# VMware Identity Manager Administration

SEP 2017
VMware AirWatch 9.2
VMware Identity Manager 3.0

vmware®

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

https://docs.vmware.com/

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 VMware Identity Manager Administration

VMware Identity Manager Administration provides information and instructions about using and maintaining the VMware Identity Manager services. With VMware Identity Manager™ you can set up and manage authentication methods and access policies, 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, Citrix-based applications, and Horizon desktop and application pools.

## Intended Audience

This information is intended for anyone who wants to configure and administer VMware Identity Manager. 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 Horizon® 7, Horizon® Cloud, and Citrix application virtualization, and authentication methods, such as RSA SecurID, is helpful if you plan to implement those features.

# Working in VMware Identity Manager Administration Console

1

The VMware Identity Manager™ administration console provides you with a centralized management console with which you can manage users and groups, add resources to the catalog, manage entitlements to resources in the catalog, configure AirWatch integration, and set up and manage authentication and access policies.

The key tasks you perform from the administration console is manage user authentication and access policies and 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.

End users can sign in to their VMware Workspace™ ONE™ portal from their desktop or mobile devices to access work resources, including desktops, browsers, shared corporate documents, and various types of applications that you entitle for their use.

This section includes the following topics:



## Navigating in the Administration Console

The tasks in the administration console are organized by tabs.

| Tab | Description |
|---|---|
| Dashboard | The User Engagement dashboard can be used to monitor user and resource use. This dashboard displays information about who signed in, which applications are being used, and how often they are being used.<br>The System Diagnostics dashboard displays a detailed overview of the health of the service in your environment and other information about the services.<br>You can create reports to track users' and groups' activities, resource and device use, and audit events by user. |
| Users and Groups | In the Users and Groups tab, you can manage and monitor users and groups imported from your Active Directory or LDAP directory, create local users and groups, and entitle the users and groups to resources. You can configure the password policy for local users. |
| Catalog | The Catalog is the repository for all the resources that you can entitle to users. In the Catalog tab, you can add Web applications, ThinApp packages, View Pools and application, Horizon Air desktops, and Citrix-based applications. You can create a new application, group applications into categories, and access information about each resource. On the Catalog Settings page, you can download SAML certificates, manage resource configurations, and customize the appearance of the user portal. |

| Tab | Description |
|---|---|
| Identity & Access Management | In the Identity & Access Management tab, you can set up the connector service, configure AirWatch integration, set up authentication methods, and apply custom branding to the sign-in page and admin console. You can manage directory settings, identity providers, and access policies. You can also configure third-party identity providers. |
| Appliance Settings | In the Appliance Settings tab, you can manage the configuration of the appliance, including configuring SSL certificates for the appliance, change the services admin and system passwords, and manage other infrastructure functions. You can also update the license settings and configure SMTP settings. |

## Supported Web Browsers to Access the Administration Console

The VMware Identity Manager administration console is a Web-based application you use to manage your tenant. You can access the administration console from the following browsers.

- Internet Explorer 11 for Windows systems
- Google Chrome 42.0 or later for Windows and Mac systems
- Mozilla Firefox 40 or later for Windows and Mac systems
- Safari 6.2.8 and later for Mac systems

**Note** In Internet Explorer 11, JavaScript must be enabled and cookies allowed to authenticate through VMware Identity Manager.

## VMware Identity Manager Workspace ONE for End Users

End users can access entitled resources from their Workspace ONE portal. Workspace ONE is the default interface used when users access and use their entitled resources with a browser.

When AirWatch is integrated with VMware Identity Manager, end users cam see all apps that they are entitled to. Native applications that are internally developed or publically available in app stores can be made available to your end users form the Workspace ONE portal.

# Identity and Access Management Settings Overview

From the Identity and Access Management tab in the administration console, you can set up and manage the authentication methods, access policies, directory service, and customize the end-user portal and administration console branding.

The following is a description of the setup settings in the Identity and Access Management tab.

## Table 1-1. Identity and Access Management Set up Settings

| Setting | Description |
|---|---|
| Setup > Connectors | The Connectors page lists the connectors that are deployed inside your enterprise network. The connector is used to sync user and group data between your enterprise directory and the service. When the connector is used as the identity provider, it authenticates users to the service.<br>When you associate a directory with a connector instance, the connector creates a partition for the associated directory called a worker. A connector instance can have multiple workers associated with it. Each worker acts as an identity provider. You define and configure authentication methods per worker.<br>The connector syncs user and group data between your enterprise directory and the service through one or more workers.<br>■ In the Worker column, select a worker to view the details about the connector and navigate to the Auth Adapters page to see the status of the available authentication methods. For information about authentication, see Chapter 5 Configuring User Authentication in VMware Identity Manager.<br>■ In the Identity Provider column, select the IdP to view, edit, or disable. See Add and Configure an Identity Provider Instance.<br>■ In the Associated Directory column, access the directory associated with this worker.<br>Before you can add a new connector, click Add Connector to generate an activation code. You paste this activation code in the Setup wizard to establish communication with the connector. |
| Setup > Custom Branding | In the Custom Branding page, you can customize the appearance of the administration console header and sign-in screen. See Customize Branding in VMware Identity Manager Service.<br>To customize the end user Web portal, mobile and tablet views, go to Catalog > Settings > User Portal Branding. See Customize Branding for the User Portal. |
| Setup > User Attributes | The User Attributes page lists the default user attributes that sync in the directory. You can add other attributes that you can map to Active Directory attributes. See the Directory Integration with VMware Identity Manager guide. |
| Setup > Network Ranges | This page lists the network ranges that you added. You configure a network range to allow users access through those IP addresses. You can add additional network ranges and you can edit existing ranges. See Add or Edit a Network Range. |
| Setup > Auto Discovery | When VMware Identity Manager and AirWatch are integrated, you can integrate the Windows Auto-Discovery service that you deployed in your AirWatch configuration with the VMware Identity Manager service. For more details about setting up auto discovery in AirWatch in on-premises deployments, see the AirWatch documentation VMware AirWatch Windows Autodiscovery Service Installation Guide available from the AirWatch Web site, http://air-watch.com<br>Register your email domain to use the auto-discovery service to make it easier for users to access their apps portal using Workspace ONE. End users can enter their email addresses instead of the organization's URL when they access their apps portal through Workspace ONE.<br>See the Guide to Deploying VMware Workspace ONE for more information about auto discovery. |
| Setup > AirWatch | On this page, you can set up integration with AirWatch. After integration is set up and saved, you can enable the unified catalog to merge applications set up in the AirWatch catalog to the unified catalog; enable compliance check to verify that managed devices adhere to AirWatch compliance policies, and enable user password authentication through the AirWatch Cloud Connector (ACC). See the Guide to Deploying VMware Workspace ONE. |

**Table 1-1. Identity and Access Management Set up Settings (Continued)**

| Setting | Description |
|---|---|
| Setup > Preferences | The Preferences page displays features that the admin can enable. This includes the following preferences.<br>■ Show the System Domain on Login Page can be enabled.<br>■ Persistent cookies can be enabled from this page. See Enable Persistent Cookie.<br>■ Enable Hide Domain Drop-Down Menu, when you do not want to require users to select their domain before they log in.<br>■ Enable the unique identifier option to display the identifier-based login pages. See Chapter 4 Managing the User Login Experience |
| Terms of Use | On this page, you can set up Workspace ONE terms of use and ensure that end users accept this terms of use before using the Workspace ONE portal. |

The following is a description of the settings used to manage the services in the Identity and Access Management tab.

**Table 1-2. Identity and Access Management Manage Settings**

| Setting | Description |
|---|---|
| Manage > Directories | The Directories page lists directories that you created. You create one or more directories and then sync those directories with your enterprise directory deployment. On this page, you can see the number of groups and users that are synced to the directory and the last sync time. You can click Sync Now, to start the directory sync.<br>See See the Directory Integration with VMware Identity Manager guide.<br>When you click a directory name, you can edit the sync settings, navigate the Identity Providers page, and view the sync log.<br>From the directories sync settings page, you can schedule the sync frequency, see the list of domains associated with this directory, change the mapped attributes list, update the user and groups list that syncs, and set the safeguard targets. |
| Manage > Identity Providers | The Identity Providers page lists the identity providers that you configured. The connector is the initial identity provider. You can add third-party identity provider instances or have a combination of both. The VMware Identity Manager Built-in identity provider can be configured for authentication.<br>See Add and Configure an Identity Provider Instance. |
| Manage > Password Recovery Assistant | On the Password Recovery Assistant page, you can change the default behavior when "Forgot password" is clicked on the sign-in screen by the end user. |
| Authentication Methods | The Authentication Methods page is used to configure authentication methods that can be associated with built-in identity providers. After you configure the authentication methods on this page, you associate the authentication method in the built-in identity provider page. |
| Manage > Policies | The Policies page lists the default access policy and any other Web application access policies you created. Policies are a set of rules that specify criteria that must be met for users to access their My Apps portal or to launch Web applications that are enabled for them. You can edit the default policy and if Web applications are added to the catalog, you can add new policies to manage access to these Web applications. See Chapter 6 Managing Access Policies. |

# Using Local Directories

2

A local directory is one of the types of directories that you can create in the VMware Identity Manager service. A local directory enables you to provision local users in the service and provide them access to specific applications, without having to add them to your enterprise directory. A local directory is not connected to an enterprise directory and users and groups are not synced from an enterprise directory. Instead, you create local users directly in the local directory.

A default local directory, named System Directory, is available in the service. You can also create multiple new local directories.

## System Directory

The System Directory is a local directory that is automatically created in the service when it is first set up. This directory has the domain System Domain. You cannot change the name or domain of the System Directory, or add new domains to it. Nor can you delete the System Directory or the System Domain.

The local administrator user that is created when you first set up the VMware Identity Manager appliance is created in the System Domain of the System Directory.

You can add other users to the System Directory. The System Directory is typically used to set up a few local administrator users to manage the service. To provision end users and additional administrators and entitle them to applications, creating a new local directory is recommended.

## Local Directories

You can create multiple local directories. Each local directory can have one or more domains. When you create a local user, you specify the directory and domain for the user.

You can also select attributes for all the users in a local directory. User attributes such as userName, lastName, and firstName are specified at the global level in the VMware Identity Manager service. A default list of attributes is available and you can add custom attributes. Global user attributes apply to all directories in the service, including local directories. At the local directory level, you can select which attributes are required for the directory. This allows you to have a custom set of attributes for different local directories. Note that userName, lastName, firstName, and email are always required for local directories.

**Note** The ability to customize user attributes at the directory level is only available for local directories, not for Active Directory or LDAP directories.

Creating local directories is useful in scenarios such as the following.

- You can create a local directory for a specific type of user that is not part of your enterprise directory. For example, you can create a local directory for partners, who are not usually part of your enterprise directory, and provide them access to only the specific applications they need.
- You can create multiple local directories if you want different user attributes or authentication methods for different sets of users. For example, you can create a local directory for distributors that has user attributes such as region and market size, and another local directory for suppliers that has user attributes such as product category and supplier type.

## Identity Provider for System Directory and Local Directories

By default, the System Directory is associated with an identity provider named System Identity Provider. The Password (Cloud Directory) method is enabled by default on this identity provider and applies to the default_access_policy_set policy for the ALL RANGES network range and the Web Browser device type. You can configure additional authentication methods and set authentication policies.

When you create a new local directory, it is not associated with any identity provider. After creating the directory, create a new identity provider of type Embedded and associate the directory with it. Enable the Password (Cloud Directory) authentication method on the identity provider. Multiple local directories can be associated with the same identity provider.

The VMware Identity Manager connector is not required for either the System Directory or for local directories you create.

For more information, see "Configuring User Authentication in VMware Identity Manager" in *VMware Identity Manager Administration*.

## Password Management for Local Directory Users

By default, all users of local directories have the ability to change their password in the Workspace ONE portal or app. You can set a password policy for local users. You can also reset local user passwords as needed.

Users can change their passwords when they are logged into the Workspace ONE portal by clicking their name in the top-right corner, selecting **Account** from the drop-down menu, and clicking the **Change Password** link. In the Workspace ONE app, users can change their passwords by clicking the triple-bar menu icon and selecting **Password**.

For information on setting password policies and resetting local user passwords, see "Managing Users and Groups" in *VMware Identity Manager Administration*.

This section includes the following topics:



# Creating a Local Directory

To create a local directory, you specify the user attributes for the directory, create the directory, and identify it with an identity provider.

## Set User Attributes at the Global Level

Before you create a local directory, review the global user attributes on the User Attributes page and add custom attributes, if necessary.

User attributes, such as firstName, lastName, email and domain, are part of a user's profile. In the VMware Identity Manager service, user attributes are defined at the global level and apply to all directories in the service, including local directories. At the local directory level, you can override whether an attribute is required or optional for users in that local directory, but you cannot add custom attributes. If an attribute is required, you must provide a value for it when you create a user.

The following words cannot be used when you create custom attributes.

**Table 2-1. Words that cannot be used as Custom Attribute Names**

| | | |
|---|---|---|
| active | addresses | costCenter |
| department | displayName | division |
| emails | employeeNumber | entitlements |
| externalId | groups | id |
| ims | locale | manager |
| meta | name | nickName |
| organization | password | phoneNumber |
| photos | preferredLanguage | profileUrl |

**Table 2-1. Words that cannot be used as Custom Attribute Names (Continued)**

| | | |
|---|---|---|
| roles | timezone | title |
| userName | userType | x509Certificate |

**Note** The ability to override user attributes at the directory level only applies to local directories, not to Active Directory or LDAP directories.

### Procedure

1 In the administration console, click the **Identity & Access Management** tab.

2 Click **Setup**, then click the **User Attributes** tab.

3 Review the list of user attributes and add additional attributes, if necessary.

**Note** Although this page lets you select which attributes are required, it is recommended that you make the selection for local directories at the local directory level. If an attribute is marked required on this page, it applies to all directories in the service, including Active Directory or LDAP directories.

4 Click **Save**.

### What to do next

Create the local directory.

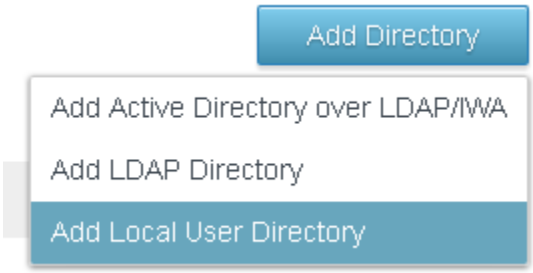
## Create a Local Directory

After you review and set global user attributes, create the local directory.

### Procedure

1 In the administration console, click the **Identity & Access Management** tab, then click the **Directories** tab

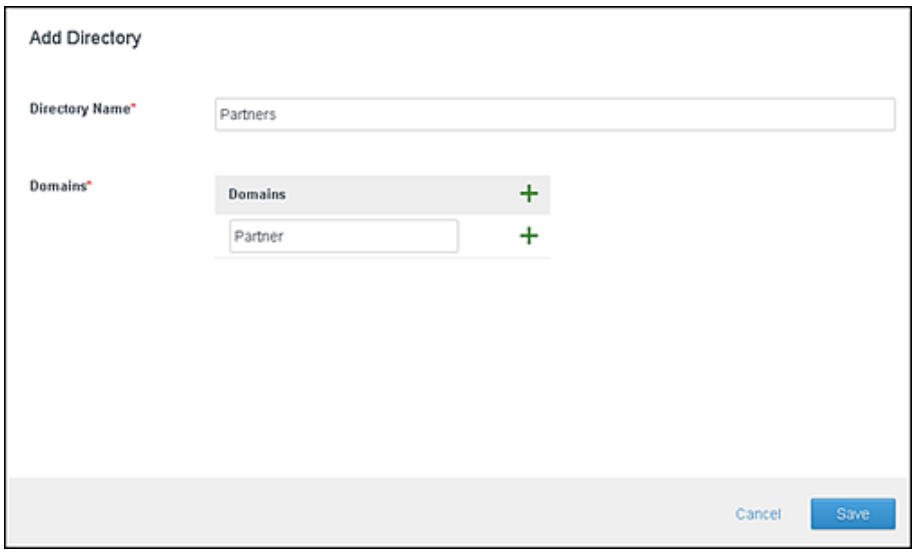
2 Click **Add Directory** and select **Add Local User Directory** from the drop-down menu.




3 In the Add Directory page, enter a directory name and specify at least one domain name.

The domain name must be unique across all directories in the service.

For example:




4 Click **Save**.

5 In the Directories page, click the new directory.

6 Click the **User Attributes** tab.

All the attributes from the Identity & Access Management > Setup > User Attributes page are listed for the local directory. Attributes that are marked required on that page are listed as required in the local directory page too.

7 Customize the attributes for the local directory.

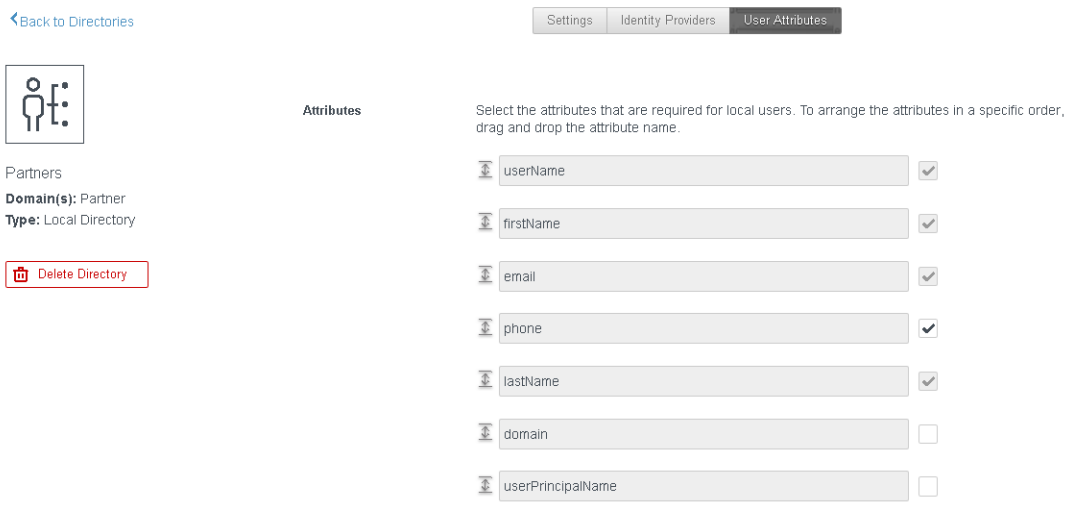
You can specify which attributes are required and which attributes are optional. You can also change the order in which the attributes appear.

**Important** The attributes userName, firstName, lastName, and email are always required for local directories.

- To make an attribute required, select the check box next to the attribute name.
- To make an attribute optional, deselect the check box next to the attribute name.
- To change the order of the attributes, click and drag the attribute to the new position.

If an attribute is required, when you create a user you must specify a value for the attribute.

For example:




8 Click **Save**.

### What to do next

Associate the local directory with the identity provider you want to use to authenticate users in the directory.

## Associate the Local Directory With an Identity Provider

Associate the local directory with an identity provider so that users in the directory can be authenticated. Create a new identity provider of type Embedded and enable the Password (Local Directory) authentication method on it.

**Note** Do not use the Built-in identity provider. Enabling the Password (Local Directory) authentication method on the Built-in identity provider is not recommended.

### Prerequisites

The Password (Local Directory) authentication method must be configured in the Identity & Access Management > Authentication Methods page.

### Procedure

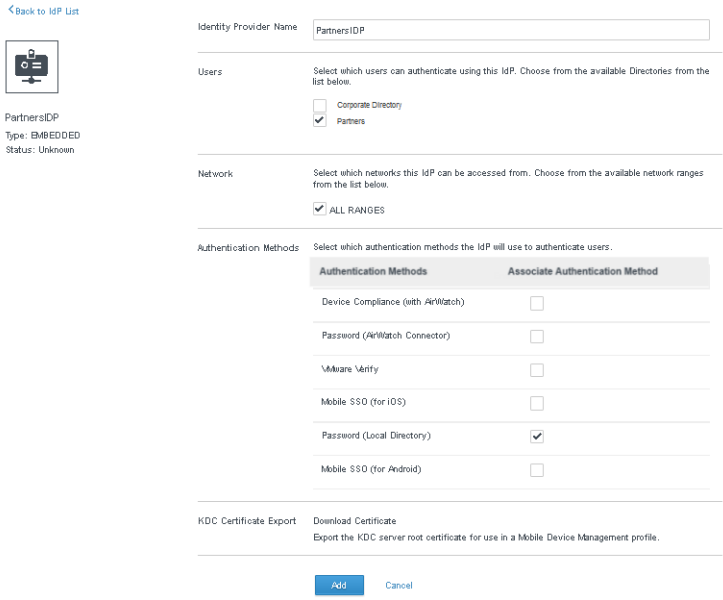
1 In the **Identity & Access Management** tab, click the **Identity Providers** tab.

2 Click **Add Identity Provider** and select **Create Built-in IDP**.

3 Enter the following information.

| Option | Description |
|---|---|
| **Identity Provider Name** | Enter a name for the identity provider. |
| **Users** | Select the local directory you created. |
| **Network** | Select the networks from which this identity provider can be accessed. |

| Option | Description |
| --- | --- |
| **Authentication Methods** | Select Password (Local Directory). |
| **KDC Certificate Export** | You do not need to download the certificate unless you are configuring mobile SSO for AirWatch-managed iOS devices. |




4 Click **Add**.

The identity provider is created and associated with the local directory. Later, you can configure other authentication methods on the identity provider. For more information about authentication, see "Configuring User Authentication in VMware Identity Manager" in *VMware Identity Manager Administration*.

You can use the same identity provider for multiple local directories.

### What to do next

Create local users and groups. You create local users and groups in the **Users & Groups** tab in the administration console. See "Managing Users and Groups" in *VMware Identity Manager Administration* for more information.

# Changing Local Directory Settings

After you create a local directory, you can modify its settings at any time.

You can change the following settings.

