Directory Integration with VMware Identity Manager

JUN 2019
VMware Identity Manager
VMware Identity Manager 19.03
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Integration with VMware Identity Manager</td>
<td>4</td>
</tr>
<tr>
<td>1  Integrating Your Enterprise Directory with VMware Identity Manager</td>
<td>5</td>
</tr>
<tr>
<td>2  Important Concepts Related to Directory Integration</td>
<td>6</td>
</tr>
<tr>
<td>3  Integrating with Active Directory</td>
<td>8</td>
</tr>
<tr>
<td>Active Directory Environments</td>
<td>8</td>
</tr>
<tr>
<td>Managing User Attributes that Sync from Active Directory</td>
<td>11</td>
</tr>
<tr>
<td>Select Attributes to Sync with Directory</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Active Directory Connection to the Service</td>
<td>12</td>
</tr>
<tr>
<td>Directory Sync Scheduling</td>
<td>19</td>
</tr>
<tr>
<td>Setting up Directory Sync Safeguards</td>
<td>20</td>
</tr>
<tr>
<td>Configure Directory Sync Safeguards</td>
<td>20</td>
</tr>
<tr>
<td>Ignore Safeguard Settings to Complete Syncing to the Directory</td>
<td>21</td>
</tr>
<tr>
<td>Enabling Users to Change Active Directory Passwords</td>
<td>21</td>
</tr>
<tr>
<td>4  Integrating with LDAP Directories</td>
<td>23</td>
</tr>
<tr>
<td>Limitations of LDAP Directory Integration</td>
<td>23</td>
</tr>
<tr>
<td>Integrating an LDAP Directory with the Service</td>
<td>24</td>
</tr>
<tr>
<td>5  Configuring High Availability for Directory Sync (On Premises VMware Identity Manager Only)</td>
<td>29</td>
</tr>
</tbody>
</table>
Directory Integration with VMware Identity Manager

Directory Integration with VMware Identity Manager provides information about integrating your enterprise directory with VMware Identity Manager™ to sync users and groups to the VMware Identity Manager service.

Intended Audience

This information is intended for experienced Windows or Linux system administrators who are familiar with Active Directory and other directory services.
Integrating Your Enterprise Directory with VMware Identity Manager

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 is a component of the VMware Identity Manager service that you deploy on premises inside your enterprise network.

- 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

Create the LDAP directory to integrate your enterprise LDAP directory with VMware Identity Manager. You can only integrate a single-domain LDAP directory. VMware Identity Manager supports only those OpenLDAP implementations that support paged search queries.

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 Chapter 2 Important Concepts Related to Directory Integration.

This chapter includes the following topics:

- Active Directory Environments
- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service
- Directory Sync Scheduling
- Setting up Directory Sync Safeguards
- Enabling Users to Change Active Directory Passwords

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

With a single Active Directory deployment, you can sync users and groups from a single Active Directory domain.

For this environment, when you add a directory to the VMware Identity Manager service, select Active Directory over LDAP/IWA as the directory to add.

For more information, see:

- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service
Multi-Domain, Single Forest Active Directory Environment

In a multi-domain, single forest Active Directory deployment, you can 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. Make sure that a direct (non-transitive) two-way trust is set up between domains in the directory and the domain that the VMware Identity Manager Connector is joined to.

  For more information, see:
  - Managing User Attributes that Sync from Active Directory
  - Configuring Active Directory Connection to the Service

- 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 Workspace ONE UEM is integrated with VMware Identity Manager and multiple Workspace ONE UEM 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

In a multi-forest Active Directory deployment with trust relationships, you can sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains. You can configure the service for this Active Directory environment as 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. Make sure that a direct (non-transitive) two-way trust is set up between domains in the directory forests and the domain that the VMware Identity Manager Connector is joined to.

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

For more information, see:

- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service

### Multi-Forest Active Directory Environment Without Trust Relationships

In a multi-forest Active Directory deployment without trust relationships, you can 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 VMware Identity Manager 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.

For more information, see:

- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service
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 VMware Identity Manager 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 3-1. Default Active Directory Attributes to Sync to Directory

<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>employeeId</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>

The following attributes cannot be used as custom attribute names because VMware Identity Manager service uses these attributes internally for user identity management.

