Horizon Workspace Administrator's Guide
Horizon Workspace 1.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
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

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

1 About the Horizon Workspace Administrator's Guide 5

2 Introduction to Horizon Workspace for Administrators 7

3 View Horizon Workspace System and Module Information 13

4 Search for Users, Groups, or Catalog Resources 15

5 Managing Users and Groups 17
   Horizon Workspace User and Group Types 17
   Manage Horizon Workspace Groups 18
   Manage Horizon Workspace Users 23
   Manage Virtual Users 27
   Update the Settings That Select Horizon Workspace Users from Active Directory 27

6 Managing the Horizon Workspace Catalog 29
   Overview of Horizon Workspace Resource Types 30
   View Horizon Workspace Resources 32
   Add Resources to Your Catalog 32

7 Providing Access to the Horizon Files Service 35
   Enable the Horizon Files Module 35
   Entitling and Provisioning Users and Groups to the Horizon Files Service 36
   Class of Service 38

8 Providing Access to Mobile Workspaces 47
   Setting Up Mobile Workspaces for iOS and Android Devices 48
   Setting Up Managed Mobile Workspaces for VMware Ready Android Devices 49
   Using Policies and Policy Sets 52
   Perform Actions on a User's Mobile Workspace 60
   Enable the Mobile Management Module 61
   Special Topics About Using Mobile Workspaces 61

9 Providing Access to Horizon View Desktop Pools 67
   Enable the View Module after Integrating Horizon View with Your Horizon Workspace System 68
   View User and Group Entitlements to Horizon View Desktop Pools 68
   View the Connection Information for a Horizon View Desktop Pool 69
   Reducing Resource Usage when Horizon View Desktops Have the Horizon Workspace Client for Windows Installed 69
10 Providing Access to Web Applications  71
   Enable the Web Applications Module to Provide Web Application Access  71
   Overview of Adding Web Applications to Your Organization's Catalog  72
   Entitle Users and Groups to Web Applications  76

11 Providing Access to Mobile Referred Applications  79
   Overview of Mobile Referred Applications  79
   Entitle Users and Groups to Mobile Referred Applications  86

12 Providing Access to VMware ThinApp Packages  89
   Enable the ThinApp Packages Module after Integrating Your ThinApps Repository with Your
      Horizon Workspace System  89
   Overview of ThinApp Packages  90
   Entitle Users and Groups to ThinApp Packages  91
   Silently Deploy Horizon Workspace Client for Windows on Users' Windows Systems  92
   Delete ThinApp Packages from Horizon Workspace  95

13 Viewing Horizon Workspace Reports  97
   Generate an Audit Event Report  97

14 Configuring Horizon Workspace Settings for Administrators  99
   Overview of Horizon Workspace Administrative Settings  99

15 Troubleshooting Horizon Workspace for Administrators  103
   Horizon Workspace Fails to Provision a User to the Horizon Files Service  103
   File Preview in the Horizon Workspace Web Client Displays Server Error and No Errors in the
      Server Logs  104
   Web Client Fails to Respond When Used In Some Workstation or VMware Fusion Environments  104
   Files With Names That Contain Invalid XML Characters Fail to Sync With the Horizon Workspace
      Clients on Windows or Mac Systems  105
   Sharing Folders or Files from the Horizon Workspace for iOS, First Edition App Fails With Error
      About Email  106

Index  107
About the Horizon Workspace Administrator's Guide

The VMware 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 data and applications and provide secure, multi-device, managed-user access to those resources. Such resources include Web applications, mobile applications, Windows applications as ThinApp packages, and VMware® Horizon View™ desktop pools. Horizon Workspace delivers a unified user and application policy 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™, RSA SecurID, Android and iOS 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 12.

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 Horizon Files service, Horizon View desktop pools, Windows applications (ThinApp packages), Web applications, and mobile applications. 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.
Introduction to Horizon Workspace for Administrators

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 Files service, which allows users to share files and folders with others.

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, Android, iOS, Web, and Software-as-a-Service (SaaS) applications to a single workspace 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 Horizon Workspace with the Horizon Web client (an agentless client), a Windows client, a Mac client, an Android client, or an iOS client. Each client provides users with access to the Horizon Workspace user interface, but access to applications, desktops, and data 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>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Workspace Web Client</td>
<td>The Horizon Workspace Web Client is an agentless client. It is the default client used when users access Horizon Workspace with a browser. Using the Horizon Workspace Web Client, users can access their Horizon Workspace files, Horizon View virtual desktops and Horizon Workspace Web applications. If an end user has a ThinApp entitled and is on a Windows system with this client installed and active, they can also view and launch their local ThinApp packages in this client.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Client for Windows</td>
<td>When this client is installed on users' Windows systems, they can access their Horizon Workspace files and Windows applications (captured as ThinApp packages) locally. When this client is installed, a user's personal and shared folders and files are synchronized between their system and Horizon Workspace.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Client for Mac</td>
<td>When this client is installed on users' Apple Mac OS X systems, they can access their Horizon Workspace files locally. When this client is installed, users' personal and shared folders and files are synchronized between their system and Horizon Workspace.</td>
</tr>
</tbody>
</table>
| VMware Horizon Workspace Client for Android | When this client is installed on users' Android devices, they can:  
  - Access their files  
  - Access their Web applications  
  - Install Android applications that you recommend for installation from Google Play. |
Table 2-2. Horizon Workspace User Client Components (Continued)

<table>
<thead>
<tr>
<th>Horizon Workspace User Client Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| VMware Horizon Workspace Client for iOS | When this client is installed on users’ iOS devices, they can:  
  - Install iOS applications that you recommend for installation from the Apple App Store.  
  - Access their files, using the Horizon Files iOS app installed on their devices.  
  - Access their Web applications.  
  Additionally, if your deployment is configured to access Horizon View desktop pools, iPad users can view their entitled virtual desktops using Horizon View Client for iOS. |
| VMware Switch                          | When this client is installed on users’ VMware Ready™ Android devices, they can provision and run a preconfigured mobile workspace on those devices. When the workspace is provisioned on the devices, the users can enter the provisioned workspace and perform their work tasks using the workspace’s policy-managed Android applications, including accessing their files and Web applications. |

User Authentication

The Connector acts as an identity provider within your network, creating an in-network federation authority that communicates with Horizon Workspace using SAML 2.0 assertions. The Connector authenticates the user with Active Directory within the enterprise network (using existing network security).

The following authentication methods are supported by Horizon Workspace: Active Directory username/password, Kerberos, and RSA SecurID.

<table>
<thead>
<tr>
<th>Horizon Workspace Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username/password</td>
<td>Active Directory username/password authentication is the default user authentication method. This method authenticates users directly against your Active Directory.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>When properly configured, Kerberos authentication provides Windows users with single sign-on access to Horizon Workspace, eliminating the requirement for Windows users to log in to Horizon Workspace after they log in to the enterprise network. The Connector validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC).</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>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>

Username/password authentication is the authentication method in use when you initially deploy Horizon Workspace. The username/password authentication method can authenticate users regardless of whether users are inside or outside the enterprise network. To provide user access to Horizon Workspace from outside the enterprise network, you can either require VPN access or you can install Horizon Workspace in a manner that allows Internet access.

If you decide to use username/password authentication to provide users outside the enterprise network access to Horizon Workspace, you can configure Horizon Workspace in one of the following ways:

- Install a reverse proxy server in the DMZ pointing to the Gateway virtual appliance.
- Configure firewall port forwarding or router port forwarding to point to the Gateway virtual appliance.
To implement Kerberos authentication or RSA SecurID authentication, you must deploy one or more additional Connector instances. See *Installing and Configuring Horizon Workspace* for information about creating additional Connector instances. To implement both Kerberos authentication and RSA SecurID authentication, you first deploy Horizon Workspace, which includes all the Horizon Workspace virtual appliances.

You can configure one or more Connector instances to handle Kerberos authentication and one or more Connector instances to handle RSA SecurID authentication. Configuring any single Connector instance to handle both Kerberos authentication and RSA SecurID authentication is not a best practice. When you use more than one Connector instance in your deployment, you must use the Administrator Web interface to configure IdP discovery.

If you decide to use Kerberos authentication to seamlessly authenticate Windows users (applies to users inside the enterprise network only) to Horizon Workspace, issue the `hznAdminTool addvm` command in the configurator-va virtual machine to add a new connector-va virtual machine. Since the Connector acts as an identity provider, when you add a new Connector instance you are adding a new identity provider instance.

If you decide to use RSA SecurID authentication to provide users outside the enterprise network access to Horizon Workspace, you must add the connector-va virtual machine using the `addvm` option of the `hznAdminTool` command. This command creates an additional identity provider. You can then configure the new identity provider using the Horizon Workspace Administrator Web interface.

The supported authentication types can be used in a variety of ways to provide users, both inside and outside the enterprise network, access to Horizon Workspace.

**Table 2-3. Overview of Providing User Access to Horizon Workspace**

<table>
<thead>
<tr>
<th>User Access From Inside the Enterprise Network</th>
<th>User Access From Outside the Enterprise Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username/password authentication: Functions by default. No additional Connector instances are required for this authentication method when users are inside the enterprise network.</td>
<td>Username/password authentication: To implement username/password authentication for users outside the enterprise network, you must enable Internet access to the Gateway virtual appliance. VPN is an option, too.</td>
</tr>
<tr>
<td>Kerberos authentication: Requires an additional Connector instance.</td>
<td>Kerberos authentication: Not applicable. This authentication method is not an option for authenticating users outside the enterprise network.</td>
</tr>
<tr>
<td>RSA SecurID authentication: Not recommended. This authentication method is not recommended for authenticating users who are inside the enterprise network.</td>
<td>RSA SecurID authentication: When practical, this authentication method is preferred for authenticating users outside the network. The best practice is to install a Connector instance dedicated to RSA SecurID authentication.</td>
</tr>
</tbody>
</table>

**NOTE** Horizon Workspace handles RSA SecurID authentication and Kerberos authentication failures differently:

- If Kerberos authentication fails for any reason, the Connector falls back to username/password authentication. In such cases, users are presented with a login page that prompts them for their username and password to access Horizon Workspace. The Connector then validates users against the directory server.

- If RSA SecurID authentication fails, the Connector does not fall back to username/password authentication. Since RSA SecurID is only recommended for users outside the enterprise network, such users will not be able to access Horizon Workspace until the cause of failure is resolved.
IdP Discovery

IdP discovery matches users from specific IP addresses with their corresponding identity providers (Connector instances). For example, users with IP addresses outside the enterprise network might be directed to a Connector instance dedicated to RSA SecurID authentication, while internal users might be directed to a Connector instance dedicated to Kerberos authentication. Though different users are directed to different Connector instances, you provide all users with a single Horizon Workspace URL since IdP discovery does the work behind the scenes to locate the appropriate Connector instance.

The default IdP discovery configuration applies to the default Horizon Workspace deployment, which uses username/password authentication with a single Connector instance. If you deploy Horizon Workspace in this manner, you do not need to change the IdP discovery configuration.

When you deploy multiple Connector instances using the `addvm` option of the `hznAdminTool` command for the purpose of maintaining multiple identity providers, you need to use the Horizon Workspace Administrator Web interface to access the `Settings > Identity Providers` page, where you must perform the following:

- Locate each additional Connector instance name in the list of identity providers. When you use the `addvm` option of the `hznAdminTool` command to create a new Connector instance, that Connector instance name is added to this page.
- Edit the order of the identity providers as necessary. The order in which the corresponding Connector instances are listed in Horizon Workspace is important if the IP ranges overlap. In such cases, the first Connector instance in the list to include an IP address is given precedence.

**CAUTION** When you remove or reset a Connector instance, you must remove the corresponding Connector name from the `Identity Providers` page.

You can deploy Horizon Workspace with IdP Discovery in a variety of ways, one of which is summarized in the example that follows.

**External RSA SecurID and Internal Kerberos Authentication Example of IdP Discovery**

This is one possible way to configure IdP Discovery for Kerberos and SecurID in the same Horizon Workspace deployment.

- Internal - First Connector instance: You configure Kerberos for this Connector instance. In the Horizon Workspace Administrator Web interface, on the Identity Providers page, you configure IP address ranges to include users within the enterprise network.

- External - Second Connector instance: You configure SecurID for this Connector instance. In Horizon Workspace, you configure a single IP address range that includes all possible users. Therefore, you set the IP address range from 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 redirected to the first Connector instance and authenticated with Kerberos or username/password authentication while users outside the enterprise network are redirected to the second Connector instance and authenticated with SecurID authentication.

**NOTE** Virtual users are not prompted for SecurID credentials even when the virtual users are external to your enterprise and are redirected to a Connector instance that enforces SecurID authentication. See “Horizon Workspace User and Group Types,” on page 17 for a description of virtual users.
## 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 2-4. 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 <code>admin</code> and the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/web">https://HorizonWorkspaceFQDN/web</a></td>
<td>Web Client (end user)</td>
<td>Manage files, launch applications, or launch View pools. (Log in as an Active Directory user or virtual user.)</td>
</tr>
<tr>
<td><a href="https://ConnectorHostname/hc/admin/">https://ConnectorHostname/hc/admin/</a></td>
<td>Connector Web interface</td>
<td>Configure additional ThinApp settings, View pool 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, and the ThinApp Packages 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 35
- “Enable the Web Applications Module to Provide Web Application Access,” on page 71
- “Enable the Mobile Management Module,” on page 61
- “Enable the View Module after Integrating Horizon View with Your Horizon Workspace System,” on page 68
- “Enable the ThinApp Packages Module after Integrating Your ThinApps Repository with Your Horizon Workspace System,” on page 89
Search for Users, Groups, or Catalog Resources

Use the search field 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 field.

   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.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users tab</td>
<td>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.</td>
</tr>
<tr>
<td>Groups tab</td>
<td>The typed-in string matches the starting characters of any word within the group's name or description.</td>
</tr>
<tr>
<td>Catalog tab</td>
<td>The typed-in string matches the starting characters of any word within the catalog resource's name or description.</td>
</tr>
</tbody>
</table>

**Note**  By default, 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 default.
Managing Users and Groups

You can manage and monitor users and groups, which includes the users and groups imported from your enterprise’s directory server and virtual users.

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 details page for a user, you can entitle that user to a resource, and from the details 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 details 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 17
- “Manage Horizon Workspace Groups,” on page 18
- “Manage Horizon Workspace Users,” on page 23
- “Manage Virtual Users,” on page 27
- “Update the Settings That Select Horizon Workspace Users from Active Directory,” on page 27

Horizon Workspace User and Group Types

With the Horizon Workspace Administrator Web interface, you can manage users, virtual 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 view and edit the group rules.

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.

Virtual Users

The virtual users feature is an optional feature that applies solely to the Horizon Files service, the file storage and 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 virtual user. Virtual 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 virtual 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 40 or “Create a Class of Service,” on page 42 for information about the External Folder Sharing Allowed option.

Manage Horizon Workspace Groups

Creating groups, configuring group rules, 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 directory server 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 directory server group names, indicating that the group is a directory server 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, edit the group rules to set the group membership. See “Configure Rules for Horizon Workspace Group Membership,” on page 19.
Configure Rules for Horizon Workspace Group Membership

You can create group rules that define 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.

Group rules 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 for which you want to configure the rules for membership.
4. Click the Users in this Group tab.
   - The system displays the list of users that are currently members in the group.
5. Click View Group Rules.
6. Select an option from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any of the following</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>All of the following</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>
7 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>
<tbody>
<tr>
<td>Group</td>
<td>Select <strong>Is</strong> 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 <strong>Is Not</strong> 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.</td>
</tr>
</tbody>
</table>

**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.

8 (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.

9 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.

Prerequisites

- Install and configure Horizon Workspace. As part of the installation, import users and, if applicable, groups from your directory server. See Installing and Configuring Horizon Workspace.

- Verify there is at least one group listed on the Users & Groups page in the Administrator Web interface. You cannot view the details of a group unless at least one group exists in the system.

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 system.

   - 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.

