VMware Workspace Portal Administrator's Guide

Workspace Portal 2.1

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

EN-001537-01

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About the VMware Workspace Portal Administrator's Guide 1

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, 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, and RSA SecurID is helpful if you plan to implement those features.

Workspace Administrator's Guide Overview

Use the *VMware Workspace Portal Administrator's Guide* after you install Workspace.

To administer Workspace, you use the Workspace Admin Console.

The key task you perform from the Workspace Admin Console 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), DaaS desktops, 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 Setting Up Resources in VMware Workspace Portal Guide.

Introduction to Workspace for Administrators 2

Workspace provides you with a centralized 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 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 Administrative Services

You manage Workspace user groups and resource administration, authentication, sync setup, and the database connection from different Workspace administrative services.

- In the Workspace Admin Console interface, you set up the resource catalog and administer your users and groups, entitlements, and reports. You can view the User Engagement dashboard and the System Diagnostics dashboard to monitor users, resource usage, and the Workspace appliance health. You log in as the administrator user role assigned from Active Directory. The URL to directly log in to the admin console is https://*WorkspaceFQDN*/SAAS/admin.
- In the Connector Services Admin pages, you configure the directory, set up authbrokers, and administer other enterprise integrations such as virtual desktops and remote apps. This includes setting up the integration to the View connection server, ThinApp repository, and Citrix published applications resources. From these pages you can also check directory sync status and alerts. You log in as the Workspace administrator, using the user name **`admin`** and the admin password you created when you set up Workspace. A link to the Connector Services Admin pages can be found at https://*Workspace_FQDN* .com:8443.
- In the Appliance Configurator pages, you can manage the Workspace database, update certificates, enable Syslog, change the Workspace and system passwords and manage other infrastructure functions. You log in as the Workspace administrator, using the admin user name and the admin password you created when you set up Workspace. A link to the Appliance Configurator pages can be found at https://*Workspace_FQDN* .com:8443. You can also access the Appliance Configurator pages from the Worksapce Admin Console, Settings > VA Configuration page.

Workspace End 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 2-1. Workspace User Client Components

Workspace User Component	Description	Available Endpoints
Workspace App Portal	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 resources, includingView 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-published resources.	Web-based apps portal is available on all supported system endpoints, such as Windows systems, Mac systems, iOS devices, Android devices.
Workspace for Windows	When this program is installed on users' Windows systems, they can work with their virtualized Windows applications captured as ThinApp packages.	Windows systems

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

Using Workspace Admin Console Dashboards to Monitor Users, Resources, and Appliance Health 3

The Workspace Administration Console includes a User Engagement dashboard and a System Diagnostics dashboard to help you monitor users, resource usage, and the Workspace appliance health.

This chapter includes the following topics:

Track Users and Resources Used in Workspace

The User Engagement Dashboard displays information about users and resources. You can see who is signed in, which applications are being used, and how often the applications are being accessed. You can create reports to track users and group activities and resources usage.

The time that displays on the User Engagement Dashboard is based on the time zone set for the browser. The dashboard updates every one minute.

Procedure

- The header displays the number of unique users that logged in on that day and displays a timeline that shows the number of daily login events over a seven day period. The Users Logged in Today number is surrounded by a circle that displays the percentage of users that is signed in. The Logins sliding graph displays login events during the week. Point to one of the points in the graph to see the number of logins on that day.
- The Users and Groups section shows the number of user accounts and groups set up in Workspace. The most recent users that logged in are displayed. You can click **See Full Reports** to create an Audit Events report that shows the users who logged in over a range of days.
- The App popularity section displays a bar graph of the number of times that apps were launched, grouped by app type, over a seven day period. Point to a specific day to see a tool tip showing which type of apps were being used and how many were launched on that day. The list below the graph displays the number of times the specific apps were launched. Click the drop-down menu arrow on the right to select to view this information over a day, a week, a month or 12 weeks. You can click **See Full Reports** to create a Resource Usage report that shows app, resource type and number of users' activity over a range of time.
- The App adoption section displays a bar graph that shows the percentage of people who opened the apps they are entitled to. Point to the app to see the tool tip that shows the actual number of adoptions and entitlements.