- Change the directory name.
- Add, delete, or rename domains.
  - Domain names must be unique across all directories in the service.
  - When you change a domain name, the users that were associated with the old domain are associated with the new domain.

  - The directory must have at least one domain.
  - You cannot add a domain to the System Directory or delete the System Domain.
- Add new user attributes or make an existing attribute required or optional.
  - If the local directory does not have any users yet, you can add new attributes as either optional or required, and change existing attributes to required or optional.
  - If you have already created users in the local directory, you can add new attributes as optional attributes only, and change existing attributes from required to optional. You cannot make an optional attribute required after users have been created.
  - The attributes userName, firstName, lastName, and email are always required for local directories.
  - As user attributes are defined at the global level in the VMware Identity Manager service, any new attributes you add will appear in all directories in the service.
- Change the order in which attributes appear.

### Procedure

1. Click the **Identity & Access Management** tab.
2. In the Directories page, click the directory you want to edit.
3. Edit the local directory settings.

| Option | Action |
|---|---|
| **Change the directory name** | a In the **Settings** tab, edit the directory name.<br>b Click **Save**. |
| **Add, delete, or rename a domain** | a In the **Settings** tab, edit the **Domains** list.<br>b To add a domain, click the green plus icon.<br>c To delete a domain, click the red delete icon.<br>d To rename a domain, edit the domain name in the text box. |
| **Add user attributes to the directory** | a Click the **Identity & Access Management** tab, then click **Setup**.<br>b Click the **User Attributes** tab.<br>c Add attributes in the **Add other attributes to use** list, and click **Save**. |
| **Make an attribute required or optional for the directory** | a In the **Identity & Access Management** tab, click the **Directories** tab.<br>b Click the local directory name and click the **User Attributes** tab.<br>c Select the check box next to an attribute to make it a required attribute, or deselect the check box to make it an optional attribute.<br>d Click **Save**. |
| **Change the order of the attributes** | a In the **Identity & Access Management** tab, click the **Directories** tab.<br>b Click the local directory name and click the **User Attributes** tab.<br>c Click and drag the attributes to the new position.<br>d Click **Save**. |

# Deleting a Local Directory

You can delete a local directory that you created in the VMware Identity Manager service. You cannot delete the System Directory, which is created by default when you first set up the service.

**Caution** When you delete a directory, all users in the directory are also deleted from the service.

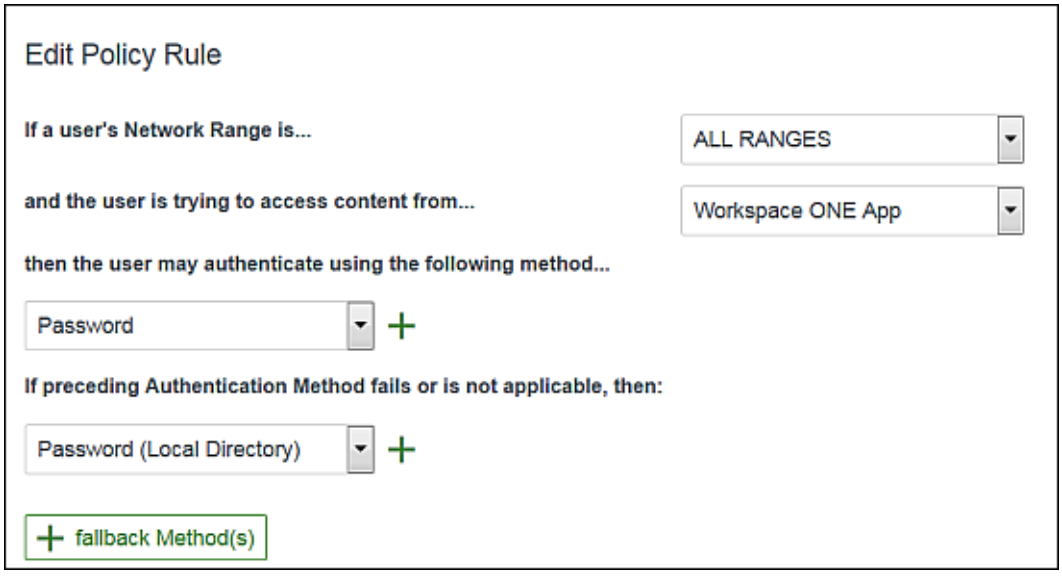
### Procedure

1. Click the **Identity & Access Management** tab, then click the **Directories** tab.
2. Click the directory you want to delete.
3. In the directory page, click **Delete Directory**.

# Configuring Authentication Method for System Admin Users

The default authentication method for admin users to log in from the System directory is Password (Local Directory). The default access policy is configured with Password (Local Directory) as a fallback method so that admins can log in to VMware Identity Manager admin console and Workspace ONE portal

If you create access policies for specific Web and desktop applications that system admins are entitled to, these policies must be configured to include Password (Local Directory) as a fallback authentication method. Otherwise, the admins cannot log in to the application.



# Just-in-Time User Provisioning

3

Just-in-Time user provisioning lets you create users in the VMware Identity Manager service dynamically at login time, using SAML assertions sent by a third-party identity provider. Just-in-Time user provisioning is available only for third-party identity providers. It is not available for the VMware Identity Manager connector.

This section includes the following topics:



## About Just-in-Time User Provisioning

Just-in-Time provisioning provides another way of provisioning users in the VMware Identity Manager service. Instead of syncing users from an Active Directory instance, with Just-in-Time provisioning users are created and updated dynamically when they log in, based on SAML assertions sent by the identity provider.

In this scenario, VMware Identity Manager acts as the SAML service provider (SP).

Just-in-Time configuration can only be configured for third-party identity providers. It is not available for the connector.

With a Just-in-Time configuration, you do not need to install a connector on premises as all user creation and management is handled through SAML assertions and authentication is handled by the third-party identity provider.

## User Creation and Management

If Just-in-Time user provisioning is enabled, when a user goes to the VMware Identity Manager service login page and selects a domain, the page redirects the user to the correct identity provider. The user logs in, is authenticated, and is redirected by the identity provider back to the VMware Identity Manager service with a SAML assertion. The attributes in the SAML assertion are used to create the user in the service. Only those attributes that match the user attributes defined in the service are used; other attributes are ignored. The user is also added to groups based on the attributes, and receives the entitlements that are set for those groups.

On subsequent logins, if there are any changes in the SAML assertion, the user is updated in the service.

Just-in-Time provisioned users cannot be deleted. To delete users, you must delete the Just-in-Time directory.

Note that all user management is handled through SAML assertions. You cannot create or update these users directly from the service. Just-in-Time users cannot be synced from Active Directory.

For information about the attributes required in the SAML assertion, see Requirements for SAML Assertions.

## Just-in-Time Directory

The third-party identity provider must have a Just-in-Time directory associated with it in the service.

When you first enable Just-in-Time provisioning for an identity provider, you create a new Just-in-Time directory and specify one or more domains for it. Users belonging to those domains are provisioned to the directory. If multiple domains are configured for the directory, SAML assertions must include a domain attribute. If a single domain is configured for the directory, a domain attribute is not required in SAML assertions but if specified, its value must match the domain name.

Only one directory, of type Just-in-Time, can be associated with an identity provider that has Just-in-Time provisioning enabled.

# Preparing for Just-in-Time Provisioning

Before you configure Just-in-Time user provisioning, review your groups, group entitlements, and user attribute settings and make changes, if necessary. Also, identify the domains you want to use for the Just-in-Time directory.

## Create Local Groups

Users provisioned through Just-in-Time provisioning are added to groups based on their user attributes and derive their resources entitlements from the groups to which they belong. Before you configure Just-in-Time provisioning, ensure that you have local groups in the service. Create one or more local groups, based on your needs. For each group, set the rules for group membership and add entitlements.

### Procedure

1. In the administration console, click the **Users & Groups** tab.
2. Click **Create Group**, provide a name and description for the group, and click **Add**.
3. In the Groups page, click the new group.
4. Set up users for the group.
   a. In the left pane, select **Users in This Group**.
   b. Click **Modify Users in This Group** and set the rules for group membership.
5. Add entitlements to the group.
   a. In the left pane, select **Entitlements**.
   b. Click **Add Entitlements** and select the applications and the deployment method for each application.
   c. Click **Save**.

## Review User Attributes

Review the user attributes that are set for all VMware Identity Manager directories in the User Attributes page and modify them, if necessary. When a user is provisioned through Just-in-Time provisioning, the SAML assertion is used to create the user. Only those attributes in the SAML assertion that match the attributes listed in the User Attributes page are used.

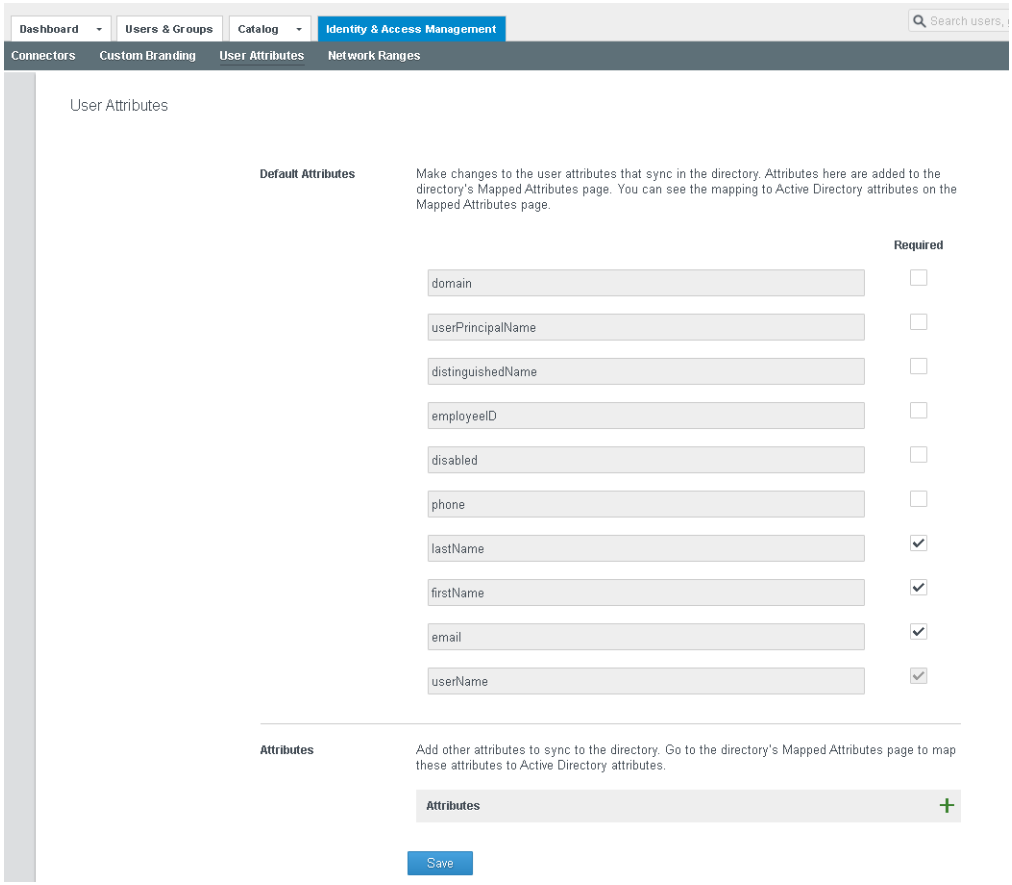
**Important** If an attribute is marked required in the User Attributes page, the SAML assertion must include the attribute, otherwise login fails.

When you make changes to the user attributes, consider the effect on other directories and configurations in your tenant. The User Attributes page applies to all directories in your tenant.

**Note** You do not have to mark the `domain` attribute required.

### Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. Click **Setup** and click **User Attributes**.
3. Review the attributes and make changes, if necessary.




# Configuring Just-in-Time User Provisioning

You configure Just-in-Time user provisioning for a third-party identity provider while creating or updating the identity provider in the VMware Identity Manager service.

When you enable Just-in-Time provisioning, you create a new Just-in-Time directory and specify one or more domains for it. Users belonging to these domains are added to the directory.

You must specify at least one domain. The domain name must be unique across all the directories in the VMware Identity Manager service. If you specify multiple domains, SAML assertions must include the domain attribute. If you specify a single domain, it is used as the domain for SAML assertions without a domain attribute. If a domain attribute is specified, its value must match one of the domains otherwise login fails.

### Procedure

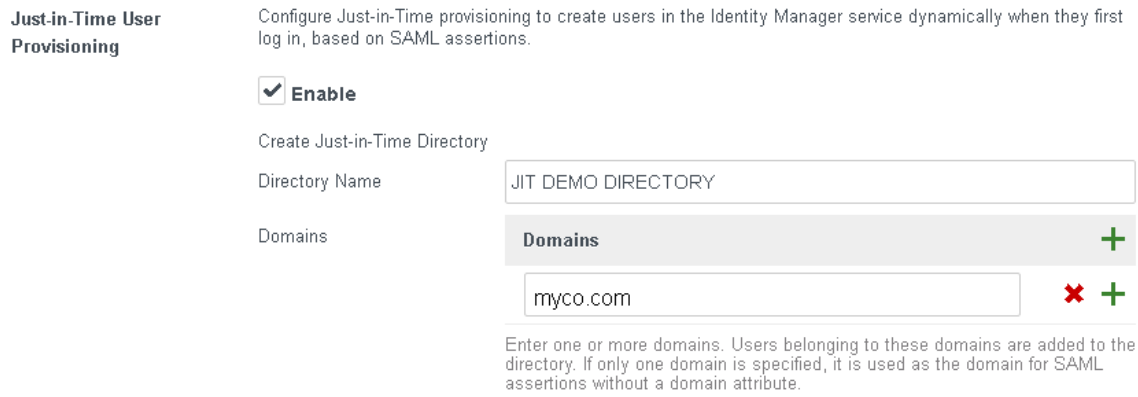
1. Log in to the VMware Identity Manager service administration console.
2. Click the **Identity & Access Management** tab, then click **Identity Providers**.
3. Click **Add Identity Provider** or select an identity provider.
4. In the **Just-in-Time User Provisioning** section, click **Enable**.

5 Specify the following information.

- A name for the new Just-in-Time directory.
- One or more domains.

> **Important** The domain names must be unique across all directories in the tenant.

For example:




6 Complete the rest of the page and click **Add** or **Save**. For information, see Configuring a Third-Party Identity Provider Instance to Authenticate Users.

# Requirements for SAML Assertions

When Just-in-Time user provisioning is enabled for a third-party identity provider, users are created or updated in the VMware Identity Manager service during login based on SAML assertions. SAML assertions sent by the identity provider must contain certain attributes.

- The SAML assertion must include the `userName` attribute.
- The SAML assertion must include all the user attributes that are marked as required in the VMware Identity Manager service.

  To view or edit the user attributes in the administration console, in the **Identity & Access Management** tab, click **Setup** and then click **User Attributes**.

  > **Important** Ensure that the keys in the SAML assertion match the attribute names exactly, including the case.

- If you are configuring multiple domains for the Just-in-Time directory, the SAML assertion must include the `domain` attribute. The value of the attribute must match one of the domains configured for the directory. If the value does not match or a domain is not specified, login fails.
- If you are configuring a single domain for the Just-in-Time directory, specifying the `domain` attribute in the SAML assertion is optional.

If you specify the `domain` attribute, ensure its value matches the domain configured for the directory. If the SAML assertion does not contain a domain attribute, the user is associated with the domain that is configured for the directory

- If you want to allow user name updates, include the `ExternalId` attribute in the SAML assertion. The user is identified by the `ExternalId`. If, on a subsequent login, the SAML assertion contains a different user name, the user is still identified correctly, log in succeeds, and the user name is updated in the Identity Manager service.

Attributes from the SAML assertion are used to create or update users as follows.

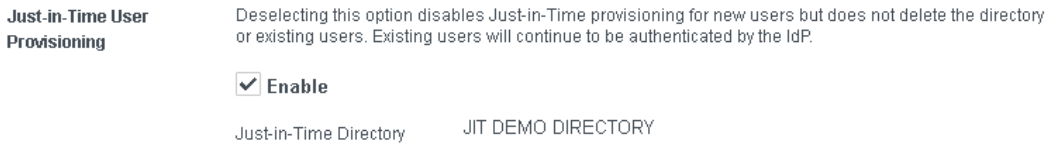
- Attributes that are required or optional in the Identity Manager service (as listed in the User Attributes page) are used.
- Attributes that do not match any attributes in the User Attributes page are ignored.
- Attributes without a value are ignored.

# Disabling Just-in-Time User Provisioning

You can disable Just-in-Time user provisioning. When the option is disabled, new users are not created and existing users are not updated during login. Existing users continue to be authenticated by the identity provider.

### Procedure

1. In the administration console, click the **Identity & Access Management** tab, then click **Identity Providers**.
2. Click the identity provider you want to edit.
3. In the **Just-in-Time User Provisioning** section, deselect the **Enable** checkbox.




# Deleting a Just-in-Time Directory

A Just-in-Time directory is the directory associated with a third-party identity provider that has Just-in-Time user provisioning enabled. When you delete the directory, all users in the directory are deleted and the Just-in-time configuration is disabled. Because a Just-in-Time identity provider can only have a single directory, when you delete the directory, the identity provider can no longer be used.

To enable Just-in-Time configuration for the identity provider again, you will need to create a new directory.

### Procedure

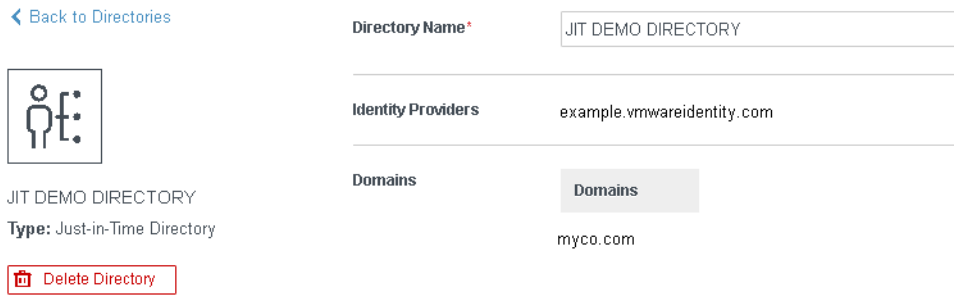
1 In the administration console, click the **Identity & Access Management** tab.

2 In the Directories page, locate the directory you want to delete.

You can identify Just-in-Time directories by looking at the directory type in the **Type** column.

3 Click the directory name.

4 Click **Delete Directory**.




# Error Messages

Administrators or end users may see errors related to Just-in-Time provisioning. For example, if a required attribute is missing in the SAML assertion, an error occurs and the user is unable to log in.

The following errors can appear in the administration console:

| Error Message | Solution |
|---|---|
| `If JIT User provisioning is enabled, at least one directory must be associated with identity provider.` | There is no directory associated with the identity provider. An identity provider with the Just-in-Time provisioning option enabled must have a Just-in-Time directory associated with it.<br>1 In the **Identity & Access Management** tab in the administration console, click **Identity Providers** and click the identity provider.<br>2 In the **Just-in-Time User Provisioning** section, specify a directory name and one or more domains.<br>3 Click **Save**.<br>A Just-in-Time directory is created. |

The following errors can appear on the log-in page:

| Error Message | Solution |
| --- | --- |
| `User attribute is missing: name.` | A required user attribute is missing in the SAML assertion sent by the third-party identity provider. All attributes that are marked required in the User Attributes page must be included in the SAML assertion. Modify the third-party identity provider settings to send the correct SAML assertions. |
| `Domain is missing and cannot be inferred.` | The SAML assertion does not include the domain attribute and the domain cannot be determined. A domain attribute is required in the following cases:<br>■ If multiple domains are configured for the Just-in-Time directory.<br>■ If domain is marked as a required attribute in the User Attributes page.<br>If a domain attribute is specified, its value must match one of the domains specified for the directory.<br>Modify the third-party identity provider settings to send the correct SAML assertions. |
| `Attribute name: name, value: value.` | The attribute in the SAML assertion does not match any of the attributes in the User Attributes page in the tenant and will be ignored. |
| `Failed to create or update a JIT user.` | The user could not be created in the service. Possible causes include the following:<br>■ A required attribute is missing in the SAML assertion.<br>Review the attributes in the User Attributes page and ensure that the SAML assertion includes all the attributes that are marked required.<br>■ The domain for the user could not be determined.<br>Specify the domain attribute in the SAML assertion and ensure that its value matches one of the domains configured for the Just-in-Time directory. |

# Managing the User Login Experience

4

The default experience for users who log in to the Workspace ONE portal from VMware Identity Manager is to select the domain to which they belong on the first login page that displays.

VMware Identity Manager displays the authentication page based on the access policy rules configured for that domain.

Users are identified uniquely by both their user name and domain. Because users select their domain first, users that have the same user name but in different domains can log in successfully. For example, you can have a user jane in domain eng.example.com and another user jane in domain sales.example.com

This section includes the following topics:



## Login Experience Using Unique Identifier

When you do not want to require users to select their domain before they log in, you can hide the domain request page. You then select a unique identifier to distinguish users across your organization.

When users log in, a page displays prompting them to enter their unique identifier. VMware Identity Manager attempts to find the user in the internal database. When the VMware Identity Manager service looks up the identifier, the information found includes the domain that the user belongs to. The authentication page that displays is based on the access policy rules for that domain.

The unique identifier can be the user name, email address, UPN, or employee ID. You select the identifier to use from the Identity & Access Management > Preferences page. The unique identifier attribute must be mapped in the User Attributes page and synced from Active Directory.

If multiple users are found that match the identifier and no unique user can be determined, an error message displays. If no user is found, the local user login page is displayed to avoid possible user name enumeration attacks.

# Set up Unique Identifier-Based Log In

When users use a user name and password authentication method, you can enable the unique identifier option to display the identifier-based login pages. Users are asked to enter their unique identifier and then are asked to enter the appropriate authentication based on the configured access policy rules.

The authentication methods that support unique identifier-based log in include the Password authentication methods, RSA SecurID, and RADIUS.

