Horizon Workspace Administrator's Guide

Horizon Workspace 1.0

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.

EN-001063-00

vmware®

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

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

Contents

About the Horizon Workspace Administrator's Guide 1

The *VMware Horizon Workspace Administrator's Guide* provides information and instructions about using and maintaining VMware Horizon Workspace. VMware Horizon Workspace is a platform that allows you to customize a service catalog for company data and applications. This platform provides an end-user management platform for secure, managed-user access to your organization's data and applications, including Windows, SaaS and mobile applications. Horizon Workspace delivers a unified user and application policy and offers your IT department unified security and management for all services and applications across all 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 View, and RSA SecurID, is helpful if you plan to implement these features.

Horizon Workspace Administrator's Guide Overview

Use the *Horizon Workspace Administrator's Guide* after you install Horizon Workspace. See *Horizon Workspace Installation Guide*.

To administer Horizon Workspace, you predominantly use the Horizon Workspace Administrator Web interface. You occasionally need to access the Configurator Web interface, the Connector Web interface, and the virtual appliance interfaces. See "Horizon Workspace Web Interface URLs," on page 11.

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

The tasks you perform as an administrator vary depending on the resource types you plan to manage. You can manage the Data service, View pools, Windows applications (ThinApp packages), Web applications, and mobile applications. The actual resource types you manage vary according to the needs of your enterprise. To entitle a resource type, you must first perform the respective preconfiguration tasks as described in the *Horizon Workspace Installation Guide*.

Introduction to Horizon Workspace for Administrators 2

VMware Horizon™ Workspace provides you with a centralized Web management console that allows you to customize the Catalog, which contains your enterprise's applications and desktops, as well as the Data module, which allows users to share files and folders with others.

Horizon Workspace detects users' attributes and enforces policies across the applications, data, and desktops. For each user, you can customize the delivery of Windows, Android, iOS, Web, and 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 consists of the following virtual appliances bundled together in a vApp.

Table 2-1. Horizon Workspace Server Components

Horizon Workspace Server Component	Description
VMware Horizon Workspace Configurator Virtual Appliance (configurator-va)	You start configuring Horizon Workspace with this virtual appliance, using both the Configurator virtual appliance interface and the Configurator Web interface. The configurations you make with the Configurator are distributed to the other virtual appliances in the vApp.
VMware Horizon Workspace Manager Virtual Appliance (service-va)	Horizon Workspace Manager handles ThinApp package synchronization and gives you access to the Administrator Web interface, from which you can manage users, groups, and resources.
VMware Horizon Workspace Connector Virtual Appliance (connector-va)	Horizon Workspace Connector provides the following services: user authentication (identity provider), directory synchronization, ThinApp-catalog loading, and View pool synchronization.
VMware Horizon Workspace Data Virtual Appliance (data-va)	Horizon Workspace Data Virtual Appliance controls the file storage and sharing service, stores users' data (files), and synchronizes users' data across multiple devices.
VMware Horizon Workspace Gateway Virtual Appliance (gateway-va)	Horizon Workspace Gateway Virtual Appliance 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.

Horizon Workspace User Client Components

Users can access Horizon Workspace with Horizon Web client (an agentless client), Windows client, Mac client, Android client, or 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

Horizon Workspace User Client Component	Description
VMware Horizon Workspace Web Client	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 Data, Horizon View Desktops and Horizon Workspace Web Applications. If an end-user has a ThinApp entitled and is on a Windows system with the Horizon Workspace for Windows Client active, they can also view and launch their local ThinApp packages in the Web Client.
VMware Horizon Workspace Client for Windows	When Horizon Workspace Client for Windows is installed on users' Windows systems, they can access their Horizon Workspace Data 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.
VMware Horizon Workspace Client for Mac	When Horizon Workspace Client for Mac is installed on users' Apple Mac OS X systems, they can access their Horizon Workspace Data locally. When this client is installed, users' personal and shared folders and files are synchronized between their system and Horizon Workspace.
VMware Horizon Workspace Client for Android	When Horizon Workspace Client for Android is installed on users' Android devices, they can access their Data and Web applications. They can also install mobile applications that you have curated from Google Play.
VMware Horizon Workspace Client for iOS	When Horizon Workspace Client for iOS is installed on users' iOS devices, they can access their Data and Web Applications. They can also install mobile applications that you have curated from the Apple App Store. Additionally, if your deployment is configured to access Horizon View desktops, iPad users can view their entitled desktops using Horizon View Client for iOS.

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.

Horizon Workspace Authentication Type	Description
Username/password	Active Directory username/password authentication is the default user authentication method. This method authenticates users directly against your Active Directory.
Kerberos	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).
RSA SecurID	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.

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 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

User Access From Inside the Enterprise Network	User Access From Outside the Enterprise Network
■ Username/password authentication: Functions by default. No additional Connector instances are required for this authentication method when users are inside the enterprise network. ■ Kerberos authentication: Requires an additional Connector instance. ■ RSA SecurID authentication: Not recommended. This authentication method is not recommended for authenticating users who are inside the enterprise network.	■ 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. ■ Kerberos authentication: Not applicable. This authentication method is not an option for authenticating users outside the enterprise network. ■ 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.

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 15 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

URL	User Interface	What you can do here
https://*HorizonWorkspaceFQDN*/admin	Administrator Web interface (Active Directory user)	Manage the Catalog, users and groups, entitlements, reports, etc. (Login as Active Directory user with administrator role.)
https://*HorizonWorkspaceFQDN*/SAAS/login/0	Administrator Web interface (non-Active Directory user)	Use this URL if you cannot login as the Active Directory user with the administrator role. (Log in as an administrator using the username **admin** and the password you set during configuration.)
https://*HorizonWorkspaceFQDN*/web	Web Client (end user)	Manage files, launch applications, or launch View pools. (Login as an Active Directory user or virtual user.)
https://*ConnectorHostname*/hc/admin/	Connector Web interface	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.)
https://*ConfiguratorHostname*/cfg	Configurator Web interface	See system information, check modules, set license key, or set admin password. (Log in as an administrator using the password you set during configuration.)

View Horizon Workspace System and Module Information

3

You can view Horizon Workspace system information and information about the Horizon Workspace modules, the Data module, the Web Applications 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** when you first log in to Horizon Workspace.

Prerequisites

Install and configure Horizon Workspace. As part of the installation, enable the modules you want enabled when you first access the Horizon Workspace administrator Web interface. If you do not enable a module during installation, you can configure it later from 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 enable modules that are not yet enabled, enable them now. See the appropriate topic.

- "Enable the Data Module," on page 30
- "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41
- "Enable the View Module," on page 39
- "Enable the ThinApp Packages Module," on page 55

Managing Users and Groups

4

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, selecting the **Users & Groups** tab gives you a user and group centric view of Horizon Workspace. For example, you can give a user access to a resource by accessing the user's user page, from which you can add a resource entitlement. You could get the same result by taking a resource centric view of Horizon Workspace. In that situation, you would go through the Catalog to access the resource page, from which you could add the user to the resource.

This chapter includes the following topics:

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 Horizon Workspace 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.

Groups let you specify which applications group members can access. Instead of defining access for each individual user, you can define access for a 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.

Virtual Users

The virtual users feature is an optional feature that applies solely to the Data 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 the virtual user feature off while configuring the COS form. See "Edit an Existing Class of Service," on page 32 or "Create a Class of Service," on page 34 for information about the External Folder Sharing Allowed option.

Manage Groups in Horizon Workspace

Creating groups, defining group rules, and deleting groups are tasks you can perform in Horizon Workspace that only apply to Horizon Workspace groups. Entitling groups to resources applies to 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 a Horizon Workspace group, select **Users & Groups > Groups**, select the check box for the Horizon Workspace group name, 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 Group Rules," on page 16.

Configure Group Rules

You can create group rules that define Horizon Workspace group membership.

Defining groups lets you specify which applications group members can access. Instead of defining access for individual users, you can define access for a group and grant access based on the rules for group membership. 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. With rules, you can define which users belong to each group.

Procedure

1 To edit group rules, click the **Users & Groups** tab, click the **Groups** tab, and click the name of the group whose rules you want to edit.

- 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.
- 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 delete directory server groups or define their membership.

2 Click the **Users in this Group** tab.

The **Edit Group Rules** dialog box appears.

