This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Contents

1 About the VMware Workspace Portal Administrator's Guide 7

2 Introduction to Workspace for Administrators 9

3 Monitor Workspace System and Module Information 13

4 Integrating Workspace with Active Directory 15
   Single Active Directory Domain Environment 15
   Multi-Domain, Single Forest Active Directory Environment 16
   Multi-Forest Active Directory Environment 16
   Add a User Store for a Multi-Forest Active Directory Environment 16
   Edit a User Store for a Multi-Forest Active Directory Environment 17

5 Configuring Workspace User Authentication 19
   Overview of Workspace User Authentication 19
   Add or Edit a Network Range 21
   Add or Edit a User Authentication Method 22
   Add and Configure an Identity Provider Instance 23
   Overview of Configuring Workspace to Use a Third-Party Identity Provider Instance 26
      Obtain the Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance 27
   Editing the Default Access Policy Set 27

6 Managing Access Policy Sets 29
   Overview of Access Policy Settings 29
   Managing Web-Application-Specific Access Policy Sets 30
   Edit an Access Policy Set 32
   Add a Web-Application-Specific Access Policy Set 33
   Apply a Web-Application-Specific Access Policy Set 34

7 Managing Users and Groups 35
   Workspace User and Group Types 35
   Manage Workspace Groups 36
      Modify Workspace Group Membership 36
      Workspace Group Information 39
   Manage Workspace Users 41
      Workspace User Information 41
      Prevent Users from Accessing Workspace 43
   Update the Settings That Select Workspace Users from Active Directory 43
8 Managing the Workspace Catalog
   Overview of Workspace Resource Types
   Overview of Using Resource Categories
   Create a Resource Category
   Apply a Category to Resources
   Remove or Delete a Category
   View Workspace Resources
   Add Resources to Your Catalog

9 Search for Users, Groups, or Catalog Resources

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

11 Providing Access to Web Applications
   Enable the Web Applications Module to Provide Web Application Access
   Establish Secure Single Sign-On to Your Web Applications Through Workspace
   Mapping Attributes in the Workspace Connector
   Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Workspace
   Adding Web Applications to Your Organization's Catalog
   Add a Web Application to Your Catalog from the Cloud Application Catalog
   Add a Web Application to Your Catalog by Creating a New Application Record
   Add a Web Application to Your Catalog by Importing a ZIP or JAR File
   Entitle Users and Groups to Web Applications

12 Providing Access to Citrix-Based Applications
   Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment
   View User and Group Entitlements to Citrix-Based Applications
   Editing Workspace Application Delivery Settings for Citrix-Based Applications
   Edit the Workspace Application Delivery Settings Globally for All Citrix-Based Applications
   Edit the Workspace Application Delivery Settings for a Single Citrix-Based Application
   Managing Categories for Citrix-Based Applications

13 Providing Access to VMware ThinApp Packages
   Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Workspace System
   Distributing and Managing ThinApp Packages with Workspace
   Offline Grace Period and ThinApp Packages
   Using the Command-Line HorizonThinAppCtrl.exe Application
   Entitle Users and Groups to ThinApp Packages
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>83</td>
<td>Updating Managed ThinApp Packages After Deployment in Workspace</td>
</tr>
<tr>
<td>84</td>
<td>Update a Managed ThinApp Package</td>
</tr>
<tr>
<td>88</td>
<td>Delete ThinApp Packages from Workspace</td>
</tr>
<tr>
<td>89</td>
<td>Make Existing ThinApp Packages Compatible with Workspace</td>
</tr>
<tr>
<td>91</td>
<td>Add ThinApp Packages to the Network Share</td>
</tr>
<tr>
<td>93</td>
<td>Configuring Workspace for Windows</td>
</tr>
<tr>
<td>99</td>
<td>Install the Workspace for Windows Application with Identical Settings to Multiple Windows Systems</td>
</tr>
<tr>
<td>101</td>
<td>Viewing Workspace Reports</td>
</tr>
<tr>
<td>101</td>
<td>Generate an Audit Event Report</td>
</tr>
<tr>
<td>103</td>
<td>Configuring Workspace Settings for Administrators</td>
</tr>
<tr>
<td>104</td>
<td>Customize Workspace Branding</td>
</tr>
<tr>
<td>107</td>
<td>Use hznAdminTool Commands to Make Changes to Your Workspace System</td>
</tr>
<tr>
<td>109</td>
<td>Troubleshooting Workspace for Administrators</td>
</tr>
<tr>
<td>110</td>
<td>ThinApp Packages Fail to Launch from the User Portal</td>
</tr>
<tr>
<td>113</td>
<td>A User Login Attempt Results in a Timeout Error</td>
</tr>
<tr>
<td>113</td>
<td>Users Accessing Citrix-based Applications Receive an Encryption Error</td>
</tr>
<tr>
<td>115</td>
<td>Index</td>
</tr>
</tbody>
</table>
About the VMware Workspace Portal Administrator's Guide

The VMware Workspace Portal Administrator's Guide provides information and instructions about using and maintaining VMware® Workspace™ Portal. With Workspace you can customize a catalog of resources for your organization's applications and provide secure, multi-device, managed-user access to those resources. Such resources include Web applications, mobile applications, Windows applications captured as ThinApp packages, Citrix-based applications, and View™ desktop and application pools. Workspace provides users with a unified experience and offers your IT department unified security and management for all services and applications across multiple devices.

Intended Audience

The VMware Workspace Portal 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®, View™, Citrix application virtualization, RSA SecurID, and Android app distribution is helpful if you plan to implement those features.

Workspace Administrator's Guide Overview


To administer Workspace, you predominantly use the Workspace Admin Console, logged in as an administrator. You occasionally need to access the Configurator Web interface, the Connector Web interface, and the virtual appliance interfaces. See “Workspace Web Interface URLs,” on page 10.

The key task you perform as a 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 View desktop and application pools, Windows applications (ThinApp packages), Citrix-based applications, and Web applications. The actual resource types you manage vary according to the needs of your organization. To entitle a resource type, you must first perform the respective preconfiguration tasks as described in the Installing and Configuring VMware Workspace Portal.
Introduction to Workspace for Administrators

Workspace provides you with a centralized Web management console with which you can customize your organization’s catalog, and manage entitlements to resources in that catalog. Your catalog contains your organization’s applications and View desktops as resources.

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

Workspace Server Components

Workspace server consists of the following virtual appliances.

Table 2-1. Workspace Server Components

<table>
<thead>
<tr>
<th>Workspace Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace Portal Configurator configurator-va</td>
<td>You start configuring Workspace with this virtual appliance, using both its console and the Configurator Web interface. The configurations you make with the configurator-va are distributed to the other virtual appliances in the vApp.</td>
</tr>
<tr>
<td>VMware Workspace Portal Manager service-va</td>
<td>This virtual appliance gives you access to the MyApps and the Workspace Admin Console, from which you can manage users, groups, and resources.</td>
</tr>
<tr>
<td>VMware Workspace Portal Connector connector-va</td>
<td>The connector-va provides the following services: user authentication (identity provider), directory synchronization, and View pool synchronization.</td>
</tr>
<tr>
<td>VMware Workspace Portal Gateway gateway-va</td>
<td>The Workspace Gateway is the single endpoint for all end user communication. User requests come to the gateway-va virtual machine, which then routes the request to the appropriate virtual appliance.</td>
</tr>
</tbody>
</table>

Workspace User Components

Users can access entitled resources using the Workspace App Portal (an agentless client) and they can access virtualized Windows applications captured as ThinApp packages from Workspace for Windows.
Table 2.2. Workspace User Client Components

<table>
<thead>
<tr>
<th>Workspace User Component</th>
<th>Description</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace App Portal</td>
<td>The Workspace app portal is an agentless web-based application. It is the default interface used when users access and use their entitled workspace assets with a browser. Using this portal, users can access their View desktops and Workspace Web applications. If an end user has entitled ThinApp applications and is on a Windows system where the Workspace for Windows program is installed and active, they can view and launch their entitled ThinApp packages from this app portal. On iOS devices, users can open this portal in a browser app like Safari and access and use their View desktops, Workspace Web applications and Citrix-based applications.</td>
<td>Web-based apps portal is available on all supported system endpoints, such as Windows systems, Mac systems, iOS devices, Android devices.</td>
</tr>
<tr>
<td>Workspace for Windows</td>
<td>When this program is installed on users' Windows systems, they can work with their virtualized Windows applications captured as ThinApp packages.</td>
<td>Windows systems</td>
</tr>
</tbody>
</table>
Table 2-3. Workspace URLs (Continued)

<table>
<thead>
<tr>
<th>URL</th>
<th>User Interface</th>
<th>What you can do here</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https://ConnectorHostname/hc/admin/</code></td>
<td>Connector Web</td>
<td>Configure additional ThinApp settings, View pool settings, Citrix published</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td>application settings, check directory sync status, or alerts. (Log in as an</td>
</tr>
<tr>
<td></td>
<td></td>
<td>administrator using the password you set during configuration.)</td>
</tr>
<tr>
<td><code>https://ConfiguratorHostname/cfg</code></td>
<td>Configurator Web</td>
<td>See system information, check modules, set license key, or set admin password. (Log</td>
</tr>
<tr>
<td></td>
<td>interface</td>
<td>in as an administrator using the password you set during configuration.)</td>
</tr>
</tbody>
</table>

Supported Web Browsers for Workspace

The Workspace administrator console is a Web-based application that is installed when you install Workspace. You can access and use the Workspace Admin Console from the following browsers.

- Internet Explorer 10 and 11 for Windows systems
- Google Chrome 34.0 or later for Windows and Mac systems
- Mozilla Firefox 28 or later for Windows and Mac systems
- Safari 6.1.3 and later for Mac systems

End users can access their Workspace App Portal from the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Safari (latest)
- Internet Explorer 8 or later
- Native browser and Google Chrome on Android devices
- Safari on iOS devices

Viewing Workspace pages with Internet Explorer 8 might not display all elements on the page correctly. For best viewing users should upgrade to a newer version.
You can monitor Workspace system information and information about the Workspace modules: the Web Applications module, the View module, the ThinApp Packages module, and the Citrix Published Applications module.

Workspace system information and information about the xxx modules is available on the Dashboard page in the Workspace Admin Console.

Prerequisites

Install and configure Workspace. During the configuration process, enable those modules for the resource types that you want to make available in your users’ workspaces. If you do not enable a module during installation, you can configure it later using the Workspace Admin Console (admin console).

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 InfoWorkspace to view system information.

What to do next

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

- “Enable the Web Applications Module to Provide Web Application Access,” on page 59
- “Enable the View Module to Integrate View with Workspace,” on page 54
- “Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Workspace System,” on page 76
- “Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment,” on page 69
Integrating Workspace with Active Directory

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

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

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

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

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

This chapter includes the following topics:

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

**Single Active Directory Domain Environment**

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

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

**Multi-Domain, Single Forest Active Directory Environment**

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

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

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

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

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

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

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

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

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

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

**Prerequisites**

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

**Procedure**

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

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

5 Click **Save**.

**What to do next**

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

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

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

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

**Prerequisites**

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

**Procedure**

1 Log in to the admin console.
2 Select **Settings > User Stores**.
3 Click **Edit** for the user store you want to configure.
4 Edit the user store settings.

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

5 Click Save.

**What to do next**

- If you changed the sync client, initiate the user and group sync process of the newly configured sync client (a Connector or a third-party identity provider service client).
- If you have not already done so, associate the user store with an identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.
Configuring Workspace User Authentication

Workspace user authentication requires the use of one or more identity provider instances, which can be Connector instances, third-party identity provider instances, or a combination of both. The identity provider instances authenticate users with Active Directory within the enterprise network.

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

This chapter includes the following topics:

- “Overview of Workspace User Authentication,” on page 19
- “Add or Edit a Network Range,” on page 21
- “Add or Edit a User Authentication Method,” on page 22
- “Add and Configure an Identity Provider Instance,” on page 23
- “Overview of Configuring Workspace to Use a Third-Party Identity Provider Instance,” on page 26
- “Editing the Default Access Policy Set,” on page 27

Overview of Workspace User Authentication

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

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

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

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

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

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

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

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

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

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

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

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

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

**Add or Edit a Network Range**

You can add a network range of IP addresses that you want to direct to a specific identity provider instance.

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

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

**Prerequisites**

Perform the necessary network range planning.

- Determine the best way to integrate Workspace with Active Directory to meet the needs of your organization. Such planning affects the number of identity provider instances in your deployment, which affects the number of network ranges needed. See Chapter 4, “Integrating Workspace with Active Directory,” on page 15.
- Based on your network topology, define network ranges for your Workspace deployment.
- To add a network range when the View module is enabled, take note of the Horizon Client access URL and port number for the network range. See View documentation for more information.

**Procedure**

1. Log in to the Workspace Admin Console.
2. Select **Settings > Network Ranges**.
3. Edit an existing network range or add a new network range.

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

4. Complete the form.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network range.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the Network Range.</td>
</tr>
<tr>
<td>View Pods</td>
<td>The View Pods option only appears when the View module is enabled.</td>
</tr>
<tr>
<td>Client Access URL Host</td>
<td>Enter the correct Horizon Client access URL for the network range.</td>
</tr>
<tr>
<td>Client Access Port</td>
<td>Enter the correct Horizon Client access port number for the network range.</td>
</tr>
<tr>
<td>IP Ranges</td>
<td>Edit or add IP ranges until all desired and no undesired IP addresses are included.</td>
</tr>
</tbody>
</table>

See “Add View Pods to Workspace,” on page 55.
What to do next

- Associate each network range with an identity provider instance. See “Add and Configure an Identity Provider Instance,” on page 23.
- Associate network ranges with access policy sets as appropriate. See Chapter 6, “Managing Access Policy Sets,” on page 29.

Add or Edit a User Authentication Method

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


The minimum authentication score of a method and the order of the method on the Authentication Methods page are significant in the process Workspace follows to select an identity provider instance for user authentication. To require users to use an authentication method of a specified minimum authentication score to access a Web application, see “Managing Web-Application-Specific Access Policy Sets,” on page 30.

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

Prerequisites

- Deploy the authentication systems that you plan to integrate with Workspace. For example, if you plan to integrate RSA SecurID into your Workspace deployment, verify that RSA SecurID is installed and configured on your network.
- Use your own criteria to determine the security levels, on a scale from 1, the lowest security, to 5, the highest security, of the authentication methods you plan to use in your Workspace deployment.

Procedure

1. Log in to the Workspace Admin Console.
2. Select Settings > Authentication Methods.
3. Edit an existing authentication method or add a new authentication method.

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

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

Click Save.

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

Add and Configure an Identity Provider Instance

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

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

Prerequisites
- Perform the necessary planning.
- Determine the best way to integrate Workspace with Active Directory to meet the needs of your organization. You can configure a single domain, a multi-domain forest, or a multi-forest Active Directory deployment. See Chapter 4, “Integrating Workspace with Active Directory,” on page 15.
- Determine the authentication types required to meet the needs of your organization. For example, you can configure Kerberos authentication for users internal to your organization and RSA SecurID authentication for users external to your organization. You can set up this type of configuration by using a single identity provider instance for both authentication methods or by using a separate identity provider instance for each authentication method.
- Deploy Workspace with a single Active Directory domain during the proof-of-concept phase of your deployment.
Prepare additional identity provider instances for your Workspace deployment.

To add additional Connector instances, use the hznAdminTool addvm command in the configurator-va virtual machine to manually add instances. That command registers the Connector instance and adds its name to the Identity Providers page. See Installing and Configuring Workspace.

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

To add a third-party identity provider instance, perform the following tasks. See “Overview of Configuring Workspace to Use a Third-Party Identity Provider Instance,” on page 26 for a complete list of tasks related to configuring Workspace to use a third-party identity provider instance.

- Verify that the third-party instances are SAML 2.0 compliant and that Workspace can reach them.
- Determine how Workspace obtains the metadata from the third-party instance and copy and save the appropriate metadata information from the third-party instance that you can paste into the Workspace Admin Console during configuration. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.
- To enable Workspace to use additional authentication methods, use the admin console to configure the additional authentication methods. See “Add or Edit a User Authentication Method,” on page 22.