### Prerequisites

- Select the unique identifier user attribute to use in the I &M Access > User Attributes page. Make sure that attribute is used only to identify unique objects.
- Make sure that the selected attributes sync to the directory.
- Verify that the default access policy rules for the user domains reflect the type of authentication to use when identifier-based login is available.

### Procedure

1. From the admin console Identity & Access Management tab, click **Preferences**.
2. To hide the domain selection login page, select the **Enable** check box.
3. Select the unique identifier to use from the drop-down menu. The options are username, email, UPN, or employee ID.
4. Click **Save**.

# Requiring Terms of Use to Access the Workspace ONE Catalog

You can write your organization's own Workspace ONE terms of use and ensure the end user accepts this terms of use before using Workspace ONE.

The terms of use display after the user signs into Workspace ONE. Users must accept the terms of use before proceeding to their Workspace ONE catalog.

The Terms of Use feature include the following configuration options.

- Create versions of existing terms of use.
- Edit terms of use.
- Create multiple terms of use that can be displayed based on the device type.
- Create language-specific copies of the terms of use.

The terms of use policies that you setup are listed in the Identity & Access Management tab. You can edit the terms of use policy to make a correction to the existing policy or create a new version of the policy. Adding a new version of the terms of use, replaces the existing terms of use. Editing a policy does not version the terms of use.

You can view the number of users who have accepted or declined the terms of use from the terms of use page. Click either the accepted or declined number to see a list of users and their status.

## Set Up and Enable Terms of Use

In the Terms of Use page, you add the terms of use policy and configure the usage parameters. After the terms of use are added, you enable the Term of Use option. When users sign in to Workspace ONE, they must accept the terms of use to access their catalog.

### Prerequisites

The text of the terms of use policy formatted in HTML to copy and paste in the Terms of Use content text box. You can add terms of use in English, German, Spanish, French, Italian, and Dutch.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup > Terms of Use**.
2. Click **Add Terms of Use**.
3. Enter a descriptive name for the terms of use.
4. Select **Any**, if the terms of use policy is for all users. To use terms up use policies by device type, select **Selected Devices Platforms** and select the device types that display this terms of use policy.
5. By default, the language of the terms of use that is displayed first is based on the browser language preference settings. Enter the terms of use content for the default language in the text box.
6. Click **Save**.

   To add a terms of use policy in another language, click **Add Language** and select another language. The Terms of Use content text box is refreshed and you can add the text in the text box.

   You can drag the language name to establish the order that the terms of use are displayed.
7. To begin using the terms of use, click **Enable Terms of Use** on the page that displays.

### What to do next

If you selected a specific device type for the terms of use, you can create additional terms of use for the other device types.

## View Status of Terms of Use Acceptance

The terms of use policies listed in the Identity & Management > Terms of Use page shows the number of users that accepted or declined the policy.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup > Terms of Use**.

2 In the Accepted / Decline column, click either the Accepted number on the left or the Declined number on the right.

   A status page displays the action taken, either accepted or declined, with the user name, device ID, version of the policy viewed, platform used, and the date.

3 Click **Cancel** to close the view.

# Configuring User Authentication in VMware Identity Manager

5

VMware Identity Manager supports multiple authentication methods. You can configure a single authentication method and you can set up chained, two-factor authentication. You can also use an authentication method that is external for RADIUS and SAML protocols.

The identity provider instance that you use with the VMware Identity Manager service creates an in-network federation authority that communicates with the service using SAML 2.0 assertions.

When you initially deploy the VMWare Identity Manager service, the connector is the initial identity provider for the service. Your existing Active Directory infrastructure is used for user authentication and management.

The following authentication methods are supported. You configure these authentication methods from the administration console.

| Authentication Methods | Description |
|---|---|
| Password (on-premise deployment) | Without any configuration after Active Directory is configured, VMware Identity Manager supports Active Directory password authentication. This method authenticates users directly against Active Directory. |
| Kerberos for desktops | Kerberos authentication provides domain users with single sign-in access to their apps porta. Users do not need to sign in to their apps portal again after they log in to the network. Two Kerberos authentication methods can be configured, Kerberos authentication for desktop with Integrated Windows Authentication, and built-in Kerberos authentication for iOS 9 mobile device when a trust relationship is set up between Active Directory and AirWatch. |
| Certificate (on-premise deployment) | Certificate-based authentication can be configured to allow clients to authenticate with certificates on their desktop and mobile devices or to use a smart card adapter for authentication.<br>Certificate-based authentication is based on what the user has and what the person knows. An X.509 certificate uses the public key infrastructure standard to verify that a public key contained within the certificate belongs to the user. |
| RSA SecurID (on-premise deployment) | When RSA SecurID authentication is configured, VMware Identity Manager is configured as the authentication agent in the RSA SecurID server. RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is an authentication method for users accessing VMware Identity Manager from outside the enterprise network. |
| RADIUS (on-premise deployment) | RADIUS authentication provides two-factor authentication options. You set up the RADIUS server that is accessible to the VMware Identity Manager service. When users sign in with their user name and passcode, an access request is submitted to the RADIUS server for authentication. |

| Authentication Methods | Description |
|---|---|
| RSA Adaptive Authentication (on-premise deployment) | RSA authentication provides a stronger multi-factor authentication than only user name and password authentication against Active Directory. When RSA Adaptive Authentication is enabled, the risk indicators specified in the risk policy set up in the RSA Policy Management application. The VMware Identity Manager service configuration of adaptive authentication is used to determine the required authentication prompts. |
| Mobile SSO (for iOS) | Mobile SSO for iOS authentication is used for single sign-on authentication for AirWatch-managed iOS devices. Mobile SSO (for iOS) authentication uses a Key Distribution Center (KDC) that is part of the Identity Manager service. You must initiate the KDC service in the VMware Identity Manager service before you enable this authentication method. |
| Mobile SSO (for Android) | Mobile SSO for Android authentication is used for single sign-on authentication for AirWatch-managed Android devices. A proxy service is set up between the VMware Identity Manager service and AirWatch to retrieve the certificate from AirWatch for authentication. |
| Password (AirWatch Connector) | The AirWatch Cloud Connector can be integrated with the VMware Identity Manager service for user password authentication. You configure the VMware Identity Manager service to sync users from the AirWatch directory. |
| VMware Verify | VMware Verify can be used as the second authentication method when two-factor authentication is required. The first authentication method is user name and password, and the second authentication method is a VMware Verify request approval or code.<br>VMware Verify uses a third-party cloud service to deliver this feature to user devices. To do so, user information such as name, email, and phone number are stored in the service but not used for any purposes other than to deliver the feature. |
| Password (Local Directory) | The Password (Local Directory) method is enabled by default for the System-IDP identity provider used with the System Directory. It is applied to the default access policy. |

After the authentication methods are configured, you create access policy rules that specify the authentication methods to be used by device type. Users are authenticated based on the authentication methods, the default access policy rules, network ranges, and the identity provider instance you configure. See Managing Authentication Methods to Apply to Users.

This section includes the following topics:

- Configuring Kerberos for VMware Identity Manager
- Configuring SecurID for VMware Identity Manager
- Configuring RADIUS for VMware Identity Manager
- Configuring RSA Adaptive Authentication in VMware Identity Manager
- Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager
- Configuring VMware Verify for Two-Factor Authentication
- Using Built-in Identity Providers
- Configure Additional Workspace Identity Providers
- Configuring a Third-Party Identity Provider Instance to Authenticate Users
- Managing Authentication Methods to Apply to Users

# Configuring Kerberos for VMware Identity Manager

Kerberos authentication provides users, who are successfully signed in to their domain, access to their apps portal without additional credential prompts.

Kerberos authentication protocol can be configured in the Identity Manager service for desktops with Integrated Windows Authentication to secure interactions between users' browsers and the Identity Manager service and for one-touch single sign-in to iOS 9 mobile devices that are managed in AirWatch. For information about Kerberos authentication on iOS 9 devices, see Using the Cloud Hosted KDC Service.

## Implementing Kerberos for Desktops with Integrated Windows Authentication

To set up Kerberos authentication for desktops, you enable Integrated Windows Authentication to allow the Kerberos protocol to secure interactions between users' browsers and the Identity Manager service.

When Kerberos authentication is enabled for desktops, the Identity Manager service validates user desktop credentials using Kerberos tickets distributed by the Key Distribution Center (KDC) implemented as a domain service in Active Directory. You do not need to directly configure Active Directory to make Kerberos function with your deployment.

You must configure the end user Web browsers to send your Kerberos credentials to the service when users sign in. See Configuring your Browser for Kerberos.

### Configure Kerberos Authentication for Desktops with Integrated Windows Authentication

To configure the VMware Identity Manager service to provide Kerberos authentication for desktops, you must join to the domain and enable Kerberos authentication on the VMware Identity Manager connector.

#### Procedure

1. In the administration console Identity & Access Management tab, select **Setup**.
2. In the Worker column for the connector click **Auth Adapters**.
3. Click **KerberosIdpAdapter**

   You are redirected to the identity manager sign in page.
4. Click **Edit** in the KerberosIdpAdapter row and configure the Kerberos authentication page.

| Option | Description |
|---|---|
| Name | A name is required. The default name is KerberosIdpAdapter. You can change this. |
| Directory UID Attribute | Enter the account attribute that contains the user name |
| Enable Windows Authentication | Select this to extend authentication interactions between users' browsers and VMware Identity Manager. |

| Option | Description |
|---|---|
| Enable NTLM | Select this to enable NT LAN Manager (NTLM) protocol-based authentication only if your Active Directory infrastructure relies on NTLM authentication. |
| Enable Redirect | Select this if round-robin DNS and load balancers do not have Kerberos support. Authentication requests are redirected to Redirect Host Name. If this is selected, enter the redirect host name in **Redirect Host Name** text box. This is usually the hostname of the service. |

5 Click **Save**.

#### What to do next

Add the authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the Kerberos authentication method to the rule in correct authentication order.

## Configuring your Browser for Kerberos

When Kerberos is enabled, you need to configure the Web browsers to send your Kerberos credentials to the service when users sign in.

The following Web browsers can be configured to send your Kerberos credentials to the Identity Manager service on computers running Windows: Firefox, Internet Explorer, and Chrome. All the browsers require additional configuration.

### Configure Internet Explorer to Access the Web Interface

You must configure the Internet Explorer browser if Kerberos is configured for your deployment and if you want to grant users access to the Web interface using Internet Explorer.

Kerberos authentication works in conjunction with VMware Identity Manager on Windows operating systems.

**Note** Do not implement these Kerberos-related steps on other operating systems.

#### Prerequisites

Configure the Internet Explorer browser for each user or provide users with the instructions after you configure Kerberos.

#### Procedure

1 Verify that you are logged into Windows as a user in the domain.

2 In Internet Explorer, enable automatic log in.

   a Select **Tools > Internet Options > Security**.

   b Click **Custom level**.

   c Select **Automatic login only in Intranet zone**.

   d Click **OK.**

3 Verify that this instance of the connector virtual appliance is part of the local intranet zone.

   a Use Internet Explorer to access the VMware Identity Manager sign in URL at *https://myconnectorhost.domain/authenticate/*.

   b Locate the zone in the bottom right corner on the status bar of the browser window.

   If the zone is Local intranet, Internet Explorer configuration is complete.

4 If the zone is not Local intranet, add the VMware Identity Manager sign in URL to the intranet zone.

   a Select **Tools > Internet Options > Security > Local intranet > Sites.**

   b Select **Automatically detect intranet network**.

   If this option was not selected, selecting it might be sufficient for adding the to the intranet zone.

   c (Optional) If you selected **Automatically detect intranet network**, click **OK** until all dialog boxes are closed.

   d In the Local Intranet dialog box, click **Advanced.**

   A second dialog box named Local intranet appears.

   e Enter the VMware Identity Manager URL in the **Add this Web site to the zone** text box.

   *https://myconnectorhost.domain/authenticate/*

   f Click **Add > Close > OK**.

5 Verify that Internet Explorer is allowed to pass the Windows authentication to the trusted site.

   a In the Internet Options dialog box, click the **Advanced** tab.

   b Select **Enable Integrated Windows Authentication**.

   This option takes effect only after you restart Internet Explorer.

   c Click **OK**.

6 Log in to the Web interface to check access.

   If Kerberos authentication is successful, the test URL goes to the Web interface.

The Kerberos protocol secures all interactions between this Internet Explorer browser instance and VMware Identity Manager. Now, users can use single sign-on to access their Workspace ONE portal.

### Configure Firefox to Access the Web Interface

You must configure the Firefox browser if Kerberos is configured for your deployment and you want to grant users access to the Web interface using Firefox.

Kerberos authentication works in conjunction with VMware Identity Manager on Windows operating systems.

#### Prerequisites

Configure the Firefox browser, for each user, or provide users with the instructions, after you configure Kerberos.

#### Procedure

1. In the URL text box of the Firefox browser, enter `about:config` to access the advanced settings.
2. Click **I'll be careful, I promise!**.
3. Double-click **network.negotiate-auth.trusted-uris** in the Preference Name column.
4. Enter your VMware Identity Manager URL in the text box.

   *https://myconnectorhost.domain.com*
5. Click **OK.**
6. Double-click **network.negotiate-auth.delegation-uris** in the Preference Name column.
7. Enter your VMware Identity Manager URL in the text box.

   *https://myconnectorhost.domain.com/authenticate/*
8. Click **OK.**
9. Test Kerberos functionality by using the Firefox browser to log in to login URL. For example, *https://myconnectorhost.domain.com/authenticate/*.

   If the Kerberos authentication is successful, the test URL goes to the Web interface.

The Kerberos protocol secures all interactions between this Firefox browser instance and VMware Identity Manager. Now, users can use single sign-on access their Workspace ONE portal.

### Configure the Chrome Browser to Access the Web Interface

You must configure the Chrome browser if Kerberos is configured for your deployment and if you want to grant users access to the Web interface using the Chrome browser.

Kerberos authentication works in conjunction with VMware Identity Manager on Windows operating systems.

**Note** Do not implement these Kerberos-related steps on other operating systems.

#### Prerequisites

- Configure Kerberos.
- Since Chrome uses the Internet Explorer configuration to enable Kerberos authentication, you must configure Internet Explorer to allow Chrome to use the Internet Explorer configuration. See Google documentation for information about how to configure Chrome for Kerberos authentication.

#### Procedure

1. Test Kerberos functionality by using the Chrome browser.
2. Log in to VMware Identity Manager at *https://myconnectorhost.domain.com/authenticate/*.

   If Kerberos authentication is successful, the test URL connects with the Web interface.

If all related Kerberos configurations are correct, the relative protocol (Kerberos) secures all interactions between this Chrome browser instance and VMware Identity Manager. Users can use single sign-on access their Workspace ONE portal.

# Configuring SecurID for VMware Identity Manager

When you configure RSA SecurID server, you must add the VMware Identity Manager service information as the authentication agent on the RSA SecurID server and configure the RSA SecurID server information on the VMware Identity Manager service.

When you configure SecurID to provide additional security, you must ensure that your network is properly configured for your VMware Identity Manager deployment. For SecurID specifically, you must ensure that the appropriate port is open to enable SecurID to authenticate users outside your network.

After you run the VMware Identity Manager Setup wizard and configured your Active Directory connection, you have the information necessary to prepare the RSA SecurID server. After you prepare the RSA SecurID server for VMware Identity Manager, you enable SecurID in the administration console.

- Prepare the RSA SecurID Server

  The RSA SecurID server must be configured with information about the VMware Identity Manager appliance as the authentication agent. The information required is the host name and the IP addresses for network interfaces.

- Configure RSA SecurID Authentication

  After the VMware Identity Manager appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecurID configuration information to the connector.

## Prepare the RSA SecurID Server

The RSA SecurID server must be configured with information about the VMware Identity Manager appliance as the authentication agent. The information required is the host name and the IP addresses for network interfaces.

### Prerequisites

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network: RSA AM 6.1.2, 7.1 SP2 and later, and 8.0 and later. The VMware Identity Manager server uses AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), which only supports the preceding versions of RSA Authentication Manager (the RSA SecurID server). For information about installing and configuring RSA Authentication Manager (RSA SecurID server), see RSA documentation.

### Procedure

1 On a supported version of the RSA SecurID server, add the VMware Identity Manager connector as an authentication agent. Enter the following information.

| Option | Description |
|---|---|
| **Hostname** | The host name of VMware Identity Manager. |
| **IP address** | The IP address of VMware Identity Manager. |
| **Alternate IP address** | If traffic from the connector passes through a network address translation (NAT) device to reach the RSA SecurID server, enter the private IP address of the appliance. |

2 Download the compressed configuration file and extract the `sdconf.rec` file.

Be prepared to upload this file later when you configure RSA SecurID in VMware Identity Manager.

### What to do next

Go to the administration console and in the Identity & Access Management tab Setup pages, select the connector and in the AuthAdapters page configure SecurID.

## Configure RSA SecurID Authentication

After the VMware Identity Manager appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecurID configuration information to the connector.

### Prerequisites

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the compressed file from the RSA SecurID server and extract the server configuration file.

### Procedure

1 In the administration console Identity & Access Management tab, select **Set Up**.

2 On the Connectors page, select the Worker link for the connector that is being configured with RSA SecurID.

3 Click **Auth Adapters** and then click **SecurIDIdpAdapter**.

You are redirected to the identity manager sign in page.

4 In the Authentication Adapters page SecurIDIdpAdapter row, click **Edit**.

5 Configure the SecurID Authentication Adapter page.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page.

| Option | Action |
|---|---|
| Name | A name is required. The default name is SecurIDIdpAdapter. You can change this. |
| Enable SecurID | Select this box to enable SecurID authentication. |
| Number of authentication attempts allowed | Enter the maximum number of failed login attempts when using the RSA SecurID token. The default is five attempts.<br>**Note** When more than one directory is configured and you implement RSA SecurID authentication with additional directories, configure **Number of authentication attempts allowed** with the same value for each RSA SecurID configuration. If the value is not the same, SecurID authentication fails. |
| Connector Address | Enter the IP address of the connector instance. The value you enter must match the value you used when you added the connector appliance as an authentication agent to the RSA SecurID server. If your RSA SecurID server has a value assigned to the Alternate IP address prompt, enter that value as the connector IP address. If no alternate IP address is assigned, enter the value assigned to the IP address prompt. |
| Agent IP Address | Enter the value assigned to the **IP address** prompt in the RSA SecurID server. |
| Server Configuration | Upload the RSA SecurID server configuration file. First, you must download the compressed file from the RSA SecurID server and extract the server configuration file, which by default is named `sdconf.rec`. |
| Node Secret | Leaving the node secret field blank allows the node secret to auto generate. It is recommended that you clear the node secret file on the RSA SecurID server and intentionally do not upload the node secret file. Ensure that the node secret file on the RSA SecurID server and on the server connector instance always match. If you change the node secret at one location, change it at the other location. |

6 Click **Save**.

### What to do next

Add the authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the SecurID authentication method to the rule. See Managing Authentication Methods to Apply to Users.

# Configuring RADIUS for VMware Identity Manager

You can configure VMware Identity Manager so that users are required to use RADIUS (Remote Authentication Dial-In User Service) authentication. You configure the RADIUS server information on the VMware Identity Manager service.

RADIUS support offers a wide range of alternative two-factor token-based authentication options. Because two-factor authentication solutions, such as RADIUS, work with authentication managers installed on separate servers, you must have the RADIUS server configured and accessible to the identity manager service.

When users sign in to their Workspace ONE portal and RADIUS authentication is enabled, a special login dialog box appears in the browser. Users enter their RADUS authentication user name and passcode in the login dialog box. If the RADIUS server issues an access challenge, the identity manager service displays a dialog box prompting for a second passcode. Currently support for RADIUS challenges is limited to prompting for text input.

After a user enters credentials in the dialog box, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism to the user's cell phone with a code. The user can enter this text and code into the login dialog box to complete the authentication.

If the RADIUS server provides the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication username and passcode.

## Prepare the RADIUS Server

Set up the RADIUS server and then configure the RADIUS server to accept RADIUS requests from the VMware Identity Manager service.

Refer to your RADIUS vendor's setup guides for information about setting up the RADIUS server. Note your RADIUS configuration information as you use this information when you configure RADIUS in the service. To see the type of RADIUS information required to configure VMware Identity Manager go to Configure RADIUS Authentication in VMware Identity Manager.

You can set up a secondary Radius authentication server to be used for high availability. If the primary RADIUS server does not respond within the server timeout configured for RADIUS authentication, the request is routed to the secondary server. When the primary server does not respond, the secondary server receives all future authentication requests.

## Configure RADIUS Authentication in VMware Identity Manager

You enable RADIUS authentication and configure the RADIUS settings in VMware Identity Manager administration console.

### Prerequisites

Install and configure the RADIUS software on an authentication manager server. For RADIUS authentication, follow the vendor's configuration documentation.

You need to know the following RADIUS server information to configure RADIUS on the service.

- IP address or DNS name of the RADIUS server.
- Authentication port numbers. Authentication port is usually 1812.
- Authentication type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 and 2).
- RADIUS shared secret that is used for encryption and decryption in RADIUS protocol messages.
- Specific timeout and retry values needed for RADIUS authentication

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup**.
2. On the Connectors page, select the Worker link for the connector that is being configured for RADIUS authentication.

3 Click **Auth Adapters** and then click **RadiusAuthAdapter**.

You are redirected to the identity manager sign-in page.