- externalUserDisabled
- employeeNumber

### 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 VMware Identity Manager 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**.

**Configuring Active Directory Connection to the Service**

In the VMware Identity Manager console, enter 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 over Integrated Windows Authentication. Active Directory over LDAP connection supports DNS Service Location lookup.

**Prerequisites**

- Install and activate a VMware Identity Manager connector instance. See Installing and Configuring VMware Identity Manager Connector (Windows).

- Select which attributes are required and add additional attributes on the User Attributes page in the VMware Identity Manager console. See Select Attributes to Sync with Directory.

- Make a list of the Active Directory users and groups to sync from Active Directory. Group names are synced to the directory immediately. Members of a group do not sync until the group is entitled to resources or added to a policy rule. Users who need to authenticate before group entitlements are configured should be added during the initial configuration.

- For Active Directory over LDAP, you need the Base DN, and the Bind user DN and password.

  The Bind user must have the following permissions in Active Directory to grant access to users and groups objects:

  - Read
  - Read All Properties
  - Read Permissions

  **Note** Using a Bind user account with a non-expiring password is recommended.
For Active Directory over Integrated Windows Authentication, you need the user name and password of the Bind user who has permission to query users and groups for the required domains.

The Bind user must have the following permissions in Active Directory to grant access to users and groups objects:

- Read
- Read All Properties
- Read Permissions

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

If your Active Directory requires access over SSL/TLS, the Intermediate (if used) and Root CA certificates of the domain controllers for all relevant Active Directory domains are required. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, all the Intermediate and Root CA certificates are required.

For Active Directory over 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.

For Active Directory over Integrated Windows Authentication:

- For all domain controllers listed in SRV records and hidden RODCs, nslookup of hostname and IP address should work.
- All the domain controllers must be reachable in terms of network connectivity.

**Procedure**

1. In the VMware Identity Manager 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>
<tbody>
<tr>
<td>Active Directory over LDAP</td>
<td>a In the Sync Connector text box, select the connector to use to sync with Active Directory.</td>
</tr>
<tr>
<td></td>
<td>b In the Authentication text box, 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 &amp; Access Management &gt; Manage &gt; Identity Providers page to add the third-party identity provider for authentication.</td>
</tr>
<tr>
<td></td>
<td>c In the Directory Search Attribute text box, select the account attribute that contains username.</td>
</tr>
<tr>
<td></td>
<td>d If you want to use DNS Service Location lookup for Active Directory, make the following selections.</td>
</tr>
<tr>
<td></td>
<td>▪ In the Server Location section, select the This Directory supports DNS Service Location check box. VMware Identity Manager finds and uses optimal domain controllers. If you don't want to use optimized domain controller selection, follow step e. instead.</td>
</tr>
</tbody>
</table>
|                             |   ▪ If your Active Directory requires access over SSL/TLS, select the This Directory requires all connections to use STARTTLS check box in the Certificates section and copy and paste the domain controllers' Intermediate (if used) and Root CA certificates into the SSL Certificate text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after another. For example:  

```plaintext
-----BEGIN CERTIFICATE-----  
...                         
<Intermediate Certificate 1> 
...                         
-----END CERTIFICATE------  
-----BEGIN CERTIFICATE-----  
...                         
<Root Certificate 1>        
...                         
-----END CERTIFICATE------  
-----BEGIN CERTIFICATE-----  
...                         
<Intermediate Certificate 2> 
...                         
-----END CERTIFICATE------  
-----BEGIN CERTIFICATE-----  
```
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>If you do not want to use DNS Service Location lookup for Active Directory, make the following selections.</td>
</tr>
<tr>
<td>e.</td>
<td>In the Server Location section, verify that the This Directory supports DNS Service Location check box is not selected and enter the Active Directory server host name and port number.</td>
</tr>
<tr>
<td></td>
<td>To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in Active Directory Environments.</td>
</tr>
<tr>
<td>e.</td>
<td>If your Active Directory requires access over SSL/TLS, select the This Directory requires all connections to use SSL check box in the Certificates section and copy and paste the domain controller’s Intermediate (if used) and Root CA certificate into the SSL Certificate field.</td>
</tr>
<tr>
<td></td>
<td>Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that the certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines.</td>
</tr>
<tr>
<td></td>
<td>If your Active Directory requires access over SSL/TLS and you do not provide the certificate, you cannot create the directory.</td>
</tr>
<tr>
<td>f</td>
<td>In the Base DN field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com.</td>
</tr>
<tr>
<td>f.</td>
<td>The Base DN will be used for authentication. Only users under the Base DN will be able to authenticate. Make sure that the group DNs and user DNs that you specify later for sync fall under this Base DN.</td>
</tr>
<tr>
<td>g</td>
<td>In the Bind User DN field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com.</td>
</tr>
<tr>
<td>g.</td>
<td>Using a Bind user account with a non-expiring password is recommended.</td>
</tr>
<tr>
<td>h</td>
<td>After you enter the Bind password, click Test Connection to verify that the directory can connect to your Active Directory.</td>
</tr>
<tr>
<td>a</td>
<td>In the Sync Connector text box, select the connector to use to sync with Active Directory.</td>
</tr>
<tr>
<td>b</td>
<td>In the Authentication text box, if this Active Directory is used to authenticate users, click Yes.</td>
</tr>
<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 text box, select the account attribute that contains username.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>d</td>
<td>If your Active Directory requires access over SSL/TLS, select the <strong>This Directory requires all connections to use STARTTLS</strong> check box in the <strong>Certificates</strong> section and copy and paste the domain controllers’ Intermediate (if used) and Root CA certificates into the <strong>SSL Certificate</strong> text box. Enter the Intermediate CA certificate first, then the Root CA certificate. Ensure that each certificate is in the PEM format and includes the BEGIN CERTIFICATE and END CERTIFICATE lines. If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after another. For example:</td>
</tr>
</tbody>
</table>

```
-----BEGIN CERTIFICATE-----
...<Intermediate Certificate 1>
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...<Root Certificate 1>
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...<Intermediate Certificate 2>
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...<Root Certificate 2>
...
-----END CERTIFICATE-----
```