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 Files 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><strong>Entitlements</strong></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 <strong>Add entitlement</strong> to entitle the group’s users to the individual resources that are available in your catalog.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you entitle the iOS or Android Horizon Files app to a group, you must also entitle the Horizon Files service to provide the file-sharing capabilities to the group’s users.</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 each resource type, you can click <strong>Edit</strong> 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 group’s entitlements to the web applications or the type of deployment for the group’s entitled web applications. Select <strong>Automatic</strong> to have the web application displayed by default in the user’s Horizon Workspace client application. Select <strong>User-Activated</strong> to allow the users to add the web application to the list of web applications that are displayed in each user’s Horizon Workspace client.</td>
</tr>
<tr>
<td></td>
<td>- For iOS apps, click <strong>Edit</strong> to change the group’s entitlements to the iOS applications. The deployment type for a referred iOS app is user-activated by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>- For managed mobile workspaces on 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.</td>
</tr>
<tr>
<td></td>
<td>- For mobile workspaces on Android devices that are not VMware Ready devices, click <strong>Edit</strong> to change the group’s entitlement to the app. Mobile referred Android apps are used for workspaces on Android devices that are not VMware Ready devices. The deployment type for a referred Android app is user-activated by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>- For the Horizon Files service, click <strong>Edit</strong> to select the class of service (COS) for the user.</td>
</tr>
<tr>
<td></td>
<td>- For each entitled resource, you can click <strong>Unentitle</strong> to remove the group’s access to use that specific resource.</td>
</tr>
<tr>
<td><strong>Users in this Group</strong></td>
<td>The group’s membership page is displayed. In this page, you can:</td>
</tr>
<tr>
<td></td>
<td>- View the list of users that belong to the group.</td>
</tr>
<tr>
<td></td>
<td>- Click a user’s name to display the details page for that user.</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>View Group Rules</strong> to view and configure the rules that define membership to the Horizon Workspace group. The <strong>View Group Rules</strong> option is available for Horizon Workspace groups, but not for directory server groups.</td>
</tr>
<tr>
<td><strong>Applied Mobile Policy Sets</strong></td>
<td>The group’s Applied Mobile Policy Sets page is displayed. In this page, you can:</td>
</tr>
<tr>
<td></td>
<td>- View the mobile policy sets that are currently applied to the group’s users.</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>Select Mobile Policy Sets</strong> to select which mobile policy sets to apply to the group.</td>
</tr>
</tbody>
</table>
Manage Horizon Workspace Users

You can manage Horizon Workspace users, the users imported from your directory server, 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 your directory server. See the 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 workspaces using the Administrator Web interface.

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 define group rules for 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><a href="https://HorizonWorkspaceFQDN/admin">https://HorizonWorkspaceFQDN/admin</a></td>
</tr>
<tr>
<td>Web Client</td>
<td>User</td>
<td><a href="https://HorizonWorkspaceFQDN/web">https://HorizonWorkspaceFQDN/web</a></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 Horizon Files service and can appear as an additional attribute for users. The attribute appears when the user is entitled to the Horizon Files 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 Horizon Files 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 Horizon Files 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 Add entitlement to entitle the user to resources that are available</td>
</tr>
<tr>
<td></td>
<td>in your catalog.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you entitle the iOS or Android Horizon Files app to a</td>
</tr>
<tr>
<td></td>
<td>user, you must also entitle the Horizon Files service to provide the</td>
</tr>
<tr>
<td></td>
<td>file-sharing capabilities to that user.</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 each resource type, you can click Edit to entitle or unentitle the</td>
</tr>
<tr>
<td></td>
<td>user to resources of that type, or to customize the options for each</td>
</tr>
<tr>
<td></td>
<td>entitled resource. From the Entitlements page, you can make the</td>
</tr>
<tr>
<td></td>
<td>following changes:</td>
</tr>
<tr>
<td></td>
<td>■ For web applications, click Edit to change the user's entitlements</td>
</tr>
<tr>
<td></td>
<td>to the web applications or the type of deployment for each of the</td>
</tr>
<tr>
<td></td>
<td>user's entitled web applications. Select Automatic to have the web</td>
</tr>
<tr>
<td></td>
<td>application displayed by default in the user's Horizon Workspace</td>
</tr>
<tr>
<td></td>
<td>client application. Select User-Activated to allow the user to add</td>
</tr>
<tr>
<td></td>
<td>the web application to the list of web applications that are</td>
</tr>
<tr>
<td></td>
<td>displayed in the user's Horizon Workspace client.</td>
</tr>
<tr>
<td></td>
<td>■ For iOS apps, click Edit to change the user's entitlements to iOS</td>
</tr>
<tr>
<td></td>
<td>applications. The deployment type for a referred iOS app is user-</td>
</tr>
<tr>
<td></td>
<td>activated by default, and you cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>■ For managed mobile workspaces on VMware Ready devices, click Edit</td>
</tr>
<tr>
<td></td>
<td>to specify the workspace image and the Android apps for the</td>
</tr>
<tr>
<td></td>
<td>workspace. The deployment type is automatic by default, and you</td>
</tr>
<tr>
<td></td>
<td>cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>■ For mobile workspaces on Android devices that are not VMware Ready</td>
</tr>
<tr>
<td></td>
<td>devices, click Edit to change the user's entitlement to the app. Mobile</td>
</tr>
<tr>
<td></td>
<td>referred Android apps are used for workspaces on</td>
</tr>
<tr>
<td></td>
<td>Android devices that are not VMware Ready devices. The deployment type</td>
</tr>
<tr>
<td></td>
<td>for a referred Android app is user-activated by default, and you</td>
</tr>
<tr>
<td></td>
<td>cannot change this setting.</td>
</tr>
<tr>
<td></td>
<td>■ For the Horizon Files service, click Edit to select the class of</td>
</tr>
<tr>
<td></td>
<td>service (COS) for the user.</td>
</tr>
<tr>
<td></td>
<td>■ For each entitled resource, you can click Unentitle to remove the</td>
</tr>
<tr>
<td></td>
<td>user's access to use that resource.</td>
</tr>
<tr>
<td><strong>Group Affiliations</strong></td>
<td>A list of the groups to which the user belongs is displayed. Each group</td>
</tr>
<tr>
<td></td>
<td>name represents a group to which the user is a member. You can click a</td>
</tr>
<tr>
<td></td>
<td>group's name to display the details page for that group.</td>
</tr>
<tr>
<td><strong>Workspaces</strong></td>
<td>The user's Workspaces page is displayed. In this page, you can:</td>
</tr>
<tr>
<td></td>
<td>■ View lists of the mobile and desktop workspaces installed on the user's</td>
</tr>
<tr>
<td></td>
<td>mobile devices and desktop systems, including the current status of</td>
</tr>
<tr>
<td></td>
<td>each workspace.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A workspace is added to the lists when the</td>
<td>A workspace is added to the lists when the user logs in to Horizon Workspace for the first time from a device or system using the appropriately installed 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 Log IN TO HORIZON Workspace FOR THE FIRST TIME.</td>
</tr>
<tr>
<td>For a mobile workspace, you can click its</td>
<td>For a mobile workspace, you can click its name to perform available actions on that mobile workspace. See “Perform Actions on a User’s Mobile Workspace,” on page 60. 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.</td>
</tr>
<tr>
<td>name to perform available actions on that</td>
<td></td>
</tr>
<tr>
<td>mobile workspace. See “Perform Actions on a</td>
<td></td>
</tr>
<tr>
<td>User’s Mobile Workspace,” on page 60. Note</td>
<td></td>
</tr>
<tr>
<td>By default, only mobile workspaces that</td>
<td></td>
</tr>
<tr>
<td>have been recently provisioned to the user</td>
<td></td>
</tr>
<tr>
<td>are initially displayed. To display the list</td>
<td></td>
</tr>
<tr>
<td>of all of the mobile workspaces that have</td>
<td></td>
</tr>
<tr>
<td>been previously provisioned to the user,</td>
<td></td>
</tr>
<tr>
<td>click View All. To toggle back to display</td>
<td></td>
</tr>
<tr>
<td>only the most recently provisioned mobile</td>
<td></td>
</tr>
<tr>
<td>workspaces, click View Latest.</td>
<td></td>
</tr>
<tr>
<td>For a desktop workspace, you can click</td>
<td>For a desktop workspace, 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.</td>
</tr>
<tr>
<td>Delete to remove the corresponding system</td>
<td></td>
</tr>
<tr>
<td>from Horizon Workspace. You might want to</td>
<td></td>
</tr>
<tr>
<td>remove a system from Horizon Workspace because the system is lost, stolen, or no longer in use.</td>
<td></td>
</tr>
</tbody>
</table>

**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</td>
<td>In your directory server, delete or disable user accounts according to the needs of your enterprise. If you disable users already entitled to the Horizon Files service and you later re-enable those users, Horizon Workspace retrieves those users’ shared files and folders.</td>
</tr>
<tr>
<td>User Accounts</td>
<td></td>
</tr>
<tr>
<td>Create Filters in Horizon Workspace for</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. If you use the create filters method with users already entitled to the Horizon Files service, their shared files and folders are deleted and not retrievable if you later add these users back. See Installing and Configuring Horizon Workspace for more information about creating filters to exclude users.</td>
</tr>
<tr>
<td>Active User Accounts in Your Directory</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></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.
Manage Virtual Users

You can view and manage information about virtual users. Virtual users are users external to Horizon Workspace whom Horizon Workspace users specifically invite to access selected folders.

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

Procedure

1. Log in to the Administrator Web interface.
2. To view and manage user information, click Users & Groups > Virtual Users.
   The Virtual Users page lists the email address, last login time, and access status of every virtual user associated with your Horizon Workspace deployment.
3. Manage virtual users as needed.
   - To delete virtual users, check the check box for each virtual user you want to delete and click Delete Users.
     This action removes virtual users from Horizon Workspace. Deleted virtual users lose access to all files previously shared with them.
   - To prevent virtual users from logging in to Horizon Workspace, click Lock for each virtual 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 virtual users, click Unlock for each virtual user to whom you want to unblock access. When you unlock virtual 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 your Horizon Workspace system. 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>
<tbody>
<tr>
<td>Change the Active Directory server information, such as the server</td>
<td>a  Click Directory.</td>
</tr>
<tr>
<td>host, port, base DN, bind DN, bind password, and so on.</td>
<td>b  Make your changes.</td>
</tr>
<tr>
<td></td>
<td>c  Click Save.</td>
</tr>
<tr>
<td>Change the mapping of Horizon Workspace user attributes to</td>
<td>a  Click User Attributes.</td>
</tr>
<tr>
<td>Active Directory user attributes.</td>
<td>b  Make your changes.</td>
</tr>
<tr>
<td></td>
<td>c  Click Save.</td>
</tr>
<tr>
<td>Change the user selection rules for the filter that defines which</td>
<td>a  Click Directory Sync.</td>
</tr>
<tr>
<td>Active Directory users are synced to Horizon Workspace.</td>
<td>b  Click Edit Directory Sync Rules.</td>
</tr>
<tr>
<td></td>
<td>c  Make your changes on the Select Users page as necessary, and click</td>
</tr>
<tr>
<td></td>
<td>Next.</td>
</tr>
<tr>
<td></td>
<td>d  Make your changes on the Select Groups page as necessary, and click</td>
</tr>
<tr>
<td></td>
<td>Next.</td>
</tr>
<tr>
<td></td>
<td>e  Click Push to Horizon.</td>
</tr>
<tr>
<td></td>
<td>f  Click Save and Continue.</td>
</tr>
</tbody>
</table>
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 your Horizon Workspace system.

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 types of resources 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>Horizon Files service</td>
<td>Enable the Horizon Files module on the Dashboard page in the Administrator Web interface. Click <strong>Services</strong> on the Catalog page.</td>
</tr>
<tr>
<td>Web application</td>
<td>Enable the Web Applications module on the Dashboard page in the Administrator Web interface. Click <strong>Web Applications</strong> on the Catalog page.</td>
</tr>
<tr>
<td>Mobile application, imported</td>
<td>Enable the Mobile Management module on the Dashboard page in the Administrator Web interface. Click <strong>Mobile Applications</strong> on the Catalog page.</td>
</tr>
<tr>
<td>Mobile application, referred</td>
<td>Enable the Mobile Management module on the Dashboard page in the Administrator Web interface. Click <strong>Mobile Applications</strong> on the Catalog page.</td>
</tr>
<tr>
<td>Workspace image, for VMware® Ready™ Android devices</td>
<td>Enable the Mobile Management module on the Dashboard page in the Administrator Web interface. Click <strong>Workspace Images</strong> on the Catalog page.</td>
</tr>
<tr>
<td>Windows application captured as a ThinApp package</td>
<td>Use the Configurator Web interface to enable the ThinApp Packages module, and also to add the ThinApp package to your catalog as a resource.</td>
</tr>
<tr>
<td>Horizon View desktop pool</td>
<td>Use the Configurator Web interface to enable the View module, and also to add the Horizon View desktop pools to your catalog as a resource.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Overview of Horizon Workspace Resource Types,” on page 30
- “View Horizon Workspace Resources,” on page 32
- “Add Resources to Your Catalog,” on page 32
Overview of Horizon Workspace Resource Types

With Horizon Workspace, you can manage Web applications, mobile applications, Windows applications captured as VMware ThinApp packages, VMware Horizon View desktop pools, and the Horizon Files service, the file storage and sharing service. Mobile applications can be mobile referred applications or imported mobile applications. Mobile referred applications can be iOS and Android applications. Imported mobile applications can be Android applications that can be provisioned to VMware Ready Android devices. You can also manage workspace images that can be provisioned to VMware Ready Android devices.

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.

Web Applications
You populate your catalog with Web applications directly on the Catalog page of the Horizon Workspace Administrator Web interface. When you click the Web application's icon displayed on the Catalog page, information about that application is displayed. From the displayed page, you can configure the Web application and provide 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 32.

Imported Mobile Applications
Imported mobile applications are mobile applications that you import directly into your catalog. Imported mobile applications are also known as managed mobile applications because the Horizon Workspace server can control them using policies after they are installed on the users' mobile devices. You populate your catalog with imported 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 imported 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 managed mobile application to users and groups.

Workspace Images
A workspace image is a version of the Android operating system that is installed as the secure Android container for managed mobile workspaces on VMware® Ready™ Android devices. By either uploading or removing a workspace image, you determine whether that workspace image is available as a resource in your catalog.

Referred Mobile Applications
Referred mobile applications are mobile applications that reside in either the Apple App Store or Google Play, and which you want your users to install on their mobile devices. When you add mobile referred applications to your catalog, you are actually creating a link in your catalog to the mobile application in Apple App Store or Google Play. Using the Catalog page of the Horizon Workspace Administrator Web interface, you configure the relevant information about the application and it becomes a resource in your catalog. On the Catalog page, when you click the icon for a referred mobile application that has been configured as a resource in your catalog, information about the application is displayed. From the displayed page, you can configure settings appropriate for the referred mobile application, and entitle it to users. Entitling a referred mobile application primarily serves as a method of recommending users to mobile applications approved for use in your enterprise. See “Add Resources to Your Catalog,” on page 32.
**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 the ThinApp packages by capturing Windows applications as ThinApp packages. See the VMware ThinApp documentation.
2. Create a Windows applications network share and move the ThinApp packages to it. See *Installing and Configuring Horizon Workspace*.
3. Configure Horizon Workspace to integrate with VMware ThinApp. See *Installing and Configuring Horizon Workspace*.

After you perform these tasks, 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 access the Windows applications captured as ThinApp packages, users must have the Horizon Workspace Client for Windows installed on their Windows systems. Users cannot see or access the applications from other clients.

**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. Configure 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*.

After you perform these tasks, the View Desktops you entitled to users in VMware Horizon View are now available as resources in your catalog.

**Horizon Files Service**

1. Perform the relevant preconfiguration steps during installation of Horizon Workspace, such as add storage to the data-va virtual appliance and configure a preview server. See *Installing and Configuring Horizon Workspace*.
2. Populate your catalog with the Horizon Files service by enabling the Horizon Files module. See "Enable the Horizon Files Module," on page 35.

After you perform these tasks, the Horizon Files service is now 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 Horizon Files Service," on page 37.
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, mobile applications, ThinApp packages, Horizon View desktop pools, and the Horizon Files service, the file storage and sharing service.

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, and ThinApp Packages module are available.
- Add resources to the catalog to meet the needs of your enterprise. See Chapter 6, “Managing the Horizon Workspace Catalog,” on page 29.

Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Click the Catalog tab.
3. Click a tab to list the resources you want to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Lists all of the resources in your catalog.</td>
</tr>
<tr>
<td>Web Applications</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>Workspace Images</td>
<td>Lists the workspace images in your catalog. 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>Mobile Applications</td>
<td>Lists only mobile applications in the catalog. Mobile applications are applications accessible from supported mobile devices. Both managed mobile applications and referred mobile applications are listed.</td>
</tr>
<tr>
<td>ThinApp Packages</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>View Pools</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>Services</td>
<td>Lists only services in your catalog. The Horizon Files service is the only service available for Horizon Workspace.</td>
</tr>
</tbody>
</table>

4. 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 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 Global Catalog,” on page 72
- “Add a Web Application to Your Catalog by Creating a New Application Record,” on page 74
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 the appropriate **+** button to add the resource.
4. Click an option depending on the resource type, and the location of the application. When importing a 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>from your Global Catalog</td>
<td>Web application, mobile referred</td>
<td>Horizon Workspace includes access to several default Web and mobile referred applications, available in the Global Catalog, that you can add to your catalog as resources.</td>
</tr>
<tr>
<td>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>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>import an APK file</td>
<td>Managed mobile application</td>
<td>You can import an Android app to make it available for users in managed mobile workspaces.</td>
</tr>
<tr>
<td>from Apple App Store</td>
<td>Mobile referred application</td>
<td>You can add iOS apps that are available in the Apple App Store as resources in your catalog. When added to your catalog, such an iOS app has the resource type of mobile referred application.</td>
</tr>
<tr>
<td>from Google Play</td>
<td>Mobile referred application</td>
<td>You can add Android apps that are available in Google Play as resources in your catalog. When added to your catalog, such Android apps have the resource type of mobile referred application.</td>
</tr>
</tbody>
</table>

5. Follow the prompts to finish adding resources to the catalog.
You can entitle Horizon Workspace users to the Horizon Files service. The Horizon Files service allows Horizon Workspace users to share files and folders with other Horizon Workspace users and with virtual users. Virtual users are users external to Horizon Workspace whom Horizon Workspace users specifically invite to access selected folders. The Horizon Files 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 configure the Horizon Files service in your catalog and entitle the service as a resource to users and groups using the Administrator Web interface.

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 Horizon Files 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 35
- “Entitling and Provisioning Users and Groups to the Horizon Files Service,” on page 36
- “Class of Service,” on page 38

**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 Horizon Files 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 12 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 Horizon Files service is available in your catalog as a resource that can be entitled to users or groups.

**What to do next**

- Edit the default class of service (COS), create a COS, or both. See “Class of Service,” on page 38
- Entitle users or groups to the Horizon Files service.
- Verify the distribution of the appropriate Horizon Workspace Client applications to users’ desktops and mobile devices.

For Mac and Windows systems, users can use a browser (Horizon Workspace Web Client) to access their files and folders. For a native experience, users can use the Horizon Workspace native clients on iOS, Android, Windows, and Mac OS X operating systems. For example, using Horizon Workspace Client for Windows, the user can modify files and add folders using Windows Explorer. The Horizon Files iOS app is the native client for iOS devices.

**NOTE** On Windows and Mac systems, the best practice for users is to install the respective client, Horizon Workspace Client for Windows or Horizon Workspace Client for Mac. These clients 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 the desktop clients manually. See *Horizon Workspace User Guide*.

To install on multiple Windows systems at once, the Horizon Workspace administrator can silently install Horizon Workspace Client for Windows. See “Silently Deploy Horizon Workspace Client for Windows on Users’ Windows Systems,” on page 92.

---

**Entitling and Provisioning Users and Groups to the Horizon Files Service**

To give users or groups of users the capability to share files and folders, you must entitle them to the Horizon Files service. If Horizon Workspace is functioning normally, when you entitle users to the Horizon Files service, the service automatically provisions them. 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 Horizon Files service as an entitled resource, and assign the appropriate class of service. See “Class of Service,” on page 38. 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.

When you entitle the Horizon Files service to individual users and groups, Horizon Workspace attempts to automatically provision those users. Provisioning refers to the creation of user records in the data-va virtual machine.
Certain problems, such as networking and timing issues, can prevent Horizon Workspace from provisioning users. In such cases, users have the permissions necessary to store and share files, but since the automated provisioning process failed they do not have access to the Horizon Files service. When you view user and group entitlements to the Horizon Files service, you can view users’ provisioning status to determine if a provisioning-related problem exists.

**CAUTION** The Horizon Files service keeps a record of all entitled users, even users who are removed from Horizon Workspace. When you follow the process of entitling a user to the Horizon Files service, removing the user from Horizon Workspace, and later adding the user back to Horizon Workspace, Horizon Workspace might not be able to provision that user to the Horizon Files service again. Entitling and unentitling the same user to and from the Horizon Files service does not cause this issue.

The Horizon Files service identifies users with the unique identifiers ID and email. When a user is added back to Horizon Workspace, the user is issued a new ID. If the user is using the same email address as before, the Horizon Files service treats the user as a different user attempting to use an existing email address. The Horizon Files service cannot provision the user in this situation and displays a provisioning error.

In this situation, you can issue the delete-account command in the data-va virtual machine to remove the user’s original account. For example, `zmprov da joe@domain.com`. See *Horizon Workspace Files Command Line Interface*.

### Entitle Users to the Horizon Files Service

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

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

**Prerequisites**

- Enable the Horizon Files module. Enabling this module makes the Horizon Files 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.

**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 Horizon Files service.
4. Click **Add Entitlement**.
5. Click the check box for the resource that corresponds to the **Horizon Files** 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 Horizon Files Service

You can entitle a group's users to the Horizon Files 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 Horizon Files service is to add a group entitlement for the Horizon Files service to a group, and add the users to that group.

Prerequisites

- Enable the Horizon Files module. Enabling this module makes the Horizon Files 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.

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 Horizon Files service.
4. Click Add Entitlement.
5. Click the check box for the resource that corresponds to the Horizon Files 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 39.

Class of Service

When you entitle users or groups to the Horizon Files 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 your Horizon Workspace deployment contains two or more data-va servers and you edit or create a new COS, wait fifteen minutes before you entitle users to the Horizon Files service. Fifteen minutes is the refresh interval for the data-va servers. This practice prevents unexpected results with the COS assignment.
Criteria for Class of Service Precedence

A Horizon Workspace user can be entitled to the Horizon Files 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 Horizon Files 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 Horizon Files 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.

Horizon Workspace follows specific resolution criteria to select the COS out of a user’s assigned classes of service, and apply the selected COS to that user. The assigned COS determines the user’s file storage and sharing policy.

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 Horizon Files service, but can be a member of an unlimited number of groups that each have a group entitlement to the Horizon Files 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 file storage and sharing policy to that user according to the order of groups as listed in the Group Entitlements section of the resource page for the Horizon Files service. To access the service’s resource page, in the Administrator Web interface, click Catalog > Services > Horizon Files. The Group Entitlements section lists all the groups entitled to the Horizon Files service. Some of the groups might have a named COS and some 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. That COS enforces the user’s file storage and sharing policy.

Changing the COS that Takes Precedence

You can change the COS that determines a user’s file storage and sharing policy by taking the steps to entitle the user to the Horizon Files service again.

If a user has a user entitlement to the Horizon Files service, you can change the COS that determines the user’s file storage and sharing policy by following the steps to entitle the user to the Horizon Files service, and selecting the COS you want as the assigned COS for that new entitlement.

If a user is entitled to the Horizon Files service through a group entitlement, you can change the COS that determines the user’s file storage and sharing policy by following the steps to add another group entitlement to the Horizon Files service, and selecting the COS you want as the assigned COS for that new group entitlement. This action might change the file storage and sharing policy 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. You can edit the default COS and any new COS that you create.

The Administrator Web interface is the main tool for configuring the Horizon Workspace Horizon Files service, but some Horizon Files 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 unless you use the command line to change the settings at the account level. 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. Select Catalog > Services.
3. Click Horizon Files.
4. Click Class of Service.
5. Click Edit for the COS you want to edit.
6. Edit the settings in the form as appropriate.

**NOTE** A value of zero (0) on the form indicates that parameter has no limit.

<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>Minimum duration of time between quote warnings</td>
<td>The frequency with which the quota warning email message is sent.</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>Form Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</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</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.</td>
</tr>
<tr>
<td>External Folder Sharing</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 virtual users.</td>
</tr>
<tr>
<td>Public Files Sharing</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 virtual users.</td>
</tr>
<tr>
<td>Public Expiration</td>
<td>The amount of time files are accessible on the Internet.</td>
</tr>
<tr>
<td>Domains Allowed or Not</td>
<td>This option enables you to restrict or allow virtual-user access to shared folders based on the virtual user's domain.</td>
</tr>
<tr>
<td>Allowed 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 virtual users can access shared folders. When this choice is selected, type the allowed domain names in the Allowed domains for external sharing field.</td>
</tr>
<tr>
<td></td>
<td>■ Restricted to specify domains from which virtual users are prevented from accessing shared folders. When this choice is selected, type the restricted domain names in the Restricted domains for external sharing field.</td>
</tr>
<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 Horizon Files service assigns new users evenly among all servers in the list. When you select more than one server, the Horizon Files 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 Horizon Files client 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 Horizon Files service.</td>
</tr>
</tbody>
</table>

7 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 and Provisioning Users and Groups to the Horizon Files Service,” on page 36.
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 Horizon Files service to that user or group. The Horizon Files service is the file storage and sharing service in Horizon Workspace.

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 Horizon Files service, but some of the Horizon Files 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 unless you use the command line to change the settings at the account level. 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. Select Catalog > Services.
3. Click Horizon Files.
4. Click Class of Service.
5. 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 Add a new COS.</td>
</tr>
<tr>
<td>Copy an existing COS as a starting point, and customize the settings.</td>
<td>Click Copy in the row of the existing COS.</td>
</tr>
</tbody>
</table>
6. Complete the form for the COS.

**NOTE** A value of zero (0) on the form indicates that parameter has no limit.

<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>Form Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>Minimum duration of time between quote warnings</td>
<td>The frequency with which the quota warning email message is sent.</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.</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 virtual 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 virtual users.</td>
</tr>
<tr>
<td>Public Expiration</td>
<td>The amount of time files are accessible on the Internet.</td>
</tr>
<tr>
<td>Domains Allowed or Not Allowed</td>
<td>This option enables you to restrict or allow virtual-user access to shared folders based on the virtual user’s domain.</td>
</tr>
<tr>
<td></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>- <strong>No Domain Policy</strong> to allow all external domains potential access to folders shared by Horizon Workspace users.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Allowed</strong> to specify domains from which virtual users can access shared folders. When this choice is selected, type the allowed domain names in the <strong>Allowed domains for external sharing</strong> field.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Restricted</strong> to specify domains from which virtual users are prevented from accessing shared folders. When this choice is selected, type the restricted domain names in the <strong>Restricted domains for external sharing</strong> field.</td>
</tr>
<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 Horizon Files service assigns new users evenly among all servers in the list. When you select more than one server, the Horizon Files 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 Horizon Files client 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 Horizon Files service.</td>
</tr>
</tbody>
</table>

7 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 and Provisioning Users and Groups to the Horizon Files Service,” on page 36.

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 Horizon Files 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 35.
- Configure one or more classes of service. See “Edit an Existing Class of Service,” on page 40 or “Create a Class of Service,” on page 42.

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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
</table>
| List all entitlements to the Horizon Files service. | 1 Click Catalog > Services.  
2 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. The provisioning status of each user and group is also listed. You can click the status to determine if users are properly provisioned. |
| Search for a specific user or group, and display the details page for that user or group. | 1 Click the Users & Groups tab.  
2 Click the Users tab or the Groups tab.  
3 Click the name of an individual user or group.  
The details page 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 unless you use the command line to change the settings at the account level. 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. Select Catalog > Services.
3. Click Horizon Files.
4 Click **Class of Service**.

5 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.
Providing Access to Mobile Workspaces

When your Horizon Workspace users use the appropriate Horizon Workspace client on their mobile devices, they can access the resources that you have authorized them to use. When accessed from the mobile device, that set of entitled resources is called the mobile workspace.

To use their mobile workspaces, users must install the appropriate client on their devices. The mobile workspace's available capabilities are determined by the device type, and the user's entitlements.

<table>
<thead>
<tr>
<th>Horizon Workspace Client</th>
<th>Device Type</th>
<th>Download Location</th>
<th>Workspace Capabilities</th>
</tr>
</thead>
</table>
| VMware Horizon Workspace Client for Android | Android | Google Play | Using the client app, the user can:  
  ■ Use the file sharing features, if you entitle the user to the Horizon Files service.  
  ■ Launch entitled Web applications.  
  ■ Install referred Android apps that you recommend to them. See Chapter 11, “Providing Access to Mobile Referred Applications,” on page 79. |
| VMware Horizon Workspace Client for iOS | iOS | Apple App Store | Using the client app, the user can:  
  ■ Launch entitled Web applications.  
  ■ Install iOS apps that you recommend to them. See Chapter 11, “Providing Access to Mobile Referred Applications,” on page 79.  
  Note: If you want your users to use the Horizon Workspace file sharing features on their iOS devices, add the Horizon Files app as a referred mobile app and entitle the users to the Horizon Files service. |
| VMware Switch | VMware Ready Android | Google Play | Using the client app, the user can provision and use a managed mobile workspace. See “Setting Up Managed Mobile Workspaces for VMware Ready Android Devices,” on page 49. |

This chapter includes the following topics:

■ “Setting Up Mobile Workspaces for iOS and Android Devices,” on page 48
■ “Setting Up Managed Mobile Workspaces for VMware Ready Android Devices,” on page 49
■ “Using Policies and Policy Sets,” on page 52
■ “Perform Actions on a User's Mobile Workspace,” on page 60
■ “Enable the Mobile Management Module,” on page 61
■ “Special Topics About Using Mobile Workspaces,” on page 61
Setting Up Mobile Workspaces for iOS and Android Devices

Mobile workspaces are for iOS devices and Android devices that are not VMware Ready Android devices.

To use a mobile workspace, users must install the Horizon Workspace app from the Apple App Store or Google Play on their mobile device. After installing the app, the user launches it, and enters the hostname for your Horizon Workspace system (the HostnameFQDN), username, and password. On iOS devices, the user also sets a passcode that is used when accessing the Horizon Workspace app. After the configuration is complete, the user can access the resources that you have entitled to that user.

Prerequisites

Verify that the appropriate resources for your Horizon Workspace users’ mobile workspaces have been added to your catalog.

Some of the default policy settings apply to the Horizon Workspace iOS app. 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 18.

Procedure

◆ Entitle the users or groups to the appropriate resources.

After a mobile workspace is provisioned to a user, you can perform actions on the provisioned workspace. See “Perform Actions on a User’s Mobile Workspace,” on page 60.

What to do next

On iOS devices, certain policies are applied to mobile workspaces by default. If you want to apply policies that are different than the default policies, see “Apply Policy Sets to a Group,” on page 59.

Entitling Users and Groups to Mobile Workspaces

To use a mobile workspace on their mobile devices, users must be entitled to the appropriate set of resources in your catalog. When they use the client application on their mobile device to connect to Horizon Workspace for the first time, Horizon Workspace sends the information about their entitled resources to that device. On iOS devices, Horizon Workspace also sends the relevant associated mobile policy settings.

The resource types that are used in mobile workspaces on Android and iOS devices are:

- Web applications
- Referred mobile applications
- Horizon Files service

**Note** On iOS devices, the Horizon Files app must be available to use the file sharing features. Add the Horizon Files app as a referred mobile app in your catalog and then entitle users to both the Horizon Files app and the Horizon Files service.

In many cases, the most effective way to entitle users to the resources for 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 76
- “Entitle Users and Groups to Mobile Referred Applications,” on page 86
- “Entitling and Provisioning Users and Groups to the Horizon Files Service,” on page 36
Setting Up Managed Mobile Workspaces for VMware Ready Android Devices

A managed mobile workspace is a mobile workspace on VMware Ready Android devices that is controlled by Horizon Workspace using policies. By applying policies, you can control what the user is allowed to do in their managed mobile workspace.

A managed mobile workspace can include managed files, managed mobile applications, and the ability to securely access Web applications. Managed mobile workspaces are deployed on VMware Ready Android devices.