4 Click **Edit** to configure these fields on the Authentication Adapter page.

| Option | Action |
|---|---|
| Name | A name is required. The default name is RadiusAuthAdapter. You can change this. |
| Enable Radius Adapter | Select this box to enable RADIUS authentication. |
| Number of authentication attempts allowed | Enter the maximum number of failed login attempts when using RADIUS to log in. The default is five attempts. |
| Number of attempts to Radius server | Specify the total number of retry attempts. If the primary server does not respond, the service waits for the configured time before retrying again. |
| Radius server hostname/address | Enter the host name or the IP address of the RADIUS server. |
| Authentication port | Enter the Radius authentication port number. This is usually 1812. |
| Accounting port | Enter 0 for the port number. The accounting port is not used at this time. |
| Authentication type | Enter the authentication protocol that is supported by the RADIUS server. Either PAP, CHAP, MSCHAP1, OR MSCHAP2. |
| Shared secret | Enter the shared secret that is used between the RADIUS server and the VMware Identity Manager service. |
| Server timeout in seconds | Enter the RADIUS server timeout in seconds, after which a retry is sent if the RADIUS server does not respond. |
| Realm Prefix | (Optional) The user account location is called the realm.<br>If you specify a realm prefix string, the string is placed at the beginning of the user name when the name is sent to the RADIUS server. For example, if the user name is entered as jdoe and the realm prefix DOMAIN-A\ is specified, the user name DOMAIN-A\jdoe is sent to the RADIUS server. If you do not configure these fields, only the user name that is entered is sent. |
| Realm Suffix | (Optional) If you specify a realm suffix, the string is placed at end of the user name. For example, if the suffix is @myco.com, the username jdoe@myco.com is sent to the RADIUS server. |
| Login page passphrase hint | Enter the text string to display in the message on the user login page to direct users to enter the correct Radius passcode. For example, if this field is configured with **AD password first and then SMS passcode**, the login page message would read **Enter your AD password first and then SMS passcode.** The default text string is **RADIUS Passcode**. |

5 You can enable a secondary RADIUS server for high availability.

Configure the secondary server as described in step 4.

6 Click **Save**.

### What to do next

Add the RADIUS authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the RADIUS authentication method to the rule. See Managing Authentication Methods to Apply to Users.

# Configuring RSA Adaptive Authentication in VMware Identity Manager

RSA Adaptive Authentication can be implemented to provide a stronger multi-factor authentication than only user name and password authentication against Active Directory. Adaptive Authentication monitors and authenticates user login attempts based on risk levels and policies.

When Adaptive Authentication is enabled, the risk indicators specified in the risk policies set up in the RSA Policy Management application and the VMware Identity Manager service configuration of adaptive authentication are used to determine whether a user is authenticated with user name and password or whether additional information is needed to authenticate the user.

## Supported RSA Adaptive Authentication Methods of Authentication

The RSA Adaptive Authentication strong authentication methods supported in the VMware Identity Manager service are out-of-band authentication via phone, email, or SMS text message and challenge questions. You enable on the service the methods of RSA Adaptive Auth that can be provided. RSA Adaptive Auth policies determine which secondary authentication method is used.

Out-of-band authentication is a process that requires an additional verification be sent along with the username and password. When users enroll in the RSA Adaptive Authentication server, they provide an email address, a phone number, or both, depending on the server configuration. When additional verification is required, RSA adaptive authentication server sends a one-time passcode through the provided channel. Users enter that passcode along with their user name and password.

Challenge questions require the user to answer a series of questions when they enroll in the RSA Adaptive Authentication server. You can configure how many enrollment questions to ask and the number of challenge questions to present on the login page.

## Enrolling Users with RSA Adaptive Authentication Server

Users must be provisioned in the RSA Adaptive Authentication database in order to use adaptive authentication for authentication. Users are added to the RSA Adaptive Authentication database when they log in the first time with their user name and password. Depending on how you configured RSA Adaptive Authentication in the service, when users log in, they can be asked to provide their email address, phone number, text messaging service number (SMS), or they might be asked to set up responses to challenge questions.

**Note** RSA Adaptive Authentication does not allow for international characters in user names. If you intend to allow multi-byte characters in the user names, contact RSA support to configure RSA Adaptive Authentication and RSA Authentication Manager.

## Configure RSA Adaptive Authentication in Identity Manager

To configure RSA Adaptive Authentication on the service, you enable RSA Adaptive Authentication; select the adaptive authentication methods to apply, and add the Active Directory connection information and certificate.

### Prerequisites

- RSA Adaptive Authentication correctly configured with the authentication methods to use for secondary authentication.
- Details about the SOAP endpoint address and the SOAP user name.
- Active Directory configuration information and the Active Directory SSL certificate available.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup**.
2. On the Connector page, Workers column, select the link for the connector that is being configured.
3. Click **Auth Adapters** and then click **RSAAAIdpAdapter**.

   You are redirected to the identity manager authentication adapter page.
4. Click the **Edit** link next to the RSAAAIdpAdapter.
5. Select the appropriate settings for your environment.

   **Note** An asterisk indicates a required field. The other fields are optional.

| Option | Description |
|---|---|
| ***Name** | A name is required. The default name is RSAAAIdpAdapter. You can change this name. |
| **Enable RSA AA Adapter** | Select the check box to enable RSA Adaptive Authentication. |
| ***SOAP Endpoint** | Enter the SOAP endpoint address for integration between the RSA Adaptive Authentication adapter and the service. |

| Option | Description |
|---|---|
| ***SOAP Username** | Enter the user name and password that is used to sign SOAP messages. |
| **RSA Domain** | Enter the domain address of the Adaptive Authentication server. |
| **Enable OOB Email** | Select this check box to enable out-of-band authentication that sends a onetime passcode to the end user via an email message. |
| **Enable OOB SMS** | Select this check box to enable out-of-band authentication that sends a onetime passcode to the end user via a SMS text message. |
| **Enable SecurID** | Select this check box to enable SecurID. Users are asked to enter their RSA token and passcode. |
| **Enable Secret Question** | Select this check box if you are going to use enrollment and challenge questions for authentication. |
| ***Number Enrollment Questions** | Enter the number of questions the user will need to setup when they enroll in the Authentication Adapter server. |
| ***Number Challenge Questions** | Enter the number of challenge questions users must answer correctly to login. |
| ***Number of authentication attempts allowed** | Enter the number of times to display challenge questions to a user trying to log in before authentication fails. |
| **Type of Directory** | The only directory supported is Active Directory. |
| **Server Port** | Enter the Active Directory port number. |
| **Server Host** | Enter the Active Directory host name. |
| **Use SSL** | Select this check box if you use SSL for your directory connection. You add the Active Directory SSL certificate in the Directory Certificate field. |
| **Use DNS Service Location** | Select this check box if DNS service location is used for directory connection. |
| **Base DN** | Enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. |
| **Bind DN** | Enter the account that can search for users. For example , CN=binduser,OU=myUnit,DC=myCorp,DC=com |
| **Bind Password** | Enter the password for the Bind DN account. |
| **Search Attribute** | Enter the account attribute that contains the username. |
| **Directory certificate** | To establish secure SSL connections, add the directory server certificate to the text box. In the case of multiple servers, add the root certificate of the certificate authority. |

6 Click **Save**.

### What to do next

Enable the RSA Adaptive Authentication auth method in the Built-in identity provider from the Identity & Access Management > Manage tab. See Using Built-in Identity Providers.

Add the RSA Adaptive Authentication auth method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add Adaptive Authentication. See Managing Authentication Methods to Apply to Users.

# Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager

You can configure x509 certificate authentication to allow clients to authenticate with certificates on their desktop and mobile devices or to use a smart card adapter for authentication. Certificate-based authentication is based on what the user has (the private key or smart card), and what the person knows (the password to the private key or the smart-card PIN.) An X.509 certificate uses the public key infrastructure (PKI) standard to verify that a public key contained within the certificate belongs to the user. With smart card authentication, users connect the smart card with the computer and enter a PIN.

The smart card certificates are copied to the local certificate store on the user's computer. The certificates in the local certificate store are available to all the browsers running on this user's computer, with some exceptions, and therefore, are available to a VMware Identity Manager instance in the browser.

**Note** When Certificate Authentication is configured and the service appliance is set up behind a load balancer, make sure that the VMware Identity Manager Connector is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the connector and the client in order to pass the certificate to the connector. When your load balancer is configured to terminate SSL at the load balancer, you can deploy a second connector behind another load balancer to support certificate authentication.

See the VMware Identity Manager Installation and Configuration guide for information about adding a second connector.

## Using User Principal Name for Certificate Authentication

You can use certificate mapping in Active Directory. Certificate and smart card logins uses the user principal name (UPN) from Active Directory to validate user accounts. The Active Directory accounts of users attempting to authenticate in the VMware Identity Manager service must have a valid UPN that corresponds to the UPN in the certificate.

You can configure the VMware Identity Manager to use an email address to validate the user account if the UPN does not exist in the certificate.

You can also enable an alternate UPN type to be used.

## Certificate Authority Required for Authentication

To enable logging in using certificate authentication, root certificates and intermediate certificates must be uploaded to the VMware Identity Manager.

The certificates are copied to the local certificate store on the user's computer. The certificates in the local certificate store are available to all the browsers running on this user's computer, with some exceptions, and therefore, are available to a VMware Identity Manager instance in the browser.

For smart-card authentication, when a user initiates a connection to the VMware Identity Manager instance, the VMware Identity Manager service sends a list of trusted certificate authorities (CA) to the browser. The browser checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user to enter a smart card PIN. If multiple valid user certificates are available, the browser prompts the user to select a certificate.

If a user cannot authenticate, the root CA and intermediate CA might not be set up correctly, or the service has not been restarted after the root and intermediate CAs were uploaded to the server. In these cases, the browser cannot show the installed certificates, the user cannot select the correct certificate, and certificate authentication fails.

## Using Certificate Revocation Checking

You can configure certificate revocation checking to prevent users who have their user certificates revoked from authenticating. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

Certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure both CRL and OCSP in the same certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the Use CRL in case of OCSP failure check box is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL. Revocation checking does not fall back to OCSP if CRL fails.

### Logging in with CRL Checking

When you enable certificate revocation, the VMware Identity Manager server reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked, authentication through the certificate fails.

### Logging in with OCSP Certificate Checking

When you configure Certificate Status Protocol (OCSP) revocation checking, VMware Identity Manager sends a request to an OCSP responder to determine the revocation status of a specific user certificate. The VMware Identity Manager server uses the OCSP signing certificate to verify that the responses it receives from the OCSP responder are genuine.

If the certificate is revoked, authentication fails.

You can configure authentication to fall back to CRL checking if it does not receive a response from the OSCP responder or if the response is invalid.

# Configure Certificate-based Authentication

You can configure x509 certificate authentication to allow clients to authenticate with certificates on their desktop and mobile devices. See Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager.

### Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.
- Consent form content, if a consent form displays before authentication.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup**.
2. On the Connectors page, select the Worker link for the connector that is being configured.
3. Click **Auth Adapters** and then click **CertificateAuthAdapter**.
4. Configure the Certificate Service Auth Adapter page.

**Note** An asterisk indicates a required field. The other fields are optional.

| Option | Description |
|---|---|
| ***Name** | A name is required. The default name is CertificateAuthAdapter. You can change this name. |
| **Enable certificate adapter** | Select the check box to enable certificate authentication. |
| ***Root and intermediate CA certificates** | Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM. |
| **Uploaded CA certificates** | The uploaded certificate files are listed in the Uploaded Ca Certificates section of the form. |
| **Use email if no UPN in certificate** | If the user principal name (UPN) does not exist in the certificate, select this check box to use the emailAddress attribute as the Subject Alternative Name extension to validate users' accounts. |
| **Certificate policies accepted** | Create a list of object identifiers that are accepted in the certificate policies extensions.<br>Enter the object ID numbers (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs. |
| **Enable cert revocation** | Select the check box to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating. |
| **Use CRL from certificates** | Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate the status of a certificate, revoked or not revoked. |

| Option | Description |
|---|---|
| **CRL Location** | Enter the server file path or the local file path from which to retrieve the CRL. |
| **Enable OCSP Revocation** | Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate. |
| **Use CRL in case of OCSP failure** | If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSP checking is not available. |
| **Send OCSP Nonce** | Select this check box if you want the unique identifier of the OCSP request to be sent in the response. |
| **OCSP URL** | If you enabled OCSP revocation, enter the OCSP server address for revocation checking. |
| **OCSP responder's signing certificate** | Enter the path to the OCSP certificate for the responder, */path/to/file.cer*. |
| **Enable consent form before authentication** | Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication. |
| **Consent form content** | Type the text that displays in the consent form in this text box. |

5 Click **Save**.

### What to do next

- Add the certificate authentication method to the default access policy. See Managing Authentication Methods to Apply to Users.
- When Certificate Authentication is configured, and the service appliance is set up behind a load balancer, make sure that the VMware Identity Manager connector is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the connector and the client in order to pass the certificate to the connector.

# Configuring VMware Verify for Two-Factor Authentication

In the VMware Identity Manager admin console, you can enable the VMware Verify service as the second authentication method when two-factor authentication is required.

You enable VMware Verify in the Built-in identity provider in the admin console and add the VMware Verify security token you receive from VMware support.

You configure two-factor authentication in the access policy rules to require users to authenticate using two authentication methods.

Users install the VMware Verify application on their devices and provide a phone number to register their device with the VMware Verify service. The device and phone number are also registered in the User & Groups user profile in the admin console.

Users enroll their account once when they sign in using password authentication first and then enter the VMware Verify passcode that displays on their device. After the initial authentication, users can authenticate through one of these three methods.

- Push approval with OneTouch notification. Users approve or deny access from VMware Identity Manager with one click. Users click either Approve or Deny on the message that is sent.

- Time-based One Time Password (TOTP) passcode. A one-time passcode is generated every 20 seconds. Users enter this passcode on the sign-in screen.
- Text message. Phone SMS is used to send a one-time verification code in a text message to the registered phone number. Users enter this verification code on the sign-in screen.

VMware Verify uses a third-party cloud service to deliver this feature to user devices. To do so, user information such as name, email, and phone number are stored in the service but not used for any purpose other than to deliver the feature.

## Enable VMware Verify

To enable two-factor authentication with the VMware Verify service, you must add a security token to the VMware Verify page and enable VMware Verify in the Built-in Identity provider.

### Prerequisites

Create a support ticket with VMware or AirWatch support to receive the security token that enables VMware Verify. The Support team staff processes your request and updates the support ticket with instructions and a security token. You add this security token to the VMware Verify page.

(Optional) Customize the logo and icon that displays in the VMware Verify application on the devices. See Customize Branding for VMware Verify Application.

### Procedure

1. In the Identity & Access Management tab, go to **Manage > Auth Methods**.
2. In the **VMware Verify** Configure column, click the icon.
3. Paste the security token you received from the VMware or AirWatch support team into the Security Token text box.
4. Select the check box **Enable VMware Verify**.
5. Click **Save**.

### What to do next

Enable VMware Verify as an authentication method in a built-in identity provider. Configure Built-in Identity Providers.

Create an access policy rule in the default access polity to add the VMware Verify authentication method as the second authentication method in the rule. See Managing Authentication Methods to Apply to Users.

Apply custom banding to the VMware Verify sign-in page. See Customize Branding for VMware Verify Application.

## Registering End Users with VMware Verify

When VMware Verify authentication is required for two-factor authentication, users install and use the VMware Verify app to register their device.

**Note** The VMware Verify application can be downloaded from the app stores.

When VMware Verify two-factor authentication is enabled, the first time users sign in to the Workspace ONE app, users are asked to enter their user name and password. When the user name and password are verified, users are prompted to enter their device phone number to enroll in VMware Verify.

When they click Enroll, the device phone number is registered with VMware Verify, and if they have not downloaded the application, they are asked to download the VMware Verify application.

When the application is installed, users are asked to enter the same phone number that was entered before and to select a notification method to receive a one-time registration code. The registration code is entered on the registration pin page.

After the device phone number is registered, users can use a time-based one-time passcode displayed in the VMware Verify application to sign in to Workspace ONE. The passcode is a unique number that is generated on the device and is constantly changing.

Users can register more than one device. The VMware Verify passcode is automatically synchronized to each of the registered devices.

## Remove Registered Phone Number from User Profile

To troubleshoot problems with signing in to Workspace ONE, you can remove the user phone number in the user profile in the VMware Identity Manager admin console.

### Procedure

1. In the admin console, click **Users & Groups**.
2. On the User page, select the user name to reset.
3. In the VMware Verify tab, click **Reset VMware Verify**.

The phone number is removed from the user profile and the User list shows N/A in the VMware Verify Phone number column. The phone number is unregistered from the VMware Verify service. When the user signs in to their Workspace ONE app, they are asked to enter the phone number to enroll in the VMware Verify service again.

# Using Built-in Identity Providers

Built-in identity providers can be configured with authentication methods that do not require the use of an on-premises connector. One built-in identity provider is available in the admin console Identity & Access Management > Identity Providers page. You can create additional built-in identity providers.

You configure the authentication methods from the Identity & Access Management Manage > Auth Methods page. When you configure the built-in identity provider, you associate the authentication methods to use in the built-in identity provider.

You can also configure the built-in identity providers to use authentication methods configured on a connector deployed in outbound-only connection mode. An outbound-only connector does not require the inbound firewall port 443 to be opened. The connector establishes an outbound-only connection (using websockets) with the cloud service, and receives authentication requests over this channel. See VMware Identity Manager Cloud Deployment guide, Deployment Models for more information about deploying an outbound-only connector.

After you associate the authentication methods in the built-in identity providers, you create access policies to apply to these authentication methods.

## Configuring Authentication Methods for Built-In Identity Providers

You configure the authentication methods in the service that can be used in the built-in identity providers. These authentication methods do not require the use of an on-premises connector.

When you configure the built-in identity provider, you enable the authentication methods to use.

The following authentication methods do not require a connector. You enable and configure the authentication methods in the Identity & Access Management Manage > Auth Methods pages and associate the authentication method to a built-in identity provider.

- Mobile SSO for iOS
- Certificate (Cloud Deployment)
- Password using the AirWatch Connector
- VMware Verify for two-factor authentication
- Mobile SSO for Android
- Device Compliance with AirWatch
- Password (Local Directory)

After you enable the authentication methods, you create access policies to apply to these authentication methods.

## Disabling Auth Methods Associated to Built-In Identity Providers

You can disable authentication methods that you configured from the Auth Methods page. When you disable an authentication method, if the authentication method is associated with any identity provider, the authentication method is disabled in that identity provider. The authentication method is also removed as an option in all the access policy rules.

**Caution** If the authentication method you disabled was configured in an access policy rule, the access policy rule must be updated to select another authentication method. If the access policy rule is not updated, users might not be able to sign in to their apps portal or access their resources.

To disable an authentication for specific built-in identity providers, in the built-in identity provider configuration page, deselect the box for the associated authentication method.

## Managing Configuration of Password Authentication to AirWatch

You can review and manage the Password (AirWatch Connector) configuration that was set up when you installed AirWatch and added the VMware Identity Manager service.

The Password (AirWatch Connector) authentication method is managed from the Identity & Access Management > Authentication Methods page and is associated to the built-in identity provider in the Identity Providers page.

**Important** When the AirWatch Cloud Connector software is upgraded, make sure that you update the VMware Identity Manager AirWatch configuration in the VMware Identity Manager admin console AirWatch page.

### Procedure

1. To review and manage the configuration, in the Identity & Access Management tab, select **Authentication Methods**.
2. In the **Password (AirWatch Connector)** Configure column, click the pencil icon.
3. Review the configuration.

| Option | Description |
|---|---|
| **Enable AirWatch Password Authentication** | This check box enables AirWatch password authentication. |
| **AirWatch Admin Console URL** | Pre-populated with the AirWatch URL. |
| **AirWatch API Key** | Pre-populated with the AirWatch Admin API key. |
| **Certificate Used for Authentication** | Pre-populated with the AirWatch Cloud Connector certificate. |
| **Password for Certificate** | Pre-populated with the password for the AirWatch Cloud Connector certificate. |
| **AirWatch Group ID** | Pre-populated with the organization group ID. |

| Option | Description |
| --- | --- |
| **Number of authentication attempts allowed** | The maximum number of failed login attempts when using AirWatch password authentication. No more log ins are allowed after the failed login attempts reach this number. The VMware Identity Manager service tries to use the fallback authentication method if it is configured. The default is five attempts. |
| **JIT Enabled** | If JIT is not enabled, select this check box to enable just-in-time provisioning of users in the VMware Identity Manager service dynamically when they log in the first time. |

4 Click **Save**.

## Enabling Compliance Checking for AirWatch Managed Devices

When users enroll their devices, samples containing data used to evaluate compliance are sent on a scheduled basis. The evaluation of this sample data ensures that the device meets the compliance rules set by the administrator in the AirWatch console. If the device goes out of compliance, corresponding actions configured in the AirWatch console are taken.

The VMware Identity Manager service includes an access policy option that can be configured to check the AirWatch server for device compliance status when users sign in from the device. The compliance check ensures that users are blocked from signing in to an application or using single sign-in to the Workspace ONE portal if the device goes out-of-compliance. When the device is compliant again, the ability to sign in is restored.

The Workspace ONE application automatically signs out and blocks access to the applications if the device is compromised. If the device was enrolled through adaptive management, an enterprise wipe command issued through the AirWatch console unenrolls the device and removes the managed applications from the device. Unmanaged applications are not removed.

For more information about AirWatch compliance policies, see the VMware AirWatch Mobile Device Management Guide, available on the AirWatch Resources website.

### Enable Compliance Checking

In VMware Identity Manager, enable device compliance in the AirWatch configuration page and configure Device Compliance in the Manage > Auth Methods page.

When Device Compliance is configured, the access policy rules can be configured to check the AirWatch server for device compliance status when users sign in form their devices. See Enabling Compliance Checking for AirWatch Managed Devices.

#### Procedure

1 In the administration console Identity & Access Management tab, select **Setup > AirWatch**.

2 In the Device Compliance section, select **Enable** and click **Save**.

3 In the Identity & Access Management tab, go to **Manage > Auth Methods**.

4 In the **Device Compliance (with AirWatch)** Configure column, click the icon.

5 Enable Device Compliance authentication and set the maximum number of failed login attempts. The other text boxes are pre-populated with the configured AirWatch values.

| Option | Description |
|---|---|
| **Enable Device Compliance Adapter** | Select this check box to enable AirWatch password authentication. |
| **AirWatch Admin Console URL** | Pre-populated with the AirWatch URL you set up on the AirWatch configuration page. |
| **AirWatch API Key** | Pre-populated with the AirWatch Admin API key. |
| **Certificate Used for Authentication** | Pre-populated with the AirWatch Cloud Connector certificate |
| **Password for Certificate** | Pre-populated with the password for the AirWatch Cloud Connector certificate. |

6 Click **Save**.

### What to do next

Associate the Device Compliance authentication method in the built-in identity provider. See Configure Built-in Identity Providers.