- The Apps launched pie chart displays resources that have been launched as a percentage of the whole. Point to a specific section in the pie chart to see the actual number by type of resources. Click the drop-down menu arrow on the right to select to view this information over a day, a week, a month or 12 weeks.
- The Workspace Clients section shows the number of Windows Clients for Workspace that is being used.

What to do next

Click the Dashboard drop-down menu to see the System Diagnostics Dashboard.

Monitor Workspace System Information and Health

The Workspace System Diagnostics Dashboard displays a detailed overview of the health of the Workspace appliances in your environment and information about the Workspace services. You can see the overall health across the Workspace database server, workspace-va virtual machines, and the services available on each virtual machine.

From the System Diagnostics Dashboard you can select the workspace-va virtual machine that you want to monitor and see the status of the services on that virtual machine, including the version of Workspace that is installed. If the database or a virtual machine is having problems, the header bar displays the machine status in red. To see the problems, you can select the virtual machine that is displayed in red.

Procedure

- User Password Expiration. The expiration dates for the Workspace appliance root and remote log in passwords are displayed. If a password expires, go to the Settings page and select **VA Configurations**. Open the **System Security** page to change the password.
- Certificates. The certificate issuer, start date, and end date are displayed. To manage the certificate, go to the Settings page and select **VA Configurations**. Open the **Install Certificate** page.
- Configurator - Application Deployment Status. The Appliance Configurator services information is displayed. Web Server Status shows whether the Tomcat Server is running. The Web Application Status shows whether the Appliance Configurator page can be accessed. The appliance version shows the version of the Workspace appliance that is installed.
- Application Manager - Application Deployment Status. The Workspace Appliance connection status is displayed.
- Connector - Application Deployment Status. The Connector Services Admin connection status is displayed. When Connection successful is displayed, you can access the Connector Services Admin pages.
- Workspace FQDN. Shows the fully qualiied domain name that users enter to access their Workspace App portal. The Workspace FQDN points to the load balancer when a load balancer is being used.
- Application Manager - Integrated Components. The Workspace database connection, audit services, and analytics connection information is displayed.
- Connector - Integrated Components. Information about services that are managed from the Connector Services Admin pages is displayed. Information about ThinApp, View, and Citrix Published App resources is displayed.
- Modules. Displays resources that are enabled in Workspace. Click **Enabled** to go to the Connector Services Admin page for that resource.

Configuring Workspace User Authentication 4

Workspace user authentication requires the use of one or more identity provider instances. This can be the Workspace instance, which is the default, 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

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

The identity provider instances that you use with Workspace creates 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.

Workspace supports Active Directory password, Kerberos, and RSA SecurID user authentication methods. 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	Description
Password	Without any configuration, Workspace supports Active Directory password authentication. This method authenticates users directly against Active Directory.
Kerberos	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).
RSA SecurID	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.

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.

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.

IMPORTANT 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 15.

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.
- 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.

Option	Description
Edit an existing range	Click **Edit** for the range to edit.
Add a range	Click **+ Network Range** to add a new range.

4. Complete the form.

Form Item	Description
Name	Enter a name for the network range.
Description	Enter a description for the Network Range.
View Pods	The View Pods option only appears when the View module is enabled. Client Access URL Host. Enter the correct Horizon Client access URL for the network range. Client Access Port. Enter the correct Horizon Client access port number for the network range. See *Setting Up Resources in VMware Workspace Portal Guide*, Providing Access To View Desktop Pools and Application chapter.
IP Ranges	Edit or add IP ranges until all desired and no undesired IP addresses are included.

What to do next

- Associate each network range with an identity provider instance. See "Add and Configure an Identity Provider Instance," on page 15.

- Associate network ranges with access policy sets as appropriate. See Chapter 5, "Managing Access Policy Sets," on page 21.

