You can find the most up-to-date technical documentation on the VMware Web site at:
https://docs.vmware.com/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
# Contents

About VMware Identity Manager Administration 7

1 Working in VMware Identity Manager Administration Console 9
   Navigating in the Administration Console 9
   Identity and Access Management Settings Overview 10

2 Integrating Your Enterprise Directory with VMware Identity Manager 13
   Important Concepts Related to Directory Integration 13

3 Integrating with Active Directory 15
   Active Directory Environments 15
   About Domain Controller Selection (domain_krb.properties file) 17
   Managing User Attributes that Sync from Active Directory 20
   Permissions Required for Joining a Domain 21
   Configuring Active Directory Connection to the Service 21
   Enabling Users to Change Active Directory Passwords 26
   Setting up Directory Sync Safeguards 27

4 Integrating with LDAP Directories 29
   Limitations of LDAP Directory Integration 29
   Integrating an LDAP Directory with the Service 30

5 Using Local Directories 35
   Creating a Local Directory 36
   Changing Local Directory Settings 41
   Deleting a Local Directory 42
   Configuring Authentication Method for System Admin Users 42

6 Just-in-Time User Provisioning 43
   About Just-in-Time User Provisioning 43
   Preparing for Just-in-Time Provisioning 44
   Configuring Just-in-Time User Provisioning 46
   Requirements for SAML Assertions 46
   Disabling Just-in-Time User Provisioning 47
   Deleting a Just-in-Time Directory 48
   Error Messages 48

7 Managing the User Login Experience 51
   Login Experience Using Unique Identifier 51
   Set Up Unique Identifier-Based Log In 51
   Requiring Terms of Use to Access the Workspace ONE Catalog 52
8 Configuring User Authentication in VMware Identity Manager 55
  Configuring Kerberos for VMware Identity Manager 56
  Configuring SecurID for VMware Identity Manager 60
  Configuring RADIUS for VMware Identity Manager 62
  Configuring RSA Adaptive Authentication in VMware Identity Manager 65
  Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager 67
  Configuring VMware Verify for Two-Factor Authentication 70
Using Built-in Identity Providers 71
Configure Additional Workspace Identity Providers 82
Configuring a Third-Party Identity Provider Instance to Authenticate Users 82
Managing Authentication Methods to Apply to Users 84

9 Managing Access Policies 87
  Configuring Access Policy Settings 87
  Managing Web and Desktop Application-Specific Policies 89
  Add a Web or Desktop Application-Specific Policy 90
  Configure Custom Access Denied Error Message 91
  Edit Default Access Policy 91
  Enabling Compliance Checking for AirWatch Managed Devices 92
  Enabling Persistent Cookie on Mobile Devices 94

10 Managing Users and Groups 95
  User and Group Types 95
  About User Names and Group Names 96
  Managing Users 97
  Create Groups and Configure Group Rules 97
  Edit Group Rules 100
  Add Resources to Groups 100
  Create Local Users 100
  Managing Passwords 102

11 Managing the Catalog 105
  Managing Resources in the Catalog 105
  Grouping Resource into Categories 109
  Managing Catalog Settings 110

12 Working in the Administration Console Dashboard 117
  Monitor Users and Resource Usage from the Dashboard 117
  Monitor System Information and Health 118
  Viewing Reports 118

13 Custom Branding for VMware Identity Manager Services 121
  Customize Branding in VMware Identity Manager Service 121
  Customize Branding for the User Portal 122
  Customize Branding for VMware Verify Application 123
 Integrating AirWatch With VMware Identity Manager  
Setting up AirWatch for Integration with VMware Identity Manager  125
Setting up an AirWatch Instance in VMware Identity Manager  129
Enable Unified Catalog for AirWatch  131
Implementing Authentication with AirWatch Cloud Connector  132
Implementing Mobile Single Sign-in Authentication for AirWatch-Managed iOS Devices  134
Implementing Mobile Single Sign-On Authentication for AirWatch-Managed Android Devices  141
Enabling Compliance Checking for AirWatch Managed Devices  147
Registering Email Domains for Auto Discovery  148

Index  151
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

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 chapter includes the following topics:

- “Navigating in the Administration Console,” on page 9
- “Identity and Access Management Settings Overview,” on page 10

Navigating in the Administration Console

The tasks in the administration console are organized by tabs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>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. The System Diagnostics dashboard displays a detailed overview of the health of the service in your environment and other information about the services. You can create reports to track users’ and groups’ activities, resource and device use, and audit events by user.</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>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.</td>
</tr>
<tr>
<td>Catalog</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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 End-User Components**

Users can access entitled resources from their Workspace ONE portal. They can access virtualized Windows applications captured as ThinApp packages from Identity Manager Desktop.

<table>
<thead>
<tr>
<th>User Component</th>
<th>Description</th>
<th>Available Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE User Apps Portal</td>
<td>The apps portal is an agentless web-based application. It is the default interface used when users access and use their entitled resources with a browser. If an end user has entitled ThinApp applications and is on a Windows computer where the Identity Manager Desktop application is installed and active, they can view and launch their entitled ThinApp packages from this apps portal.</td>
<td>Web-based apps portal is available on all supported system endpoints, such as Windows computers, Mac computers, iOS devices, Android devices.</td>
</tr>
<tr>
<td>Identity Manager Desktop</td>
<td>When this program is installed on users' Windows computers, they can work with their virtualized Windows applications captured as ThinApp packages.</td>
<td>Windows computers</td>
</tr>
</tbody>
</table>

**Identity and Access Management Settings Overview**

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

The following is a description of the setup settings in the Identity and Access Management tab.
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, and when it is used as the identity provider, authenticates users to the service.
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.
The connector syncs user and group data between your enterprise directory and the service through one or more workers.
- 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 8, “Configuring User Authentication in VMware Identity Manager,” on page 55.
- In the Identity Provider column, select the IdP to view, edit or disable. See “Add and Configure an Identity Provider Instance,” on page 83.
- In the Associated Directory column, access the directory associated with this worker.
Before you can add a new connector, you click Add Connector to generate an activation code that you paste in the Setup wizard to establish communication with the connector.
Join Domain | You click Join Domain to join the connector to a specific Active Directory domain. For example when you configure Kerberos authentication, you must join the Active Directory domain either containing users or having trust relationship with the domains containing users.
- When you configure a directory with an Integrated Windows Authentication Active Directory, the connector joins the domain according to the configuration details.
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,” on page 121.
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,” on page 122.
Setup > User Attributes | The User Attributes page lists the default user attributes that sync in the directory and you can add other attributes that you can map to Active Directory attributes. See “Select Attributes to Sync with Directory,” on page 20.
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,” on page 84.
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, see the AirWatch documentation VMware AirWatch Windows Autodiscovery Service Installation Guide available from the AirWatch website, http://air-watch.com
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.
See the Setting up the VMware Workspace ONE App on Devices guide for more information about auto discovery.
Table 1-2. Identity and Access Management Setup Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup &gt; AirWatch</td>
<td>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 Chapter 14, “Integrating AirWatch With VMware Identity Manager,” on page 125.</td>
</tr>
<tr>
<td>Setup &gt; Preferences</td>
<td>The Preferences page displays features that the admin can enable. This includes:</td>
</tr>
<tr>
<td></td>
<td>- Persistent cookies can be enabled from this page. See “Enable Persistent Cookie,” on page 94.</td>
</tr>
<tr>
<td></td>
<td>- When local users are configured in your service, to show Local Users as a domain option on the sign in page, enable Show Local Users on the login page.</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>On the Terms of Use page, you can write your company’s own Workspace ONE terms of use and ensure that end users accept this terms of use before using Workspace ONE.</td>
</tr>
</tbody>
</table>

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

Figure 1-2. Identity & Access Management Manage Pages

Table 1-3. Identity and Access Management Manage Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage &gt; Directories</td>
<td>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. See Chapter 2, “Integrating Your Enterprise Directory with VMware Identity Manager,” on page 13. When you click a directory name, you can edit the sync settings, navigate the Identity Providers page, and view the sync log. 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.</td>
</tr>
<tr>
<td>Manage &gt; Identity Providers</td>
<td>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. See “Add and Configure an Identity Provider Instance,” on page 83.</td>
</tr>
<tr>
<td>Manage &gt; Password Recovery Assistant</td>
<td>On the Password Recovery Assistant page, you can change the default behavior when &quot;Forgot password&quot; is clicked on the sign-in screen by the end user.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>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 to the built-in identity provider.</td>
</tr>
<tr>
<td>Manage &gt; Policies</td>
<td>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 9, “Managing Access Policies,” on page 87.</td>
</tr>
</tbody>
</table>
You integrate your enterprise directory with VMware Identity Manager to sync users and groups from your enterprise directory to the VMware Identity Manager service.

The following types of directories are supported.

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication
- LDAP directory

To integrate your enterprise directory, you perform the following tasks.

- Specify the attributes that you want users to have in the VMware Identity Manager service.
- Create a directory in the VMware Identity Manager service of the same type as your enterprise directory and specify the connection details.
- Map the VMware Identity Manager attributes to attributes used in your Active Directory or LDAP directory.
- Specify the users and groups to sync.
- Sync users and groups.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration, set up a sync schedule to sync regularly, or start a sync at any time.

**Important Concepts Related to Directory Integration**

Several concepts are integral to understanding how the VMware Identity Manager service integrates with your Active Directory or LDAP directory environment.

**VMware Identity Manager Connector**

The VMware Identity Manager Connector, a component of the service, performs the following functions.

- Syncs user and group data from your Active Directory or LDAP directory to the VMware Identity Manager service.
- When being used as an identity provider, authenticates users to the VMware Identity Manager service.
The connector is the default identity provider. You can also use third-party identity providers that support the SAML 2.0 protocol. Use a third-party identity provider for an authentication type the connector does not support, or if the third-party identity provider is preferable based on your enterprise security policy.

**Note** If you use third-party identity providers, you can either configure the connector to sync user and group data or configure Just-in-Time user provisioning. See the Just-in-Time User Provisioning section in *VMware Identity Manager Administration* for more information.

**Directory**

The VMware Identity Manager service has its own concept of a directory, corresponding to the Active Directory or LDAP directory in your environment. This directory uses attributes to define users and groups. You create one or more directories in the service and then sync those directories with your Active Directory or LDAP directory. You can create the following directory types in the service.

- **Active Directory**
  - Active Directory over LDAP. Create this directory type if you plan to connect to a single Active Directory domain environment. For the Active Directory over LDAP directory type, the connector binds to Active Directory using simple bind authentication.
  - Active Directory, Integrated Windows Authentication. Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment. The connector binds to Active Directory using Integrated Windows Authentication.

The type and number of directories that you create varies depending on your Active Directory environment, such as single domain or multi-domain, and on the type of trust used between domains. In most environments, you create one directory.

- **LDAP Directory**

The service does not have direct access to your Active Directory or LDAP directory. Only the connector has direct access. Therefore, you associate each directory created in the service with a connector instance.

**Worker**

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.

The connector syncs user and group data between your Active Directory or LDAP directory and the service through one or more workers.

**Important** You cannot have two workers of the Active Directory, Integrated Windows Authentication type on the same connector instance.

**Security Considerations**

For enterprise directories integrated with the VMware Identity Manager service, security settings such as user password complexity rules and account lockout policies must be set in the enterprise directory directly. VMware Identity Manager does not override these settings.
Integrating with Active Directory

You can integrate VMware Identity Manager with your Active Directory deployment to sync users and groups from Active Directory to VMware Identity Manager.

See also “Important Concepts Related to Directory Integration,” on page 13.

This chapter includes the following topics:

- “Active Directory Environments,” on page 15
- “About Domain Controller Selection (domain_krb.properties file),” on page 17
- “Managing User Attributes that Sync from Active Directory,” on page 20
- “Permissions Required for Joining a Domain,” on page 21
- “Configuring Active Directory Connection to the Service,” on page 21
- “Enabling Users to Change Active Directory Passwords,” on page 26
- “Setting up Directory Sync Safeguards,” on page 27

Active Directory Environments

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

Single Active Directory Domain Environment

A single Active Directory deployment allows you to sync users and groups from a single Active Directory domain.

For this environment, when you add a directory to the service, select the Active Directory over LDAP option.

For more information, see:

- “About Domain Controller Selection (domain_krb.properties file),” on page 17
- “Managing User Attributes that Sync from Active Directory,” on page 20
- “Configuring Active Directory Connection to the Service,” on page 21

Multi-Domain, Single Forest Active Directory Environment

A multi-domain, single forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains within a single forest.
You can configure the service for this Active Directory environment as a single Active Directory, Integrated Windows Authentication directory type or, alternatively, as an Active Directory over LDAP directory type configured with the global catalog option.

- The recommended option is to create a single Active Directory, Integrated Windows Authentication directory type.

  When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.

  For more information, see:
  - “About Domain Controller Selection (domain_krb.properties file),” on page 17
  - “Managing User Attributes that Sync from Active Directory,” on page 20
  - “Configuring Active Directory Connection to the Service,” on page 21

- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory type and select the global catalog option.

  Some of the limitations with selecting the global catalog option include:
  - The Active Directory object attributes that are replicated to the global catalog are identified in the Active Directory schema as the partial attribute set (PAS). Only these attributes are available for attribute mapping by the service. If necessary, edit the schema to add or remove attributes that are stored in the global catalog.
  - The global catalog stores the group membership (the member attribute) of only universal groups. Only universal groups are synced to the service. If necessary, change the scope of a group from a local domain or global to universal.
  - The bind DN account that you define when configuring a directory in the service must have permissions to read the Token-Groups-Global-And-Universal (TGGAU) attribute.
  - When AirWatch is integrated with VMware Identity Manager and multiple AirWatch organization groups are configured, the Active Directory Global Catalog option cannot be used.

  Active Directory uses ports 389 and 636 for standard LDAP queries. For global catalog queries, ports 3268 and 3269 are used.

  When you add a directory for the global catalog environment, specify the following during the configuration.
  - Select the Active Directory over LDAP option.
  - Deselect the check box for the option This Directory supports DNS Service Location.
  - Select the option This Directory has a Global Catalog. When you select this option, the server port number is automatically changed to 3268. Also, because the Base DN is not needed when configuring the global catalog option, the Base DN text box does not display.
  - Add the Active Directory server host name.
  - If your Active Directory requires access over SSL, select the option This Directory requires all connections to use SSL and paste the certificate in the text box provided. When you select this option, the server port number is automatically changed to 3269.

**Multi-Forest Active Directory Environment with Trust Relationships**

A multi-forest Active Directory deployment with trust relationships allows you to sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains.

When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.
Multi-Forest Active Directory Environment Without Trust Relationships

A multi-forest Active Directory deployment without trust relationships allows you to sync users and groups from multiple Active Directory domains across forests without a trust relationship between the domains. In this environment, you create multiple directories in the service, one directory for each forest. The type of directories you create in the service depends on the forest. For forests with multiple domains, select the Active Directory (Integrated Windows Authentication) option. For a forest with a single domain, select the Active Directory over LDAP option.

About Domain Controller Selection (domain_krb.properties file)

The domain_krb.properties file determines which domain controllers are used for directories that have DNS Service Location (SRV records) lookup enabled. It contains a list of domain controllers for each domain. The connector creates the file initially, and you must maintain it subsequently. The file overrides DNS Service Location (SRV) lookup.

The following types of directories have DNS Service Location lookup enabled:
- Active Directory over LDAP with the **This Directory supports DNS Service Location** option selected
- Active Directory (Integrated Windows Authentication), which always has DNS Service Location lookup enabled

When you create additional directories that have DNS Service Location enabled, or add new domains to an Integrated Windows Authentication directory, the new domains, and a list of domain controllers for them, are added to the file.

You can override the default selection at any time by editing the domain_krb.properties file. As a best practice, after you create a directory, view the domain_krb.properties file and verify that the domain controllers listed are the optimal ones for your configuration. For a global Active Directory deployment that has multiple domain controllers across different geographical locations, using a domain controller that is in close proximity to the connector ensures faster communication with Active Directory.

You must also update the file manually for any other changes. The following rules apply.
- The file is created, and auto-populated with domain controllers for each domain, when you first create a directory that has DNS Service Location lookup enabled.
- Domain controllers for each domain are listed in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.
- The file is updated only when you create a new directory that has DNS Service Location lookup enabled or when you add a domain to an Integrated Windows Authentication directory. The new domain and a list of domain controllers for it are added to the file.

Note that if an entry for a domain already exists in the file, it is not updated. For example, if you created a directory, then deleted it, the original domain entry remains in the file and is not updated.
The file is not updated automatically in any other scenario. For example, if you delete a directory, the domain entry is not deleted from the file.

- If a domain controller listed in the file is not reachable, edit the file and remove it.
- If you add or edit a domain entry manually, your changes will not be overwritten.

For information on editing the domain_krb.properties file, see “Editing the domain_krb.properties file,” on page 19.