Configure the default access policy to create rules to use device compliance with AirWatch. See Configure Access Policy Rule.

## Configure the Local Directory Password Authentication Method

Configure password authentication for local directories in the Identity & Access management Manage > Auth Methods page.

After the authentication method is configured, you associate the Password (Local Directory) authentication method in the built-in identity provider associated to the local directory.

### Procedure

1 In the Identity & Access Management tab, go to **Manage > Auth Methods**.

2 In the **Password (Local Directory)** Configure column, click the icon.

3 Select the check box **Enable Local Directory Password Authentication**.

4 In the **Number of password tries** text box enter the maximum number of failed login attempts. No more logins are allowed after the failed login attempts reach this number. The default is five attempts.

5 Click **Save**.

### What to do next

- Associate the Password (Local Directory) authentication method in the built-in identity provider.

## Configure Certificate-based Authentication

You can configure x509 certificate authentication to allow clients to authenticate with certificates on their desktop and mobile devices. See Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager.

### Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.
- Consent form content, if a consent form displays before authentication.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup**.
2. On the Connectors page, select the Worker link for the connector that is being configured.
3. Click **Auth Adapters** and then click **CertificateAuthAdapter**.
4. Configure the Certificate Service Auth Adapter page.

**Note** An asterisk indicates a required field. The other fields are optional.

| Option | Description |
|---|---|
| ***Name** | A name is required. The default name is CertificateAuthAdapter. You can change this name. |
| **Enable certificate adapter** | Select the check box to enable certificate authentication. |
| ***Root and intermediate CA certificates** | Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM. |
| **Uploaded CA certificates** | The uploaded certificate files are listed in the Uploaded Ca Certificates section of the form. |
| **Use email if no UPN in certificate** | If the user principal name (UPN) does not exist in the certificate, select this check box to use the emailAddress attribute as the Subject Alternative Name extension to validate users' accounts. |
| **Certificate policies accepted** | Create a list of object identifiers that are accepted in the certificate policies extensions.<br>Enter the object ID numbers (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs. |
| **Enable cert revocation** | Select the check box to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating. |
| **Use CRL from certificates** | Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate the status of a certificate, revoked or not revoked. |
| **CRL Location** | Enter the server file path or the local file path from which to retrieve the CRL. |
| **Enable OCSP Revocation** | Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate. |
| **Use CRL in case of OCSP failure** | If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSP checking is not available. |
| **Send OCSP Nonce** | Select this check box if you want the unique identifier of the OCSP request to be sent in the response. |

| Option | Description |
|---|---|
| **OCSP URL** | If you enabled OCSP revocation, enter the OCSP server address for revocation checking. |
| **OCSP responder's signing certificate** | Enter the path to the OCSP certificate for the responder, */path/to/file.cer*. |
| **Enable consent form before authentication** | Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication. |
| **Consent form content** | Type the text that displays in the consent form in this text box. |

5 Click **Save**.

### What to do next

- Add the certificate authentication method to the default access policy. See Managing Authentication Methods to Apply to Users.
- When Certificate Authentication is configured, and the service appliance is set up behind a load balancer, make sure that the VMware Identity Manager connector is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the connector and the client in order to pass the certificate to the connector.

## Configuring Mobile SSO for iOS Authentication in VMware Identity Manager

You configure the Mobile SSO for iOS authentication method from the Authentication Methods page in the administration console. Associate the Mobile SSO authentication method to the built-in identity provider.

### Using the Cloud Hosted KDC Service

To support using Kerberos authentication for Mobile SSO for iOS, VMware Identity Manager provides a cloud hosted KDC service.

The KDC service hosted in the cloud must be used when the VMware Identity Manager service is deployed with AirWatch in a Windows environment.

To use the KDC managed in the VMware Identity Manager appliance, see the Preparing to Use Kerberos Authentication on iOS devices in the VMware Identity Manager Installation and Configuration Guide.

When you configure Mobile SSO for iOS authentication, you configure the realm name for the cloud hosted KDC service. The realm is the name of the administrative entity that maintains authentication data. When you click Save, the VMware Identity Manager service is registered with the cloud hosted KDC service. The data that is stored in the KDC service is based on your configuration of the Mobile SSO for iOS authentication method, which includes the CA certificate, the OCSP signing certificate, and the OCSP request configuration details. No other user-specific information is stored in the cloud service.

The logging records are stored in the cloud service. The Personally Identifiable Information (PII) in the logging records include the Kerberos principal name from the user's profile, the subject DN and UPN and EMAIL SAN values, the device ID from the user's certificate, and the FQDN of the IDM service that the user is accessing.

To use the cloud hosted KDC service, VMware Identity Manager must be configured as follows.

- The FQDN of the VMware Identity Manager service must be reachable from the Internet. The SSL/TLS certificate used by VMware Identity Manager must be publically signed.
- An outbound request/response port 88 (UDP) and port 443 (HTTPS/TCP) must be accessible from the VMware Identity Manager service.
- If you enable OCSP, the OCSP responder must be reachable from the Internet.

### Configure Mobile SSO for iOS Authentication

You configure the Mobile SSO for iOS authentication method from the Auth Methods page in the administration console. Select the Mobile SSO (for IOS) authentication method to use in the built-in identity provider.

#### Prerequisites

- Certificate authority PEM or DER file used to issue certificates to users in the AirWatch tenant.
- For revocation checking, the OCSP responder's signing certificate.
- For the KDC service select, the realm name of the KDC service. If using the built-in KDC service, the KDC should be initialized. See the Installing and Configuring VMware Identity Manager for the built-in KDC details.

#### Procedure

1. In the Identity & Access Management tab, go to **Manage > Auth Methods**.
2. In the **Mobile SSO (for iOS)** Configure column, click the icon.
3. Configure the Kerberos authentication method.

| Option | Description |
|---|---|
| **Enable KDC Authentication** | Select this check box to enable users to sign in using iOS devices that support Kerberos authentication. |
| **Realm** | If you are using the cloud hosted KDC, enter the pre-defined supported realm name that is supplied to you. The text in this parameter must be entered in all caps. For example, OP.VMWAREIDENTITY.COM<br>If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays. |
| **Root and Intermediate CA Certificate** | Upload the certificate authority issuer certificate file. The file format can be either PEM or DER. |
| **Uploaded CA Certificate Subject DNs** | The content of the uploaded certificate file is displayed here. More than one file can be uploaded and whatever certificates that are included are added to the list. |
| **Enable OCSP** | Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate. |
| **Send OCSP Nonce** | Select this check box if you want the unique identifier of the OCSP request to be sent in the response. |
| **OCSP Responder’s Signing Certificate** | Upload the OCSP certificate for the responder.<br>When you are using the AirWatch Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the AirWatch certificate here as well. |

| Option | Description |
|---|---|
| **OCSP Responder's Signing Certificate Subject DN** | The uploaded OCSP certificate file is listed here. |
| **Enable Cancel Link** | When authentication is taking too long, give the user the ability to click Cancel to stop the authentication attempt and cancel the sign-in.<br>When the Cancel link is enabled, **Cancel** appears at the end of the authentication error message that displays. |
| **Cancel Message** | Create a custom message that displays when the Kerberos authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials.` |

4 Click **Save**.

### What to do next

- Associate the Mobile SSO (for iOS) authentication method in the built-in identity provider.
- Configure the default access policy rule for Kerberos authentication for iOS devices. Make sure that this authentication method is the first method set up in the rule.
- Go to the AirWatch admin console and configure the iOS device profile in AirWaAirWatchtch and add the KDC server certificate issuer certificate from VMware Identity Manager.

## Configure Mobile SSO for Android Authentication in the Built-in Identity Provider

To provide single sign-on from AirWatch-managed Android devices, you configure Mobile SSO for Android authentication in the VMware Identity Manager built-in identity provider.

### Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.

### Procedure

1 In the administration console, Identity & Access Management tab, select **Manage > Identity Providers**.

2 Click the identity provider labeled **Built-in**.

3 Verify that the Users and Network configuration in the built-in identity provider is correct.

If it is not, edit the Users and Network sections as needed.

**Note** The network range that you use in the policy rule for Mobile SSO for Android should consist of only the IP addresses used to receive requests coming from the VMware Tunnel proxy server.

4 In the Authentication Methods section, click the **Mobile SSO (for Android devices)** gear icon.

5 In the CertProxyAuthAdapter page configure the authentication method.

| Option | Description |
|---|---|
| **Enable Certificate Adapter** | Select this check box to enable Mobile SSO for Android. |
| **Root and Intermediate CA Certificate** | Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded. The file format can be either PEM or DER. |
| **Uploaded CA Certificate Subject DNs** | The contents of the uploaded certificate file is displayed here. |
| **Use email if no UPN in certificate** | If the user principal name (UPN) does not exist in the certificate, select this check box to use the emailAddress attribute as the Subject Alternative Name extension to validate user accounts. |
| **Certificate policies accepted** | Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID number (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs. |
| **Enable Cert Revocation** | Select the check box to enable certificate revocation checking. This prevents users who have revoked user certificates from authenticating. |
| **Use CRL from certificates** | Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate a certificate's status of revoked or not revoked. |
| **CRL Location** | Enter the server file path or the local file path from which to retrieve the CRL. |
| **Enable OCSP Revocation** | Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate. |
| **Use CRL in case of OCSP failure** | If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSAP checking is not available. |
| **Send OCSP Nonce** | Select this check box if you want the unique identifier of the OCSP request to be sent in the response. |
| **OCSP URL** | If you enabled OCSP revocation, enter the OCSP server address for revocation checking. |
| **OCSP Responder's Signing Certificate** | Enter the path to the OCSP certificate for the responder. Enter as `/path/to/file.cer` |

6 Click **Save**.

7 Click **Save** on the built-in identity provider page.

### What to do next

Configure the default access policy rule for Mobile SSO for Android.

## Configure Built-in Identity Providers

You can configure multiple built-in identity providers and associate authentication methods that have been configured in the Identity & Access Management Manage > Auth Methods page.

### Procedure

1 In the Identity & Access Management tab, go to **Manage > Identity Providers**.

2 Click **Add Identity Provider**, and select **Create Built-in IDP**.

| Option | Description |
|---|---|
| **Identity Provider Name** | Enter the name for this built-in identity provider instance. |
| **Users** | Select which users to authentication. The configured directories are listed. |
| **Network** | The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication. |
| **Authentication Methods** | The authentication methods that are configured on the service are displayed. Select the check box for the authentication methods to associate to this built-in identity provider.<br>For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page. |

3 Click **Add**.

### What to do next

Configure the default access policy rule to add the authentication policy to the rule. See Configure Access Policy Rule

## Using Outbound Connector for Authentication in Built-in Identity Providers

A built-in identity provider can be configured to service authentication methods that do not require a connector installed behind a firewall. The connector is installed in outbound connection mode and does not require the inbound firewall port 443 to be opened.

The connector establishes an outbound-only connection (using websockets) with the cloud service, and receives authentication requests over this channel.

Authentication methods that are configured on a connector deployed behind the DMZ in an outbound-only connection mode can be associated to the identity provider when you configure a built-in identity provider.

The following connector authentication methods can be configured.

- Password (cloud deployment)
- RSA Adaptive Auth (cloud deployment)
- RSA SecurID (cloud deployment)
- RADIUS (cloud deployment)

After you configure the authentication methods, you then must create access policies to apply to these authentication methods.

# Configure a Built-in Identity Provider with Authentication Methods Configured on an Outbound-Only Connector

Authentication methods that are configured on a connector deployed behind the DMZ in an outbound-only connection mode can be associated to the built-in identity provider when you configure the built-in identity provider.

### Prerequisites

- Users and groups located in an enterprise directory must be synced to VMware Identity Manager Directory.
- List of the network ranges that you want to direct to the built-in identity provider instance for authentication.
- To enable authentication methods from the built-in identity provider, make sure that the authentication methods are configured in the connector.

### Procedure

1. In the Identity & Access Management tab, go to **Manage > Identity Providers**.
2. Select the identity provider labeled Built-in and configure the identity provider details.

| Option | Description |
|---|---|
| **Identity Provider Name** | Enter the name for this built-in identity provider instance. |
| **Users** | Select which users to authentication. The configured directories are listed. |
| **Network** | The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication. |
| **Authentication Methods** | The authentication methods that are configured in the Identity & Access Management Manage > Auth Methods page are displayed. Select the check box for the authentication methods to associate to the identity provider.<br>For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page. |
| **Connector(s)** | Select the connector that is configured in outbound-only connection mode. |
| **Connector Authentication Methods** | Authentication methods configured on the connector are listed in this section. Select the check box to associate the authentication methods. |

3. If you are using Built-in Kerberos authentication, download the KDC issuer certificate to use in the AirWatch configuration of the iOS device management profile.
4. Click **Save**.

# Configure Additional Workspace Identity Providers

When the VMware Identity Manager connector is initially configured, when you enable the connector to authenticate users, a Workspace IDP is created as the identity provider and password authentication is enabled.

Additional connectors can be configured behind different load balancers. When your environment includes more than one load balancer, you can configure a different Workspace identity provider for authentication in each load balanced configuration. See the Installing Additional Connector Appliances topics in the Installing and Configuring VMWare Identity Manager Guide.

The different Workspace identity providers can be associated with the same directory or if you have multiple directors configured, you can select which directory to use.

### Procedure

1. In the administration console, Identity & Access Management tab, select **Manage > Identity Providers**.
2. Click **Add Identity Provider** and select **Create Workspace IDP**.
3. Edit the identity provider instance settings.

| Option | Description |
|---|---|
| **Identity Provider Name** | Enter a name for this Workspace identity provider instance. |
| **Users** | Select the VMware Identity Manager directory of the users who can authenticate using this Workspace identity provider. |
| **Connector(s)** | Connectors that are not associated with the directory you selected are listed. Select the connector to associate to the directory. |
| **Network** | The existing network ranges configured in the service are listed.<br>Select the network ranges for the users based on their IP addresses that you want to direct to this identity provider instance for authentication. |

4. Click **Add**.

# Configuring a Third-Party Identity Provider Instance to Authenticate Users

You can configure a third-party identity provider that is used to authenticate users in the VMware Identity Manager service.

Complete the following tasks before using adding the third-party identity provider instance.

- Verify that the third-party instances are SAML 2.0 compliant and that the service can reach the third-party instance.
- Obtain the appropriate third-party metadata information to add when you configure the identity provider in the administration console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

# Add and Configure an Identity Provider Instance

By adding and configuring identity provider instances for your VMware Identity Manager 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.

### Prerequisites

- Configure the network ranges that you want to direct to this identity provider instance for authentication. See Add or Edit a Network Range.
- Access to the third-party metadata document. This can be either the URL to the metadata or the actual metadata.

### Procedure

1. In the admin console Identity & Access Management tab select **Identity Providers**.
2. Click **Add Identity Provider**.
3. Edit the identity provider instance settings.

| Form Item | Description |
|---|---|
| Identity Provider Name | Enter a name for this identity provider instance. |
| SAML Binding | Select how the AuthnRequest should be sent, either HTTP POST or HTTP Redirect<br>HTTP Redirect is the default. |
| SAML Metadata | Add the third-party identity provider XML-based metadata document to establish trust with the identity provider.<br>1 Enter the SAML metadata URL or the xml content into the text box.<br>2 Click **Process IdP Metadata**. The NameID formats supported by the IdP are extracted from the metadata and added to the Name ID Format table.<br>3 In the Name ID value column, select the user attribute in the service to map to the ID formats displayed. You can add custom third-party name ID formats and map them to the user attribute values in the service.<br>4 (Optional) Select the NameIDPolicy response identifier string format. |
| Just-in-Time Provisioning | N/A |
| Users | Select the **Other Directory** which includes the users who can authenticate using this identity provider. |
| Network | The existing network ranges configured in the service are listed.<br>Select the network ranges for the users based on their IP addresses, that you want to direct to this identity provider instance for authentication. |
| Authentication Methods | Add the authentication methods supported by the third-party identity provider. Select the SAML authentication context class that supports the authentication method. |

| Form Item | Description |
|---|---|
| Single Sign-Out Configuration | Enable single sign-out to log users out of their identity provider session when they sign out. If single sign-out is not enabled, when users sign out, their identity provider session is still active.<br>(Optional) If the identity provider supports the SAML single logout profile, enable single sign-out and leave the **Redirect URL** text box blank. If the identity provider does not support the SAML single logout profile, enable single sign-out and enter the sign-out URL of the identity provider where users are redirected to when they sign out from VMware Identity Manager.<br>If you configured the redirect URL and if you want users to return to the VMware Identity Manager sign-in page after being redirected to the identity provider sign-out URL, enter the parameter name used by the identity provider redirect URL. |
| SAML Signing Certificate | Click **Service Provider (SP) Metadata** to see URL to VMware Identity Manager SAML service provider metadata URL. Copy and save the URL. This URL is configured when you edit the SAML assertion in the third-party identity provider to map VMware Identity Manager users. |
| IdP Hostname | If the Hostname text box displays, enter the host name where the identity provider is redirected to for authentication. If you are using a non-standard port other than 443, you can set the host name as Hostname:Port. For example, myco.example.com:8443. |

4 Click **Add**.

### What to do next

- Edit the third-party identity provider's configuration to add the SAML Signing Certificate URL that you saved.

# Managing Authentication Methods to Apply to Users

The VMware Identity Manager service attempts to authenticate users based on the authentication methods, the default access policy, network ranges, and the identity provider instances you configure.

When users attempt to log in, the service evaluates the default access policy rules to select which rule in the policy to apply. The authentication methods are applied in the order they are listed in the rule. The first identity provider instance that meets the authentication method and network range requirements of the rule is selected. The user authentication request is forwarded to the identity provider instance for authentication. If authentication fails, the next authentication method configured in the rule is applied.

You can add rules that specify the authentication methods to be used by either the device type or by the device type and from a specific network range. For example, you might configure a rule that requires users who sign in using iOS devices from a specific network to authenticate using RSA SecurID. Then configure another rule that requires users who sign in using any type of device from the internal network IP address to authenticate using their password.

# Add or Edit a Network Range

Create network ranges to define the IP addresses from which users can log in. You add the network ranges you create to specific identity provider instances and to access policy rules.

One network range, called ALL RANGES, is created as the default. This network range includes every IP address available on the Internet, 0.0.0.0 to 255.255.255.255. If your deployment has a single identity provider instance, you can change the IP address range and add other ranges to exclude or include specific IP addresses to the default network range. You can create other network ranges with specific IP addresses that you can apply for a specific purpose.

**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

- Define network ranges for your VMware Identity Manager deployment based on your network topology.

### Procedure

1. In the administration console Policies tab, select **Network Ranges**.
2. Edit an existing network range or add a new network range.

| Option | Description |
|---|---|
| **Edit an existing range** | Click the network range name to edit. |
| **Add a range** | Click **Add Network Range** to add a new range. |

3. Edit the Add Network Range page.

| Form Item | Description |
|---|---|
| Name | Enter a name for the network range. |
| Description | Enter a description for the network range. |
| 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.
- Associate network ranges with an access policy rule as appropriate. See Chapter 6 Managing Access Policies.

# Applying the Default Access Policy

The VMware Identity Manager service includes a default access policy that controls user access to their Workspace ONE portals and their Web applications. You can edit the policy to change the policy rules as necessary.

When you enable authentication methods other than password authentication, you must edit the default policy to add the enabled authentication method to the policy rules.

Each rule in the default access policy requires that a set of criteria be met to allow user access to the applications portal. You apply a network range, select which type of user can access content, and select the authentication methods to use. See Chapter 6 Managing Access Policies.

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

## Apply Authentication Methods to Policy Rules

Only the password authentication method is configured in the default policy rules. You must edit the policy rules to select the other authentication methods you configured and set the order in which the authentication methods are used for authentication.

See Configuring Access Policy Settings to learn more about setting up policy rules.

### Prerequisites

Enable and configure the authentication methods that your organization supports. See Chapter 5 Configuring User Authentication in VMware Identity Manager.

### Procedure

1. In the administration console Identity & Access Management tab, select **Manage > Policies**.
2. Click the default access policy to edit.
3. In the Policy Rules section, click the authentication method to edit, or to add a new policy rule, click the **+** icon.
   a. Verify that the network range is correct. If adding a new rule, select the network range for this policy rule.
   b. Select the device that this rule manages from the **and the user is trying to access content from** drop-down menu.

c If you this access rule is going to apply to specific groups, click **Edit Groups** and select the groups.

If you do not select a group, the access policy applies to all users.

d Configure the authentication order. In the **then the user must authenticate using the following method** drop-down menu, select the authentication method to apply first.

To require users to authenticate through two authentication methods, click **+** and in the drop-down menu select a second authentication method.

e (Optional) To configure additional fallback authentication methods, in the **If preceding Authentication Method fails, then:** drop-down menu, select another enabled authentication method.