Use the admin console to configure network ranges. See “Add or Edit a Network Range,” on page 21

To integrate Workspace into a multi-forest Active Directory deployment, use the admin console to add the necessary number of user stores. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16.

**Procedure**

1. Log in to the Workspace Admin Console.
2. Select Settings > Identity Providers.
3. Edit an existing Connector instance or add a third-party identity provider instance.

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

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

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

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

Pre-Configuration

Complete the following tasks prior to using the Workspace admin console to add the third-party identity provider instance.

1. Verify that the third-party instances are SAML 2.0 compliant and that Workspace can reach them.
2. Determine how Workspace obtains the metadata from the third-party instance and copy and save the appropriate metadata information from the third-party instance that you can paste into the Workspace admin console during configuration. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.
3. To enable Workspace to use authentication methods supported by the third-party identity provider, use the admin console to configure the additional authentication methods. See “Add or Edit a User Authentication Method,” on page 22.
4. Edit an authentication methods by selecting the Default Method checkbox. This action allows Workspace to use that authentication method in case of an issue with the third-party authentication method. See “Add or Edit a User Authentication Method,” on page 22.

Configuration

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

1. Click the + Add Identity Provider button and select Manual from the Type drop-down menu.
2. Select the authentication methods supported by the third-party-identity provider instance that you plan to use with Workspace.
3. Use the Configure Via option to select how to transfer the metadata of the third-party identity provider instance to Workspace, either by using a URL to the metadata or by copying and pasting the metadata.

Post Configuration

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

1. Use the Workspace admin console to gather the SAML information necessary to configure the third-party identity provider instance.
2. Configure the third-party identity provider instance by applying the SAML information you gathered from Workspace.
Obtain the Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance

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

Prerequisites

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

Procedure

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

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

      | Method                  | Description                                                      |
      |-------------------------|------------------------------------------------------------------|
      | Copy the URL of the Page| Copy and save the URL of the Service Provider (SP) metadata page.|
      | Copy the XML on the Page| Copy and save the content of the page to a text file.            |

3. Determine the user mapping from the third-party identity provider instance to Workspace.

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

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

What to do next

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

Editing the Default Access Policy Set

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

Each policy in the default access policy set requires that a set of criteria be met in order for Workspace to allow access to the apps portal. See Chapter 6, “Managing Access Policy Sets,” on page 29.
The following access policy set serves as an example of how you can configure the default access policy set to control access to the Workspace apps portal. See “Edit an Access Policy Set,” on page 32 for instructions.

**Example Default Access Policy Set**

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

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

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

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

**Default Access Policy, Browser Use Case**

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

2. **External.** To access Workspace from an external (All Ranges) network, the user is required to login with SecurID, which for this example has an authentication score of 3. The user logs in using a browser and now has access to the apps portal for a four-hour session.

2. When a user attempts to access a resource, except for a Web application covered by a Web-application-specific policy set, the default portal access policy set applies.

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

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

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

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

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

Workspace has a default access policy set that you can edit. This access policy set controls access to Workspace as a whole. See “Editing the Default Access Policy Set,” on page 27. To control access to specific Web applications, you can create additional access policy sets. If you do not apply an access policy set to a Web application, the default access policy set applies.

This chapter includes the following topics:

- “Overview of Access Policy Settings,” on page 29
- “Managing Web-Application-Specific Access Policy Sets,” on page 30
- “Edit an Access Policy Set,” on page 32
- “Add a Web-Application-Specific Access Policy Set,” on page 33
- “Apply a Web-Application-Specific Access Policy Set,” on page 34

**Overview of Access Policy Settings**

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

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

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

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

Minimum Authentication Score

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

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

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

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

Workspace denies the request to access the app portal or to launch a Web application under the following conditions.

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

Time-To-Live

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

Managing Web-Application-Specific Access Policy Sets

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

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

The following Web-application-specific access policy set provides an example of a policy set you can create to control access to specified Web applications. See Chapter 6, “Managing Access Policy Sets,” on page 29.

Example 1 Web-Application-Specific Policy Set

This example illustrates a policy set you might create and apply to a sensitive application.
Policy Name | Network | Minimum Authentication Score | TTL (hours)  
---|---|---|---
Internal | Internal Range | 1 | 8  
External | All Ranges | 3 | 4  

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

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

**Strict Web-Application-Specific Access Policy Set, Browser Use Case**

1. To access Workspace from outside the enterprise network, the user is required to login with RSA SecurID, which has a minimum authentication score of 3 according to the example. See the External policy example in “Editing the Default Access Policy Set,” on page 27. The user logs in using a browser and now has access to the app portal for a four hour session as provided by the default access policy set.

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

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

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

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

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

Policy Name | Network | Minimum Authentication Score | TTL (hours)  
---|---|---|---
ExtraSensitive | All Ranges | Level 3 | 1  

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

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

1. User logs in from an inside the enterprise network using the Password authentication method, which is level 1 according to the example. See the Internal policy example in “Editing the Default Access Policy Set,” on page 27.

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

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

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

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

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

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

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

You can edit an existing policy set, either the default access policy set or a Web-application-specific access policy set, by removing existing policies from the set, editing existing policies in the set, or adding new policies to the set. For an overview of access policy sets, see Chapter 6, “Managing Access Policy Sets,” on page 29.

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


Prerequisites

- Configure the appropriate identity providers for your deployment. See “Add and Configure an Identity Provider Instance,” on page 23.

- Configure the appropriate network ranges for your Workspace deployment. See “Add or Edit a Network Range,” on page 21.

- Configure the appropriate authentication methods for your deployment. See “Add or Edit a User Authentication Method,” on page 22.

Procedure

1. Log in to the Workspace Admin Console.
3. (Optional) To permanently delete a Web-application-specific access policy set, click Remove for the policy set.

   The Remove option is not available for the default access policy set. The default access policy set cannot be deleted.

4. Click Edit for the existing policy set to configure.
5. (Optional) If appropriate, change the policy set name and description in the respective text boxes.

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

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

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

7 Click Save.

The edited access policy set takes effect immediately.

**What to do next**

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

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

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

For an overview of access policy sets, see Chapter 6, “Managing Access Policy Sets,” on page 29. For information and examples of Web-application-specific access policy sets, see “Managing Web-Application-Specific Access Policy Sets,” on page 30.

**Prerequisites**

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

**Procedure**

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

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

Click **Add**.

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

Click **Save** to save the policy set.

**What to do next**

Apply the policy set to one or more Web applications.

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

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

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

**Prerequisites**

If not already created, create a Web-application-specific access policy set to control user access to a specific Web application. See “Add a Web-Application-Specific Access Policy Set,” on page 33

**Procedure**

1. Click the Catalog tab.
2. Click **Any Application Type > Web Applications**.
3. Click the Web application to which to apply a Web-application-specific access policy set.
   - The information page for the Web application appears with the Entitlements tab selected by default.
4. Click **Access Policies**.
5. From the Access Policy Set drop-down menu, select the Web-application-specific access policy set to apply to the application.
6. Click **Save**.

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

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

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

This chapter includes the following topics:

- “Workspace User and Group Types,” on page 35
- “Manage Workspace Groups,” on page 36
- “Manage Workspace Users,” on page 41
- “Update the Settings That Select Workspace Users from Active Directory,” on page 43

Workspace User and Group Types

With the Workspace admin console, you can manage users, guest users, and groups.

Users

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

Groups

The types of groups that can appear in the Workspace Admin Console are groups imported from your directory server and Workspace groups, which are groups you create yourself using Workspace.
### Manage Workspace Groups

Creating groups, modifying the membership of groups, and deleting groups are tasks you can perform in Workspace that only apply to Workspace groups. Entitling groups to resources is a task you can perform for both Workspace groups and Active Directory groups.

**Procedure**

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

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

**What to do next**

After you create a Workspace group, you can modify the membership of the group. See “Modify Workspace Group Membership,” on page 36.

### Modify Workspace Group Membership

You can modify Workspace group membership.

Use groups to entitle more than one user to the same resources at the same time, instead of entitling each user individually.

You use group rules to define which users are members of a particular Workspace group. A user can belong to multiple groups. For example, if you create a Sales group and a Management group, a sales manager can belong to both groups. You can specify which mobile policy settings apply to the group’s members.

**Procedure**

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

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

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

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

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

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

You can nest rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select <strong>Is</strong> to choose a group to associate with this Workspace group. Type a group name in the text box. As you type, a list of group names appears. Select <strong>Is Not</strong> to choose a group to exclude from this Workspace group. Type a group name in the text box. As you type, a list of group names appears.</td>
</tr>
</tbody>
</table>

Attribute Rules

The following rules are available for all attributes, including default attributes and any additional custom attributes that your enterprise configured. Examples of attributes are email and phone.

**Note**: Rules are not case-sensitive.

- Select **Matches** to grant group membership for directory server entries that exactly match the criteria you enter. For example, your organization might have a business travel department that shares the same central phone number. If you want to grant access to a travel booking application for all employees who share that phone number, you can create a rule such as **Phone Matches (555) 555-1000**.

- Select **Does Not Match** to grant group membership to all directory server entries except those that match the criteria you enter. For example, if one of your departments shares a central phone number, you can exclude that department from access to a social networking application by creating a rule such as **Phone Does Not Match (555) 555-2000**. Directory server entries with other phone numbers have access to the application.

- Select **Starts With** to grant group membership for directory server entries that start with the criteria you enter. For example, your organization's email addresses might begin with the departmental name, such as **sales_username@example.com**. If you want to grant access to an application to everyone on your sales staff, you can create a rule, such as **Email Starts With sales_**.

- Select **Does Not Start With** to grant group membership to all directory server entries except those that start with the criteria you enter. For example, if the email addresses of your human resources department are in the format **hr_username@example.com**, you can deny access to an application by setting up a rule, such as **Email Does Not Start With hr_**. Directory server entries with other email addresses have access to the application.

Any of the following

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

All of the following

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

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

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

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

Procedure

1. Log in to the Workspace Admin Console.

2. Select Users & Groups > Groups.

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

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

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

3. Click a group’s name.

   The group’s details page is displayed with the group’s name listed at the top of the page.
Click the tab that corresponds to the information you want to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Entitlements      | The group’s Entitlements page is displayed. In this page, you can:  
  - View the list of resources entitled to the users of the group.  
  - Click **Add entitlement** to entitle the group’s users to the individual resources that are available in your catEntitlementsalog.  
  - Click the name of a listed entitled resource to display that resource’s Edit page.  
  - For resource types that have an **Edit** button, you can click the button to entitle or unentitle the group’s users to resources of that type, or to customize the options for each entitled resource. From the Entitlements page, you can make the following changes:  
    - For web applications, click **Edit** to change the group’s entitlements to the web applications or the type of deployment for the group’s entitled web applications. Select **Automatic** to have the Web application displayed by default in the user portal. Select **User-Activated** to allow the users to add the web application to the user’s My Apps area from the App Center collection of applications available to that user.  
    - For View desktop and application pools, you can view the group’s existing entitlements to the View pools that are integrated with your Workspace system. Entitlements to View desktop and application pools are configured in the View Connection Server instances that are integrated with your Workspace system. You cannot change entitlements to View pools using the group’s Entitlements page.  
    - For ThinApp packages, click **Edit** to change the group’s entitlements to the ThinApp packages or the type of deployment for the group’s entitled ThinApp packages. Select **Automatic** to have the ThinApp package displayed by default in the My Apps area of the user portal. Select **User-Activated** to allow the users to manually add the ThinApp package from the App Catalog to their My Apps area.  
    - For Citrix Published Applications, you can view the group’s existing entitlements to the Citrix-based applications that are integrated with your Workspace system. Entitlements to Citrix-based applications are configured in the Citrix deployments that are integrated with your Workspace system. You cannot change entitlements to Citrix-based applications using the group’s Entitlements page.  
    - For resources types that have an **Unentitle** button, you can click the button to remove the group’s access to use that specific resource.  
  **Note:** The Provisioning Status column is not used. By default, for the table rows that have filled-in entries on this page, the Provisioning Status columns display Not Enabled, and you cannot change this value. |
| Users in this Group | The group’s membership page is displayed. In this page, you can:  
  - View the list of users that belong to the group.  
  - Click a user’s name to display the details page for that user.  
  - Click **Modify Users in This Group** to view and configure the rules that define membership to the Workspace group. The **Modify Users in This Group** option is available for Workspace groups, but not for directory server groups. |
Manage Workspace Users

You can manage Workspace users, the users imported from Active Directory, using the Workspace Admin Console.

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

Workspace User Information

You can view detailed information about a user such as the user’s entitled resources, group affiliations, and provisioned desktop systems and mobile devices using the Workspace Admin Console.

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

- To modify membership of a Workspace group. For example, if you use the manager attribute in Active Directory, you can map the manager attribute to Workspace. You can create a group where the group rules restrict membership to users with the manager attribute in their 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 Workspace user record.

Procedure

1. Log in to the Workspace Admin Console.
2. Select **Users & Groups > Users**.
   The page displays a list of all your Workspace users.
3. Click a user’s name.
   The user’s details page is displayed. The user’s name, email address, and role are listed at the top of the page.
4. (Optional) Click the name of the displayed role, **User** or **Administrator**, to change the user’s role.

You can promote users to the administrator role, allowing them access to configure the Workspace admin console. Individuals assigned the administrator role can still access the their app portal from the Web as a user. The URL to access the admin console is different than the URL to access the app portal.

For the following URLs, replace the **WorkspaceFQDN** placeholder with the actual value.

<table>
<thead>
<tr>
<th>Web Interface</th>
<th>Required Role</th>
<th>URL Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Admin Console</td>
<td>Administrator</td>
<td><a href="https://WorkspaceFQDN/admin">https://WorkspaceFQDN/admin</a></td>
</tr>
<tr>
<td>Workspace App Portal</td>
<td>User</td>
<td><a href="https://WorkspaceFQDN/web">https://WorkspaceFQDN/web</a></td>
</tr>
</tbody>
</table>

5. (Optional) Click **Show additional attributes** to see additional attributes assigned to the user, such as directory server attributes.
6 Click the tab that corresponds to the information you want to view.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Entitlements | The user's Entitlements page is displayed. In this page, you can:  
- View the list of resources entitled to the user.  
- Click **Add entitlement** to entitle the user to resources that are available in your catalog.  
- Click the name of a listed entitled resource to display that resource's Edit page.  
- For resource types that have an **Edit** button, you can click the button to entitle or unentitle the group's users to resources of that type, or to customize the options for each entitled resource. From the Entitlements page, you can make the following changes:  
  - For web applications, click **Edit** to change the user's entitlements to the web applications or the type of deployment for each of the user's entitled web applications. Select **Automatic** to have the web application displayed by default in the user portal. Select **User-Activated** to allow the user to add the web application to the user's My Apps area from the App Center collection of applications available to that user.  
  - For View desktop and application pools, you can view the user's existing entitlements to the View pools that are integrated with your Workspace system. Entitlements to View desktop and application pools are configured in the View Connection Server instances that are integrated with your Workspace system. You cannot change entitlements to View pools using the user's Entitlements page.  
  - For ThinApp packages, click **Edit** to change the user's entitlements to the ThinApp packages or the type of deployment for the user's entitled ThinApp packages. Select **Automatic** to have the ThinApp package displayed by default in the My Apps area of the user portal. Select **User-Activated** to allow the user to manually add the ThinApp package from the App Catalog to the My Apps area.  
  - For Citrix Published Applications, you can view the user's existing entitlements to the Citrix-based applications that are integrated with your Workspace system. Entitlements to Citrix-based applications are configured in the Citrix deployments that are integrated with your Workspace system. You cannot change entitlements to Citrix-based applications using the user's Entitlements page.  
  - For resources types that have an **Unentitle** button, you can click the button to remove the user's access to use that resource.  
  