How Domain Controllers are Selected to Auto-Populate the domain_krb.properties File

To auto-populate the domain_krb.properties file, domain controllers are selected by first determining the subnet on which the connector resides (based on the IP address and netmask), then using the Active Directory configuration to identify the site of that subnet, getting the list of domain controllers for that site, filtering the list for the appropriate domain, and picking the two domain controllers that respond the fastest.

To detect the domain controllers that are the closest, VMware Identity Manager has the following requirements:

- The subnet of the connector must be present in the Active Directory configuration, or a subnet must be specified in the runtime-config.properties file. See “Overriding the Default Subnet Selection,” on page 18.

  The subnet is used to determine the site.

- The Active Directory configuration must be site aware.

If the subnet cannot be determined or if your Active Directory configuration is not site aware, DNS Service Location lookup is used to find domain controllers, and the file is populated with a few domain controllers that are reachable. Note that these domain controllers may not be at the same geographical location as the connector, which can result in delays or timeouts while communicating with Active Directory. In this case, edit the domain_krb.properties file manually and specify the correct domain controllers to use for each domain. See “Editing the domain_krb.properties file,” on page 19.

Sample domain_krb.properties File

example.com=host1.example.com:389,host2.example.com:389

Overriding the Default Subnet Selection

To auto-populate the domain_krb.properties file, the connector attempts to find domain controllers that are at the same site so there is minimal latency between the connector and Active Directory.

To find the site, the connector determines the subnet on which it resides, based on its IP address and netmask, then uses the Active Directory configuration to identify the site for that subnet. If the subnet is not in Active Directory, or if you want to override the automatic subnet selection, you can specify a subnet in the runtime-config.properties file.

Procedure

1. Save and close the file.
2. Restart the service.

   service horizon-workspace restart
Editing the domain_krb.properties file

The domain_krb.properties file determines the domain controllers to use for directories that have DNS Service Location lookup enabled. You can edit the file at any time to modify the list of domain controllers for a domain, or to add or delete domain entries. Your changes will not be overridden.

The file is initially created and auto-populated by the connector. You need to update it manually in some cases, such as the following scenarios.

- If the domain controllers selected by default are not the optimal ones for your configuration, edit the file and specify the domain controllers to use.
- If you delete a directory, delete the corresponding domain entry from the file.
- If any domain controllers in the file are not reachable, remove them from the file.

See also “About Domain Controller Selection (domain_krb.properties file),” on page 17.

Procedure

1. Edit the domain_krb.properties file to add or edit the list of domain to host values.

   Use the following format:

   `domain=host:port,host2:port,host3:port`

   For example:

   `example.com=examplehost1.example.com:389,examplehost2.example.com:389`

   List the domain controllers in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.

   **Important** Domain names must be in lowercase.

2. Change the owner of the domain_krb.properties file to horizon and group to www.

3. Restart the service.

Troubleshooting domain_krb.properties

Use the following information to troubleshoot the domain_krb.properties file.

"Error resolving domain" error

If the domain_krb.properties file already includes an entry for a domain, and you try to create a new directory of a different type for the same domain, an "Error resolving domain" occurs. You must edit the domain_krb.properties file and manually remove the domain entry before creating the new directory.

Domain controllers are unreachable

Once a domain entry is added to the domain_krb.properties file, it is not updated automatically. If any domain controllers listed in the file become unreachable, edit the file manually and remove them.
Managing User Attributes that Sync from Active Directory

During the VMware Identity Manager service directory setup, you select Active Directory user attributes and filters to select which users sync in the VMware Identity Manager directory. You can change the user attributes that sync from the administration console, Identity & Access Management tab, Setup > User Attributes.

Changes that are made and saved in the User Attributes page are added to the Mapped Attributes page in the VMware Identity Manager directory. The attributes changes are updated to the directory with the next sync to Active Directory.

The User Attributes page lists the default directory attributes that can be mapped to Active Directory attributes. You select the attributes that are required, and you can add other attributes that you want to sync to the directory. When you add attributes, the attribute name you enter is case-sensitive. For example, address, Address, and ADDRESS are different attributes.

<table>
<thead>
<tr>
<th>VMware Identity Manager Directory Attribute Name</th>
<th>Default Mapping to Active Directory Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>userPrincipalName</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>distinguishedName</td>
<td>distinguishedName</td>
</tr>
<tr>
<td>employeeld</td>
<td>employeeID</td>
</tr>
<tr>
<td>domain</td>
<td>canonicalName. Adds the fully qualified domain name of object.</td>
</tr>
<tr>
<td>disabled (external user disabled)</td>
<td>userAccountControl. Flagged with UF_Account_Disable When an account is disabled, users cannot log in to access their applications and resources. The resources that users were entitled to are not removed from the account so that when the flag is removed from the account users can log in and access their entitled resources</td>
</tr>
<tr>
<td>phone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>lastName</td>
<td>sn</td>
</tr>
<tr>
<td>firstName</td>
<td>givenName</td>
</tr>
<tr>
<td>email</td>
<td>mail</td>
</tr>
<tr>
<td>userName</td>
<td>sAMAccountName.</td>
</tr>
</tbody>
</table>

Select Attributes to Sync with Directory

When you set up the VMware Identity Manager directory to sync with Active Directory, you specify the user attributes that sync to the directory. Before you set up the directory, you can specify on the User Attributes page which default attributes are required and add additional attributes that you want to map to Active Directory attributes.

When you configure the User Attributes page before the directory is created, you can change default attributes from required to not required, mark attributes as required, and add custom attributes.

After the directory is created, you can change a required attribute not to be required, and you can delete custom attributes. You cannot change an attribute to be a required attribute.

Procedure

1. In the administration console, Identity & Access Management tab, click User Attributes.
2. In the Default Attributes section, review the required attribute list and make appropriate changes to reflect which attributes should be required.
3. Click Save.

Permissions Required for Joining a Domain

You may need to join the VMware Identity Manager connector to a domain in some cases. For Active Directory over LDAP directories, you can join a domain after creating the directory. For directories of type Active Directory (Integrated Windows Authentication), the connector is joined to the domain automatically when you create the directory. In both scenarios, you are prompted for credentials.

To join a domain, you need Active Directory credentials that have the privilege to "join computer to AD domain". This is configured in Active Directory with the following rights:

- Create Computer Objects
- Delete Computer Objects

When you join a domain, a computer object is created in the default location in Active Directory, unless you specify a custom OU.

If you do not have the rights to join a domain, follow these steps to join the domain.

1. Ask your Active Directory administrator to create the computer object in Active Directory, in a location determined by your company policy. Provide the host name of the connector. Ensure that you provide the fully-qualified domain name, for example, server.example.com.

2. After the computer object is created, join the domain using any domain user account in the VMware Identity Manager administration console.

The Join Domain command is available on the Connectors page, accessed by clicking Identity & Access Management > Setup > Connectors.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Select or enter the Active Directory domain to join. Ensure that you enter the fully-qualified domain name. For example, server.example.com.</td>
</tr>
<tr>
<td>Domain User</td>
<td>The username of an Active Directory user who has the rights to join systems to the Active Directory domain.</td>
</tr>
<tr>
<td>Domain Password</td>
<td>The password of the user.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>(Optional) The organizational unit (OU) of the computer object. This option creates a computer object in the specified OU instead of the default Computers OU. For example, ou=testou,dc=test,dc=example,dc=com.</td>
</tr>
</tbody>
</table>

Tip: You can see the host name in the Host Name column on the Connectors page in the administration console. Click Identity & Access Management > Setup > Connectors to view the Connectors page.

Configuring Active Directory Connection to the Service

In the administration console, specify the information required to connect to your Active Directory and select users and groups to sync with the VMware Identity Manager directory.

The Active Directory connection options are Active Directory over LDAP or Active Directory Integrated Windows Authentication. Active Directory over LDAP connection supports DNS Service Location lookup.
Prerequisites

- Select which attributes are required and add additional attributes, if necessary, on the User Attributes page. See “Select Attributes to Sync with Directory,” on page 20.

**IMPORTANT** If you plan to sync XenApp resources with VMware Identity Manager, you must make `distinguishedName` a required attribute. You must make this selection before creating a directory as attributes cannot be changed from optional to required after a directory is created.

- List of the Active Directory groups and users to sync from Active Directory.
- For Active Directory over LDAP, the information required includes the Base DN, Bind DN, and Bind DN password.

**Note** Using a Bind DN user account with a non-expiring password is recommended.

- For Active Directory Integrated Windows Authentication, the information required includes the domain’s Bind user UPN address and password.

**Note** Using a Bind DN user account with a non-expiring password is recommended.

- If the Active Directory requires access over SSL or STARTTLS, the Root CA certificate of the Active Directory domain controller is required.

- For Active Directory Integrated Windows Authentication, when you have multi-forest Active Directory configured and the Domain Local group contains members from domains in different forests, make sure that the Bind user is added to the Administrators group of the domain in which the Domain Local group resides. If this is not done, these members are missing from the Domain Local group.

Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. On the Directories page, click **Add Directory**.
3. Enter a name for this VMware Identity Manager directory.
Select the type of Active Directory in your environment and configure the connection information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Active Directory over LDAP**                      | **a** In the Sync Connector field, select the connector to use to sync with Active Directory.  
                                                                                                                | **b** In the Authentication field, if this Active Directory is used to authenticate users, click Yes.  
                                                                                                                | If a third-party identity provider is used to authenticate users, click No. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication.  
                                                                                                                | **c** In the Directory Search Attribute field, select the account attribute that contains username.  
                                                                                                                | **d** If the Active Directory uses DNS Service Location lookup, make the following selections.  
                                                                                                                | **-** In the Server Location section, select the This Directory supports DNS Service Location checkbox.  
                                                                                                                | **-** A domain_krb.properties file, auto-populated with a list of domain controllers, will be created when the directory is created. See “About Domain Controller Selection (domain_krb.properties file),” on page 17.  
                                                                                                                | **-** If the Active Directory requires STARTTLS encryption, select the This Directory requires all connections to use SSL check box in the Certificates section and copy and paste the Active Directory Root CA certificate into the SSL Certificate field.  
                                                                                                                | **-** Ensure the certificate is in PEM format and include the “BEGIN CERTIFICATE” and “END CERTIFICATE” lines.  
                                                                                                                | **-** **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.  
                                                                                                                | **e** If the Active Directory does not use DNS Service Location lookup, make the following selections.  
                                                                                                                | **-** In the Server Location section, verify that the This Directory supports DNS Service Location checkbox is not selected and enter the Active Directory server host name and port number.  
                                                                                                                | **-** To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in “Active Directory Environments,” on page 15.  
                                                                                                                | **-** If the Active Directory requires access over SSL, select the This Directory requires all connections to use SSL check box in the Certificates section and copy and paste the Active Directory Root CA certificate into the SSL Certificate field.  
                                                                                                                | **-** Ensure the certificate is in PEM format and include the “BEGIN CERTIFICATE” and “END CERTIFICATE” lines.  
                                                                                                                | **-** **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory.  
                                                                                                                | **f** In the Base DN field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com.  
                                                                                                                | **g** In the Bind DN field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com.  
                                                                                                                | **-** **Note** Using a Bind DN user account with a non-expiring password is recommended.  
                                                                                                                | **h** After you enter the Bind password, click Test Connection to verify that the directory can connect to your Active Directory.  
                                                                                                                | **Active Directory (Integrated Windows Authentication)**   | **a** In the Sync Connector field, select the connector to use to sync with Active Directory.  
<pre><code>                                                                                                            | **b** In the Authentication field, if this Active Directory is used to authenticate users, click Yes. |
</code></pre>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If a third-party identity provider is used to authenticate users, click No. After you configure the Active Directory connection to sync users and groups, go to the Identity &amp; Access Management &gt; Manage &gt; Identity Providers page to add the third-party identity provider for authentication.</td>
</tr>
<tr>
<td>c</td>
<td>In the Directory Search Attribute field, select the account attribute that contains username.</td>
</tr>
<tr>
<td>d</td>
<td>If the Active Directory requires STARTTLS encryption, select the This Directory requires all connections to use STARTTLS checkbox in the Certificates section and copy and paste the Active Directory Root CA certificate into the SSL Certificate field. Ensure the certificate is in PEM format and include the &quot;BEGIN CERTIFICATE&quot; and &quot;END CERTIFICATE&quot; lines.</td>
</tr>
<tr>
<td></td>
<td>If the directory has multiple domains, add the Root CA certificates for all domains, one at a time. <strong>Note</strong> If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.</td>
</tr>
<tr>
<td>e</td>
<td>In the Bind User UPN field, enter the User Principal Name of the user who can authenticate with the domain. For example, <a href="mailto:username@example.com">username@example.com</a>. <strong>Note</strong> Using a Bind DN user account with a non-expiring password is recommended.</td>
</tr>
<tr>
<td>f</td>
<td>Enter the Bind User password.</td>
</tr>
</tbody>
</table>

5 Click **Save & Next**.

The page with the list of domains appears.

6 For Active Directory over LDAP, the domains are listed with a check mark. For Active Directory (Integrated Windows Authentication), select the domains that should be associated with this Active Directory connection.

**Note** If you add a trusting domain after the directory is created, the service does not automatically detect the newly trusting domain. To enable the service to detect the domain, the connector must leave and then rejoin the domain. When the connector rejoins the domain, the trusting domain appears in the list.

Click **Next**.

7 Verify that the VMware Identity Manager directory attribute names are mapped to the correct Active Directory attributes and make changes, if necessary, then click **Next**.
Select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Specify the group DNs</strong></td>
<td>To select groups, you specify one or more group DNs and select the groups</td>
</tr>
<tr>
<td>a Click + and specify the</td>
<td>under them.</td>
</tr>
<tr>
<td>group DN. For example,</td>
<td>CBDN=users,DC=example,DC=company,DC=com.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong> Specify</td>
<td>group DNs that are under the Base DN that you entered. If a group DN is</td>
</tr>
<tr>
<td>group DNs that are under the</td>
<td>outside the Base DN, users from that DN will be synced but will not be able</td>
</tr>
<tr>
<td>Base DN that you entered.</td>
<td>to log in.</td>
</tr>
<tr>
<td>b Click Find Groups.</td>
<td>The Groups to Sync column lists the number of groups found in the DN.</td>
</tr>
<tr>
<td>c To select all the groups</td>
<td>otherwise click Select and select the specific groups to sync.</td>
</tr>
<tr>
<td>in the DN, click Select All</td>
<td><strong>NOTE</strong> When you sync a group, any users that do not have Domain Users</td>
</tr>
<tr>
<td></td>
<td>as their primary group in Active Directory are not synced.</td>
</tr>
</tbody>
</table>

**Sync nested group members**

The Sync nested group members option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are syncd. In the VMware Identity Manager directory, these users will be members of the parent group that you selected for sync.

If the Sync nested group members option is disabled, when you specify a group to sync, all the users that belong directly to that group are syncd.

Users that belong to nested groups under it are not syncd. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

9 Click Next.

10 Specify additional users to sync, if required.

a Click + and enter the user DNs. For example,

CBDN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

**IMPORTANT** Specify user DNs that are under the Base DN that you entered. If a user DN is outside the Base DN, users from that DN will be synced but will not be able to log in.

b (Optional) To exclude users, create a filter to exclude some types of users.

You select the user attribute to filter by, the query rule, and the value.

11 Click Next.

12 Review the page to see how many users and groups are syncing to the directory and to view the sync schedule.

To make changes to users and groups, or to the sync frequency, click the Edit links.

13 Click Sync Directory to start the sync to the directory.

The connection to Active Directory is established and users and groups are synced from the Active Directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.

**What to do next**

- If you created a directory that supports DNS Service Location, a domain_krb.properties file was created and auto-populated with a list of domain controllers. View the file to verify or edit the list of domain controllers. See “About Domain Controller Selection (domain_krb.properties file),” on page 17.
Set up authentication methods. After users and groups sync to the directory, if the connector is also used for authentication, you can set up additional authentication methods on the connector. If a third party is the authentication identity provider, configure that identity provider in the connector.

Review the default access policy. The default access policy is configured to allow all appliances in all network ranges to access the Web browser, with a session time out set to eight hours or to access a client app with a session time out of 2160 hours (90 days). You can change the default access policy and when you add Web applications to the catalog, you can create new ones.

Apply custom branding to the administration console, user portal pages and the sign-in screen.

### Enabling Users to Change Active Directory Passwords

You can provide users the ability to change their Active Directory passwords from the Workspace ONE portal or app whenever they want. Users can also reset their Active Directory passwords from the VMware Identity Manager login page if the password has expired or if the Active Directory administrator has reset the password, forcing the user to change the password at the next login.

You enable this option per directory, by selecting the **Allow Change Password** option in the Directory Settings page.

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**.

Expired passwords or passwords reset by the administrator in Active Directory can be changed from the login page. When a user tries to log in with an expired password, the user is prompted to reset the password. The user must enter the old password as well as the new password.