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.

Workspace supports Active Directory password, Kerberos, and RSA SecurID user authentication methods. By adding a third-party identity provider that supports another authentication method, such as smart-card based authentication, you can enable Workspace to enforce that authentication method. See "Add and Configure an Identity Provider Instance," on page 15. See "Overview of Configuring Workspace to Use a Third-Party Identity Provider Instance," on page 17 for a complete list of tasks related to configuring Workspace to use a third-party identity provider instance.

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 22.

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.

Option	Description
Edit an Existing Authentication Method	Click **Edit** for the existing authentication method to configure.
Add a New Authentication Method	Click **+ Add Authentication Method** to add a new authentication method. For example, when adding a new third-party identity provider instance to your deployment.

4 Edit the authentication method settings.

Form Item	Description
Name	Type a name for this identity provider instance.

Form Item	Description
SAML Context	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.
Authentication Score	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.
Default Method	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.

5. Click **Save**.

What to do next

- Associate each authentication method with the appropriate identity provider instance. See "Add and Configure an Identity Provider Instance," on page 15.
- 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.

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 or a multi-domain forest.
  - 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 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 17 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 14.
- Use the admin console to configure network ranges. See "Add or Edit a Network Range," on page 13

Procedure

1. Log in to the Workspace Admin Console.
2. Select **Settings > Identity Providers**.
3. Click **Add Identity Provider**. This option prompts you for information that enables Workspace to register an existing third-party identity provider instance.
4. Edit the identity provider instance settings.

Form Item	Description
Type	Select **Manual** for third-party identity provider instances. NOTE Do not select Automatic unless VMware technical support instructs you to do so.
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. ■ Select Auto-discovery URL 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. ■ Select Meta-data XML and copy the XML metadata from the identity provider instance and paste it in the **Meta data 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.

5 Click **Save**.

6 If necessary, change the order of the identity provider instances.

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

a Click **Edit Order of Identity Providers**.

b Use the up and down arrows to move an identity provider instance to the appropriate location.

c Click **Save**.

What to do next

- If you are configuring Workspace for a multi-forest environment, inform your Workspace users of their respective domains and explain that when they log in, they must select a domain from the drop-down menu. Inform them that they can check the **Remember this setting** check box to prevent the prompt from being repeated at each login.
- If you added a third-party identity provider instance, copy and save the Workspace information required to configure a third-party identity provider instance. See "Obtain the Workspace SAML Information Required to Configure a Third-Party Identity Provider Instance," on page 18.

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 14

4 To edit an authentication methods select 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 14.

Configuration

When adding an identity provider instance, perform the following steps specific to third-party identity providers. See "Add and Configure an Identity Provider Instance," on page 15.

1 In the admin console, Settings > Identity Providers page, 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 18.

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.

Procedure

1. Log in to the admin console.
2. Select **Settings > SAML Certificate**
3. Copy and save the SAML signing certificate that displays in Workspace.
   a. Copy the certificate information that is in the Signing Certificate section.
   b. Save the certificate information to a text file for later use when you configure the third-party identity provider instance.
4. 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 displayed 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.

5. 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.

NameID Format	User Mapping
urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress	The NameID value in the SAML assertion is mapped to the email address attribute in Workspace.
urn:oasis:names:tc:SAML:2.0nameid-format:unspecified	The NameID value in the SAML assertion is mapped to the username attribute in Workspace.

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 to change 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 5, "Managing Access Policy Sets," on page 21.

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 24 for instructions.

Example Default Access Policy Set

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

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 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.
   - 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 5

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 19. 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

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 5, “Managing Access Policy Sets,” on page 21.

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 19. 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 19.

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 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 5, "Managing Access Policy Sets," on page 21.

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

- "Editing the Default Access Policy Set," on page 19.
- "Managing Web-Application-Specific Access Policy Sets," on page 22.