**Note:** The Provisioning Status column is not used. By default, for the table rows that have filled-in entries on this page, the Provisioning Status columns display Not Enabled, and you cannot change this value. |
| Group Affiliations | A list of the groups to which the user belongs is displayed. Each group name represents a group to which the user is a member. You can click a group's name to display the details page for that group.                                                                                           |
| Workspaces   | The user's Workspaces page is displayed. In this page, you can view the desktop workspace that have been provisioned to the user's desktop systems, including the current status of the workspace.  
- For a desktop system, you can click **Delete** to remove the corresponding system from Workspace. You might want to remove a system from Workspace because the system is lost, stolen, or no longer in use. |
Prevent Users from Accessing Workspace

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

Procedure

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete or Disable Directory Server User Accounts</td>
<td>In your directory server, delete or disable user accounts according to the needs of your enterprise.</td>
</tr>
<tr>
<td>Create Filters in Workspace for Active User Accounts in Your Directory Server</td>
<td>Using the Connector Web interface of Workspace, create filters to exclude user accounts from being transferred from the directory server to Workspace during synchronizations.</td>
</tr>
</tbody>
</table>

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

Update the Settings That Select Workspace Users from Active Directory

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

Prerequisites

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

Procedure

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

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

2. Perform the appropriate action.

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

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

Display your catalog by clicking the Catalog tab in the Workspace admin console. On the Catalog page, you can perform the following tasks:

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

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>How to See the Resource in Your Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web application</td>
<td>Enable the Web Applications module. Using the admin console, select the <strong>Web Applications</strong> application type on the Catalog page.</td>
</tr>
<tr>
<td>Virtualized Windows application captured as a ThinApp package</td>
<td>Enable the ThinApp Packages module. Using the Connector Web interface, sync ThinApp packages to your catalog. Using the admin console, select the <strong>ThinApp Packages</strong> application type on the Catalog page.</td>
</tr>
<tr>
<td>View Desktop Pool</td>
<td>Enable the View module. Using the Connector Web interface, synch View Pools to your catalog. Using the admin console, select the <strong>View Desktop Pools</strong> application type on the Catalog page.</td>
</tr>
<tr>
<td>View Hosted Applications</td>
<td>Enable the View module. Using the Connector Web interface, synch View Pools to your catalog. Using the admin console, select the <strong>View Hosted Applications</strong> as the application type on the Catalog page.</td>
</tr>
<tr>
<td>Citrix-based application</td>
<td>Enable the Citrix Published Applications module. Using the Connector Web interface, sync Citrix-based applications to your catalog. Using the admin console, select the <strong>Citrix Published Applications</strong> application type on the Catalog page.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Overview of Workspace Resource Types,” on page 46
- “Overview of Using Resource Categories,” on page 47
- “View Workspace Resources,” on page 49
- “Add Resources to Your Catalog,” on page 50
Overview of Workspace Resource Types

The types of resources that you can define in your catalog for entitlement and distribution to users are Web applications, Windows applications captured as VMware ThinApp packages, Citrix-based applications, VMware View desktop pools and View Hosted Applications.

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

Web Applications

You populate your catalog with Web applications directly on the Catalog page of the Workspace admin console. When you click a Web application displayed on the Catalog page, information about that application is displayed. From the displayed page, you can configure the Web application, such as by providing the appropriate SAML attributes to configure single sign-on between Workspace and the target Web application. When the Web application is configured, you can then entitle users and groups to that Web application. See “Add Resources to Your Catalog,” on page 50.

ThinApp Packages

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

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

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

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

4. If not already enabled, enable the ThinApp Package module on the Dashboard page of the admin console.

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

To launch and run the ThinApp packages that are distributed and managed by Workspace, users must have the Workspace for Windows installed on their Windows systems. See “Distributing and Managing ThinApp Packages with Workspace,” on page 76.

Citrix Published Applications

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

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

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

3. If not already enabled, enable the Citrix Published Applications module on the Dashboard page of the admin console. See “Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment,” on page 69.

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

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

1. If not already deployed, deploy View desktop pools in VMware View, which includes entitled users to desktops. See the VMware View documentation.
2. Integrate your Workspace deployment with VMware View. See Installing and Configuring Workspace.
3. If not already enabled, enable the View module on the Dashboard page of the admin console. See “Enable the View Module to Integrate View with Workspace,” on page 54.

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

View Hosted Applications

You populate your catalog with View application pools by performing the following tasks.

1. Make sure that application pools are deployed in View as a remote desktop service. See the View documentation.
2. Integrate your Workspace deployment with View. See Installing and Configuring Workspace.
3. If not already enabled, enable the View module on the Dashboard page of the admin console. See “Enable the View Module to Integrate View with Workspace,” on page 54.

After you perform these tasks, the hosted application pools that you entitled to users with View are now available as resources in your catalog.

Overview of Using Resource Categories

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

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

Create a Resource Category

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

Procedure

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

Workspace creates the new category, but does not apply it.

7 (Optional) To apply the category to the selected resources, click the checkbox for the new category name.

Workspace applies the category to the selected resources.

**What to do next**

If appropriate, apply the category to resources. See “Apply a Category to Resources,” on page 48.

### Apply a Category to Resources

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

**Prerequisites**

Create a resource category.

**Procedure**

1. Log in to the Workspace Admin Console.
2. Click the **Catalog** tab.
3. Click the checkboxes of all the resources to which to apply the category.
4. Click **Apply Categories** and select the name of the category to apply.

   The category is applied to the selected resources.

### Remove or Delete a Category

You can disassociate a category from a resource and you can permanently remove a category from the catalog.

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

**Procedure**

1. Log in to the Workspace Admin Console.
2. Click the **Catalog** tab.
3. Click the checkbox of one or more resources.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Category from Resources</td>
<td>The checkbox of the label is selected. Click that box to remove the category label from the selected resource.</td>
</tr>
<tr>
<td>Delete Category Permanently</td>
<td>Hover over the category. An x appears. Click the x to permanently remove the category from the catalog.</td>
</tr>
</tbody>
</table>
View Workspace Resources

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

Prerequisites

- Enable the resource modules that correspond to the resource types to which you want to entitle users. The Web Applications module, Mobile Management module, View module, ThinApp Packages module, and Citrix Published Applications module are available.
- Add resources to the catalog to meet the needs of your enterprise. See Chapter 8, "Managing the Workspace Catalog," on page 45.
- To view resources by category, create and apply categories. See “Overview of Using Resource Categories,” on page 47.

Procedure

1. Log in to the Workspace Admin Console.
2. Click the Catalog tab.
   Workspace lists all the resources in the catalog.
3. (Optional) To change the sort method click Application or Application type.
4. (Optional) To view resources by a specific type, select a resource type from the Any Application Type drop-down menu.
   Application types that you have not added to Workspace do not appear in the drop-down menu.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Application Type</td>
<td>Lists all of the resources in your catalog.</td>
</tr>
<tr>
<td>Web Applications</td>
<td>Lists only Web applications in your catalog. Web applications include SaaS applications and Web applications managed internally by your enterprise.</td>
</tr>
<tr>
<td>ThinApp Packages</td>
<td>Lists only Windows applications captured as ThinApp packages. ThinApp packages appear in your catalog if you add ThinApp packages to your deployment while configuring Workspace prior to accessing the admin console.</td>
</tr>
<tr>
<td>View Desktop Pools</td>
<td>Lists only the View desktop pools. View desktop pools appear in your catalog if you integrate Workspace with VMware View prior to accessing the Workspace Admin Console.</td>
</tr>
<tr>
<td>View Hosted Applications</td>
<td>Lists only the View hosted applications. View Hosted Applications appear in your catalog if you integrate Workspace with View prior to accessing the admin console.</td>
</tr>
<tr>
<td>Citrix Published Applications</td>
<td>Lists only Citrix-based applications. Citrix-based applications appear in your catalog if you integrate Workspace with your Citrix deployment prior to accessing the admin console.</td>
</tr>
</tbody>
</table>
5. (Optional) To view resources by a specific category, select one or more category names from the Any Category drop-down menu.
   Workspace lists all the resources that meet the criteria you selected.
   - If you select one category, Workspace lists all the resources marked with that category label.
   - If you select more than one category, Workspace only lists resources that marked with all of those category labels.
6 Click the icon for a specific resource to view the details of that resource.

Add Resources to Your Catalog

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

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

- “Add a Web Application to Your Catalog from the Cloud Application Catalog,” on page 63
- “Add a Web Application to Your Catalog by Creating a New Application Record,” on page 65
- “Add a Web Application to Your Catalog by Importing a ZIP or JAR File,” on page 66

The following instructions provide an overview of the steps involved in adding these types of resources to your catalog.

Procedure

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

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Resource Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application ...from the cloud application catalog</td>
<td>Web application</td>
<td>Workspace includes access to several default Web applications, available in the cloud application catalog, that you can add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... create a new one</td>
<td>Web application</td>
<td>By filling out the appropriate form, you can create an application record for the Web applications you want to add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... import a ZIP or JAR file</td>
<td>Web application</td>
<td>You can import a Web application that you previously configured in Workspace. You might want to use this method to roll a Workspace deployment from staging to production. In such a situation, you export a Web application from the staging deployment as a ZIP file. You then import the ZIP file into the production deployment.</td>
</tr>
</tbody>
</table>

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

Use the search text box in the Workspace Admin Console to search for Workspace users, groups, or resources in your catalog.

Procedure

1. Log in to the Workspace Admin Console.
2. Enter a string into the search text box.

   For example, to search for all users that have an email address mycompany.com, enter *mycompany.com*.

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

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

**Note**: Up to 100 results are returned for each record type. For example, if the string appears in the records of more than 100 users, a maximum of 100 results is listed on the **Users** tab. You cannot change this maximum.
Providing Access to View Desktop and Application Pools

By integrating your organization’s View™ Connection Server instance with your Workspace system, you give your VMware Workspace Portal users the ability to use the Workspace App Portal to access their entitled View desktop and applications pools. Additionally, when the View module is enabled, you can use the Workspace admin console to see the associations between Workspace users and groups and their entitled View pools.

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

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

- You can use the Workspace admin console to monitor user and group entitlements to View desktop and application pools.
- Your Workspace users can use the Workspace App Portal to access their entitled View desktop and application pools.
  
  To ensure the best user experience on iPads, users should install the Horizon Client for iOS on their devices.

If the View module was not enabled during the installation and configuration of your Workspace system, you can enable the module after integrating your organization’s View Connection Server instance with your Workspace system. See “Enable the View Module to Integrate View with Workspace,” on page 54.

This chapter includes the following topics:

- “Enable the View Module to Integrate View with Workspace,” on page 54
- “View User and Group Entitlements to View Desktop and Application Pools,” on page 54
- “View the Connection Information for a View Desktop and Application Pools,” on page 55
- “Add View Pods to Workspace,” on page 55
- “Reducing Resource Usage and Increasing Performance of Workspace for Windows In Non-Persistent View Desktops,” on page 56
Enable the View Module to Integrate View with Workspace

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

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

Procedure

1. Log in to the Workspace Admin Console.
2. Select Dashboard > Modules, if not already selected.
3. In the View module, click Enable this module.
4. Perform the configurations required to complete the integration of View with Workspace.

The View module is enabled.

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

What to do next

Monitor user and group entitlements to View pools. See “View User and Group Entitlements to View Desktop and Application Pools,” on page 54.

View User and Group Entitlements to View Desktop and Application Pools

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

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

Prerequisites

- Verify that your Workspace system is integrated with your View system according to the steps in Installing and Configuring Workspace.
- Synchronize information and the respective entitlements from the View Connection Server instances with your Workspace system. You can force a sync using the following steps:
  1. Open the Connector Web interface in your browser. The Connector Web interface URL is https://ConnectorHostname/hc/admin/, where ConnectorHostname is the hostname for your Workspace Connector.
  2. Log in to the Connector Web interface using the administrative password for your Workspace system.
  3. Click View pools and click Sync Now.

Procedure

1. Log in to the Workspace Admin Console.
2. View user and group entitlements to View desktop and application pools.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the list of users and groups entitled to a specific View desktop</td>
<td>a) Click the Catalog tab.</td>
</tr>
<tr>
<td>pool.</td>
<td>b) Click Any Application Type &gt; View Desktop Pools or View Hosted</td>
</tr>
<tr>
<td></td>
<td>Applications.</td>
</tr>
<tr>
<td></td>
<td>c) Click the icon for the View pool for which you want to list</td>
</tr>
<tr>
<td></td>
<td>entitlements.</td>
</tr>
<tr>
<td></td>
<td>The Entitlements tab is selected by default. Group entitlements and</td>
</tr>
<tr>
<td></td>
<td>user entitlements are listed in separate tables.</td>
</tr>
</tbody>
</table>

| View the list of View desktop and application pool entitlements for a   | a) Click the Users & Groups tab.                                        |
| specific user or group.                                                | b) Click the Users tab or the Groups tab.                               |
|                                                                        | c) Click the name of an individual user or group.                       |
|                                                                        | The Entitlements tab is selected by default. Entitled View desktop and |
|                                                                        | application pools, if any, are listed in the View Pools tables on the  |
|                                                                        | Entitlements page.                                                     |

View the Connection Information for a View Desktop and Application Pools

You can view the information about the connection between Workspace and a View desktop or application pool.

Procedure

1. Log in to the Workspace Admin Console.
2. Click the Catalog tab.
3. Click Any Application Type > View Desktop Pool to view desktop pools. Click View Hosted Applications to view application pools.
4. Click the name of a View application.
5. Click the Details tab.
6. View the connection information, which consists of attributes retrieved from the View Connection Server instance.

   See the View documentation for details about these attributes.

Add View Pods to Workspace

You can add multiple View pod instances from the same Active Directory to Workspace. In Workspace, you add the View pod information in the Connector server View Pools page. Next you configure client access URLs for the different pods in the Workspace Admin Console, Settings > Network Range page.

Prerequisites

Verify that your Workspace system is integrated with your View system according to the steps in Installing and Configuring Workspace.

**NOTE** If you enable the smart card authentication option when you configure the View pod, users can only use the Horizon Client to access their View desktops.

Procedure

1. Log in to the Connector administrator web interface.
2. Click View Pools in the Navigation pane.
3 To permit access to the View Pools from Workspace, check the box Enable View Pools.
4 Click Add View Pod.
5 In the Connector Server text box, type the name of the View Connect Server.
6 In the Username text box, type the administrator's username for this View pod.
7 In the Password text box, enter the administrator's password for this View pod.
8 If users use smart card authentication to sign in to this View pod instead of passwords, enable the check box.
9 Select how often you want this information to sync from the View Connection Server.
10 Click Sync Now.
11 Log in to the Workspace Admin Console to finish the View Pod configuration.
   a Select Settings > Network Ranges.
   b Select an existing network range and click Edit.
   c In the View Pods section of the form, enter the View Pod client access URL host name and port number for the network range.

Reducing Resource Usage and Increasing Performance of Workspace for Windows In Non-Persistent View Desktops

To reduce resource usage and increase performance when using the Workspace App Portal in non-persistent desktops, also known as stateless desktops, you can configure the client with settings optimized for using it in a non-persistent View desktop.

Problem

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

Cause

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


Solution

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

<table>
<thead>
<tr>
<th>/v Installer Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_AUTOUPDATE = 0</td>
<td>Prevents the automatic update of the Workspace for Windows application to a newer version. Typically, your View administrator updates the application in the template.</td>
</tr>
<tr>
<td>/v Installer Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>INSTALL_MODE = RUN_FROM_SHARE</td>
<td>If you plan to have the users use ThinApp packages in these View desktops, use this option to have the ThinApp packages streamed from the server instead of downloaded to the Windows system.</td>
</tr>
</tbody>
</table>

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

```
Workspace-n.n.n-nnnnnnn.exe /v HORIZONURL=https://server.company.com ENABLE_AUTOUPDATE=0 INSTALL_MODE=RUN_FROM_SHARE
```
You can entitle Workspace users to your organization's external Web applications.