The requirements for the new password are determined by the Active Directory password policy. The number of tries allowed also depends on the Active Directory password policy.

The following limitations apply.

- When a directory is added to VMware Identity Manager as a Global Catalog, the **Allow Change Password** option is not available. Directories can be added as Active Directory over LDAP or Integrated Windows Authentication, using ports 389 or 636.

- The password of a Bind DN user cannot be reset from VMware Identity Manager, even if it expires or the Active Directory administrator resets it.

**NOTE** Using a Bind DN user account with a non-expiring password is recommended.

- Passwords of users whose login names consist of multibyte characters (non-ASCII characters) cannot be reset from VMware Identity Manager.

### Prerequisites

- Port 464 must be open from VMware Identity Manager to the domain controllers.

- If you use additional, standalone connector virtual appliances, note that the **Allow Change Password** option is only available with connector version 2016.11.1 and later.

### Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. In the **Directories** tab, click the directory.
3. In the **Allow Change Password** section, select the **Enable change password** checkbox.
4. Enter the Bind DN password in the **Bind User Details** section, and click **Save**.
Setting up Directory Sync Safeguards

Sync safeguards threshold limits can be configured in the directory to help prevent unintended configuration changes to the users and groups that sync to the directory from Active Directory.

The sync safeguard thresholds that are set limit the number of changes that can be made to the users and groups when the directory syncs. If any directory safeguard threshold is met, the directory synchronization stops and a message is displayed on the directory’s Sync Log page. When SMTP is configured in the VMware Identity Manager administration console, you receive an email message when synchronization fails because of a safeguard violation.

When synchronization fails, you can go to the directory’s Sync Settings > Sync Log page to see a description of the type of safeguard violation.

To successfully complete the synchronization, you can either increase the percentage threshold of the safeguard on the Sync Safeguard settings page, or you can schedule a dry run of the sync and check Ignore Safeguards. When you select to ignore the safeguard threshold value, the safeguard values are not enforced for this sync session only.

When directory sync is run the first time, the sync safeguard values are not enforced.

**Note** If you do not want to use the sync safeguards feature, delete the values from the drop-down menu. When the sync safeguard threshold text boxes are empty, sync safeguards are not enabled.

Configure Directory Sync Safeguards

Configure the sync safeguard threshold settings to limit the number of changes that can be made to the users and groups when the directory syncs.

**Note** If you do not want to use the sync safeguards feature, delete the values from the drop-down menu. When the sync safeguard threshold text boxes are empty, sync safeguards are not enabled.

**Procedure**

1. To change the safeguards settings, in the Identity & Access Management tab select **Manage > Directories**.
2. Select the directory to set the safeguards and click **Sync Settings**.
3. Click **Safeguards**.
4. Set the percentage of changes to trigger the sync to fail.
5. Click **Save**.

Ignore Safeguard Settings to Complete Syncing to the Directory

When you receive notification that the sync did not complete because of a safeguard violation, to override the safeguard setting and complete the sync you can schedule a dry run of the sync and check Ignore Safeguards.

**Procedure**

1. In the Identity & Access Management tab select **Manage > Directories**.
2. Select the directory that did not complete the sync and go to the **Sync Log** page.
3. To see the type of safeguard violation, in the Sync Details column, click **Failed to complete sync. Please check safeguards**.
4. Click **OK**.
To continue the sync without changing the safeguard settings, click **Sync Now**.

On the Review page, select the check box **Ignore Safeguards**.

Click **Sync Directory**.

The directory sync is run and the safeguard threshold settings are ignored for this sync session only.
You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

See also “Important Concepts Related to Directory Integration,” on page 13.

This chapter includes the following topics:

- “Limitations of LDAP Directory Integration,” on page 29
- “Integrating an LDAP Directory with the Service,” on page 30

### Limitations of LDAP Directory Integration

The following limitations currently apply to the LDAP directory integration feature.

- You can only integrate a single-domain LDAP directory environment.
  
  To integrate multiple domains from an LDAP directory, you need to create additional VMware Identity Manager directories, one for each domain.

- The following authentication methods are not supported for VMware Identity Manager directories of type LDAP directory.
  - Kerberos authentication
  - RSA Adaptive Authentication
  - ADFS as a third-party identity provider
  - SecurID
  - Radius authentication with Vasco and SMS Passcode server

- You cannot join an LDAP domain.

- Integration with View or Citrix-published resources is not supported for VMware Identity Manager directories of type LDAP directory.

- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.

- If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required in the User Attributes page, except for userName, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.

- If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the VMware Identity Manager service. You can specify the names when you select the groups to sync.
The option to allow users to reset expired passwords is not available.

The `domain_krb.properties` file is not supported.

**Integrating an LDAP Directory with the Service**

You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

To integrate your LDAP directory, you create a corresponding VMware Identity Manager directory and sync users and groups from your LDAP directory to the VMware Identity Manager directory. You can set up a regular sync schedule for subsequent updates.

You also select the LDAP attributes that you want to sync for users and map them to VMware Identity Manager attributes.

Your LDAP directory configuration may be based on default schemas or you may have created custom schemas. You may also have defined custom attributes. For VMware Identity Manager to be able to query your LDAP directory to obtain user or group objects, you need to provide the LDAP search filters and attribute names that are applicable to your LDAP directory.

Specifically, you need to provide the following information.

- LDAP search filters for obtaining groups, users, and the bind user
- LDAP attribute names for group membership, UUID, and distinguished name


**Prerequisites**

- Review the attributes in the Identity & Access Management > Setup > User Attributes page and add additional attributes that you want to sync. You will map the VMware Identity Manager attributes to your LDAP directory attributes when you create the directory. These attributes will be synced for the users in the directory.

  **Note** When you make changes to user attributes, consider the effect on other directories in the service. If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required except for `userName`, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.

- A Bind DN user account. Using a Bind DN user account with a non-expiring password is recommended.

- In your LDAP directory, the UUID of users and groups must be in plain text format.

- In your LDAP directory, a domain attribute must exist for all users and groups.

  You map this attribute to the VMware Identity Manager `domain` attribute when you create the VMware Identity Manager directory.

- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.

- If you use certificate authentication, users must have values for `userPrincipalName` and email address attributes.

**Procedure**

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

2. In the Directories page, click Add Directory and select Add LDAP Directory.
3 Enter the required information in the Add LDAP Directory page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Name</td>
<td>A name for the VMware Identity Manager directory.</td>
</tr>
<tr>
<td>Directory Sync and Authentication</td>
<td>In the Sync Connector field, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. You do not need a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. For the scenarios in which you need additional connectors, see the Installing and Configuring VMware Identity Manager guide, Installing Additional Connector Appliances.</td>
</tr>
<tr>
<td></td>
<td>In the Authentication field, if you want to use this LDAP directory to authenticate users, select Yes. If you want to use a third-party identity provider to authenticate users, select No. After you add the directory connection to sync users and groups, go to the Identity &amp; Access Management &gt; Manage &gt; Identity Providers page to add the third-party identity provider for authentication.</td>
</tr>
<tr>
<td></td>
<td>In the Directory Search Attribute field, specify the LDAP directory attribute to be used for user name. If the attribute is not listed, select Custom and type the attribute name. For example, cn.</td>
</tr>
<tr>
<td>Server Location</td>
<td>Enter the LDAP Directory server host and port number. For the server host, you can specify either the fully-qualified domain name or the IP address. For example, myLDAPserver.example.com or 100.00.00.0. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.</td>
</tr>
<tr>
<td>LDAP Configuration</td>
<td>Specify the LDAP search filters and attributes that VMware Identity Manager can use to query your LDAP directory. Default values are provided based on the core LDAP schema.</td>
</tr>
<tr>
<td>LDAP Queries</td>
<td>Get groups: The search filter for obtaining group objects. For example: (\text{objectClass=group})</td>
</tr>
<tr>
<td></td>
<td>Get bind user: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: (\text{objectClass=person})</td>
</tr>
<tr>
<td></td>
<td>Get user: The search filter for obtaining users to sync. For example: (\text{(&amp;(objectClass=user)(objectCategory=person))})</td>
</tr>
<tr>
<td>Attributes</td>
<td>Membership: The attribute that is used in your LDAP directory to define the members of a group. For example: member</td>
</tr>
<tr>
<td></td>
<td>Object UUID: The attribute that is used in your LDAP directory to define the UUID of a user or group. For example: entryUUID</td>
</tr>
<tr>
<td></td>
<td>Distinguished Name: The attribute that is used in your LDAP directory for the distinguished name of a user or group. For example: entryDN</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificates</td>
<td>If your LDAP directory requires access over SSL, select the <strong>This Directory requires all connections to use SSL</strong> and copy and paste the LDAP directory server’s root CA SSL certificate. Ensure the certificate is in PEM format and include the “BEGIN CERTIFICATE” and “END CERTIFICATE” lines.</td>
</tr>
<tr>
<td>Bind User Details</td>
<td><strong>Base DN</strong>: Enter the DN from which to start searches. For example, <code>cn=users,dc=example,dc=com</code></td>
</tr>
<tr>
<td></td>
<td><strong>Bind DN</strong>: Enter the user name to use to bind to the LDAP directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Using a Bind DN user account with a non-expiring password is recommended.</td>
</tr>
<tr>
<td></td>
<td><strong>Bind DN Password</strong>: Enter the password for the Bind DN user.</td>
</tr>
</tbody>
</table>

4. To test the connection to the LDAP directory server, click **Test Connection**. If the connection is not successful, check the information you entered and make the appropriate changes.

5. Click **Save & Next**.

6. In the Domains page, verify that the correct domain is listed, then click **Next**.

7. In the Map Attributes page, verify that the VMware Identity Manager attributes are mapped to the correct LDAP attributes. These attributes will be synced for users.

**IMPORTANT** You must specify a mapping for the domain attribute.

You can add attributes to the list from the User Attributes page.

8. Click **Next**.

9. In the groups page, click + to select the groups you want to sync from the LDAP directory to the VMware Identity Manager directory.

If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the groups page.

The **Sync nested group users** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will appear as members of the top-level group that you selected for sync. In effect, the hierarchy under a selected group is flattened and users from all levels appear in VMware Identity Manager as members of the selected group.

If this option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

10. Click **Next**.

11. Click + to add additional users. For example, enter `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`.

To exclude users, create a filter to exclude some types of users. You select the user attribute to filter by, the query rule, and the value.

Click **Next**.

12. Review the page to see how many users and groups will sync to the directory and to view the default sync schedule.

To make changes to users and groups, or to the sync frequency, click the **Edit** links.
13 Click **Sync Directory** to start the directory sync.

The connection to the LDAP directory is established and users and groups are synced from the LDAP directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.
Using Local Directories

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 chapter includes the following topics:

- “Creating a Local Directory,” on page 36
- “Changing Local Directory Settings,” on page 41
- “Deleting a Local Directory,” on page 42
- “Configuring Authentication Method for System Admin Users,” on page 42

**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>
<thead>
<tr>
<th>Table 5-1. Words that cannot be used as Custom Attribute Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
</tr>
<tr>
<td>department</td>
</tr>
<tr>
<td>emails</td>
</tr>
<tr>
<td>externalId</td>
</tr>
<tr>
<td>ims</td>
</tr>
<tr>
<td>meta</td>
</tr>
<tr>
<td>organization</td>
</tr>
<tr>
<td>photos</td>
</tr>
<tr>
<td>roles</td>
</tr>
<tr>
<td>userName</td>
</tr>
</tbody>
</table>

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.

![Add Directory](image)

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:

   **Add Directory**

   **Directory Name**: Partners

   **Domains**:

   - **Domains**: Partner

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter a name for the identity provider.</td>
</tr>
<tr>
<td>Users</td>
<td>Select the local directory you created.</td>
</tr>
<tr>
<td>Network</td>
<td>Select the networks from which this identity provider can be accessed.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>Select Password (Local Directory).</td>
</tr>
<tr>
<td>KDC Certificate Export</td>
<td>You do not need to download the certificate unless you are configuring mobile SSO for AirWatch-managed iOS devices.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the directory name</td>
<td>a  In the Settings tab, edit the directory name.</td>
</tr>
<tr>
<td></td>
<td>b  Click Save.</td>
</tr>
<tr>
<td>Add, delete, or rename a domain</td>
<td>a  In the Settings tab, edit the Domains list.</td>
</tr>
<tr>
<td></td>
<td>b  To add a domain, click the green plus icon.</td>
</tr>
<tr>
<td></td>
<td>c  To delete a domain, click the red delete icon.</td>
</tr>
<tr>
<td></td>
<td>d  To rename a domain, edit the domain name in the text box.</td>
</tr>
<tr>
<td>Add user attributes to the directory</td>
<td>a  Click the Identity &amp; Access Management tab, then click Setup.</td>
</tr>
<tr>
<td></td>
<td>b  Click the User Attributes tab.</td>
</tr>
<tr>
<td></td>
<td>c  Add attributes in the Add other attributes to use list, and click Save.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Make an attribute required or optional for the directory</td>
<td>a. In the Identity &amp; Access Management tab, click the Directories tab.&lt;br&gt;b. Click the local directory name and click the User Attributes tab.&lt;br&gt;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.&lt;br&gt;d. Click Save.</td>
</tr>
<tr>
<td>Change the order of the attributes</td>
<td>a. In the Identity &amp; Access Management tab, click the Directories tab.&lt;br&gt;b. Click the local directory name and click the User Attributes tab.&lt;br&gt;c. Click and drag the attributes to the new position.&lt;br&gt;d. Click Save.</td>
</tr>
</tbody>
</table>

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

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 chapter includes the following topics:
- “About Just-in-Time User Provisioning,” on page 43
- “Preparing for Just-in-Time Provisioning,” on page 44
- “Configuring Just-in-Time User Provisioning,” on page 46
- “Requirements for SAML Assertions,” on page 46
- “Disabling Just-in-Time User Provisioning,” on page 47
- “Deleting a Just-in-Time Directory,” on page 48
- “Error Messages,” on page 48

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,” on page 46.

**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.

### User Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>userPrincipalName</td>
<td></td>
</tr>
<tr>
<td>distinguishedName</td>
<td></td>
</tr>
<tr>
<td>employeeID</td>
<td></td>
</tr>
<tr>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>phone</td>
<td></td>
</tr>
<tr>
<td>initials</td>
<td></td>
</tr>
<tr>
<td>firstName</td>
<td></td>
</tr>
<tr>
<td>email</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td></td>
</tr>
</tbody>
</table>

Make changes to the user attributes that sync in the directory. Attributes here are added to the directory’s Mapped Attributes page. You can see the mapping to Active Directory attributes on the Mapped Attribute page.

Add other attributes to sync to the directory. Go to the directory’s Mapped Attributes page to map those attributes to Active Directory attributes.
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:

<table>
<thead>
<tr>
<th>Just-in-Time User Provisioning</th>
<th>Configure Just-in-Time provisioning to create users in the Identity Manager service dynamically when they first log in, based on SAML assertions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>☑</td>
</tr>
<tr>
<td>Create Just-in-Time Directory</td>
<td></td>
</tr>
<tr>
<td>Directory Name</td>
<td>JIT DEMO DIRECTORY</td>
</tr>
<tr>
<td>Domains</td>
<td>Domains:&lt;br&gt; myco.com</td>
</tr>
</tbody>
</table>

   Enter one or more domains. Users belonging to these domains are added to the directory. If only one domain is specified, it is used as the domain for SAML assertions without a domain attribute.

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,” on page 82.

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:

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Solution</th>
</tr>
</thead>
</table>
| 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.  
1. In the Identity & Access Management tab in the administration console, click Identity Providers and click the identity provider.  
2. In the Just-in-Time User Provisioning section, specify a directory name and one or more domains.  
3. Click Save.  
A Just-in-Time directory is created. |

The following errors can appear on the log-in page:
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User attribute is missing: name.</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
| **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:  
  - If multiple domains are configured for the Just-in-Time directory.  
  - If domain is marked as a required attribute in the User Attributes page.  
  If a domain attribute is specified, its value must match one of the domains specified for the directory.  
  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:  
  - A required attribute is missing in the SAML assertion.  
    Review the attributes in the User Attributes page and ensure that the SAML assertion includes all the attributes that are marked required.  
  - The domain for the user could not be determined.  
    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. |
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 chapter includes the following topics:

- “Login Experience Using Unique Identifier,” on page 51
- “Set Up Unique Identifier-Based Log In,” on page 51
- “Requiring Terms of Use to Access the Workspace ONE Catalog,” on page 52

**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**

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.
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 syncs to the directory.
- Verify that the default access policy rules for the user domains reflect the type of authentication to use when identifier-based logins 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**

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.