3 Click **View Group Rules**.

4 Select an option from the drop-down menu.

Option	Action
Any of the following	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 **Any of the following** for the rules Group Is Sales and Group Is Marketing, sales and marketing staff are granted membership to this group.
All of the following	Grants group membership when all of the conditions for group membership are met. This works like an AND condition. For example, if you select **All of the following** 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.

5 Configure one or more rules for your group.

You can nest rules.

Option	Action
Group	■ Select **Is** to choose a group to associate with this Horizon Workspace group. Type a group name in the text box. As you type, a list of group names appears. ■ Select **Is Not** to choose a group to exclude from this Horizon Workspace group. Type a group name in the text box. As you type, a list of group names appears.
Attribute Rules	The following rules are available for all attributes, including default attributes and any additional custom attributes that your enterprise configured. Examples of attributes are email and phone. NOTE Rules are **not** case-sensitive. ■ Select **Matches** to grant group membership for directory server entries that exactly match the criteria you enter. For example, your organization might have a business travel department that shares the same central phone number. If you want to grant access to a travel booking application for all employees who share that phone number, you can create a rule such as Phone Matches (555) 555-1000. ■ Select **Does Not Match** to grant group membership to all directory server entries except those that match the criteria you enter. For example, if one of your departments shares a central phone number, you can exclude that department from access to a social networking application by creating a rule such as Phone Does Not Match (555) 555-2000. Directory server entries with other phone numbers have access to the application. ■ Select **Starts With** to grant group membership for directory server entries that start with the criteria you enter. For example, your organization's email addresses might begin with the departmental name, such as sales_username@example.com. If you want to grant access to an application to everyone on your sales staff, you can create a rule, such as Email Starts With sales_. ■ Select **Does Not Start With** to grant group membership to all directory server entries except those that start with the criteria you enter. For example, if the email addresses of your human resources department are in the format hr_username@example.com, you can deny access to an application by setting up a rule, such as Email Does Not Start With hr_. Directory server entries with other email addresses have access to the application.
Any of the following	Group membership to be granted when any of the conditions for group membership are met for this rule. This is a way to nest rules. For example, you can create a rule that says All of the following: Group Is Sales; Group is California. For Group is California, Any of the following: Phone Starts With 415; Phone Starts With 510. The group member must belong to your California sales staff and have a phone number that starts with either 415 or 510.
All of the following	All of the conditions to be met for this rule. This is a way to nest rules. For example, you can create a rule that says Any of the following: Group Is Managers; Group is Customer Service. For Group is Customer Service, all of the following: Email Starts With cs_; Phone Starts With 555. The group members can be either managers or customer service representatives, but customer service representatives must have an email that starts with cs_ and a phone number that starts with 555.

6 (Optional) Add specific users to add or exclude by checking the check box and typing user names.

7 Click **Next**, and click **Save**.

View Group Information

You can view information about groups in Horizon Workspace.

Prerequisites

- Install and configure Horizon Workspace. As part of the installation, import users and, if applicable, groups from your directory server. See the *Horizon Workspace Installation Guide*.
- Create Horizon Workspace groups. See "Manage Groups in Horizon Workspace," on page 16.
- Add resources to your Catalog. From your Catalog, you can entitle users of a group to mobile applications, Web applications, and the Data service. The other resources, View Desktops and ThinApp packages, are added to the Catalog outside of the Administrator Web interface. See the *Horizon Workspace Installation Guide*. For instructions about entitling groups to Web applications, mobile referred applications, or the Data service, see the appropriate topic.
  - For Web applications, see "Entitle Users and Groups to Web Applications," on page 45.
  - For mobile referred applications, see "Entitle Users and Groups to Mobile Referred Applications," on page 52.
  - For the Data service, see "Entitle Groups to the Data Service," on page 37.

Procedure

1 To view information about a group, select **Users & Groups > Groups**, and click the name of a group.
   - 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.
   - 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 delete directory server groups or define their membership.

2 Select the information you want to view.

Option	Description
Entitlements	■ You can view the list of resources entitled to the users of the group. ■ **Add Entitlement** allows you to entitle the users of this group to mobile applications, Web applications, and the Data service, as available in your Catalog. ■ Each entitlement name links to that resource's Edit page. ■ **Edit** allows you to edit how that specific resource is deployed to users of the group. ■ **Unentitle** allows you to unentitle users of this group from that specific resource.
Users in this Group	■ A list of users in the group. ■ Each user name links to the user page of that user. ■ **View Group Rules** is an available option for Horizon Workspace groups, but not for directory server groups. The option allows you to view and configure rules that define membership to the Horizon Workspace group.

Manage Horizon Workspace Users

You can manage Horizon Workspace users, the users imported from your directory server.

Using the Administrator Web interface you can view information about Horizon Workspace users and you can entitle the users to resources.

Prerequisites

- Install and configure Horizon Workspace. As part of the installation, import users from your directory server. See the *Horizon Workspace Installation Guide*.
- Add resources to your Catalog. From your Catalog, you can entitle users to mobile applications, Web applications, and the Data service. The other resources, View Desktops and ThinApp packages, are added to the Catalog outside of the Administrator Web interface. See the *Horizon Workspace Installation Guide*. For instructions about entitling groups to Web applications, mobile referred applications, or the Data service, see the appropriate topic.
  - For Web applications, see "Entitle Users and Groups to Web Applications," on page 45.
  - For mobile referred applications, see "Entitle Users and Groups to Mobile Referred Applications," on page 52.
  - For the Data service, see "Entitle Users to the Data Service," on page 37.

View Horizon Workspace User Information

You can view the resource entitlements, group affiliations, and device entitlements of Horizon Workspace users.

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 Select **Users & Groups > Users**.

The page displays a list of all your Horizon Workspace users.

2 Click a user's name.

The user's name, email address, role, and the COS, if one is assigned to them, are listed at the top of the user's page.

3 (Optional) Click **User** or **Administrator** to toggle the user's role.

You can use this toggle to 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.

Web Interface	Required Role	URL Example
Administrator Web Interface	Administrator	https://*HorizonWorkspaceFQDN*/admin
Web Client	User	https://*HorizonWorkspaceFQDN*/web

4 (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 Data service and can appear as an additional attribute for users. The attribute appears when the user is entitled to the Data service. The value assigned to the attribute is the name of the data server to which a user's data is stored. You can use this information for troubleshooting purposes if a user cannot access the Data service.

5 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 Data service, a class of service (COS) is assigned to the user. The COS includes information such as the account quota, maximum file size, and share expiration.

6 Click a tab to manage the resources for a specific user.

Option	Description
Entitlements	■ You can view the resources entitled to the user. ■ **Add Entitlement** allows you to entitle the user to mobile applications, Web applications, and the Data service, as available in your Catalog. ■ Each entitlement name links to that resource's Edit page. ■ **Edit** allows you to edit how that specific resource is deployed to that user. ■ **Unentitle** allows you to unentitle the user from that specific resource.
Group Affiliations	■ You can view the groups to which the user is a member. ■ Each group name represents a group to which the user is a member and links to the page for that group.
Devices	■ You can view the list of device names registered by the user. Device names are added to this list when a device initially connects to Horizon Workspace. To make an initial connection, the user must log in from the device, which requires that a Horizon Workspace client (for Windows, Mac, Android, or iOS) is installed on the device. ■ **Delete** allows you to remove a specific device, for example because the device is lost, stolen, or no longer in use.

Prevent Users from Accessing Horizon Workspace

You can prevent specific directory server users from accessing Horizon Workspace by creating filters in Horizon Workspace or by deleting or disabling directory server user accounts. If you disable user accounts, you must perform specific steps to ensure that the users of the disabled accounts do not continue to have access to Horizon Workspace.

Different methods exist for preventing users from accessing Horizon Workspace. Use the method that best suits the needs of your enterprise.