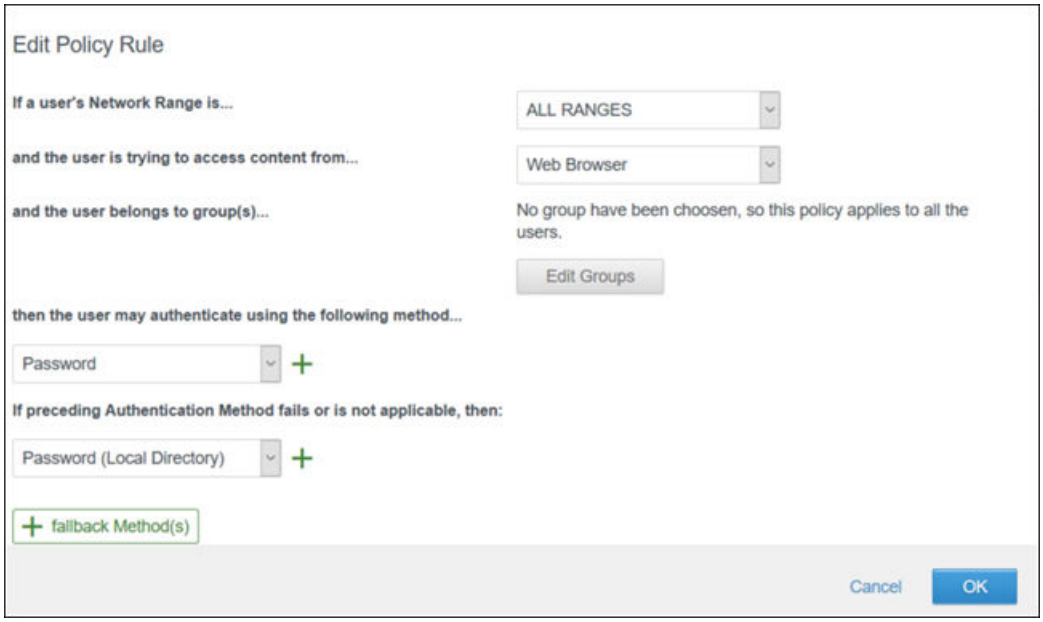
You can add multiple fallback authentication methods to a rule.

f In the **Re-Authenticate after** drop-down menu, select length of the session, after which users must authenticate again.

g (Optional) Create a custom access denied message that displays when user authentication fails. You can use up to 4000 characters, which is about 650 words. If you want to send users to another page, in the **Link URL** text box, enter the URL link address. In the **Link text** text box, enter the text that should display as the link. If you leave this text box blank, the word `Continue` displays.

h Click **Save**.

4 Click **Save**.



# Managing Access Policies

6

To provide secure access to the users' apps portal and to launch Web and desktop applications, you configure access policies. Access policies include rules that specify criteria that must be met to sign in to their apps portal and to use their resources.

Policy rules map the requesting IP address to network ranges and designate the type of devices that users can use to sign in. The rule defines the authentication methods and the number of hours the authentication is valid. You can select one or more groups to associate with the access rule.

The VMware Identity Manager service includes a default policy that controls access to the service as a whole. This policy is set up to allow access to all network ranges, from all device types, for all users. The session timeout is eight hours and the authentication method is password authentication. You can edit the default policy.

**Note** The policies do not control the length of time that an application session lasts. They control the amount of time that users have to launch an application.

This section includes the following topics:



## Configuring Access Policy Settings

A policy contains one or more access rules. Each rule consists of settings that you can configure to manage user access to their Workspace ONE portal as a whole or to specific Web and desktop applications.

A policy rule can be configured to take actions such as block, allow, or step-up authenticate users based on conditions such as network, device type, AirWatch device enrollment and compliant status, or application being accessed You can add groups to a policy to manage authentication for specific groups.

## Network Range

For each rule, 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 Identity & Access Management tab, Setup > Network Ranges page before configuring access policy sets.

Each identity provider instance in your deployment links network ranges with authentication methods. When you configure a policy rule, ensure that the network range is covered by an existing identity provider instance.

You can configure specific network ranges to restrict from where users can log in and access their applications.

## Device Type

Select the type of device that the rule manages. The client types are Web Browser, Workspace ONE App, iOS, Android, Windows 10, OS X, and All Device Types.

You can configure rules to designate which type of device can access content and all authentication requests coming from that type of device use the policy rule.

## Add Groups

You can apply different policies for authentication based on user's group membership. To assign groups of users to log in through a specific authentication flow, you can add groups to the access policy rule. Groups can be groups that are synced from your enterprise directory and local groups that you created in the admin console. Group names must be unique within a domain.

To use groups in access policy rules, you select a unique identifier from the Identity & Access Management > Preferences page. The unique identifier attribute must be mapped in the User Attributes page and the selected attribute synced to the directory. The unique identifier can be the user name, email address, UPN, or employee ID. See Login Experience Using Unique Identifier.

When groups are used in an access policy rule, the user login experience for the user changes. Instead of asking users to select their domain and then enter their credentials, a page displays prompting them to enter their unique identifier. VMware Identity Manager finds the user in the internal database, based on the unique identifier and displays the authentication page configured in that rule.

When a group is not select, the access policy rule applies to all users. When you configure access policy rules that include rules based on groups and a rule for all users, make sure that the rule designated for all users is the last rule listed in the Policy Rules section of the policy.

## Authentication Methods

In the policy rule, you set the order that authentication methods are applied. The authentication methods are applied in the order they are listed. The first identity provider instance that meets the authentication method and network range configuration in the policy is selected. The user authentication request is forwarded to the identity provider instance for authentication. If authentication fails, the next authentication method in the list is selected.

## Authentication Session Length

For each rule, you set the number of hours that this authentication is valid. The **re-authenticate after** value determines the maximum time users have since their last authentication event to access their portal or to start a specific application. For example, a value of 4 in a Web application rule gives users four hours to start the Web application unless they initiate another authentication event that extends the time.

## Custom Access Denied Error Message

When users attempt to sign in and fail because of invalid credentials, misconfiguration or system error, an access denied message is displayed. The default message is `Access denied as no valid authentication methods were found.`

You can create a custom error message for each access policy rule that overrides the default message. The custom message can include text and a link for a call to action message. For example, in a policy rule for mobile devices that you want to manage, if a user tries to sign in from an unenrolled device, you can create the following custom error message. `Enroll your device to access corporate resources by clicking the link at the end of this message. If your device is already enrolled, contact support for help.`

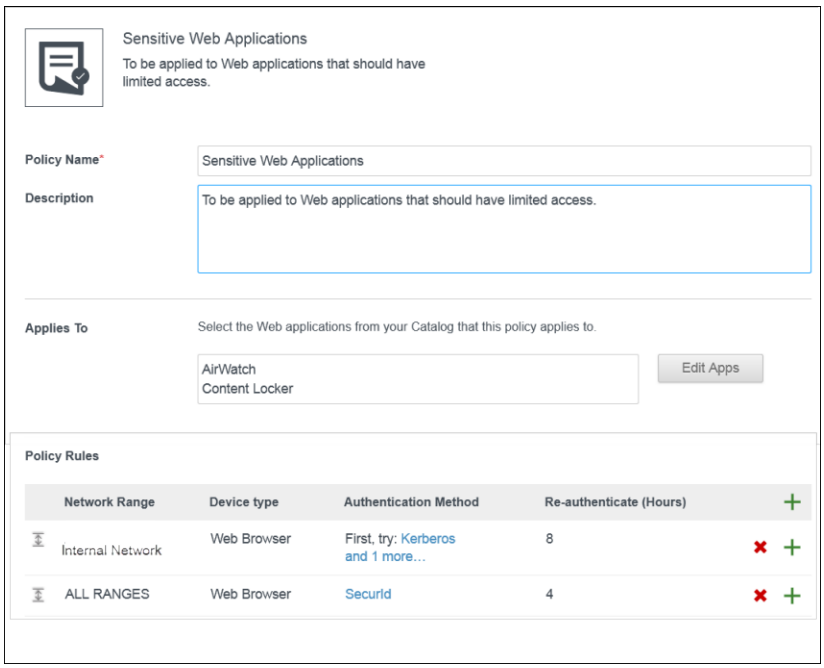
# Managing Web and Desktop Application-Specific Policies

When you add Web and desktop applications to the catalog, you can create application-specific access policies. For example, you can create a policy with rules 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.

The following Web-application-specific policy provides an example of a policy you can create to control access to specified Web applications.

## Example 1 Strict Web-Application-Specific Policy

In this example, a new policy is created and applied to a sensitive Web application.




1 To access the service from outside the enterprise network, the user is required to log in with RSA SecurID. The user signs in using a browser and now has access to the apps portal for a four-hour session as provided by the default access rule.

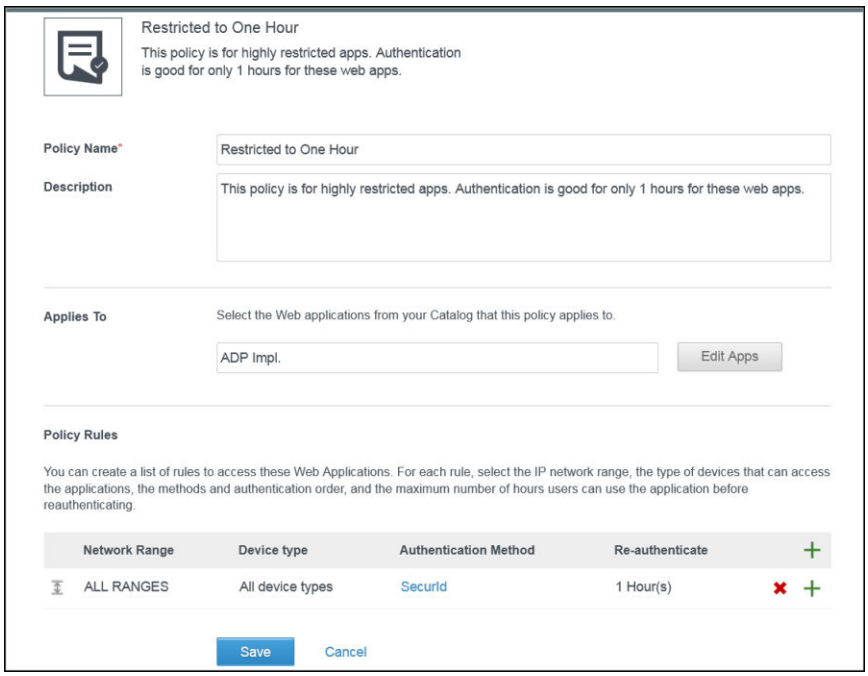
2 After four hours, the user tries to start a Web application with the Sensitive Web Applications policy set applied.

3 The service checks the rules in the policy and applies the policy with the ALL RANGES network range because the user request is coming from a Web browser and from the ALL RANGES network range.

   The user signed in with the RSA SecurID authentication method, but the session just expired. The user is redirected for reauthentication. The reauthentication provides the user with another four-hour session and the ability to start the application. For the next four hours, the user can continue to run the application without having to reauthenticate.

## Example 2 Stricter Web-Application-Specific Policy

For a stricter rule to apply to extra sensitive Web applications, you could require reauthentication with SecurId on any device after one hour. The following is an example of how this type of a policy access rule is implemented.




1 User logs in from inside the enterprise network using the Kerberos authentication method.

   Now, the user can access the apps portal for eight hours, as set up in Example 1.

2 The user immediately tries to start a Web application with the Example 2 policy rule applied, which requires RSA SecurID authentication.

3 The user is redirected to RSA SecurID authentication sign-in page.

4 After the user successfully signs in, the service launches the application and saves the authentication event.

   The user can continue to run this application for up to one hour but is asked to reauthenticate after an hour, as dictated by the policy rule.

# Add a Web or Desktop Application-Specific Policy

You can create application-specific policies to manage user access to specific Web and desktop applications.

### Prerequisites

- Configure the appropriate network ranges for your deployment. See Add or Edit a Network Range.
- Configure the appropriate authentication methods for your deployment.

- If you plan to edit the default policy (to control user access to the service as a whole), configure it before creating an application-specific policy.
- Add the web and desktop application to the catalog. At least one application must be listed in the Catalog page before you can add an application-specific policy.

To add access policies for legacy authentication for Office 365 clients, you configure the client access policies in the Office 365 application from the Catalog page. See the VMware Identity Manager Integration with Office 365 guide.

### Procedure

1. In the administration console Identity & Access Management tab, select **Manage > Policies**.
2. Click **Add Policy**.
3. Add a policy name and description in the respective text boxes.
4. In the **Applies To** section, click **Select** and in the page that appears, select the applications to associate with this policy.
5. In the Policy Rules section, click **+** to add a rule.

   The Add a Policy Rule page appears.

   a. Select the network range to apply to this rule.

   b. Select the type of device that can access the applications for this rule.

   c. Select the authentication methods to use in the order the authentication method should be applied.

   d. Specify the number of hours an application session can be open.

   e. Click **Save**.
6. Configure additional rules as appropriate.
7. Click **Save**.

## Configure Custom Access Denied Error Message

For each policy rule, you can create a custom access denied error message that displays when users attempt to sign in and fail because their credentials are invalid.

The custom message can include text and a link to another URL to help users resolve their issues. You can use up to 4000 characters, which is about 650 words.

### Procedure

1. In the administration console Identity & Access Management tab, select **Manage > Policies**.
2. Click the access policy to edit.
3. To open a policy rule page, click the authentication name in the Authentication Method column for the rule to be edited.

4 In the **Custom error message** text box, type the error message.

5 To add a link to a URL, in the **Link text** box enter a description of the link and in **Link URL** enter the URL.

The link is displayed at the end of the custom message. If you do not add text in the Link text box but add a URL, the text link that displays is

```
Continue.
```

6 Click **Save**.

### What to do next

Create custom error messages for other policy rules.

# Edit Default Access Policy

You can edit the default access policy to change the policy rules, and you can edit application-specific policies to add or remove applications and to change policy rules.

You can remove an application-specific access policy at anytime. The default access policy is permanent. You cannot remove the default policy.

### Prerequisites

- Configure the appropriate network ranges for your deployment. See Add or Edit a Network Range.

### Procedure

1 In the administration console Policies tab, select **Edit Default Policy**.

2 In the Policy Rules section, Authentication Method column, select the rule to edit.

The Edit a Policy Rule page appears with the existing configuration displayed.

3 To configure the authentication order, in the **then the user must authenticate using the following method** drop-down menu, select the authentication method to apply first.

4 (Optional) To configure a fallback authentication method if the first authentication fails, select another enabled authentication method from the next drop-down menu.

You can add multiple fallback authentication methods to a rule.

5 Click **Save** and click **Save** again on the Policy page.

The edited policy rule takes effect immediately.

### What to do next

If the policy is an application-specific access policy, you can also apply the policy to applications from the Catalog page. See Add a Web or Desktop Application-Specific Policy

# Enabling Compliance Checking for AirWatch Managed Devices

When users enroll their devices, samples containing data used to evaluate compliance are sent on a scheduled basis. The evaluation of this sample data ensures that the device meets the compliance rules set by the administrator in the AirWatch console. If the device goes out of compliance, corresponding actions configured in the AirWatch console are taken.

The VMware Identity Manager service includes an access policy option that can be configured to check the AirWatch server for device compliance status when users sign in from the device. The compliance check ensures that users are blocked from signing in to an application or using single sign-in to the Workspace ONE portal if the device goes out-of-compliance. When the device is compliant again, the ability to sign in is restored.

The Workspace ONE application automatically signs out and blocks access to the applications if the device is compromised. If the device was enrolled through adaptive management, an enterprise wipe command issued through the AirWatch console unenrolls the device and removes the managed applications from the device. Unmanaged applications are not removed.

For more information about AirWatch compliance policies, see the VMware AirWatch Mobile Device Management Guide, available on the AirWatch Resources website.

## Configure Access Policy Rule

To provide secure access to the users' Workspace ONE app portal and to launch Web and desktop applications, you configure access policies. Access policies include rules that specify criteria that must be met to sign in and to use their resources.

You must edit the default policy rules to select the authentication methods you configured. A policy rule can be configured to take actions such as block, allow, or authenticate users based on conditions such as network, device type, AirWatch device enrollment and compliant status, or application being accessed. You can add groups to a policy to manage authentication for specific groups.

When Compliance Check is enabled, you create an access policy rule that requires authentication and device compliance verification for devices managed by AirWatch.

The compliance checking policy rule works in an authentication chain with Mobile SSO for iOS, Mobile SSO for Android, and Certificate cloud deployment. The authentication method to use must precede the device compliance option in the policy rule configuration.

#### Prerequisites

Authentication methods configured and associated to a built-in identity provider.

Compliance checking enabled in the VMware Identity Manager AirWatch page.

#### Procedure

1 In the Identity & Access Management tab, go to **Manage > Policies**.

2 Select the access policy to edit.

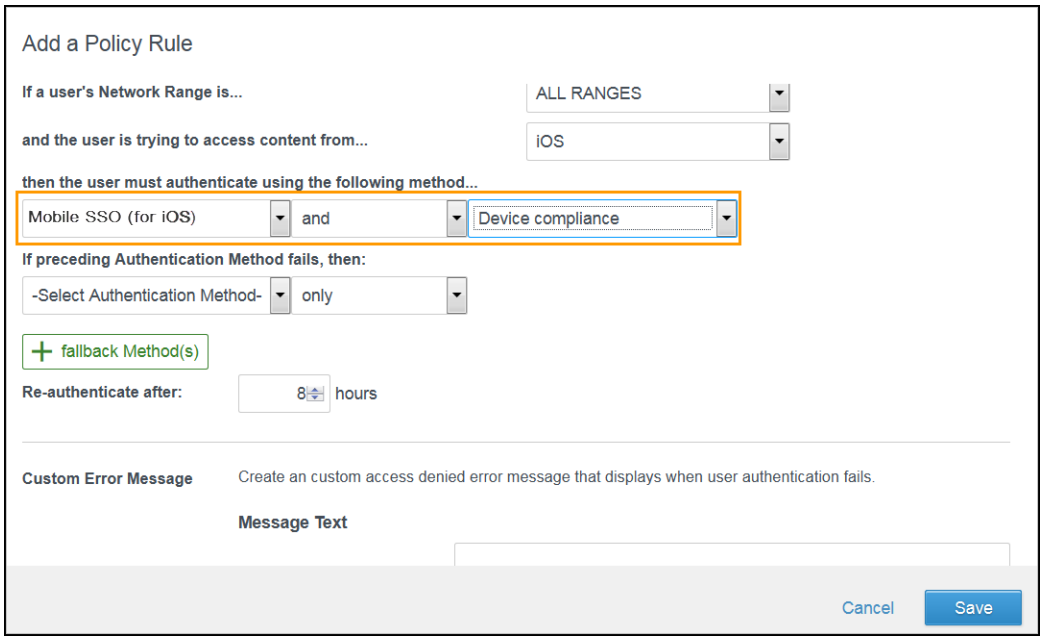
3 In the Policy Rules section, select the policy rule to edit.

4 In the drop-down menu for **then the user must authenticate using the following method**, click **+** and select the authentication method to use.

5 In the second drop-down menu for **then the user must authenticate using the following method**, select **Device Compliance (with AirWatch)**.

6 (Optional) In the Custom Error **Message Text** text box, create a custom message that displays when user authentication fails because of the device is not compliant. In the **Custom Error Link** text box, you can add a link in the message.

7 Click **Save**.




# Enabling Persistent Cookie on Mobile Devices

Enable persistent cookie to provide single sign-in between the system browser and native apps and single sign-in between native apps when apps use Safari View Controller on iOS devices and Chrome Custom Tabs on Android devices.

The persistent cookie stores users' sign-in session details so that users do not need to reenter their user credentials when they access their managed resources through VMware Identity Manager. The cookie timeout can be configured in the access policy rules you set up for iOS and Android devices.

**Note** Cookies are vulnerable and susceptible in common browser cookie-theft and cross site script attacks.

# Enable Persistent Cookie

The persistent cookie stores users' sign-in session details so that users do not need to reenter their user credentials when accessing their managed resources from their iOS or Android mobile devices.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup > Preferences**.
2. Check **Enable Persistent Cookie**.
3. Click **Save**.

### What to do next

To set the persistent cookie session timeout, edit the re-authentication value in the access policy rules for the iOS and Android devices types.

# Managing Users and Groups

7

Users and groups in the VMware Identity Manager service are imported from your enterprise directory or are created as local users and groups in the VMware Identity Manager administration console.

In the administration console, the Users & Groups pages provides a user-and-group-centric view of the service. You can manage users and groups entitlements, group affiliations, and VMware Verify phone numbers. For local users, you also can manage the password policies.

This section includes the following topics:



## User and Group Types

Users in the VMware Identity Manager service can be users that are synced from your enterprise directory, local users that you provision in the admin console, or users created with just-in-time provisioning.

Groups in the VMware Identity Manager service can be groups that are synced from your enterprise directory and local groups that you create in the admin console.

Users and groups imported from your enterprise directory are updated in the VMware Identity Manager directory according to your server synchronization schedule. You can view the user and group accounts from the User & Groups pages. You cannot edit or delete these users and groups.

You can create local users and groups. Local users are added to a local directory. You manage the local user attribute mapping and password policies. You can create local groups to manage resource entitlements for users.

Users created with just-in-time provisioning are created and updated dynamically when the user logs in, based on SAML assertions sent by the identity provider. All user management is handled through SAML assertions. To use just-in-time provision, see Chapter 3 Just-in-Time User Provisioning.

# About User Names and Group Names

In the VMware Identity Manager service, users and groups are identified uniquely by both their name and domain. This allows you to have multiple users or groups with the same name in different Active Directory domains. User names and group names must be unique within a domain.

## User Names

The VMware Identity Manager service supports having multiple users with the same name in different Active Directory domains. User names must be unique within a domain. For example, you can have a user jane in domain eng.example.com and another user jane in domain sales.example.com.

Users are identified uniquely by both their user name and domain. The userName attribute in VMware Identity Manager is used for user names and is typically mapped to the sAMAccountName attribute in Active Directory. The domain attribute is used for domains and is typically mapped to the canonicalName attribute in Active Directory.

During directory sync, users that have the same user name but different domains are synced successfully. If there is a user name conflict within a domain, the first user is synced and an error occurs for subsequent users with the same user name.

**Note** If you have an existing VMware Identity Manager directory in which the user domain is incorrect or missing, check the domain settings and sync the directory again. See Sync Directory to Correct Domain Information.

In the admin console, you can identify users uniquely by both their user name and domain. For example:

- In the Dashboard tab Users and Groups column, users are listed as user (domain). For example, jane (sales.example.com).
- In the Users & Groups tab, Users page, the DOMAIN column indicates the domain to which the user belongs.
- Reports that display user information, such as the Resource Entitlements report, include a DOMAIN column.

When end users log in to the user portal, on the login page they select the domain to which they belong. If multiple users have the same user name, each can log in successfully using the appropriate domain.