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password (on-premise deployment)</td>
<td>Without any configuration after Active Directory is configured, VMware Identity Manager supports Active Directory password authentication. This method authenticates users directly against Active Directory.</td>
</tr>
<tr>
<td>Kerberos for desktops</td>
<td>Kerberos authentication provides domain users with single sign-in access to their apps portals. 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.</td>
</tr>
<tr>
<td>Certificate (on-premise deployment)</td>
<td>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. 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.</td>
</tr>
<tr>
<td>RSA SecurID (on-premise deployment)</td>
<td>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.</td>
</tr>
<tr>
<td>RADIUS (on-premise deployment)</td>
<td>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.</td>
</tr>
<tr>
<td>RSA Adaptive Authentication (on-premise deployment)</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile SSO (for iOS)</td>
<td>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.</td>
</tr>
<tr>
<td>Mobile SSO (for Android)</td>
<td>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.</td>
</tr>
<tr>
<td>Password (AirWatch Connector)</td>
<td>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.</td>
</tr>
<tr>
<td>VMware Verify</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Password (Local Directory)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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,” on page 84.

This chapter includes the following topics:

- “Configuring Kerberos for VMware Identity Manager,” on page 56
- “Configuring SecurID for VMware Identity Manager,” on page 60
- “Configuring RADIUS for VMware Identity Manager,” on page 62
- “Configuring RSA Adaptive Authentication in VMware Identity Manager,” on page 65
- “Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager,” on page 67
- “Configuring VMware Verify for Two-Factor Authentication,” on page 70
- “Using Built-in Identity Providers,” on page 71
- “Configure Additional Workspace Identity Providers,” on page 82
- “Configuring a Third-Party Identity Provider Instance to Authenticate Users,” on page 82
- “Managing Authentication Methods to Apply to Users,” on page 84

**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 “Implementing Mobile Single Sign-in Authentication for AirWatch-Managed iOS Devices,” on page 134.
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,” on page 58.

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. On the Connectors page, for the connector that is being configured for Kerberos authentication, click Join Domain.
3. On the Join Domain page, enter the information for the Active Directory domain.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Enter the fully qualified domain name of the Active Directory. The domain name you enter must be the same Windows domain as the connector server.</td>
</tr>
<tr>
<td>Domain User</td>
<td>Enter the user name of an account in the Active Directory that has permissions to join systems to that Active Directory domain.</td>
</tr>
<tr>
<td>Domain Password</td>
<td>Enter the password associated with the AD Username. This password is not stored by VMware Identity Manager.</td>
</tr>
</tbody>
</table>

Click Save.

The Join Domain page is refreshed and displays a message that you are currently joined to the domain.

4. In the Worker column for the connector click Auth Adapters.
5. Click KerberosIdpAdapter
   You are redirected to the identity manager sign in page.
6. Click Edit in the KerberosIdpAdapter row and configure the Kerberos authentication page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name is required. The default name is KerberosIdpAdapter. You can change this.</td>
</tr>
<tr>
<td>Directory UID</td>
<td>Enter the account attribute that contains the user name</td>
</tr>
<tr>
<td>Enable Windows Authentication</td>
<td>Select this to extend authentication interactions between users’ browsers and VMware Identity Manager.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable NTLM</td>
<td>Select this to enable NT LAN Manager (NTLM) protocol-based authentication only if your Active Directory infrastructure relies on NTLM authentication.</td>
</tr>
<tr>
<td>Enable Redirect</td>
<td>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.</td>
</tr>
</tbody>
</table>

7 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** on page 61

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.
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_v8.1.3.312.06_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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The host name of VMware Identity Manager.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of VMware Identity Manager.</td>
</tr>
<tr>
<td>Alternate IP address</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 **SecurIDldpAdapter**.
You are redirected to the identity manager sign in page.

4 In the Authentication Adapters page SecurIDldpAdapter 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name is required. The default name is SecurIDldpAdapter. You can change this.</td>
</tr>
<tr>
<td>Enable SecurID</td>
<td>Select this box to enable SecurID authentication.</td>
</tr>
<tr>
<td>Number of authentication attempts allowed</td>
<td>Enter the maximum number of failed login attempts when using the RSA SecurID token. The default is five attempts. <strong>Note</strong>: When more than one directory is configured and you implement RSA SecurID authentication with additional directories, configure <strong>Number of authentication attempts allowed</strong> with the same value for each RSA SecurID configuration. If the value is not the same, SecurID authentication fails.</td>
</tr>
<tr>
<td>Connector Address</td>
<td>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.</td>
</tr>
<tr>
<td>Agent IP Address</td>
<td>Enter the value assigned to the <strong>IP address</strong> prompt in the RSA SecurID server.</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>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 <strong>sdconf.rec</strong>.</td>
</tr>
<tr>
<td>Node Secret</td>
<td>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.</td>
</tr>
</tbody>
</table>

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,” on page 84.

**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 RADIUS 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,” on page 63.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name is required. The default name is RadiusAuthAdapter. You can change this.</td>
</tr>
<tr>
<td>Enable Radius Adapter</td>
<td>Select this box to enable RADIUS authentication.</td>
</tr>
<tr>
<td>Number of authentication attempts allowed</td>
<td>Enter the maximum number of failed login attempts when using RADIUS to log in. The default is five attempts.</td>
</tr>
<tr>
<td>Number of attempts to Radius server</td>
<td>Specify the total number of retry attempts. If the primary server does not respond, the service waits for the configured time before retrying again.</td>
</tr>
<tr>
<td>Radius server hostname/address</td>
<td>Enter the host name or the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Authentication port</td>
<td>Enter the Radius authentication port number. This is usually 1812.</td>
</tr>
<tr>
<td>Accounting port</td>
<td>Enter 0 for the port number. The accounting port is not used at this time.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Enter the authentication protocol that is supported by the RADIUS server. Either PAP, CHAP, MSCHAP1, OR MSCHAP2.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret that is used between the RADIUS server and the VMware Identity Manager service.</td>
</tr>
<tr>
<td>Server timeout in seconds</td>
<td>Enter the RADIUS server timeout in seconds, after which a retry is sent if the RADIUS server does not respond.</td>
</tr>
<tr>
<td>Realm Prefix</td>
<td>(Optional) The user account location is called the realm. 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.</td>
</tr>
<tr>
<td>Realm Suffix</td>
<td>(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 <a href="mailto:jdoe@myco.com">jdoe@myco.com</a> is sent to the RADIUS server.</td>
</tr>
<tr>
<td>Login page passphrase hint</td>
<td>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.</td>
</tr>
</tbody>
</table>

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,” on page 84.
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 **RSAAAldpAdapter**. You are redirected to the identity manager authentication adapter page.
4. Click the **Edit** link next to the RSAAAldpAdapter.
5. Select the appropriate settings for your environment.

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

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

6. Click **Save**.
What to do next


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,” on page 84.

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 OCSP responder or if the response is invalid.

**Configure Certificate-based Authentication**

You enable and configure certificate authentication from the administration console.

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,” on page 67.

**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**.
On the Connectors page, select the Worker link for the connector that is being configured.

Click **Auth Adapters** and then click **CertificateAuthAdapter**.

Configure the Certificate Service Auth Adapter page.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name is required. The default name is CertificateAuthAdapter. You can change this name.</td>
</tr>
<tr>
<td>Enable certificate adapter</td>
<td>Select the check box to enable certificate authentication.</td>
</tr>
<tr>
<td>Root and intermediate CA</td>
<td>Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM.</td>
</tr>
<tr>
<td>certificates</td>
<td>The uploaded certificate files are listed in the Uploaded CA Certificates section of the form.</td>
</tr>
<tr>
<td>Use email if no UPN in certificate</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate policies accepted</td>
<td>Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID numbers (OID) for the Certificate Issuing Policy. Click <strong>Add another value</strong> to add additional OIDs.</td>
</tr>
<tr>
<td>Enable cert revocation</td>
<td>Select the check box to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.</td>
</tr>
<tr>
<td>Use CRL from certificates</td>
<td>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.</td>
</tr>
<tr>
<td>CRL Location</td>
<td>Enter the server file path or the local file path from which to retrieve the CRL.</td>
</tr>
<tr>
<td>Enable OCSP Revocation</td>
<td>Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.</td>
</tr>
<tr>
<td>Use CRL in case of OCSP</td>
<td>If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSP checking is not available.</td>
</tr>
<tr>
<td>failure</td>
<td></td>
</tr>
<tr>
<td>Send OCSP Nonce</td>
<td>Select this check box if you want the unique identifier of the OCSP request to be sent in the response.</td>
</tr>
<tr>
<td>OCSP URL</td>
<td>If you enabled OCSP revocation, enter the OCSP server address for revocation checking.</td>
</tr>
<tr>
<td>OCSP responder's signing</td>
<td>Enter the path to the OCSP certificate for the responder, /path/to/file.cer.</td>
</tr>
<tr>
<td>certificate</td>
<td></td>
</tr>
<tr>
<td>Enable consent form before</td>
<td>Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication.</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
</tr>
<tr>
<td>Consent form content</td>
<td>Type the text that displays in the consent form in this text box.</td>
</tr>
</tbody>
</table>

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,” on page 84.

- 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,” on page 123.

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

Create an access policy rule in the default access policy to add the VMware Verify authentication method as the second authentication method in the rule. See “Managing Authentication Methods to Apply to Users,” on page 84.

Apply custom banding to the VMware Verify sign-in page. See “Customize Branding for VMware Verify Application,” on page 123.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable AirWatch Password</td>
<td>This check box enables AirWatch password authentication.</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>AirWatch Admin Console URL</td>
<td>Pre-populated with the AirWatch URL.</td>
</tr>
<tr>
<td>AirWatch API Key</td>
<td>Pre-populated with the AirWatch Admin API key.</td>
</tr>
<tr>
<td>Certificate Used for</td>
<td>Pre-populated with the AirWatch Cloud Connector certificate.</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Password for Certificate</td>
<td>Pre-populated with the password for the AirWatch Cloud Connector certificate.</td>
</tr>
<tr>
<td>AirWatch Group ID</td>
<td>Pre-populated with the organization group ID.</td>
</tr>
<tr>
<td>Number of authentication attempts allowed</td>
<td>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.</td>
</tr>
<tr>
<td>JIT Enabled</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. Click Save.

**Enabling Compliance Checking for AirWatch Managed Devices**

When users enroll their devices through the AirWatch Agent application, 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,” on page 73.

Procedure

1. In the administration console Identity & Access Management tab, select Setup > AirWatch.
2. In the Device Compliance section, select Enable and click Save.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Device Compliance Adapter</td>
<td>Select this check box to enable AirWatch password authentication.</td>
</tr>
<tr>
<td>AirWatch Admin Console URL</td>
<td>Pre-populated with the AirWatch URL you set up on the AirWatch configuration page.</td>
</tr>
<tr>
<td>AirWatch API Key</td>
<td>Pre-populated with the AirWatch Admin API key.</td>
</tr>
<tr>
<td>Certificate Used for Authentication</td>
<td>Pre-populated with the AirWatch Cloud Connector certificate</td>
</tr>
<tr>
<td>Password for Certificate</td>
<td>Pre-populated with the password for the AirWatch Cloud Connector certificate.</td>
</tr>
</tbody>
</table>

6. Click Save.

What to do next


Configure the default access policy to create rules to use device compliance with AirWatch. See “Configure Access Policy Rule,” on page 92.

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. To deploy a local directory, see the VMware Identity Manager Cloud Deployment guide, Chapter 5, “Using Local Directories,” on page 35.

**Configure Certificate-based Authentication**

You enable and configure certificate authentication from the administration console.

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,” on page 67.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>A name is required. The default name is CertificateAuthAdapter. You can change this name.</td>
</tr>
<tr>
<td><strong>Enable certificate adapter</strong></td>
<td>Select the check box to enable certificate authentication.</td>
</tr>
<tr>
<td><strong>Root and intermediate CA certificates</strong></td>
<td>Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM.</td>
</tr>
<tr>
<td><strong>Uploaded CA certificates</strong></td>
<td>The uploaded certificate files are listed in the Uploaded Ca Certificates section of the form.</td>
</tr>
<tr>
<td><strong>Use email if no UPN in certificate</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Certificate policies accepted</strong></td>
<td>Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID numbers (OID) for the Certificate Issuing Policy. Click Add another value to add additional OIDs.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable cert revocation</td>
<td>Select the check box to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.</td>
</tr>
<tr>
<td>Use CRL from certificates</td>
<td>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.</td>
</tr>
<tr>
<td>CRL Location</td>
<td>Enter the server file path or the local file path from which to retrieve the CRL.</td>
</tr>
<tr>
<td>Enable OCSP Revocation</td>
<td>Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.</td>
</tr>
<tr>
<td>Use CRL in case of OCSP failure</td>
<td>If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSP checking is not available.</td>
</tr>
<tr>
<td>Send OCSP Nonce</td>
<td>Select this check box if you want the unique identifier of the OCSP request to be sent in the response.</td>
</tr>
<tr>
<td>OCSP URL</td>
<td>If you enabled OCSP revocation, enter the OCSP server address for revocation checking.</td>
</tr>
<tr>
<td>OCSP responder’s signing certificate</td>
<td>Enter the path to the OCSP certificate for the responder, /path/to/file.cer.</td>
</tr>
<tr>
<td>Enable consent form before authentication</td>
<td>Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication.</td>
</tr>
<tr>
<td>Consent form content</td>
<td>Type the text that displays in the consent form in this text box.</td>
</tr>
</tbody>
</table>

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,” on page 84.

- 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 the Built-in Identity Provider

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

For iOS device, you integrate the service with Kerberos. Kerberos authentication provides users, who are successfully signed in to their domain, access to their application portal without additional credential prompts.

VMware Identity Manager uses an identity provider that is built in to the identity manager service to provide access to Mobile SSO authentication. This authentication method for iOS devices uses a Key Distribution Center (KDC) without the use of a connector or a third-party system.

In the VMware Identity Manager service, Kerberos can be integrated in one of two ways.

- KDC as a VMware Identity Manager cloud hosted service. Using KDC in the cloud requires selecting the appropriate realm name in the iOS authentication adapter page.

  **Note** The KDC service hosted in the cloud is the only option when VMware Identity Manager is deployed with AirWatch in a Windows environment.

- Built-in KDC on the appliance. The built-in KDC requires initializing KDC on the appliance and creating public DNS entries to allow the Kerberos clients to find the KDC.
**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 in the Built-In Identity Provider**

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable KDC Authentication</strong></td>
<td>Select this check box to enable users to sign in using iOS devices that support Kerberos authentication.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>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 If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays.</td>
</tr>
<tr>
<td><strong>Root and Intermediate CA Certificate</strong></td>
<td>Upload the certificate authority issuer certificate file. The file format can be either PEM or DER.</td>
</tr>
<tr>
<td><strong>Uploaded CA Certificate Subject DNs</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable OCSP</strong></td>
<td>Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.</td>
</tr>
<tr>
<td><strong>Send OCSP Nonce</strong></td>
<td>Select this check box if you want the unique identifier of the OCSP request to be sent in the response.</td>
</tr>
<tr>
<td><strong>OCSP Responder’s Signing Certificate</strong></td>
<td>Upload the OCSP certificate for the responder. When you are using the AirWatch Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the AirWatch certificate here as well.</td>
</tr>
<tr>
<td><strong>OCSP Responder’s Signing Certificate Subject DN</strong></td>
<td>The uploaded OCSP certificate file is listed here.</td>
</tr>
<tr>
<td><strong>Enable Cancel Link</strong></td>
<td>When authentication is taking too long, give the user the ability to click Cancel to stop the authentication attempt and cancel the sign-in. When the Cancel link is enabled, Cancel appears at the end of the authentication error message that displays.</td>
</tr>
<tr>
<td><strong>Cancel Message</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

4 Click Save.

What to do next

- Associate the Mobile SSO (for iOS) authentication method in the built-in identity provider.
- In the KDC Certificate Export section, click **Download Certificate**. Save this certificate to a file that can be access from the AirWatch admin console. You upload this certificate when you configure the iOS device profile in AirWatch.
- 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 AirWatch and add the KDC server certificate issuer certificate from 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.

