package from Horizon Workspace.

When you delete a ThinApp package from Horizon Workspace, you permanently remove it. You can no longer entitle users to the ThinApp package unless you add it back to Horizon Workspace.

**Procedure**

1 Delete the ThinApp package subfolder from the network file share that is the ThinApp package repository connected to your Horizon Workspace system.

2 Delete the application from Horizon Workspace.
   a Log in to the Administrator Web interface.
   b Click the Catalog tab.
   c Click Any Application Type > ThinApp Packages.
   d Search for the ThinApp package to delete.
   e Click the ThinApp package name to display its resource page.
   f Click Delete, read the message, and if you agree, click Yes.

The ThinApp package does not exist in your Horizon Workspace catalog.
Make Existing ThinApp Packages Compatible with Horizon Workspace

You can convert a ThinApp package from one that is not compatible with Horizon Workspace to one that Horizon Workspace can distribute and manage. You can use one of the following methods: use the ThinApp 4.7.2 relink command, rebuild the package from its ThinApp project files after editing the project's Package.ini file to add the necessary Horizon Workspace parameters, or recapture the Windows application with the appropriate Horizon Workspace settings selected in the ThinApp Setup Capture program.

**Note** A ThinApp package that is compatible with Horizon Workspace can only be used for a Horizon Workspace deployment. Only Horizon Workspace users who have the Horizon Workspace Client for Windows installed can launch and run these enabled packages. At runtime, the ThinApp package loads a specifically named DLL, and uses that DLL to verify the user's entitlement with their Horizon Workspace system. Because the DLL is installed with the Horizon Workspace Client for Windows, such ThinApp packages can only be run on Windows systems on which that client is installed.

**Prerequisites**

Verify that you have access to the necessary items for your chosen method.

- If you are using the relink command, verify that you have the executable files for the ThinApp package that you are converting and the ThinApp 4.7.2 relink.exe application.
- If you are updating the ThinApp project's Package.ini file and rebuilding the package, verify that you have the project files needed by the ThinApp 4.7.2 program to rebuild the package.
- If you are recapturing the Windows application, verify that you have the ThinApp 4.7.2 Setup Capture program and the application installer and other items that the program needs to recapture the application. See the ThinApp User's Guide for details.

Verify that you have access to the ThinApp network share used by your Horizon Workspace system, and can make subfolders and copy files to it.
**Procedure**

- Using a version of the ThinApp program that is supported by Horizon Workspace, create a compatible ThinApp package using one of the available methods.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use the relink -h command.</strong></td>
<td>Using the relink -h command is the easiest method. You must use the relink.exe program from ThinApp 4.7.2 or later. Use this method in one of the following situations:</td>
</tr>
<tr>
<td></td>
<td>- You cannot use the rebuild method because you do not have the project folder.</td>
</tr>
<tr>
<td></td>
<td>- Using Setup Capture to recapture the application would take too long.</td>
</tr>
<tr>
<td></td>
<td>- You do not have the application installer that is required for recapturing with Setup Capture.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The ThinApp runtime is always updated when you run the relink -h command on a ThinApp package.</td>
</tr>
<tr>
<td></td>
<td>You can run the relink command from the ThinApp Program Files directory to get help on the command’s syntax.</td>
</tr>
<tr>
<td></td>
<td>To create a compatible package, use the basic syntax of the command:</td>
</tr>
<tr>
<td></td>
<td>relink -h executable-*.*</td>
</tr>
<tr>
<td></td>
<td>Where executable-*.* is a folder containing the executables of the ThinApp package you want to update.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>When you use the relink command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Horizon Workspace environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point relink to a copy of the folder of executables.</td>
</tr>
<tr>
<td></td>
<td>Other use cases for the relink command are covered in the VMware knowledge base article at <a href="http://kb.vmware.com/kb/2021928">http://kb.vmware.com/kb/2021928</a>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Update the Package.ini file manually with the necessary Horizon Workspace parameters, and then rebuild the package.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this method when you do not have the application installer for the recapture process, when you want to avoid doing the up-front setup that recapturing the application requires, or when you want to incorporate functionality from a newer ThinApp version more than what the relink command would provide. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new Package.ini parameter that you want to set.</td>
</tr>
<tr>
<td>In the [Build Options] section of the Package.ini file, add the following parameters:</td>
</tr>
<tr>
<td>;--------- Horizon Parameters ---------------</td>
</tr>
<tr>
<td>AppID=genid</td>
</tr>
<tr>
<td>NotificationDLLs=HorizonPlugin.dll</td>
</tr>
<tr>
<td>HorizonPlugin.dll is the DLL that the ThinApp runtime calls to verify the Horizon Workspace user’s entitlement to use the virtualized application.</td>
</tr>
<tr>
<td>You can optionally include the HorizonOrgURL parameter and set it to your Horizon Workspace fully qualified domain name (HorizonWorkspaceFQDN). See Installing and Configuring Horizon Workspace.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recapture using Setup Capture, and select the necessary Horizon Workspace settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this method when you would prefer to recapture the application rather than use one of the other methods. To create a compatible package using ThinApp Setup Capture, select the appropriate settings in the wizard to manage the package with Horizon Workspace during the capture process. See the ThinApp User’s Guide for details on the capture process.</td>
</tr>
</tbody>
</table>

You have a set of files (EXE files, and optionally DAT files) for a ThinApp package that Horizon Workspace can distribute and manage.
What to do next

Add the ThinApp package to the repository that your Horizon Workspace system uses, by completing the steps in “Add ThinApp Packages to the Network Share,” on page 133.

Add ThinApp Packages to the Network Share

To make ThinApp packages available for your Horizon Workspace to distribute them, you add the packages to the ThinApp packages repository that is integrated with your Horizon Workspace system. This repository is a network share that is connected to your Horizon Workspace server.

Prerequisites

Verify that your Horizon Workspace system is integrated with your ThinApp packages repository, according to the steps in Installing and Configuring Horizon Workspace.

Verify that you have access to the network share and can make subfolders and copy files to it.

Verify that the ThinApp packages are compatible with Horizon Workspace, and you have all of the EXE and DAT files for the packages.

Procedure

1. In the network share, create a network share subfolder for each ThinApp package.

   Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named appshare on a host named server, and the application is called abceditor, the subfolder for the ThinApp package is `\server\appshare\abceditor`.

   **Note** Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Horizon Workspace. Non-ASCII characters are not supported.

2. For each ThinApp package, copy its files, such as its EXE and DAT files, to the subfolder that is named for that package's virtualized application.

   After copying the files, you have a set of subfolders and files that are similar to these files:

   - `\server\appshare\abceditor\abceditor.exe`
   - `\server\appshare\abceditor\abceditor.dat`

3. (Optional) If you do not want to wait for the next scheduled sync time, you can manually sync your Horizon Workspace system with the network share using the ThinApp Packages page of the Connector Web interface.