Table 4-1. Methods for Preventing Specific Users from Accessing Horizon Workspace

Method for Preventing User Access	Description
Create Filters in Horizon Workspace	Using the Connector Web interface of Horizon Workspace, you can create filters to exclude specific users from being transferred from the directory server to Horizon Workspace during synchronizations. If you use the create filters method with existing Horizon Workspace Data users, their shared files and folders are deleted and not retrievable if you later add these users back. See *Installing Horizon Workspace* for information about selecting users.
Delete User Accounts in the Directory Server	When you delete user accounts in the directory server, during the next synchronization, Horizon Workspace invalidates the active tokens associated with the deleted user accounts. As a result, Horizon Workspace users with deleted directory server accounts lose access to Horizon Workspace. See the procedure that follows.
Disable User Accounts in the Directory Server	When you disable user accounts in the directory server, Horizon Workspace does not invalidate the active tokens associated with the disabled user accounts. As a result, Horizon Workspace users with disabled directory server accounts might continue to have access to Horizon Workspace until their associated tokens expire, or until you implement steps to prevent continued access. See the procedure that follows.

Procedure

- Prevent deleted and disabled directory server users from accessing Horizon Workspace by implementing the task that best suits your enterprise.

Option	Steps
Deleted user accounts	After you delete a user account in the directory server, no further configuration is necessary to prevent users from accessing Horizon Workspace.
Disabled user accounts	■ After you disable user accounts in the directory server, prevent the respective users from accessing Horizon Workspace by implementing one of the following tasks, depending on the task that best suits the needs of your enterprise. ■ Use the Connector Web interface to prevent user access to Horizon Workspace by creating filters to exclude the users or groups of users whose accounts you disabled from syncing with Horizon Workspace. See *Installing Horizon Workspace* for information about selecting users. If you implement this task for existing Horizon Workspace Data users, their shared files and folders are deleted and not retrievable if you later add these users back. ■ Use the Administrator Web interface to prevent the users whose accounts you disabled from accessing Horizon Workspace. a Delete the devices of the users whose accounts you disabled. 1 Select **Users & Groups > Users**. 2 Click the name of a user whose account you disabled. 3 Click the **Devices** tab. 4 Click **Delete** and **OK** for every device on the list. b Unentitle the entitled resources of the users whose accounts you disabled. If you implement this task for existing Horizon Workspace Data users, their shared files and folders are not deleted and will be retrieved if you later add these users back.

After the next directory sync, the users whose accounts you deleted or disabled in directory server 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 To view and manage user information, select **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.

2 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.

Managing the Horizon Workspace Catalog

5

The Horizon Workspace Catalog is the repository of all the resources that you can entitle to users. You can view all resource types in the Catalog. You add Web applications and mobile applications to the Catalog directly from the Catalog. You add ThinApp packages and View Pools to the Catalog with configuration tasks performed outside of the Catalog. You add the Data service, the file storage and sharing service, to the Catalog by enabling the Data module.

The Catalog is visible in the **Catalog** tab in the Horizon Workspace Administrator Web interface. In the Catalog you can perform the following tasks:

- Add new resources to the Catalog.
- View the resources to which you can currently entitle users.

You populate the Catalog with Web and mobile applications directly in the **Catalog** tab of the Horizon Workspace Administrator Web interface. For Web applications, you must first enable the Web Applications module.

Data, View pools, and Windows applications captured as ThinApp packages are not added directly from the Catalog.

This chapter includes the following topics:

Overview of Horizon Workspace Resource Types

With Horizon Workspace, you can manage Web applications, mobile applications, Windows applications captured as VMware ThinApp packages, VMware View desktops, and the Data service, the file storage and sharing service.

Web Applications

You populate the Catalog with Web applications directly on the **Catalog** tab of the Horizon Workspace Administrator Web interface. When you click the Web application icon in the Catalog, details about the application appear. You can then configure the application and provide the appropriate SAML attributes to configure single sign-on between Horizon Workspace and the target Web application. You can then entitle users to Web applications. See "Add Resources to the Catalog," on page 27.

Mobile Applications

You populate the Catalog with mobile applications directly on the **Catalog** tab of the Horizon Workspace Administrator Web interface by accessing the Apple App Store or Google Play. You can then entitle users to mobile applications, which serves as a method of recommending users to approved mobile applications. See "Add Resources to the Catalog," on page 27.

ThinApp Packages

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

1 If ThinApp packages to which you want to provide users access do not already exist, create ThinApp packages by capturing Windows applications as ThinApp packages. See VMware ThinApp documentation.

2 Create a Windows applications network share and move the ThinApp packages to it. See *Installing Horizon Workspace.*

3 Configure Horizon Workspace to integrate with VMware ThinApp. See *Installing Horizon Workspace.*

4 Enable the Windows Applications module.

After you perform these tasks, Windows applications, the ThinApp packages that you added to the network share, are now available in the Catalog. You can then entitle users to the Windows applications.

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.

View Desktops

You populate the Catalog with View Pools by performing the following tasks.

1 Configure View pools in VMware View, which includes entitling users to desktops. See VMware View documentation.

2 Integrate your Horizon Workspace deployment with VMware View. see *Installing Horizon Workspace*.

3 Enable the View module. See "Enable the View Module," on page 39.

After you perform these tasks, the View Desktops you entitled to users are now available in the Catalog.

Data Service

1 Perform the Data preconfiguration steps during installation of Horizon Workspace, such as add storage to the Data virtual appliance and configure a Data preview server. See *Installing Horizon Workspace*.

2 Populate the Catalog with the Data resource by enabling the Data module. See "Enable the Data Module," on page 30.

After you perform these tasks, the Data module is now available in the Catalog. You can then entitle users to the Data service, allowing them to share their files and folders with other users. See "Entitle Users to the Data Service," on page 37.

View Horizon Workspace Resources

You can access the Catalog to view Horizon Workspace Web applications, mobile applications, ThinApp packages, View pools, and the Data 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 Data module, Web Applications module, View module, and ThinApp Packages module are available. The Web applications module allows you to entitle users to both Web applications and mobile applications.
- Add resources to the Catalog to meet the needs of your enterprise.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click a tab to list the resources you want to view.

Option	Description
All	Lists all of the resources in the Catalog.
Web Applications	Lists only Web applications in the Catalog. Web applications include SaaS applications and Web applications managed internally by your enterprise.
Mobile Apps	Lists only mobile applications in the Catalog. Mobile applications are applications accessible from supported mobile devices.
ThinApp Packages	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.
View Pools	Lists only the View pools. View pools appear in you Catalog if you integrate Horizon Workspace with VMware View prior to accessing the Administrator Web interface.
Services	Lists only services in the Catalog. The Data service is the only service available.

3 Click a specific resource to view the details of that resource.

Add Resources to the Catalog

You can add Web applications and mobile applications to the Catalog directly in the **Catalog** tab of the Horizon Workspace administrator Web interface.

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

- "Add a Web Application to Your Catalog from the Global Catalog," on page 42
- "Add a Web Application to Your Catalog by Creating a New Application Record," on page 43
- "Add a Web Application to Your Catalog by Importing a ZIP or JAR File," on page 44
- "Add a Mobile Referred Application to Your Catalog from the Global Catalog," on page 48
- "Add a Mobile Referred Application to Your Catalog from Apple App Store," on page 50
- "Add a Mobile Referred Application to Your Catalog from Google Play," on page 51

The following instructions provide an overview of the steps involved.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add Application**.

4 Click an option depending on the resource type, Web application or mobile application, and the location of the application.

Link Name	Resource Types	Description
from your Global Catalog	Web and Mobile Applications	Horizon Workspace includes access to several default Web and mobile applications, available in the Global Catalog, that you can add to your Catalog.
create a new one	Web Applications	By filling out the appropriate form, you can create an application record for the Web applications you want to add to the Catalog.
import a ZIP or JAR file	Web Applications	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.
from Apple App Store	Mobile Applications	You can refer iPhone and iPad applications available in the Apple App Store.
from Google Play	Mobile Applications	You can refer Android applications available in Google Play.

5 Follow the prompts to finish adding resources to the catalog.

Providing Access to the Data Service 6

You can entitle Horizon Workspace users to the Data service. The Data 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 Data 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 Data module, you can then configure the Data Service in the Catalog using the Horizon Workspace Administrator Web interface.

The way users use the Data service is defined by a COS. A class of service (COS) is a set of file storage and sharing attributes, such as account quota, maximum file size allowed, file types disallowed, and so on. Horizon Workspace includes a default class of service. You can edit the default class of service and create new classes of service. You can assign a COS 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:

Entitling and Provisioning Users to the Data Service

To use the Data service, users must be entitled and provisioned to the service. If Horizon Workspace is functioning normally, when you entitle users to the Data service, the service automatically provisions them.