Prerequisites

- Configure the appropriate identity providers for your deployment. See "Add and Configure an Identity Provider Instance," on page 15.
- Configure the appropriate network ranges for your Workspace deployment. See "Add or Edit a Network Range," on page 13.
- Configure the appropriate authentication methods for your deployment. See "Add or Edit a User Authentication Method," on page 14.

Procedure

1. Log in to the Workspace Admin Console.
2. Select **Policies > Access Policy Sets**.
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.

Option	Description
Edit an Existing Policy	a Click the name of the policy to configure. b Change policy settings as appropriate. c Click **Apply**.
Remove an Existing Policy	a Click the name of the policy to remove. b Click **Remove**.
Add a New Policy	a Click **+ Access Policy** to add a new policy. b Configure policy settings as appropriate. c Click **Add**.

7 Click **Save**.

The edited access policy set takes effect immediately.

What to do next

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

Add a Web-Application-Specific Access Policy Set

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

For an overview of access policy sets, see Chapter 5, "Managing Access Policy Sets," on page 21. For information and examples of Web-application-specific access policy sets, see "Managing Web-Application-Specific Access Policy Sets," on page 22.

Prerequisites

- Configure the appropriate identity providers for your deployment. See "Add and Configure an Identity Provider Instance," on page 15.
- Configure the appropriate network ranges for your Workspace deployment. See "Add or Edit a Network Range," on page 13.
- Configure the appropriate authentication methods for your deployment. See "Add or Edit a User Authentication Method," on page 14.
- 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.

6 Configure policy settings as appropriate.

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

7 Click **Add**.

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

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

What to do next

Apply the policy set to one or more Web applications.

Apply a Web-Application-Specific Access Policy Set

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

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 25

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 6

You can manage and monitor users and groups, which includes the users and groups imported from Active Directory 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 27
- "Manage Workspace Groups," on page 28
- "Manage Workspace Users," on page 31
- "Changing User and Groups that Sync from Active Directory," on page 34

Workspace User and Group Types

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

Users

Workspace users are users imported from Active Directory. 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.

Group Type	Description
Directory Server Groups	You use the Connector Services Admin Directory Sync, Select Groups page to import groups from Active Directory to Workspace. In the admin console, a lock icon next to a group name indicates that the group is a directory server group. You cannot use Workspace to edit or delete directory server groups. Imported directory server groups are updated in Workspace according to your directory server synchronization schedule.
Workspace Groups	You use the Workspace Admin Console to create Workspace groups, which are groups you customize to best suit the use of Workspace within your enterprise. You can create Workspace groups by adding a combination of users and groups. The groups you add can be either preexisting Workspace groups, or groups imported from your directory server. In the admin console, a check box next to a group name indicates that the group is a Workspace group. You can use Workspace to delete a Workspace group or to modify the users in the group.

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

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

- To create a Workspace group, select **Users & Groups > Groups**, click **Create Group**, and provide the group name and description.
- 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 a Active Directory group and that you cannot use Workspace to edit or delete the group.

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 be a member of both groups.

Procedure

1. Log in to the Workspace Admin Console.
2. Select **User & Groups > Groups**.
   - 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.

Option	Action
Any of the following	Grants group membership when any of the conditions for group membership are met. This option works like an OR condition. For example, if you select **Any of the following** for the rules Group Is Sales and Group Is Marketing, sales and marketing staff are granted membership to this group.
All of the following	Grants group membership when all of the conditions for group membership are met. This works like an AND condition. For example, if you select **All of the following** for the rules Group Is Sales and Email Starts With 'western_region', only sales staff in the western region are granted membership to this group. Sales staff in other regions are not granted membership.

7 Configure one or more rules for your Workspace group.

You can nest rules.

Option	Action
Group	■ Select **Is** 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 **Is Not** 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.
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.