For information about configuring the Certificate authentication method, see “Configuring a Certificate or Smart Card Adapter for Use with VMware Identity Manager,” on page 67.
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.
4. In the Authentication Methods section, click the Mobile SSO (for Android devices) gear icon.
5. In the CertProxyAuthAdapter page configure the authentication method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Certificate Adapter</td>
<td>Select this check box to enable Mobile SSO for Android.</td>
</tr>
<tr>
<td>Root and Intermediate CA</td>
<td>Select the certificate files to upload. You can select multiple root CA and</td>
</tr>
<tr>
<td>Certificate</td>
<td>intermediate CA certificates that are encoded. The file format can be either</td>
</tr>
<tr>
<td></td>
<td>PEM or DER.</td>
</tr>
<tr>
<td>Uploaded CA Certificate Subject DNs</td>
<td>The contents of the uploaded certificate file is displayed here.</td>
</tr>
<tr>
<td>Use email if no UPN in certificate</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate policies accepted</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Cert Revocation</td>
<td>Select the check box to enable certificate revocation checking. This prevents users who have revoked user certificates from authenticating.</td>
</tr>
<tr>
<td>Use CRL from certificates</td>
<td>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.</td>
</tr>
<tr>
<td>CRL Location</td>
<td>Enter the server file path or the local file path from which to retrieve the CRL.</td>
</tr>
<tr>
<td>Enable OCSP Revocation</td>
<td>Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.</td>
</tr>
<tr>
<td>Use CRL in case of OCSP failure</td>
<td>If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSP checking is not available.</td>
</tr>
<tr>
<td>Send OCSP Nonce</td>
<td>Select this check box if you want the unique identifier of the OCSP request to be sent in the response.</td>
</tr>
<tr>
<td>OCSP URL</td>
<td>If you enabled OCSP revocation, enter the OCSP server address for revocation checking.</td>
</tr>
<tr>
<td>OCSP Responder's Signing</td>
<td>Enter the path to the OCSP certificate for the responder. Enter as /path/to/file.cer</td>
</tr>
</tbody>
</table>

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. See “Managing Authentication Methods to Apply to Users,” on page 84

**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 AirWatch Tunnel proxy server.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter the name for this built-in identity provider instance.</td>
</tr>
<tr>
<td>Users</td>
<td>Select which users to authentication. The configured directories are listed.</td>
</tr>
<tr>
<td>Network</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>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. For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page.</td>
</tr>
</tbody>
</table>

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. See “Using the Cloud Hosted KDC Service,” on page 77.
4. Click Add.

What to do next

Make sure that the authentication methods that you selected is configured in the access policies.

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)
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.

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

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 directories 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.

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

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,” on page 84.
- 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.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider Name</td>
<td>Enter a name for this identity provider instance.</td>
</tr>
<tr>
<td>SAML Binding</td>
<td>Select how the AuthnRequest should be sent, either HTTP POST or HTTP Redirect. HTTP Redirect is the default.</td>
</tr>
<tr>
<td>SAML Metadata</td>
<td>Add the third-party identity provider XML-based metadata document to establish trust with the identity provider.</td>
</tr>
<tr>
<td></td>
<td>1. Enter the SAML metadata URL or the xml content into the text box.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>4. (Optional) Select the NameIDPolicy response identifier string format.</td>
</tr>
<tr>
<td>Just-in-Time Provisioning</td>
<td>N/A</td>
</tr>
<tr>
<td>Users</td>
<td>Select the Other Directory which includes the users who can authenticate using this identity provider.</td>
</tr>
<tr>
<td>Network</td>
<td>The existing network ranges configured in the service are listed. Select the network ranges for the users based on their IP addresses, that you want to direct to this identity provider instance for authentication.</td>
</tr>
<tr>
<td>Authentication Methods</td>
<td>Add the authentication methods supported by the third-party identity provider. Select the SAML authentication context class that supports the authentication method.</td>
</tr>
<tr>
<td>Single Sign-Out Configuration</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Form Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAML Signing Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>IdP Hostname</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

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

3 Edit the Add Network Range page.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network range.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the network range.</td>
</tr>
<tr>
<td>IP Ranges</td>
<td>Edit or add IP ranges until all desired and no undesired IP addresses are included.</td>
</tr>
</tbody>
</table>

**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 9, “Managing Access Policies,” on page 87.

**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 9, “Managing Access Policies,” on page 87.

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,” on page 87 to learn more about setting up policy rules.

**Prerequisites**

Enable and configure the authentication methods that your organization supports. See Chapter 8, “Configuring User Authentication in VMware Identity Manager,” on page 55.

**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

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 chapter includes the following topics:

- “Configuring Access Policy Settings,” on page 87
- “Managing Web and Desktop Application-Specific Policies,” on page 89
- “Add a Web or Desktop Application-Specific Policy,” on page 90
- “Configure Custom Access Denied Error Message,” on page 91
- “Edit Default Access Policy,” on page 91
- “Enabling Compliance Checking for AirWatch Managed Devices,” on page 92
- “Enabling Persistent Cookie on Mobile Devices,” on page 94

**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,” on page 51.

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.
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,” on page 84.
- 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.

Procedure

1. In the administration console Policies tab, click Add Policy to add a new policy.
2 Add a policy name and description in the respective text boxes.
3 In the Applies To section, click Select and in the page that appears, select the applications to associate with this policy.
4 In the Policy Rules section, click + to add a rule.
   a The Add a Policy Rule page appears.
   b Select the network range to apply to this rule.
   c Select the type of device that can access the applications for this rule.
   d Select the authentication methods to use in the order the authentication method should be applied.
   e Specify the number of hours an application session can be open.
   f Click Save.
5 Configure additional rules as appropriate.
6 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,” on page 84.

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,” on page 90

Enabling Compliance Checking for AirWatch Managed Devices

When users enroll their devices through the AirWatch Agent application, 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’ 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.

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 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.
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.
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 chapter includes the following topics:

- “User and Group Types,” on page 95
- “About User Names and Group Names,” on page 96
- “Managing Users,” on page 97
- “Create Groups and Configure Group Rules,” on page 97
- “Edit Group Rules,” on page 100
- “Add Resources to Groups,” on page 100
- “Create Local Users,” on page 100
- “Managing Passwords,” on page 102

### 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 6, “Just-in-Time User Provisioning,” on page 43.
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,” on page 97.

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 6, “Just-in-Time User Provisioning,” on page 43 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**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>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 <strong>Group Is Sales</strong> and <strong>Group Is Marketing</strong>, sales and marketing staff are granted membership to this group.</td>
</tr>
<tr>
<td>All</td>
<td>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 <strong>Group Is Sales</strong> and <strong>Email Starts With 'western_region'</strong>, only sales staff in the western region are granted membership to this group. Sales staff in other regions is not granted membership.</td>
</tr>
</tbody>
</table>
8 Configure one or more rules for your group. You can nest rules.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>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.</td>
</tr>
<tr>
<td>Attribute Rules</td>
<td>The following rules are available depending on the attribute you selected.</td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>- 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 can create a rule such as Phone matches (555) 555-1000.</td>
<td></td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>- 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 <a href="mailto:sales_username@example.com">sales_username@example.com</a>. If you want to grant access to an application to everyone in your sales staff, you can create a rule, such as email starts with sales_.</td>
<td></td>
</tr>
<tr>
<td>- 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 <a href="mailto:hr_username@example.com">hr_username@example.com</a>, 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.</td>
<td></td>
</tr>
<tr>
<td>Using Attribute Any or All</td>
<td>(Optional) To include the attributes Any or All as part of the group rule, add this rule last.</td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
<tr>
<td>- 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.</td>
<td></td>
</tr>
</tbody>
</table>

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.
   - To disable the account, deselect the Enable check box
   - 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length for passwords</td>
<td>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.</td>
</tr>
<tr>
<td>Lowercase characters</td>
<td>Minimum number of lowercase characters. Lowercase a-z</td>
</tr>
<tr>
<td>Uppercase characters</td>
<td>Minimum number of uppercase characters. Uppercase A-Z</td>
</tr>
<tr>
<td>Numerical characters (0-9)</td>
<td>Minimum number of numerical characters. Base ten digits (0-9)</td>
</tr>
<tr>
<td>Special characters</td>
<td>Minimum number of non-alphanumeric characters, for example &amp; # % $ !</td>
</tr>
<tr>
<td>Consecutive identical characters</td>
<td>Maximum number of identical adjacent characters. For example, if you enter 1, the following password is allowed: p@$$word, but this password is not allowed: p@$$word.</td>
</tr>
<tr>
<td>Password history</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary password lifetime</td>
<td>Number of hours a password reset or forgot password link is valid. The default is 168 hours</td>
</tr>
<tr>
<td>Password lifetime</td>
<td>Maximum number of days that a password can exist before the user must change it.</td>
</tr>
<tr>
<td>Password reminder</td>
<td>Number of days before a password expiration that the password expiry notice is sent.</td>
</tr>
<tr>
<td>Password reminder notification frequency</td>
<td>After the first password expiry notice is sent, how frequently reminders are sent.</td>
</tr>
</tbody>
</table>

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

4. Click Save.
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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>How to See the Resource in Your Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web application</td>
<td>In the admin console Catalog page, select the Web Applications application type.</td>
</tr>
<tr>
<td>Virtualized Windows application captured as a</td>
<td>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.</td>
</tr>
<tr>
<td>ThinApp package</td>
<td></td>
</tr>
<tr>
<td>View Desktop Pool</td>
<td>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.</td>
</tr>
<tr>
<td>View Hosted Applications</td>
<td>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.</td>
</tr>
<tr>
<td>Citrix-based application</td>
<td>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.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Managing Resources in the Catalog,” on page 105
- “Grouping Resource into Categories,” on page 109
- “Managing Catalog Settings,” on page 110

**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 View desktop pools and View Hosted applications, or Citrix-based applications.

To integrate and enable View 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.

**Web Applications**

You populate your catalog with Web applications directly on the Catalog page of the administration console. When you click a Web application displayed on the Catalog page, information about that application is displayed. From the displayed page, you can configure the Web application, such as by providing the appropriate SAML attributes to configure single sign-on between VMware Identity Manager and the target Web application. When the Web application is configured, you can then entitle users and groups to that Web application. See “Adding Web Applications to Your Catalog,” on page 106.

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

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Resource Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application ...from the cloud application catalog</td>
<td>Web application</td>
<td>VMware Identity Manager includes access to default Web applications available in the cloud application catalog that you can add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... create a new one</td>
<td>Web application</td>
<td>By filling out the appropriate form, you can create an application record for the Web applications you want to add to your catalog as resources.</td>
</tr>
<tr>
<td>Web Application ... import a ZIP or JAR file</td>
<td>Web application</td>
<td>You can import a Web application that you previously configured. 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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the application.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the application that users can read.</td>
</tr>
<tr>
<td>Icon</td>
<td><strong>Click Browse</strong> to upload an icon for the application. Icons in PNG, JPG, and ICON file formats, up to 4MB, are supported. 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.</td>
</tr>
<tr>
<td>Categories</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlements</td>
<td>Entitle users and groups to the application. You can configure entitlements while initially configuring the application or anytime in the future.</td>
</tr>
<tr>
<td>Access Policies</td>
<td>Apply an access policy to control user access to the application.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Configure approval tracking. Add license information for the application to track license use in reports. Approvals must be enabled and configured in the Catalog &gt; Settings page. You must also register the callback URI of the approval request handler.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>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 <a href="https://www.vmware.com/support/pubs/vidm_webapp_sso.html">https://www.vmware.com/support/pubs/vidm_webapp_sso.html</a> for configuration guides for these applications.</td>
</tr>
</tbody>
</table>

**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.
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,” on page 109.

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.

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

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.

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

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 Clients 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 in the admin console **Catalog > Settings** page.

The SDK uses OAuth based authentication to connect to VMware Identity Manager. You must create a client ID value and a clientSecret value in the admin console.

**Create 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.

**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.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Type</td>
<td>Options are User Access Token or Service Client Token.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Enter a unique client ID for the resource to be registered with VMware Identity Manager.</td>
</tr>
<tr>
<td>Application</td>
<td>Select Identity Manager.</td>
</tr>
<tr>
<td>scope</td>
<td>Select the appropriate scope. When you select NAAPS, OpenID is also selected.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>Enter the registered redirect URI.</td>
</tr>
<tr>
<td>Advanced Section</td>
<td>Click <strong>Generate Shared Secret</strong> to generate a secret that is shared between this service and the application resource service.</td>
</tr>
<tr>
<td></td>
<td>Copy and save the client secret to configure in the application setup.</td>
</tr>
<tr>
<td></td>
<td>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 apps.</td>
</tr>
<tr>
<td>Issue Refresh Token</td>
<td>Deselect the checkbox.</td>
</tr>
<tr>
<td>Token Type</td>
<td>Select Bearer</td>
</tr>
<tr>
<td>Token Length</td>
<td>Leave the default setting, 32 Bytes.</td>
</tr>
<tr>
<td>Issue Refresh Token</td>
<td>Check Refresh Token.</td>
</tr>
<tr>
<td>Access Token TTL</td>
<td>(Optional) Change the <strong>Access Token Time-To-Live</strong> settings.</td>
</tr>
<tr>
<td>Refresh Token TTL</td>
<td>(Optional)</td>
</tr>
<tr>
<td>User Grant</td>
<td>Do not check Prompt users for access.</td>
</tr>
</tbody>
</table>

4. Click **Add**.
The client configuration is displayed on the OAuth2 Client page, along with the shared secret that was generated.

**What to do next**

Enter the Client ID and the shared secret in the resources configuration pages. 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.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template ID</td>
<td>Enter a unique identifies for this resource.</td>
</tr>
<tr>
<td>Application</td>
<td>Select Identity Manager</td>
</tr>
<tr>
<td>scope</td>
<td>Select the appropriate scope. When you select NAAPS, OpenID is also selected.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>Enter the registered redirect URI.</td>
</tr>
</tbody>
</table>

**Advanced Section**

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Select Bearer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Length</td>
<td>Leave the default setting, 32 Bytes.</td>
</tr>
<tr>
<td>Issue Refresh Token</td>
<td>Check Refresh Token.</td>
</tr>
<tr>
<td>Access Token TTL</td>
<td>(Optional)</td>
</tr>
<tr>
<td>Refresh Token TTL</td>
<td>(Optional)</td>
</tr>
<tr>
<td>User Grant</td>
<td>Do not check Prompt users for access.</td>
</tr>
</tbody>
</table>

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 the 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URI</strong></td>
<td>Enter the callback URI of the REST resource that listens for the callout request.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>(Optional) Enter the password of the user.</td>
</tr>
<tr>
<td>PEM-format SSL Certificate</td>
<td>(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.</td>
</tr>
</tbody>
</table>

**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.
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 chapter includes the following topics:

- “Monitor Users and Resource Usage from the Dashboard,” on page 117
- “Monitor System Information and Health,” on page 118
- “Viewing Reports,” on page 118

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 12-1. Report Types

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recent Activity</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Usage</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Entitlements</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Activity</td>
<td>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.</td>
</tr>
<tr>
<td>Group Membership</td>
<td>Group membership is a lists the members of a group you specify.</td>
</tr>
<tr>
<td>Role Assignment</td>
<td>Role assignment lists the users that are either API-only administrators or administrators and their email addresses.</td>
</tr>
<tr>
<td>Users</td>
<td>Users report lists all the users and provides details about each user, such as the user’s email address, role, and group affiliations.</td>
</tr>
<tr>
<td>Concurrent Users</td>
<td>Concurrent users report shows the number of user sessions that were opened at one time and the date and time.</td>
</tr>
<tr>
<td>Device Usage</td>
<td>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.</td>
</tr>
<tr>
<td>Audit events</td>
<td>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 &gt; Settings &gt; Auditing page. See “Generate an Audit Event Report,” on page 119.</td>
</tr>
</tbody>
</table>

Generate an Audit Event Report

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

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

Prerequisites

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.

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

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.
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 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 chapter includes the following topics:

- “Customize Branding in VMware Identity Manager Service,” on page 121
- “Customize Branding for the User Portal,” on page 122
- “Customize Branding for VMware Verify Application,” on page 123

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.

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

**Sign-In Screen Tab**
### 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.

<table>
<thead>
<tr>
<th>Form Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logo</strong></td>
<td>Add a masthead logo to be the banner at the top of the admin console and Workspace ONE portal Web pages. The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG, or GIF.</td>
</tr>
<tr>
<td><strong>Masthead Background Color</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Masthead Text Color</strong></td>
<td>Enter a six-digit hexadecimal color code over the existing one to change the color of the text that displays in the masthead.</td>
</tr>
</tbody>
</table>
### Background Color
The color that displays for the background of the Web portal screen. 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.

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.

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 Transparency
To set a transparency color, move the slider on the transparency bar.

### Name and Icon Color
You can select the text color for names listed under the icons on the app portal pages. 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.

### 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.

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

3 Click **Save**.
AirWatch provides enterprise mobility management for devices and VMware Identity Manager provides single sign-on and identity management for users.

When AirWatch and VMware Identity Manager are integrated, users from AirWatch enrolled devices can log in to their enabled apps securely without entering multiple passwords.

When AirWatch is integrated with VMware Identity Manager, you can configure the following integrations with AirWatch:

- An AirWatch directory that syncs AirWatch users and groups to a directory in VMware Identity Manager service and then set up password authentication through the AirWatch Cloud Connector.
- Single sign-on to a unified catalog containing entitled apps from both AirWatch and VMware Identity Manager managed.
- Single sign-on using Kerberos authentication to iOS 9 devices.
- Access policy rules to check that AirWatch-managed iOS 9 devices are in compliance.