To use a managed mobile workspace, users must install the VMware Switch client app from Google Play on their VMware Ready Android devices. The user must have a VMware Ready Android device to see the Switch application in Google Play. After installing the Switch application, the user launches it, and enters the hostname for your Horizon Workspace system (the HostnameFQDN), username, and password. Then the Switch application downloads and installs both the secure Android container that contains the managed workspace on the device and any managed 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 mobile workspace. On the initial access, the user accepts your end user terms and creates a passcode. This passcode is used to securely access the managed mobile workspace.

Setting up a managed mobile workspace that can be provisioned to users’ mobile devices involves several steps.

**Prerequisites**

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 18.

**Procedure**

1. **Importing Mobile Applications and Workspace Images into Your Catalog** on page 50
   
   To provide managed mobile workspaces for users’ VMware Ready Android devices, you must have at least one workspace image in your catalog. Then you import Android applications into your catalog as resources. Horizon Workspace includes a standard workspace image by default. Horizon Workspace also includes some Android applications in your catalog by default.

2. **Entitling Users and Groups to Managed Mobile Workspaces** on page 51
   
   To use a managed mobile workspace on their mobile devices, users must be entitled to the set of files and applications that make up that managed mobile workspace. When they use the client application on their mobile device to connect to Horizon Workspace for the first time, Horizon Workspace provisions their entitled managed mobile workspace to that device, as well as the relevant associated mobile policy settings.

After a managed mobile workspace is provisioned to a user, you can perform actions on the provisioned workspace, such as disabling it, resetting the password, and wiping it. See “Perform Actions on a User’s Mobile Workspace,” on page 60.

**What to do next**

Certain policies are applied to managed mobile workspaces by default. If you want to apply policies to the managed mobile workspaces that are different than the default policies, see “Apply Policy Sets to a Group,” on page 59.
Importing Mobile Applications and Workspace Images into Your Catalog

To provide managed mobile workspaces for users' VMware Ready Android devices, you must have at least one workspace image in your catalog. Then you import Android applications into your catalog as resources. Horizon Workspace includes a standard workspace image by default. Horizon Workspace also includes some Android applications in your catalog by default.

Import a Workspace Image into Your Catalog

A 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 a 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 workspace image you want to import. Workspace images are provided in a ZIP file format from VMware. Only workspace images provided by VMware are supported. Horizon Workspace includes at least one standard workspace image.

Procedure

1. Log into the Administrator Web interface as an administrator.
2. Select Catalog > Mobile Applications.
3. Click Workspace Image.
4. Click Choose File to browse to and select the workspace image’s ZIP file.
5. (Optional) Specify a description.
6. Click Upload.
   The upload might take some time.

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

Import a Mobile Application into Your Catalog

To make an Android app available for inclusion in a managed mobile workspace, you must first import it into your catalog as a resource.

IMPORTANT Horizon Workspace includes some Android applications in your catalog by default. 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’ managed mobile workspaces. The version number of the application is provided on its resources page. See “View Horizon Workspace Resources,” on page 32.

To update an imported Android application, import 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 managed mobile workspace:
- The Google Maps API
- Android Cloud to Device Messaging (C2DM)
Procedure

1. Log in to the Administrator Web interface as an administrator.
2. Select Catalog > Mobile Applications.
   A window opens in which you choose the mobile application's file.
4. Click Choose File, and locate and select the file.
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.

Entitling Users and Groups to Managed Mobile Workspaces

To use a managed mobile workspace on their mobile devices, users must be entitled to the set of files and applications that make up that managed mobile workspace. When they use the client application on their mobile device to connect to Horizon Workspace for the first time, Horizon Workspace provisions their entitled managed mobile workspace to that device, as well as the relevant associated mobile policy settings.

In many cases, the most effective way to entitle users to managed mobile applications, and the 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 workspace images is more appropriate.

There are two available methods for entitling users and groups to managed mobile workspaces.
<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</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. In the Workspace Images section, click the workspace image.  
   On the 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.  
3. Click Add group entitlement or Add user entitlement as appropriate.  
4. 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.  
5. Click Save.  
6. Click Done on the Entitlements page.  
7. In the Mobile Applications section, click the icon for the imported Android application to which you want to entitle users and groups.  
   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.  
8. Click Add group entitlement or Add user entitlement as appropriate.  
9. 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.  
10. Click Save.  
11. 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. |
| Access the details page for the user or group, and add the workspace image and mobile application entitlements from that page. | 1. Click the Users & Groups tab.  
2. Click the appropriate tab: Users or Groups.  
3. Click the name of an individual user or group.  
   On the user's or group's page, the Entitlements tab is selected by default.  
4. 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 Email app is entitled by default, and you cannot change this setting.  
5. Click Save. |

**Using Policies and Policy Sets**

Use policies to control the required behavior of the mobile workspace and the actions that users can and cannot perform in the mobile workspace.

Policies determine capability-related settings for users' mobile workspaces. 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.

What you can control in the mobile workspace using policies depends on the type of mobile device. Policies are not used for mobile workspaces on Android devices that are not VMware Ready devices.
Control

Applicable Mobile Device Type

The required behavior of the mobile workspace. For example, you can require that a workspace be automatically wiped if it fails to communicate with the server within a specified time interval.

VMware Ready Android, iOS

The actions that users can and cannot perform in their mobile workspace and its managed applications. For example, you can prevent the user from using the on-device camera with the mobile workspace and its managed applications.

VMware Ready Android

The policies that you can set in Horizon Workspace are grouped into four categories:

- Data containment policies
- Workspace lifetime policies
- Passcode policies
- Secure network access policies

One policy set from each category is applied to a group. Therefore, every group in Horizon Workspace has four policy sets applied to it, one from each category.

Horizon Workspace includes standard policy sets, and applies 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 Policy Set. See “Standard Policy Sets Included In Horizon Workspace,” on page 53. 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 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 Policy Set. 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 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 Base Policy Set’s name.
Data Containment Policies

Data containment policies control the access and flow of data within the managed mobile workspace, to and from the managed applications that are installed on the mobile device.

### Table 8-1. Policies that control behaviors related to data containment

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
<th>Applicable devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow copy &amp; paste</td>
<td>When set to <strong>Yes</strong>, users can copy and paste between their personal applications and the managed mobile applications.</td>
<td>VMware Ready Android</td>
</tr>
<tr>
<td>Allow use of camera</td>
<td>When set to <strong>Yes</strong>, users can use the camera in the managed mobile workspace. When set to <strong>No</strong>, 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>
<td>VMware Ready Android</td>
</tr>
<tr>
<td>Enable ADB</td>
<td>Determines whether Android Debug Bridge (ADB) is enabled. If enabled, ADB commands can be executed in the managed mobile workspace.</td>
<td>VMware Ready Android</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 in the device.</td>
<td>VMware Ready Android</td>
</tr>
<tr>
<td>Location accuracy</td>
<td>Controls the accuracy to which applications in the managed workspace can track the device’s location.</td>
<td>VMware Ready Android</td>
</tr>
</tbody>
</table>

Workspace Lifetime Policies

Workspace lifetime policies control what happens to the mobile workspace when the mobile device has not appropriately communicated with the Horizon Workspace server.

These policies control the interval at which a mobile workspace’s lease is renewed, and when an automatic disable or automatic wipe is performed after lease renewal failures. These policies protect the administrator’s ability to control the workspace on the mobile device by automatically restricting access if the client on the device has not communicated with the server.
### Table 8-2. Policies that control behaviors related to workspace lifetime

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
<th>Applicable devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lease interval</strong></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 Mobile Workspaces,” on page 61. A value of less than 15 minutes can cause noticeable battery consumption. <strong>Note</strong>: For iOS devices, the lease interval is always set to 15 minutes by default, and is not set by this Lease interval value.</td>
<td>VMware Ready Android, iOS</td>
</tr>
<tr>
<td><strong>Auto disable</strong></td>
<td>The amount of time after which a mobile workspace will be automatically disabled if the workspace 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, the workspace is disabled. The disabled workspace continues its standard attempts to contact the server. Access is automatically restored the next time that contact is successful and the lease is renewed.</td>
<td></td>
</tr>
<tr>
<td><strong>Auto wipe</strong></td>
<td>The amount of time after which a workspace will be automatically wiped if the workspace has not contacted the management server. A value of at least seven days is recommended, unless your company has a requirement for stricter settings.</td>
<td></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 passcode strength, frequency of expiration, and the circumstances for which the mobile workspace is automatically locked if the correct passcode is not entered.

The user must enter the passcode to use the mobile workspace.

On VMware Ready devices, the workspace password protection policy is also used for the VMware Email application in the managed workspace. Therefore, you should set the workspace password protection policy to the same strength and expiration settings as your email server’s policy settings.
### Table 8-3. Policies that control behaviors related to passcodes

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
<th>Applicable devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min length</td>
<td>Sets the minimum length of the passcode.</td>
<td>VMware Ready Android, iOS</td>
</tr>
<tr>
<td>Min digits</td>
<td>Sets the minimum number of digits the passcode must have.</td>
<td></td>
</tr>
<tr>
<td>Min letters</td>
<td>Sets the minimum number of letters the passcode must have.</td>
<td></td>
</tr>
<tr>
<td>Min uppercase letters</td>
<td>Sets the minimum number of uppercase letters the passcode must have.</td>
<td></td>
</tr>
<tr>
<td>Min lowercase letters</td>
<td>Sets the minimum number of lowercase letters the passcode must have.</td>
<td></td>
</tr>
<tr>
<td>Min special characters</td>
<td>Sets the minimum number of non-alphanumeric characters the passcode must have.</td>
<td></td>
</tr>
<tr>
<td>Passcode timeout</td>
<td>Sets the amount of grace time for which a user can re-enter the mobile workspace without having to re-enter the passcode.</td>
<td></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 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 Attempts before lockout setting before being locked out of the workspace for a second five minute period. If the user enters a third set of incorrect attempts, up to the number set by the Attempts before lockout setting, the workspace is wiped. For example, when Attempts before lockout 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>
<td></td>
</tr>
<tr>
<td>Passcode expiration</td>
<td>Sets the amount of time after which the passcode expires and must be changed.</td>
<td></td>
</tr>
</tbody>
</table>
Secure Network Access Policies

These policies determine how the managed mobile workspace’s applications access the corporate network from the device.

**Note** When you specify Yes for the Require VPN policy setting, a user with a VMware Ready device must perform the following steps before launching the Switch application to provision the workspace:

1. Install the appropriate VPN client application from Google Play
2. Create a connection using the VPN connection settings appropriate for that workspace.

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 users with the required VPN information, which includes the name of the appropriate VPN client and the connection information.

### Table 8-4. Policies that control how managed applications access the corporate network

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
<th>Applicable Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require VPN</td>
<td>When set to Yes, the managed mobile workspace uses VPN for network access to the corporate network. When set to Yes, the user must have the appropriate VPN client installed from Google Play and configured with a connection that uses the appropriate corporate settings before provisioning the device. Otherwise, a policy violation occurs and the user cannot open the workspace. Obtain the name of the appropriate VPN client and the connection information for your organization.</td>
<td>VMware Ready Android</td>
</tr>
<tr>
<td>VPN client</td>
<td>Specifies the VPN client software used in the managed mobile workspace. Select the VPN client, and type a server name in the VPN Server URL field. If you select Cisco AnyConnect or F5 Edge, your Horizon Workspace users must manually enter your organization’s VPN concentrator URL in their VPN client. If you select Juniper Junos Pulse, you must type the VPN server name in the VPN server URL field. <strong>Note</strong> When Juniper Junos Pulse is selected, the VPN client application in the workspace does not activate a VPN connection unless the user first launches the Juniper Junos Pulse VPN client on the personal phone side and accepts the End User License Agreement (EULA).</td>
<td></td>
</tr>
<tr>
<td>VPN server URL</td>
<td>Type the VPN server name, using either a symbolic name format (such as vpn.mycorporation.com) or a dotted IP address (such as 127.0.0.1).</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-4. Policies that control how managed applications access the corporate network (Continued)

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
<th>Applicable Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a proxy</td>
<td>When set to <strong>Yes</strong>, a proxy server is used for the VPN connection. Type a proxy server name and port number in the <strong>Proxy server URL</strong> field.</td>
<td></td>
</tr>
</tbody>
</table>

| Proxy server URL | Type the proxy server name and port number, using either a symbolic name format (such as `myproxy.mycompany.com:3128`) or a dotted IP address (such as `127.0.0.1:3128`). |                |

## 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 Policy Set, are applied to all groups, which applies the settings to every Horizon Workspace user. 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 the **Policies** tab.
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 the managed mobile workspace’s data. See “Data Containment Policies,” on page 54.</td>
</tr>
<tr>
<td>Workspace Lifetime Policy Set</td>
<td>Policies that determine how a mobile workspace is protected when it has not communicated with the Horizon Workspace server over a period of time. See “Workspace Lifetime Policies,” on page 54.</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 workspace is automatically locked or wiped if the correct passcode is not entered. See “Passcode Policies,” on page 55.</td>
</tr>
<tr>
<td>Secure Network Access Policy Set</td>
<td>Policies that determine how the managed mobile workspace’s applications access the corporate network from the device. See “Secure Network Access Policies,” on page 57.</td>
</tr>
</tbody>
</table>

4. In the **Policy Set Name** text box, type a name for the new policy set.
5. In the **Description** text box, type a meaningful description.
6. In the **Enable Policy** column, select the check box for the policy that you want to set, and then specify the policy setting. For example, to prevent use of the camera in the managed mobile workspace, select **No** for the **Allow use of camera policy** setting.

    Each policy setting’s row displays icons that indicate to which type of mobile device the policy applies.

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 Policy Sets to a Group,” on page 59.

Apply Policy Sets to a Group

You can apply policy sets to a group. Depending on the type of mobile device, the policy settings are applied to the mobile workspaces of 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 5, “Managing Users and Groups,” on page 17.

Create the policy sets that you want to associate with the group. See “Create Mobile Policy Sets,” on page 58.

Procedure

1. Log in to the Administrator Web interface as an administrator.
2. Select Users & Groups > Groups.
3. Click the group name to which you want to apply policy sets.
4. Click Applied Mobile Policy Sets.
   The mobile policy sets currently applied to the group are listed according to the policy category.
5. Click Select Mobile Policy Sets.
6. 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, named Base Policy Set, for each policy category. Each category’s Base Policy Set 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 Policies page. See “Standard Policy Sets Included In Horizon Workspace,” on page 53.

7. Click Save.
Perform Actions on a User's Mobile Workspace

After a mobile workspace is provisioned to a user, you can perform actions on the provisioned workspace, such as disabling it, resetting the passcode, and wiping it. You can also collect log information from the workspace to help VMware Support diagnose issues.

Mobile workspaces on VMware Ready Android and iOS devices can be disabled, enabled, or wiped. You can also reset the user's passcode for those workspaces, if the user has forgotten it. Mobile workspaces on other device types can be deleted.

**NOTE** On iOS devices, when you enable a previously disabled workspace or reset a password, a timeout period must elapse before the client can poll the Horizon Workspace server to renew the lease, and re-enable the workspace or reset the password on the device. As a result, the user cannot use the client app on the device until the time has elapsed and the client renews the lease after the timeout period. The timeout period lasts about fifteen minutes.

The first time the user launches the Horizon Workspace app after you have re-enabled the workspace, an error message stating that the workspace is disabled might appear. If this occurs, have the user launch the Horizon Workspace app a second time.

**Prerequisites**

Verify the user has a provisioned mobile workspace. In the Administrator Web interface, open the page for the user and click Workspaces. The user's mobile workspaces are listed in the Mobile Workspaces section.