Option	Action
Any of the following	Group membership to be granted when any of the conditions for group membership are met for this rule. This is a way to nest rules. For example, you can create a rule that says All of the following: Group Is Sales; Group is California. For Group is California, Any of the following: Phone Starts With 415; Phone Starts With 510. The group member must belong to your California sales staff and have a phone number that starts with either 415 or 510.
All of the following	All of the conditions to be met for this rule. This is a way to nest rules. For example, you can create a rule that says Any of the following: Group Is Managers; Group is Customer Service. For Group is Customer Service, all of the following: Email Starts With cs_; Phone Starts With 555. The group members can be either managers or customer service representatives, but customer service representatives must have an email that starts with cs_ and a phone number that starts with 555.

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

Type of Information	Description
Number Users	The number members in the group.
Number Applications	The number of resources entitled to the group as a whole.
User Store	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.

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.

4 Click the tab that corresponds to the information you want to view.

Option	Description
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 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 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 the users imported from Active Directory using the Workspace Admin Console.

Managing users in Workspace includes tasks such as entitling 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 the Workspace admin console. Individuals assigned the administrator role can still access 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.

Web Interface	Required Role	URL Example
Workspace Admin Console	Administrator	https://*WorkspaceFQDN*/admin
Workspace App Portal	User	https://*WorkspaceFQDN*/web

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.

Option	Description
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.

Changing User and Groups that Sync from Active Directory

During the Workspace setup, you entered the information to connect to the Active Directory server; selected Active Directory user attributes and filters to specify which users sync in the Workspace Directory, and selected which Active Directory groups to add. You can change these settings from the Connector Services Admin, Directory Sync pages.

Changes that are made and saved on these pages are automatically updated in Workspace after the next directory sync. See "Change Settings That Select Users for Workspace," on page 34

Changing the Map User Attributes Page

The Map User Attributes page displays the mapping between the attributes in Active Directory and the attributes in Workspace. If you want to include additional information from Active Directory about users, you can add the user attributes to the Map User Attributes page.

One of the default user attributes mapped in the Map User Attributes page is the attribute to disable an account. The UserAccountControl attribute is mapped to the Workspace disabled attribute. Users are disabled in the Workspace directory when the Active Directory UserAccountControl attribute is flagged UF_Account_Disable.

When an account is disabled, users cannot log in to access their applications and resources. The resources that users were entitled to are not removed from the account so that when the flag is removed from the account users can log in and access their entitled resources

Change Settings That Select Users for Workspace

During the Workspace setup, you specify the Active Directory, user attributes, and filters to select those Active Directory users that you want to use with Workspace. You can update these settings using from the Connector Services Admin pages.

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, groups to include.

Procedure

1 Log in to the Connector Services Admin using the Workspace administrator password.

2 Perform the appropriate action.

Option	Action
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 **Map User Attributes**. b Make your changes. c Click **Save**.
Create filters to exclude specific Active Directory user syncing to Workspace and update Active Directory groups that 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 **Save**. d Make your changes on the Select Groups page as necessary, and click **Save**. e Click **Push to Workspace**. f Click **Save and Continue**.

Managing the Workspace Catalog 7

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.

To display your catalog click 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. See the *Setting Up Resources in VMware Workspace Portal Guide* for information about setting up resources.

Resource	How to See the Resource in Your Catalog
Web application	Enable the Web Applications module. Use the admin console to select the **Web Applications** application type on the Catalog page.
Virtualized Windows application captured as a ThinApp package	Sync ThinApp packages to your catalog from the Connector Services Admin, Packaged Apps - ThinApp page. Use the admin console to select the **ThinApp Packages** application type on the Catalog page.
View Desktop Pool	Sync View Pools to your catalog from the Connector Services Admin, View Pools page. Use the admin console to select the **View Desktop Pools** application type on the Catalog page.
View Hosted Applications	Sync View Hosted Applications to your catalog from the Connector Services Admin, View Pools page. Use the admin console to select the **View Hosted Application** as the application type on the Catalog page.
Citrix-based application	Sync Citrix-based applications to your catalog from the Connector Services Admin, Published Apps - Citrix page. Use the admin console to select the **Citrix Published Applications** application type on the Catalog page.

This chapter includes the following topics:

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.