**Note** If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory. |
| e      | In the **Bind User Details** section, enter the user name and password of the bind user who has permission to query users and groups for the required domains. Enter the user name as sAMAccountName@domain, where domain is the fully-qualified domain name. For example, jdoe@example.com. **Note** Using a Bind user account with a non-expiring password is recommended. |

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 over 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**.

8 Select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

When groups are added here, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule. Any subsequent scheduled syncs bring updated information from Active Directory for these group names.

<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 under them.</td>
</tr>
<tr>
<td></td>
<td>a Click + and specify the group DN. For example, CN=users,DC=example,DC=company,DC=com.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> Specify group DNs that are under the Base DN that you entered in the Base DN text box in the Add Directory page. If a group DN is outside the Base DN, users from that DN will be synced but will not be able to log in.</td>
</tr>
<tr>
<td></td>
<td>b Click <strong>Find Groups</strong>. The Groups to Sync column lists the number of groups found in the DN.</td>
</tr>
<tr>
<td></td>
<td>c To select all the groups in the DN, click <strong>Select All</strong>, otherwise click <strong>Select</strong> and select the specific groups to sync.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.</td>
</tr>
<tr>
<td><strong>Sync nested group members</strong></td>
<td>The <strong>Sync nested group members</strong> 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 when the group is entitled. 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 be members of the parent group that you selected for sync.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>Sync nested group members</strong> 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 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.</td>
</tr>
</tbody>
</table>
9  Click **Next**.

10 Specify the users to sync.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

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

\[\text{CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.}\]

**Important**  Specify user DNs that are under the Base DN that you entered in the **Base DN** text box in the Add Directory page. 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 filters to exclude users based on attribute chosen. You can create multiple exclude filters.