This chapter includes the following topics:

- “Setting up AirWatch for Integration with VMware Identity Manager,” on page 125
- “Setting up an AirWatch Instance in VMware Identity Manager,” on page 129
- “Enable Unified Catalog for AirWatch,” on page 131
- “Implementing Authentication with AirWatch Cloud Connector,” on page 132
- “Implementing Mobile Single Sign-in Authentication for AirWatch-Managed iOS Devices,” on page 134
- “Implementing Mobile Single Sign-On Authentication for AirWatch-Managed Android Devices,” on page 141
- “Enabling Compliance Checking for AirWatch Managed Devices,” on page 147
- “Registering Email Domains for Auto Discovery,” on page 148

**Setting up AirWatch for Integration with VMware Identity Manager**

You configure settings in the AirWatch admin console to communicate with VMware Identity Manager before you configure AirWatch settings in the VMware Identity Manager admin console.

To integrate AirWatch and VMware Identity Manager, the following is required:

- The organization group in AirWatch for which you are configuring VMware Identity Manager is **Customer**.
A REST API admin key for communication with the VMware Identity Manager service and a REST enrolled user API key for AirWatch Cloud Connector password authentication are created at the same organization group where VMware Identity Manager is configured.

- API Admin account settings and the admin auth certificate from AirWatch added to the AirWatch settings in the VMware Identity Manager admin console.
- Active Directory user accounts set up at the same organization group where VMware Identity Manager is configured.
- If end users are placed into a child organization group from where VMware Identity Manager is configured after registration and enrollment, User Group mapping in the AirWatch enrollment configuration must be used to filter users and their respective devices to the appropriate organization group.

The following are set up in the AirWatch admin console.

- REST admin API key for communication with the VMware Identity Manager service
- API Admin account for VMware Identity Manager and the admin auth certificate that is exported from AirWatch and added to the AirWatch settings in VMware Identity Manager
- REST enrolled user API key used for AirWatch Cloud Connector password authentication

Create REST API Keys in AirWatch

REST Admin API access and enrolled users access must be enabled in the AirWatch admin console to integrate VMware Identity Manager with AirWatch. When you enable API access, an API key is generated.

**Procedure**

1. In the AirWatch admin console, select the Global > Customer-level organization group and navigate to Groups & Settings > All Settings > System > Advanced > API > Rest API.
2. In the General tab, click **Add** to generate the API key to use in the VMware Identity Manager service. The account type should be Admin.
   - Provide a unique service name. Add a description, such as **AirWatchAPI for IDM**.
3. To generate the enrollment user API key, click **Add** again.
4. In the Account Type drop-down menu, select **Enrollment User**.
   - Provide a unique service name. Add a description such as **UserAPI for IDM**.
Copy the two API keys and save the keys to a file. You add these keys when you set up AirWatch in the VMware Identity Manager admin console.

![Image of REST API settings in AirWatch admin console]

Click Save.

### Create Admin Account and Certificate in AirWatch

After the admin API key is created, you add an admin account and set up certificate authentication in the AirWatch admin console.

For REST API certificate-based authentication, a user level certificate is generated from the AirWatch admin console. The certificate used is a self-signed AirWatch certificate generated from the AirWatch admin root cert.

#### Prerequisites

The AirWatch REST admin API key is created.

#### Procedure

1. In the AirWatch admin console, select the Global > Customer-level organization group and navigate to Accounts > Administrators > List View.
2. Click Add > Add Admin.
3 In the Basic tab, enter the certificate admin user name and password in the required text boxes.

![Add / Edit Admin](image)

4 Select the Roles tab and choose the current organization group and click the second text box and select **AirWatch Administrator**.

5 Select the API tab and in the Authentication text box, select **Certificates**.

6 Enter the certificate password. The password is the same password entered for the admin on the Basic tab.

7 Click **Save**.

   The new admin account and the client certificate are created.

8 In the List View page, select the admin you created and open the API tab again.

   The certificates page displays information about the certificate.

9 Enter the password you set in the Certificate Password text box, click **Export Client Certificate** and save the file.

![Add / Edit Admin](image)
The client certificate is saved as a .p12 file type.

What to do next
Configure your AirWatch URL settings in the VMware Identity Manager admin console.

Setting up an AirWatch Instance in VMware Identity Manager
After you configure the settings in the AirWatch admin console, in the VMware Identity Manager admin console Identity & Access Management page, you enter the AirWatch URL, the API key values, and the certificate. After AirWatch settings are configured, you can enable feature options available with AirWatch integration.

Mapping VMware Identity Manager Domains to Multiple Organization Groups in AirWatch
When setting up users and devices in AirWatch, AirWatch uses organization groups (OG) to organize and group users and to establish permissions. When AirWatch is integrated with VMware Identity Manager, the admin and enrollment user REST API keys can only be configured at the AirWatch organization group of type Customer.

In AirWatch environments configured for multi-tenancy, many organization groups are created for users and devices. Devices become registered or enrolled into an organization group. Organization groups can be set up in unique configurations in a multi-tenancy environment. For example, organization groups by separate geographies, departments, or use cases. In the AirWatch integration page, you add the organization group ID and enter the AirWatch admin API key that is used to make API requests.

You can link domains configured in VMware Identity Manager to specific organization groups in AirWatch to manage device registration through Workspace ONE. When users log in to Workspace ONE, a device registration event is triggered within VMware Identity Manager. During the device registration, a request is sent to AirWatch to pull any applications that the user and device combination is entitled to.

The device organization groups must be identified when AirWatch is integrated with VMware Identity Manager so that identity manager can locate the user and successfully register the device into the appropriate organization group.

When you configure the AirWatch settings in the VMware Identity Manager service, you can enter device organization group IDs and the API keys to map multiple OG to a domain. When users sign in to Workspace ONE from their devices, the user records are verified and the device is registered to the appropriate organization group in AirWatch.

Note When AirWatch is integrated with VMware Identity Manager and multiple AirWatch organization groups are configured, the Active Directory Global Catalog option cannot be configured for use with the VMware Identity Manager service.

Add AirWatch Settings in VMware Identity Manager Admin Console
Configure the AirWatch settings in the VMware Identity Manager admin console to integrate AirWatch with VMware Identity Manager.

You can link domains configured in VMware Identity Manager to specific organization groups in AirWatch to facilitate device registration in AirWatch. See Mapping VMware Identity Manager Domains to Multiple Organization Groups.

Prerequisites
- AirWatch server URL that the admin uses to log in to the AirWatch admin console.
- AirWatch admin API key that is used to make API requests from VMware Identity Manager to the AirWatch server to set up integration.

- AirWatch certificate file used to make API calls and the certificate password. The certificate file must be in the .p12 file format.

- AirWatch enrolled user API key.

- AirWatch group ID for your tenant, which is the tenant identifier in AirWatch.

**Procedure**

1. In the VMware Identity Manager administration console, Identity & Access Management tab, click Setup > AirWatch.

2. Enter the AirWatch integration settings in the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch API URL</td>
<td>Enter the AirWatch URL. For example, <a href="https://myco.airwatch.com">https://myco.airwatch.com</a></td>
</tr>
<tr>
<td>AirWatch API Certificate</td>
<td>Upload the certificate file used to make API calls.</td>
</tr>
<tr>
<td>Certificate Password</td>
<td>Enter the certificate password.</td>
</tr>
<tr>
<td>AirWatch Admin API Key</td>
<td>Enter the admin API key value. Example of an API key value</td>
</tr>
<tr>
<td></td>
<td>FPseqC5ataGcn3f8/Rvahzn/4jwkZENGkZyyc+jveeYs=</td>
</tr>
<tr>
<td>AirWatch Enrolled User API Key</td>
<td>Enter the enrolled user API key value.</td>
</tr>
<tr>
<td>AirWatch Group ID.</td>
<td>Enter the AirWatch group ID for the organization group that the API key and admin account were created in.</td>
</tr>
</tbody>
</table>

3. To map domains to multiple organization groups, select the **Map Domains to Multiple Organization Groups** check box.

   a. Select the domain to map from the drop-down menu and . Click + to map additional organization groups to the domain.

   b. Enter the organization group name and the admin API key for that group in the text boxes that display.

   c. Click + to map additional organization groups to the domain.

   d. To map another domain, click + next to the drop-down menu.
4 Click Save.

What to do next

- Enable the feature option Unified Catalog to merge apps set up in the AirWatch catalog to the unified catalog.
- Enable Compliance check to verify that AirWatch managed devices adhere to AirWatch compliance policies.

Enable Unified Catalog for AirWatch

When you configure VMware Identity Manager with your AirWatch instance, you can enable the unified catalog so that end users see all apps that they are entitled to from both VMware Identity Manager and AirWatch.

When AirWatch is not integrated with the unified catalog, end users see only the apps that they are entitled to from the VMware Identity Manager service.

Prerequisites

AirWatch configured in VMware Identity Manager.

Procedure

1. In the administration console, Identity & Access Management tab, click Setup > AirWatch.
2. In the Unified Catalog section on this page, select Enable.
3. Click Save.
What to do next

Notify AirWatch end users about how to access the unified catalog and view their Workspace ONE portal through VMware Identity Manager.

Implementing Authentication with AirWatch Cloud Connector

AirWatch Cloud Connector (ACC) component of VMware Enterprise Systems Connector is integrated with VMware Identity Manager for user password authentication in Workspace ONE.

**NOTE** You install ACC and configure the ACC component in AirWatch. See the VMware Enterprise Systems Connector Installation and Configuration guide for information about installing and configuring the AirWatch Cloud Connector. After the ACC is installed and configured, you integrate the AirWatch directory services with Active Directory. See the VMware AirWatch Directory Services Guide for information about enabling the directory services.

To implement AirWatch Cloud Connector authentication for Workspace ONE, in the VMware Identity Manager admin console, the Password (AirWatch Connector) authentication method is associated to a built-in identity provider.

You can enable just-in-time support in AirWatch to add new users to the VMware Identity Manager directory when users sign in for the first time. When just-in-time support is enabled, users do not need to wait for the next scheduled sync from the AirWatch server to access Workspace ONE. Instead, new users log in to their Workspace ONE portal, either from an iOS or Android device or their desktop computer and enter their Active Directory user name and password. The VMware Identity Manager service authenticates the Active Directory credentials through the AirWatch Cloud Connector and adds the user profile to the directory.

After you associate the authentication methods in the built-in identity provider, you create access policies to apply to this authentication method.

**NOTE** User name and password authentication are integrated into the AirWatch Cloud Connector deployment. To authenticate users using other VMware Identity Manager-supported authentication methods, the VMware Identity Manager connector must be configured.

Managing User Attributes Mapping

You can configure the user attribute mapping between the AirWatch directory and the VMware Identity Manager directory.

The User Attributes page in the VMware Identity Manager, Identity & Access Management tab lists the default directory attributes that are mapped to AirWatch Directory attributes. Attributes that are required are marked with an asterisk. Users missing a required attribute in their profile are not synced to the VMware Identity Manager service.

<table>
<thead>
<tr>
<th>VMware Identity Manager User Attribute Name</th>
<th>Default Mapping to AirWatch User Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>userPrincipalName</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>distinguishedName</td>
<td>distinguishedName</td>
</tr>
<tr>
<td>employeeID</td>
<td>employeeID</td>
</tr>
<tr>
<td>domain</td>
<td>Domain</td>
</tr>
<tr>
<td>disabled (external user disabled)</td>
<td>disabled</td>
</tr>
<tr>
<td>phone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>lastName</td>
<td>lastname*</td>
</tr>
</tbody>
</table>
Table 14-1. Default AirWatch Directory Attributes Mapping (Continued)

<table>
<thead>
<tr>
<th>VMware Identity Manager User Attribute Name</th>
<th>Default Mapping to AirWatch User Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>firstName</td>
<td>firstname*</td>
</tr>
<tr>
<td>email</td>
<td>Email*</td>
</tr>
<tr>
<td>userName</td>
<td>username*</td>
</tr>
</tbody>
</table>

Sync Users and Groups from AirWatch Directory to VMware Identity Directory

You configure the VMware Identity Manager settings in the AirWatch admin console to establish a connection between your organization group instance of the AirWatch Directory and VMware Identity Manager. This connection is used to sync users and groups to a directory created in the VMware Identity Manager service.

The VMware Identity Manager directory can be used with the AirWatch Cloud Connector for password authentication.

Users and groups initially sync to the VMware Identity Manager directory manually. The AirWatch sync schedule determines when users and groups sync with the VMware Identity Manager directory.

When a user or a group is added or deleted on the AirWatch server, the change is reflected on the VMware Identity Manager service immediately.

Prerequisites

- VMware Identity Manager local admin name and password.
- Identify attribute values to map from the AirWatch directory. See “Managing User Attributes Mapping,” on page 132.

Procedure

1. In the AirWatch admin console, Groups & Settings, All Settings page, select the Global > Customer-level organization group and navigate to System > Enterprise Integration > VMware Identity Manager.

2. In the Server section, click Configure.

**NOTE** The configuration button is only available when the Directory Service is also configured for the same organization group. If the Configure button is not visible, you are not in the correct organization group. You can change the organization group in the Global drop-down menu.

3. Enter the VMware Identity Manager settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter your tenant VMware URL. For example, <a href="https://myco.identitymanager.com">https://myco.identitymanager.com</a>.</td>
</tr>
<tr>
<td>Admin Username</td>
<td>Enter the VMware Identity Manager local admin user name.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the VMware Identity Manager local admin user's password.</td>
</tr>
</tbody>
</table>

4. Click Next.

5. Enable custom mapping to configure the user attributes mapping from AirWatch to the VMware Identity Manager service.

6. Click Test Connection to verify that the settings are correct.

7. Click Sync Now to manually sync all users and groups to VMware Identity Manager service.

**NOTE** To control the system load, manual sync can only be performed four hours after a previous sync.
An AirWatch directory is created in the VMware Identity Manager service and the users and groups are synced to a directory in VMware Identity Manager.

What to do next
Review the Users and Groups tab in the VMware Identity Manager admin console to verify that the user and group names are synced.

Updating VMware Identity Manager after Upgrading AirWatch
When you upgrade AirWatch to a new version, you must update the Unified Catalog and User Password Authentication through AirWatch configuration options in the VMware Identity Manager service.

When you save these option after you upgrade AirWatch, the AirWatch settings in the VMware Identity Manager service are updated with the new version of AirWatch.

Procedure
1. After you upgrade AirWatch, sign in to the VMware Identity Manager admin console.
2. In the Identity & Access Management tab, click Setup > AirWatch.
3. Scroll down the page to the Unified Catalog section and click Save.
4. Scroll down to the User Password Authentication through AirWatch section and click Save.

The AirWatch configuration is updated with the new version in the VMware Identity Manager service.

Implementing Mobile Single Sign-in Authentication for AirWatch-Managed iOS Devices
For iOS device authentication, VMware Identity Manager uses an identity provider that is built in to the VMware Identity Manager service to provide access to mobile SSO authentication. This authentication method for iOS devices uses a Key Distribution Center (KDC) without the use of a connector or a third-party system. Kerberos authentication provides users, who are successfully signed in to their domain, access to their Workspace ONE apps portal without additional credential prompts.

VMware Identity Manager Cloud tenants do not need to manage or configure the KDC.

For the VMware Identity Manager service on premises, two KDC service options are available. One option is to use the built-in KDC that you initialize in the VMware Identity Manager appliance before you enable the mobile SSO authentication method from the administration console. The second option is to use the VMware Identity Manager KDC cloud hosted service. For more information about the built-in KDC, see the Installing and Configuring VMware Identity Manager guide. To use the Cloud Hosted KDC Service, see “Using the Cloud Hosted KDC Service,” on page 77.

When the identity manager is configured with AirWatch in a Windows environment, the iOS Mobile authentication method must be configured to use the VMware Identity Manager cloud hosted KDC service.

Implementing Mobile SSO authentication for AirWatch-managed iOS 9 or later devices requires the following configuration steps.

- Download the issuer certificate to configure Mobile SSO for iOS
  - If you are using Active Directory Certificate Services, configure a certificate authority template for Kerberos certificate distribution in the Active Directory Certificate Services. Then configure AirWatch to use Active Directory Certificate Authority. Add the Certificate template in the AirWatch admin console. Download the issuer certificate to configure Mobile SSO for iOS.
  - If you are using AirWatch Certificate Authority, enable Certificates in the VMware Identity Manager Integrations page. Download the issuer certificate to configure Mobile SSO for iOS.
Configure the iOS device profile and enable single sign-in from the AirWatch admin console.

Configure the Mobile SSO (iOS) authentication method

Configure the built-in identity provider and associate the Mobile SSO for iOS authentication in the VMware Identity Manager administration console.

**Configure Active Directory Certificate Authority in AirWatch**

To set up single sign-on authentication to AirWatch managed iOS 9 mobile devices, you can set up a trust relationship between Active Directory and AirWatch and enable the Mobile SSO for iOS authentication method in VMware Identity Manager.