For information, requirements, installation and configuration of these resources, see the *Setting Up Resources in VMware Workspace Portal Guide*.

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 40.

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.
3. Configure Workspace to integrate with the packages on the network share.

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.

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.

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 entitling users to desktops. See the VMware View documentation.

2 Integrate your Workspace deployment with VMware View.

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.

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 38.

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**.

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

Access 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 7, "Managing the Workspace Catalog," on page 35.
- To view resources by category, create and apply categories. See "Overview of Using Resource Categories," on page 37.

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.

Option	Description
Any Application Type	Lists all of the resources in your catalog.
Web Applications	Lists only Web applications in your catalog. Web applications include SaaS applications and Web applications managed internally by your enterprise.
ThinApp Packages	Lists only Windows applications captured as ThinApp packages. ThinApp packages appear in your catalog if you add ThinApp packages to your deployment while configuring Workspace prior to accessing the admin console.
View Desktop Pools	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.
View Hosted Applications	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.
Citrix Published Applications	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.

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 to your catalog directly using the Catalog page of the Workspace admin console.

See the Setting Up Resources in VMware Workspace Portal Guide, Providing Access to Web Applications chapter for detailed instructions about adding a Web application to your catalog.

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.

Link Name	Resource Type	Description
Web Application ...from the cloud application catalog	Web application	Workspace includes access to several default Web applications, available in the cloud application catalog, that you can add to your catalog as resources.
Web Application ... create a new one	Web application	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.
Web Application ... import a ZIP or JAR file	Web application	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.

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

Search for Users, Groups, or Catalog Resources 8

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.

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

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

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

NOTE Up to 100 results are returned for each record type. For example, if the string appears in the records of more than 100 users, a maximum of 100 results is listed on the **Users** tab. You cannot change this maximum.

Viewing Workspace Reports 9

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 9-1. Workspace Report Types

Workspace Report	Description
Recent Activity	This report lists what type of action user performed in Workspace for the past day, past month, or past 12 weeks. You can click **Show Events** to see the date, time, and user details for the activity.
Resource Usage	This report lists of all your resources with respective details for each resource, such as number of users and licenses.
Resource Entitlements	This report lists the user entitlements for a resource you specify.
Group Membership	This report list the members of a group you specify.
Users	This report lists all your Workspace users, and provides details about each user, such as the user's email address, role, and group affiliations.
Concurrent Users	This report shows the number of user sessions that were opened at one time.
Audit events	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 43.

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 45.

Procedure

1 Log in to the Workspace Admin Console.

2 Select **Reports > Audit events**

3 Select audit event criteria.

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

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.

Configuring Workspace Settings for Administrators 10

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

You can configure several Workspace administrative settings.

You access the administrative settings using the Workspace Admin Console.

Setting	Description
VA Configuration	Select **Settings > VA Configuration** to go to the Appliance Configurator pages. On these pages you can update and change settings for the Workspace database, SSL certificates, and external syslog server, change Workspace and system passwords, and view log files.
License	Select **Settings > License** to enter your Workspace license key.
SMTP	Select **Settings > SMTP** to enter the SMTP settings.
Password Recovery	Select **Settings > Password Recovery** to configure the behavior of the Forgot password link that displays on the user log in page when they click Forgot password.
User Stores	Select **Settings > User Stores** to configure user stores for multi-forest Active Directory deployments without trust relationships. See the *Installing and Configuring Workspace* guide, Managing Active Directory Connections with Workspace chapter.
Network Ranges	Select **Settings > Network Ranges** 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 13.
Authentication Methods	Select **Settings > Authentication Methods** 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 14.