When you entitle the Data 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 Data service. When you view user and group entitlements to the Data service, you can view users' provisioning status to determine if a provisioning-related problem exists.

CAUTION The Data 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 Data 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 Data service again. Entitling and unentitling the same user to and from the Data service does not cause this issue.

The Data 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 Data service treats the user as a different user attempting to use an existing email address. The Data 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 *CLI Commands for Horizon Workspace Data*.

Enable the Data Module

To allow Horizon Workspace users to share files and folders, enable the Data module.

Prerequisites

Install Horizon Workspace. As part of the installation, implement the Data module preconfiguration steps, such as adding storage and configuring a document preview application. See the *Horizon Workspace Installation Guide*.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 On the **Dashboard** tab, click the **Enable** link in the Data module.

The Data module is now enabled.

What to do next

- Edit the default class of service (COS), create a COS, or both. See "Class of Service," on page 31
- Verify the distribution of the appropriate Horizon Workspace clients to users' desktops and mobile devices.

  For Mac and Windows systems, users can use a browser (Horizon Workspace Web Client) to access the Data service. For a native experience, users can use the Horizon Workspace native clients on iOS, Android, Windows and Mac operating system. For example, using Horizon Workspace for Windows, the user can modify files and add folders using Windows Explorer.

  Therefore, on Windows and Mac systems, the best practice for users is to install the respective client, Horizon Workspace Client for Mac or Horizon Workspace Client for Windows. 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 for Desktop*. However, for Windows systems, you can silently install Horizon Workspace Client for Windows to multiple Windows systems at once. See "Silently Deploy Horizon Workspace Client for Windows on Users' Windows Systems," on page 58

Class of Service

When you entitle users or groups to the Data 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 Data module, you can edit the default class of service to fit your enterprise needs. You can also create one or more additional classes of service.

To provide Horizon Workspace users or groups access to the file storage and sharing service, entitle them to the Data service, which involves assigning a COS to them.

CAUTION As a best practice, when your Horizon Workspace deployment contains two or more Data servers and you edit or create a new COS, wait 15 minutes before you entitle users to the Data service. Fifteen minutes is the refresh interval for Data 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 Data service multiple times, which can result in the assignment of several different classes of service. 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 Data service by adding user entitlements and group entitlements. Through this process, you can entitle users to the Data service multiple times with several different classes of service. A single COS determines the file storage and sharing policy of a given user. The name of that COS is listed on the user's page accessible in the Administrator Web interface by selecting **User & Groups > Users** and clicking the user's name.

Horizon Workspace follows specific criteria to select the COS out of a user's assigned classes of service that determines the user's file storage and sharing policy.

User Entitlement Takes Precedence

A COS assigned to a user as a user entitlement takes precedence over a COS assigned to the user as a group entitlement. A user can only have one user entitlement to the Data service, but can be a member of an unlimited number of groups that each have a group entitlement to the Data service. In such a situation, a user can be assigned to several different classes of service. 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 as a user entitlement, but has multiple classes of service assigned as group entitlements, Horizon Workspace enforces file storage and sharing policy according to the order of groups in the Group Entitlements section of the Data page. To access the Data page, in the Administrator Web interface, select **Catalog > Services > Data**. The Group Entitlements section lists all the groups entitled to the Data service. Some of the groups might have an assigned COS and some might not. The group highest on the list that has an assigned 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 entitling the user to the Data service again.

If a user has a user entitlement to the Data service, you can change the COS that determines the user's file storage and sharing policy by adding another user entitlement with a different COS for that user to the Data service.

If a user is entitled to the Data service through a group entitlement, you can change the COS that determines the user's file storage and sharing policy by adding another group entitlement with a different COS for that group to the Data service. This action can change the file storage and sharing policy of 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 the default class of service. You might want to edit the default COS settings to suit your enterprise needs. If you create a new class of service, you can edit it in the future.

The Administrator Web interface is the main tool for configuring the Horizon Workspace Data service, but some Horizon Workspace Data functionality can only be configured using the CLI utility. *See Using CLI Commands for Workspace Data Administrator Tasks*

CAUTION If you assign a COS to users, then configure an existing setting in the COS, such as Account Quota or Max File Size, 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.

Prerequisites

Enable the Data module.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Select **Catalog > Services**.

3 Click the **Data** resource.

4 Click **Class of Service**.

5 Click **Edit** for the COS you want to edit.

6 Edit the Edit Class of Service form as appropriate.

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

Form Item	Description
COS Name	The name for the class of service. After you create a COS, you cannot edit the COS name.
Description	Optional. A description for the class of service.
Account Quota (MB)	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.
Quota Warning Msg	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.
Threshold (%)	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.
Minimum duration of time between quote warnings	The frequency with which the quota warning email message is sent.
Max File size (MB)	The maximum size of a file that users can upload to Horizon Workspace.

Form Item	Description
File Types Disallowed	Extensions for file types you want to block. Users cannot upload files with these extensions to Horizon Workspace.
Trashed File Lifetime Value	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.
Internal Expiration	The amount of time shared files and folders can be accessed by your enterprise's Horizon Workspace users.
External Folder Sharing Allowed	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.
Public Sharing of Files	When this box is checked, Horizon Workspace users can make files available on the Internet.
External Expiration	The amount of time shared folders can be accessed by virtual users.
Public Expiration	The amount of time files are accessible on the Internet.
Domains Allowed or Not Allowed	This option enables you to restrict or allow virtual-user access to shared folders based on the virtual user's domain. When you check a radio button for this option, you select one of the following external folder sharing controls: ■ **No Domain Policy** to allow all external domains potential access to folders shared by Horizon Workspace users. ■ **Allowed** to show the following text box: Allowed domains for external sharing. ■ **Restricted** to show the following text box: Restricted domains for external sharing.
Allowed domains for external sharing	This option allows you to grant virtual users from specified domains access to shared folders
Restricted domains for external sharing	This option allows you to prevent virtual users from specified domains from accessing shared folders.
Host Pool	This option is applicable when your Horizon Workspace deployment contains two or more Data servers. When you add a new Data server to your deployment, it appears in the Host Pool list. You can select the Data server to which newly provisioned users are assigned. The user's data is then stored in the assigned Data server. When either no server is selected or all servers are selected, the Data service assigns new users evenly among all servers in the list. When you select more than one server, the Data service assigns new users evenly among the selected servers. Horizon Workspace uses the Host Pool setting to assign users to specific Data servers. After users are assigned to a Data server, you cannot change the assigned Data 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 Data server. The Data 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 user page. Select **Users & Groups > Users** and click the user's name.
Pin/Passcode Required	When this box is checked, mobile-device users are prompted to set up a passcode to access Horizon Workspace from their mobile devices.
Open/Edit with	This box is checked by default. When this box is checked, users can use third-party applications on their mobile devices to edit files.

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 associate users and groups to specific classes of service. See "Data Entitlements," on page 37.

Create a Class of Service

You can create a class of service with which to entitle users to the Data service, the file storage and sharing service.

Horizon Workspace includes the default class of service that you can use as is, or edit. You also can create a class of service.

The Administrator Web interface is the main tool for configuring the Horizon Workspace Data service, but some Horizon Workspace Data functionality can only be configured using the CLI utility. *See Using CLI Commands for Workspace Data Administrator Tasks*

CAUTION If you assign a COS to users, then configure an existing setting in the COS, such as Account Quota or Max File Size, 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.

Prerequisites

Enable the Data module.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Select **Catalog > Services**.

3 Click the **Data** resource.

4 Click **Class of Service**.

5 Use a class of service template that best suits your needs.

Option	Action
Use the default class of service template.	Click **Add a new COS**.
Use an existing class of service as a template.	Click **Copy** to duplicate the existing class of service

6 Complete the Add a new Class of Service form.

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

Form Item	Description
COS Name	The name for the class of service. After you create a COS, you cannot edit the COS name.
Description	Optional. A description for the class of service.
Account Quota (MB)	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.
Quota Warning Msg	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.
Threshold (%)	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.