After you configured the certificate authority and certificate template for Kerberos certificate distribution in the Active Directory Certificate Services, you enable AirWatch to request the certificate used for authentication and add the certificate authority to the AirWatch admin console.

**Procedure**

1. In the AirWatch admin console main menu, navigate to Devices > Certificates > Certificate Authorities.
2. Click Add.
3. Configure the following in the Certificate Authority page.

   **Note** Make sure that Microsoft AD CS is selected as the Authority Type before you start to complete this form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the new Certificate Authority.</td>
</tr>
<tr>
<td>Authority Type</td>
<td>Make sure that Microsoft AD CS is selected.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select ADCS as the protocol.</td>
</tr>
<tr>
<td>Server Hostname</td>
<td>Enter the URL of the server. Enter the hostname in this format https://{servername.com}/certsrv.adcs/. The site can be http or https depending on how the site is set up. The URL must include the trailing /. <strong>Note</strong> If the connection fails when you test the URL, remove the http:// or https:// from the address and test the connection again.</td>
</tr>
<tr>
<td>Authority Name</td>
<td>Enter the name of the certificate authority that the ADCS end point is connected to. This name can be found by launching the Certification Authority application on the certificate authority server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Make sure that Service Account is selected.</td>
</tr>
<tr>
<td>Username and Password</td>
<td>Enter the user name and password of the AD CS admin account with sufficient access to allow AirWatch to request and issue certificates.</td>
</tr>
</tbody>
</table>

4. Click Save.

**What to do next**

Configure the Certificate Template in AirWatch.

**Configuring AirWatch to use Active Directory Certificate Authority**

Your certificate authority template must be properly configured for Kerberos certificate distribution. In the Active Directory Certificate Services (AD CS), you can duplicate the existing Kerberos Authentication template to configure a new certificate authority template for the iOS Kerberos authentication.

When you duplicate the Kerberos Authentication template from AD CS, you must configure the following information in the Properties of New Template dialog box.
Add Certificate Template in AirWatch

You add the certificate template that associates the certificate authority used to generate the user’s certificate.

Prerequisites

Configure the Certificate Authority in AirWatch.

Procedure

1. In the AirWatch admin console, navigate to System > Enterprise Integration > Certificate Authorities.
2. Select the Request Template tab and click Add.
3. Configure the following in the certificate template page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the new request template in AirWatch.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>In the drop-down menu, select the certificate authority that was created.</td>
</tr>
<tr>
<td>Issuing Template</td>
<td>Enter the Microsoft CA certificate template name exactly as you created in AD CS. For example, iOSKerberos.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subject Name</td>
<td>After CN=, enter <code>{EnrollmentUser}</code>, where the {} text box is the AirWatch lookup value. The text entered here is the Subject of the certificate, which can be used to determine who received the certificate.</td>
</tr>
<tr>
<td>Private Key Length</td>
<td>This private key length matches the setting on the certificate template that is being used by AD CS. It is usually 2048.</td>
</tr>
<tr>
<td>Private Key Type</td>
<td>Select the check box for Signing and Encryption.</td>
</tr>
<tr>
<td>San Type</td>
<td>For the Subject Alternate Name, select User Principal Name. The value must be <code>{EnrollmentUser}</code>. If device compliance check is configured with Kerberos authentication, you must set a second SAN type to include the UDID. Select the San type DNS. The value must be UDID={DeviceUid}.</td>
</tr>
<tr>
<td>Automatic Certificate Renewal</td>
<td>Select the check box to have certificates using this template automatically renewed before their expiration date.</td>
</tr>
<tr>
<td>Auto Renewal Period (days)</td>
<td>Specify the auto renewal in days.</td>
</tr>
<tr>
<td>Enable Certificate Revocation</td>
<td>Select the check box to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.</td>
</tr>
<tr>
<td>Publish Private Key</td>
<td>Select this check box to publish the private key.</td>
</tr>
<tr>
<td>Private Key Destination</td>
<td>Either Directory Service or Custom Web Service</td>
</tr>
</tbody>
</table>

4 Slick Save.

![Certificate Template - Add / Edit](image)

**What to do next**

In the Identity Provider admin console, configure the built-in identity provider with the Mobile SSO for iOS authentication method.
Configure Apple iOS Profile in AirWatch Using Active Directory Certificate Authority and Certificate Template

Create and deploy the Apple iOS device profile in AirWatch to push the Identity Provider settings to the device. This profile contains the information necessary for the device to connect to the VMware Identity Provider and the certificate that the device used to authenticate. Enable single sign-on to allow seamless access without requiring authentication into each app.

**Prerequisites**

- Mobile SSO for iOS is configured in VMware Identity Manager.
- iOS Kerberos certificate authority file saved to a computer that can be accessed from the AirWatch admin console.
- Your Certificate Authority and Certificate Template is properly configured in AirWatch.
- List of URLs and application bundle IDs that use Mobile SSO for iOS authentication on iOS devices.

**Procedure**

1. In the AirWatch admin console, navigate to Devices > Profiles & Resources > Profiles.
2. Select Add > Add Profile and select Apple iOS.
3. Enter the name as iOSKerberos and configure the General settings.
4. In the left navigation pane, select Credentials > Configure to configure the credential.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Source</td>
<td>Select Defined Certificate Authority from the drop-down menu.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Select the certificate authority from the list in the drop-down menu.</td>
</tr>
<tr>
<td>Certificate Template</td>
<td>Select the request template that references the certificate authority from the drop-down menu. This is the certificate template created in Adding the Certificate Template in AirWatch.</td>
</tr>
</tbody>
</table>

5. Click + in the lower right corner of the page again and create a second credential.
6. In the Credential Source drop-down menu, select Upload.
7. Enter a credential name.
8. Click Upload to upload the KDC server root certificate that is downloaded from the Identity & Access Management > Manage > Identity Providers > Built-in Identity provider page.
9. In the left navigation pane, select Single Sign-On and click Configure.
10. Enter the connection information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Enter Kerberos.</td>
</tr>
<tr>
<td>Kerberos Principal Name</td>
<td>Click + and select [EnrollmentUser].</td>
</tr>
<tr>
<td>Realm</td>
<td>Enter the realm name you used when you initialized KDC in the VMware Identity Manager appliance. For example, EXAMPLE.COM</td>
</tr>
<tr>
<td>Renewal Certificate</td>
<td>Select Certificate #1 from the drop-down menu. This is the Active Directory CA cert that was configured first under credentials.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
**URL Prefixes** | Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. Enter the VMware Identity Manager server URL as https://myco.example.com.

**Applications** | Enter the list of application identities that are allowed to use this sign-on. To perform single sign-on using iOS built-in Safari browser, enter the first application bundle ID as com.apple.mobilesafari. Continue to enter application bundle IDs. The applications listed must support SAML authentication.

11 Click **Save & Publish**.

When the iOS profile is successfully pushed to users' devices, users can sign in to Workspace ONE using the Mobile SSO for iOS authentication method without entering their credentials.

**What to do next**

Create another profile to configure any other desired features, for example, Web Clips to create icons for Web Apps that you push from AirWatch to iOS device home pages or the app catalog.

**Using AirWatch Certificate Authority for Kerberos Authentication**

You can use the AirWatch Certificate Authority instead of the Active Directory Certificate Authority to set up single sign-on with built-in Kerberos authentication to AirWatch managed iOS 9 mobile devices. You can enable AirWatch Certificate Authority in the AirWatch admin console and export the CA issuer certificate for use in the VMware Identity Manager service.

The AirWatch Certificate Authority is designed to follow Simple Certificate Enrollment Protocol (SCEP) and is used with AirWatch managed devices that support SCEP. VMware Identity Manager integration with AirWatch uses the AirWatch Certificate Authority to issue certificates to iOS 9 mobile devices as part of the profile.

The AirWatch Certificate Authority issuer root certificate is also the OCSP signing certificate.

**Enable and Export the AirWatch Certificate Authority**

When VMware Identity Manager is enabled in AirWatch, you can generate the AirWatch issuer root certificate and export the certificate for use with the Mobile SSO for iOS authentication on managed iOS 9 mobile devices.

**Procedure**

1. In the AirWatch admin console, navigate to **System > Enterprise Integration > VMware Identity Manager**.
2. To enable AirWatch Certificate Authority, the organization group type must be Customer.
   
   **Tip** To view or change the group type, navigate to Groups & Settings, **Groups > Organization Groups > Organization Group Details**.
3. In the CERTIFICATE section, click **Enable**.
   The page displays the issuer root certificate details.
4. Click **Export** and save the file.
What to do next

In the VMware Identity Manager console, select the KDC service option to use. See “Configuring Mobile SSO for iOS Authentication in the Built-in Identity Provider,” on page 76.

In the VMware Identity Manager admin console, configure Kerberos Authentication in the built-in identity provider and add the certificate authority issuer certificate.

Configure Apple iOS Profile in AirWatch Using AirWatch Certificate Authority

Create and deploy the Apple iOS device profile in AirWatch to push the Identity Provider settings to the device. This profile contains the information necessary for the device to connect to the VMware Identity Provider and the certificate that the device uses to authenticate.

Prerequisites

- Built-in Kerberos configured in Identity Manager.
- VMware Identity Manager KDC server root certificate file saved to a computer that can be accessed from the AirWatch admin console.
- Certificate enabled and downloaded from the AirWatch admin console System > Enterprise Integration > VMware Identity Manager page.
- List of URLs and application bundle IDs that use Built-in Kerberos authentication on iOS devices.

Procedure

1. In the AirWatch admin console, navigate to Devices > Profiles & Resources > Profile > Add Profile and select Apple IOS.
2. Configure the profile’s General settings and enter the name of the device as iOSKerberos.
3. In the left navigation pane, select SCEP > Configure to configure the credential.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Source</td>
<td>Select AirWatch Certificate Authority from the drop-down menu.</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>Select the AirWatch Certificate Authority from the drop-down menu.</td>
</tr>
<tr>
<td>Certificate Template</td>
<td>Select Single Sign On to set the type of certificate that is issued by the</td>
</tr>
<tr>
<td></td>
<td>AirWatch Certificate Authority.</td>
</tr>
</tbody>
</table>

4. Click Credentials > Configure and create a second credential.
5. In the Credential Source drop-down menu, select Upload.
6. Enter the iOS Kerberos credential name.
7. Click Upload to upload the VMware Identity Manager KDC server root certificate that is downloaded from the Identity & Access Management > Manage > Identity Providers > Built-in Identity provider page.
8. In the left navigation pane, select Single Sign-On.
9. Enter the Connection information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Enter Kerberos.</td>
</tr>
<tr>
<td>Kerberos Principal Name</td>
<td>Click + and select [EnrollmentUser].</td>
</tr>
<tr>
<td>Realm</td>
<td>Enter the realm name you used when you initialized KDC in the VMware</td>
</tr>
<tr>
<td></td>
<td>Identity Manager appliance. For example, EXAMPLE.COM.</td>
</tr>
</tbody>
</table>
### Implementing Mobile Single Sign-On Authentication for AirWatch-Managed Android Devices

Mobile SSO for Android is an implementation of the certificate authentication method for AirWatch-managed Android devices.

The AirWatch Tunnel mobile application is installed on the Android device. The AirWatch Tunnel client is configured to access the VMware Identity Manager service for authentication. The tunnel client uses the client certificate to establish a mutually authenticated SSL session and the VMware Identity Manager service retrieves the client certificate for authentication.

**Note** Mobile SSO authentication for Android is supported for Android devices 4.4 and later.

### Mobile Single Sign-on without VPN Access

Mobile Single Sign-on authentication for Android devices can be configured to bypass the Tunnel server when VPN access is not required. Implementing Mobile SSO for Android authentication without using a VPN uses the same configuration pages as used for configuring the AirWatch Tunnel. Because you are not installing the Tunnel server, you do not enter the AirWatch Tunnel server host name and port. You still set up a profile using the AirWatch Tunnel profile form, but traffic is not directed to the Tunnel server. The Tunnel client is used only for single sign-on.

In the AirWatch admin console you configure the following settings.

- **Per App Tunnel component in the AirWatch Tunnel.** This configuration allows Android devices access to internal and managed public apps through the AirWatch Tunnel mobile app client.
- **Per App Tunnel Profile.** This profile is used to enable the per app tunneling capabilities for Android.
- **In the Network Traffic Rules page, because the Tunnel server is not configured, you select Bypass so that no traffic is directed towards a Tunnel server.”

---

**Option**  | **Description**  
--- | ---  
Renewal Certificate | On iOS 8 and later devices, select the certificate used to reauthenticate the user automatically without any need for user interaction when the user’s single sign-on session expires.  
URL Prefixes | Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. Enter the VMware Identity Manager server URL as `https://myco.example.com`.  
Applications | Enter the list of application identities that are allowed to use this sign-in. To perform single sign-on using iOS built-in Safari browser, enter the first application bundle ID as `com.apple.mobilesafari`. Continue to enter application bundle IDs. The applications listed must support SAML authentication.  

10 Click **Save & Publish**.

When the iOS profile is successfully pushed to users’ devices, users can sign in to VMware Identity Manager using the Built-in Kerberos authentication method without entering their credentials.

**What to do next**

Create another profile to configure any other desired features for iOS Kerberos, for example Web Clips to create icons for Web Apps that you push from AirWatch to iOS device home pages or the app catalog.
Mobile Single Sign-on with VPN Access

When the application configured for single sign-on also is used to access intranet resources behind the firewall, configure VPN access and set up the Tunnel server. When single sign-on is configured with VPN, the Tunnel client can optionally route application traffic and login requests through the Tunnel server. Instead of the default configuration used for the Tunnel client in the console in the single sign-on mode, the configuration should point to the Tunnel server.

Implementing Mobile SSO for Android authentication for AirWatch managed Android devices requires configuring the AirWatch Tunnel in the AirWatch admin console and installing the AirWatch Tunnel server before you configure Mobile SSO for Android in the VMware Identity Manager administration console. The AirWatch Tunnel service provides per app VPN access to AirWatch managed apps. AirWatch Tunnel also provides the ability to proxy traffic from a mobile application to VMware Identity Manager for single sign-on.

In the AirWatch admin console you configure the following settings.

- Per App Tunnel component in the AirWatch Tunnel. This configuration allows Android devices access to internal and managed public applications through the AirWatch Tunnel mobile app client.

  After the AirWatch Tunnel settings are configured in the admin console, you download the AirWatch Tunnel installer and proceed with the installation of the AirWatch Tunnel server.

- Android VPN profile. This profile is used to enable the per app tunneling capabilities for Android.

- Enable VPN for each app that uses the application tunnel functionality from the admin console.

- Create device traffic rules with a list of all the applications that are configured for per app VPN, the proxy server details, and the VMware Identity Manager URL.

For detailed information about installing and configuring the AirWatch Tunnel, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

Configure Single-Sign-on for Android Device from AirWatch Admin Console

Configure single sign-on for Android devices to allow users to sign in securely to enterprise apps, without entering their password.

To configure single-sign-on for Android devices, you do not need to configure the VMware Tunnel, but you configure single sign-on using many of the same fields

Prerequisites

- Android 4.4 or later

- Applications must support SAML or another supported federation standard

Procedure

1. In the AirWatch admin console, navigate to System > Enterprise Integration > VMware Tunnel.

2. The first time you configure VMware Tunnel, select Configure and follow the configuration wizard. Otherwise, select Override and select the Enable VMware Tunnel check box. Then click Configure.

3. In the Configuration Type page, enable Per-App Tunnel (Linux Only). Click Next.

   Leave Basic as the deployment model.

4. In the Details page, enter a dummy value in the text box, as this field is not required for the single sign-on configuration. Click Next.
5 In the SSL page, configure the Per-App Tunneling SSL Certificate. To use a public SSL, select the Use Public SSL Certificate check box. Click Next.

The Tunnel Device Root Certificate is automatically generated.

**NOTE** SAN certificates are not supported. Make sure that your cert is issued for the corresponding server host name or is a valid wildcard certificate for the corresponding domain.

6 In the Authentication page, select the certificate authentication type to use. Click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Select Default to use the AirWatch issued certificates.</td>
</tr>
<tr>
<td>Enterprise CA</td>
<td>A drop-down menu listing the certificate authority and certificate template that you configured in AirWatch is displayed. You can also upload the root certificate of your CA.</td>
</tr>
</tbody>
</table>

If you select Enterprise CA, make sure that the CA template contains the subject name **CN=UDID**. You can download the CA certificates from the VMware Tunnel configuration page.

7 Click Next.

8 In the Profile Association page, associate an existing or create a new VMware Tunnel VPN profile for Android.

   If you create the profile in this step, you still must publish the profile. See Configure Android Profile in AirWatch.

9 Review the summary of your configuration and click **Save**.

   You are directed to the system settings configuration page.

**Configure AirWatch Tunnel VPN Access Settings from AirWatch Admin Console**

You enable the Per App Tunnel component in the AirWatch Tunnel settings to set up per app tunneling functionality for Android devices. Per app tunneling allows your internal and managed public applications to access your corporate resources on an app-by-app basis.