You select the user attribute to filter by and the query filter to apply to the value you define.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains</td>
<td>Excludes all users who match the attribute and value set. For example, <strong>name contains Jane</strong> excludes users named &quot;Jane&quot;.</td>
</tr>
<tr>
<td>Does not contain</td>
<td>Excludes all users except for those who match the attribute and value set. For example, <strong>telephoneNumber does not contain 800</strong>, includes only users with a telephone number that includes &quot;800&quot;.</td>
</tr>
<tr>
<td>Begins with</td>
<td>Exclude all users where the characters begin with &lt;xxx&gt; in the attribute value. For example, <strong>employeeID begins with ACME0</strong>, excludes all users that have an employee ID that includes &quot;ACME0&quot; at the beginning of their ID number.</td>
</tr>
<tr>
<td>Ends with</td>
<td>Exclude all users where characters end with &lt;yyy&gt; in the attribute value. For example, <strong>mail ends with example1.com</strong>, excludes all users that have an email address that ends in &quot;example1.com&quot;.</td>
</tr>
</tbody>
</table>

The value is case-insensitive. The following symbols cannot be in the value string.

- Asterisk `*`
- Caret `^`
- Parentheses `( )`
- Question mark `?`
- Exclamation point `!`
- Dollar sign `$`

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 group names are synced from the Active Directory to the VMware Identity Manager directory. The Bind user has an administrator role in VMware Identity Manager by default.

For more information about how groups are synced, see "Managing Users and Groups" in *VMware Identity Manager Administration*.

**What to do next**

- Set up authentication methods. After users and group names 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 portal, 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.

- (On premises) Apply custom branding to the VMware Identity Manager console, user portal pages and the sign-in screen, if necessary.

### Directory Sync Scheduling

Active Directory users and groups are synced into the VMware Identity Manager service through the VMware Identity Manager Connector.

A schedule can be created to sync users and groups either weekly, daily, every hour or every 15 minutes. You can also select to manually sync users and groups. When you set the schedule to manually, on the Directories page, you can click Sync Now next to a directory to start the sync process.

Schedule the sync intervals to be longer than the time to sync. If users and groups are being synced to the directory when the next sync is scheduled, the new sync starts immediately after the end of the previous sync. With this schedule, the sync process is continuous.

**Procedure**

1. To set the sync frequency settings for users and groups, in the Identity & Access Management tab select **Directories**.

2. Select the directory to set the sync schedule.

3. Click **Sync Settings**.

4. In the Sync Frequency tab, set the sync frequency, the day, and the time of day to run. Set the sync time based on UTC standard time.

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

Review the sync safeguard limits configured in the Safeguards tab. See Setting up Directory Sync Safeguards.

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 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. In the VMware Identity Manager console 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 VMware Identity Manager console 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.
5. To continue the sync without changing the safeguard settings, click Sync Now.
6. On the Review page, select the check box Ignore Safeguards.
7. Click Sync Directory.

The directory sync is run and the safeguard threshold settings are ignored for this sync session only.

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.

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.

**Note**  The Allow Change Password option cannot be enabled for ACC directories.

**Prerequisites**

- The domain functional level of the Active Directory domain controllers must be set to Windows 2008 or later.
- Port 464 must be open from VMware Identity Manager to the domain controllers. In a SaaS deployment, port 464 must be open from the VMware Identity Manager connector to the domain controllers.
- The Active Directory must use one of the following UPN formats:
  - Regular UPN format: samaccountname@domain
  - Alternative UPN prefix format: alternativePrefix@domain
  - Alternative UPN suffix format: samaccountname@alternativeSuffix
  
  The UPN format of alternativePrefix@alternativeSuffix is not supported.
- Clocks on the connector and the domain controllers must be synchronized.
- The **Allow Change Password** option is available with connector version 2016.11.1 and later.

**Procedure**

1. In the VMware Identity Manager 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**.
Integrating with LDAP Directories

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.

For the types of LDAP directories supported, see the VMware Identity Manager Release Notes.

See also Chapter 2 Important Concepts Related to Directory Integration.

This chapter includes the following topics:

- Limitations of LDAP Directory Integration
- Integrating an LDAP Directory with the Service

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.
  
  To integrate multiple domains from an LDAP directory, you create multiple 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 Horizon 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 as Required in the User Attributes page. The UserName attribute is the exception and can be marked as Required. The settings mapped in the User Attributes page apply to all directories in the service. If an attribute is marked as 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.