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

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

This chapter includes the following topics:

- “Enable the Web Applications Module to Provide Web Application Access,” on page 59
- “Establish Secure Single Sign-On to Your Web Applications Through Workspace,” on page 60
- “Adding Web Applications to Your Organization's Catalog,” on page 63
- “Entitle Users and Groups to Web Applications,” on page 67

**Enable the Web Applications Module to Provide Web Application Access**

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

**Prerequisites**

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

**Procedure**

1. Log in to the Configurator Web interface.
   
   See “Workspace Web Interface URLs,” on page 10 for the URL for the Configurator Web interface.

2. Click the **Module Configuration** tab.

3. Click **Enable this module** in the Web Applications module.

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

Add Web applications to the catalog. Configure Web applications as necessary, which might include configuring license tracking and provisioning for applications. See “Adding Web Applications to Your Organization’s Catalog,” on page 63.

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

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

Configuring Web Applications that Use SAML Protocol

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

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

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

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

To set up single-sign on Workspace, you

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

End User Authentication to Office 365 from Native Clients

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

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Native Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows computers</td>
<td>Microsoft Outlook Client</td>
</tr>
<tr>
<td>Apple Mac computers</td>
<td>Microsoft Outlook Client, Mac Outlook Web App</td>
</tr>
<tr>
<td>iPhone and iPad devices</td>
<td>iOS Email, Outlook Web App</td>
</tr>
<tr>
<td>Android devices</td>
<td>Android Email</td>
</tr>
</tbody>
</table>

A forgotten password cannot be retrieved. If users forget their passwords, they go back to the Office 365 app and enter a new password. They also must change this password on the native client.
Office 365 Requirements

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

Mapping Attributes in the Workspace Connector

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

Procedure

1. Log in to the Connector Web interface using the administrative password for your Workspace server.
   The Connector Web interface URL is https://ConnectorHostname/hc/admin/.
2. Verify that the Workspace userPrincipalName attribute is mapped to the Directory userPrincipalName attribute.
3. Click Add and add the Workspace attribute objectGUID and map it to the Directory attribute objectGUID.
4. Click Save.
5. To sync your changes to Active Directory immediately, select Directory Sync and click Edit Directory Sync Rules to run the Workspace Connector Sync wizard, otherwise your changes are synced to Active Directory at your next scheduled sync interval.
6. Exit the Connector.

What to do next

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

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

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

Prepare your Office 365 domain to use Workspace for authentication.

Prerequisites

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

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

<table>
<thead>
<tr>
<th>Line of cmdlet</th>
<th>cmdlet Variable or Variables</th>
<th>Replace with</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-DomainName</code></td>
<td><code>domain_name</code></td>
<td>The name of the Workspace domain that is registered with Microsoft.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.mycompanydomain_name.com</td>
</tr>
<tr>
<td><code>-IssuerUri</code></td>
<td><code>horizon_org_name</code></td>
<td>The unique identifier of the domain in the Office 365 identity platform used in Workspace, such as <code>example</code>.</td>
</tr>
<tr>
<td><code>-FederationBrandName</code></td>
<td><code>Federation_server_name</code></td>
<td>The name of the string value shown to users when signing in, such as <code>Mycompany Inc</code>.</td>
</tr>
<tr>
<td><code>-PassiveLogOnUri</code></td>
<td><code>host</code> and <code>port</code></td>
<td>The URL that Web-based clients are directed to when signing in, such as <a href="https://example123.mycompany.com:443/SAAS/API/1.0/POST/sso">https://example123.mycompany.com:443/SAAS/API/1.0/POST/sso</a>.</td>
</tr>
<tr>
<td><code>-ActiveLogOnUri</code></td>
<td><code>host</code> and <code>port</code></td>
<td>The URL that specifies the end point used by active clients when authenticating with domain set up for single sign-on. such as <a href="https://example123.mycompany.com/SAAS/auth/wsfed/activelogon">https://example123.mycompany.com/SAAS/auth/wsfed/activelogon</a>.</td>
</tr>
<tr>
<td><code>-LogOffUri</code></td>
<td><code>host</code> and <code>port</code></td>
<td>The URL clients are redirected to when they sign out, such as <a href="https://login.microsoftonline.com/logout.srf">https://login.microsoftonline.com/logout.srf</a>.</td>
</tr>
<tr>
<td><code>-MetadataExchangeUri</code></td>
<td><code>host</code> and <code>port</code></td>
<td>The URL that specifies the metadata exchange end point used for authentication, such as <a href="https://example123.mycompany.com/SAAS/auth/wsfed/services/mex">https://example123.mycompany.com/SAAS/auth/wsfed/services/mex</a>.</td>
</tr>
<tr>
<td><code>-SigningCertificate</code></td>
<td>SAML signing cert from Application Manager</td>
<td>The Workspace Manager signing certificate. On the Workspace Admin Console, go to Settings &gt; SAML Certificate, and copy the Signing Certificate and paste this as the value for SigningCertificate. Exclude “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” Exclude “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” from the certificate content. <strong>Note:</strong> Make sure you do not include additional spaces or extra line returns when you paste the certificate or it will not work.</td>
</tr>
</tbody>
</table>

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

**Example: Example of Output From Powershell Cmdlet**

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

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

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

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

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

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

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

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

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

Prerequisites

Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 59.

When you add a Web application to the catalog, you can apply a Web-application-specific access policy set to control user access to the application. If such a Web-application-specific access policy set does not already exist and you intend to apply one to this Web application, create the access policy set now. See “Managing Web-Application-Specific Access Policy Sets,” on page 30.
Procedure

1. Log in to the Workspace Admin Console.

2. Click the Catalog tab.

3. Click + Add Application > Web Application ...from the cloud application catalog.

4. Click the icon of the Web application to add to your organization’s catalog.

   The application record is added to your catalog, and record’s Details page displays with the name and authentication profile already specified in the form.

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

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

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

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

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

6. Click Save.

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

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

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

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

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

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

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

**Provisioning**  Select a provisioning adapter. Workspace ships with the provisioning adapters for Google Apps and Mozy. If you are configuring either of these Web applications, you can select the appropriate provisioning adapter.

Provisioning provides automatic application user management from a single location. Provisioning adapters allow the Web application to retrieve specific information from Workspace as required. For example, to enable automatic user provisioning to Google Apps, user account information, such as user ID, first name, and last name must exist in the Google Apps database. An application might require other information, such as group-membership and authorization-role information.

### What to do next

For details about adding user and group entitlements for Web applications, see “Entitle Users and Groups to Web Applications,” on page 67.

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

You create an application record when the Web application to add to your catalog is not available in the cloud application catalog.

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

### Prerequisites

Enable the Web Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 59.

When you add a Web application to the catalog, you can apply a Web-application-specific access policy set to control user access to the application. If such a Web-application-specific access policy set does not already exist and you intend to apply one to this Web application, create the access policy set now. See “Managing Web-Application-Specific Access Policy Sets,” on page 30

### Procedure

1. Log in to the Workspace Admin Console.
2. Click the Catalog tab.
3. Click + Add Application > Web Application ...create a new one.

   The application record is added to your catalog, and the system displays the record’s Details page.
4. Complete the information on the Details page, and click Next.

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

### Authentication Profile

Specify the appropriate federation protocol, if any.

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

Some of the items on the form are prepopulated.

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

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

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

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

What to do next

See “Entitle Users and Groups to Web Applications,” on page 67 for details about adding user and group entitlements for Web applications.

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

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

This process involves exporting the application bundle of a Web application from a Workspace instance and importing the bundle to another Workspace instance. Because you import the Web application from a Workspace deployment, the application might not require further configuration, especially if you thoroughly tested the configuration values in the original deployment. To further configure the Web application after importing it, see “Add a Web Application to Your Catalog from the Cloud Application Catalog,” on page 63 or “Add a Web Application to Your Catalog by Creating a New Application Record,” on page 65.
Prerequisites

Verify the following items:

- The Web Applications module is enabled. See “Enable the Web Applications Module to Provide Web Application Access,” on page 59.
- You can log in as an administrator to the Workspace instance that has the Web application to add to your catalog.

Procedure

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

What to do next

For details about adding user and group entitlements for Web applications, see “Entitle Users and Groups to Web Applications,” on page 67.

Entitle Users and Groups to Web Applications

You can entitle users and groups to Web applications.

You can only entitle Workspace users, users who are imported from your directory server, to Web applications. When you entitle a user to a Web application, the user sees the application and can launch it from their Workspace App Portal. 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 Applications module. See “Enable the Web Applications Module to Provide Web Application Access,” on page 59.
- Add one or more Web applications to your catalog. See “Adding Web Applications to Your Organization's Catalog,” on page 63.
Procedure

1. Log in to the Workspace Admin Console.

2. Entitle users to a Web application.

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

The selected user or group is now entitled to use the Web application.
Providing Access to Citrix-Based Applications

You can provide Workspace users access to Citrix-based applications.

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

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

Typically, you integrate your Citrix deployment with Workspace while deploying Workspace. To complete the integration, you can enable the Citrix Published Applications module using the admin console.

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

This chapter includes the following topics:

- “Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment,” on page 69
- “View User and Group Entitlements to Citrix-Based Applications,” on page 70
- “Editing Workspace Application Delivery Settings for Citrix-Based Applications,” on page 71
- “Managing Categories for Citrix-Based Applications,” on page 72

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

If you did not enable the Citrix Published Applications module when you installed and configured Workspace, you can enable it later from the **Modules** tab on the Dashboard page of the Workspace Admin Console.

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

**Procedure**

1. Log in to the Workspace Admin Console.
2. Select **Dashboard > Modules**.
3. In the Citrix Published Applications module, click **Enable this module**.
4 Perform the configurations required to complete the Integration of your Citrix deployment with Workspace.

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

What to do next

To edit the delivery settings of Citrix-based applications, such as the settings for streaming or security, use the admin console. See “Editing Workspace Application Delivery Settings for Citrix-Based Applications,” on page 71.

View User and Group Entitlements to Citrix-Based Applications

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

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

Prerequisites

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

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

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

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

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

Procedure

1. Log in to the Workspace Admin Console.

2. View user and group entitlements to Citrix-based applications.

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

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

You can use the Workspace Admin Console to edit the delivery settings of Citrix-based applications. You can edit the delivery settings globally for all of the Citrix-based applications available from your Workspace deployment, or individually for specific Citrix-based applications.

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

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

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

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

You can use the Workspace Admin Console to edit the global settings for the Citrix-based applications in your Workspace deployment.

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

Prerequisites

Enable the Citrix Published Applications module. See “Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment,” on page 69

Procedure

1. Log in to the Workspace Admin Console as an administrator.
2. Select Settings > Citrix Published Applications.
3. Edit the ICA properties according to Citrix guidelines.

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

4. Click Save.

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

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

You can use the Workspace Admin Console to edit the settings for individual Citrix-based applications in your Workspace deployment.

The ICA properties text boxes for individual applications are empty until you manually add properties.
When you edit the application delivery settings, the ICA properties, of an individual Citrix-based application, those settings take precedence over the global settings. You can configure the global ICA property settings from the Citrix Published Applications page by selecting Settings > Citrix Published Application.

Prerequisites
Enable the Citrix Published Applications module. See “Enable the Citrix Published Applications Module to Integrate Workspace with Your Citrix Deployment,” on page 69.

Procedure
1. Log in to the Workspace Admin Console as an administrator.
2. Click the Catalog tab.
3. Click Any Application Type > Citrix Published Applications.
4. Click the name of the Citrix-based application to edit.
5. Click Configuration.
6. View the information about the application as carried forward from your Citrix deployment.
   The page provides several details about the application, such as the application name, application ID, server name, and so on. Also, the page displays information about the application’s enablement. If the Enabled check box is not selected, the application is disabled in your Citrix deployment.
7. If the Enabled check box is not selected and you want to hide the application from users, select the Hide When Disabled check box.
8. In the ICA properties text boxes, add properties or edit existing properties according to Citrix guidelines.
   The ICA Client Properties and the ICA Launch Properties text boxes work together. They must both have content or they must both be empty.
9. Click Save.

Your Citrix deployment applies the ICA properties listed on the Workspace Configuration page of an application when it delivers the Citrix-based application to users.

Managing Categories for Citrix-Based Applications
You can use the Workspace Admin Console and your Citrix deployment to manage Citrix-based application categories.

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

After the integration, you can continue to create categories in your Citrix deployment. Those categories are carried over to Workspace during the next sync. You can also create categories directly in Workspace. See “Overview of Using Resource Categories,” on page 47.

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

When you create a category in Workspace, the category never appears in your Citrix deployment.
When you create a category in your Citrix deployment, the category appears in Workspace at the next sync. When you update a category name in your Citrix deployment, the updated category name appears in Workspace while the original category name remains. If you want to remove the original category name from Workspace, you must remove it manually.
Providing Access to VMware ThinApp Packages

With Workspace, you can centrally distribute and manage ThinApp packages. ThinApp packages are virtualized Windows applications, and are used on Windows systems. Entitled users who have the Workspace for Windows application installed on their Windows systems can launch and use their entitled ThinApp packages on those Windows systems.

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

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

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

This chapter includes the following topics:

- “Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Workspace System,” on page 76
- “Distributing and Managing ThinApp Packages with Workspace,” on page 76
- “Entitle Users and Groups to ThinApp Packages,” on page 81
- “Updating Managed ThinApp Packages After Deployment in Workspace,” on page 83
- “Delete ThinApp Packages from Workspace,” on page 88
- “Make Existing ThinApp Packages Compatible with Workspace,” on page 89
Enable the ThinApp Packages Module after Integrating Your ThinApp Repository with Your Workspace System

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

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

Prerequisites

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

Procedure

1. Log in to the Workspace Admin Console.
2. Select Dashboard > Modules.
3. In the ThinApp Packages module, click Enable this module.

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

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

What to do next

As appropriate, distribute the Workspace Client for Windows to users’ Windows systems for those users to whom you want to entitle ThinApp packages. See “Deploying the Workspace for Windows Application To Use ThinApp Packages,” on page 77.

Distributing and Managing ThinApp Packages with Workspace

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

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

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

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

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

**Deploying the Workspace for Windows Application To Use ThinApp Packages**

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

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

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

One method for installing the Workspace for Windows application to multiple Windows systems is to use a script to install the application silently to the Windows systems. You can install the client silently to multiple Windows systems at the same time.

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

You set a value in the script to indicate whether the clients installed by that script deploy ThinApp packages using the ThinApp streaming mode, or RUN_FROM_SHARE option, or one of the ThinApp download modes, such as the COPY_TO_LOCAL or HTTP_DOWNLOAD option. See “Install the Workspace for Windows Application with Identical Settings to Multiple Windows Systems,” on page 99.
Determining the Appropriate Deployment Mode for ThinApp Packages on Windows Endpoints

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

With streaming mode, when the Workspace for Windows application synchronizes with Workspace, the client downloads application shortcuts for the ThinApp packages' virtualized Windows applications to the Windows desktop, and when the user launches the ThinApp packages, the virtualized Windows applications run from the file share on which the ThinApp packages reside. Therefore, streaming mode is best appropriate for systems that will always be connected to the network share, such as View desktops.

With download mode, at the first use or update of a ThinApp package, the user must wait for the ThinApp package to download to the Windows system first, and shortcuts are created. After the initial download, the user launches and runs the virtualized Windows application on the local Windows system.

**IMPORTANT** For non-persistent View desktops, also known as floating or stateless View desktops, you are expected to set the client to use ThinApp streaming mode by using the command-line installer option /v INSTALL_MODE=RUN_FROM_SHARE when installing the client. The RUN_FROM_SHARE option provides the most optimal runtime experience for using ThinApp packages in floating View desktops. See “Command-Line Installer Options for Workspace for Windows,” on page 93.
Table 13-1. ThinApp Deployment Mode for the Virtualized Applications Captured as ThinApp Packages

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

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

**Offline Grace Period and ThinApp Packages**

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

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

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

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

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

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

### Set the Offline Grace Period for ThinApp Packages

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

**Prerequisites**

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

**Procedure**

1. Open the Windows system's registry in the Registry Editor.
2. Locate the OfflineGracePeriod registry key.

   Windows System | Registry Key |
   --- | --- |
   Windows 32-bit | HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc. \Horizon ThinApp\OfflineGracePeriod |
   Windows 64-bit | HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc. \Horizon ThinApp\OfflineGracePeriod |

   The OfflineGracePeriod key has type REG_DWORD. The default settings is 720 (30 days).
3. Update the OfflineGracePeriod value to a timespan in hours.
4. Exit the Registry Editor.