**Note** This information applies to users synced from Active Directory. If you use a third-party identity provider and have configured Just-in-Time user provisioning, see Chapter 3 Just-in-Time User Provisioning for information. Just-in-Time user provisioning also supports multiple users with the same user name in different domains.

## Group Names

The VMware Identity Manager service supports having multiple groups with the same name in different Active Directory domains. Group names must be unique within a domain. For example, you can have a group called ***allusers*** in the domain eng.example.com and another group called ***allusers*** in the domain sales.example.com.

Groups are identified uniquely by both their name and domain.

During directory sync, groups that have the same name but different domains are synced successfully. If there is a group name conflict within a domain, the first group is synced and an error occurs for subsequent groups with the same name.

In the admin console User & Groups tab, the Groups page, Active Directory groups are listed by their group name and domain. This lets you distinguish between groups that have the same name. Groups that are created locally in the VMware Identity Manager service are listed by the group name. The domain is listed as Local Users.

## Sync Directory to Correct Domain Information

If you have an existing VMware Identity Manager directory in which the user domain is incorrect or missing, you must check the domain settings and sync the directory again. Checking the domain settings is required so that users or groups that have the same name in different Active Directory domains are synced to the VMware Identity Manager directory successfully and users can log in.

#### Procedure

1. In the admin console, go to the **Identity & Access Management > Directories** page.
2. Select the directory to sync, then click **Sync Settings** and click the **Mapped Attributes** tab.
3. In the Mapped Attributes page, verify that the VMware Identity Manager attribute **domain** is mapped to the correct attribute name in Active Directory.

   The domain attribute is typically mapped to the canonicalName attribute in Active Directory.

   The domain attribute is not marked Required.
4. Click **Save & Sync** to sync the directory.

# Managing Users

The Users page in the admin console shows users that are enabled to sign in to Workspace ONE.

Select a user name to see detailed user information.

## User Profile

The user profile page displays the personal data associated with the user and the assigned role, either User or Admin. User information that syncs from an external directory can also include the principal name, distinguished name, and external ID data. A local user's profile page displays the available user attributes for users in the local user's directory.

The data in the user profile page for users that sync from your external directory cannot be edited. You can change the role of the user.

# Create Groups and Configure Group Rules

You can create groups, add members to groups, and create group rules that allow you to populate groups based on rules you define.

Use groups to entitle more than one user to the same resources at the same time, instead of entitling each user individually. 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 policy settings apply to the members of a group. Users in groups are defined by the rules you set for a user attribute. If a user's attribute value changes from the defined group rule value, the user is removed from the group.

### Procedure

1. In the administration console, Users & Groups tab, click **Groups**.
2. Click **Add Group**.
3. Enter a group name and description of the group. Click **Next**.
4. To add users to the group, enter the letters of the user name. As you enter text, a list of names that match is displayed.
5. Select the user name and click **+Add user**.

   Continue to add members to the group.
6. After the users are added to the group, click **Next**.

7 In the Group Rules page, select how group membership is granted. In the drop-down menu, select either **any** or **all**.

| Option | Action |
| --- | --- |
| **Any** | Grants group membership when any of the conditions for group membership are met. This action works like an OR condition. For example, if you select **Any** for the rules **Group Is Sales** and **Group Is Marketing**, sales and marketing staff are granted membership to this group. |
| **All** | Grants group membership when all the conditions for group membership are met. Using All 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 is not granted membership. |

8 Configure one or more rules for your group. You can nest rules.

| Option | Description |
| --- | --- |
| **Attribute** | Select one of these attributes from the first column drop-down menu. Select Group to add an existing group to the group you are creating. You can add other types of attributes to manage which users in the groups are members of the group you create. |
| **Attribute Rules** | The following rules are available depending on the attribute you selected.<br>■ Select **is** to select a group or directory to associate with this group. Enter a name in the text box. As you type, a list of the available groups or directories appears.<br>■ Select **is not** to select a group or directory to exclude. Enter a name in the text box. As you type, a list of the available groups or directories appears.<br>■ Select **matches** to grant group membership to entries that exactly match the criteria you enter. For example, your organization might have a business travel department that shares a central phone number. If you want to grant access to a travel booking application for all employees who share that phone number, you create a rule such as Phone matches (555) 555-1000.<br>■ 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.<br>■ Select **starts with** to grant group membership for directory server entries that start with the criteria you enter. For example, the 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 n your sales staff, you can create a rule, such as email starts with sales_.<br>■ Select **does not start with** to grant group membership to all directory server entries except those that begin 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. |
| **Using Attribute Any or All** | (Optional) To include the attributes Any or All as part of the group rule, add this rule last.<br>■ Select **Any**for group membership to be granted when any of the conditions for group membership are met for this rule. Using Any 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. |

| Option | Description |
| --- | --- |
| | ■ Select **All** for all 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 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. |

9 (Optional) To exclude specific users, enter a user name in the text box and click **Exclude user**.

10 Click **Next** and review the group information. Click **Create Group**.

### What to do next

Add the resources that the group is entitled to use.

# Edit Group Rules

You can edit group rules to change the group name, add and remove users, and change the group rules.

### Procedure

1 In the administration console, click **Users & Groups > Groups**.

2 Click the group name to edit.

3 Click **Edit Users in Group**.

4 Click through the pages to make the changes to the name, users in the group, and rules.

5 Click **Save**.

# Add Resources to Groups

The most effective way to entitle users to resources is to add the entitlements to a group. All members of the group can access the applications that are entitled to the group.

### Prerequisites

Applications are added to the Catalog page.

### Procedure

1 In the administration console, click **Users & Groups > Groups**.

The page displays a list of the groups.

2 To add resources to a group, click the group name.

3 Click the **Apps** tab and then click **Add Entitlement**.

4 Select the type of application to entitle from the drop-down menu.

   The application types shown in the drop-down is based on the types of applications that are added to the catalog.

5 Select the applications to entitle to the group. You can search for a specific application or you can check the box next to **Applications** to select all displayed applications.

   If an application is already entitled to the group, the application is not listed.

6 Click **Save**.

The applications are listed on the Apps page and users in the group are immediately entitled to the resources.

# Create Local Users

You can create local users in the VMware Identity Manager service to add and manage users who are not provisioned in your enterprise directory. You can create different local directories and customize the attribute mapping for each directory.

You create a directory and select attributes and create custom attributes for that local directory. The required user attributes userName, lastName, firstName, and email are specified at the global level in the Identity & Access Management > User Attributes page. In the local directory user attribute list, you can select other required attributes and create custom attributes to have custom sets of attributes for different local directories. See Using Local Directories in the Installing and Configuring VMware Identity Manager guide.

Create local users when you want to let users access your applications but do not want to add them to your enterprise directory.

- You can create a local directory for a specific type of user that is not part of your enterprise directory. For example, you can create a local directory for partners, who are not usually part of your enterprise directory, and provide them access to only the specific applications they need.
- You can create multiple local directories if you want different user attributes or authentication methods for different sets of users. For example, you can create a local directory for distributors that has user attributes labeled region and market size. You create another local directory for suppliers that has user attribute labeled product category.

You configure the authentication method local users use to sign in to your enterprise Web site. A password policy is enforced for the local user password. You can define the password restrictions and password management rules.

After you provision a user, an email message is sent with information about how to sign in to enable their account. When they sign in, they create a password and their account is enabled.

## Add Local Users

You create one user at a time. When you add the user, you select the local directory that is configured with the local user attributes to use and the domain that the user signs in to.

In addition to adding user information, you select the user role, either as user or admin. The admin role allows the user to access the administration console to manage the VMware Identity Manager services.

### Prerequisites

- Local directory created
- Domain identified for local users
- User attributes that are required selected in the local directory User Attributes page
- Password policies configured
- SMTP server configured in the Appliance Settings tab to send an email notification to newly created local users

### Procedure

1. In the administration console Users & Groups tab, click **Add User**.
2. In the **Add a user page**, select the local directory for this user.

   The page expands to display the user attributes to configure.
3. Select the domain that this user is assigned to and complete the required user information.
4. If this user role is as an admin, in the User text box, select **Admin**.
5. Click **Add**.

The local user is created. An email is sent to the user asking them to sign in to enable their account and create a password. The link in the email expires according to the value set in the Password Policy page. The default is seven days. If the link expires, you can click Rest Password to resend the email notification.

A user is added to existing groups based on the group attribute rules that are configured.

### What to do next

Go the local user account to review the profile, add the user to groups, and entitle the user to the resources to use.

If you created an admin user in the system directory who is entitled to resources that are managed by a specific access policy, make sure that the application policy rules include Password (Local Directory) as a fallback authentication method. If Password (Local Directory) is not configured, the admin cannot sign in to the app.

## Disable or Enable Local Users

You can disable local users to prevent users from signing in and accessing their portal and entitled resources rather than deleting them.

### Procedure

1. In the administration console, click **Users & Groups**.

2 In the Users page, Select the user.

   The User Profile page appears.

3 Depending on the status of the local user, do one of the following.

   a To disable the account, deselect the Enable check box

   b To enable the account, select Enable.

Disabled users cannot sign in to the portal or to resources they were entitled to. If they are working in an entitled resource when the local user is disabled, the local user can access the resource until the session times out.

## Delete Local Users

You can delete local users.

**Procedure**

1 In the administration console, click **Users & Groups**.

2 Select the user to delete.

   The User Profile page appears.

3 Click **Delete User**.

4 In the confirmation box, click **OK.**

   The user is removed from the Users list.

Deleted users cannot sign in to the portal or to resources they were entitled to.

# Managing Passwords

You can create a password policy to manage local user passwords. Local users can change their password according to the password policy rules.

Local users can change their password from the Workspace ONE portal, in the Account selection from the drop-down menu by their name.

## Configure Password Policy for Local Users

The local user password policy is a set of rules and restrictions on the format and expiration of the local user passwords. The password policy applies only to local users that you created from the VMware Identity Manager admin console.

The password policy can include password restrictions, a maximum lifetime of a password, and for password resets, the maximum lifetime of the temporary password.

The default password policy requires six characters. The password restrictions can include a combination of uppercase, lowercase, numerical, and special characters to require strong passwords be set.

### Procedure

1 In the administration console, select **Users & Groups > Settings**

2 Click **Password Policy** to edit the password restriction parameters.

| Option | Description |
|---|---|
| **Minimum length for passwords** | Six characters is the minimum length, but you can require more than six characters. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements. |
| **Lowercase characters** | Minimum number of lowercase characters. Lowercase a-z |
| **Uppercase characters** | Minimum number of uppercase characters. Uppercase A-Z |
| **Numerical characters (0-9)** | Minimum number of numerical characters. Base ten digits (0-9) |
| **Special characters** | Minimum number of non-alphanumeric characters, for example & # % $ ! |
| **Consecutive identical characters** | Maximum number of identical adjacent characters. For example, if you enter 1, the following password is allowed: p@s$word, but this password is not allowed: p@$$word. |
| **Password history** | Number of the previous passwords that cannot be selected. For example, if a user cannot reuse any of the last six passwords, type 6. To disable this feature, set the value to 0. |

3 In the **Password Management** section, edit the password lifetime parameters.

| Option | Description |
|---|---|
| **Temporary password lifetime** | Number of hours a password reset or forgot password link is valid. The default is 168 hours |
| **Password lifetime** | Maximum number of days that a password can exist before the user must change it. |
| **Password reminder** | Number of days before a password expiration that the password expiry notice is sent. |
| **Password reminder notification frequency** | After the first password expiry notice is sent, how frequently reminders are sent. |

Each box must have a value to set up the password lifetime policy. To not set a policy option, enter 0.

4 Click **Save**.

# Managing the Catalog

8

The Catalog is the repository of all the resources that you can entitle to users. You add applications to the Catalog directly from the Catalog tab. To see the applications added to the catalog, click the **Catalog** tab in the administration 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.

Web applications can be added to your catalog directly from the Catalog page.

Other resource types require you to take action outside the administration console. See the *Setting Up Resources in VMware Identity Manager* for information about setting up resources.

| Resource | How to See the Resource in Your Catalog |
|---|---|
| Web application | In the admin console Catalog page, select the **Web Applications** application type. |
| Virtualized Windows application captured as a ThinApp package | Sync ThinApp packages to your catalog from the administration console, Packaged Apps - ThinApp page. In the admin console Catalog page, select the **ThinApp Packages** application type. |
| VMware Horizon HTML Access Desktop Pool | Sync View Pools to your catalog from the administration console, View Pools page. In the admin console Catalog page, select the **View Desktop Pools** application type. |
| Horizon Hosted Applications | Sync View Hosted Applications to your catalog from the administration console, View Pools page. In the admin console Catalog page, select the **View Hosted Application** as the application type. |
| Citrix-based application | Sync Citrix-based applications to your catalog from the administration console, Published Apps - Citrix page. In the admin console Catalog page, select the **Citrix Published Applications** application type. |

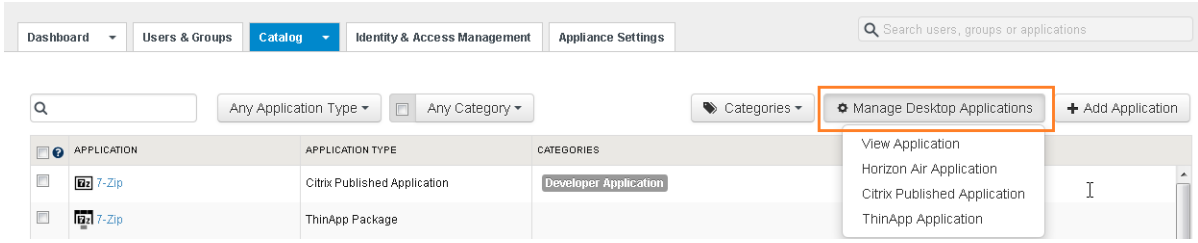
This section includes the following topics:

# Managing Resources in the Catalog

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.

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, Horizon Client desktop pools and Horizon virtual applications, or Citrix-based applications.

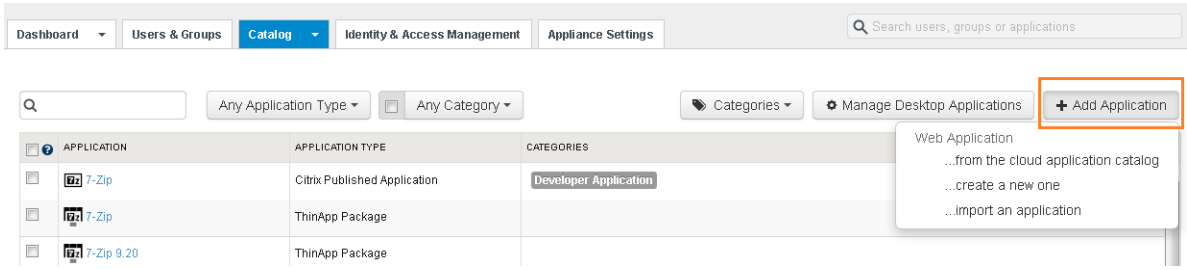
To integrate and enable Horizon Client desktop and application pools, Citrix-published resources, or ThinApp packaged applications, you use the Manage Desktop Applications menu in the Catalog tab.




For information, requirements, installation and configuration of these resources, see *Setting Up Resources in VMware Identity Manager*.

## Adding Web Applications to Your Catalog

You can add Web applications to your catalog directly using the Catalog page in the administration console.




See *Setting Up Resources in VMware Identity Manager*, 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 In the administration console, click the **Catalog** tab.

2 Click **+ Add Application**.

3 Click an option depending on the resource type, and the location of the application.

| Link Name | Resource Type | Description |
|---|---|---|
| **Web Application ...from the cloud application catalog** | Web application | VMware Identity Manager includes access to 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. You might want to use this method to roll a 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. |

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

## Add Web Applications to your Catalog

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

### Procedure

1 In the administration console, click the **Catalog** tab.

2 Click **Add Application > Web Application ...from the cloud application catalog**.

3 Click the icon of the Web application you want to add.

The application record is added to your catalog, and the Details page appears with the name and authentication profile already specified.

4 (Optional) Customize the information on the Details page for your organization's needs.

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

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

| Form Item | Description |
|---|---|
| **Name** | The name of the application. |
| **Description** | A description of the application that users can read. |
| **Icon** | Click **Browse** to upload an icon for the application. Icons in PNG, JPG, and ICON file formats, up to 4MB, are supported.<br>The app icons that you upload must be a minimum of 180 x 180 pixels. If the icon is too small, the icon does not display. The Workspace ONE icon displays instead. |
| **Categories** | To allow the application to appear in a category search of catalog resources, select a category from the drop-down menu. You must have created the category earlier. |

5 Click **Save**.

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

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

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

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

| Tab | Description |
|---|---|
| **Entitlements** | Entitle users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future. |
| **Access Policies** | Apply an access policy to control user access to the application. When you add the Office 365 with Provisioning application to the catalog, you can configure client access policies that control user access to Office 365 services that use the legacy authentication flow. See the VMware Identity Manager Integration with Office 365 guide. |
| **Licensing** | Configure approval tracking. Add license information for the application to track license use in reports. Approvals must be enabled and configured in the Catalog > Settings page. You must also register the callback URI of the approval request handler. |
| **Provisioning** | Provision a Web application to retrieve specific information from the VMware Identity Manager service. If provisioning is configured for a Web application, when you entitle a user to the application, the user is provisioned in the Web Application. Currently, a provisioning adapter is available for Google Apps and Office 365. Go to VMware Identity Manager Integrations at https://www.vmware.com/support/pubs/vidm_webapp_sso.html for configuration guides for these applications. |

## Adding Horizon 7 Desktop and Hosted Applications

You populate your catalog with Horizon 7 desktop pools and hosted applications, and you integrate your VMware Identity Manager deployment with Horizon 7.

When you click Horizon 7 Application from the Catalog > Manage Desktop Applications menu, you are redirected to the Horizon 7 Pools page. Select **Enable Horizon 7 Pools** to add pods, perform a directory sync for Horizon 7, and configure the type of deployment the service uses to extend Horizon 7 resources entitlements to users.

After you perform these tasks, the Horizon 7 desktops and hosted applications that you entitled to users with Horizon are available as resources in your catalog.

You can return to the page at any time to modify the configuration or to add or remove pods.

For detailed information about integrating Horizon 7 with VMware Identity Manager, refer to Providing Access to Horizon 7 Desktops in the Setting Up Resource guide.

## Adding Citrix Published Applications

You can use VMware Identity Manager to integrate with existing Citrix deployments and then populate your catalog with Citrix-based applications.

When you click Citrix Published Application from the Catalog > Manage Desktop Applications menu, you are redirected to the Published Apps - Citrix page. Select Enable Citrix-based Applications to establish communication and schedule the synchronization frequency between VMware Identity Manager and the Citrix server farm.

For detailed information about integrating Citrix-published applications with VMware Identity Manager, see Providing Access to Citrix-Published Resources in the Setting Up Resources guide.

## Adding Horizon Cloud Applications

You can enable Horizon Cloud desktops and applications in VMware Identity Manager service.

When you click Horizon Cloud Application from the Catalog > Manage Desktop Applications menu, you are redirected to the Horizon Cloud Resources page. Select Enable Horizon Cloud Desktops and Applications to configure Horizon Cloud for VMware Identity Manager and set up the sync schedule.

# Grouping Resource into Categories

You can organize resources into logical categories to make it easier for users to locate the resource they need in their Workspace ONE portal workspace.

When you create categories consider the structure of your organization, the job function of the resources, and type of resource. You can assign more than one category to a resource. For example, you might create a category called Text Editor and another category called Recommended Resources. Assign Text Editor to all the text editor resources in your catalog. Also assign Recommended Resources to a specific text editor resource you would prefer your users to use.

## Create a Resource Category

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

### Procedure

1. In the administration console, click the **Catalog** tab.
2. To create and apply categories at the same time, select the check boxes of the applications to which to apply the new category.
3. Click **Categories**.
4. Enter a new category name in the text box.
5. Click **Add category...**.

   A new category is created, but not applied to any resource.

6 To apply the category to the selected resources, select the check box for the new category name.

The category is added to the application and is listed in the Categories column.

### What to do next

Apply the category to other applications . See Apply a Category to Resources.

## Apply a Category to Resources

After you create a category, you can apply that category to any of the resources in the catalog. You can apply multiple categories to the same resource.

### Prerequisites

Create a category.

### Procedure

1 In the administration console, click the **Catalog** tab.

2 Select the check boxes of all the applications to which to apply the category.

3 Click **Categories** and select the name of the category to apply.

The category is applied to the selected applications.

## Remove a Category from an Application

You can disassociate a category from an application.

### Procedure

1 In the administration console, click the **Catalog** tab.

2 Select the check boxes of applications to remove a category.

3 Click **Categories**.

The categories that are applied to the applications are checked.

4 Deselect the category to be removed from the application and close the menu box.

The category is removed from the application's Categories list.

## Delete a Category

You can permanently remove a category from the catalog.

### Procedure

1 In the administration console, click the **Catalog** tab.

2 Click **Categories**.

3 Hover over the category to be deleted. An x appears. Click the **x**.

4 Click **OK** to remove the category.

The category no longer appears in the Categories drop-down menu or as a label to any application to which you previously applied it.

# Managing Catalog Settings

The Catalog Settings page can be used to manage resources in the catalog, download a SAML certificate, customize the user portal, and set global settings.

## SAML Signing Certificates

SAML signing certificates ensure that messages are coming from the expected identity and service providers. The SAML certificate is used to sign SAML requests, responses, and assertions from the service to relying applications, such as WebEx or Google Apps.

The Catalog > Settings SAML Metadata page displays the SAML signing certificate and includes links for the SAML Identity Provider and Service Provider metadata files. The metadata includes configuration information and the certificates.

A self-signed certificate is automatically created in the VMware Identity Manager service for SAML signing. If your organization requires a certificate from a certificate authority, you can generate a Certificate Signing Request (CSR) from the admin console and use the CSR for generating a certificate. When you receive the signed certificate, you upload the certificate to the VMware Identity Manager service, replacing the self-signed certificate. The SAML signing certificate and the SAML metadata files are updated with the new certificate.