**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 mobile workspace.
6. 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>On Android devices that are not VMware Ready Android devices, this action unlinks the mobile device from the Horizon Workspace user's account. The device no longer has access to the user's account. This action does not prevent the user from reconfiguring the Horizon Workspace app with their account information.</td>
</tr>
<tr>
<td>Wipe Workspace</td>
<td>On VMware Ready Android devices, this action removes the workspace and its associated applications. On iOS devices, this action removes the user's access to the Horizon Workspace app and unlinks the iOS device from the Horizon Workspace user's account. For VMware Ready devices, this action does not prevent the user from downloading and installing a new managed mobile workspace. To reinstall a mobile workspace on an iOS device, the user must delete the Horizon Workspace iOS app and reinstall it, and then repeat the setup process.</td>
</tr>
<tr>
<td>Disable Workspace</td>
<td>On VMware Ready Android devices, this action disables the managed mobile workspace. If the user newly provisions the workspace, the user is prevented from accessing a newly provisioned workspace and its associated applications until you enable the workspace using the Enable Workspace button. On iOS devices, this action disables the Horizon Workspace app. The user cannot access the Horizon Workspace app until you enable the workspace using the Enable Workspace button.</td>
</tr>
<tr>
<td>Enable Workspace</td>
<td>Enables a previously disabled mobile workspace.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reset Password</td>
<td>Resets the user’s passcode for accessing the mobile workspace.</td>
</tr>
<tr>
<td>Retrieve Logs</td>
<td>If the user consents, the workspace sends diagnostic information to the management server when the lease is renewed.</td>
</tr>
</tbody>
</table>

### Enable the Mobile Management Module

To enable the capabilities in Horizon Workspace that are used with both managed mobile applications and referred mobile applications, you must enable the Mobile Management module.

#### 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 12 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 mobile workspaces according to your organization’s needs, as described in Chapter 8, “Providing Access to Mobile Workspaces,” on page 47.

### Special Topics About Using Mobile Workspaces

As appropriate for your organization’s needs, use this information to advise your Horizon Workspace users who use their workspaces on mobile devices.

### Horizon Workspace Server Leasing Process and Mobile Workspaces

On iOS and VMware Ready Android devices, Horizon Workspace uses a leasing process to remotely manage the lifecycles of the mobile workspaces. Using this leasing process, the client application on the mobile device communicates with the Horizon Workspace server to receive updates of policies and entitlements, and to respond to administrative commands that you issue using the Administrator Web interface, such as wiping the mobile workspace.

On iOS and VMware Ready Android devices, the mobile workspaces use the following client applications.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Client Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS devices</td>
<td>Horizon Workspace Client for iOS</td>
</tr>
<tr>
<td>VMware Ready devices</td>
<td>VMware Switch Android app</td>
</tr>
</tbody>
</table>
The client application polls the Horizon Workspace server to obtain a lease from the server. The lease brings information to the client about policies, entitlements, and any administrative commands that have been issued to the client's corresponding workspace. Each time the client 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 the client 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 the client receives it.

### Lease Renewal Attempts on iOS Devices

On iOS devices, the client 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, and launches the Horizon Workspace app, the client polls the server to renew the lease.</td>
</tr>
<tr>
<td>The user presses the home button and power button, turning off the display.</td>
<td>When the user reawakens the display and launches the Horizon Workspace app, the client polls the server to renew the lease.</td>
</tr>
<tr>
<td>The workspace passcode times out.</td>
<td>The user must enter the workspace passcode to use the Horizon Workspace app, and the client polls the server to renew the lease. The passcode timeout is set by the <strong>Passcode timeout</strong> policy setting. See “Passcode Policies,” on page 55.</td>
</tr>
<tr>
<td>The user manually forces the client to poll the server.</td>
<td>In the Horizon Workspace app, when the user touches <strong>Settings &gt; Last Lease</strong>, the client polls the server to renew the lease.</td>
</tr>
</tbody>
</table>

**NOTE** Except for manual renewals, the client does not poll the server if less than fifteen minutes have elapsed since the previous lease renewal. For example, in the following sequence, the lease is not renewed in the last step.

1. The user presses the home button and power button, and then immediately reawakens the display and launches the Horizon Workspace app. The client polls the server to renew the lease, and the lease is renewed.

2. Five minutes later, the user again presses the home button and power button, and then immediately reawakens the device and launches Horizon Workspace app. The client does not poll the server this time, because less than fifteen minutes have passed since the previous renewal.

The client always polls the server when the user manually forces the lease renewal using the **Last Lease** setting.

### Lease Renewal Attempts on VMware Ready Devices

On VMware Ready devices, the client 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 the client 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 the client is running, it polls the server to renew the lease.</td>
</tr>
<tr>
<td>The managed workspace passcode times out.</td>
<td>The user must enter the workspace passcode to use the managed workspace and its apps, and the client polls the server to renew the lease. The passcode timeout is set by the <strong>Passcode timeout</strong> policy setting. See “Passcode Policies,” on page 55.</td>
</tr>
</tbody>
</table>
### Situation Description

The user manually forces the client to poll the server by syncing the account associated with the Switch app on the device.

Typically, the user can view the account in the accounts list on the device, and touch **Sync now** to sync the Switch app with the Horizon Workspace server.

The time elapsed since the last successful lease renewal exceeds the lease interval.

The lease interval is set in the **Lease interval** policy setting, and it determines how frequently the client attempts to renew the lease. When the amount of time that has elapsed since the last lease renewal exceeds the lease interval, the client polls the server. See “Workspace Lifetime Policies,” on page 54.

### Failing to Renew a Lease

The lease renewal process can fail, such as when there is no network connectivity between the client and the server or the client 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 54. When the user launches the client app, the time periods for **Auto disable** and **Auto wipe** are checked.

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Result</th>
</tr>
</thead>
</table>
| **Auto disable** | If there is no successful lease renewal before this time period elapses, the client is automatically disabled.  
On VMware Ready devices, the disabled client 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.  
On iOS devices, the disabled client is dormant until the user tries to use the Horizon Workspace app. Then the client polls the server to try to renew the lease. Access is automatically restored the next time the client successfully renews the lease.  
*Note* Under slow networking conditions, the iOS device might display a message that says the workspace is disabled. In this situation, the user can try launching the Horizon Workspace app again until the client reaches the server. |
| **Auto wipe** | If there is no successful lease renewal before this time period elapses, the mobile workspace is automatically wiped.  
The client application remains installed on the device. To reprovision a mobile workspace on the device, the user must launch the client application and repeat the setup process.  
*Note* On iOS devices, the user must delete the Horizon Workspace app and reinstall it before repeating the setup process. |

*Note* If the client application 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 the client application starts up or is launched, it makes a final attempt to renew the lease. If that attempt fails to renew the lease, the mobile workspace is automatically wiped from the device.
Establish SSL Trust Between Horizon Workspace and Mobile Devices

The Secure Sockets Layer (SSL) protocol protects communications to Horizon Workspace. If your Horizon Workspace system is configured to use a self-signed certificate, or with a certificate that is not signed by a standard Certificate Authority (CA), the mobile devices must install the certificate to establish trust between Horizon Workspace and the devices.

During the initial configuration of Horizon Workspace, the Configurator randomly generates a self-signed Horizon Workspace root CA certificate. For production systems, you typically replace this self-signed certificate with a certificate signed by a standard Certificate Authority (CA). For proof-of-concept systems, or if you are using certificates that are not signed by a standard CA, the mobile devices can establish trust with your Horizon Workspace system if the certificates are installed on the devices.

**NOTE** If you have a load balancer configured for your Horizon Workspace system, the root CA certificate on the load balancer must be installed on the mobile devices if the certificate is not signed by a standard CA.

To install the Horizon Workspace root CA on to a mobile device, use a browser on the device to browse to the location for the root CA file on the gateway-va, and install the certificate on the device.

**Procedure**

1. On the mobile device, launch a browser app and go to the location `http://gatewayhostname/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.

2. 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.

Configuring the Horizon Workspace iOS App Over Networks That Use Automatic Redirects

Locations such as public Wi-Fi hotspots often redirect requests automatically to the hotspot provider’s login screen, for example to accept the provider’s terms of usage, before completing the Internet connection to the mobile device. To ensure the smoothest configuration process at a networked location, first satisfy the network provider’s login process to connect the device to the Internet before launching the Horizon Workspace iOS app.

The typical example of when a mobile device user encounters a network that uses automatic redirects is when the user is at a hotel and opens a browser app to access a Web site over the Wi-Fi network. The hotel’s login screen appears and usually has a button or similar method for the user to accept terms and subsequently access the Internet.

If a user is at such a location, and is configuring the Horizon Workspace iOS app for the first time, ensure the device is connected to the Internet and can reach the Horizon Workspace system before launching the Horizon Workspace iOS app.

1. Connect the device to the provider’s network by following the provider’s instructions for using their network, for example by choosing a Wi-Fi SSID and connecting to it. If the provider’s login screen is automatically displayed at this step, satisfy the requirements to use the provider’s network to reach the Internet.

2. Open a browser app on the device and attempt to reach the Horizon Workspace server URL. If the automatic redirect displays the provider’s login screen at this step instead of at the previous step, satisfy the requirements to use the provider’s network.
3 Verify the device can connect to the Horizon Workspace system by typing the URL into the browser again. If the Internet connection exists, the Horizon Workspace home page appears.

4 Launch the Horizon Workspace iOS app by touching its icon, and begin the configuration process.
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 client on their systems and devices to access their entitled Horizon View desktop pools.

**Note** Access to Horizon View desktop pools is provided only in the Horizon Workspace Web client and the Horizon Workspace Client for iOS running on iPads.

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

**Note** You can add the Horizon View Client for iOS to your catalog as a mobile referred app and then entitle it to your users so that they are alerted to install it. See Chapter 11, “Providing Access to Mobile Referred Applications,” on page 79.

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 after Integrating Horizon View with Your Horizon Workspace System,” on page 68.

This chapter includes the following topics:

- “Enable the View Module after Integrating Horizon View with Your Horizon Workspace System,” on page 68
- “View User and Group Entitlements to Horizon View Desktop Pools,” on page 68
- “View the Connection Information for a Horizon View Desktop Pool,” on page 69
Enable the View Module after Integrating Horizon View with Your Horizon Workspace System

If you did not enable the View 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.

Prerequisites
Verify that your Horizon Workspace system is integrated with your Horizon View system 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 View module, click Enable this module.

The View module is enabled.

If a message displays telling you to go to all connectors, then the prerequisite 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 68.

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 | a. Select Catalog > View Pools.  
  desktop pool.            | b. 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 | a. Click the Users & Groups tab.  
  user or group.           | 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. Select Catalog > View Pools and click a Horizon View desktop pool.
3. Click the Details tab.
4. 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 when Horizon View Desktops Have the Horizon Workspace Client for Windows Installed

To reduce resource usage from the re-syncing of data, you can disable the Horizon Files service for a Horizon Workspace client for Windows that is installed in a Horizon View desktop. Users can continue to use the Horizon Workspace client in their Horizon View desktops to access the other features provided in the client.

Problem

When a Horizon View desktop has the Horizon Workspace client for Windows 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

The resource usage occurs because the user data is re-synced at run time, when the Horizon View desktop session starts.

You can avoid the resource usage by disabling the Horizon Files feature for the installed Horizon Workspace client. You disable the feature by defining a string value in the Windows registry in the Horizon View desktop.
Solution

1. In the Windows operating system for the Horizon View desktop, run regedit to open the Windows registry.

2. In the registry, go to the appropriate path.

<table>
<thead>
<tr>
<th>Windows version</th>
<th>Registry path</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Horizon Workspace\Config</td>
</tr>
<tr>
<td>64-bit</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware Horizon Workspace\Config</td>
</tr>
</tbody>
</table>

3. Create a string value named EnableData, and set it to the appropriate value.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableData &lt; 0 or EnableData &gt; 1 or EnableData is not set</td>
<td>Horizon Files is disabled in the client</td>
</tr>
<tr>
<td>EnableData == 1</td>
<td>Horizon Files is enabled in the client</td>
</tr>
</tbody>
</table>

**Note** The user must be entitled to the Horizon Files service in the Horizon Workspace server to have the capability to sync files in the Horizon Workspace client.
Providing Access to Web Applications

You can entitle Horizon Workspace users to external Web applications.

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

- The Web application supports federation standards SAML 1.1 or 2.0.
- 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 71
- “Overview of Adding Web Applications to Your Organization’s Catalog,” on page 72
- “Entitle Users and Groups to Web Applications,” on page 76

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 12 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 “Overview of Adding Web Applications to Your Organization’s Catalog,” on page 72.
Overview of Adding Web Applications to Your Organization's Catalog

After the Web Applications module is enabled, you can add Web applications to your organization's catalog to provide access to those Web applications for your Horizon Workspace users and groups. Adding a Web application to your catalog involves creating an entry in the catalog and configuring the entry that points Horizon Workspace to an existing Web application.

When you add an entry for a Web application to the catalog, you are adding an application record. The application record is a template that Horizon Workspace uses to establish a connection with the Web application by using Security Assertion Markup Language (SAML). The form for the application record includes a field for entering the URL to the existing Web application.

On the Catalog page of the Administrator Web interface, the following methods are available for entering an appropriate application record in your catalog for a Web application.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From your Global Catalog</td>
<td>Horizon Workspace includes access to several default Web applications, available in the Global Catalog, that you can add to your catalog. The application record is partially completed for Global Catalog applications. 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 provided in the Global Catalog. The application record for Web applications that Horizon Workspace does not include are slightly more generic than that of Global Catalog applications. In this situation, you must create the application record form.</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. You then import the ZIP file to the production deployment.</td>
</tr>
</tbody>
</table>

After you add Web applications to the catalog, you can configure them individually.

Add a Web Application to Your Catalog from the Global Catalog

The Web applications in the Global Catalog are populated with some information in their application records. When you add a Web application to your catalog from the Global Catalog, you must provide additional information to complete the application record.

When you add a Web application to your catalog, you are creating an entry in the catalog 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. The Global Catalog is populated with several Web applications and mobile referred applications. When you add a Web application from the Global Catalog, the application record is partially completed with information about that Web application, and you complete the rest of the form.

Prerequisites

Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 71.

Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Select Catalog > Web Applications.
3. Select Web Application > from your Global Catalog.
4 Click the icon of the Web application in the Global Catalog to add to your organization’s catalog. The application record is added to your catalog, and the system displays the record’s Details page. Because Web applications in the Global Catalog have partially completed application records, information like the name and authentication profile are already specified and appear in the form.

5 (Optional) Customize the information on the Details page for your organization’s needs. 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.

Items on the page are populated with information specific to the Web application. 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, 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>
<tr>
<td>Authentication Profile</td>
<td>Displays the SAML profile that this Web application uses.</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.

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>Entitles users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Configures license tracking. Add license information for the application to track license use in reports.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Selects 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 might be required by an application.</td>
</tr>
</tbody>
</table>

**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 76.
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 Global 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 71.

Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Select Catalog > Web Applications.
3. Select 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>
<tr>
<td>Authentication Profile</td>
<td>Specify the SAML profile for the Web application.</td>
</tr>
</tbody>
</table>

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>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 76 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 Global Catalog,**” on page 72 or “**Add a Web Application to Your Catalog by Creating a New Application Record,**” on page 74.

**Prerequisites**

Verify the following items:

- The Web Applications module is enabled. See “**Enable the Web Applications Module to Provide Web Application Access,**” on page 71.
- 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 the icon of the Web application in to export.
4 Click **Export this Application**.
5 Click **Export**.
6 Save the zipped application bundle to your local system.
7 Log in to the Horizon Workspace Administrator Web interface of the Horizon Workspace instance to which to import the Web application.

8 Select Catalog > Web Applications Catalog tab.

9 Select Web Application > import a zip or jar file.

10 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.

11 Edit the information on the Details, Configuration, Entitlements, Licensing, and Provisioning pages as necessary.

**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 76.

### 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**

- Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 71.

- Add one or more Web applications to your catalog. See “Overview of Adding Web Applications to Your Organization’s Catalog,” on page 72.

**Procedure**

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

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

The selected user or group is now entitled to use the Web application.
You entitle Horizon Workspace users to a mobile referred application by pointing them to a mobile application that already exists in Google Play or Apple App Store. Through this process you are communicating to users that a mobile application is recommended for download to their mobile devices and for use on the enterprise’s network.

To enable users to access a mobile referred application through Horizon Workspace, perform the following prerequisites:

- Verify that the mobile application exists in Google Play or Apple App Store.
- Verify that the mobile application satisfies your enterprise’s requirements. When you add a mobile referred application to your catalog, you should verify that no issues exist, such as interoperability issues, configuration issues, version compatibility issues, and so on, to ensure a friendly user experience on your enterprise’s network.
- Enable the Mobile Management module. Enabling the Mobile Management module allows you to add mobile referred applications to your catalog using the Horizon Workspace Administrator Web interface. See “Enable the Mobile Management Module,” on page 61.
- Verify that users install the appropriate client on their mobile devices: Horizon Workspace Client for Android or Horizon Workspace Client for iOS.