### Using the Command-Line HorizonThinAppCtrl.exe Application

The Workspace for Windows application includes a command-line application, HorizonThinAppCtrl.exe, that you can use to perform operations related to using ThinApp packages on the user’s Windows system.

The installation process for Workspace for Windows installs HorizonThinAppCtrl.exe in the \HorizonThinApp folder in the Windows directory location where the Workspace for Windows is installed.

To use the HorizonThinAppCtrl.exe application to perform one of its supported commands, provide the command as the first argument, followed by the command’s available options, as appropriate.

HorizonThinAppCtrl.exe command options
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HorizonThinAppCtrl.exe recheck</td>
<td>This command immediately does an entitlement check of the ThinApp packages that are associated with the user account that is logged into the Workspace for Windows client. Any newly entitled or updated ThinApp packages are synced.</td>
</tr>
</tbody>
</table>
| HorizonThinAppCtrl.exe set InstallMode=install_mode | This command changes the ThinApp deployment mode used for ThinApp packages on this Windows system. Because this command changes the registry keys associated with the ThinApp deployment mode, only administrators with the appropriate registry permissions are able to change the install mode using this command. Available values for install_mode are:  
- CopyToLocal  
- RunFromShare  
- HttpDownload |
| HorizonThinAppCtrl.exe authorize guid=ThinApp_GUID path=package_path | This command verifies whether a ThinApp package can be launched. This command does not actually launch the ThinApp package. Provide the ThinApp package's GUID and the path to the package's executable file. If ThinApp download mode is used for the packages on the Windows client system, the path is relative to the local cache root folder, which is the same as the path relative to the repository root. An example is HorizonThinAppCtrl.exe authorize guid= 436E1D7D-552C-4F70-8197-DB1B95D03994 path="FileZilla Client 3.3.2/FileZilla.exe"  
You can see the ThinApp package's GUID, application path, and executable file name on its resources page in the admin console. |
| HorizonThinAppCtrl.exe quit | This command tells the Workspace for Windows to exit cleanly. |
| HorizonThinAppCtrl.exe launch app=package_path url=launch_url | This command is used to manually launch a ThinApp package, where package_path is the path to the package's executable file, and launch_url is the Workspace protocol URL for that package, in the form horizon://package_path. An example is HorizonThinAppCtrl.exe launch app="FileZilla Client 3.3.2/FileZilla.exe" url="horizon://FileZilla Client 3.3.2/FileZilla.exe"  
This command is not typically used by end users, who can launch their entitled ThinApp packages from their My Apps area in the user portal. This command is typically used for debugging. |

### Entitle Users and Groups to ThinApp Packages

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

You can only entitle Workspace users, users who are imported from your directory server, to ThinApp packages. When you entitle a user to a ThinApp package, the user sees the application and can start it from the Workspace for Windows application on their system. If you remove the entitlement, the user cannot see or start the application.

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

### Prerequisites

Configure Workspace to sync ThinApp packages to your Workspace catalog. When the ThinApp packages are synced to your catalog, you can entitle them to your users and groups.

Use the Configurator Web Interface or the Connector Web Interface to sync ThinApp packages to your catalog. You cannot add ThinApp packages directly to your catalog from the Workspace Admin Console.

### Procedure

1. Log in to the Workspace Admin Console.
2 Entitle users to a ThinApp package.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Access a ThinApp package and entitle users or groups to it.** | a Click the Catalog tab.  
   b Click Any Application Type > ThinApp Packages.  
   c Click the ThinApp package to which to entitle users and groups.  
   The Entitlements tab is selected by default. Group entitlements are listed in one table, user entitlements are listed in another table.  
   d Click Add group entitlement or Add user entitlement.  
   e Type the names of the groups or users.  
   You can search for users or groups by starting to type a search string and allowing the autocomplete feature to list the options. You can click browse to view the entire list.  
   f From the drop-down menu, select the activation method for the ThinApp package.  
   - **Automatic** Users have immediate access to the ThinApp package the next time they log in to the Workspace client.  
   - **User-Activated** Users must activate the ThinApp package in Workspace for Windows before they can use the application.  
   g Click Save. |
| **Access a user or group and add ThinApp package entitlements to that user or group.** | a Click the Users & Groups tab.  
   b Click the Users or Groups tab.  
   c Click the name of an individual user or group.  
   d Click Add entitlement.  
   e Click the check boxes next to the ThinApp packages to which to entitle the user or group.  
   f From the drop-down menu, select the activation method for the ThinApp package.  
   - **Automatic** Users have immediate access to the ThinApp package the next time they log in to the Workspace client.  
   - **User-Activated** Users must activate the ThinApp package in Workspace for Windows 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 Workspace for Windows application is installed on users' Windows systems.
Updating Managed ThinApp Packages After Deployment in Workspace

After adding a ThinApp package to your organization’s catalog and entitling your Workspace users to that ThinApp package, your organization might want to update that package and have the users use a newer, or rebuilt, version of the ThinApp package, without having to unentitle the users from the current package and then entitlement them to the newer package.

An updated ThinApp package might be made available because a newer version of the Windows application for that package is released, or because the packager of the application has changed the values of parameters used by the package.

ThinApp 4.7.2 and newer versions provide an update mechanism for ThinApp packages used in a Workspace system. This ThinApp update mechanism is different from other update mechanisms for ThinApp packages used outside of a Workspace environment. The updated ThinApp package must have been updated with this mechanism for you to be able to deploy the updated package in Workspace and have users automatically see the newer version.

For ThinApp packages that are managed in a Workspace system, two Package.ini parameters are used by Workspace to determine that a package is an updated version of another package.

**AppID**

The unique identifier for the ThinApp package in Workspace. All entry points (executables) for the package’s application are assigned the same AppID. After a ThinApp package is synced to your organization’s Workspace catalog, the package’s AppID is displayed in the GUID column in the ThinApp package’s resource page. This value consists of alphanumeric characters in a pattern of character sets, each set separated by dashes, such as in the following example:

```
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

Workspace considers any ThinApp package with the same AppID to be versions of the same application.

**VersionID**

The version number of the ThinApp package. Workspace uses the VersionID to keep track of different versions of the managed ThinApp package. You increment the VersionID value by one (1) to mark that ThinApp package as an update of another package, retaining the same AppID.

You place the updated package in a new folder in the network share folder configured for the managed ThinApp packages. See *Installing and Configuring Workspace*. When Workspace performs the scheduled sync with the network share folder and it encounters an application that has the same AppID as another application, it compares the VersionID values. The ThinApp package with the highest VersionID is used as the most recent update. Workspace automatically incorporates the previous user entitlements to the ThinApp package with the highest VersionID, and shortcuts on the users’ systems are synced to point to the updated package.

**IMPORTANT** The standard ThinApp InventoryName parameter is important to successful updates of managed ThinApp packages. Both the previous and updated ThinApp packages must have the same value for the InventoryName parameter. If the person creating the ThinApp package changes the InventoryName in a package, and then creates an updated package, you must make sure the InventoryName values match for the updates to work properly in your Workspace system.

See the *ThinApp Package.ini Parameters Reference Guide* for details about the various parameters that are used in a ThinApp package’s Package.ini file.
Update a Managed ThinApp Package

Updating a ThinApp package that is already managed by Workspace and in your organization's catalog involves multiple steps. The updated ThinApp package might be provided to you by another group in your organization. To ensure that your Workspace system can automatically use the updated package in place of the existing one for the entitled users, you must ensure the updated package was created using the same AppID as the current package, has a VersionID value that is higher than the existing package's VersionID value, and is enabled for management by Workspace.

Prerequisites

Verify that you have access to the location where your managed ThinApp packages reside and can create subfolders at that location.

Procedure

1. Obtain the AppID and VersionID values of a Managed ThinApp Package on page 84
   
   To ensure that Workspace automatically uses the updated ThinApp package in place of the current one, the updated ThinApp package must be created using the AppID of the currently managed ThinApp package and a higher VersionID value than the current version.

2. Create the Updated ThinApp Package on page 85
   
   The AppID and VersionID values of the currently managed ThinApp package are used for creating the updated package. The updated package uses the same AppID value and a higher VersionID value.

3. Copy an Updated ThinApp Package to the Network Share on page 87
   
   After you create the updated ThinApp package, you copy the appropriate files to a new subfolder at the same level as the existing subfolder on the network share.

What to do next

Your Workspace catalog displays the new version of the updated ThinApp package after the next sync of your Workspace system with your ThinApp package location. If you want to see the new version reflected in the ThinApp package's resources page, you can manually sync using the ThinApp Packages page of the Connector Web interface. See Installing and Configuring Workspace.

Obtain the AppID and VersionID values of a Managed ThinApp Package

To ensure that Workspace automatically uses the updated ThinApp package in place of the current one, the updated ThinApp package must be created using the AppID of the currently managed ThinApp package and a higher VersionID value than the current version.

When the Setup Capture process is used to create an updated ThinApp package, the AppID value is automatically retrieved by the Setup Capture program from the existing ThinApp package's executables, and the VersionID value is automatically incremented. However, the person who is creating the updated ThinApp package might use a different method for creating the updated package. When the Setup Capture process is not used to create the updated ThinApp package, the person creating the package must obtain the AppID and VersionID values for the ThinApp package that is currently managed by your Workspace system. The AppID and VersionID values are displayed on pages in the ThinApp package's resource page in the Workspace Admin Console.

Procedure

1. Click the Catalog tab.

2. Click Any Application Type > ThinApp Packages.

3. Click the ThinApp package to open its resource page.

4. Click Details.
5 Make note of the value listed in the **Version** field on the Details page.

6 Click **ThinApp Package** to display the ThinApp Package page.

7 Make note of the **AppID** value listed in the GUID column.

   The value listed in the GUID column is the value that Workspace uses to identify this ThinApp package.

**What to do next**

The person who is creating the updated ThinApp package should complete the steps in “Create the Updated ThinApp Package,” on page 85.

**Create the Updated ThinApp Package**

The **AppID** and **VersionID** values of the currently managed ThinApp package are used for creating the updated package. The updated package uses the same **AppID** value and a higher **VersionID** value.

Sometimes the updated ThinApp package is provided to you by another team in your organization. The person who creates the updated ThinApp package can use one of the described methods.

**Prerequisites**

Verify that you have the **AppID** and **VersionID** values of the current ThinApp package by completing the steps in “Obtain the AppID and VersionID values of a Managed ThinApp Package,” on page 84.

Verify that you have a version of the ThinApp program that is compatible with your version of Workspace. For information about specific ThinApp versions, see the **VMware Product Interoperability Matrixes** at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
**Procedure**

- Using a version of the ThinApp program that is supported by Workspace, create the updated ThinApp package using one of the available methods.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Recapture using Setup Capture.** | Use this method when the project folder for the existing ThinApp package managed by Workspace is unavailable. To create an updated package with Setup Capture, you need only the following items:  
- The application executables from the existing ThinApp package  
- The application installer  
- Setup Capture and the ThinApp program at a version supported by Workspace.  
During the capture process, select to manage the package with Workspace and that the package is an update of an existing base ThinApp package. Browse to the folder that contains the executables for the currently managed ThinApp package. Point to the folder, and not to specific executables.  
With this method, you do not need to obtain the AppID or VersionID values in advance of creating the updated package. After you designate the package as an update and point to the prior version in Setup Capture, the capture process reads the AppID of the prior package and reuses it for the updated package. The process also provides an incremented VersionID for the updated package, and assigns the same InventoryName. |
| **Update the Package.ini file manually and then rebuild the package.** | Use this method when you do not have the application installer for the recapture process, or when you need to update the package to a newer ThinApp version and want to update more than what the relink command would handle. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new Package.ini parameter that you want to set.  
To mark the new package as an update, edit the following Workspace parameters in the [Build Options] section of the Package.ini file:  
- Set the AppID parameter to match the AppID value of the currently managed ThinApp application. You cannot reuse a value of genid for AppID, because then a new AppID value will be generated for the updated package and your Workspace system will not recognize the new package as an update to the existing one.  
- Increment the value of the VersionID parameter to a higher integer than the currently managed ThinApp package. If there is no VersionID parameter set for the currently managed package, its value is 1 by default, and you would add a line for the VersionID parameter to Package.ini and set it to a value of 2 (VersionID = 2)  
- Make sure the InventoryName parameter value matches the InventoryName value of the currently managed package. The InventoryName values for the current package and the updated package must be identical. |
| **Use the relink –h command with the AppID and VersionID options.** | Use this method in one of the following situations:  
- You do not have the project folder for the application.  
- You have already captured, built, and tested the package in a test environment that was not a Workspace system, and the only remaining steps are to enable the updated package for Workspace and place it in the network share used by the Workspace system.  
- You are updating the package only to update the ThinApp runtime for the package to incorporate bug fixes available in that new ThinApp version. |
Option | Description
--- | ---
For example, if you have changed the project directory, including the Package.ini file, for a virtual application, rebuilt the package, and tested the package, the test environment might not have been Workspace. The final stage of updating the application is to enable it for Workspace. At that point, the easiest route is to use the `relink -h` command, instead of recapturing or rebuilding.

**NOTE** The ThinApp runtime is always updated when you run the `relink -h` command on a ThinApp package.

You can run the `relink` command from the ThinApp Program Files directory to get help on the command's syntax.

When the existing ThinApp package is already enabled for use by Workspace, you can run the following command to reuse the package's existing AppID and increment the VersionID:

```
relink -h -VersionID + executable-folder/*. *
```

Where `executable-folder` is a folder containing the executables of the ThinApp package you want to update.

**IMPORTANT** When you use the `relink` command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Workspace environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point `relink` to a copy of the folder of executables.

Other use cases for the `relink` command, including enabling a ThinApp package for use in a Workspace environment, are covered in the VMware knowledge base article at http://kb.vmware.com/kb/2021928.

You have a set of files (EXE files, and optionally DAT files) for the updated ThinApp package.

**What to do next**

Copy the files to a new subfolder on the network share, by completing the steps in “Copy an Updated ThinApp Package to the Network Share,” on page 87.

**Copy an Updated ThinApp Package to the Network Share**

After you create the updated ThinApp package, you copy the appropriate files to a new subfolder at the same level as the existing subfolder on the network share.

**Prerequisites**

Verify that you have the files for the updated ThinApp package, as a result of completing the steps in “Create the Updated ThinApp Package,” on page 85 and incrementing the VersionID value.

Verify that you have access to the network share and can make subfolders and copy files to it.

**Procedure**

1. In the network share folder, create a new subfolder for the updated ThinApp package.

   Retain the existing subfolder for the ThinApp package that you are updating, and do not alter its contents.

   After the next scheduled sync, Workspace ignores the older package, when it recognizes the new package has the same AppID value and a higher VersionID value.
Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named appshare on a host named server, and the application is called abceditor, the subfolder for the ThinApp package is `\server\appshare\abceditor`.

**NOTE** Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Workspace. Non-ASCII characters are not supported.

2. Copy the EXE and DAT files for the updated ThinApp package into that new subfolder.

3. (Optional) If you do not want to wait for the next scheduled sync time, you can manually sync your Workspace system with the network share using the ThinApp Packages page of the Connector Web interface.

When Workspace performs the scheduled sync with the network share folder and it encounters an application that has the same AppID as another application, it compares the VersionID values. The ThinApp package with the highest VersionID is used as the most recent update. Workspace automatically incorporates the previous user entitlements to the ThinApp package with the highest VersionID, and shortcuts on the users’ systems are synced to point to the updated package.

### Delete ThinApp Packages from Workspace

You can permanently remove a ThinApp package from Workspace.

When you delete a ThinApp package from Workspace, you permanently remove it. You can no longer entitle users to the ThinApp package unless you add it back to Workspace.

**Procedure**

1. Delete the ThinApp package subfolder from the network file share that is the ThinApp package repository connected to your Workspace system.

2. Delete the application from Workspace.
   a. Log in to the Workspace Admin Console.
   b. Click the Catalog tab.
   c. Click **Any Application Type > ThinApp Packages**.
   d. Search for the ThinApp package to delete.
   e. Click the ThinApp package name to display its resource page.
   f. Click **Delete**, read the message, and if you agree, click **Yes**.

The ThinApp package does not exist in your Workspace catalog.
Make Existing ThinApp Packages Compatible with Workspace

You can convert a ThinApp package from one that is not compatible with Workspace to one that Workspace can distribute and manage. You can use one of the following methods: use the ThinApp 4.7.2 relink command, rebuild the package from its ThinApp project files after editing the project’s Package.ini file to add the necessary Workspace parameters, or recapture the Windows application with the appropriate Workspace settings selected in the ThinApp Setup Capture program.

**Note** A ThinApp package that is compatible with Workspace can only be used for a Workspace deployment. Only Workspace users who have the Workspace Client for Windows installed can launch and run these enabled packages. At runtime, the ThinApp package loads a specifically named DLL, and uses that DLL to verify the user’s entitlement with their Workspace system. Because the DLL is installed with the Workspace Client for Windows, such ThinApp packages can only be run on Windows systems on which that client is installed.

**Prerequisites**

Verify that you have access to the necessary items for your chosen method.

- If you are using the relink command, verify that you have the executable files for the ThinApp package that you are converting and the ThinApp 4.7.2 relink.exe application.

- If you are updating the ThinApp project’s Package.ini file and rebuilding the package, verify that you have the project files needed by the ThinApp 4.7.2 program to rebuild the package.

- If you are recapturing the Windows application, verify that you have the ThinApp 4.7.2 Setup Capture program and the application installer and other items that the program needs to recapture the application. See the ThinApp User’s Guide for details.

Verify that you have access to the ThinApp network share used by your Workspace system, and can make subfolders and copy files to it.
Procedure

- Using a version of the ThinApp program that is supported by Workspace, create a compatible ThinApp package using one of the available methods.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use the relink –h command. | Using the relink –h command is the easiest method. You must use the relink.exe program from ThinApp 4.7.2 or later. Use this method in one of the following situations:  
- You cannot use the rebuild method because you do not have the project folder.  
- Using Setup Capture to recapture the application would take too long.  
- You do not have the application installer that is required for recapturing with Setup Capture.  

**Note** The ThinApp runtime is always updated when you run the relink –h command on a ThinApp package.  
You can run the relink command from the ThinApp Program Files directory to get help on the command’s syntax.  
To create a compatible package, use the basic syntax of the command:  
relink –h executable-folder/*.  
Where executable-folder is a folder containing the executables of the ThinApp package you want to update.  

**Important** When you use the relink command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Workspace environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point relink to a copy of the folder of executables.  
Other use cases for the relink command are covered in the VMware knowledge base article at http://kb.vmware.com/kb/2021928. |
| Update the Package.ini file manually with the necessary Workspace parameters, and then rebuild the package. | Use this method when you do not have the application installer for the recapture process, when you want to avoid doing the up-front setup that recapturing the application requires, or when you want to incorporate functionality from a newer ThinApp version more than what the relink command would provide. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new Package.ini parameter that you want to set.  
In the [Build Options] section of the Package.ini file, add the following parameters:  
`;-------- Workspace Parameters ----------`  
`AppID=genid`  
`NotificationDLLs=HorizonPlugin.dll`  
HorizonPlugin.dll is the DLL that the ThinApp runtime calls to verify the Workspace user's entitlement to use the virtualized application.  
You can optionally include the `HorizonOrgURL` parameter and set it to your Workspace fully qualified domain name (WorkspaceFQDN). See Installing and Configuring Workspace. |
| Recapture using Setup Capture, and select the necessary Workspace settings. | Use this method when you would prefer to recapture the application rather than use one of the other methods. To create a compatible package using ThinApp Setup Capture, select the appropriate settings in the wizard to manage the package with Workspace during the capture process. See the ThinApp User's Guide for details on the capture process. |

You have a set of files (EXE files, and optionally DAT files) for a ThinApp package that Workspace can distribute and manage.
What to do next
Add the ThinApp package to the repository that your Workspace system uses, by completing the steps in “Add ThinApp Packages to the Network Share,” on page 91.

Add ThinApp Packages to the Network Share
To make ThinApp packages available for your Workspace to distribute them, you add the packages to the ThinApp packages repository that is integrated with your Workspace system. This repository is a network share that is connected to your Workspace server.

Prerequisites
Verify that your Workspace system is integrated with your ThinApp packages repository, according to the steps in Installing and Configuring Workspace.
Verify that you have access to the network share and can make subfolders and copy files to it.
Verify that the ThinApp packages are compatible with Workspace, and you have all of the EXE and DAT files for the packages.

Procedure
1. In the network share, create a network share subfolder for each ThinApp package.
   Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named `appshare` on a host named `server`, and the application is called `abcditor`, the subfolder for the ThinApp package is `\server\appshare\abcditor`.
   
   **Note**: Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Workspace. Non-ASCII characters are not supported.

2. For each ThinApp package, copy its files, such as its EXE and DAT files, to the subfolder that is named for that package's virtualized application.
   After copying the files, you have a set of subfolders and files that are similar to these files:
   
   - `\server\appshare\abcditor\abcditor.exe`
   - `\server\appshare\abcditor\abcditor.dat`

3. (Optional) If you do not want to wait for the next scheduled sync time, you can manually sync your Workspace system with the network share using the ThinApp Packages page of the Connector Web interface.
   The ThinApp packages are available for your Workspace server to distribute and manage.
Before your Workspace users can run their ThinApp packages that are registered to them using Workspace, those users must have the Workspace for Windows application installed and running on their Windows systems.

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

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

**NOTE** If any browser windows are open during installation of the Workspace for Windows application, problems might occur with launching ThinApp packages from the user portal. Either close all browser windows before installing the application, or immediately after installing the application, restart your browsers. See “ThinApp Packages Fail to Launch from the User Portal,” on page 110.

This chapter includes the following topics:

- “Command-Line Installer Options for Workspace for Windows,” on page 93
- “Install the Workspace for Windows Application with Identical Settings to Multiple Windows Systems,” on page 99

### Command-Line Installer Options for Workspace for Windows

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

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

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

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

### Table 14-1. Installer Command-Line Options

<table>
<thead>
<tr>
<th>Installer Option</th>
<th>Value</th>
<th>Description</th>
<th>Long Form Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>/c</td>
<td>path to configuration file/filename</td>
<td>Provides a configuration file to use in the installation process.</td>
<td>/cfgfile</td>
</tr>
<tr>
<td>/T</td>
<td>path to temporary directory</td>
<td>Provides a directory to use as a temporary extraction location during the installation process.</td>
<td>/Temp</td>
</tr>
<tr>
<td>/S</td>
<td>path to search for files</td>
<td>Provides a set of paths for the installer to search for files, in addition to the installer package file.</td>
<td>/SearchPaths</td>
</tr>
<tr>
<td>/P</td>
<td>path to package file/filename</td>
<td>Provides a package file to use in the installation process.</td>
<td>/Package</td>
</tr>
<tr>
<td>/s</td>
<td>No values</td>
<td>Runs the installation silently. A silent installation does not display messages or windows during deployment. You typically use this option when using a deployment script to run the installer program in an unattended install process, and you want to suppress the display of interactive messages and windows. You can use this option with the /x or /uninst option to silently uninstall the application.</td>
<td>/silent</td>
</tr>
<tr>
<td>/nsr</td>
<td>No values</td>
<td>Suppresses an automatic reboot after a successful silent installation process.</td>
<td>/noSilentReboot</td>
</tr>
<tr>
<td>/f2</td>
<td>path to log file</td>
<td>Provides the location of the installation log file.</td>
<td>/log</td>
</tr>
<tr>
<td>/d</td>
<td>No values</td>
<td>Write debugging information to the installation log file.</td>
<td>/debug</td>
</tr>
<tr>
<td>/V</td>
<td>No values</td>
<td>Sets verbose logging.</td>
<td>/verbose</td>
</tr>
<tr>
<td>/L</td>
<td>English language name or localized language name or three-letter language abbreviation or language identifier</td>
<td>Runs the installer in the named language, for example, Workspace-\textit{n.n.n-nnnnnnn} /lang French where \textit{n.n.n-nnnnnnn} is the file version and build number for your downloaded installer program.</td>
<td>/lang</td>
</tr>
<tr>
<td>/v</td>
<td>key-value pairs</td>
<td>Provides a set of arguments to use in the installation process as a key-value pair, provided in the format key=value. These arguments are passed to the MSI file and configure runtime for the ThinApp packages capabilities provided by the Windows application.</td>
<td>/msi_args</td>
</tr>
<tr>
<td>/x</td>
<td>No values</td>
<td>Uninstalls the application.</td>
<td>/uninst</td>
</tr>
<tr>
<td>/clean</td>
<td>No values</td>
<td>Cleans out the installation registration information.</td>
<td>No long form alternative</td>
</tr>
</tbody>
</table>

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

The following table describes the available key-value pairs used for the /v installer option.
<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HORIZONURL</td>
<td>URL</td>
<td>Provides the URL to your Workspace system, where HTTPS is the required protocol, to allow the Windows application to communicate with your Workspace system, for example HORIZONURL=<a href="https://WorkspaceFQDN">https://WorkspaceFQDN</a>. <strong>Note</strong> The value must include the full URL, including the protocol portion, such as https://.</td>
</tr>
<tr>
<td>PROMPTFORAUTH</td>
<td>0 or 1</td>
<td>Presents users with a login window if Kerberos authentication fails. Set the value of this variable to 1 to enable the client application to respond to a Kerberos failure by prompting users to log in from a browser window. Workspace-n.n.n-nnnnnnnn /v PROMPTFORAUTH=1 Setting the value of this variable to 0 is the same as not including the variable in the command. The result is that upon a Kerberos failure the client application does not automatically open the login in a browser window. However, the user receives an indication in the Windows system tray that the client is not authenticated to the server yet and can start the process manually.</td>
</tr>
<tr>
<td>Keys for the /v Option</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>INSTALL_MODE</td>
<td>COPY_TO_LOCAL</td>
<td>Sets the deployment mode for how the Workspace for Windows application obtains ThinApp packages at runtime. ThinApp packages are virtualized Windows applications. The ThinApp packages reside on a network share that is integrated with your Workspace system using the Connector. With COPY_TO_LOCAL, the user’s entitled packages are downloaded to the client Windows system using a file copy. When the user launches a ThinApp package, the virtualized application runs locally on that system. Before the user’s first download and use of an entitled ThinApp package and to continue synchronizing the packages to the client Windows system, the client Windows system must join the same Active Directory domain to which the ThinApp packages’ network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and copy files from the network share. IMPORTANT For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in the Workspace Connector must be configured for account-based access. See Installing and Configuring Workspace.</td>
</tr>
<tr>
<td></td>
<td>HTTP_DOWNLOAD</td>
<td>With HTTP_DOWNLOAD, the user’s entitled packages are downloaded to the client Windows system using the HTTP protocol. When the user launches a ThinApp package, the virtualized application runs locally on that system. The Workspace client uses the user’s Workspace system account to authenticate to your Workspace Server to obtain the list of the user’s entitled packages to download. The share user account provided in the Connector Web interface for enabling account-based access to the ThinApp packages’ network share is the account used by the Workspace Connector to access the ThinApp packages from the repository. That share user account for the Connector needs read permission on the network share. The account that the user used to log in to the client Windows system and the user’s Workspace system account do not need to have any permissions on the network share. The client Windows system does not have to join the same domain to which the ThinApp packages’ network share is joined. This download method is typically slower than using the other modes. The benefit to this mode is that the client Windows system does not have to join the Active Directory domain to obtain and run the virtualized application. IMPORTANT For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in the Workspace Connector must be configured for account-based access. See Installing and Configuring Workspace.</td>
</tr>
<tr>
<td></td>
<td>RUN_FROM_SHARE</td>
<td>With RUN_FROM_SHARE, the virtualized application is streamed to the client Windows system from the network share when the user launches the ThinApp package. The RUN_FROM_SHARE option is best suited for Windows systems that will always have connectivity to the network share where the ThinApp packages reside, because the ThinApp packages are not present on the Windows system and the virtualized applications only run if the Windows system can connect to the network share. The client Windows system must join the same Active Directory domain to which the ThinApp packages' network share is joined. This download method is typically slower than using the other modes. The benefit to this mode is that the client Windows system does not have to join the Active Directory domain to obtain and run the virtualized application. IMPORTANT For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in the Workspace Connector must be configured for account-based access. See Installing and Configuring Workspace.</td>
</tr>
</tbody>
</table>
**Table 14-2. Keys for the /v Installer Command-Line Option (Continued)**

<table>
<thead>
<tr>
<th>Keys for the /v Option</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
</table>
| packages' network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and execute files on the network share. For all of the modes, the network share must have the appropriate file and sharing permissions configured. See *Installing and Configuring Workspace*. **IMPORTANT** When installing Workspace for Windows in floating View desktops, you best use the RUN_FROM_SHARE option to avoid copying the ThinApp packages into those stateless View desktop systems. When the client application is installed with one of these configurations, the user account that logs into the Windows system must have the appropriate file and sharing permissions on the network share to be able to obtain the ThinApp packages:  
  - The RUN_FROM_SHARE option  
  - The COPY_TO_LOCAL option, without also having the AUTO_TRY_HTTP option enabled and account-based access configured on the Workspace Connector  
  **NOTE** The INSTALL_MODE key replaces the deprecated DOWNLOAD key used in previous releases of the Workspace for Windows application. |
| POLLINGINTERVAL frequency | Enables you to set the frequency, measured in seconds, of synchronizations between the installed client application and your Workspace system to check for new ThinApp packages or entitlements. If unspecified, the default value of 300 seconds (5 minutes) applies. |
| ENABLE_AUTOUUPDATE 0 or 1 | Enables you to disable the automatic update check and download activity. If enabled, the installed Workspace for Windows application automatically checks if a newer application is available for downloading in your Workspace system. If there is a newer version available, the Workspace for Windows application automatically downloads and updates itself to the newer version. This option is enabled by default.  
  Set the value of this variable to 0 to disable automatic update. If unspecified, the default value of 1 applies.  
  **NOTE** An updated Workspace for Windows application is not installed if the logged-in user account does not have administrator privileges. |
| ENABLE_THINAP 0 or 1 | Enables you to disable syncing of ThinApp packages by the client application. Set the value of this variable to 0 to disable the syncing of ThinApp packages. If unspecified, the default value of 1 applies. |
Table 14-2. Keys for the /v Installer Command-Line Option (Continued)

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

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

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

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

You would create a script that invokes the following command:

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

where you replace the n.n.n-nnnnnnn portion of the file name to match the name of your downloaded Workspace for Windows installer.

Deprecated Command-Line Options

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

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

The /v DOWNLOAD option is superseded by the /v INSTALL_MODE option.

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

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

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

Typically, this deployment scenario is used for Windows systems that are View desktops. For a description of settings to use for non-persistent, also known as floating or stateless, View desktops, see “Reducing Resource Usage and Increasing Performance of Workspace for Windows In Non-Persistent View Desktops,” on page 56.

**Prerequisites**

- Verify that the Windows systems are running Windows operating systems that are supported for the version of the Workspace for Windows application you are installing. See the Workspace User Guide or the release notes that apply for that Workspace for Windows application.