### Download SAML Certificates to Configure with Relying Applications

You copy the SAML signing certificate and the SAML service provider metadata from the service and edit the SAML assertion in the third-party identity provider to map VMware Identity Manager users.

#### Procedure

1 In the administration console Catalog tab, select **Settings > SAML Metadata**.

   a Copy the certificate information that is in the Signing Certificate section.

2 Make the SAML SP metadata available to the third-party identity provider instance.

   a On the Download SAML Certificate page, click **Service Provider (SP) metadata**.

   b Copy and save the displayed information using the method that best suits your organization.

      Use this copied information later when you configure the third-party identity provider.

3 Determine the user mapping from the third-party identity provider instance to VMware Identity Manager.

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

| NameID Format | User Mapping |
|---|---|
| **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** | The NameID value in the SAML assertion is mapped to the email address attribute in VMware Identity Manager. |
| **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** | The NameID value in the SAML assertion is mapped to the username attribute in VMware Identity Manager. |

### What to do next

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

## Generate a Certificate Signing Request

To use an external certificate for SAML signing, you must generate a Certificate Signing Request (CSR) from the admin console. The CSR is sent to a certificate authority to generate the SSL certificate.

**Note** A certificate generated without the CSR from the admin console is not supported.

### Procedure

1 In the Catalog tab, select **Settings > SAML Metadata**.

2 Click **Generate CSR**

3 Enter the requested information. Options with an asterisk (*) are required.

| Option | Description |
|---|---|
| **Common Name*** | Enter the fully qualified domain name. For example, `www.example.com` |
| **Organization*** | Enter the legally registered name of the organization. For example, `Mycompany, Inc.` |
| **Department** | Enter the department in your company that is added in the certificate. For example, `IT Services`. |
| **City*** | Enter the city where your organization is legally located. |
| **State/Province*** | Enter the state or region where your organization is located. Do not abbreviate. |
| **Country*** | Enter a few letters of your country name to select the correct country from the list. |
| **Key Generation Algorithm*** | Select the secure hash algorithm used to sign the CSR. |
| **Key Size*** | Select the number of bits used in the key. RSA 2048 is recommended. RSA key size smaller than 2048 is considered insecure. |

4 Click **Generate**.

Give the CSR to the certificate authority to create the certificate.

### What to do next

When you receive the certificate, upload the certificate to the VMware Identity Manager service. The CA replaces the self-signed certificate.

## Upload a New Certificate Authority for SAML Signing Certificates

After the signed certificate is issued, upload the file from the Catalog SAML Metadata page and restart the service to update the metadata.

### Prerequisites

Generate the Certificate Signing Request.

Save the signed certificate that you receive to a file that you can access from the admin console.

### Procedure

1. In the Catalog tab, select **Settings > SAML Metadata**.
2. Click **Generate CSR**.
3. Click **Upload Certificate** and navigate to the certificate.
4. Click **Open**.

   The SAML signing certificate and the SAML metadata files are updated with the new certificate.
5. Go to the Identity & Access Management tab, **Setup > Connectors** and click **Restart**.

   The metadata is updated in the connector.

### What to do next

**Important** Reconfigure all SAML service provider and identity provider configurations with the updated SAML metadata file. This includes reconfiguring additional connector that are configured. If this is not done, SAML transactions fail and single sign-on does not work.

# Disable Prompt for Downloading Helper Applications

View desktops, Citrix published apps, and ThinApp resources require the following helper applications be installed on the users' computers or device.

- View desktops use Horizon Client.
- Citrix-published apps require Citrix Receiver.
- ThinApp resources require VMware Identity Manager for Desktops.

Users are asked to download helper applications to their desktop or device the first time they launch applications from these resources types. You can completely disable this prompt from displaying each time the resource is launched from the Catalog > Settings > Global Settings page.

Disabling the prompt from display is a good option when computers or devices are managed, and you know the helper applications are on the user's local image.

**Procedure**

1. In the administrator console, select **Catalog > Settings**.
2. Select **Global Settings**.
3. Select the operating systems that should not ask to launch the helper applications.
4. Click **Save**.

# Creating Client to Enable Access to Remote Applications

You can create a single client to enable a single application to register with VMware Identity Manager to allow user access to a specific application enabled in the Catalog > Settings page.

You can also create a template to enable a group of clients to register dynamically with VMware Identity Manager service to allow access to specified applications.

The initial user authentication request follows the authentication flow defined in the OIDC spec.

## Managing Access Token Time to Live

The access token provides temporary secure access to the application. Access tokens have a limited lifetime. When you create the client credentials, the access token is configured with a time to live (TTL). The time configured is the maximum time that the access token is valid for use within an application.

If users frequently use an application, such as Workspace ONE, you can configure the client credentials not to require these users to have to log in every time the access token expires.

Enable Issue Refresh Token so that when the access token expires, the application uses the refresh token to request a new access token. The refresh token is configured with a TTL. New access tokens can be requested until the refresh token expires. When the refresh token expires, the user must log in to the application.

You can configure how long a refresh token can be idle before it cannot be used again. If the refresh token is not used by the refresh token idle TTL, users must log in to the application again.

## Example: How Access Token Time to Live Works

The access token time-to-live (TTL) settings in the client credentials are configured as follows.

- Access Token TTL is set to nine hours
- Refresh Token TTL is set to three months
- Refresh Token Idle TTL is set to seven days

If the user uses the application every day, the user does not need to log in again for three months, based on the Refresh Token TTL setting. However, if the user is idle and does not use the application for seven days, the user would need to log in after seven days, based on the Refresh Token idle TTL setting.

## Set up Remote Access to a Single Catalog Resource

You can create a client to enable a single application to register with VMware Identity Manager services to allow user access to a specific application.

Registering the details of the application identifies the application as a trusted client for the OAuth service.

You register the client ID, client secret, and a redirect URI with VMware Identity Manager service.

### Procedure

1. In the administration console Catalog tab, select **Settings > Remote App Access**.
2. On the Clients page, click **Create Client**.
3. On the Create Client page, enter the following information about the application.

| Label | Description |
|---|---|
| Access Type | Options are User Access Token or Service Client Token. Set to **Service Client Token**. This indicates that the application accesses the APIs on its own behalf, not on behalf of a user. |
| Client ID | Enter a unique client identifier for the application to use to authenticate to VMware Identity Manager. The client id must not match any client id in your tenant. The following characters can be used, alphanumeric (A-Z, a-z, 0-9) period (.), underscore (_), and hyphen (-) and at sign (@). |
| Application | Select Identity Manager. |
| Scope | Select the information that the token contains. When you select NAAPS, OpenID is also selected. |
| Redirect URI | Enter the registered redirect URI. |
| Advanced Section | Click **Advanced**. |
| Shared Secret | Click **Generate Shared Secret** to generate a secret that is shared between this service and the application resource service.<br>Copy and save the client secret to configure in the application setup.<br>The client secret must be kept confidential. If a deployed app cannot keep the secret confidential, then the secret is not used. The shared secret is not used with Web browser-based applications. |
| Issue Refresh Token | To use refresh tokens, leave this option enabled. |
| Token Type | Select Bearer. This attribute tells the application what type of access token it was given. For VMware Identity Manager, the tokens are bearer tokens. |
| Access Token TTL | The access token expires in the number of seconds set in**Access Token Time-To-Live**. If Issue Refresh Token is enabled, when the access token expires, the application uses the refresh token to request a new access token. |
| Refresh Token TTL | Set the Refresh Token time to live. New access tokens can be requested until the refresh token expires. |
| Idle Token TTL | Configure how long a refresh token can be idle before it cannot be used again. |
| User Grant | Do not check **Prompt users for access**. |

4. Click **Add**.

The client configuration is displayed on the OAuth2 Client page.

### What to do next

In the resource application, configure the Client ID and the generated shared secret. See the application documentation.

## Create Remote Access Template

You can create a template to enable a group of clients to register dynamically with the VMware Identity Manager service to allow users access to a specific application.

### Procedure

1 In the administration console Catalog tab, select **Settings > Remote App Access**.

2 Click **Templates**.

3 Click **Create Template**.

4 On the Create Template page, enter the following information about the application.

| Label | Description |
|---|---|
| Template ID | Enter a unique name that identifies this template. |
| Application | Select Identity Manager |
| Scope | Select the information that the token contains. When you select NAAPS, OpenID is also selected. |
| Redirect URI | Enter the registered redirect URI. |
| Advanced Section | Click **Advanced**. |
| Token Type | Select Bearer. This attribute tells the application what type of access token it was given. For VMware Identity Manager, the tokens are bearer tokens. |
| Token Length | Leave the default setting, 32 Bytes. |
| Issue Refresh Token | To use refresh tokens, leave this option enabled. |
| Access Token TTL | Set the access token time to live length. The access token expires based on the TTL set in**Access Token Time-To-Live**. If Issue Refresh Token is enabled, when the access token expires, the application uses the refresh token to request a new access token. |
| Refresh Token TTL | Set the Refresh Token time to live. New access tokens can be requested until the refresh token expires. |
| Idle Token Time-to-Live (TTL) | Configure how long a refresh token can be idle before it cannot be used again. |
| User Grant | Do not check Prompt users for access. |

5 Click **Add**.

### What to do next

In the resource application, set up the VMware Identity Manager service URL as the site that supports integrated authentication.

## Editing ICA Properties in Citrix Published Applications

You can edit the settings for individual Citrix-published applications and desktops in your VMware Identity Manager deployment from the Catalog > Settings > Citrix Published Application pages.

The ICA Configuration page is configured for individual applications. The ICA properties text boxes for individual applications are empty until you manually add properties. When you edit the application delivery settings, the ICA properties, of an individual Citrix-published resource, those settings take precedence over the global settings.

In the NetScaler Configuration page, you can configure the service with the appropriate settings so that when users launch Citrix based applications, the traffic is routed through NetScaler to the XenApp server.

When you edit the ICA properties in the Citrix Published Applications > Netscaler ICA Configuration tab, the settings apply to application launch traffic that is routed through NetScaler.

For information about configuring ICA properties, see the Configuring NetScaler topic and the Editing VMware Identity Manager Application Delivery Settings for a Single Citrix-Published Resource topic in the documentation center.

## Enabling Application Approval for Resource Usage

You enable Approvals from the Catalog Settings page and configure licensing in the application to manage access to applications that require approval from your organization.

When the licensing option is configured, users view the application in their Workspace ONE catalog and request use of the application. The application icon display a Pending notification

VMware Identity Manager sends the approval request message to the organization's configured approval REST endpoint URL. The server workflow process reviews the request and sends back an approved or denied message to VMware Identity Manager. When an application is approved Pending is changed to Added and the application displays in the user's Workspace ONE launcher page.

Two approval engines are available.

- REST API. The REST API approval engine uses an external approval tool that routes through your Webserver REST API to perform the request and approval responses. You enter your REST API URL in th eVMware Identity Manager service and configure your REST APIs with the VMware Identity Manager OAuth client credential values and the callout request and response action.
- REST API via Connector. The REST API via Connector approval engine routes the callback calls through the connector using the Websocket-based communication channel. You configure your REST API endpoint with the callout request and response action.....

You can view the VMware Identity Manager resource usage and resource entitlements reports to see the number of approved applications being used.

## Set up the REST API Approval Engine

You can register your callout REST URI to integrate your application management system with VMware Identity Manager.

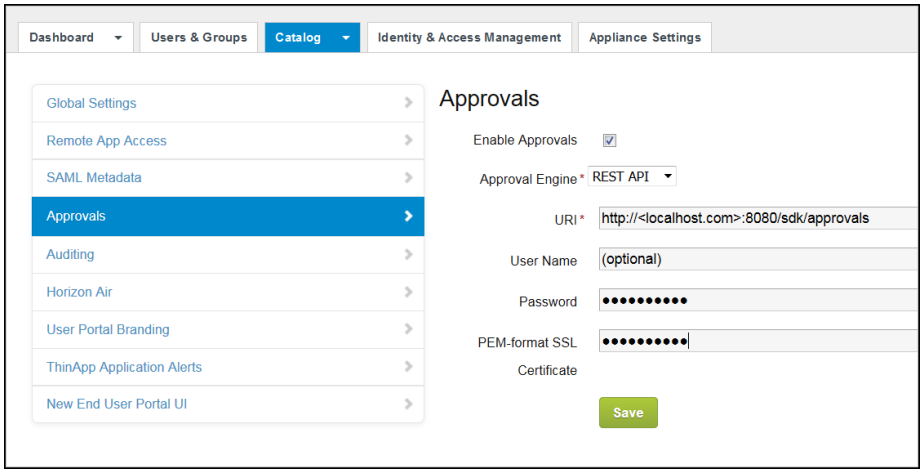
### Prerequisites

When you select the REST API approval engine, your application management system must be configured, and the URI available through the callout REST API that receives the requests from VMware Identity Manager.

### Procedure

1. In the administration console Catalog tab, select **Settings > Approvals**.
2. Check **Enable Approvals**.
3. In the Approval Engine drop-down menu, select **REST API**.
4. Configure the following text boxes.

| Option | Description |
|---|---|
| **URI** | Enter the callback URI of the REST resource that listens for the callout request. |
| **User Name** | (Optional) If the REST API requires a user name and password to access, enter the name here. If no authentication is required, you can leave user name and password blank. |
| **Password** | (Optional) Enter the password of the user. |
| **PEM-format SSL Certificate** | (Optional) If your REST resource is running on a server that has a self-signed certificate or a certificate not trusted by a public certificate authority and is using HTTPS, add the SSL certificate in PEM format here. |




### What to do next

Go to the Catalog page and configure the Licensing feature for those apps that require approval before users can use the app.

# Working in the Administration Console Dashboard

9

Two dashboards are available in the administration console. The User Engagement dashboard can be used to monitor users and resource usage. The System Diagnostics dashboard can be used to monitor the health of the VMware Identity Manager service.

This section includes the following topics:



## Monitor Users and Resource Usage from the Dashboard

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 VMware Identity Manager. The most recent users that logged in are displayed first. 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 grouped by app type of the number of times that apps were launched 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. Expand the 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. Expand the arrow on the right to select to view this information over a day, a week, a month or 12 weeks.
- The Clients section shows the number of Identity Manager Desktops being used.

# Monitor System Information and Health

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

From the System Diagnostics Dashboard you can select the virtual machine that you want to monitor and see the status of the services on that virtual machine, including the version of VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager appliance that is installed.
- Application Manager - Application Deployment Status. The VMware Identity Manager Appliance connection status is displayed.

- Connector - Application Deployment Status. The administration console connection status is displayed. When Connection successful is displayed, you can access the administration console pages.
- VMware Identity Manager FQDN. Shows the fully qualified domain name that users enter to access their VMware Identity Manager App portal. The VMware Identity Manager FQDN points to the load balancer when a load balancer is being used.
- Application Manager - Integrated Components. The VMware Identity Manager 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 VMware Identity Manager. Click **Enabled** to go to the Connector Services Admin page for that resource.

# Viewing Reports

You can create reports to track users and group activities and resource usage. You can view the reports in the administration console Dashboard > Reports page.

You can export reports in an comma-separated value (csv) file format.

**Table 9-1. Report Types**

| Report | Description |
|---|---|
| Recent Activity | Recent activity is a report about the actions that users performed while using their Workspace ONE portal for the past day, past week, past month, or past 12 weeks. The activity can include user information such as how many unique user logins, how many general logins and resource information such as number of resources launched, resource entitlements added. You can click **Show Events** to see the date, time, and user details for the activity. |
| Resource Usage | Resource usage is a report of all resources in the Catalog with details for each resource about the number of users, launches, and licenses. You can select to view the activities for the past day, past week, past month, or past 12 weeks. |
| Resource Entitlements | Resource entitlements is a report by resource that shows the number of users entitled to the resource, number of launches, and number of licenses used. |
| Resource Activity | The resource activity report can be created for all users or a specific group of users. The resource activity information lists the user name, the resource entitled to the user and the date the resource was last accessed, and information about the type of device the user used to access the resource. |
| Group Membership | Group membership is a lists the members of a group you specify. |
| Role Assignment | Role assignment lists the users that are either API-only administrators or administrators and their email addresses. |
| Users | Users report lists all the users and provides details about each user, such as the user's email address, role, and group affiliations. |
| Concurrent Users | Concurrent users report shows the number of user sessions that were opened at one time and the date and time. |

**Table 9-1. Report Types (Continued)**

| Report | Description |
|---|---|
| Device Usage | The device usage report can show device usage for all users or a specific group of users. The device information is listed by individual user and includes the user's name, device name, operating system information, and date last used. |
| Audit events | The audit events report lists the events related to a user you specify, such as user logins for the past 30 days. You can also view the audit event details. This feature is useful for troubleshooting purposes. To run audit events reports, auditing must be enabled in the Catalog > Settings > Auditing page. See Generate an Audit Event Report. |

# 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

Auditing must be enabled. To verify if it is enabled, in the administration console, go to the **Catalog > Settings** page and select **Auditing**.

### Procedure

1 In the administration console, select **Reports > Audit events**

2 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 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. |

3 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.

4 For more information about an audit event, click **View Details** for that audit event.

# Custom Branding for VMware Identity Manager Services

10

You can customize the logos, fonts, and background that appear in the administration console, the user and administrator sign-in screens, the Web view of the Workspace ONE applications portal, and the Web view of the Workspace ONE application on mobile devices.

You can use the customization tool to match the look and feel of your company's colors, logos, and design.

This section includes the following topics:



## Customize Branding in VMware Identity Manager Service

You can add your company name, product name, and favicon to the address bar for the administration console and the user portal. You can also customize the sign-in page to set background colors to match your company's colors and logo design.

### Procedure

1. In the administration console Identity & Access Management tab, select **Setup > Custom Branding**.
2. Edit the following settings in the form as appropriate.

| Form Field | Description |
|---|---|
| | Names and Logos Tab |
| Company Name | Company Name applies to both desktops and mobile devices. You can add your company's name as the title that appears in the browser tab.<br>Enter a new company name over the existing one to change the name. |
| Product Name | Product Name applies to both desktops and mobile devices. The product name displays after the company name in the browser tab. |
| Favicon | A favicon is an icon associated with a URL that is displayed in the browser address bar.<br>The maximum size of the favicon image is 16 x 16 px. The format can be JPEG, PNG, GIF, or ICO.<br>Click **Upload** to upload a new image to replace the current favicon. You are prompted to confirm the change. The change occurs immediately. |

| Form Field | Description |
|---|---|
| | Sign-In Screen Tab |
| 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.<br>The minimum image size recommended 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. |
| Background Color | The color that displays for the background of the sign-in screen.<br>Enter the six-digit hexadecimal color code over the existing one to change the background color. |
| Box background color | The sign-in screen box color can be customized.<br>Enter the six-digit hexadecimal color code over the existing code. |
| Login button background color | The color of the login button can be customized.<br>Enter the six-digit hexadecimal color code over the existing one. |
| Login button text color | The color of the text that displays on the login button can be customized.<br>Enter the six-digit hexadecimal color code over the existing one. |

When you customize the sign-in screen, you can see your changes in the Preview pane before you save your changes.

3 Click **Save**.

Custom branding updates to the administration console and the sign-in pages are applied within five minutes after you click Save.

### What to do next

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

Update the appearance of the end-user Workspace ONE portal and mobile and tablet view. See Customize Branding for the User Portal

# Customize Branding for the User Portal

You can add a logo, change the background colors, and add images to customize the Workspace ONE portal.

### Procedure

1 In the administration console Catalogs tab, select **Settings > User Portal Branding**.

2 Edit the settings in the form as appropriate.

| Form Item | Description |
|---|---|
| Logo | Add a masthead logo to be the banner at the top of the admin console and Workspace ONE portal Web pages.<br>The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG or GIF. |
| | Portal |

| Form Item | Description |
|---|---|
| Masthead Background Color | Enter a six-digit hexadecimal color code over the existing one to change the background color of the masthead. The background color changes in the application portal preview screen when you type in a new color code. |
| Masthead Text Color | Enter a six-digit hexadecimal color code over the existing one to change the color of the text that displays in the masthead. |
| Background Color | The color that displays for the background of the Web portal screen.<br>Enter a new six-digit hexadecimal color code over the existing one to change the background color. The background color changes in the application portal preview screen when you type in a new color code.<br>Select **Background Highlight** to accent the background color. If Background Highlight is enabled, browsers that support multiple background images show the overlay in the launcher and catalog pages.<br>Select **Background Pattern** to set the predesigned triangle pattern in the background color. |
| Icon Background Color | Enter a six-digit hexadecimal color code to change the background color box surrounding application icons. |
| Icon Background Opacity | To set a transparency, move the slider on the bar. |
| Name and Icon Color | You can select the text color for names listed under the icons on the app portal pages.<br>Enter a hexadecimal color code over the existing one to change the font color. |
| Lettering effect | Select the type of lettering to use for the text on the Workspace ONE portal screens. |
| Background Highlight | If enabled, for browsers that support multiple background images, the background overlay displays in the bookmark and catalog pages. |
| Background Pattern | If enabled, for browsers that support multiple bg images, the background overlays display in the bookmark and catalog pages. |
| Image (Optional) | To add an image to the background on the app portal screen instead of a color, upload an image. |

3 Click **Save**.

Custom branding updates are refreshed every 24 hours for the user portal. To push the changes sooner, as the administrator, open a new tab and enter this URL, substituting your domain name for myco.example.com. `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

### What to do next

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

# Customize Branding for VMware Verify Application

If you enabled VMware Verify for two-factor authentication, you can customize the sign-in page with your company logo.

### Prerequisites

VMware Verify enabled.

### Procedure

1 In the administration console Catalogs tab, select **Settings > User Portal Branding**.

2 Edit the VMware Verify section.

| Form Item | Description |
|---|---|
| Logo | Upload the company logo that displays on the approval request pages.<br>The size of the image is 540 x 170 px., PNG format, and 128 kB or smaller. |
| Icon | Upload an icon that is displayed on the device when VMware Verify is launched.<br>The size of the image is 81 x 81 px., PNG format, and 128 kB or smaller. |

3 Click **Save**.