   The ThinApp packages are available for your Horizon Workspace server to distribute and manage.
Horizon Workspace generates several reports, such as reports about users, resources, and audit events. You can view the reports in the **Reports** tab of the Administrator Web interface.

You can use Horizon Workspace to generate several reports.

**Table 17-1. Horizon Workspace Report Types**

<table>
<thead>
<tr>
<th>Horizon Workspace Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Usage</td>
<td>This report lists all your resources with respective details for each resource, such as number of users and licenses.</td>
</tr>
<tr>
<td>Resource Entitlements</td>
<td>This report lists the user entitlements for a resource you specify.</td>
</tr>
<tr>
<td>Group Membership</td>
<td>This report list the members of a group you specify.</td>
</tr>
<tr>
<td>Users</td>
<td>This report lists all your Horizon Workspace users, and provides details about each user, such as the user’s email address, role, and group affiliations.</td>
</tr>
<tr>
<td>Horizon Files Usage</td>
<td>This report lists all of the users entitled to use the features of the Horizon Workspace file-sharing service, with details provided for each account, such as quota allotted, percent of quota used, and the assigned data-va instance. The information for the Horizon Files Usage report is sent from the data-va instances approximately every hour. When viewing the Horizon Files Usage report, account for the discrepancies that might be caused by the hourly update schedule. <strong>Note</strong> At times when the auditing subsystem is restarting, the Horizon Files Usage page might display an error message and not render the report. If you see such an error message about not rendering the report, wait a few minutes and then try again.</td>
</tr>
<tr>
<td>Audit events</td>
<td>This report lists the audit events related to a search you specify, such as user logins for the past 30 days. This feature is useful for troubleshooting purposes. See “Generate an Audit Event Report,” on page 135.</td>
</tr>
</tbody>
</table>

**Generate an Audit Event Report**

You can generate a report of audit events that you specify.

Audit event reports can be useful as a method of troubleshooting.

**Prerequisites**

Enable auditing. See “Overview of Horizon Workspace Administrative Settings,” on page 137.

**Procedure**

1. Log in to the Administrator Web interface.
2. Select **Reports > Audit events**
3 Select audit event criteria.

<table>
<thead>
<tr>
<th>Audit Event Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>This text box allows you to narrow the search of audit events to those generated by a specific user.</td>
</tr>
<tr>
<td>Type</td>
<td>This drop-down list allows you to narrow the search of audit events to a specific audit event type. The drop-down list does not display all potential audit event types. The list only displays event types that have occurred in your Horizon Workspace deployment. Audit event types that are listed with all uppercase letters are access events, such as LOGIN and LAUNCH, which do not generate changes in the database. Other audit event types generate changes in the database.</td>
</tr>
<tr>
<td>Action</td>
<td>This drop-down list allows you to narrow your search to specific actions. The list displays events that make specific changes to the database. If you select an access event in the Type drop-down list, which signifies a non-action event, do not specify an action in the Action drop-down list.</td>
</tr>
<tr>
<td>Object</td>
<td>This text box allows you to narrow the search to a specific object. Examples of objects are groups, users, and devices. Objects are identified by a name or an ID number.</td>
</tr>
<tr>
<td>Date range</td>
<td>These text boxes allow you to narrow your search to a date range in the format of &quot;From ___ days ago to ___ days ago.&quot; The maximum date range is 30 days. For example, from 90 days ago to 60 days ago is a valid range while 90 days ago to 45 days ago is an invalid range because it exceeds the 30 day maximum.</td>
</tr>
</tbody>
</table>

4 Click Show.

An audit event report appears according to the criteria you specified.

**Note**: At times when the auditing subsystem is restarting, the Audit Events page might display an error message and not render the report. If you see such an error message about not rendering the report, wait a few minutes and then try again.

5 For more information about an audit event, click View Details for that audit event.
After you install Horizon Workspace and perform the initial configuration, you can configure several administrative settings.

This chapter includes the following topics:

- “Overview of Horizon Workspace Administrative Settings,” on page 137
- “Customize Horizon Workspace Branding,” on page 138
- “Use hznAdminTool Commands to Make Changes to Your Horizon Workspace System,” on page 140

## Overview of Horizon Workspace Administrative Settings

You can configure several Horizon Workspace administrative settings.

You access the administrative settings using the Administrator Web interface.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Configuration</td>
<td>Select <strong>Settings &gt; VA Configuration</strong> to access the Configurator Web interface. The Configurator Web interface allows you to use a Web interface to edit the underlying Configurator virtual appliance. You can perform actions such as the following from the Configurator Web interface: View system information. Change the database from internal to external. Configure an SSL certificate for external access to Horizon Workspace. Enable modules: Horizon Files, Web Applications, Mobile Management, View, ThinApp Packages, and Citrix Published Applications. Enter a new license key. Change the admin user password for the service-va, configurator-va, and connector-va. View a list of the log file locations. On the VA Configuration page, click <strong>View Virtual Appliance System Configuration</strong> to load the login page of the Configurator Web interface in your browser.</td>
</tr>
<tr>
<td>Password Recovery</td>
<td>Select <strong>Settings &gt; Password Recovery</strong> to configure the behavior of user password recovery. This setting allows you to configure the behavior of the Forgot password link on the user log in page.</td>
</tr>
<tr>
<td>User Stores</td>
<td>Select <strong>Settings &gt; User Stores</strong> to configure user stores, which are required when you configure Horizon Workspace in a multi-forest Active Directory environment. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16.</td>
</tr>
<tr>
<td>Network Ranges</td>
<td>Select <strong>Settings &gt; Network Ranges</strong> to configure network ranges for your organization, so that you can associate IP address ranges with identity provider instances. See “Add or Edit a Network Range,” on page 21.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>Select <strong>Settings &gt; Authentication Methods</strong> to configure the default authentication methods or to add authentication methods not supported by Horizon Workspace directly, but supported indirectly through third-party identity providers. See “Add or Edit a User Authentication Method,” on page 22.</td>
</tr>
</tbody>
</table>
## Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Identity Providers       | Select **Settings > Identity Providers** to edit an existing or to add a new identity provider instance, either a Connector instance or a third-party identity provider instance.  
  The initial installation of Horizon Workspace includes a single Connector instance as the default identity provider deployment. Edit the initial Connector instance as necessary, such as by selecting authentication methods and adding network address ranges.  
  Add additional identity provider instances to your Horizon Workspace deployment for high availability purposes. Also, when Horizon Workspace is deployed in a multi-forest Active Directory environment, add an additional identity provider instance for each user store you plan to add to your deployment.  
  When the Identity Providers page lists more than one identity provider instance, you can edit the order of the instances. The order is important when IP addresses are assigned to multiple identity provider instances.  
  See “Add and Configure an Identity Provider Instance,” on page 23 for details about adding or editing identity provider instances and about editing the order of identity provider instances. |
| Remote App Access        | Select **Settings > Remote App Access** to create clients or templates that enable applications to register with Horizon Workspace. |
| SAML Certificate         | Select **Settings > SAML Certificate** to view the SAML-signing certificate. If a Web application requires the use of SAML assertions to authenticate users, both Horizon Workspace and the Web application must have copies available locally of the same SAML-signing certificate. |
| Approvals                | Select **Settings > Approvals** to enable or disable license approval. Enabling license approval applies when you integrate your license-management system with Horizon Workspace. |
| Auditing                 | Select **Settings > Auditing** to enable or disable the collection of information for the audit events report, which is accessible on the **Reports** tab. |
| Citrix Published Application | Select **Settings > Citrix Published Application** to edit the Horizon Workspace global application delivery settings for Citrix-based applications available in the Horizon Workspace catalog. See “Edit the Horizon Workspace Application Delivery Settings Globally for All Citrix-Based Applications,” on page 113. You can configure settings such as application streaming and application security.  
  For instructions about editing the settings for a single Citrix-based application, see “Edit the Horizon Workspace Application Delivery Settings for a Single Citrix-Based Application,” on page 114. |
| Custom Branding          | Select **Settings > Custom Branding** to customize the branding on Horizon Workspace interfaces. See “Customize Horizon Workspace Branding,” on page 138. |