- Verify that the Windows systems have installed browsers that are supported by the Windows application you are installing.

- If you want the ability to run a command to familiarize yourself with the available options before you create the deployment script, verify that you have a Windows system on which you can run that command. The command to list the options is only available on a Windows system. See “Command-Line Installer Options for Workspace for Windows,” on page 93.

**Procedure**

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

   One method for obtaining the executable file is to download it using the your Workspace system’s download page. If you have set up your Workspace system to provide the Windows application installer from the download page, you can download the executable file by opening the download page's URL in a browser. The download page’s URL is https://WorkspaceFQDN/download, where WorkspaceFQDN is the fully qualified domain name for your Workspace system.

2. Using the installer's command-line options, create a deployment script that fits the needs of your organization.

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

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

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

   where you replace the n.n.n-nnnnnnn portion of the file name to match that of your downloaded file.
3 Run the deployment script against the Windows systems.

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

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

**What to do next**

Verify that Workspace for Windows is properly installed on the Windows systems by trying some of the typical user tasks.
Workspace generates several reports, such as reports about users, resources, and audit events. You can view the reports in the Reports tab of the Workspace Admin Console.

You can use Workspace to generate several reports.

**Table 15-1. Workspace Report Types**

<table>
<thead>
<tr>
<th>Workspace Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recent Activity</td>
<td>This report lists what type of action user performed in Workspace for the past day, past month, or past 12 weeks. You can click <strong>Show Events</strong> to see the date, time, and user details for the activity.</td>
</tr>
<tr>
<td>Resource Usage</td>
<td>This report lists all your resources with respective details for each resource, such as number of users and licenses.</td>
</tr>
<tr>
<td>Resource Entitlements</td>
<td>This report lists the user entitlements for a resource you specify.</td>
</tr>
<tr>
<td>Group Membership</td>
<td>This report list the members of a group you specify.</td>
</tr>
<tr>
<td>Users</td>
<td>This report lists all your Workspace users, and provides details about each user, such as the user's email address, role, and group affiliations.</td>
</tr>
<tr>
<td>Concurrent Users</td>
<td>This report shows the number of user sessions that were opened at one time.</td>
</tr>
<tr>
<td>Audit events</td>
<td>This report lists the audit events related to a search you specify, such as user logins for the past 30 days. This feature is useful for troubleshooting purposes. See “Generate an Audit Event Report,” on page 101.</td>
</tr>
</tbody>
</table>

**Generate an Audit Event Report**

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

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

**Prerequisites**

Enable auditing. See “Overview of Workspace Administrative Settings,” on page 103.

**Procedure**

1. Log in to the Workspace Admin Console.
2. Select Reports > Audit events
3 Select audit event criteria.

<table>
<thead>
<tr>
<th>Audit Event Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>This text box allows you to narrow the search of audit events to those generated by a specific user.</td>
</tr>
<tr>
<td>Type</td>
<td>This drop-down list allows you to narrow the search of audit events to a specific audit event type. The drop-down list does not display all potential audit event types. The list only displays event types that have occurred in your Workspace deployment. Audit event types that are listed with all uppercase letters are access events, such as LOGIN and LAUNCH, which do not generate changes in the database. Other audit event types generate changes in the database.</td>
</tr>
<tr>
<td>Action</td>
<td>This drop-down list allows you to narrow your search to specific actions. The list displays events that make specific changes to the database. If you select an access event in the Type drop-down list, which signifies a non-action event, do not specify an action in the Action drop-down list.</td>
</tr>
<tr>
<td>Object</td>
<td>This text box allows you to narrow the search to a specific object. Examples of objects are groups, users, and devices. Objects are identified by a name or an ID number.</td>
</tr>
<tr>
<td>Date range</td>
<td>These text boxes allow you to narrow your search to a date range in the format of &quot;From ___ days ago to ___ days ago.&quot; The maximum date range is 30 days. For example, from 90 days ago to 60 days ago is a valid range while 90 days ago to 45 days ago is an invalid range because it exceeds the 30 day maximum.</td>
</tr>
</tbody>
</table>

4 Click **Show**.

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

**NOTE** At times when the auditing subsystem is restarting, the Audit Events page might display an error message and not render the report. If you see such an error message about not rendering the report, wait a few minutes and then try again.

5 For more information about an audit event, click **View Details** for that audit event.
After you install Workspace and perform the initial configuration, you can configure several administrative settings.

This chapter includes the following topics:

- “Overview of Workspace Administrative Settings,” on page 103
- “Customize Workspace Branding,” on page 104
- “Use hznAdminTool Commands to Make Changes to Your Workspace System,” on page 107

### Overview of Workspace Administrative Settings

You can configure several Workspace administrative settings.

You access the administrative settings using the Workspace Admin Console.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| VA Configuration      | Select **Settings > VA Configuration** to access the Configurator Web interface. The Configurator Web interface allows you to use a Web interface to edit the underlying Configurator virtual appliance. You can perform actions such as the following from the Configurator Web interface:  
  - View system information.  
  - Change the database from internal to external.  
  - Configure an SSL certificate for external access to Workspace.  
  - Enter a new license key.  
  - Change the admin user password for the service-va, configurator-va, and connector-va.  
  - View a list of the log file locations.  
  On the VA Configuration page, click **View Virtual Appliance System Configuration** to load the login page of the Configurator Web interface in your browser. |
<p>| Password Recovery     | Select <strong>Settings &gt; Password Recovery</strong> to configure the behavior of user password recovery. This setting allows you to configure the behavior of the Forgot password link on the user log in page. |
| User Stores           | Select <strong>Settings &gt; User Stores</strong> to configure user stores, which are required when you configure Workspace in a multi-forest Active Directory environment. See “Add a User Store for a Multi-Forest Active Directory Environment,” on page 16. |
| Network Ranges        | Select <strong>Settings &gt; Network Ranges</strong> to configure network ranges for your organization, so that you can associate IP address ranges with identity provider instances. See “Add or Edit a Network Range,” on page 21. |
| Authentication Methods| Select <strong>Settings &gt; Authentication Methods</strong> to configure the default authentication methods or to add authentication methods not supported by Workspace directly, but supported indirectly through third-party identity providers. See “Add or Edit a User Authentication Method,” on page 22. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Providers</td>
<td>Select Settings &gt; Identity Providers to edit an existing or to add a new identity provider instance, either a Connector instance or a third-party identity provider instance. The initial installation of Workspace includes a single Connector instance as the default identity provider deployment. Edit the initial Connector instance as necessary, such as by selecting authentication methods and adding network address ranges. Add additional identity provider instances to your Workspace deployment for high availability purposes. Also, when Workspace is deployed in a multi-forest Active Directory environment, add an additional identity provider instance for each user store you plan to add to your deployment. When the Identity Providers page lists more than one identity provider instance, you can edit the order of the instances. The order is important when IP addresses are assigned to multiple identity provider instances. See “Add and Configure an Identity Provider Instance,” on page 23 for details about adding or editing identity provider instances and about editing the order of identity provider instances.</td>
</tr>
<tr>
<td>Remote App Access</td>
<td>Select Settings &gt; Remote App Access to create clients or templates that enable applications to register with Workspace.</td>
</tr>
<tr>
<td>SAML Certificate</td>
<td>Select Settings &gt; SAML Certificate to view the SAML-signing certificate. If a Web application requires the use of SAML assertions to authenticate users, both Workspace and the Web application must have copies available locally of the same SAML-signing certificate.</td>
</tr>
<tr>
<td>Approvals</td>
<td>Select Settings &gt; Approvals to enable or disable license approval. Enabling license approval applies when you integrate your license-management system with Workspace.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Select Settings &gt; Auditing to enable or disable the collection of information for the audit events report, which is accessible on the Reports tab.</td>
</tr>
<tr>
<td>Citrix Published Application</td>
<td>Select Settings &gt; Citrix Published Application to edit the Workspace global application delivery settings for Citrix-based applications available in the Workspace catalog. See “Edit the Workspace Application Delivery Settings Globally for All Citrix-Based Applications,” on page 71. You can configure settings such as application streaming and application security. For instructions about editing the settings for a single Citrix-based application, see “Edit the Workspace Application Delivery Settings for a Single Citrix-Based Application,” on page 71.</td>
</tr>
<tr>
<td>Custom Branding</td>
<td>Select Settings &gt; Custom Branding to customize the branding on Workspace interfaces. See “Customize Workspace Branding,” on page 104.</td>
</tr>
</tbody>
</table>

**Customize Workspace Branding**

You can customize the logos, fonts, Web clips, and background that appear in various interfaces, such as the Workspace Admin Console, the user and administrator sign-in screens, the Web view of the apps portal and the Web view of the apps portal on mobile devices.

You can customize the branding used in the Web view of the apps portal and the Workspace Admin Console.

**Procedure**

1. Log in to the Workspace Admin Console.
2. Select Settings > Custom Branding.
3 Edit the settings in the form as appropriate.

### Table 16-1. Custom Branding Configuration

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Brand Names and Logos</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Logo</strong></td>
<td>The Logo option allows you to change the logo that appears in the user's App portal and the admin console. The maximum size of the logo image is 350 x 100 px. The format can be JPEG, PNG, or GIF. Click <strong>Change</strong> to upload a new image to replace the current logo. When you click <strong>Confirm</strong>, the change occurs immediately.</td>
</tr>
<tr>
<td><strong>Favicon</strong></td>
<td>The Favicon option allows you to change the favicon used in Web browsers. This option applies to both desktops and mobile devices. The maximum size of the favicon image is 16 x 16px. The format can be JPEG, PNG, GIF, or ICO. Click <strong>Change</strong> to upload a new image to replace the current favicon. You are prompted to confirm the change. If you click <strong>Confirm</strong>, the change occurs immediately.</td>
</tr>
<tr>
<td><strong>Company Name</strong></td>
<td>The Company Name option applies to both desktops and mobile devices. This option allows you to change the company name that appears in the Web browser screen title before the product name. Type a new company name over the existing one to change the name.</td>
</tr>
<tr>
<td><strong>Product Name</strong></td>
<td>The Product Name option applies to both desktops and mobile devices. This option allows you to change the name that appears in the Web browser screen title after the company name. Type a product company name over the existing one to change the name.</td>
</tr>
<tr>
<td><strong>Sign-In Screen</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Background Color</strong></td>
<td>The color that displays for the background of the sign-in screens. Type a new hexadecimal color code over the existing one to change the background color. Check <strong>Background Highlight</strong> to accent the background color. Check <strong>Background Pattern</strong> to set the predesigned triangle pattern in the background color.</td>
</tr>
<tr>
<td><strong>Masthead color</strong></td>
<td>The color that displays in the heading area in sign-in screens. Type a new hexadecimal color code over the existing one to change the masthead color. Check <strong>Masthead Pattern</strong> to set the predesigned triangle pattern in the masthead color.</td>
</tr>
<tr>
<td><strong>Image (Optional)</strong></td>
<td>To add an image to the background instead of a color, upload an image. The maximum size of the image is 1400 x 900 px. The format can be JPEG, PNG, or GIF.</td>
</tr>
<tr>
<td><strong>Logo</strong></td>
<td>Click <strong>Upload</strong> to upload a new logo to replace the current logo on the sign-in screens. When you click <strong>Confirm</strong>, the change occurs immediately. The maximum size of the logo image is 350 x 100 px. The format can be JPEG, PNG, or GIF.</td>
</tr>
<tr>
<td><strong>Portal (Web View)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Background Color</strong></td>
<td>The color that displays for the background of the Web portal screen. Type a new hexadecimal color code over the existing one to change the background color. To demonstrate how the background color will appear in the app portal, the background color changes in the app portal preview when you type in a new color code. However, if the <strong>include background image</strong> checkbox is selected, the background color might not be visible in the preview. Check <strong>Background Highlight</strong> to accent the background color. Check <strong>Background Pattern</strong> to set the predesigned triangle pattern in the background color.</td>
</tr>
</tbody>
</table>
### Table 16-1. Custom Branding Configuration (Continued)

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Icon Color</td>
<td>The color of the font that is used for resource names listed on the app portal screen. The name of the resource is located directly under the icon of the resource. Type a hexadecimal color code over the existing one to change the font color. The App Name text in the app portal preview changes when you type in a new color code to demonstrate how the text will appear in the app portal.</td>
</tr>
<tr>
<td>Lettering effect</td>
<td>Select the type of lettering to use for the text on the MyApps screen.</td>
</tr>
<tr>
<td>Image (Optional)</td>
<td>To add an image to the background on the app portal screen instead of a color, upload an image.</td>
</tr>
<tr>
<td><strong>Portal (Mobile and Tablet Views)</strong></td>
<td></td>
</tr>
<tr>
<td>Background Color</td>
<td>Type a hexadecimal color code over the existing one to change the background color of the My Apps screen viewed from a mobile device.</td>
</tr>
<tr>
<td>Title bar color</td>
<td>Type a hexadecimal color code over the existing one to change the title bar color viewed from a mobile device. Select Title Bar pattern to set the predesigned triangle pattern in the title bar color.</td>
</tr>
<tr>
<td>Title color</td>
<td>Type a hexadecimal color code over the existing one to change the font color used in the title bar heading.</td>
</tr>
<tr>
<td>Name color</td>
<td>The color of the font that is used for resource names listed on the app portal screen. The name of the resource is located directly under the icon of the resource. Type a hexadecimal color code over the existing one to change the font color of the application names.</td>
</tr>
<tr>
<td>Lettering effect</td>
<td>Select the type of lettering to use for the text on the MyApps screen.</td>
</tr>
<tr>
<td>Use the same values for both the Launcher and the Catalog</td>
<td>If you want to use the same branding design for the App Center screen view as used for the My Apps screen view on mobile devices, check this box. If you want to design the App Center screen differently, leave this box unchecked and configure the background, title bar color and title color for the App Center screen.</td>
</tr>
<tr>
<td><strong>First-Time User Tour</strong></td>
<td></td>
</tr>
<tr>
<td>First-Time User Tour</td>
<td>When first time users launch their app portal, they are shown a slideshow about the Workspace features. You can remove the checkmark to disable this feature.</td>
</tr>
<tr>
<td><strong>Mobile Devices</strong></td>
<td></td>
</tr>
<tr>
<td>Web Clip Icon</td>
<td>The Workspace icon, that appears when users save the App Portal URL as a bookmark to their mobile device home screens. This Web clip icon launches the Workspace App Portal. The maximum size of the image is 512 x 512 px. The format can be JPEG or PNG. Click Change to upload a new image to replace the current Web clip icon. You are prompted to confirm the change. If you click Confirm, the change occurs immediately.</td>
</tr>
<tr>
<td>Web Clip Title</td>
<td>The title that accompanies the Workspace Web clip icon. The tile must be less than 20 characters.</td>
</tr>
</tbody>
</table>

4 Click **Save**.

Custom branding updates to Workspace are applied across the Connectors within five minutes after you click **Save**.

**What to do next**

Check the appearance of the branding changes in the various interfaces.
Use hznAdminTool Commands to Make Changes to Your Workspace System

When you need to update settings related to the vCenter instance or SMTP system configured for your Workspace system, or to reset the password for the admin user that is used to log in to the Configurator Web interface, use the hznAdminTool command in the configurator-va virtual appliance interface.

Prerequisites

Verify that you can log in to the configurator-va virtual appliance interface, either directly using the vSphere client and the root account and password, or remotely using ssh and the sshuser account and password. The password for the root account is set during installation when you configure basic Workspace settings using the configurator-va virtual appliance interface. See Installing and Configuring Workspace.

Procedure

1. Log in to the configurator-va virtual machine using the configurator-va virtual appliance interface.

2. Enter the hzAdminTool with the appropriate option for the configuration setting that you want to update.

   To see a list of all editable properties for the hzAdminTool editproperty command, run hznAdminTool editproperty -- list. To set an editable property, run hznAdminTool editproperty -- set=property: value, where property is the property and value is the value you want to set.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hzAdminTool resetpasswd</td>
<td>Run this command to set the password for the default administrator account, named admin, that is typically used to log in to the Connector Web interface.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=vim_host:your_vCenter_host</td>
<td>Run this command to set the address for the vCenter instance associated with this Workspace system.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=vim_port:your_vCenter_port</td>
<td>Run this command to set the port number for the vCenter instance that is associated with this Workspace system.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=vim_username:username</td>
<td>Run this command to configure your Workspace system with the name used for the associated vCenter instance's administrator account.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=vim_password:password</td>
<td>Run this command to configure your Workspace system with the password used for the associated vCenter instance's administrator account.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=smtp_host:your_smtp_host</td>
<td>Run this command to set the address for the SMTP server associated with this Workspace system.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=smtp_port:your_smtp_port</td>
<td>Run this command to set the port for the associated SMTP server.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=smtp_username:username</td>
<td>Run this command to configure your Workspace system with the name used to access the SMTP server to send email messages. The Workspace file-sharing service sends email using the configured SMTP server when a user shares a folder or file with another user. Set this SMTP username when your SMTP server requires credentials to access it so that the file-sharing service can send emails.</td>
</tr>
<tr>
<td>hzAdminTool editproperty -- set=smtp_password:password</td>
<td>Run this command to configure your Workspace system with the password for the username that is used to access the SMTP server to send email messages.</td>
</tr>
</tbody>
</table>

3. Apply the changes to your Workspace system by running the configurator-tc restart command to restart the configurator-va's Tomcat server.

   After the Tomcat server restarts, your changes go into effect.
Troubleshooting Workspace for Administrators

You can troubleshoot issues that you or your Workspace users might experience after you install and configure Workspace.

This chapter includes the following topics:

- “Blank Screen Displays When Installing Update to Workspace for Windows,” on page 109
- “ThinApp Packages Fail to Launch from the User Portal,” on page 110
- “A User Login Attempt Results in a Timeout Error,” on page 113
- “Users Accessing Citrix-based Applications Receive an Encryption Error,” on page 113

Blank Screen Displays When Installing Update to Workspace for Windows

When you have the Workspace for Windows application already installed, and then you download a more recent version, and start to install it, a blank screen displays.

Problem

When you already have the Workspace for Windows application installed, and you start the installer for a more recent version, sometimes a blank screen displays and you cannot complete the installation.

When you look at the log files for the installer, you see lines at the end of file similar to the following lines:

```
20130918112739:INFO CBootstrapCmd::LuaUIShow: calling StartSequence('reboot_prompt')
20130918112739:INFO CHtmlUI::StartSequence: About to Run UI Sequence reboot_prompt 00000120 01F386F8 1
20130918112739:INFO CHtmlUI::StartSequence: Running UI Sequence reboot_prompt
20130918112739:ERROR CHtmlDialog::CallJScript: Failed to obtain required jscript ID; COM Error: -2147352570
```

Cause

This problem can occur if one or more registry key settings are incorrect. For descriptions of similar symptoms and other potential solution steps, see the VMware knowledge base article at http://kb.vmware.com/kb/1027986 and the Microsoft Knowledge Base article 831430 at http://support.microsoft.com/kb/831430.

Solution

1. Reboot the Windows system, and then try running the installer again.

   If rebooting the system does not resolve the problem, continue with the next step.
2 Re-register the jschrit.dll and vbscript.dll files.
   a Open a command prompt on the Windows system.
   b Run the following commands to re-register the necessary files and details.
      If the system is a 32-bit version of Windows, run these commands:
      regsvr32 jscript.dll
      regsvr32 vbscript.dll
      If the system is a 64-bit version of Windows, run these commands:
      cd C:\windows\syswow64
      regsvr32 C:\windows\system32\jscript.dll
      regsvr32 C:\windows\system32\vbscript.dll

3 Restart Windows.

ThinApp Packages Fail to Launch from the User Portal

When a user tries to launch a ThinApp package from the user portal, a browser message might appear that prompts the user to download and install Workspace for Windows even when the application is already installed and running.

Problem

After installing Workspace for Windows, when the user opens the user portal in a browser on that Windows system, logs in, and tries to launch a ThinApp package, a message might appear stating that Workspace for Windows must be installed on the system, and prevents the ThinApp package from starting. This message might appear even when the Workspace process is running on the Windows system. The Workspace for Windows client might report that all files are up to date.

Cause

This problem can occur for multiple reasons.
### Cause

<table>
<thead>
<tr>
<th>The Workspace for Windows browser plugin is not properly installed or it is not activated in the browser window for the browser in which the user is trying to launch the ThinApp package.</th>
</tr>
</thead>
</table>

Because installation of the Workspace for Windows application is required to run ThinApp packages on the Windows system, the user portal uses a browser plugin to verify whether the application is installed before launching the ThinApp package from the user portal. When the user clicks the icon for a ThinApp package in the user portal, the Workspace for Windows browser plugin checks to see if the application is installed before launching the package. If the browser plugin is not installed and active in the browser, the verification cannot happen, the message appears, and the package does not launch.

If there are browser windows open during the Workspace for Windows installation process, the browser plugin might not be properly installed for that browser. The browser plugin might become deactivated in the browser if the user disabled the plugin in the browser’s add-ons or plug-ins page.

<table>
<thead>
<tr>
<th>The custom protocol handler used to launch the ThinApp package from the browser has been disabled for the browser in which the user is trying to launch the ThinApp package.</th>
</tr>
</thead>
</table>

On the My Apps page in the user portal, ThinApp packages are represented using a link with a horizon:// protocol. When the Workspace for Windows client is installed, the installer registers a protocol handler for that horizon:// protocol. The protocol handler is an executable named HorizonThinAppLauncher.exe, and is registered as a handler by the registry entry HKEY_CLASSES_ROOT\horizon\shell\open\command. When the user tries to launch a ThinApp package from its icon in My Apps, this HorizonThinAppLauncher.exe application is launched.

If the user has disabled the use of all protocol handlers in the browser, or disabled the use of the handler for the horizon:// protocol, ThinApp packages will not launch using their icons in the My Apps page. Some browsers present a warning when protocol handlers are launched and give the user the option to select to execute the protocol handler. One way in which the user might have disabled the use of the horizon:// protocol handler is when the user clicked one of the ThinApp package icons for the first time, when the browser warning dialog appeared to ask for permission to run the protocol handler, the user selected No or a similar choice to prevent the launch, and also selected Remember my selection or a similar choice that prevents the launch for all such links. Because permission to run the protocol handler was not given and is remembered, none of the ThinApp packages launch from the My Apps page.

### Solution

1. **Verify the user has signed into the Workspace for Windows client with the user’s Workspace user account.**

   The user signs into the client using the Workspace icon in the Windows system tray.

2. **If this problem appears shortly after the application is installed on the system, close all open browser windows, reopen the browser, log in to the user portal, and try launching the ThinApp package.**
3 If the problem appears even after closing the open browser windows and reopening the browser, verify the browser plugin appears in the browser's list of plugins and is active.

<table>
<thead>
<tr>
<th>Browser</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>For Internet Explorer, a COM server is registered instead of a browser plugin or add-on. To test whether the COM server is installed, create a test HTML file with the following contents and open that file in Internet Explorer. The result tells whether the COM server is installed or not.</td>
</tr>
</tbody>
</table>
|                  | <html><script type="text/vbscript">On Error Resume Next<br>dim objName<br>objName = "HorizonAgentFinder.HorizonFinder"
|                  | dim obj<br>Set obj = CreateObject(objName)<br>document.write(objName & " is ")<br>if IsEmpty(obj) then<br>    document.write("not installed")
|                  | else<br>    document.write("installed")
|                  | end if<br></script><br></html>|
| Firefox          | Open Firefox’s Add-ons Manager by clicking **Tools > Add-ons**. On the Plugins page, verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate.                                          |
| Chrome           | Open Chrome’s content settings by opening the Settings page and clicking **Show advanced settings > Content settings**. Click **Disable individual plug-ins** to display the list of plugins. Verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate. |
| Safari for Windows| Open Safari's list of installed plugins by clicking **Help > Installed Plug-ins**. Verify that plugin is activated for Safari.                                                                                  |

4 Verify the registry entry **HKEY_CLASSES_ROOT\horizon\shell\open\command** exists and has a value that is a path that points to the location of the required protocol handler, named HorizonThinAppLauncher.exe, where Workspace for Windows was installed on the Windows system.

If the registry entry does not exist, or does not have a value that points to the location where Workspace for Windows was installed, uninstall Workspace for Windows and reinstall it.

5 If the registry entry exists and has a value that points to the location of the HorizonThinAppLauncher.exe executable, verify the executable exists at that location and has not been moved or deleted.

If the registry entry does not exist, or does not have a value that points to the location where Workspace for Windows was installed, uninstall Workspace for Windows and reinstall it.

6 If the registry entry exists and has a value that points to the location of the HorizonThinAppLauncher.exe executable, verify that the (Default) value for the registry entry **HKEY_CLASSES_ROOT\horizon** has a Data value of URL:horizon Protocol and that the URL Protocol value for the **HKEY_CLASSES_ROOT\horizon** entry exists.

If the Data value for the (Default) value of the **HKEY_CLASSES_ROOT\horizon** registry entry is not set to URL:horizon Protocol, update the Data value to set it to URL:horizon Protocol. If the URL Protocol value does not exist for the **HKEY_CLASSES_ROOT\horizon** entry, you can create it using a value name URL Protocol and no value data.
7 Determine if the user disabled the `horizon://` protocol for the browser, or if all protocol handlers are disabled in the browser, and if so, enable the protocol handler for the browser as appropriate for your organization's needs.

In most situations, the browsers rely on the settings in the registry for information about the protocol handlers available for that Windows system. For some browsers, when the user clicks a link that is associated with a protocol handler, a dialog prompt appears that asks the user a question such as *Do you want to allow this website to open a program on your computer?* or *This link needs to be opened with an application* or a similar statement about needing to launch an external application to handle the link. Typically, the dialog provides the user with the option of not launching the external application and to remember that choice for all links of that type. The steps to re-enable the ability to launch the application associated with the protocol handler are usually different depending on the browser type. Consult the documentation for the user's type of browser on how to enable protocol handlers for that browser type.

## A User Login Attempt Results in a Timeout Error

The gateway timeout limit might be insufficient for your deployment.

**Problem**

A user attempting to log in to Workspace receives a 502 Gateway timeout error.

**Cause**

A situation where user authentication takes longer than allowed by the default timeout limit. For example, the user exists in another Active Directory forest or domain that is not part of the identity provider instance's base DN.

**Solution**

1. Log in to the gateway-va virtual machine as `root`.
2. Open the `/opt/vmware/ngix/conf/proxy-timeout.conf` file.
   
   The file has two attributes. The default value for both attributes is `2m`, for two minutes.
3. Increase both values according to your Active Directory deployment structure.

**NOTE** When you upgrade Workspace, changes that were made to the `proxy-timeout.conf` file are carried forward to the update release.

## Users Accessing Citrix-based Applications Receive an Encryption Error

The XenApp ICA properties on the Workspace server must include the encryption property set to the same encryption level as configured on the XenApp servers in the farm, otherwise users cannot access their Xenapp application.

**Problem**

When a user connects to a Citrix application from Workspace, the following error message is displayed.

*You do not have the proper encryption level to access this Session*

**Cause**

Workspace does not set encryption levels. If the encryption level set on the XenApp server is set higher than the default setting used in the Citrix-Receiver users see this error.

You must set a higher encryption level in Workspace.
Solution

1. Log in to the Workspace Admin Console as an administrator.

2. Select Settings > Citrix Published Applications.

3. Edit the ICA Client Properties text box. To set the encryption level to 128, enter
   
   EncryptionLevelSession=EncRC5–128.

4. Edit the ICA Launch Properties text box. To set the encryption level to 128, enter as
   
   [EncRC5–128]
   
   DriverNameWin16=pdc128w.dll
   DriverNameWin32=pdc128n.dll
## Index

### A
- access events 101
- access policies
  - Auth Strength 27
  - Client Type 27
  - minimum authentication score 29, 30
  - network 29, 30
- Network 27
- relationship to identity providers 29, 32, 33
- TTL 27, 29, 30
- Web-application-specific 30, 32–34
- access policy set
  - applying 34
  - default 33, 34
  - portal 34
- access policy sets
  - creating 33
  - default 27, 29, 32
  - editing 32
  - portal 29, 33
- Web-application-specific 30, 32–34, 63, 65, 66
- Active Directory
  - deployment 23
  - domain 16, 17
  - forest 16, 17
  - multi-domain 15
  - multi-forest 15–17
  - single domain 15
- Add Identity Provider button 23
- additional user attributes 41
- admin user, reset password 107
- administrative settings 103
- administrator settings 103
- App Portal, URL 9
- application records
  - Web applications 65
  - Web applications from the cloud application catalog 63
- applications
  - mobile 50
  - Web 50, 59, 63, 65, 66
- audience 7
- Audit Event report 101
- authentication method 22, 23
- authentication methods, relationship to access policies 29, 32, 33

### B
- branding 104
- branding elements 103

### C
- catalog
  - managing 45
  - viewing resources 49
- Web applications 63
  - categories
    - applying 48
    - creating 47
    - deleting 48
    - removing 48
- Citrix deployment 69
- Citrix-based, delivery settings 71
- Citrix-based applications
  - categories 72
  - Client application folder 72
  - global application settings 71
  - hide disabled 71
  - individual application settings 71
- Citrix-Based Application Error 113
- cloud application catalog, Web applications 63
- company logo 103
- Configurator Web interface, access 103
- configure SAML protocol 60
- configure Web applications 60
- Connector 19, 23
- Connector Web interface, URL 9

### D
- desktop systems, configuring 93
- directory server groups 35

### E
- entitlements
  - ThinApp packages 81
  - Web applications 67
Group Membership report 101
  groups
    Active Directory 35, 36
    membership report 101
    modify membership rules 36
    searching for 51
    viewing information 39
  Workspace 35, 36
  guest users 9, 35

hzn-admin tool 9, 103
hznAdminTool command 107

ICA properties 71
identity provider
  Connector 19
  third-party 19, 27
identity providers
  relationship to access policies 29
  third-party 26
identity provider instances
  adding 103
  editing 103
  editing the order 103
  selection 19
identity provider selection, configuring 23
Independent Computing Architecture 71
installation options, Windows application 93
IP range 21

License, approval 103

mobile applications, resource type 46
modules
  Citrix Published Applications 69
  ThinApp Packages 76
  View 54
  viewing information 13
  Web Applications 59
multiple desktop systems, deploying the Windows application 99
multitenant Web applications 59

network range 21, 23
network ranges, relationship to access policies 29, 32, 33

Office 365
  convert to Workspace authentication 61
  example of Powershell cmdlet 61
  mapping attributes to AD user attributes 61
  powershell 61

password recovery, user 103
proof-of-concept 23

removing user access 43
reports 101
Resource Entitlement report 101
Resource Usage report 101
resources, categories 47, 48
roles 41

SAML
  certificate 27
  metadata 27
  third-party identity providers 26
SAML certificate 103
settings, administrative 103
single sign-on to Web applications 60
single sign-on, Office 365 61
sync client 16, 17
system information 13

ThinApp packages
  adding to the network share 91
  deleting 88
  deploying Workspace for Windows 99
  enabling for management 89
  entitling to users and groups 81
  HorizonThinAppCtrl.exe 80
  modifying the offline grace period 80
  offline grace period 79
  overview 76
  providing access 75
  setting options when installing the Windows application 93
  updating 83–85, 87
ThinApp download mode 76
ThinApp package AppID, obtaining 84
ThinApp Packages module 76
ThinApp streaming mode 76
third-party identity provider 23
timeout error 113
token 43
troubleshooting
  launching a ThinApp package 110
  updating Workspace for Windows 109

U
user password, recovery 103
user authentication method 22
user store 16, 17, 23, 103
users
  Active Directory 35
  adding to groups 36
  attributes 41
  removing access 43
  searching for 51
  updating the sync filter to Active Directory 43
  View Hosted Applications 54
  viewing information 41
  viewing entitlements to Citrix-based applications 70
  viewing entitlements to View desktop pools 54
  Workspace 35
Users report 101

V
View entitlements 55
View application pools 55
View Connection Server 55
View desktop pools, See View desktop pools
View desktop pools View desktop pools, providing access 53
View Hosted Application 55
View pods 55
virtual appliances, Workspace Workspace 9

W
Web applications
  adding 59, 63
  entitling 67
  multitenant 59
Web Applications module 59
Web application bundle 66
Windows application
  deploying to multiple systems 99
  installer options 93
Windows applications 46
Workspace, virtual appliances 9
workspace images 46
Workspace for Windows, troubleshooting 109
Workspace groups Workspace groups 35
Workspaces page 41
WS-Federation protocol 60