Form Item	Description
Minimum duration of time between quote warnings	The frequency with which the quota warning email message is sent.
Max File size (MB)	The maximum size of a file that users can upload to Horizon Workspace.
File Types Disallowed	Extensions for file types you want to block. Users cannot upload files with these extensions to Horizon Workspace.
Trashed File Lifetime Value	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.
Internal Expiration	The amount of time shared files and folders can be accessed by your enterprise's Horizon Workspace users.
External Folder Sharing Allowed	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.
Public Sharing of Files	When this box is checked, Horizon Workspace users can make files available on the Internet.
External Expiration	The amount of time shared folders can be accessed by virtual users.
Public Expiration	The amount of time files are accessible on the Internet.
Domains Allowed or Not Allowed	This option enables you to restrict or allow virtual-user access to shared folders based on the virtual user's domain. When you check a radio button for this option, you select one of the following external folder sharing controls: ■ **No Domain Policy** to allow all external domains potential access to folders shared by Horizon Workspace users. ■ **Allowed** to show the following text box: Allowed domains for external sharing. ■ **Restricted** to show the following text box: Restricted domains for external sharing.
Allowed domains for external sharing	This option allows you to grant virtual users from specified domains access to shared folders
Restricted domains for external sharing	This option allows you to prevent virtual users from specified domains from accessing shared folders.
Host Pool	This option is applicable when your Horizon Workspace deployment contains two or more Data servers. When you add a new Data server to your deployment, it appears in the Host Pool list. You can select the Data server to which newly provisioned users are assigned. The user's data is then stored in the assigned Data server. When either no server is selected or all servers are selected, the Data service assigns new users evenly among all servers in the list. When you select more than one server, the Data service assigns new users evenly among the selected servers. Horizon Workspace uses the Host Pool setting to assign users to specific Data servers. After users are assigned to a Data server, you cannot change the assigned Data 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 Data server. The Data 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 user page. Select **Users & Groups > Users** and click the user's name.
Pin/Passcode Required	When this box is checked, mobile-device users are prompted to set up a passcode to access Horizon Workspace from their mobile devices.
Open/Edit with	This box is checked by default. When this box is checked, users can use third-party applications on their mobile devices to edit files.

7 Click **Save**.

What to do next

After you configure one or more classes of service, you can associate users and groups to specific classes of service. See "Data Entitlements," on page 37.

View the Associated Class of Service for Users or Groups

You can view a COS that is associated with a user or group.

After you entitle users to the Data service, you can continue using the Horizon Workspace Administrator Web interface to view which COS a user or group is associated with.

Prerequisites

- Enable the Data module. See "Enable the Data Module," on page 30
- Configure one or more classes of service. See "Edit an Existing Class of Service," on page 32 or "Create a Class of Service," on page 34.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 View the class of service associated with users and groups.

Option	Action
List all Data entitlements.	a Select **Catalog > Services**. b Click the **Data** resource. The **Entitlements** tab is selected by default. Group Entitlements and User Entitlements are listed in separate tables. The class of service 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.	a Click the **Users & Groups** tab. b Click the **Users** tab or the **Groups** tab. c Click the name of an individual user or group. If the user or group has an associated COS, the name of the COS appears as a link to the 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 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Select **Catalog > Services**.

3 Click the **Data** resource.

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 assigned to those users and groups.

Data Entitlements

To allow users to share files and folders, you must entitle them to the Data service, which involves assigning a class of service (COS) to users or groups.

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 Data service by assigning a class of service to them. See "Class of Service," on page 31. You assign a class of service to users by adding either a new user entitlement or a new group entitlement.

Entitle Users to the Data Service

You can entitle individual users to the Data service, which includes assigning the users to a class of service.

In many cases, the most effective way to entitle users to the Data service is to add a Data entitlement to a group of users. In certain situations, entitling individual users to the Data service is more appropriate.

Prerequisites

- Configure one or more classes of service as appropriate for the file storage and sharing needs of your enterprise.
- Review "Criteria for Class of Service Precedence," on page 31.

Procedure

1. Using a browser, log in to the Horizon Workspace Administrator Web interface.
2. Select **Users & Groups > Users**.
3. Click the name of a user to whom you want to entitle the Data service.
4. Click **Add Entitlement**.
5. Click the check box for the **Data** resource.
6. From the **Active COS** drop-down menu, select the COS to which you want to assign 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 Data Service

You can entitle the users in a group to the Data service, which includes assigning the group to a class of service.

In many cases, the most effective way to entitle users to the Data service is to add a Data entitlement to a group of users.

Prerequisites

- Configure one or more classes of service as appropriate for the file storage and sharing needs of your enterprise.
- Review "Criteria for Class of Service Precedence," on page 31.

Procedure

1. Using a browser, log in to the Horizon Workspace Administrator Web interface.
2. Select **Users & Groups > Groups**.
3. Click the name of a group to which you want to entitle the Data service.

4 Click **Add Entitlement**.

5 Click the check box for the **Data** resource.

6 From the **Active COS** drop-down menu, select the COS to which you want to entitle the group.

7 Click **Save**.

The result might vary for users in the group according to 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 31.

7 Providing Access to View Desktops

View is a Horizon Workspace module that enables users to access their entitled VMware View desktops using Horizon Workspace.

You integrate VMware View with Horizon Workspace as part of the installation process. See *Installing Horizon Workspace*. Entitle Horizon Workspace users to VMware View pools using the View Connection Server. To complete the integration of VMware View with Horizon Workspace, enable the View module. See "Enable the View Module," on page 39. You can then monitor user and group entitlements to View pools using the Horizon Workspace Administrator Web interface.

This chapter includes the following topics:

Enable the View Module

To allow Horizon Workspace users to access View desktops through the Horizon Workspace Web Client, you must first enable the View module.

Prerequisites

- Deploy VMware View in your enterprise, which includes entitling users to View pools directly in the View Connection Server instance and installing View Client on users' systems.
- See *Horizon Workspace Installation Guide* for instructions on integrating VMware View with Horizon Workspace.

Procedure

- Integrate VMware View with Horizon Workspace, either while you are installing Horizon Workspace or after you install Horizon Workspace by using the Connector Web interface. Integration includes enabling the View module.

The View module is now enabled.

What to do next

Monitor user and group entitlements to View pools. See "View User and Group Entitlements to VMware View Pools," on page 40.

View User and Group Entitlements to VMware View Pools

You can see to which View pools users and groups are entitled.

IMPORTANT You cannot use Horizon Workspace to make changes to View pools. If a View administrator makes any changes to View Pools, such as by entitling and unentitling users, or by changing the supported client types, you must implement a View pool sync from Horizon Workspace to propagate the changes to Horizon Workspace. See *Installing Horizon Workspace*.

Prerequisites

Configure Horizon Workspace to sync View pool information and the respective entitlements from View Connection Server instances. You can perform this synchronization task when you first install Horizon Workspace or any time after installation using the Connector Web interface. This task connects Horizon Workspace to one or more View Connection servers, which makes the View pools defined in the View Connection servers available in the Catalog.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 View user and group entitlements to View pools.

Option	Action
View the list of users and groups entitled to a specific View pool.	a Select **Catalog > View Pools**. b Click the icon for the View 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 View pool entitlements for a specific user or group.	a Click the **Users & Groups** tab. b Click the **Users** tab or the **Groups** tab. c Click the name of an individual user or group. A page appears with a list of entitled resources for that user or group. View pools, if any, are listed among the other entitled resources for that user or group.

View the Connection Information for a View Pool

You can view the information about the connection between Horizon Workspace and a View pool.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Select **Catalog > View Pools** and click a View pool.

3 Click the **Details** tab.

4 View the connection information, which consists of attributes retrieved from the View Connection Server instance.

See VMware View documentation for details about these attributes.

Providing Access to Web Applications 8

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 multi-tenant application, Horizon Workspace points to your instance of the application.

Enabling the Web Applications module allows you to add both Web and mobile applications to your Catalog using the Horizon Workspace Administrator Web interface.

This chapter includes the following topics:

Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access

To allow Horizon Workspace users to access Web applications and mobile referred applications, you must enable the Web Applications module.

Prerequisites

Install Horizon Workspace. See the *Horizon Workspace Installation Guide*.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 On the **Dashboard** tab, click the **Enable** link in the Web Applications module.

The Web Applications module is now enabled.

What to do next

Add Web applications and Mobile referred 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 Catalog," on page 42. Configure mobile referred applications as necessary. See "Overview of Mobile Referred Applications," on page 47.

Overview of Adding Web Applications to Your Catalog

Adding a Web application to your Catalog involves pointing Horizon Workspace to an existing Web application. Three methods exist for creating an appropriate pointer to the Web application.

After you have enabled the Web Applications module, you must add Web applications to the Catalog and configure them individually. When you add a Web application to the Catalog, you are actually adding an application record, a form that includes a URL to the pre-existing Web application. You have three ways to add a Web application to your Catalog.

Link Name	Description
from your Global Catalog	Horizon Workspace ships with 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.
create a new one	You can add Web applications to your Catalog that are not provided in the Global Catalog. The application record for Web applications that do not ship with Horizon Workspace are slightly more generic than that of Global Catalog applications. In this situation, you must create the application record form from scratch.
import a ZIP or JAR file	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.

Add a Web Application to Your Catalog from the Global Catalog

The Web applications in the Global Catalog come with some information pre-populated in the application record, which is a template that Horizon Workspace uses to establish a connection with the Web application using SAML. 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 Web applications to the Catalog you are actually creating a link in the Catalog indirectly to the Web application. The Global Catalog comes populated with several Web applications and mobile referred applications.

Prerequisites

Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add an Application**.

4 Click **from your Global Catalog** in the Add Web Application section.

5 Click the icon of the Web application in the Global Catalog that you want to add to your enterprise's Catalog.

6 If not already selected, click **Details**, edit the Basic Information form as necessary, and click **Save**.

Form Item	Description
Application Name	If necessary, edit the name of the application.
Description	Optional. Edit the description of the application.

Form Item	Description
Icon	Optional. Use the **Browse** 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** link, edit the application record as necessary, and click **Save**.

Some of the items on the form are pre-populated with information specific to the Web application. Some of the pre-populated 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 and Configure the remaining links as appropriate: **Entitlements**, **Licensing**, and **Provisioning**.

Link	Description
Entitlements	Click this link to entitle users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future.
Licensing	Click this link to configure license tracking. Add license information for the application to track license usage in reports.
Provisioning	Click this link to select a provisioning adapter. Horizon Workspace ships with the provisioning adapters for the two following Web applications: Google Apps and Mozy. 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, as well.

What to do next

See "Entitle Users and Groups to Web Applications," on page 45 for details about adding user and group entitlements for Web applications.

Add a Web Application to Your Catalog by Creating a New Application Record

You create an application record from scratch when the Web application that you want to add to the Catalog is not available in the Global Catalog. When you successfully complete the application record for a Web application, the Web application and Horizon Workspace are able to communicate with each other using SAML.

When you add Web applications to the Catalog you are actually creating a link in the Catalog indirectly to the Web Application.

Prerequisites

Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add an Application**.

4 Click **create a new one**.

5 If not already selected, click **Details** and complete the Basic Information form.

Form Item	Description
Application Name	Provide the name of the application.
Description	Optional. Provide a description of the application.
Icon	Optional. Use the **Browse** 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.

6 Click the **Configuration** link, edit the application record as necessary, and click **Save.**

Some of the items on the form are pre-populated while others are not.

The Configure Via section allows you to select how the application metadata is retrieved, Auto-discovery, Meta-data XML, or Manual configuration.

- Configure Via Auto-discovery (meta-data) URL.

  If the XML metadata is accessible on the Internet, provide the URL.

- Configure Via Meta-data XML.

  If the XML metadata is not accessible on the Internet, but is available to you, paste the XML in the text box provided

- Configure Via Manual configuration.

  If the XML metadata is not available to you, complete the XML manual configuration items.

7 Select and Configure the remaining links as appropriate: **Entitlements**, **Licensing**, and **Provisioning**.

Link	Description
Entitlements	Click this link to entitle users and groups to the appplication. You can configure entitlements while initially configuring the application or anytime in the future.
Provisioning	Click this link to select a provisioning adapter. Horizon Workspace ships with the provisioning adapters for the two following Web applications: Google Apps and Mozy. 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, as well.

What to do next

See "Entitle Users and Groups to Web Applications," on page 45 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

This process involves exporting the application bundle of a Web application from a Horizon Workspace instance and importing the bundle into 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. See "Add a Web Application to Your Catalog from the Global Catalog," on page 42 or "Add a Web Application to Your Catalog by Creating a New Application Record," on page 43 if you want to further configure the Web application after importing it.

Prerequisites

You can import a Web application that you previously configured in Horizon Workspace.

- Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.
- Add a Web application to your Catalog by choosing either of the following options: **from your Global Catalog** or **create a new one**. See "Add a Web Application to Your Catalog from the Global Catalog," on page 42 and "Add a Web Application to Your Catalog by Creating a New Application Record," on page 43 respectively.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface of the Horizon Workspace instance from which you want to export a Web application.

2 Click the **Catalog** tab.

3 Click the icon of the Web application in your Catalog that you want to export.

4 Click **Export this Application**.

5 Click **Export.**

6 Save the zipped application bundle to your local system.

7 Using a browser, log in to the Horizon Workspace Administrator Web interface of the Horizon Workspace instance to which you want to import the Web application.

8 Click the **Catalog** tab.

9 Click **Add an Application**.

10 Click **import a zip or jar file**.

11 Browse to the location on your local system where you saved the compressed application bundle as a ZIP file and click **Submit**.

12 Edit the Details Configuration, Entitlements, Licensing and Provisioning pages as necessary.

What to do next

See "Entitle Users and Groups to Web Applications," on page 45 for details about adding user and group entitlements for Web applications.

Entitle Users and Groups to Web Applications

You can entitle users and groups to Web applications.

You can only entitle Horizon Workspace users, users 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 the user interface. If you remove the entitlement, the user cannot see or launch the application.

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 Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.
- Add one or more Web applications to your Catalog. See "Overview of Adding Web Applications to Your Catalog," on page 42.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Entitle users to a Web application.

Option	Description
Access a Web application and entitle users or groups to it.	a Select **Catalog > Web Applications**. b Click the Web application to which you want to entitle users and groups. The **Entitlements** tab is selected by default. Group Entitlements are listed in one table while User Entitlements are listed in another. c Click **Add group entitlement** or **Add user entitlement** as appropriate. d 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.. e Use the drop-down menu to select how to activate each selected Web application: Automatic or User-Activated. ■ Automatic: Users have immediate access to the Web application the next time they log in to the Horizon Workspace Web Client. ■ User-Activated: Users must activate the Web application from the Horizon Workspace Web Client before they can use the application. f Click **Save**.
Access a user or group and add Web application entitlements to that user or group.	a Click the **Users & Groups** tab. b Click the appropriate tab: **Users** or **Groups**. c Click the name of an individual user or group. d Click **Add Entitlement**. e Click the check boxes next to the Web applications to which you want to entitle the user or group. f Use the drop-down menu to select how to activate each selected Web application: Automatic or User-Activated. ■ Automatic: Users have immediate access to the Web application the next time they log in to the Horizon Workspace Web Client. ■ User-Activated: Users must activate the Web application from the Horizon Workspace Web Client before they can use the application. g Click **Save**.

The selected user or group is now entitled to use the Web application.

Providing Access to Mobile Referred Applications

9

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 Web Applications module. Enabling the Web Applications module allows you to add both Web applications and mobile referred applications to your Catalog using the Horizon Workspace Administrator Web interface. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.
- Verify that users install the appropriate client on their mobile devices: Horizon Workspace Client for Android or Horizon Workspace Client for iOS.

Overview of Mobile Referred Applications

Adding a mobile referred application to your Catalog allows you to use Horizon Workspace to recommend a mobile application to users for download. To see the application on their devices, Horizon Workspace users must download the application from the appropriate store to a compatible mobile device.

Adding Mobile Referred Applications to Your Catalog

After you have enabled the Web Applications module, you can add mobile referred applications to the Catalog. When you add a mobile referred application to the 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, they have access to the application 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 48. If users who have access to a mobile referred application choose to install the application on their device, the application appears on their mobile phone launcher. From that point forward, they can launch that application from their mobile phone launcher. Launching a mobile referred application from the Horizon Workspace user interface is not an option.

You have three ways to add a mobile referred application to your Catalog.