The VPN can automatically connect when a specified app is launched. For detailed AirWatch Tunnel configuration instructions, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

**Procedure**

1 In the AirWatch admin console, navigate to **System > Enterprise Integration > AirWatch Tunnel**.

2 The first time you configure AirWatch Tunnel, select **Configure** and follow the configuration wizard. Otherwise, select **Override** and select the **Enable AirWatch Tunnel** check box. Then click **Configure**.

3 In the Configuration Type page, enable **Per-App Tunnel (Linux Only)**. Click **Next**.

   Leave **Basic** as the deployment model.

4 In the Details page, for the Per-App Tunneling Configuration enter the AirWatch Tunnel server host name and port. For example, enter as tunnel.example.com. Click **Next**.

5 In the SSL page, configure the Per-App Tunneling SSL Certificate. To use a public SSL, select the Use Public SSL Certificate check box. Click **Next**.

   The Tunnel Device Root Certificate is automatically generated.

**NOTE** SAN certificates are not supported. Make sure that your cert is issued for the corresponding server host name or is a valid wildcard certificate for the corresponding domain.
In the Authentication page, select the certificate authentication type to use. Click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Select Default to use the AirWatch issued certificates.</td>
</tr>
<tr>
<td>Enterprise CA</td>
<td>A drop-down menu listing the certificate authority and certificate template that you configured in AirWatch is displayed. You can also upload the root certificate of your CA.</td>
</tr>
</tbody>
</table>

If you select Enterprise CA, make sure that the CA template contains the subject name CN=UDID. You can download the CA certificates from the AirWatch Tunnel configuration page.

If device compliance check is configured for Android, make sure that the CA template contains the subject name CN=UDID or set a SAN type to include the UDID. Select the San type DNS. The value must be UDID={DeviceUid}.

Click Next.

In the Profile Association page, associate an existing or create a new AirWatch Tunnel VPN profile for Android.

If you create the profile in this step, you still must publish the profile. See Configure Android Profile in AirWatch.

(Optional) In the Miscellaneous page, enable the access logs for the Per-App Tunnel components. Click Next.

You must enable these logs before you install the AirWatch Tunnel server.

Review the summary of your configuration and click Save.

You are directed to the system settings configuration page.

Select the General tab and download the Tunnel virtual appliance.

You can use VMware Access Point to deploy the Tunnel server.

What to do next

Install the AirWatch Tunnel server. For instructions, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

Configure Per App Tunnel Profile for Android

After you configured and installed the AirWatch Tunnel Per App Tunnel component, you can configure the Android VPN profile and add a version to the profile.

Procedure

1. In the AirWatch admin console, navigate to Devices > Profiles > Add Profile and select Android or Android for Work.
2. Configure the General settings for Android if they are not already set up.
3. In the left column, select VPN and click Configure.
4. Complete the VPN Connection information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Select AirWatch Tunnel.</td>
</tr>
<tr>
<td>Connection Name</td>
<td>Enter a name for this connect. For example, AndroidSSO Configuration.</td>
</tr>
<tr>
<td>Server</td>
<td>The AirWatch Tunnel server URL is automatically entered.</td>
</tr>
<tr>
<td>Per-App VPN Rules</td>
<td>Select the Per-App VPN Rules check box.</td>
</tr>
</tbody>
</table>
5 Click Add Version.
6 Click Save & Publish.

What to do next
Enable per-app VPN for the Android apps that can be accessed using Mobile SSO for Android. See “Enable Per-App VPN for Android Apps,” on page 145.

Enable Per-App VPN for Android Apps
The Per-App VPN Profile setting is enabled for Android apps that are accessed with VMware Identity Manager Mobile SSO for Android.

Prerequisites
- AirWatch Tunnel configured with the Per-App Tunnel component installed.
- Android VPN profile created.

Procedure
1 In the AirWatch admin console, navigate to Apps & Books > Applications > List View.
2 Select the Internal tab.
3 Select Add Application and add an app.
4 Click Save & Assign.
5 In the Assignment page, select Add Assignment and in the Advanced section Per-App VPN Profile drop-down menu select the Android VPN profile you created.
6 Click Save & Publish.

Enable Per-App VPN for every Android app that is accessed with Mobile SSO for Android. For more information about adding or editing apps, see the VMware AirWatch Mobile Application Management Guide, on the AirWatch Resources Web site.

What to do next

Configure Traffic Rules in AirWatch
Configure the network traffic rules so that the AirWatch Tunnel client routes traffic to the HTTPS proxy for Android devices. You list the Android apps that are configured with the per app VPN option to the traffic rules, and configure the proxy server address and the destination host name.

Configure the device traffic rules to control how devices handle traffic from specified applications. Device traffic rules force the AirWatch Tunnel app to send traffic through the tunnel, block all traffic to specified domains, bypass the internal network straight to the Internet, or send traffic to an HTTPS proxy site.

For detailed information about creating network traffic rules, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

Prerequisites
- The AirWatch Tunnel option configured with the per-app tunnel component installed.
- Android VPN profile created.
- Per-App VPN enabled for each Android App that is added to the Network Traffic rules.
Procedure

1. In the AirWatch admin console, navigate to System > Enterprise Integration > AirWatch Tunnel > Network Traffic Rules.

2. In the Device Traffic Rules tab, configure the device traffic rules settings as described in the AirWatch Tunnel Guide. Specific to the Mobile SSO for Android configuration, configure the following settings.
   a. Select the default action.
      
      | Option | Description |
      |--------|-------------|
      | Tunnel | For the VPN configuration with single-sign on to Android, select Tunnel as the default action. All apps on the device configured for Per App VPN send the network traffic through the tunnel. |
      | Bypass | For single sign-on to Android, select Bypass as the default action. **Important** With Bypass as the default action, all apps configured for Per App VPN on the device bypass the tunnel and connect to the Internet directly. With this implementation, no traffic is sent to the Tunnel server when the Tunnel client is used only for single sign-on. For single sign-on to Android with using VPN, select Bypass as the default action. **Important** With Bypass as the default action, all apps configured for Per App VPN on the device bypass the tunnel and connect to the Internet directly. With this implementation, no traffic is sent to the Tunnel server when the Tunnel client is used only for single sign-on. |

   b. In the Application column, add the Android apps that are configured with the per app VPN profile.
   c. In the Action column, select Proxy and specify the HTTPS proxy information. Enter the VMware Identity Manager host name and port. For example `login.example.com:5262`.
      
      **Note** If you are providing external access to the VMware Identity Manager host, the firewall port 5262 must be opened or port 5262 traffic must be proxied through reverse proxy in the DMZ.
   d. In the Destination Hostname column, enter your destination VMware Identity Manager host name. For example `myco.example.com`. The AirWatch Tunnel client routes the traffic to the HTTPS proxy from the VMware Identity Manager host name.

3. Click Save.
What to do next

Publish these rules. After the rules are published, the device receives an update VPN profile and the AirWatch Tunnel application is configured to enable SSO.

Go the VMware Identity Manager administration console and configure Mobile SSO for Android in the Built-in Identity Provider page. See the VMware Identity Manager Administration Guide.

Enabling Compliance Checking for AirWatch Managed Devices

When users enroll their devices through the AirWatch Agent application, 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’ 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.

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 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.

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.

Registering Email Domains for Auto Discovery

You can register your email domain in the auto discovery service in to make it easier for end users to access their apps portal through the Workspace ONE application. End users enter their email address instead of the organization's URL.

When the email domain of the organization is registered for auto discovery, end users enter only their email address in the sign-in page to access their apps portal. For example, they enter username@myco.com.

When auto discovery is not used, the first time that end users open the Workspace One application, they must provide the complete organization URL. For example, they enter myco.vmwareidentity.com.

Set up Auto Discovery in VMware Identity Manager

To register a domain, you enter your email domain and email address in the identity manager admin console Auto Discovery page.

An email message with an activation-token is sent to your email address on the domain. To activate the domain registration, you enter the token in the Auto Discovery page and verify that the domain you registered is your domain.

**Note** To set up auto discovery for VMware Identity Manager on-premises deployments, you must log in to the admin console as the local admin. You enter the AirWatch ID and password that you created in the AirWatch Web site, https://secure.air-watch.com/register.

Procedure

1 In the administration console, Identity & Access Management tab, click Setup > Auto Discovery.
Configure the AirWatch auto discovery URL.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Discovery URL</td>
<td>Enter the URL as <a href="https://discovery.awmdm.com">https://discovery.awmdm.com</a>.</td>
</tr>
<tr>
<td>AirWatch ID</td>
<td>Enter the email address you registered with AirWatch to log in to their Web site.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the AirWatch account.</td>
</tr>
</tbody>
</table>

3. In the **Email Domain** text box, enter your organizations email domain to register.

4. In the **Confirmation Email Address** text box, enter an email address on that email domain to receive the verification token.

5. Click **OK**.
   - The status of this email domain registration is marked Pending. You can have only one pending email domain at a time.

6. Navigate to the email and copy the activation token that is in the message.

7. Return to the **Identity & Access Management > Auto Discovery** page and paste the token in the Activation Token text box

8. Click **Verify** to register the domain.

The email domain is registered and is added to the list of registered email domains on the Auto Discovery page.

End users can now enter their email address in the Workspace ONE application to access their app portal.

**What to do next**

If you have more than one email domain, add another email domain to register.
Index

A
access events 119
access policies
  Auth Strength 85
  Client Type 85
  minimum authentication score 87, 89
  network 87, 89
  Network 85
  relationship to identity providers 87, 90, 91
  TTL 85, 87, 89
  Web-application-specific 89–91
access denied message, configure 85
access policy set, default 90
access policy sets
  creating 90
  default 85, 87, 91
  portal 87, 90
  Web-application-specific 89–91
Active Directory
  attribute mapping 20
  deployment 83
  Integrated Windows Authentication 13
  integrating 15
  Active Directory Certificate Authority 135
  Active Directory Global Catalog 15
  Active Directory over LDAP 13, 21
  add groups 97
  Add Identity Provider button 83
  add Web app 107
  add Active Directory 21
  add local user 101
  add local users 100
  admin tab descriptions 9
  admin, authentication 42
  administration console 9
  AirWatch
    admin account 127
    certificate 127
    configure iOS profile 138, 140
    device compliance check 92, 147
    enable unified catalog 131
  AirWatch Cloud Connector, configure 73
  AirWatch API key 126
  AirWatch Certificate Authority, OCSP 139
  AirWatch certificate authority, enable 139
  AirWatch Cloud Connector Authentication 132
  AirWatch Cloud Password Authentication 81
  AirWatch directory, user attributes 132
  AirWatch Tunnel, configure 143
  AirWatch upgrade, update service 134
  AirWatch, configure 125
  AirWatch, integrating with Identity Manager 125
  AirWatch, network traffic rules 145
  AirWatch, setting up in VMware Identity Manager 129
  Android authentication, network traffic rules 145
  Android, single sign-in 142
  android, per-app VPN 145
  API key 125, 126
  app popularity 117
  Apple iOS profile in AirWatch 140
  appliance status 118
  application, categories 110
  applications
    mobile 106
    Web 106
  approvals 115
  attributes
    default 20
    mapping 20
  Audit Event report 119
  authentication
    AirWatch Cloud Connector 73
    per-app VPN for Android apps 145
    RADIUS 62
  authentication chaining 87
  authentication method 83
  authentication methods
    adding to policy 85
    relationship to access policies 87, 90, 91
    RSA Adaptive Authentication 65
  authentication error message 91
  authentication in built-in IdP 72
  authentication method order 85
  authentication method, Android, mobile SSO 78
  authentication, mobile SSO for Android 141
  authentication, AirWatch Password 81
  authentication, Android profile 144
  authentication; AirWatch Cloud Connector 132
  auto discovery 148
AWCA 139

B
branding, VMware Verify 123
browsers, supported 9
browsers for kerberos 58
built-in identity provider, enable 80
built-in identity provider, configure 81
built-in identity provider, configure 80

C
catalog
  add web app 107
  managing 105
catalog settings, Citrix Published Applications 114
catalog, View 108
catalog, Citrix Published Applications 108
categories
  applying 109
  creating 109
  deleting 110
  removing 110
certificate authentication, Android 78
certificate signing request, generate for SAML 111
certificate authority for AirWatch, Kerberos authentication 135
certificate authority, smart card 67
certificate template for AirWatch, Kerberos 136
certificate, SAML 110
challenge questions 65
change Active Directory password 26
change AD password 26
Chrome 60
Citrix-published applications, enable 108
compliance check with AirWatch 92, 147
compliance check in AirWatch 73, 92, 147
compliance checking, enable 74
Configure AirWatch 125
configure iOS device profile 138
configure AirWatch integration 129
configure built-in identity provider 77
configure Mobile SSO for Android 78
configure RSA Adaptive Authentication 65
custom branding, setup 10
custom attribute names, do not use 20
custom error message 91
customize branding 121
customize portal page 122

dashboard 117
database, monitor 118
delete local user 102
device usage report 118
directories, add 10
directory
  add 13
  adding 21
  sync safeguards 27
  synchronization safeguards 27
directory integration 13
directory server groups 95
directory, AirWatch 133
disable
  Citrix Receiver download 112
  Horizon Client download 112
disable account 20
disable an account 20
disable local users 102
DNS service location lookup 17–19
domain 21
domain_krb.properties file 17–19

e-mail domain
  register 148
  register for auto discovery 148
enable compliance check 73, 74, 92, 147
enable AirWatch Certificate Authority 139
enable license approval 115
enable persistent cookie 94
enable terms of use 52
enable unified catalog 129
end user, Workspace ONE 9
entitlements, user 97
export AirWatch Certificate Authority 139

F
Firefox 59

G
global settings, disable helper application 112
group
  add users 97
  entitle resources 97, 100
  group affiliations, user 97
Group Membership report 118
group names 96, 97
Index

VMware, Inc.  153
O
one touch notification 70
organization groups 129
other directory 133
out-of-band authentication 65
outbound connector 80
overview, Identity and Access Management Settings 10

P
password 102
password authentication, local users 74
password history, setting 103
password policy 103
password (local directory), admin 42
password reminder notification 103
passwords, expired 26
per app tunnel profile for Android 144
persistent cookie, enable 94
policy, editing 91
policy rules, authentication chaining 87
policy rule, compliance check 92, 147
portal page, customize 122
preferences, persistent cookie 94
proof-of-concept 83

R
RADIUS authentication 62
RADIUS configuration 63
RADIUS server 63
re-authenticate session time, configure 85
register, email domain 148
register users in VMware Verify 71
Remote App Access, client 113
report
device usage 118
resource activity 118
roles 118
reports 118
reset Active Directory password 26
reset VMware Verify 71
resource, license approval 115
resource activity report 118
Resource Entitlement report 118
Resource Usage report 118
resources
categories 109, 110
entitle 100
entitle to groups 97
percentage of types being used 117
REST API 115
REST API key 126
revocation checking, smart card 68
role assignment report 118
roles, user 97
RSA Adaptive Authentication, enroll users 65
RSA Adaptive Authentication, configure 65
RSA SecurID server 61
rules 91
runtime-config.properties file 18

S
safeguard 10
safeguard settings, ignore 27
safeguards, directory synchronization 27
safeguards, threshold 27
SAML
certificate 111
metadata 111
third-party identity providers 82
SAML assertions, Just-in-Time 46
SAML certificate 110
SecurID, configure 61
settings, catalog 110
sign in page, customize 121
single forest active directory 15
single logout, identity provider 83
siteaware.subnet property 18
smart card authentication 67
smart card certificate authority 67
smart card certificate revocation 68
smart card, configure 68, 75
SMS 70
SRV lookup 17–19
sync domain, user 97
sync safeguards, ignore 27
sync settings 20
System Directory 35
System Domain 35
system information 118
system diagnostics dashboard 118
System Identity Provider 35

T
tablet view, customize 122
terms of use 52
terms of use, set up 52
third-party identity provider 83
TOTP 70
troubleshooting domain_krb.properties 19
tunnel, AirWatch 142
two-factor authentication 70

U
unified catalog, enable for AirWatch 131
upgrade AirWatch Cloud Connector  134
UPN  67
user, entitlements  97
user attributes, setup  10
user portal, customize  121
user profile  97
User Attributes page  20
user attributes for local directories  37
user attributes, AirWatch directory  132
user names  96, 97
user store  83
userName  96
users
  Active Directory  95
  user attributes  20
users logged in, number of  117
Users report  118

V
version  118
View, enable  108
viewing user information  97
VMware Verify, branding  123
VMware Verify, enable  70
VMware Verify reset  97
  security token  70
VMware Verify, register users  71
VMware Verify, two-factor authentication  70
VMware Verify, unregister from  71

W
Web applications  105, 106
worker  13
Workspace IDP  82
workspace images  105
Workspace ONE, terms of use  52