This chapter includes the following topics:

- “Overview of Mobile Referred Applications,” on page 79
- “Entitle Users and Groups to Mobile Referred Applications,” on page 86

**Overview of Mobile Referred Applications**

When you add a mobile referred application as a resource in your catalog, you create a way to recommend a mobile application to your Horizon Workspace users for download and installation on their mobile devices. The mobile application is listed in a user’s Horizon Workspace client application when you entitle the user to that mobile referred application in your catalog. To use the application on their devices, Horizon Workspace users must download and install the application from the appropriate store to a compatible mobile device.

**Adding Mobile Referred Applications to Your Catalog**

After you have enabled the Mobile Management module, you can add mobile referred applications to your catalog. When you add a mobile referred application to your catalog, you are implying that you have tested the mobile application and that your enterprise supports the application’s use on the enterprise’s network.
After you entitle users to a mobile referred application, it is made available to the entitled users through the Horizon Workspace client on their mobile device if the application is supported by the mobile device. See “User Access to Mobile Referred Applications,” on page 80. When those users who are entitled to a mobile referred application choose to install the application on their device, the application appears on their mobile phone launcher after installation. From that point forward, the users launch the installed mobile application directly from their mobile phone launcher, instead of launching the mobile application from within the Horizon Workspace client application.

You can add a mobile referred application to your catalog using one of the following options on the Catalog page of the Administrator Web interface.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Mobile Application &gt; from your Global Catalog.</td>
<td>Horizon Workspace provides access by default to several mobile referred applications, available in the Global Catalog, that you can add to your catalog. Each mobile referred application in the Global Catalog has an application record that points to the actual mobile application in either Apple App Store or Google Play.</td>
</tr>
<tr>
<td>Select Mobile Application &gt; from Apple App Store.</td>
<td>You can add mobile applications available in Apple App Store to your catalog that are not provided in the Global Catalog. <strong>Note:</strong> If you want your users to use the Horizon Workspace file sharing services on their iOS devices, add the Horizon Files app that is available in the Apple App Store.</td>
</tr>
<tr>
<td>Select Mobile Application &gt; from Google Play.</td>
<td>You can add mobile applications available in Google Play to your catalog that are not provided in the Global Catalog.</td>
</tr>
</tbody>
</table>

**User Access to Mobile Referred Applications**

For Horizon Workspace users to see a mobile referred application as available in the Horizon Workspace client on their device, the following requirements must be met.

- You must entitle the user to the mobile referred application.
- The user’s device must meet the minimum requirements of the mobile referred application, as documented on its page in the Apple App Store or Google Play.

Read the requirements information for the mobile referred application on its page in the Apple App Store or Google Play. If a particular user’s device does not meet the minimum requirements of the mobile referred application, as stated in its page in the Apple App Store or Google Play, that mobile referred application will not display in the list in the Horizon Workspace client on that user’s mobile device.

The following examples illustrate how the compatibility requirements work for mobile referred applications.

**Example of device compatibility and a referred Android application**

The Google Play page for an Android application named **ABC** states that it requires **Android 3.0 and up**. An entitled user that has the Horizon Workspace Client for Android running on an Android 3.0 device sees the **ABC** app listed in that user’s Horizon Workspace client. However, an entitled user that has the Horizon Workspace Client for Android running on an Android 2.3 device does not see the **ABC** app listed in the Horizon Workspace client because that user’s device is running Android 2.3, which is a lower Android version than the **ABC** app requires.
To verify compatibility requirements for a referred Android application in your catalog, click the Android application's icon on the Catalog page, click Configuration, and examine the value in the Minimum API Level field. Click View latest Android API levels to match the API level to the Android level, for example, Android 2.3.3 matches API level 10.

The iTunes page for an iOS application named MNO states that it requires iOS 6.1 or later. An entitled user that has the Horizon Workspace Client for iOS running on an iOS 6.1 device sees the MNO app listed in that user's Horizon Workspace client. However, an entitled user that has the Horizon Workspace client running on an iOS 6.0 device does not see the MNO app listed in the Horizon Workspace client because that user's device is running iOS 6.0, which is a lower version than the MNO app requires.

Add a Mobile Referred Application to Your Catalog from the Global Catalog

Each mobile referred application in the Global Catalog uses an application record to point to the respective application in the Apple App Store or Google Play. When you add a mobile referred application from the Global Catalog to your catalog, you must activate the application record by saving it either in its default state or after you customize it.

When you add mobile referred applications to your catalog you are actually creating a link in your catalog to the mobile application in the Apple App Store or Google Play. Through this process you can recommend mobile applications to users for download. Once users download and install a mobile referred application, they do not use the Horizon Workspace client on their mobile device to access the application. They can launch the application using its icon on their mobile device.

The Global Catalog comes populated with several mobile referred applications.

Prerequisites

Enable the Mobile Management module. See “Enable the Mobile Management Module,” on page 61.

Procedure

1 Log in to the Administrator Web interface.
2 Select Catalog > Mobile Applications.
3 Select Mobile Application > from your Global Catalog.
4 Click the icon of the mobile referred application in the Global Catalog that you want to add to your catalog.

The mobile referred application is added to your catalog, and the application’s resource page is displayed.

The items in an application’s resource page are pre-populated with information specific to the mobile application. The available information varies slightly depending on the operating system of the mobile application.

5 Customize the basic information about the application, according to the needs of your organization, and click Save.

For some mobile referred applications in the Global Catalog, some fields are not customizable.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Edit the name of the application.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. Edit the description of the application.</td>
</tr>
</tbody>
</table>
6 Click the **Configuration** tab, edit the application’s configuration details as necessary, and click **Save**.

The application's configuration details are pre-populated with information specific to the mobile application. The details vary slightly depending on the operating system of the mobile application.

### Table 11-1. Application Configuration Details for Android Applications

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>If necessary, edit the ID or package name for this application. Use a browser to search the Google Play Web site for the application. Find the application ID within the Google Play URL of the application. For example, an application called exampleApp might use the following URL: <a href="https://play.google.com/store/apps/details?id=com.exampleApp.android">https://play.google.com/store/apps/details?id=com.exampleApp.android</a>. For the preceding example, the application ID is as follows: com.exampleApp.android.</td>
</tr>
<tr>
<td>Google Play URL</td>
<td>This field displays the URL to install this mobile referred application from Google Play. If necessary, edit the URL for the application. Use a browser to search the Google Play Web site for the application. For example, an application called exampleApp might use the following URL: <a href="https://play.google.com/store/apps/details?id=com.exampleApp.android">https://play.google.com/store/apps/details?id=com.exampleApp.android</a>. Using the URL for the application, you can create the install URL by starting with the word market. For example, market://details?id=com.exampleApp.android. Click <strong>Check App</strong> to open the displayed URL and verify it leads to the application you want.</td>
</tr>
<tr>
<td>Minimum API Level</td>
<td>If necessary, edit the minimum Android API level upon which the application can operate. The Android API level is directly associated with the Android version. If a specific Android version is required for an application, find the required version number on the Google Play page for the application by clicking <strong>Check App</strong>. Search the Internet to find which API levels are associated with which Android versions.</td>
</tr>
</tbody>
</table>

### Table 11-2. Application Configuration Details for iOS Applications

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>If necessary, edit the ID for the application. You can access the page of an iOS application that you want to add to your catalog from the Apple App Store. You can access the page using a browser or using the iTunes desktop application. If you use the iTunes desktop application, obtain the URL for the application by right clicking the application's icon and copying the link. Find the application ID within the install URL of the application. For example, an application called exampleApp, might use the following URL: <a href="https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1">https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1</a>. For the preceding example, the application ID is as follows: id123456789.</td>
</tr>
<tr>
<td>iTunes URL</td>
<td>This field displays the URL to install this mobile referred application from the Apple App Store. If necessary, edit the URL for the application. For example, an application called exampleApp might use the following URL: <a href="https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1">https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1</a>.</td>
</tr>
<tr>
<td>Minimum OS Version</td>
<td>If necessary, edit the minimum version of iOS upon which the application can operate. Find minimum version information on the Apple App Store page for the application, which is accessible with the iTunes URL.</td>
</tr>
<tr>
<td>Devices Supported</td>
<td>If necessary, use the drop-down menu to change the setting for supported devices. Find supported device information on the Apple App Store page for the application, which is accessible with the iTunes URL.</td>
</tr>
</tbody>
</table>

7 Click the **Entitlements** tab, and configure as appropriate.

Click this tab to entitle users and groups to the mobile referred application. You can configure entitlements while initially configuring the application or anytime in the future.
What to do next
See “Entitle Users and Groups to Mobile Referred Applications,” on page 86 for details about adding user and group entitlements for mobile referred applications.

Add a Mobile Referred Application to Your Catalog from the Apple App Store

When you want to add a mobile referred application to your catalog for iOS devices but the application is not available in the Global Catalog, you can add the application as a resource that points to where it resides in the Apple App Store.

When you add mobile referred applications to your catalog you are actually creating a link in your catalog to the mobile application in the Apple App Store or Google Play. Through this process you can recommend mobile applications to users for download. Once users download and install a mobile referred application, they do not use the Horizon Workspace client on their mobile device to access the application. They can launch the application using its icon on their mobile device.

Prerequisites
- Enable the Mobile Management module. See “Enable the Mobile Management Module,” on page 61.
- Access the page of an iOS application that you want to add to your catalog from the Apple App Store. You can access the page using a browser or using the iTunes desktop application. If you use the iTunes desktop application, obtain the URL for the application by right clicking the application's icon and copying the link. Information from the application page, such as the URL and application specifics, are required to complete this task. As an example, an application called exampleApp, might use the following URL: https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1.

Procedure
1. Log in to the Horizon Workspace Administrator Web interface.
2. Select Catalog > Mobile Applications.
3. Select Mobile Application > from Apple App Store.
4. Type the iTunes URL and click Import.
   The form refreshes and displays the application name, description, and icon obtained from the Apple App Store.
5. Shorten the description to less than 1024 characters, and then click Add.
   The mobile referred application is added as a resource to your catalog and the application’s resource page is displayed.
   The items in an application’s resource page are pre-populated with information specific to the mobile application. The available information varies slightly depending on the operating system of the mobile application.
6. Click the Details tab to customize basic information about the application, according to the needs of your organization, and click Save.
   For some mobile referred applications, some fields are not customizable.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Provide the application name as listed on the Apple App Store page for the application</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. Provide a description of the application.</td>
</tr>
</tbody>
</table>
Form Item | Description
--- | ---
**Icon** | Optional. Use the Choose File button 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.

7 Click the **Configuration** tab, edit the application’s configuration details as necessary, and click **Save**.

Form Item | Description
--- | ---
**Application ID** | If necessary, edit the ID for the application. You can access the page of an iOS application that you want to add to your catalog from the Apple App Store. You can access the page using a browser or using the iTunes desktop application. If you use the iTunes desktop application, obtain the URL for the application by right clicking the application’s icon and copying the link. Find the application ID within the install URL of the application. For example, an application called exampleApp, might use the following URL: https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1. For the preceding example, the application ID is as follows: id123456789.

**iTunes URL** | This field displays the URL to install this mobile referred application from the Apple App Store. If necessary, edit the URL for the application. For example, an application called exampleApp might use the following URL: https://itunes.apple.com/us/app/exampleApp/id123456789?ex=1.

**Minimum OS Version** | If necessary, edit the minimum version of iOS upon which the application can operate. Find minimum version information on the Apple App Store page for the application, which is accessible with the iTunes URL.

**Devices Supported** | If necessary, use the drop-down menu to change the setting for supported devices. Find supported device information on the Apple App Store page for the application, which is accessible with the iTunes URL.

8 Click the **Entitlements** tab, and configure as appropriate.

Click this tab to entitle users and groups to the mobile referred application. You can configure entitlements while initially configuring the application or anytime in the future.

**What to do next**

See “Entitle Users and Groups to Mobile Referred Applications,” on page 86 for details about adding user and group entitlements for mobile referred applications.

**Add a Mobile Referred Application to Your Catalog from Google Play**

When you want to add a mobile referred application to your catalog for Android devices but the application is not available in the Global Catalog, you can add the application as a resource that points to where it resides in Google play.

When you add mobile referred applications to your catalog you are actually creating a link in your catalog to the mobile application in the Apple App Store or Google Play. Through this process you can recommend mobile applications to users for download. Once users download and install a mobile referred application, they do not use the Horizon Workspace client on their mobile device to access the application. They can launch the application using its icon on their mobile device.

**Prerequisites**

- Enable the Mobile Management module. See “Enable the Mobile Management Module,” on page 61.
- Use a browser to access the page of a mobile application that you want to add to your catalog from Google play. Information from the application page, such as the URL and application specifics, are required to complete this task. As an example, an application called exampleApp, might use the following URL: https://play.google.com/store/apps/details?id=com.exampleApp.android.
Procedure

1. Log in to the Horizon Workspace Administrator Web interface.
2. Select Catalog > Mobile Applications.
3. Click Add an Application.
4. Select Mobile Application > from Google Play.

An application resource page is displayed.

5. If not already selected, click the Details tab, and complete the form with basic information about the mobile referred application you want to add to your catalog and click Next.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Provide the application name as listed on the Google Play page for the application.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. Provide a description of the application.</td>
</tr>
<tr>
<td>Icon</td>
<td>Optional. Use the Choose File button 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>

When you click Next, the page refreshes to display the configuration details for the application.

6. If the configuration details are not displayed, click the Configuration tab, edit the application’s configuration details, and click Save.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>Provide the ID or package name for this application. Use a browser to search the Google Play Web site for the application. Find the application ID within the Google Play URL of the application. For example, an application called exampleApp might use the following URL: <a href="https://play.google.com/store/apps/details?id=com.exampleApp.android">https://play.google.com/store/apps/details?id=com.exampleApp.android</a>. For the preceding example, the application ID is as follows: com.exampleApp.android</td>
</tr>
<tr>
<td>Google Play URL</td>
<td>Provide the URL to install this mobile referred application from Google Play. If necessary, edit the URL for the application. Use a browser to search the Google Play Web site for the application. For example, an application called exampleApp might use the following URL: <a href="https://play.google.com/store/apps/details?id=com.exampleApp.android">https://play.google.com/store/apps/details?id=com.exampleApp.android</a>. Using the URL for the application, you can create the install URL by starting with the word market. For example, market://details?id=com.exampleApp.android. Click Check App to open the displayed URL and verify it leads to the application you want.</td>
</tr>
<tr>
<td>Minimum API Level</td>
<td>Provide the minimum Android API level upon which the application can operate. The Android API level is directly associated with the Android version. If a specific Android version is required for an application, find the required version number on the Google Play page for the application by clicking Check App. Search the Internet to find which API levels are associated with which Android versions.</td>
</tr>
</tbody>
</table>

7. Click the Entitlements tab and configure as appropriate.

Click this tab to entitle users and groups to the mobile referred application. You can configure entitlements while initially configuring the application or anytime in the future.

What to do next

See “Entitle Users and Groups to Mobile Referred Applications,” on page 86 for details about adding user and group entitlements for mobile referred applications.
Entitle Users and Groups to Mobile Referred Applications

You can entitle users and groups to mobile referred applications.

You can only entitle Horizon Workspace users, users imported from your directory server, to mobile referred applications. When you entitle a user to a mobile referred application, they can see the reference to the application in the Horizon Workspace client on their mobile device, and can choose to install the application on the device. If you remove the entitlement, the reference disappears, whether users installed the application already or not. If users installed the mobile application on their devices before you removed the entitlement, removing the entitlement does not uninstall the application from their devices.

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

Prerequisites

- Enable the Mobile Management module. See “Enable the Mobile Management Module,” on page 61.
- Add one or more mobile referred applications to your catalog as resources. See “Overview of Mobile Referred Applications,” on page 79.