Link Name	Description
...from your Global Catalog	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.
...from Apple App Store	You can add mobile applications available in Apple App Store to your Catalog that are not provided in the Global Catalog.
...from Google Play	You can add mobile applications available in Google Play to your Catalog that are not provided in the Global Catalog.

User Access to Mobile Referred Applications

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

- Entitle the user to the mobile referred application.
- The user's device must meet the minimum requirements of the application. If the user's device does not meet the minimum requirements of the application, the application will not appear in the user's list of available mobile referred applications. The following examples illustrate how the compatibility requirements work.
  - If a mobile application is compatible with Android 2.3 devices, the user's device must run on Android 2.3 or greater for the user to see the mobile referred application using Horizon Workspace Client for Android.
  - If a mobile application is compatible with iOS 5.0.1 on an iPad, the user's device must be an iPad running iOS 5.0.1 or greater for the user to see the mobile referred application using Horizon Workspace Client for iOS.

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 Apple App Store or Google Play. To 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 edit it.

When you add mobile referred applications to the Catalog you are actually creating a link in the Catalog to the mobile application in Apple App Store or Google Play. Through this process you can recommend mobile applications to users for download. Once users download a mobile referred application, they do not use Horizon Workspace again to access the application. The Global Catalog comes populated with several mobile referred applications.

Prerequisites

Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add an Application**.

4 Click **from your Global Catalog** in the Add a Mobile Application section.

5 Click the icon of the mobile application in the Global Catalog that you want to add to your enterprise's Catalog.

6 If not already selected, click **Details** and edit the Basic Information form, if necessary.

Form Item	Description
Application Name	If necessary, edit the name of the application.
Description	Optional. Edit the description of the application.
Icon	Optional. Use the **Browse** 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** link, edit the application record as necessary, and click **Save**.

The items on this form are pre-populated with information specific to the mobile application. The application record varies slightly depending on the operating system of the mobile application.

Table 9-1. Application Record for Android Applications

Form Item	Description
Application ID	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 install URL of the application. For example, an application called exampleApp might use the following URL: https://play.google.com/store/apps/details?id=com.exampleApp.android. For the preceding example, the application ID is as follows: com.exampleApp.android
Install URL	If necessary, edit the install 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: https://play.google.com/store/apps/details?id=com.exampleApp.android. 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.
Minimum API Level	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, which is accessible with the install URL. Search the Internet to find which API levels are associated with which Android versions.

Table 9-2. Application Record for iOS Applications

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 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.
Install URL	If necessary, edit the install 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 install 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 install URL.

8 Select **Entitlements** and configure as appropriate.

Click this link to entitle users and groups to the 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 52 for details about adding user and group entitlements for mobile referred applications.

Add a Mobile Referred Application to Your Catalog from 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 create an application record for the application and point it to the application in Apple App Store.

When you add mobile referred applications to the Catalog for iOS devices you are actually creating a link in the Catalog to the mobile application in Apple App Store. Through this process you can recommend mobile applications to users for download. Once users download a mobile referred application, they do not use Horizon Workspace again to access the application.

Prerequisites

- Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.
- Access the page of an iOS application that you want to add to your Catalog from 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 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add an Application**.

4 Click **from Apple App Store** in the Add a Mobile Application section.

5 If not already selected, click **Details**, complete the Basic Information form with information about an application you want to add to your Catalog and click **Next**.

Form Item	Description
Application Name	Provide the application name as listed on the Apple App Store page for the application
Description	Optional. Provide a description of the application.
Icon	Optional. Use the **Browse** 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.

6 Click the **Configuration** link, complete the application record, and click **Save**.

Form Item	Description
Application ID	Provide the ID for this application. 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.
Install URL	Provide the install 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	Provide the minimum iOS version upon which the application can operate. Find minimum version information on the Apple App Store page for the application, which is accessible with the install URL.
Devices Supported	Use the drop-down menu to set the supported devices for this application. Find supported device information on the Apple App Store page for the application, which is accessible with the install URL.

7 Select **Entitlements** and configure as appropriate.

Click this link to entitle users and groups to the 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 52 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 create an application record for the application and point it to the application in Google play.

When you add mobile referred applications to the Catalog for Android devices you are actually creating a link in the Catalog to the mobile application in Google play. Through this process you can recommend mobile applications to users for download. Once users download a mobile referred application, they do not use Horizon Workspace again to access the application.

Prerequisites

- Enable the Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.
- 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 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Click the **Catalog** tab.

3 Click **Add an Application**.

4 Click **from Google play** in the Add a Mobile Application section.

5 If not already selected, click **Details**, complete the Basic Information form with information about an application you want to add to your Catalog and click **Next**.

Form Item	Description
Application Name	Provide the application name as listed on the Google play page for the application
Description	Optional. Provide a description of the application.
Icon	Optional. Use the **Browse** 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.

6 Click the **Configuration** link, complete the application record, and click **Save**.

Form Item	Description
Application ID	Provide the ID for this application. Use a browser to search the Google play Web site for the application. Find the application ID within the install URL of the application. For example, an application called exampleApp might use the following URL: https://play.google.com/store/apps/details?id=com.exampleApp.android. For the preceding example, the application ID is as follows: com.exampleApp.android
Install URL	Provide the install 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: https://play.google.com/store/apps/details?id=com.exampleApp.android. 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.
Minimum API Level	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, which is accessible with the install URL. Then, search the Internet to find which API levels are associated with which Android versions.

7 Select **Entitlements** and configure as appropriate.

Click this link to entitle users and groups to the 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 52 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 users to a mobile referred application, they can see the reference to the application in the Horizon Workspace user interface and can choose to install the application on the their devices. 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 remove 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 Web Application Module. See "Enable the Web Applications Module to Provide Web Application and Mobile Referred Application Access," on page 41.

- Add one or more mobile referred applications to your Catalog. See "Overview of Mobile Referred Applications," on page 47.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Entitle users to a mobile referred application.

Option	Description
Access a mobile referred application and entitle users or groups to it.	a Select **Catalog > Mobile Apps**. b Click 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 table while User Entitlements are listed in another. c Click **Add group entitlement** or **Add user entitlement** as appropriate. d 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.. e Click **Save**.
Access a user or group and add mobile referred application entitlements to that user or group.	a Click the **Users & Groups** tab. b Click the appropriate tab: **Users** or **Groups**. c Click the name of an individual user or group. d Click **Add Entitlement**. e Click the check boxes next to the mobile referred applications to which you want to entitle the user or group. f Click **Save**.

The selected users or groups are now entitled to access the mobile referred application using the Horizon Workspace user interface of their mobile devices.

Providing Access to VMware ThinApp Packages 10

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

To allow Horizon Workspace users to access ThinApp packages, you must enable the ThinApp Packages module.

Prerequisites

- If necessary, create ThinApp packages using VMware ThinApp 4.72 or later. See VMware ThinApp documentation.
- Populate a Windows application network file share, a Windows CIFS share accessed over SMB, with ThinApp packages for Horizon Workspace. See *Installing Horizon Workspace*.
- Install Horizon Workspace. See the *Horizon Workspace Installation Guide*

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 On the **Dashboard** tab, click the **Enable** link in the ThinApp Packages module.

The ThinApp Packages module is now enabled and the ThinApp packages you previously added to Windows application network file share are visible in your Catalog.

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 56.

Overview of ThinApp Packages

For users to access ThinApp packages, Horizon Workspace Client for Windows must be installed on their Windows systems. You determine how to deploy the client. 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 VMware View desktop. The client is used for both the Data service, the file storage and sharing service, and ThinApp packages. While Horizon Workspace Client for Windows enhances the user experience with the Data 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 Horizon Workspace Client for Windows. 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. ThinApp download mode is the default deployment mode. Users do not have the option of selecting the deployment mode. To select ThinApp streaming mode, install Horizon Workspace Client for Windows silently.

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 58.

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 10-1. User Access to Applications Captured as ThinApp Packages

Mode	Description
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: ■ VMware View stateless desktops with excellent connectivity to the file share ■ View physical desktops with excellent connectivity to the file share ■ Users with non-View physical 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 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 user interface. 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 the Catalog with the Administrator Web interface. Therefore, you cannot add ThinApp packages to the Catalog directly from the Catalog.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Entitle users to a ThinApp package.

Option	Description
Access a ThinApp package and entitle users or groups to it.	a Select **Catalog > ThinApp Packages**. b Click the ThinApp package to which you want to entitle users and groups. The **Entitlements** tab is selected by default. Group Entitlements are listed in one table while User Entitlements are listed in another. c Click **Add group entitlement** or **Add user entitlement** as appropriate. d 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.. e Use the drop-down menu to select how to activate each selected ThinApp package: Automatic or User-Activated. ■ Automatic: Users have immediate access to the ThinApp package the next time they log in to Horizon Workspace. ■ User-Activated: Users must activate the ThinApp package in Horizon Workspace before they can use the application. f Click **Save**.
Access a user or group and add ThinApp package entitlements to that user or group.	a Click the **Users & Groups** tab. b Click the appropriate tab: **Users** or **Groups**. c Click the name of an individual user or group. d Click **Add Entitlement**. e Click the check boxes next to the ThinApp packages to which you want to entitle the user or group. f Use the drop-down menu to select how to activate each selected ThinApp package: Automatic or User-Activated. ■ Automatic: Users have immediate access to the ThinApp package the next time they log in to the Horizon Workspace. ■ User-Activated: Users must activate the ThinApp package in Horizon Workspace before they can use the application. g Click **Save**.

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

What to do next

Verify that the Horizon Workspace 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 Data 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 Data service. See "Deploying Horizon Workspace Client for Windows," on page 56. To provide the Data 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 Horizon Workspace*.
  - To enable users to share files and folders, as part of the Horizon Workspace installation, implement the steps related to the Data 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," on page 55.
  - Determine how you want ThinApp packages to deploy: ThinApp streaming mode or ThinApp download mode. See "Determining the Appropriate Deployment Mode for ThinApp Package Access," on page 56
- If making the Data service available to Horizon Workspace users, perform the prerequisites in the Horizon Workspace Administrator Web interface specific to the Data service.
  - Enable the Data module. See "Enable the Data Module," on page 30.
  - Associate users with classes of service. See "Data Entitlements," on page 37

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.

2 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:

- `nnnnn` 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`** or blank denotes streaming mode. If unspecified, the default value of **`0`** 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. Using a browser, log in to the Horizon Workspace 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.

Viewing Horizon Workspace Reports 11

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.

This chapter includes the following topics:

Resource Usage Report

The Resource Usage report is a list of all your resources with respective details for each resource, such as number of users and licenses.

Resource Entitlement Reports

Resource Entitlement reports list the user and group entitlements for a resource you specify.

Group Membership Reports

Group Membership reports list the members of a group you specify.

Users Report

The Users report is a list of all your Horizon Workspace users, with details provided about each user, such as the email address, role, and group affiliations.

Data Usage Report

The Data Usage report is a list of all the Data service accounts, with details provided for each account, such as quota allotted, percent of quota used, and the assigned Data server.

The information for the Data Usage report is sent from the Data server instances approximately every hour. When viewing the Data Usage report, account for the discrepancies that might be caused by the hourly update schedule.

Audit Events Reports

Audit Events reports list the audit events related to a search you specify, such as user logins for the past 30 days. This feature is useful for troubleshooting purposes.

See "Generate an Audit Event Report," on page 64.

Generate an Audit Event Report

You can generate a report of audit events that you specify.

Audit event reports can be useful as a method of troubleshooting.

Prerequisites

Enable auditing. See "Enabling the Logging of Auditing Events," on page 68.

Procedure

1 Using a browser, log in to the Horizon Workspace Administrator Web interface.

2 Select **Reports > Audit events**

3 Select audit event criteria.

Audit Event Criteria	Description
User	This text box allows you to narrow the search of audit events to those generated by a specific user.
Type	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.
Action	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.
Object	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.
Date range	These text boxes allow you to narrow your search to a date range in the format of "From ___ days ago to ___ days ago." The maximum date range is 30 days. For example, from 100 days ago to 70 days ago.

4 Click **Show**.

An audit event report appears according to the criteria you specified.

5 To see the code for a specific audit event, click **View Details** for that audit event.

Configuring Horizon Workspace Settings for Administrators

12

After you install Horizon Workspace and perform the initial configuration, you can configure several administrative settings.

This chapter includes the following topics:

Accessing the Configurator Web interface

You can use the Administrator Web interface to access the Configurator Web interface to facilitate the configuration of Horizon Workspace.

To use the Administrator Web interface to access the Configurator Web interface, select **Settings > VA Configuration**. The Configurator Web interface allows you to use a Web interface to edit the underlying Configurator virtual appliance. You can perform actions such as the following from the Configurator Web interface:

- View system information.
- Change the database from internal to external.
- Configure an SSL certificate for external access to Horizon Workspace.
- Enable modules: Data, Web Applications, ThinApp Packages, and View.
- Enter a new license key.
- Change the admin user password for the service-va, configurator-va, and connector-va.
- View a list of the log file locations.

Configuring User Password Recovery

You can configure the password recovery method for users.

To use the Administrator Web interface to configure the user password recovery method, select **Settings > VA Configuration**. This feature allows you to configure the behavior of the **Forgot password** link on the user log in page.

Configuring Identity Providers

You can add Connector instances to your Horizon Workspace deployment.

You can 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 > 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 66.

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. The IDP discovery feature allows you to balance the load of Horizon Workspace activity to multiple Connector instances or your to use a different authentication type for different users, according to their IP address.

Creating multiple Connector instances and configuring IdP Discovery enables Horizon Workspace to 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.

The Connector acts as an identity provider and is the only identity provider that Horizon Workspace supports.

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. See Chapter 2, "Introduction to Horizon Workspace for Administrators," on page 7 for information on IdP Discovery.
- Issue the `hznAdminTool addvm` command in the configurator-va virtual machine to create the additional Connector instances necessary for your deployment. See *Installing Horizon Workspace*.

Procedure

1 Using a browser, log in to the Horizon Workspace 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.

Adding an Identity Provider from the Identity Providers Page

Unless VMware technical support instructs you to use the **Add Identity Provider** button to add Connector instances, add Connector instances using the `hznAdminTool addvm` command in the configurator-va virtual machine.

See "Configuring Identity Providers," on page 66 for information about adding Connector Instances to your Horizon Workspace deployment.

Connector Activation Code

The Connector Activation Code page appears when you add Connector instances using the **Add Identity Provider** button. Unless VMware technical support instructs you to use the **Add Identity Provider** button to add Connector instances, add Connector instances using the `hznAdminTool addvm` command in the configurator-va virtual machine.

See "Configuring Identity Providers," on page 66 for information about adding Connector Instances to your Horizon Workspace deployment.

Creating a Client for Remote App Access

You can create a client to enable a single application to register with Horizon Workspace to allow user access to a specific application.

To use the Administrator Web interface to create a client for single application registration, select **Settings > Remote App Access > Clients**.

Creating a Template for Remote App Access

You can create a template to enable a group of clients to register dynamically with Horizon Workspace to allow user access to a specific application.

To use the Administrator Web interface to create a template for multiple-client registration, select **Settings > Remote App Access > Templates**.

Configuring a SAML-Signing Certificate

You can make a SAML-signing certificate available in Horizon Workspace for Web applications that require the use of SAML assertions to authenticate users.

To view or add a SAML-signing certificate in Horizon Workspace, select **Settings > SAML Certificate**. You can paste the certificate in the Signing Certificate text box. 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.

Enabling License Approval

If you use the Horizon Workspace SDK to integrate your license-management system with Horizon Workspace, you can enable and disable the license approval process.

Select **Settings > Approvals** to enable or disable license approval.

Enabling the Logging of Auditing Events

You can enable Horizon Workspace to log auditing events that you can retrieve as reports in the Administrator Web interface.

Select **Settings > Auditing** to enable or disable the collection of information for audit events reports, which is accessible on the **Reports** tab.

Troubleshooting Horizon Workspace for Administrator's 13

You can troubleshoot issues that you experience after you install and configure Horizon Workspace.

Horizon Workspace Fails to Provision a User to the Data Service

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

Problem

One or more users cannot access the Data 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 Data service while not being provisioned to the Data 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 Data service and you later add the user back to Horizon Workspace. See Chapter 6, "Providing Access to the Data Service," on page 29 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 Data service.

   a Use the command tool of the Data 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 Data service.

   Example: `zmprov da joe@domain.com`

Index