### Customize Horizon Workspace Branding

You can customize the logos, fonts, Web clips, and background that appear in various interfaces, such as the Administrator Web interface, the user and administrator login screens, and the user portal.

You can customize the branding used in the user portal and the Administrator Web interface.

**Procedure**

1. Log in to the Horizon Workspace Administrator Web interface.
2. Select **Settings > Custom Branding**.
3 Edit the settings in the form as appropriate.

Table 18-1. Custom Branding Configuration

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Brand Names and Logos</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Logo                  | The Logo option allows you to change the logo that appears in the following locations:  
                          - The administrator and user login pages.  
                          - The user portal.  
                          - The Administrator Web interface.  
                          - The mobile workspace, applicable to VMware Horizon Workspace Switch.  
                          Click **Change** to upload a new image to replace the current logo. You are prompted to confirm the change. If you click **Confirm**, the change occurs immediately. |
| Favicon               | The Favicon option allows you to change the favicon used in Web browsers. This option applies to both desktops and mobile devices.  
                          Click **Change** to upload a new image to replace the current favicon. You are prompted to confirm the change. If you click **Confirm**, the change occurs immediately. |
| Company Name          | The Company Name option applies to both desktops and mobile devices. This option allows you to change the company name that appears in the Web browser page title before the product name.  
                          Type a new company name over the existing one to change the name.                                                                 |
| Product Name          | The Product Name option applies to both desktops and mobile devices. This option allows you to change the name that appears in the Web browser page title after the company name.  
                          Type a product company name over the existing one to change the name.                                                                 |
| **User Portal Color and Background** |                                                                                                                                             |
| Apps Font Color       | The color of the font that Horizon Workspace uses for resource names in the user portal. The name of the resource is located directly under the icon of the resource.  
                          Type a new hexadecimal color code over the existing one to change the font color. The App Name text in the user portal preview changes when you type in a new color code to demonstrate how the text will appear in the user portal. |
| Background Color      | The color that Horizon Workspace displays for the background of the user portal and in log in screens.  
                          Type a new hexadecimal color code over the existing one to change the background color. To demonstrate how the background color will appear in the user portal, the background color changes in the user portal preview when you type in a new color code. However, if the **include background image** checkbox is selected, the background color might not be visible in the preview. |
| Background image      | The background image that Horizon Workspace displays in the user portal and in login screens when the **Include background image** checkbox is selected.  
                          1 If not selected, click the **Include background image** checkbox to display the background image in the user portal.  
                          2 Click **Change** to upload a new image to replace the current background or, if available, click **Use Default** to replace the current background with the default background. |
| **Mobile Devices**     |                                                                                                                                             |
| Web Clip Icon         | The Horizon Workspace icon, whose appearance is triggered by users when they save the Horizon Workspace User Portal URL as a bookmark to their home screens. This Web clip icon launches the Horizon Workspace User Portal.  
                          Click **Change** to upload a new image to replace the current Web clip icon. You are prompted to confirm the change. If you click **Confirm**, the change occurs immediately. |
| Web Clip Title        | The title that accompanies the Horizon Workspace Web clip icon.                                                                             |

4 Click **Save**.
Horizon Workspace applies the branding changes to the appropriate interfaces.

**What to do next**
Check the appearance of the branding changes in the various interfaces.

**Use hznAdminTool Commands to Make Changes to Your Horizon Workspace System**

When you need to update settings related to the vCenter instance or SMTP system configured for your Horizon Workspace system, or to reset the password for the admin user that is used to log in to the Configurator Web interface, use the hznAdminTool command in the configurator-va virtual appliance interface.

**Prerequisites**
Verify that you can log in to the configurator-va virtual appliance interface, either directly using the vSphere client and the root account and password, or remotely using ssh and the sshuser account and password. The password for the root account is set during installation when you configure basic Horizon Workspace settings using the configurator-va virtual appliance interface. See *Installing and Configuring Horizon Workspace.*

**Procedure**

1. Log in to the configurator-va virtual machine using the configurator-va virtual appliance interface.
2. Enter the hznAdminTool with the appropriate option for the configuration setting that you want to update.

To see a list of all editable properties for the hznAdminTool editproperty command, run `hznAdminTool editproperty -- list`. To set an editable property, run `hznAdminTool editproperty -- set=property: value`, where property is the property and value is the value you want to set.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hznAdminTool resetpasswd</td>
<td>Run this command to set the password for the default administrator account, named admin, that is typically used to log in to the Connector Web interface.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=vim_host:your_vCenter_host</td>
<td>Run this command to set the address for the vCenter instance associated with this Horizon Workspace system.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=vim_port:your_vCenter_port</td>
<td>Run this command to set the port number for the vCenter instance that is associated with this Horizon Workspace system.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=vim_username:username</td>
<td>Run this command to configure your Horizon Workspace system with the name used for the associated vCenter instance's administrator account.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=vim_password:password</td>
<td>Run this command to configure your Horizon Workspace system with the password used for the associated vCenter instance's administrator account.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=smtp_host:your_smtp_host</td>
<td>Run this command to set the address for the SMTP server associated with this Horizon Workspace system.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=smtp_port:your_smtp_port</td>
<td>Run this command to set the port for the associated SMTP server.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=smtp_username:username</td>
<td>Run this command to configure your Horizon Workspace system with the username that is used to access the SMTP server to send email messages. The Horizon Workspace file-sharing service sends email using the configured SMTP server when a user shares a folder or file with another user. Set this SMTP username when your SMTP server requires credentials to access it so that the file-sharing service can send emails.</td>
</tr>
<tr>
<td>hznAdminTool editproperty -- set=smtp_password:password</td>
<td>Run this command to configure your Horizon Workspace system with the password for the username that is used to access the SMTP server to send email messages.</td>
</tr>
</tbody>
</table>
Apply the changes to your Horizon Workspace system by running the `configurator-tc restart` command to restart the configurator-va's Tomcat server.

After the Tomcat server restarts, your changes go into effect.
You can troubleshoot issues that you or your Horizon Workspace users might experience after you install and configure Horizon Workspace.

This chapter includes the following topics:

- “Mobile Device Users Cannot Authenticate to Your Horizon Workspace System,” on page 143
- “File Preview in the Horizon Workspace User Portal Displays Server Error and No Errors in the Server Logs,” on page 145
- “Files With Names That Contain Invalid XML Characters Fail to Sync With the Horizon Workspace Application on Windows or Mac Systems,” on page 145
- “Sharing Folders or Files from the Horizon Workspace for iOS, First Edition App Fails With Error About Email,” on page 146
- “Blank Screen Displays When Installing Update to Horizon Workspace for Windows,” on page 147
- “ThinApp Packages Fail to Launch from the User Portal,” on page 148
- “A User Login Attempt Results in a Timeout Error,” on page 150
- “Horizon Workspace Desktop Client Stops Responding With Unexpected Server Error During Indexing,” on page 150

### Mobile Device Users Cannot Authenticate to Your Horizon Workspace System

The Secure Sockets Layer (SSL) protocol protects communications to your Horizon Workspace system and to any third-party identity providers you might have configured for that system. If your Horizon Workspace deployment is configured to use certificates signed by a private, untrusted Certificate Authority (CA), either for the Horizon Workspace server, the vApp, or for any configured identity providers and users cannot log in from their mobile devices or see a message about an untrusted certificate, you might need to install the certificates on those mobile devices that are used with your Horizon Workspace system to establish trust between Horizon Workspace and those devices.

During the initial configuration of Horizon Workspace, the Configurator randomly generates a private, untrusted Horizon Workspace root CA certificate.

For production deployments, you typically replace the private, untrusted certificates used for your Horizon Workspace system and all associated identity provider instances with certificates signed by a trusted Certificate Authority (CA). Because the operating systems on mobile devices typically include a root store that includes root CA certificates from the standard industry trusted CAs, if the Horizon Workspace
system and the associated identity providers use certificates signed by a trusted CA, you do not need to take special steps to install those certificates on the mobile devices. However, in proof-of-concept deployments, or if you are using certificates that are not signed by a trusted CA, the mobile devices might need to have the certificates installed to them before they can establish trust with your Horizon Workspace server.

**NOTE** If you have a load balancer using an SSL certificate signed by a root CA that is not trusted, the root CA certificate must be installed on the mobile devices that communicate with that load balancer.

Mobile devices can obtain root CA certificates in a variety of ways, for example, by opening a browser on the device to the location of the certificate file on a Web site or by opening an email message with the certificate file as an attachment. The following steps describe one method. Use a method that is appropriate for your organization's needs.

**Procedure**

1. **Install the Horizon Workspace system's root CA certificate on a mobile device.**

   One way to install the Horizon Workspace system's root CA certificate on a mobile device is to use a browser on the device to browse to the location for the root CA file on the Horizon Workspace FQDN server, and follow the prompts on the device to install the certificate on the device.

   a. On the mobile device, launch a browser and go to `http://HorizonWorkspaceFQDN/horizon_workspace_rootca.pem`.

   A message appears that indicates the identity cannot be verified or that the certificate is untrusted. You can view the certificate information to verify that it was issued by Horizon Workspace.

   b. Depending on the displayed options, install the certificate by clicking **Continue** or **Install**.

   The Horizon Workspace root CA certificate is added to the set of trusted certificates on the device.

2. **If you have configured identity providers for your Horizon Workspace system and those identity providers use SSL certificates that are not signed by a trusted root CA, install the providers' root CA certificates on the mobile device.**

   One way to install the identity provider's root CA certificate on a mobile device is to obtain the file from the identity provider and make the file available from a Web page in your organization's network that your mobile device users can access.

   a. Obtain the file for the identity provider's root CA certificate.

   b. Make the file available from a Web page in your organization's network.

   c. Send the Web page location to the mobile device user.

   d. On the mobile device, launch a browser and go to the Web page location.

   e. Touch the link for the file.

   A message appears that indicates the identity cannot be verified or that the certificate is untrusted. You can view the certificate information to verify that it was issued by the appropriate identity provider.

   f. Depending on the displayed options, install the certificate by clicking **Continue** or **Install**.

   That identity provider's root CA certificate is added to the set of trusted certificates on the device.

   g. Repeat the steps for all of the identity providers that are configured for your Horizon Workspace system and which use untrusted SSL certificates.
File Preview in the Horizon Workspace User Portal Displays Server Error and No Errors in the Server Logs

In the Horizon Workspace user portal, an HTTP error 500 appears when the user tries to preview a file. No related errors are written to the Horizon Workspace logs.

Problem

When you click a file in the Horizon Workspace user portal, the preview of the file does not appear in the preview pane. Instead, the following message appears:

HTTP ERROR 500 Server Error

When you check the log files, no errors are logged.

Cause

This problem can occur when your Horizon Workspace system has the Microsoft Windows Preview configured, and you have an activation error with your Microsoft Office installation. For example, if the associated Microsoft Windows Server cannot reach its activation server, it can become deactivated and this problem occurs.

Solution

1. Verify that your Microsoft Office installation is active.
2. If your Microsoft Office installation is deactivated, activate it according to the standard Microsoft documentation and your deployment environment.

Files With Names That Contain Invalid XML Characters Fail to Sync With the Horizon Workspace Application on Windows or Mac Systems

When a file's name contains characters that are not valid XML characters, and you are using Horizon Workspace for Windows or Horizon Workspace for Mac, the file fails to sync with the server. The user sees a message about having an incompatible server.

Problem

On a Windows or Mac system, the user sees a message from the installed Horizon Workspace application that says Incompatible Server - This version of Horizon client is not compatible with the Horizon server, and the files do not sync. The diagnostic information from the client shows that the server threw an unmarshal exception because an invalid character is found in the file name.

Cause

On Windows and Mac systems, the Horizon Workspace application uses XML to communicate with the Horizon Workspace server. If file names contain characters that are not valid XML characters, the files do not sync and an error message appears.

Invalid characters that can cause this problem include control characters, such as Ctrl plus a letter. A common situation is introducing the backspace character to a file name. The backspace character is CONTROL-H, Ctrl-H, ^H, or \\010. Users accidentally introduce the Ctrl-H character to the file names when they use the backspace during a file naming operation and their terminal is incorrectly configured. Other examples of control characters that are often introduced to file names are ^B, ^M, and ^]. The user can accidentally introduce the ^M combination to a file name when they use the FTP command to move the file from Windows to a Mac system.
Introduction of control characters to file names tends to happen more frequently to users who work in the terminal on Mac systems. On a Mac system, a user can check whether the files contain control characters in their names by opening the terminal and using the `ls -B` command in the Horizon Workspace directory that their client uses. The `ls -B` command lists the files and shows where invisible characters are present in the file names.

**Solution**

1. Generate the diagnostic logs from the installed Horizon Workspace application.
   a. Click the Horizon icon on the system tray or menu bar.
   b. Click Options.
   c. Click Collect diagnostic information.

   When the collection is ready, a message appears with the location of the ZIP file.

2. Extract the log file for Horizon Workspace from the ZIP file, and open the log file in a text editor.

3. Search for the line that contains `UnmarshalException`.

4. After that line, locate a line further down in the log file that contains `Protocol error. Client and server may be incompatible`.

   The line that contains the text `Protocol error. Client and server may be incompatible` contains the name of the file that contains invalid XML characters.

5. Locate that file in the Horizon folder and rename it.

6. Continue searching for lines in the log file that contain `UnmarshalException` and `Protocol error. Client and server may be incompatible` to identify all files that might contain invalid XML characters in their names. Rename the files as necessary to remove the invalid characters.

**Sharing Folders or Files from the Horizon Workspace for iOS, First Edition App Fails With Error About Email**

When a user has the VMware Horizon Workspace for iOS, First Edition app installed on an iOS device, sets up that client with a URL for a Horizon Workspace system of version 1.5 or higher, and tries to use the feature for sharing folders and files, an error appears and the folder or file is not shared.

**Problem**

When they are trying to share a folder or file, the user sees an error message that states `EMail could not be sent. Error 715 services.UNKNOWN_DOCUMENT`.

**Cause**

This problem occurs when the user installs the Horizon Workspace for iOS, First Edition app and sets it up using the URL for a Horizon Workspace system of version 1.5 or higher. Use of the Horizon Workspace for iOS, First Edition app with a Horizon Workspace system at a higher version level is not supported, even though some features in the iOS app might appear to work.

**Solution**

- Uninstall the Horizon Workspace for iOS, First Edition App and install the Horizon Workspace iOS app that is compatible with your Horizon Workspace system version level.
Blank Screen Displays When Installing Update to Horizon Workspace for Windows

When you have the Horizon Workspace for Windows application already installed, and then you download a more recent version, and start to install it, a blank screen displays.

**Problem**

When you already have the Horizon Workspace for Windows application installed, and you start the installer for a more recent version, sometimes a blank screen displays and you cannot complete the installation.

When you look at the log files for the installer, you see lines at the end of file similar to the following lines:

- `20130918112739:INFO CBootstrapCmd::LuaUIShow: calling StartSequence('reboot_prompt')`
- `20130918112739:INFO CHtmlUI::StartSequence: About to Run UI Sequence reboot_prompt 00000120 01F386F8 1`
- `20130918112739:INFO CHtmlUI::StartSequence: Running UI Sequence reboot_prompt`
- `20130918112739:ERROR CHtmlDialog::CallJScript: Failed to obtain required required jscript ID; COM Error: -2147352570`

**Cause**

This problem can occur if one or more registry key settings are incorrect. For descriptions of similar symptoms and other potential solution steps, see the VMware knowledge base article at [http://kb.vmware.com/kb/1027986](http://kb.vmware.com/kb/1027986) and the Microsoft Knowledge Base article 831430 at [http://support.microsoft.com/kb/831430](http://support.microsoft.com/kb/831430).

**Solution**

1. Reboot the Windows system, and then try running the installer again.
   
   If rebooting the system does not resolve the problem, continue with the next step.

2. Re-register the jscript.dll and vbscript.dll files.
   
   a. Open a command prompt on the Windows system.
   
   b. Run the following commands to re-register the necessary files and details.
      
      If the system is a 32-bit version of Windows, run these commands:
      ```
      regsvr32 jscript.dll
      regsvr32 vbscript.dll
      ```
      
      If the system is a 64-bit version of Windows, run these commands:
      ```
      cd C:\windows\syswow64
      regsvr32 C:\windows\system32\jscript.dll
      regsvr32 C:\windows\system32\vbscript.dll
      ```

ThinApp Packages Fail to Launch from the User Portal

When a user tries to launch a ThinApp package from the user portal, a browser message might appear that prompts the user to download and install Horizon Workspace for Windows even when the application is already installed and running.

Problem

After installing Horizon Workspace for Windows, when the user opens the user portal in a browser on that Windows system, logs in, and tries to launch a ThinApp package, a message might appear stating that Horizon Workspace for Windows must be installed on the system, and prevents the ThinApp package from starting. This message might appear even when the Horizon Workspace process is running on the Windows system. The Horizon Workspace for Windows client might report that all files are up to date.

Cause

This problem can occur for multiple reasons.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VMware Horizon Agent Finder browser plugin is not properly installed or it is not activated in the browser window for the browser in which the user is trying to launch the ThinApp package.</td>
<td>Because installation of the Horizon Workspace for Windows application is required to run ThinApp packages on the Windows system, the user portal uses a browser plugin to verify whether the application is installed before launching the ThinApp package from the user portal. When the user clicks the icon for a ThinApp package in the user portal, the VMware Horizon Agent Finder browser plugin checks to see if the application is installed before launching the package. If the browser plugin is not installed and active in the browser, the verification cannot happen, the message appears, and the package does not launch. If there are browser windows open during the Horizon Workspace for Windows installation process, the VMware Horizon Agent Finder browser plugin might not be properly installed for that browser. The browser plugin might become deactivated in the browser if the user disabled the plugin in the browser's add-ons or plug-ins page.</td>
</tr>
<tr>
<td>The custom protocol handler used to launch the ThinApp package from the browser has been disabled for the browser in which the user is trying to launch the ThinApp package.</td>
<td>On the My Apps page in the user portal, ThinApp packages are represented using a link with a horizon:// protocol. When the Horizon Workspace for Windows client is installed, the installer registers a protocol handler for that horizon:// protocol. The protocol handler is an executable named HorizonThinAppLauncher.exe, and is registered as a handler by the registry entry HKEY_CLASSES_ROOT\horizon\shell\open\command. When the user tries to launch a ThinApp package from its icon in My Apps, this HorizonThinAppLauncher.exe application is launched. If the user has disabled the use of all protocol handlers in the browser, or disabled the use of the handler for the horizon:// protocol, ThinApp packages will not launch using their icons in the My Apps page. Some browsers present a warning when protocol handlers are launched and give the user the option to select to execute the protocol handler. One way in which the user might have disabled the use of the horizon:// protocol handler is when the user clicked one of the ThinApp package icons for the first time, when the browser warning dialog appeared to ask for permission to run the protocol handler, the user selected No or a similar choice to prevent the launch, and also selected Remember my selection or a similar choice that prevents the launch for all such links. Because permission to run the protocol handler was not given and is remembered, none of the ThinApp packages launch from the My Apps page.</td>
</tr>
</tbody>
</table>

Solution

1. Verify the user has signed into the Horizon Workspace for Windows client with the user’s Horizon Workspace user account.
   
   The user signs into the client using the Horizon Workspace icon in the Windows system tray.

2. If this problem appears shortly after the application is installed on the system, close all open browser windows, reopen the browser, log in to the user portal, and try launching the ThinApp package.
If the problem appears even after closing the open browser windows and reopening the browser, verify the VMware Horizon Agent Finder browser plugin appears in the browser's list of plugins, and is active.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>For Internet Explorer, a COM server is registered instead of a browser plugin or add-on. To test whether the COM server is installed, create a test HTML file with the following contents and open that file in Internet Explorer. The result tells whether the COM server is installed or not.</td>
</tr>
</tbody>
</table>
|               | `<html>`
|               | `<script type="text/vbscript">` On Error Resume Next
|               |   `dim objName` `objName = "HorizonAgentFinder.HorizonFinder"` `dim obj` `Set obj = CreateObject(objName)`
|               |   `document.write(objName & " is ")` `if IsEmpty(obj) then` `document.write("not installed")` `else` `document.write("installed")` `end if` `</script>` `</html>` |
| Firefox       | Open Firefox's Add-ons Manager by clicking **Tools > Add-ons**. On the Plugins page, verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate. |
| Chrome        | Open Chrome's content settings by opening the Settings page and clicking **Show advanced settings > Content settings**. Click **Disable individual plug-ins** to display the list of plugins. Verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate. |
| Safari for Windows | Open Safari's list of installed plugins by clicking **Help > Installed Plug-ins**. Verify the VMware Horizon Agent Finder browser plugin is listed. Verify that plugin is activated for Safari. |

Verify the registry entry `HKEY_CLASSES_ROOT\horizon\shell\open\command` exists and has a value that is a path that points to the location of the required protocol handler, named `HorizonThinAppLauncher.exe`, where Horizon Workspace for Windows was installed on the Windows system.

If the registry entry does not exist, or does not have a value that points to the location where Horizon Workspace for Windows was installed, uninstall Horizon Workspace for Windows and reinstall it.

If the registry entry exists and has a value that points to the location of the `HorizonThinAppLauncher.exe` executable, verify the executable exists at that location and has not been moved or deleted.

If the registry entry does not exist, or does not have a value that points to the location where Horizon Workspace for Windows was installed, uninstall Horizon Workspace for Windows and reinstall it.

If the registry entry exists and has a value that points to the location of the `HorizonThinAppLauncher.exe` executable, verify that the (Default) value for the registry entry `HKEY_CLASSES_ROOT\horizon` has a Data value of `URL:horizon Protocol` and that the URL Protocol value for the `HKEY_CLASSES_ROOT\horizon` entry exists.

If the Data value for the (Default) value of the `HKEY_CLASSES_ROOT\horizon` registry entry is not set to `URL:horizon Protocol`, update the Data value to set it to `URL:horizon Protocol`. If the URL Protocol value does not exist for the `HKEY_CLASSES_ROOT\horizon` entry, you can create it using a value name `URL Protocol` and no value data.
Determine if the user disabled the horizon:// protocol for the browser, or if all protocol handlers are disabled in the browser, and if so, enable the protocol handler for the browser as appropriate for your organization’s needs.

In most situations, the browsers rely on the settings in the registry for information about the protocol handlers available for that Windows system. For some browsers, when the user clicks a link that is associated with a protocol handler, a dialog prompt appears that asks the user a question such as Do you want to allow this website to open a program on your computer? or This link needs to be opened with an application or a similar statement about needing to launch an external application to handle the link. Typically, the dialog provides the user with the option of not launching the external application and to remember that choice for all links of that type. The steps to re-enable the ability to launch the application associated with the protocol handler are usually different depending on the browser type. Consult the documentation for the user’s type of browser on how to enable protocol handlers for that browser type.

A User Login Attempt Results in a Timeout Error

The gateway timeout limit might be insufficient for your deployment.

Problem
A user attempting to log in to Horizon Workspace receives a 502 Gateway timeout error.

Cause
A situation where user authentication takes longer than allowed by the default timeout limit. For example, the user exists in another Active Directory forest or domain that is not part of the identity provider instance’s base DN.

Solution
1. Log in to the gateway-va virtual machine as root.
2. Open the /opt/vmware/ngix/conf/proxy-timeout.conf file.
   The file has two attributes. The default value for both attributes is 2m, for two minutes.
3. Increase both values according to your Active Directory deployment structure.

   NOTE When you upgrade Horizon Workspace, changes that were made to the proxy-timeout.conf file are carried forward to the update release.

Horizon Workspace Desktop Client Stops Responding With Unexpected Server Error During Indexing

The Horizon Workspace desktop client stops responding and exits with an error message that states Horizon Workspace encountered an unexpected server error during indexing. Restarting the desktop client, or uninstalling and reinstalling the client has no effect.

Problem
The user’s desktop client appears to be in a prolonged state of sync, and then the client exits and the following error messages appears:

Horizon Workspace encountered an unexpected server error during indexing. Please contact your Horizon administrator.
Cause

This problem can occur when your Horizon Workspace server gets into a state where it is reporting multiple stack overflows when the client is syncing the user's files or folders. The client stops syncing and exits with the error message. Typically, the stack overflows occur when syncing a particular folder.

To resolve the stack overflows occurring on the server, you must clear the flags column for the user’s items for which the stack overflows occurred. The flags column is located in a database table in the embedded database used for the file-sharing service. When the server’s stack overflows for this user are cleared, the client can sync normally.

Solution

Prerequisites

- Verify that you can log in to the data-va virtual machine’s command-line interface either using the data-va virtual machine's console in the vSphere Client and the root user and the root user’s password or using ssh and the sshuser account and the sshuser account’s password. You must be able to perform command-line operations in the data-va virtual machine's filesystem.

  For the steps on how to connect to the data-va using ssh, see the VMware knowledge base article at http://kb.vmware.com/kb/2061672.

  To set a password for the sshuser account on the data-va if the password has not been previously set, log in to the data-va as the root user using the vSphere client and the data-va virtual machine’s console. Run the command `passwd sshuser` to set the password.

- Obtain the user’s email address that is used in the user’s Horizon Workspace account for the user who is experiencing the problem. One way to obtain the appropriate email address is to view the user’s information using the Administrator Web interface. See “View Horizon Workspace User Information,” on page 43.

- Enable debug logging for the Horizon Workspace desktop client that is having the syncing problem. See “Enable Debug Logging for the Horizon Workspace Desktop Client,” on page 153.

- Obtain the log files from the user after debug logging was enabled and the sync issue occurs again.
Procedure

1. From the user's log files, obtain the UUID of the item for which the stack overflow error first appears in the log.
   a. Search the log file for a line that contains `java.lang.StackOverflowError`.

      2014-Mar-31 22:11:01.411051 25685277246 ERROR 48643 0x1025b9d30 sync:connection
daemon/http/HttpConnectionPool.cpp:65 <?xml version="1.0" encoding="UTF-8"
standalone="yes"?><error><cause>java.lang.StackOverflowError

   b. Above the line that contains `java.lang.StackOverflowError`, locate a line that contains HTTP Error: 500.

      2014-Mar-31 22:11:01.410938 25685277133 ERROR 48643 0x1025b9d30 sync:connection
daemon/http/HttpConnectionPool.cpp:788 HTTP Error: 500

   c. Above the line containing HTTP Error: 500 is a line that contains the words DEBUG and Processing and ends with the item's UUID.

      2014-Mar-31 22:11:01.030374 25684896570 DEBUG 48643 0x1025b9d30
octopus:remote_change_detector daemon/remote_change_detector.cpp:690 Processing
child item 23705556-be7c-4655-93fd-498c37682658.

   In this example, the UUID of the item is 23705556–be7c–4655–93fd–498c37682658.

2. Log in to the data-va's command-line interface.

3. Change to the Zimbra user.
   
   su – zimbra

4. Determine the account ID of the affected user by using the `zmprov` command.

   In the `zmprov` command, use the email address for that user's Horizon Workspace account.

   zmprov ga email_address hznDataId

   The zmprov command returns the account ID for the user with that email_address, for example

   hznDataId: 601

5. Access the embedded database's command-line-interface by entering `mysql` at the command prompt.

   mysql

6. Determine the user's mailbox ID and mailbox group ID by running a select query on `zimbra.mailbox` using the user's account ID, `user_account_id`, that was returned by the `zmprov` command.

   SELECT id, group_id, account_id, comment FROM zimbra.mailbox WHERE account_id =
user_account_id;

   The mailbox ID is the `id` value and the mailbox group ID is the `group_id` value.

   SELECT id, group_id, account_id, comment FROM zimbra.mailbox WHERE account_id=601;

   +------+------------+-------------+--------------------+
   | id   | group_id   | account_id  |   comment          |
   +------+------------+-------------+--------------------+
   | 109  | 9          | 601         | user1@hzn.local    |
The command returns the table row with the id, group_id, account_id, and comment columns. The value of the comment column is the user's email address, so you can verify that this data belongs to the user having the problem. You use the mailbox group ID to identify the user's mailbox database. The user's mailbox database is named mboxgroup appended by the group_id value, for example mboxgroup9 for a group_id value of 9.

7 Verify that the syncing item exists on the server for that user and that it has the NO_INHERIT flag set by running a select query on the user's mailbox database, mboxgroupN.mail_item, using the user's mailbox ID and the UUID of the syncing file or folder that was reported in the client's log file with debug logging enabled.

```sql
SELECT id, name, uuid, flags FROM mboxgroupN.mail_item WHERE mailbox_id = user_mailbox_id AND uuid = item_UUID;
```

The bitmask for the NO_INHERIT flag is 4194304, which is \(2^{22}\).

```sql
SELECT id, name, uuid, flags FROM mboxgroup9.mail_item WHERE mailbox_id = 109 AND uuid = 23705556-be7c-4655-93fd-498c37682658;
```

<table>
<thead>
<tr>
<th>id</th>
<th>name</th>
<th>uuid</th>
<th>flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>264</td>
<td>ABC.ppt</td>
<td>23705556-be7c-4655-93fd-498c37682658</td>
<td>4194304</td>
</tr>
</tbody>
</table>

8 Clear the value from the flags column for that syncing item by running an update SQL command on that database entry.

```sql
UPDATE mboxgroupN.mail_item SET flags = 0 WHERE mailbox_id = user_mailbox_id AND uuid = item_UUID;
```

```sql
UPDATE mboxgroup9.mail_item SET flags = 0 WHERE mailbox_id = 109 AND uuid = 23705556-be7c-4655-93fd-498c37682658;
```

**What to do next**

After you have resolved the problem, disable debug logging on the client system. See “Enable Debug Logging for the Horizon Workspace Desktop Client,” on page 153.

## Enable Debug Logging for the Horizon Workspace Desktop Client

To troubleshoot some situations involving syncing files and folders between the Horizon Workspace server and the desktop client, you might need additional debugging information from the Horizon Workspace desktop client. To have the Horizon Workspace desktop client write this detailed information to the client's log files on the desktop system, you must enable debug logging, which increases the logging level and the size and number of log files.

**Prerequisites**

Verify that you have access to the desktop system and that you have the appropriate permission level for the type of desktop system. For a Macintosh system, verify that you can run commands in the terminal. For a Windows system, you must have administrator permission so that you can modify the registry.
Procedure

1. On the desktop system, increase the logging for the local and remote scan, and increase the size and number of log files.

<table>
<thead>
<tr>
<th>Desktop system</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>a. Create the registry key HKEY_CURRENT_USER\Software\VMware, Inc.\Horizon Data\config, if it does not already exist.&lt;br&gt;b. Add a REG_SZ value named log.debugmask under that registry key, and set the value equal to `mordor:http:.*</td>
</tr>
</tbody>
</table>

2. Restart the client.

Debug logging is enabled for the Horizon Workspace desktop client.

What to do next

Allow the client to run and attempt to sync files and folders until the issue that you are troubleshooting occurs.

When you have collected the log files that you need for troubleshooting, disable the debug logging and restart the client. Disabling debug logging prevents the size and number of the log files from increasing over time.