Procedure

1. Log in to the Administrator Web interface.
2. Entitle users to a mobile referred application using one of the available methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Access the mobile referred application's resource page, and entitle users or groups to the resource. | 1. Select Catalog > Mobile Applications.  
2. Click the icon for the mobile referred application to which you want to entitle users and groups.  
The Entitlements tab is selected by default. Group entitlements are listed in one area of the page, while user entitlements are listed in another.  
3. Click Add group entitlement or Add user entitlement as appropriate.  
4. 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.  
5. Click Save.  
6. Click Done on the Entitlements page. |

Access the details page for the user or group, and add the mobile referred application entitlement from that page. | 1. Click the Users & Groups tab.  
2. Click the appropriate tab: Users or Groups.  
3. Click the name of an individual user or group.  
4. Click Add entitlement.  
5. Click the check boxes next to the mobile referred applications to which you want to entitle the user or group.  
The user-activated deployment method is selected by default for mobile referred applications. Users must install mobile referred applications directly on their mobile devices.  
6. Click Save. |
The selected users or groups are now entitled to access the mobile referred application using the Horizon Workspace client application on their mobile devices.

**NOTE** Users that use the VMware Switch client for their entitled workspaces do not get access to referred Android apps using that client, even if they are entitled to such apps. Referred Android apps are those Android apps that you add to your catalog by referring to their URL in Google Play or from the Global Catalog. Even though you can use the Administrator Web interface to entitle referred Android apps to all of your users, when users provision their workspaces using the VMware Switch client, those referred Android apps are not included in the managed mobile workspaces on those users' VMware Ready Android devices. Horizon Workspace manages your imported Android apps in the managed mobile workspaces on VMware Ready Android devices, and not referred Android apps. See Chapter 8, “Providing Access to Mobile Workspaces,” on page 47.
You can provide Horizon Workspace users on Windows systems access to Windows applications that have been captured as ThinApp packages.

When you configure Horizon Workspace to provide user access to ThinApp packages, the ThinApp packages appear in your catalog. You can then entitle users and groups to the ThinApp packages.

This chapter includes the following topics:

- “Enable the ThinApp Packages Module after Integrating Your ThinApps Repository with Your Horizon Workspace System,” on page 89
- “Overview of ThinApp Packages,” on page 90
- “Entitle Users and Groups to ThinApp Packages,” on page 91
- “Silently Deploy Horizon Workspace Client for Windows on Users' Windows Systems,” on page 92
- “Delete ThinApp Packages from Horizon Workspace,” on page 95

Enable the ThinApp Packages Module after Integrating Your ThinApps 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.

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 displays telling you to go to all connectors, 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 enabling the ThinApp Packages module.
What to do next

Verify the distribution of Horizon Workspace Client for Windows to users’ Windows systems. See “Deploying Horizon Workspace Client for Windows,” on page 90.

Overview of ThinApp Packages

For Horizon Workspace users to access ThinApp packages, Horizon Workspace Client for Windows must be installed on their Windows systems. You determine how to deploy the client to their systems. You also determine how ThinApp packages are deployed to users’ systems.

Deploying Horizon Workspace Client for Windows

Horizon Workspace Client for Windows is a component that can be installed on users’ Windows systems, such as on a Windows desktop, Windows laptop, or Horizon View desktop. The client is used for both the Horizon Files service, the file storage and sharing service, and ThinApp packages. While Horizon Workspace Client for Windows enhances the user experience with the Horizon Files service, it is a required component for users to access ThinApp packages through Horizon Workspace.

You can install Horizon Workspace Client for Windows either manually one system at a time or silently to multiple systems.

To install Horizon Workspace Client for Windows manually, users access Horizon Workspace by using a browser to access Horizon Workspace Web Client. In the Web Client, users can download the executable file for installing the Horizon Workspace Client for Windows. Then the users run the installer to install the client. Users must have local administrator privileges to install Horizon Workspace Client for Windows. See Horizon Workspace User Guide: Using the Desktop Client for information about installing Horizon Workspace Client for Windows manually. When the client is installed manually, the ThinApp download mode is the default deployment mode. Users do not have the option of selecting the deployment mode. For the ability to provide the ThinApp streaming mode, you can use the silent deployment method of installing Horizon Workspace Client for Windows.

As an administrator, you can install Horizon Workspace Client for Windows silently to multiple users at the same time by using a script. A silent installation does not display messages or windows during deployment. For a silent installation, you must select how the ThinApp packages will be deployed: ThinApp streaming mode or ThinApp download mode. See “Silently Deploy Horizon Workspace Client for Windows on Users’ Windows Systems,” on page 92.

Determining the Appropriate Deployment Mode for ThinApp Package Access

Each ThinApp package can be used for both ThinApp streaming mode and ThinApp download mode. When you install a ThinApp package silently, you indicate the ThinApp package deployment mode in a script that deploys Horizon Workspace Client for Windows to selected endpoints, such as desktop and laptop computers. You should choose the deployment mode that best fits the network environment for the selected endpoints, considering details such as network latency.

With streaming mode, when Horizon Workspace Client for Windows synchronizes with Horizon Workspace, the client downloads application shortcuts to the desktop, and then the user launches the applications immediately from the file share. With download mode, the user must wait for the applications to download first, and then shortcuts are created. The user launches applications from the local device.
### Table 12-1. User Access to Applications Captured as ThinApp Packages

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| ThinApp Streaming Mode| In ThinApp streaming mode, applications are streamed each time they are launched. The following environments could potentially provide the consistency and stability required:  
  - Horizon View stateless desktops with excellent connectivity to the file share  
  - Horizon View physical desktops with excellent connectivity to the file share  
  - Users with physical 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. |
| ThinApp Download Mode | In ThinApp download mode, applications are downloaded to an end user device and launched locally. While both streaming and download mode work well in a Horizon Workspace environment on a local network, you might prefer ThinApp download mode for the following use cases:  
  - Persistent Horizon View desktops  
  - LAN-connected desktops that are periodically offline  
  - A LAN with poor network latency |

### Entitle Users and Groups to ThinApp Packages

You can entitle users and groups to Windows applications captured as ThinApp packages.

You can only entitle Horizon Workspace users, users imported from your directory server, to ThinApp packages. When you entitle a user to a ThinApp package, the user sees the application and can launch it from the appropriate Horizon Workspace client on their system. If you remove the entitlement, the user cannot see or launch the application.

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

#### Prerequisites

Configure Horizon Workspace to provide user access to ThinApp packages.

**Note** You can use the Configurator Web Interface or the Connector Web Interface to provide user access to ThinApp packages. You cannot add ThinApp packages to your catalog with the Administrator Web interface. Therefore, you cannot add ThinApp packages to your catalog directly from the Catalog page.

#### 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>
<tbody>
<tr>
<td>Access a ThinApp package and entitle users or groups to it.</td>
<td>a Select Catalog &gt; ThinApp Packages.</td>
</tr>
<tr>
<td></td>
<td>b Click the ThinApp package to which you want to entitle users and groups.</td>
</tr>
<tr>
<td></td>
<td>The Entitlements tab is selected by default. Group entitlements are listed in one table while user entitlements are listed in another.</td>
</tr>
<tr>
<td></td>
<td>c Click Add group entitlement or Add user entitlement as appropriate.</td>
</tr>
<tr>
<td></td>
<td>d Enter the names of the groups or users as appropriate.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>e Use the drop-down menu to select how to activate each selected ThinApp package: Automatic or User-Activated.</td>
</tr>
<tr>
<td></td>
<td>▪ Automatic: Users have immediate access to the ThinApp package the next time they log in to Horizon Workspace.</td>
</tr>
<tr>
<td></td>
<td>▪ User-Activated: Users must activate the ThinApp package in the Horizon Workspace client before they can use the application.</td>
</tr>
<tr>
<td></td>
<td>f Click Save.</td>
</tr>
</tbody>
</table>

Access a user or group and add ThinApp package entitlements to that user or group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a Click the Users &amp; Groups tab.</td>
</tr>
<tr>
<td></td>
<td>b Click the appropriate tab: Users or Groups.</td>
</tr>
<tr>
<td></td>
<td>c Click the name of an individual user or group.</td>
</tr>
<tr>
<td></td>
<td>d Click Add entitlement.</td>
</tr>
<tr>
<td></td>
<td>e Click the check boxes next to the ThinApp packages to which you want to entitle the user or group.</td>
</tr>
<tr>
<td></td>
<td>f Use the drop-down menu to select how to activate each selected ThinApp package: Automatic or User-Activated.</td>
</tr>
<tr>
<td></td>
<td>▪ Automatic: Users have immediate access to the ThinApp package the next time they log in to Horizon Workspace.</td>
</tr>
<tr>
<td></td>
<td>▪ User-Activated: Users must activate the ThinApp package in the Horizon Workspace client before they can use the application.</td>
</tr>
<tr>
<td></td>
<td>g Click Save.</td>
</tr>
</tbody>
</table>

The selected users or groups are now entitled to use the ThinApp package.

**What to do next**

Verify that the Horizon Workspace Client for Windows is installed on users Windows systems.

**Silently Deploy Horizon Workspace Client for Windows on Users' Windows Systems**

Horizon Workspace Client for Windows interacts with ThinApp packages and the Horizon Files service, the file storage and sharing service. Silently installing Horizon Workspace Client for Windows allows you to implement a script that installs the client on multiple users' Windows systems at the same time.

Horizon Workspace Client for Windows is a required component for ThinApp package access and a recommended component for the Horizon Files service. See “Deploying Horizon Workspace Client for Windows,” on page 90. To provide the Horizon Files service to users on devices other than Windows systems, verify that the respective client is installed on users' non-Windows devices.
Prerequisites

- Install and configure Horizon Workspace. See *Installing and Configuring Horizon Workspace*.
  - To enable users to share files and folders, as part of the Horizon Workspace installation, implement the steps related to the Horizon Files service, such as adding storage and configuring a document preview server.
  - To enable users to access ThinApp packages, as part of the Horizon Workspace installation, perform all the steps for ThinApp-package integration. For example, create ThinApp packages using VMware ThinApp 4.72 or later, populate a Windows application network file share, and complete the ThinApp-package related steps in the Configurator Web interface.
- Verify that users’ Windows systems are connected from inside the enterprise network. This configuration is required to deploy Horizon Workspace Client for Windows.
- Verify that users’ systems run Windows 7 or Windows XP and use Internet Explorer 8 or 9 or Firefox 6 or later.
- If making ThinApp packages available to Horizon Workspace users, perform the prerequisites in the Horizon Workspace Administrator Web interface specific to ThinApp packages.
  - Enable the ThinApp Packages module. See “Enable the ThinApp Packages Module after Integrating Your ThinApps Repository with Your Horizon Workspace System,” on page 89.
- If making the Horizon Files service available to Horizon Workspace users, perform the prerequisites in the Horizon Workspace Administrator Web interface specific to the Horizon Files service.
  - Enable the Horizon Files module. See “Enable the Horizon Files Module,” on page 35.
  - Associate users with classes of service. See “Entitling and Provisioning Users and Groups to the Horizon Files Service,” on page 36.

Procedure

1. Download the Horizon Workspace Client for Windows executable file to the Windows system from which you want to silently deploy the client.
   - To download the Horizon Workspace Client for Windows executable file, you must follow the initial steps required to download the client manually.
     a. Using a browser, log in to the Horizon Workspace Web Client as a user.
        - The following is an example of the URL to access the Web Client:
          https://HorizonWorkspaceFQDN/web.
     b. Click your user name and click **Download Horizon**.
     c. Click the **Windows Desktop Client** icon.
     d. Save the file to your Windows system.
     e. Open a command window and change directories to the location of the Horizon Workspace Client for Windows executable file.
     f. View the usage options related to the executable file by implementing a command in the command window, such as the following:
        ```
        VMware-Horizon-Workspace-1.0.0-nnnnn /?
        ```
        A dialog box appears that lists the command options for the executable file. You can familiarize yourself with the options before you create the script to deploy Horizon Workspace Client for Windows to users systems.
Apply a script for Horizon Workspace Client for Windows installations in whichever manner you choose to deploy Horizon Workspace Client for Windows. For example, Active Directory group policy script, login script, VB script, batch file, SCCM, and so on.

Use the command options and variables that best fit your requirements. The following is an example command for installing Horizon Workspace Client for Windows silently: 
```
VMware-Horizon-Workspace-1.0.0-nnnnn.exe /s /z HORIZONSERVER=https://HorizonWorkspaceFQDN SSLBYPASS=1 /v DOWNLOAD=0 POLLINGINTERVAL=60
```

For example:
```
VMware-Horizon-Workspace-1.0.0-12345.exe /s /z HORIZONSERVER=https://HorizonWorkspaceHost.com SSLBYPASS=1 /v DOWNLOAD=0 POLLINGINTERVAL=60
```

Where:
- nnnn in the executable name represents the Horizon Workspace build number.
- The s option runs the installation silently. A silent installation does not display messages or windows during deployment.
- The z option allows you to specify a variable key equal to a variable value: "Key"="value". The allowed keys for this option are HORIZONSERVER and SSLBYPASS.
- The v option is specific to ThinApp packages and allows you to specify a variable key equal to a variable value: "Key"="value". The allowed keys for this option are DOWNLOAD and POLLINGINTERVAL.
- The HORIZONSERVER variable key accepts a URL as its variable value. Provide the URL to your Horizon Workspace instance, where HTTPS is the required protocol, to allow Horizon Workspace Client for Windows to communicate with Horizon Workspace.
- The SSLBYPASS variable key allows you to bypass the SSL certificate verification error. When your deployment doesn’t use a trusted third party SSL certificate, you receive an error. Set the value of this variable to 1 to bypass the SSL certificate verification error. If unspecified, the default value of 0 applies.
- The DOWNLOAD variable key enables you to select the ThinApp package deployment mode: 1 denotes download mode, 0 denotes streaming mode. If unspecified, the default value of 1, download mode, applies.
- The POLLINGINTERVAL variable key enables you to set the frequency, measured in seconds, of synchronizations between Horizon Workspace Client for Windows and Horizon Workspace to check for new applications or entitlements. If unspecified, the default value of 180 applies.

**Note** When you entitle a ThinApp package to users, the ThinApp package is streamed or cached after the polling interval. Users might then see the ThinApp package in the Horizon Workspace Web Client. However, the ThinApp package will not launch until the client syncs the application on the next polling interval.

If the silent installation is successful, Horizon Workspace Client for Windows is deployed on users’ devices. At that time, users can access entitled ThinApp packages from their Windows systems.

**Note** Error messages do not appear on screen when you deploy Horizon Workspace Client 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.

**What to do next**
- Provide user access to Horizon Workspace by providing the appropriate URL. For example: https://HorizonWorkspaceFQDN/web.
Verify that Horizon Workspace Client for Windows is properly installed on users’ Windows systems. See Horizon Workspace User Guide: Using the Desktop Client.

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.

Prerequisites

Procedure

1. Delete the ThinApp package subfolder from the Windows application network file share.

2. Delete the application from Horizon Workspace.
   a. Log in to the Administrator Web interface.
   b. Click Catalog > ThinApp Packages.
   c. Click the icon of the ThinApp package you want to delete.
   d. Click Delete, read the message, and if you agree click Yes.

3. Use the Connector virtual appliance interface to issue commands to remove the ThinApp database.
   a. Select Login and Log in to the underlying Linux operating system of the Connector virtual appliance.
   b. Issue the following command to stop the ThinApp service: `/opt/likewise/bin/lwsm stop thinapprepo`
   c. Issue the following command to delete the ThinApp database: `rm /var/lib/vmware/tam/repo/repodb`
   d. Issue the following command to restart the ThinApp service: `/opt/likewise/bin/lwsm start thinapprepo`

4. Exit the Connector virtual appliance interface.

The ThinApp package no longer exists in Horizon Workspace.
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>
<thead>
<tr>
<th>Table 13-1. Horizon Workspace Report Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Workspace Report</td>
</tr>
<tr>
<td>Resource Usage</td>
</tr>
<tr>
<td>Resource Entitlements</td>
</tr>
<tr>
<td>Group Membership</td>
</tr>
<tr>
<td>Users</td>
</tr>
<tr>
<td>Horizon Files Usage</td>
</tr>
<tr>
<td>Audit events</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


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 100 days ago to 70 days ago.</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 To see the code for a specific 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.

### 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 Settings &gt; VA Configuration 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:</td>
</tr>
<tr>
<td></td>
<td>- View system information.</td>
</tr>
<tr>
<td></td>
<td>- Change the database from internal to external.</td>
</tr>
<tr>
<td></td>
<td>- Configure an SSL certificate for external access to Horizon Workspace.</td>
</tr>
<tr>
<td></td>
<td>- Enter a new license key.</td>
</tr>
<tr>
<td></td>
<td>- Change the admin user password for the service-va, configurator-va, and connector-va.</td>
</tr>
<tr>
<td></td>
<td>- View a list of the log file locations.</td>
</tr>
<tr>
<td></td>
<td>On the VA Configuration page, click View Virtual Appliance System Configuration to load the login page of the Configurator Web interface in your browser.</td>
</tr>
<tr>
<td>Password Recovery</td>
<td>Select Settings &gt; Password Recovery 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>Identity Providers</td>
<td>You can add additional Connector instances to balance the load of your Horizon Workspace deployment or to use different authentication types for different users, according to users' IP addresses. When your Horizon Workspace deployment consists of multiple Connector instances, the IdP discovery feature facilitates the process by locating the correct Connector instance. See Chapter 2, “Introduction to Horizon Workspace for Administrators,” on page 7 for information on IdP Discovery. Add Connector instances using the hznAdminTool addvm command in the configurator-va virtual machine. Newly added Connector instances appear on the Identity Providers page, accessible by using the Administrator Web interface to select Settings &gt; Identity Providers. To control the Connector instance to which an IP address is directed, configure the Identity Providers page. See “Direct IP Addresses to Specific Connector Instances,” on page 100. Unless VMware technical support instructs you to use the Add Identity Provider button to create a Connector activation code, use the hznAdminTool addvm command to add Connector instances.</td>
</tr>
<tr>
<td>Remote App Access</td>
<td>Select Settings &gt; Remote App Access to create clients or templates that enable applications to register with Horizon Workspace.</td>
</tr>
<tr>
<td>SAML Certificate</td>
<td>Select Settings &gt; 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.</td>
</tr>
</tbody>
</table>
Setting | Description
--- | ---
Approvals | Select Settings > Approvals to enable or disable license approval. Enabling license approval applies when you use the Horizon Workspace SDK to integrate your license-management system with Horizon Workspace.
Mobile Workspace | Select Settings > Mobile Workspace to configure branding elements for mobile workspaces, such as your enterprise’s end user agreement allowing users to use your workspace on their mobile devices and an image for your enterprise’s logo. See “Configure Mobile Workspace Branding Elements,” on page 101.
Auditing | Select Settings > Auditing to enable or disable the collection of information for the audit events report, which is accessible on the Reports tab.

**Direct IP Addresses to Specific Connector Instances**

By configuring IdP discovery, you enable Horizon Workspace to direct users with specific IP addresses to specific Connector instances for authentication. This feature helps balance the load of Horizon Workspace activity to multiple Connector instances, and gives you the ability to use a different authentication type for different users, according to their IP address.

The Connector acts as an identity provider for your Horizon Workspace system and is the only identity provider that Horizon Workspace supports. By using multiple Connector instances with IdP discovery configured, you can use different types of authentication to authenticate users, such as RSA SecurID and Kerberos, according to the IP address of the user. See Chapter 2, “Introduction to Horizon Workspace for Administrators,” on page 7 for information on IdP Discovery.

**Prerequisites**

- Install and configure Horizon Workspace.
- Determine the different authentication types required to meet the needs of your enterprise. For example, you could configure one Connector instance to use Kerberos authentication for users internal to your enterprise and one Connector instance to use RSA SecurID authentication for users external to your enterprise.
- Issue the `hznAdminTool addvm` command in the configurator-va virtual machine to create the additional Connector instances necessary for your deployment. See Installing and Configuring Horizon Workspace.

**Procedure**

1. Log in to the Administrator Web interface.
2. Select Settings > Identity Providers and verify that the new Connector instance appears in the list of identity providers.
   
   The names of the Connector instances you added to your deployment as a prerequisite task using the `hznAdminTool addvm` command appear in the list of identity providers.
3. Click Edit for the newly created identity provider.
4. Configure the IP addresses in the Allowed IP Addresses section.
   
   Edit the IP Address and if required click Add IP Range to add additional IP address ranges. For example, to include only users within your enterprise network, create IP ranges that encompass all the IP addresses within your enterprise.
5. Click Save.
6 If you want to change the order of the newly created Connector instance, click **Edit Order of Identity Providers**, use the up and down arrows to move the Connector instance to the appropriate location, and click **Save**.

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

**Configure Mobile Workspace Branding Elements**

For your enterprise's mobile workspaces on iOS and VMware Ready Android devices, you can configure branding elements such as a logo image and any terms and conditions for using the mobile workspace to which your enterprise wants users' confirmation and agreement.

**Prerequisites**

Verify that you have the text of your enterprise's terms and conditions to which you want your users to agree for their use of the mobile workspace and its applications. The text can be 10,000 characters or less. When a user activates the mobile workspace for the first time on the mobile device, this text is displayed and the user has the opportunity to accept the terms and conditions.

Verify that you have an image for your enterprise's logo. Supported file types are PNG and JPEG. The maximum file size is 5 MB. Images larger than 200x80 pixels are re-sized to those dimensions. When a user activates the mobile workspace for the first time on the mobile device, this image is displayed.

**Procedure**

1. Select **Settings > Mobile Workspace > EULA & Branding**.
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**.
4. In the Workspace Branding area, click **Choose File**.
5. Select the image file that you are using to brand the first activation of the mobile workspace.
6. Click **Save**.

The selected image is displayed so that you can verify the image.
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:

- “Horizon Workspace Fails to Provision a User to the Horizon Files Service,” on page 103
- “File Preview in the Horizon Workspace Web Client Displays Server Error and No Errors in the Server Logs,” on page 104
- “Web Client Fails to Respond When Used In Some Workstation or VMware Fusion Environments,” on page 104
- “Files With Names That Contain Invalid XML Characters Fail to Sync With the Horizon Workspace Clients on Windows or Mac Systems,” on page 105
- “Sharing Folders or Files from the Horizon Workspace for iOS, First Edition App Fails With Error About Email,” on page 106

**Horizon Workspace Fails to Provision a User to the Horizon Files Service**

When you entitle a user to the Horizon Files service, the provisioning of the user might fail.

**Problem**

One or more users cannot access the Horizon Files service and the provisioning status page in the Administrator Web interface displays a provisioning error message for such users.

**Cause**

Users can be entitled to the Horizon Files service while not being provisioned to the Horizon Files service. A variety of causes, such as networking issues, might prevent Horizon Workspace from provisioning users.

Also, this problem can occur when you remove a user from Horizon Workspace who was, at one time, entitled and provisioned to the Horizon Files service and you later add the user back to Horizon Workspace. See Chapter 7, “Providing Access to the Horizon Files Service,” on page 35 for a detailed description of this problem.

**Solution**

1. Use the command tool of the Horizon Workspace Manager Virtual Appliance to search the horizon.log files.

   If the log contains wording indicating that the account already exists, such as "email address already exists.", continue with this task.
2 Verify that the user account already exists in the Horizon Files service.
   a Use the command tool of the Horizon Files Virtual Appliance, the data-va virtual appliance, to check for the existence of the user's account.
      Example: zmprov ga joe@domain.com
   b If the user's account exists, continue.

3 Delete the user's original account in the Horizon Files service.
   Example: zmprov da joe@domain.com

File Preview in the Horizon Workspace Web Client Displays Server Error and No Errors in the Server Logs

   In the Horizon Workspace Web client, an HTTP error 500 is displayed when the user tries to preview a file, and no related errors are written to the Horizon Workspace logs.

   Problem
   When you click a file displayed in the Horizon Workspace Web client, the preview of the file is not displayed in the preview pane. Instead, the following message is displayed

   HTTP ERROR 500 Server Error
   When you look at 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 has been deactivated, activate it according to the standard Microsoft documentation and your deployment environment.

Web Client Fails to Respond When Used In Some Workstation or VMware Fusion Environments

   When you are running Windows 8 in VMware® Workstation™ or VMware Fusion®, and open the Horizon Workspace Web client in a Firefox browser of version 18 or higher, after you log in, the client's user interface becomes unresponsive.

   Problem
   This problem occurs when you use version 18 or higher of the Firefox browser in Windows 8 in Workstation or VMware Fusion. When you open the Horizon Workspace Web client in that environment, even though you can log in, the client's user interface becomes unresponsive. When you click on the tabs, nothing happens.

   Cause
   This problem was introduced in Firefox version 18. Firefox browser versions prior to version 18 do not have the problem.
Solution

To avoid the problem, use one of the following options to run the Horizon Workspace Web client in a supported browser other than Firefox version 18.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run Internet Explorer version 10 in version 9 browser mode</td>
<td>By default, Windows 8 comes with Internet Explorer version 10. Because the Horizon Workspace Web client is not officially supported for use in Internet Explorer version 10, use the Developer Tools in Internet Explorer version 10 to set the browser mode to run as Internet Explorer version 9.</td>
</tr>
<tr>
<td>Firefox version 17</td>
<td>In the Windows 8 operating system in the Workstation or VMware Fusion environment, uninstall Firefox and install Firefox version 17.</td>
</tr>
<tr>
<td>Google Chrome (latest version)</td>
<td>Install Google Chrome in the Windows 8 operating system in the Workstation or VMware Fusion environment.</td>
</tr>
</tbody>
</table>

Files With Names That Contain Invalid XML Characters Fail to Sync With the Horizon Workspace Clients on Windows or Mac Systems

When a file’s name contains characters that are not valid XML characters, and you are using either the Horizon Workspace Client for Windows or the Horizon Workspace Client 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 Horizon Workspace client 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 the server threw an unmarshal exception because an invalid character is found in the file name.

Cause

The clients on Windows and Mac systems use 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 is displayed.

Invalid characters that can cause this problem include control characters, such as Ctrl plus a letter. A common situation is introducing the backspace character into a file name. The backspace character is CONTROL-H, Ctrl-H, ^H, or \010. Users accidentally introduce the Ctrl-H character into 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 into file names are ^B, ^M, and ^]. The ^M combination can be accidentally introduced into a file name when the FTP command is used to move the file from Windows to a Mac system.

Introduction of control characters into file names tends to happen more frequently to users that 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 1s –8 command in the Horizon Workspace directory used by their client. The 1s –8 command lists the files and shows where any invisible characters are present in the file names.

Solution

1. Generate the diagnostic logs from the client.
   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 displays with the location of the zip file.
2 Extract the log file for Horizon Workspace from the zip, 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 1.5 server, and then tries to use the feature for sharing folders and files, an error displays and the folder or file is not shared.

Problem

When 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 1.5 server. Use of the Horizon Workspace for iOS, First Edition app with a Horizon Workspace 1.5 server is not supported in this release, even though some features in the client 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 a Horizon Workspace 1.5 server.
Index

A
access events 97
Add Identity Provider button 99
additional user attributes 23
administrative settings 99
Android apps, importing into the catalog 50
Apple App Store 83
application records
  mobile referred applications from Google Play 84
  mobile referred applications from the Apple App Store 83
  mobile referred applications from the Global Catalog 81
Web applications 74
Web applications from the Global Catalog 72
applications
  mobile 79
  mobile referred 81, 83, 84
Web 71, 72, 74, 75
audience 5
Audit Event report 97
automatic disable policy 54
automatic wipe policy 54

B
branding elements, mobile workspaces 99, 101

C
catalog
  imported mobile applications 50
  managing 29
  mobile referred applications 79
  viewing resources 32
Web applications 72
class of service
  about 38
  assigning to users 37
  creating 42
  deleting 44
  editing 40
  precedence 39
  viewing for users and groups 44
company logo, mobile workspaces 99, 101
Configurator Web interface, access 99
Connector instance, adding 99
Connector activation code 99
Connector Web interface, URL 7

data containment policies 54
Data Node Hostname attribute 23
default class of service 38
directory server groups 17
ende user license agreement, mobile workspaces 99, 101
entitlements
  Horizon Files service 36
  managed mobile workspaces 51
  mobile workspaces 48
  mobile referred applications 86
  ThinApp packages 91
  Web applications 76
EULA, mobile workspaces 99, 101

directory server groups 17

E
end user license agreement, mobile workspaces 99, 101
entitlements
  Horizon Files service 36
  managed mobile workspaces 51
  mobile workspaces 48
  mobile referred applications 86
  ThinApp packages 91
  Web applications 76
EULA, mobile workspaces 99, 101

F
file preview, troubleshooting 104

groups
  Horizon Files service 38
  membership report 97
  membership rules 19
  policy sets 59
  searching for 15
  viewing information 21

H
Horizon Files module 35
Horizon Workspace, virtual appliances 7
Horizon Files service
  about 35
  entitling 36
  provisioning 36
  resource type 30
  troubleshooting 103
  usage report 97
Horizon Files Usage report 97
Horizon View entitlements 69
Horizon View Connection Server 69
Horizon View desktop pools, providing access 67
Horizon Workspace groups 17
hzn-admin tool 7, 99

| I | identity provider, adding 99 |
|   | IDP Discovery, configuring 100 |
|   | importing mobile applications 50 |

| L | lease interval policy 54 |
|   | leasing process 61 |
|   | license, approval 99 |

| M | managed mobile applications 50 |
|   | managed mobile workspaces  |
|   | disabling 60 |
|   | entitling users and groups 51 |
|   | policies 52 |
|   | resetting passcodes 60 |
|   | setting up 49 |
|   | wiping 60 |
|   | Mobile Management module 61 |
|   | mobile referred applications  |
|   | adding 79 |
|   | entitling to users and groups 86 |
|   | mobile applications  |
|   | adding 50, 79 |
|   | resource type 30 |
|   | mobile policy sets, creating 58 |
|   | mobile workspaces  |
|   | Android devices 48 |
|   | branding elements 99, 101 |
|   | entitling users and groups 48 |
|   | EULA 99, 101 |
|   | iOS devices 48 |
|   | providing access to 47 |
|   | using 61 |
|   | modules  |
|   | Horizon Files 35 |
|   | Mobile Management 61 |
|   | ThinApp Packages 89 |
|   | View 68 |
|   | viewing information 13 |
|   | Web Applications 71 |
|   | multitenant Web applications 71 |

| P | passcode policies 55 |
|   | password recovery, user 99 policies  |
|   |   data containment 54 |
|   |   passcode 55 |
|   |   secure network access 57 |
|   |   workspace lifetime 54 |
|   |   policy sets  |
|   |   applying to groups 59 |
|   |   managing 52 |
|   |   policy resolution 52 |

| R | removing user access 26 |
|   | reports 97 |
|   | Resource Entitlement report 97 |
|   | Resource Usage report 97 |
|   | resources 32 |
|   | roles 23 |
|   | rules for group membership 19 |

| S | SAML 71, 72, 74 |
|   | SAML certificate 99 |
|   | secure network access policies 57 |
|   | settings, administrative 99 |
|   | SSL trust and mobile devices 64 |
|   | standard policy sets 53 |
|   | system information 13 |

| T | ThinApp packages  |
|   | deleting 95 |
|   | deploying Horizon Workspace client for Windows 92 |
|   | entitling to users and groups 91 |
|   | overview 90 |
|   | providing access 89 |
|   | ThinApp download mode 90 |
|   | ThinApp Packages module 89 |
|   | ThinApp streaming mode 90 |
|   | token 26 |
|   | troubleshooting  |
|   |   file preview 104 |
|   |   file syncing 105 |
|   |   Horizon Files service 103 |
|   |   sharing a file using previous iOS client 106 |

| U | user password, recovery 99 |
|   | users  |
|   |   assigning a class of service 37 |
attributes 23
removing access 26
rules for adding to groups 19
searching for 15
updating the sync filter to Active Directory 27
viewing information 23
viewing entitlements to Horizon View desktop pools 68
Users report 97

V
vApp, Horizon Workspace 7
View desktop pools, See Horizon View desktop pools
virtual appliances, Horizon Workspace 7
virtual users 7, 17, 27, 35
VMware Ready Android, importing workspace images 50

W
Web applications
adding 71, 72
entitling 76
multitenant 71
Web Client, URL 7
Web application bundle 75
Web Applications module 71
Web client, troubleshooting in Windows 8 in Workstation and VMware Fusion 104
Windows applications 30
workspace images 30
workspace lifetime policies 54
workspace images for VMware Ready Android 50
Workspaces page 23