Setting	Description
Identity Providers	Select **Settings > Identity Providers** to edit an existing or to add a new identity provider instance. The initial installation of Workspace includes a default identity provider deployment. Edit the Workspace default identity provider configuration as necessary to select authentication methods and add network address ranges. Add additional identity provider instances to your Workspace deployment for high availability purposes. 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 15 for details about adding or editing identity provider instances and about editing the order of identity provider instances.
Remote App Access	Select **Settings > Remote App Access** to create clients or templates that enable applications to register with Workspace.
SAML Certificate	Select **Settings > SAML Certificate** to view the SAML-signing certificate. If a Web application requires the use of SAML assertions to authenticate users, both Workspace and the Web application must have copies available locally of the same SAML-signing certificate.
Approvals	Select **Settings > Approvals** to enable or disable license approval. Enabling license approval applies when you integrate your license-management system with Workspace.
Auditing	Select **Settings > Auditing** to enable or disable the collection of information for the audit events report, which is accessible on the **Reports** tab.
Citrix Published Application	Select **Settings > Citrix Published Application** to edit the Workspace global application delivery settings for Citrix-based applications available in the Workspace catalog. For instructions about editing the settings for a single Citrix-based application, see *Setting Up Resources in VMware Workspace Portal Guide*.
Custom Branding	Select **Settings > Custom Branding** to customize the branding on Workspace interfaces. See "Customize Workspace Branding," on page 46.

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 10-1. Custom Branding Configuration

Form Item	Description
	Brand Names and Logos
Logo	The Logo option allows you to change the logo that appears in the user's App portal and the admin console. The minimum image size recommened to upload is 350 x 100 px. If you upload images that are larger than 350 x 100 px, the image is scaled to fit 350 x 100 px size. The format can be JPEG, PNG, or GIF. Click **Change** to upload a new image to replace the current logo. When you click **Confirm**, the change occurs immediately.

Table 10-1. Custom Branding Configuration (Continued)

Form Item	Description
Favicon	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 **Change** to upload a new image to replace the current favicon. You are prompted to confirm the change. If you click **Confirm**, the change occurs immediately.
Company Name	The Company Name option applies to both desktops and mobile devices. This option allows you to change the company name that appears in the Web browser screen title before the product name. Type a new company name over the existing one to change the name.
Product Name	The Product Name option applies to both desktops and mobile devices. This option allows you to change the name that appears in the Web browser screen title after the company name. Type a product company name over the existing one to change the name.
	Sign-In Screen
Background Color	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 **Background Highlight** to accent the background color. Check **Background Pattern** to set the predesigned triangle pattern in the background color.
Masthead color	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 **Masthead Pattern** to set the predesigned triangle pattern in the masthead color.
Image (Optional)	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.
Logo	Click **Upload** to upload a new logo to replace the current logo on the sign-in screens. When you click **Confirm**, the change occurs immediately. The minimum image size recommened to upload is 350 x 100 px. If you upload images that are larger than 350 x 100 px, the image is scaled to fit 350 x 100 px. The format can be JPEG, PNG, or GIF.
	Portal (Web View)
Background Color	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 **include background image** checkbox is selected, the background color might not be visible in the preview. Check **Background Highlight** to accent the background color. Check **Background Pattern** to set the predesigned triangle pattern in the background color.
Name and Icon Color	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.
Lettering effect	Select the type of lettering to use for the text on the MyApps screen.
Image (Optional)	To add an image to the background on the app portal screen instead of a color, upload an image.
	Portal (Mobile and Tablet Views)
Background Color	Type a hexadecimal color code over the existing one to change the background color of the My Apps screen viewed from a mobile device.

Table 10-1. Custom Branding Configuration (Continued)

Form Item	Description
Title bar color	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.
Title color	Type a hexadecimal color code over the existing one to change the font color used in the title bar heading.
Name color	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.
Lettering effect	Select the type of lettering to use for the text on the MyApps screen.
Use the same values for both the Launcher and the Catalog	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.
	First-Time User Tour
First-Time User Tour	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.
	Mobile Devices
Web Clip Icon	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.
Web Clip Title	The title that accompanies the Workspace Web clip icon. The tile must be less than 20 characters.

4 Click **Save**.

Custom branding updates to Workspace are applied within five minutes after you click Save.

What to do next

Check the appearance of the branding changes in the various interfaces.

Index