<table>
<thead>
<tr>
<th>Desktop system</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Macintosh</td>
<td>In the terminal, run the following command to disable debug logging: <code>defaults delete com.vmware.HorizonWorkspace configVars</code></td>
</tr>
<tr>
<td>Windows</td>
<td>Edit the registry to remove the log.debugmask registry value under HKEY_CURRENT_USER\Software\VMware, Inc.\Horizon Data\config.</td>
</tr>
</tbody>
</table>

After disabling debug logging, restart the client.
Index

A
access events 135
access policies
  Auth Strength 28
  Client Type 28
minimum authentication score 31, 32
network 31, 32
Network 28
relationship to identity providers 31, 34, 35
TTL 28, 31, 32
Web-application-specific 32, 34–36
access policy set
  applying 36
  default 35, 36
  portal 36
access policy sets
  creating 35
  default 28, 31, 34
  editing 34
  portal 31, 35
Web-application-specific 32, 34–36
Active Directory
deployment 23
domain 16, 17
forest 16, 17
multi-domain 15
multi-forest 15–17
single domain 15
Add Identity Provider button 23
additional user attributes 43
admin user, reset password 140
administrative settings 137
administrator settings 137
Android apps, uploading into the catalog 85
Android workspace images for VMware Ready devices 84
application records
  Web applications 107
  Web applications from the cloud application catalog 105
applications
  mobile 56
  Web 56, 101, 105, 107, 108
audience 7
Audit Event report 135
authentication method 22, 23
authentication methods, relationship to access policies 31, 34, 35
automatic disable policy 89
automatic wipe policy 89
B
branding 138
branding elements 137
C
catalog
  imported mobile applications 85
  managing 51
  viewing resources 55
Web applications 105
categories
  applying 54
  creating 54
  deleting 55
  removing 55
certificate
  mobile devices 143
  private 143
  untrusted 143
Citrix deployment 111
Citrix-based, delivery settings 113
Citrix-based applications
categories 115
  Client application folder 115
  global application settings 113
  hide disabled 114
  individual application settings 114
class of service
  about 74
  assigning groups 73
  assigning users 72
  assigning to users 72
  creating 77
  deleting 80
  editing 75
  precedence 74
  viewing for users and groups 79
cloud application catalog, Web applications 105
company logo 137
configuration profiles, VPN 93
Configurator Web interface, access 137
configure SAML protocol 102
configure Web applications 102
Connector 19, 23
Connector Web interface, URL 9

D
data containment policies 89
Data Node Hostname attribute 43
default class of service 74
desktop systems, configuring 61
directory server groups 37

E
enable debug logging for the desktop client 153
end user license agreement, mobile workspaces 84
entitlements
file-sharing service 72
mobile workspaces 94
ThinApp packages 123
VMware Ready devices 86
Web applications 109
EULA
mobile workspaces 84
mobile device enrollment 84

F
file preview, troubleshooting 145
file sharing, setting options when installing the Windows application 62
file-sharing service
about 71
enabling 71
entitling 72
entitling groups 73
entitling users 72
resource type 52

G
Group Membership report 135
groups
Active Directory 37, 38
Horizon Workspace 37, 38
membership report 135
modify membership rules 39
policy sets 92
searching for 59
viewing information 41
guest users 9, 37, 49, 71

H
Horizon Files Usage, report 135
Horizon Workspace, virtual appliances 9

Horizon Workspace for Windows
enable debug logging 153
troubleshooting 147
Horizon Files 75, 77
Horizon Files module, enabling 71
Horizon Files Usage report 135
Horizon View entitlements 99
Horizon View Connection Server 99
Horizon View desktop pools, providing access 97
Horizon Workspace groups 37
Horizon Workspace for Mac, enable debug logging 153
hzn-admin tool 9, 137
hznAdminTool command 140

I
ICA properties 113, 114
identity provider
Connector 19
third-party 19, 27
identity providers
relationship to access policies 31
third-party 26
identity provider instances
adding 137
editing 137
editing the order 137
selection 19
identity provider selection, configuring 23
Independent Computing Architecture 113
installation options, Windows application 62
IP range 21

L
lease interval policy 89
leasing process 95
license, approval 137

M
managed mobile workspaces
disabling 47
policies 87
resetting passcodes 47
VMware Ready devices 83
wiping 47
Mobile Management module 82
mobile workspaces
entitling users and groups 94
EULA 84
mobile applications
resource type 52
uploading into your catalog 85
mobile device enrollment, end user license agreement 84
mobile devices, access to resources 81
mobile policy sets, creating 91
modules
   Citrix Published Applications 111
   Horizon Files 71
   Mobile Management 82
   ThinApp Packages 118
View 98
viewing information 13
Web Applications 101
multiple desktop systems, deploying the Windows application 68
multitenant Web applications 101

N
network range 21, 23
network ranges, relationship to access policies 31, 34, 35

O
Office 365
   convert to Horizon Workspace authentication 103
   example of Powershell cmdlet 103
   mapping attributes to AD user attributes 103
   powershell 103

P
passcode policies 90
password recovery, user 137
policies
   data containment 89
   passcode 90
   workspace lifetime 89
policy sets
   applying to groups 92
   managing 87
   policy resolution 87
   proof-of-concept 23

R
removing user access 47
reports 135
Resource Entitlement report 135
Resource Usage report 135
resources, categories 54, 55
roles 43

S
SAMl
   certificate 27
metadata 27
third-party identity providers 26
SAML certificate 137
settings, administrative 137
single sign-on to Web applications 102
single sign-on, Office 365 103
SSL trust and mobile devices 143
standard policy sets 88
sync client 16, 17
system information 13

T
ThinApp packages
   64-bit 69
   adding to the network share 133
deleting 130
deploying Horizon Workspace for Windows 68
enabling for management 131
entitling to users and groups 123
HorizonThinAppCtrl.exe 122
modifying the offline grace period 122
offline grace period 122
overview 118
providing access 117
setting options when installing the Windows application 62
updating 125–127, 129
ThinApp download mode 118
ThinApp package AppID, obtaining 126
ThinApp Packages module 118
ThinApp streaming mode 118
third-party identity provider 23
timeout error 150
token 47
troubleshooting
desktop client hangs 150
file preview 145
file syncing 145
launching a ThinApp package 148
sharing a file using previous iOS client 146
updating Horizon Workspace for Windows 147

U
user password, recovery 137
User Portal, URL 9
user authentication method 22
user store 16, 17, 23, 137
users
   Active Directory 37
   adding to groups 39
   attributes 43
Horizon Workspace  37
removing access  47
searching for  59
updating the sync filter to Active Directory  50
viewing information  43
viewing entitlements to Citrix-based applications  112
viewing entitlements to Horizon View desktop pools  98
Users report  135

V
View desktop pools, See Horizon View desktop pools
virtual appliances, Horizon Workspace  9
VMware Ready Android, importing Android workspace images  84
VMware Ready devices, workspaces  83
VMware Ready Android devices  82

W
Web applications
adding  101, 105
entitling  109
multitenant  101
Web Applications module  101
Web application bundle  108
Windows application
deploying to multiple systems  68
installer options  62
Windows applications  52
workspace images  52
workspace lifetime policies  89
Workspaces page  43
WS-Federation protocol  102