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 the 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 might be based on default schemas or custom schemas. It may also have 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 or equivalent attribute

Certain limitations apply to the LDAP directory integration feature. See Limitations of LDAP Directory Integration.

Prerequisites

- Review the attributes in the Identity & Access Management > Setup > User Attributes page and add additional attributes that you want to sync. You map the VMware Identity Manager attributes to your LDAP directory attributes when you create the directory. These attributes are 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 VMware Identity Manager 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><strong>Directory Name</strong></td>
<td>A name for the VMware Identity Manager directory.</td>
</tr>
<tr>
<td><strong>Directory Sync and Authentication</strong></td>
<td>In the <strong>Sync Connector</strong> text box, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. You do not need to use 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 <em>Installing and Configuring VMware Identity Manager</em>.</td>
</tr>
<tr>
<td></td>
<td>a</td>
</tr>
<tr>
<td></td>
<td>In the <strong>Authentication</strong> text box, if you want to use this LDAP directory to authenticate users, select <strong>Yes</strong>. If you want to use a third-party identity provider to authenticate users, select <strong>No</strong>. After you add the directory connection to sync users and groups, go to the <strong>Identity &amp; Access Management &gt; Manage &gt; Identity Providers page</strong> to add the third-party identity provider for authentication.</td>
</tr>
<tr>
<td></td>
<td>b</td>
</tr>
<tr>
<td></td>
<td>In the <strong>Directory Search Attribute</strong> text box, select the LDAP directory attribute to use for user name. If the attribute is not listed, select <strong>Custom</strong> and type the custom attribute name to use for users and for groups. For example, <em>cn</em>.</td>
</tr>
<tr>
<td><strong>Server Location</strong></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, <em>myLDAPserver.example.com</em> or <em>100.00.00.0</em>. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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><strong>Filter Queries</strong></td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>The search filter for obtaining group objects.</td>
</tr>
<tr>
<td>For example: ((objectClass=groupOfNames))</td>
<td></td>
</tr>
<tr>
<td>Bind User</td>
<td>The search filter for obtaining the bind user object, that is, the user that can bind to the directory.</td>
</tr>
<tr>
<td>For example: ((objectClass=person))</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>The search filter for obtaining users to sync.</td>
</tr>
<tr>
<td>For example: (&amp;((objectClass=user)(objectCategory=person)))</td>
<td></td>
</tr>
<tr>
<td><strong>Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>Membership</td>
<td>The attribute that is used in your LDAP directory to define the members of a group.</td>
</tr>
<tr>
<td>For example: member</td>
<td></td>
</tr>
<tr>
<td>Object UUID</td>
<td>The attribute that is used in your LDAP directory to define the UUID of a user or group object.</td>
</tr>
<tr>
<td>For example: entryUUID</td>
<td></td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>(Optional) The attribute that is used in your LDAP directory for the distinguished name of a user or group.</td>
</tr>
<tr>
<td>For example: dn</td>
<td>By default, the distinguished name attribute is used to uniquely identify user and group objects. If your LDAP schema does not have the distinguished name attribute, select the Enable advanced LDAP configuration option and enter the values to use to identify groups and users.</td>
</tr>
<tr>
<td>Enable advanced LDAP configuration</td>
<td>Select the check box to view advanced LDAP configuration options. Use the advanced configuration if your LDAP schema does not have the distinguished name attribute or if it uses posixGroups.</td>
</tr>
<tr>
<td>Group Filter</td>
<td>The value to use to query and identify groups. This value is required if your LDAP schema does not have the distinguished name attribute.</td>
</tr>
<tr>
<td>For example: cn</td>
<td></td>
</tr>
<tr>
<td>User Filter</td>
<td>The value to use to query and identify users. This value is required if your LDAP schema does not have the distinguished name attribute.</td>
</tr>
<tr>
<td>For example: uid</td>
<td></td>
</tr>
<tr>
<td>User Membership Mapping Filter</td>
<td>(Optional) This option is typically required for LDAP directories that use posixGroups. The User Membership Mapping Filter is used to query and identify users returned by the Membership attribute.</td>
</tr>
<tr>
<td>For example: uidNumber</td>
<td></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 This Directory requires all connections to use SSL check box and copy and paste the LDAP directory server's root CA SSL certificate into the text box. Ensure the certificate is in PEM format and include the &quot;BEGIN CERTIFICATE&quot; and &quot;END CERTIFICATE&quot; lines.</td>
</tr>
</tbody>
</table>

| Bind User Details      | **Base DN**: Enter the DN from which to start searches. For example, cn=users,dc=example,dc=com  
|                        | **Bind DN**: Enter the user name to use to bind to the LDAP directory.  
|                        | **Note**: Using a Bind DN user account with a non-expiring password is recommended.  
|                        | **Bind User Password**: Enter the password for the Bind DN user. |

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.  
   When groups are added, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule.  
   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 when the group is entitled. 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 users. For example, enter `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

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 group names 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 group names 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.
Configuring High Availability for Directory Sync (On Premises VMware Identity Manager Only)

You can configure high availability for directory sync by associating the directory with multiple connector instances and then setting up a Sync Connectors list for the directory. The connectors in the Sync Connectors list are arranged in failover order. The VMware Identity Manager service uses the first connector in the list to sync users and groups for the directory. If the first connector is unavailable, it uses the next connector in the list, and so on.

Each directory has its own Sync Connectors list.

As a best practice, set up your deployment in a way that the same connector does not sync multiple directories at the same time. You can use the following strategies.

- Use a different set of connectors for different directories.
- If you use the same set of connectors in the same failover order, schedule the sync at different times for each directory.
- If you use the same set of connectors for multiple directories, set a different failover order for each directory so that sync does not fall back to the same connector.

This feature is available beginning with the VMware Identity Manager 19.03 on-premises release. To use this feature, upgrade all connectors to version 19.03.0.0, then follow this procedure to set up the Sync Connectors list. Take into account the following situations.

- For existing directories, the Sync Connectors list is empty. Until you configure the Sync Connectors list, the connector that was originally configured for the directory continues to be used for sync and no fallback is available if the connector fails.
- New directories created in an upgraded or new environment have one connector listed in the Sync Connectors list. This connector is the one you selected as the sync connector while creating the directory.

**Important** This feature is only available in VMware Identity Manager on-premises installations. It is not available in VMware Identity Manager cloud.

**Prerequisites**

- You have installed and configured additional connector instances. See Install and Configure Additional VMware Identity Manager Connector Instances in Installing and Configuring VMware Identity Manager Connector 19.03.0.0 (Windows).
All connectors associated with the VMware Identity Manager service must be version 19.03.0.0 or later. If any connectors are an older version, the Sync Connectors tab does not appear in the directory's Sync Settings page.

**Procedure**

1. Associate the new connector instances with the Workspace IDP of the directory.
   a. In the VMware Identity Manager console, click the **Identity & Access Management** tab.
   b. In the Directories page that appears, click the directory for which you want to configure high availability.
   c. In the **Directory Sync and Authentication** section, click the WorkspaceIDP link.
   d. In the WorkspaceIDP page, scroll to the **Connector(s)** section, select each new connector instance from the drop-down menu, and click **Add Connector**.
   e. Click **Save**.

2. Click the **Directories** tab, then click the directory name.

3. Click **Sync Settings**.

4. Click the **Sync Connectors** tab.
5  Select the connector instances to be used to sync users and groups for this directory.
   a  From the Select a Connector list, which displays all the connectors added to the service, select a connector and click the + icon.
      The connector is added to the Sync Connectors list.
   b  Add all the connectors that you want to use for sync to the Sync Connectors list.
   c  In the Sync Connectors list, arrange the connectors in failover order by using the up and down arrow keys.
      To perform a directory sync, VMware Identity Manager tries to use the first connector in the list. If the first connector is unavailable, it tries to use the second connector, and so on.
      For example:

6  Click Save.
   The list of sync connectors for the directory is saved and is applied from the next sync onwards.
   You can view which connectors were used for sync in the Sync Log tab of the directory page.
   For example: