

(Legacy) Directory Integration with Workspace ONE Access

Legacy Admin Console-Based Documentation (prior to April
2022)

JAN 2022

VMware Workspace ONE Access

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

<https://docs.vmware.com/>

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

Copyright © 2017-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Directory Integration with VMware Workspace ONE Access	5
1 Workspace ONE Access Directory Integration Requirements and Supported Directories	6
2 About Integrating Your Enterprise Directory with Workspace ONE Access	8
3 Managing User Attributes in Workspace ONE Access	10
Select Attributes to Sync with Workspace ONE Access Directory	12
4 Integrating Active Directory with Workspace ONE Access	13
Best Practices to Avoid Network Latency	15
Configuring Active Directory Connection to the Workspace ONE Access Service	16
Allowing Users to Change Active Directory Passwords from Intelligent Hub	26
Syncing Users Migrated Between Domains (Workspace ONE Access Cloud Only)	27
5 Integrating LDAP Directories with Workspace ONE Access	28
Integrating an LDAP Directory with the Workspace ONE Access Service	29
6 Configuring High Availability for Directory Sync in Workspace ONE Access	35
7 Managing Directory Settings in Workspace ONE Access	37
Setting up a Directory Sync Schedule in Workspace ONE Access	37
Syncing a Directory Manually in Workspace ONE Access	38
Viewing Directory Sync Status in Workspace ONE Access	39
Setting up Directory Sync Safeguards in Workspace ONE Access	40
Configure Directory Sync Safeguards in Workspace ONE Access	40
Ignore Safeguard Settings to Complete Syncing to Workspace ONE Access Directory	41
Updating Domains to Sync to Workspace ONE Access Directory	41
Selecting Users and Groups to Sync to Your Workspace ONE Access Directory	42
Specifying Filters for Directory Sync in Workspace ONE Access	45
8 Deleting a Workspace ONE Access Directory	47
9 Converting a Directory of Type Other in Workspace ONE Access	48
Convert Other Directory to Active Directory over LDAP or Active Directory over Integrated Windows Authentication	49
Stop Directory Sync from Workspace ONE UEM to Workspace ONE Access	51

10 Troubleshooting Workspace ONE Access Directory Integration 53

Directory Integration with VMware Workspace ONE Access

You can integrate your enterprise directory with VMware Workspace ONE[®] Access[™] (formerly known as VMware Identity Manager[™]) to sync users and groups to the Workspace ONE Access service. Workspace ONE Access supports integration with Active Directory and with LDAP directories such as OpenLDAP.

When you integrate a directory, a limited number of user and group attributes, specified by the administrator, are synced to the Workspace ONE Access service. User passwords and any attributes other than the ones specified by the administrator are not synced.

The Directory Sync service is required for directory integration. Before using this document, install the Directory Sync service, which is available as a component of the Workspace ONE Access connector beginning with version 20.01. See the latest version of *Installing VMware Workspace ONE Access Connector* for information.

Related Information

Workspace ONE Access also supports other types of directories, such as local directories and Just-in-Time directories. For information about creating those types of directories, see the *Workspace ONE Access Administration* guide.

Workspace ONE Access Directory Integration Requirements and Supported Directories

1

You can integrate Active Directory over LDAP or Active Directory over Integrated Windows Authentication with the Workspace ONE Access service. You can also integrate LDAP directories such as OpenLDAP or OracleLDAP. Review the following information for supported environments and versions.

Requirements

The Directory Sync service is required for directory integration. Before you integrate your enterprise directory, install one or more instances of the Directory Sync service. The Directory Sync service is available as a component of the Workspace ONE Access connector. See [Workspace ONE Access documentation center](#) for information.

Supported Active Directory Environments and Versions

You can integrate Active Directory over LDAP or over Integrated Windows Authentication.

- Supported Active Directory environments:
 - Single Active Directory domain
 - Multiple domains in a single Active Directory forest
 - Multiple domains across multiple Active Directory forests
- Supported versions:
 - Active Directory on Windows Server 2012 R2, 2016, and 2019 with a Domain functional level and Forest functional level of Windows 2003 and later.

Note A higher functional level may be required for some features. For example, to allow users to change their Active Directory passwords from Workspace ONE, the Domain functional level must be Windows 2008 or later.

Supported LDAP Directories

You can integrate the following types of LDAP directories:

- OpenLDAP - 2.4

- Oracle LDAP - Directory Server Enterprise Edition 11g, Release 1 (11.1.1.7.0)
- IBM Tivoli Directory Server 6.3.1

Security Considerations

For enterprise directories integrated with the Workspace ONE Access service, security settings such as user password complexity rules and account lockout policies must be set in the enterprise directory directly. Workspace ONE Access does not override or enforce these settings.

About Integrating Your Enterprise Directory with Workspace ONE Access

2

Integrating your enterprise directory with Workspace ONE Access requires you to install the Directory Sync service, create a directory in the Workspace ONE Access service, and configure the connection to your enterprise directory.

Directory Sync Service

The Directory Sync service syncs user and group data from your Active Directory or LDAP directory to the Workspace ONE Access service. The Directory Sync service is a component of the Workspace ONE Access connector that you deploy on premises inside your enterprise network.

Workspace ONE Access Directory

The directory you create in the Workspace ONE Access service corresponds 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 Workspace ONE Access 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 Directory Sync service binds to Active Directory using simple bind authentication. The connection to Active Directory could be over SSL/TLS.
 - Active Directory over Integrated Windows Authentication: Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment. The Directory Sync service binds to Active Directory using Integrated Windows Authentication. The connection to Active Directory could be over SSL/TLS.

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 an LDAP directory to integrate your enterprise LDAP directory with Workspace ONE Access. You can only integrate a single-domain LDAP directory. Workspace ONE Access supports paged search queries and VLV for Oracle OpenLDAP.

Integration Process

Integrating your enterprise directory with Workspace ONE Access involves the following high-level tasks.

- Install the Directory Sync service.

A single instance of the Directory Sync service can sync multiple directories if the sync schedules do not overlap.

- Specify the attributes that you want users to have in the Workspace ONE Access service.
- Create a directory in the Workspace ONE Access service of the same type as your enterprise directory and configure the connection to the enterprise directory.
- Map the Workspace ONE Access attributes to attributes used in your Active Directory or LDAP directory.
- Specify sync settings.
- Specify 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.

Managing User Attributes in Workspace ONE Access

3

During the Workspace ONE Access directory setup process, you select the user attributes to sync to the Workspace ONE Access directory. The list of user attributes is managed from the **Identity & Access Management > Setup > User Attributes** page.

The User Attributes page lists the default Workspace ONE Access directory attributes that can be mapped to Active Directory or LDAP directory attributes. You select which attributes are required and which ones are optional. Attributes marked required must be populated for all synced user records. User records that are missing values for the required attributes will not be synced to Workspace ONE Access. Also keep in mind that you can only mark attributes required before any directory is created in the Workspace ONE Access service. After a directory is created, you can no longer change an attribute to be a required attribute.

Table 3-1. Default Attributes to Sync to Directory

Workspace ONE Access Directory Attribute Name	Default Mapping to Active Directory Attribute
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
domain	canonicalName. Adds the fully qualified domain name of object.
disabled (external user disabled)	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.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

On the User Attributes page, you can also enter additional 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.

The following attributes cannot be used as custom attribute names because the Workspace ONE Access service uses these attributes internally for user identity management.

Table 3-2. Attributes that Cannot be Used as Custom Attribute Names

active	externalId	locale	phoneNumbers	timezone
addresses	externalUserDisabled	meta	photos	title
displayName	groups	name	preferredLanguage	userName
emails	id	nickName	profileUrl	userType
employeeNumber	ims	password	schemas	x509Certificates

Note If your enterprise directory includes any of these attributes and you need to sync the attribute to Workspace ONE Access, create a custom attribute in Workspace ONE Access with a different name and map it to the directory attribute. For example, to sync the employeeNumber attribute from your directory to Workspace ONE Access, you can create an attribute named newEmployeeID in Workspace ONE Access and map it to the employeeNumber attribute when you create the Workspace ONE Access directory.

Attributes on the User Attributes page apply to all directories in the Workspace ONE Access service. When you make changes to user attributes, consider the effect on all directories. For example, if you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required except for **userName**. If an attribute is marked required, user records that do not contain a value for that attribute are not synced to the Workspace ONE Access service.

When you create a directory, the list of attributes from the User Attributes page appears on the Mapped Attributes page of the Add Directory wizard and you can specify the mapping between the Workspace ONE Access attributes and the Active Directory or LDAP directory attributes. After you create the directory, the Mapped Attributes page is available from the directory's Sync Settings page.

After any directory is created in the Workspace ONE Access service, you can no longer mark attributes required on the User Attributes page. The following changes to user attributes are still allowed:

- Add custom attributes (User Attributes page)
- Delete custom attributes (User Attributes page)
- Change required attributes to optional (User Attributes page)
- Change the mapping of attributes (directory's Sync Settings page)

Changes that are made and saved in the User Attributes page after a directory is created are applied to the directory with the next sync.

This chapter includes the following topics:

- [Select Attributes to Sync with Workspace ONE Access Directory](#)

Select Attributes to Sync with Workspace ONE Access Directory

Before creating the Workspace ONE Access directory, review the User Attributes page and specify which default attributes are required and add additional attributes if needed.

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

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

Procedure

- 1 In the Workspace ONE Access console, go to the **Identity & Access Management > Setup > User Attributes** page.
- 2 In the **Default Attributes** section, review the required attribute list and make appropriate changes to reflect which attributes should be required.
- 3 In the **Add other attributes to use** section, add other attributes to sync to the directory, if necessary.
- 4 Click **Save**.

Integrating Active Directory with Workspace ONE Access

4

You can integrate Workspace ONE Access with your Active Directory deployment to sync users and groups from Active Directory to the Workspace ONE Access service. The type of Active Directory environment that you have determines the type of directory you create in the Workspace ONE Access service.

Active Directory Environments

You can integrate the Workspace ONE Access 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 domain deployment, you can sync users and groups from a single Active Directory domain.

For this environment, you can create a directory either of type Active Directory over LDAP or type Active Directory over Integrated Windows Authentication in the Workspace ONE Access service.

For more information, see:

- [Chapter 3 Managing User Attributes in Workspace ONE Access](#)
- [Configuring Active Directory Connection to the Workspace ONE Access 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.

For this environment, in the Workspace ONE Access service you can create either a single Active Directory over Integrated Windows Authentication directory, or an Active Directory over LDAP directory configured with the Global Catalog option.

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

When you add a directory for this environment, select the Active Directory over 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 Directory Bind user is a member of.

For more information, see:

- [Chapter 3 Managing User Attributes in Workspace ONE Access](#)
- [Configuring Active Directory Connection to the Workspace ONE Access Service](#)
- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory 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.
- Users can sync to the Workspace ONE Access Global Catalog directory from multiple Active Directory domains, either directly or through group memberships. You must make sure that no other directory in the Workspace ONE Access tenant syncs users from the same domains, otherwise the conflict can cause sync failures.
- When Workspace ONE UEM is integrated with Workspace ONE Access 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.

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. In the Workspace ONE Access service, for this Active Directory environment create a single Active Directory over Integrated Windows Authentication directory.

When you add a directory for this environment, select the Active Directory over 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 Directory Bind user is a member of.

For more information, see:

- [Chapter 3 Managing User Attributes in Workspace ONE Access](#)
- [Configuring Active Directory Connection to the Workspace ONE Access 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 Workspace ONE Access service, one directory for each forest.

For more information, see:

- [Chapter 3 Managing User Attributes in Workspace ONE Access](#)
- [Configuring Active Directory Connection to the Workspace ONE Access Service](#)

This chapter includes the following topics:

- [Best Practices to Avoid Network Latency](#)
- [Configuring Active Directory Connection to the Workspace ONE Access Service](#)
- [Allowing Users to Change Active Directory Passwords from Intelligent Hub](#)
- [Syncing Users Migrated Between Domains \(Workspace ONE Access Cloud Only\)](#)

Best Practices to Avoid Network Latency

Follow these best practices for setting up the Workspace ONE Access connector and Active Directory domain controllers to avoid issues with network latency. This information is applicable for directories of type Active Directory over LDAP or Active Directory over Integrated Windows Authentication (IWA) in Workspace ONE Access.

- Avoid firewalls and Virtual IP Addresses (VIPs) on the path from the Workspace ONE Access connectors to the domain controllers. Firewalls and VIPs add more hops when the connector connects to the domain controllers.
- Ensure that network latency for LDAP simple bind between the connector nodes and the domain controllers is in milliseconds only, ideally less than 20 ms.
- Set the DNS A* records to point to the closest domain controllers for the connector's site specific configuration in Active Directory. This helps reduce latency.
- Configure multiple domain controllers for the domains to provide resiliency.
- Use the following commands from the connector server to help identify the nearest domain controllers for the domain:

```
nltest /dsgetdc:domain /try_next_closest_site
```

(This command gets the closest domain controller cached by the OS.)

```
nlttest /dsgetdc:domain /force
```

(This command clears the OS cache and tries to identify the closest domain controller again.)

Note To determine if domain controller network latency is an issue in your installation, see [Chapter 10 Troubleshooting Workspace ONE Access Directory Integration](#).

Configuring Active Directory Connection to the Workspace ONE Access Service

In the Workspace ONE Access console, enter the information required to connect to your Active Directory and select the users and groups to sync to the Workspace ONE Access 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 the Directory Sync service, which is available as a component of the Workspace ONE Access connector beginning with version 20.01.0.0. See the latest version of *Installing VMware Workspace ONE Access Connector* for information.

If you want to use the User Auth service to authenticate users of the directory, also install the User Auth service component.

- Select which user attributes are required and add additional attributes, if necessary, on the **Identity & Access Management > Setup > User Attributes** page in the Workspace ONE Access console. See [Chapter 3 Managing User Attributes in Workspace ONE Access](#). Keep the following considerations in mind:
 - If a user attribute is required, its value must be set for all the users that you want to sync. Users that do not have a value set are not synced.
 - Attributes apply to all directories.
 - After one or more directories are configured in the Workspace ONE Access service, attributes can longer be marked required.

- 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.

Note Workspace ONE Access connector version 19.03 and older versions do not support the / and \$ characters in a group's name or distinguishedName attribute. This limitation applies to groups that you add to the group DN as well as to groups that are not directly added to the group DN but are synced as part of a parent group when nested group memberships are selected.

Do not use the / or \$ character in a group's name or distinguishedName attribute if you plan to sync the group to VMware Identity Manager and you are using connector version 19.03 or older versions.

-
- If you are creating a directory of type Active Directory over LDAP using the Global Catalog option, you must make sure that no other directories in the Workspace ONE Access tenant sync users from the same domains as the Global Catalog directory. The conflict can cause sync failures.
 - 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.

Note For directories of type Active Directory over Integrated Windows Authentication, SASL Kerberos binding is used for encryption automatically. A certificate is not 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 Workspace ONE Access console, navigate to **Identity & Access Management > Manage > Directories**.
- 2 Click **Add Directory** and select **Active Directory**.
- 3 Enter a name for the Workspace ONE Access directory.
- 4 Select the type of Active Directory you are integrating, **Active Directory over LDAP** or **Active Directory over Integrated Windows Authentication**.

- 5 If you are integrating **Active Directory over LDAP**, follow these steps, otherwise proceed to step 6.
- a In the **Directory Sync and Authentication** section, make the following selections.

Option	Description
Directory Sync Hosts	<p>Select one or more Directory Sync service instances to use to sync this directory. All Directory Sync service instances that are registered with the tenant are listed. You can only select instances that are in Active state.</p> <p>If you select multiple instances, Workspace ONE Access uses the first selected instance in the list to sync the directory. If the first instance is unavailable, it uses the next selected instance, and so on. You can reorder the list from the directory's Sync Settings page after creating the directory.</p>
Authentication	<p>Select Yes if you want to authenticate users of this directory with the User Auth service. The User Auth service must already be installed. If you select Yes, the Password (cloud deployment) authentication method and an identity provider named IDP for <i>directoryName</i> of type Embedded are automatically created for the directory.</p> <p>Select No if you do not want to authenticate users of this directory with the User Auth service. If you decide to use the User Auth service later, you can create the Password (cloud deployment) authentication method and identity provider for the directory manually. When you do so, create a new identity provider for the directory by selecting Add Identity Provider > Create Built-in IDP in the Identity & Access Management > Identity Providers page. Using the pre-created identity provider named Built-in is not recommended.</p>
User Auth Hosts	<p>This option appears when Authentication is set to Yes. Select one or more User Auth service instances to use to authenticate users of this directory. All User Auth service instances that are registered with the tenant and that are in Active state are listed.</p> <p>If you select multiple instances, Workspace ONE Access sends authentication requests to the selected instances in round-robin order.</p>
User Name	Select the account attribute that contains username.
External ID	<p>The attribute that you want to use as the unique identifier for users in the Workspace ONE Access directory. The default value is objectGUID.</p> <p>You can set External ID to any of the following attributes:</p> <ul style="list-style-type: none"> ■ Any string attribute such as sAMAccountName or distinguishedName ■ The binary attributes objectSid, objectGUID, or mS-DS-ConsistencyGuid <p>The External ID setting only applies to users in Workspace ONE Access. For groups, External ID is always set to objectGUID and cannot be changed.</p> <p>Important All users must have a unique and non-empty value defined for the attribute. The value must be unique across the Workspace ONE Access tenant. If any users do not have a value for the attribute, the directory will not be synced.</p>

Keep the following considerations in mind while setting the External ID:

Option	Description
	<ul style="list-style-type: none">■ If you are integrating Workspace ONE Access with Workspace ONE UEM, make sure that you set the External ID to the same attribute in both products.■ You can change the External ID after creating the directory. However, the best practice is to set the External ID before syncing users to Workspace ONE Access. When you change the External ID, users are recreated. As a result, all users will be logged out and will have to log in again. You will also have to reconfigure user entitlements for Web apps and ThinApps. Entitlements for Horizon, Horizon Cloud, and Citrix will be deleted and then recreated at the next entitlements sync.■ The External ID option is available with Workspace ONE Access connector 20.10 and 19.03.0.1. All connectors associated with the Workspace ONE Access service must be version 20.10 or they must all be version 19.03.0.1. If different versions of the connector are associated with the service, the External ID option does not display.

b In the **Server Location** and **Encryption** sections, select from the following options.

Option	Description
If you want to use DNS Service Location lookup for Active Directory	<p>With this option, Workspace ONE Access finds and uses optimal domain controllers. If you do not want to use optimized domain controller selection, do not select this option.</p> <ol style="list-style-type: none">1 In the Server Location section, select the This Directory supports DNS Service Location check box.2 If your Active Directory requires access over SSL/TLS, select the STARTTLS required for all connections check box in the Encryption section. <p>Note If the This Directory supports DNS Service Location option is selected, STARTTLS is used for encryption over port 389. If the This Directory supports DNS Service Location option is deselected, LDAPS is used for encryption over port 636.</p> <ol style="list-style-type: none">3 Copy and paste the domain controllers' Intermediate (if used) and Root CA certificates into the SSL Certificate(s) 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. <p>If the domain controllers have certificates from multiple Intermediate and Root Certificate Authorities, enter all the Intermediate-Root CA certificate chains, one after another.</p> <p>For example:</p> <pre>-----BEGIN CERTIFICATE----- ... <Intermediate Certificate 1> ... -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ... <Root Certificate 1></pre>

Option	Description
	<pre>... -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ... <Intermediate Certificate 2> ... -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ... <Root Certificate 2> ... -----END CERTIFICATE-----</pre>
	<p>Note If your Active Directory requires access over SSL/TLS and you do not provide the certificates, you cannot create the directory.</p>
If you do not want to use DNS Service Location lookup for Active Directory	<ol style="list-style-type: none"><li data-bbox="673 651 1422 850">1 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. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in Chapter 4 Integrating Active Directory with Workspace ONE Access.<li data-bbox="673 861 1422 955">2 If your Active Directory requires access over SSL/TLS, select the LDAPS required for all connections check box in the Encryption section. Note If the This Directory supports DNS Service Location option is selected, STARTTLS is used for encryption over port 389. If the This Directory supports DNS Service Location option is deselected, LDAPS is used for encryption over port 636.<li data-bbox="673 1113 1422 1270">3 Copy and paste the domain controller's Intermediate (if used) and Root CA certificate into the SSL Certificate(s) text box. 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. Note If your Active Directory requires access over SSL/TLS and you do not provide the certificate, you cannot create the directory.
If you are integrating the directory as a Global Catalog	<ol style="list-style-type: none"><li data-bbox="673 1365 1422 1428">1 In the Server Location section, deselect the This directory supports DNS Service Location option.<li data-bbox="673 1438 1422 1470">2 Select the This Directory has a Global Catalog option.<li data-bbox="673 1480 1422 1543">3 In the Server Host text box, enter the Active Directory server host name.<li data-bbox="673 1554 1422 1606">4 The Server Port is set to 3268. If you select SSL/TLS in the Encryption section, the port is set to 3269.<li data-bbox="673 1617 1422 1669">5 If your Active Directory requires access over SSL/TLS, select the option LDAPS required for all connections in the Encryption section.

Option	Description
	6 Copy and paste the domain controller's Intermediate (if used) and Root CA certificate into the SSL Certificate(s) text box. 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.

- c In the **Bind User Details** section, enter the following information.

Option	Description
Base DN	<p>Enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com.</p> <p>Important 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.</p> <p>Note If you are adding the directory as a Global Catalog, the Base DN is not needed and the option does not appear.</p>
Bind User DN	<p>Enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com.</p> <p>Note Using a Bind user account with a non-expiring password is recommended.</p>
Bind User Password	The bind user password.

- 6 If you are integrating **Active Directory over Integrated Windows Authentication**, follow these steps.
- a In the **Directory Sync and Authentication** section, make the following selections.

Option	Description
Directory Sync Hosts	<p>Select one or more Directory Sync service instances to use to sync this directory. All Directory Sync service instances that are registered with the tenant and that are in Active state are listed.</p> <p>If you select multiple instances, Workspace ONE Access uses the first selected instance in the list to sync the directory. If the first instance is unavailable, it uses the next selected instance, and so on. You can reorder the list from the directory's Sync Settings page after creating the directory.</p>
Authentication	<p>Select Yes if you want to authenticate users of this directory with the User Auth service. The User Auth service must already be installed. If you select Yes, the Password (cloud deployment) authentication method and an identity provider named IDP for <i>directory</i> of type Embedded are automatically created for the directory.</p> <p>Select No if you do not want to authenticate users of this directory with the User Auth service. If you change your mind later, you can create the Password (cloud deployment) authentication method and identity provider for the directory manually. When you do so, create a new identity provider for the directory by selecting Add Identity Provider > Create Built-in IDP in the Identity & Access Management > Identity Providers page. Using the pre-created identity provider named Built-in is not recommended.</p>
User Auth Hosts	<p>This option appears when Authentication is set to Yes. Select one or more User Auth service instances to use to authenticate users of this directory. All User Auth service instances that are registered with the tenant and that are in Active state are listed.</p> <p>If you select multiple instances, Workspace ONE Access sends authentication requests to the selected instances in round-robin order.</p>
User Name	Select the account attribute that contains username.
External ID	<p>The attribute that you want to use as the unique identifier for users in the Workspace ONE Access directory. The default value is objectGUID.</p> <p>You can set External ID to any of the following attributes:</p> <ul style="list-style-type: none"> ■ Any string attribute such as sAMAccountName or distinguishedName ■ The binary attributes objectSid, objectGUID, or mS-DS-ConsistencyGuid <p>The External ID setting only applies to users in Workspace ONE Access. For groups, External ID is always set to objectGUID and cannot be changed.</p> <p>Important All users must have a unique value defined for the attribute. The value must be unique across the Workspace ONE Access tenant.</p> <p>Keep the following considerations in mind while setting the External ID:</p> <ul style="list-style-type: none"> ■ If you are integrating Workspace ONE Access with Workspace ONE UEM, make sure that you set the External ID to the same attribute in both products.

Option	Description
	<ul style="list-style-type: none"><li data-bbox="662 210 1423 472">■ You can change the External ID after creating the directory. However, the best practice is to set the External ID before syncing users to Workspace ONE Access. When you change the External ID, users are recreated. As a result, all users will be logged out and will have to log in again. You will also have to reconfigure user entitlements for Web apps and ThinApps. Entitlements for Horizon, Horizon Cloud, and Citrix will be deleted and then recreated at the next entitlements sync.<li data-bbox="662 472 1423 642">■ The External ID option is available with Workspace ONE Access connector 20.10 and 19.03.0.1. All connectors associated with the Workspace ONE Access service must be version 20.10 or they must all be version 19.03.0.1. If different versions of the connector are associated with the service, the External ID option does not display.

- b No action is required in the **Encryption** section. Directories of type Active Directory over Integrated Windows Authentication use SASL Kerberos binding automatically and do not require you to select LDAPS or STARTTLS.
- c 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.

7 Click **Save & Next**.

8 In the Select the Domains page, select domains if applicable, then click **Next**.

- For a directory of type Active Directory over LDAP, the domains are listed and already selected.
- For a directory of type Active Directory over Integrated Windows Authentication, select the domains that should be associated with this Active Directory connection. All the domains with a two-way trust relationship with the base domain are listed.

If domains with a two way trust relationship with the base domain are added to Active Directory after the Workspace ONE Access directory is created, you can add them from the directory's **Sync Settings > Domains** page by clicking the refresh icon to get the latest list.

Tip Choose trusted domains one by one instead of selecting all the domains at once. This ensures that domain save is not a long-running operation that can potentially time out. Choosing domains sequentially ensures that the Directory Sync service spends time trying to resolve a single domain only.

- If you are creating an Active Directory over LDAP directory with the Global Catalog option selected, the Domains tab does not appear.

- 9 In the Map User Attributes page, verify that the Workspace ONE Access directory attribute names are mapped to the correct Active Directory attributes and make changes, if necessary, then click **Next**.

Important If an attribute is marked required, its value must be set for all the users that you want to sync. User records that are missing values for the required attributes will not be synced.

- 10 Follow the instructions in [Selecting Users and Groups to Sync to Your Workspace ONE Access Directory](#) to add groups in the **Select the groups you want to sync** page and users in the **Select the users you would like to sync** page.
- 11 In the Sync Frequency page, set up a sync schedule to sync users and groups at regular intervals or select **Manually** in the **Sync Frequency** drop-down list if you do not want to set a schedule.

The time is set in UTC.

Tip 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.

If you select **Manually**, you must click the **Sync** button on the directory page whenever you want to sync the directory.

- 12 Click **Save** to create the directory or **Sync Directory** to create the directory and start syncing it.

Results

The connection to Active Directory is established. If you clicked **Sync Directory**, users, and group names, are synced from Active Directory to the Workspace ONE Access directory.

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

What to do next

- If you set the Authentication option to Yes, an identity provider named **IDP for *directoryname*** and a Password (cloud deployment) authentication method are automatically created for the directory. You can view these on the **Identity & Access Management > Manage > Identity Providers** and **Connector Authentication Methods** pages. You can also create more authentication methods for the directory from the **Connector Authentication Methods** tab. For information about creating authentication methods, see [Managing User Authentication Methods in Workspace ONE Access](#).
- Review the default access policy on the **Identity & Access Management > Manage > Policies** page.
- Review the default sync safeguards settings and make changes if required. See [Setting up Directory Sync Safeguards in Workspace ONE Access](#) for information.

Allowing Users to Change Active Directory Passwords from Intelligent Hub

By configuring settings in Workspace ONE Access, you can provide users the ability to change their Active Directory passwords from the Workspace ONE Intelligent Hub app or portal whenever they want. Users can also reset their Active Directory passwords from the 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 set this option per directory, by selecting the **Allow Change Password** option in the directory's settings page.

Users can change their passwords when they are logged into Intelligent Hub from a browser by clicking their name in the top-right corner, selecting **Account** from the drop-down menu, and clicking the **Change Password** link. In the Intelligent Hub 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 Workspace ONE Access 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 Workspace ONE Access, 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 Workspace ONE Access.

Note The Allow Change Password option cannot be selected 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 the Directory Sync service 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 Directory Sync service host 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 Workspace ONE Access console, navigate to the **Identity & Access Management > Setup > Directories** page.
- 2 Click the directory you want to configure.
- 3 In the **Allow Change Password** section, select the **Enable Change Password** check box.
- 4 Enter the Bind DN password in the **Bind User Details** section, and click **Save**.

Syncing Users Migrated Between Domains (Workspace ONE Access Cloud Only)

Workspace ONE Access supports syncing users that are migrated from one Active Directory domain to another without requiring any additional configuration. This feature is supported with Workspace ONE Access connector version 20.01 and later.

Follow these guidelines:

- If a user is migrated from one domain to another domain within the same Workspace ONE Access Integrated Windows Authentication (IWA) directory, Workspace ONE Access automatically syncs the user to the correct domain during the next sync.
- If a user is migrated from one domain to another domain within the same Workspace ONE Access Global Catalog directory, Workspace ONE Access automatically syncs the user to the correct domain during the next sync.
- If a user is migrated from a domain in one Workspace ONE Access directory to a domain in another Workspace ONE Access directory, perform the following steps:
 - a After migrating the user in Active Directory, go to the Workspace ONE Access console and sync the source directory (the directory to which the user originally belonged).
The migrated user is deleted from the Workspace ONE Access directory during the sync.
 - b Sync the target directory (the directory to which the user was migrated).
The migrated user is synced to the Workspace ONE Access directory.

Note If you sync the target directory before the source directory, the migrated user is not added to the target directory in Workspace ONE Access and an alert appears in the directory's Sync Log page. To resolve the issue, sync the source directory, then sync the target directory again.

Integrating LDAP Directories with Workspace ONE Access

5

You can integrate your enterprise LDAP directory, such as OpenLDAP or OracleLDAP directories, with Workspace ONE Access to sync users and groups from the LDAP directory to the Workspace ONE Access service.

For the types of LDAP directories supported, see [Chapter 1 Workspace ONE Access Directory Integration Requirements and Supported Directories](#).

Limitations of LDAP Directory Integration

The following limitations apply to LDAP directory integration.

- You can only integrate a single-domain LDAP directory.
To integrate multiple domains from an LDAP directory, you create multiple VMware Workspace ONE Access directories, one for each domain.
- The following authentication methods are not supported for VMware Workspace ONE Access directories of type LDAP directory.
 - Kerberos authentication
 - SecurID
 - RADIUS
- You cannot join an LDAP domain.
- Integration with Horizon or Citrix-published resources is not supported for VMware Workspace ONE Access 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 Workspace ONE Access service.

- If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the VMware Workspace ONE Access 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.

This chapter includes the following topics:

- [Integrating an LDAP Directory with the Workspace ONE Access Service](#)

Integrating an LDAP Directory with the Workspace ONE Access Service

You can integrate your enterprise LDAP directory with VMware Workspace ONE Access to sync users and groups from the LDAP directory to the VMware Workspace ONE Access service.

To integrate your LDAP directory, you create a corresponding VMware Workspace ONE Access directory and sync users and groups from the LDAP directory to the VMware Workspace ONE Access 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 Workspace ONE Access attributes.

Your LDAP directory configuration might be based on default schemas or custom schemas. It might also have custom attributes. For VMware Workspace ONE Access 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, External ID, and distinguished name or equivalent attribute

Certain limitations apply to the LDAP directory integration feature. See [Chapter 5 Integrating LDAP Directories with Workspace ONE Access](#) .

Prerequisites

- Install the Directory Sync service, which is available as a component of the Workspace ONE Access connector beginning with version 20.01.0.0. See the latest version of *Installing VMware Workspace ONE Access Connector* for information.

If you want to use the User Auth service to authenticate users of the directory, also install the User Auth service component.

- 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 Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access 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 Workspace ONE Access **domain** attribute when you create the VMware Workspace ONE Access 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 Workspace ONE Access console, go to the **Identity & Access Management > Manage > Directories** page.
- 2 Click **Add Directory** and select **LDAP Directory**.

3 Enter the required information in the Add Directory page.

Option	Description
Directory Name	Enter a name for the VMware Workspace ONE Access directory.
Directory Sync and Authentication	<p>a For Directory Sync Hosts, select one or more Directory Sync service instances to use to sync this directory. All Directory Sync service instances that are registered with the tenant are listed. You can only select instances that are in Active state.</p> <p>If you select multiple instances, Workspace ONE Access uses the first selected instance in the list to sync the directory. If the first instance is unavailable, it uses the next selected instance, and so on. You can reorder the list from the directory's Sync Settings page after creating the directory.</p> <p>b For Authentication, select Yes if you want to authenticate users of this directory with the User Auth service. The User Auth service must already be installed. If you select Yes, the Password (cloud deployment) authentication method and an identity provider named IDP for <i>directoryName</i> of type Embedded are automatically created for the directory.</p> <p>Select No if you do not want to authenticate users of this directory with the User Auth service. If you decide to use the User Auth service later, you can create the Password (cloud deployment) authentication method and identity provider for the directory manually. When you do so, create a new identity provider for the directory by selecting Add Identity Provider > Create Built-in IDP in the Identity & Access Management > Identity Providers page. Using the pre-created identity provider named Built-in is not recommended.</p> <p>c The User Auth Hosts option appears when Authentication is set to Yes. Select one or more User Auth service instances to use to authenticate users of this directory. All User Auth service instances that are registered with the tenant and that are in Active state are listed.</p> <p>If you select multiple instances, Workspace ONE Access sends authentication requests to the selected instances in round-robin order.</p> <p>d In the User Name text box, select the LDAP directory attribute to use for user name. If the attribute is not listed, select Custom and type the custom attribute name to use for users and for groups. For example, cn.</p>
Server Location	<p>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.</p> <p>If you have a cluster of servers behind a load balancer, enter the load balancer information instead.</p>

Option	Description
LDAP Configuration	<p>Specify the LDAP search filters and attributes that VMware Workspace ONE Access can use to query your LDAP directory. Default values are provided based on the core LDAP schema.</p> <p>Filter Queries</p> <ul style="list-style-type: none"> ■ Groups: The search filter for obtaining group objects. For example: <code>(objectClass=groupOfNames)</code> ■ Bind User: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: <code>(objectClass=person)</code> ■ Users: The search filter for obtaining users to sync. For example: <code>(&(objectClass=user)(objectCategory=person))</code> <p>Attributes</p> <ul style="list-style-type: none"> ■ Membership: The attribute that is used in your LDAP directory to define the members of a group. For example: <code>member</code> ■ External ID: The attribute that you want to use as the unique identifier for users and groups in the Workspace ONE Access directory. The default value is entryUUID. <hr/> <p>Important All users must have a unique and non-empty value defined for the attribute. The value must be unique across the Workspace ONE Access tenant. If any users do not have a value for the attribute, the directory will not be synced.</p> <hr/> <p>Keep the following considerations in mind while setting the External ID:</p> <ul style="list-style-type: none"> ■ If you are integrating Workspace ONE Access with Workspace ONE UEM, make sure that you set the External ID to the same attribute in both products. ■ You can change the External ID after creating the directory. However, the best practice is to set the External ID before syncing users to Workspace ONE Access. When you change the External ID, users are recreated. As a result, all users will be logged out and will have to log in again. You will also have to reconfigure user entitlements for Web apps and ThinApps. Entitlements for Horizon, Horizon Cloud, and Citrix will be deleted and then recreated at the next entitlements sync. ■ The External ID option is available with Workspace ONE Access connector 20.10 and 19.03.0.1. All connectors associated with the Workspace ONE Access service must be version 20.10 or they must all be version 19.03.0.1. If different versions of the connector are associated with the service, the External ID option does not display. ■ Distinguished Name: (Optional) The attribute that is used in your LDAP directory for the distinguished name of a user or group. For example: <code>dn</code> <p>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.</p>

Option	Description
	<ul style="list-style-type: none">■ Enable advanced LDAP configuration: 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.■ Group Filter: The value to use to query and identify groups. This value is required if your LDAP schema does not have the distinguished name attribute. For example: <code>cn</code>■ User Filter: The value to use to query and identify users. This value is required if your LDAP schema does not have the distinguished name attribute. For example: <code>uid</code>■ User Membership Mapping Filter: (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. For example: <code>uidNumber</code>
Encryption	If your LDAP directory requires access over SSL, select the LDAPS required for all connections 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 "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.
Bind User Details	<p>Base DN: Enter the DN from which to start searches. For example, <code>cn=users,dc=example,dc=com</code></p> <p>Bind User DN: Enter the user name to use to bind to the LDAP directory.</p> <hr/> <p>Note Using a Bind DN user account with a non-expiring password is recommended.</p> <hr/> <p>Bind User Password: Enter the password for the Bind DN user.</p>

- 4 Click **Save & Configure**.
- 5 In the Domains page, verify that the correct domain is listed, then click **Next**.
- 6 In the Map Attributes page, verify that the VMware Workspace ONE Access attributes are mapped to the correct LDAP directory attributes and make changes if necessary.

These attributes will be synced for users.

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

You can add attributes and manage the list of required attributes from the **Setup > User Attributes** page.

Important If an attribute is marked required, its value must be set for all the users that you want to sync. User records that are missing values for the required attributes will not be synced.

- 7 Click **Next**.
- 8 Follow the instructions in [Selecting Users and Groups to Sync to Your Workspace ONE Access Directory](#) to add groups in the **Select the groups you want to sync** page and users in the **Select the users you would like to sync** page.
- 9 In the Sync Frequency page, set up a sync schedule to sync users and groups at regular intervals or select **Manually** in the **Sync Frequency** drop-down list if you do not want to set a schedule.

The time is set in UTC.

Tip 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.

If you select **Manually**, you must click the **Sync** button on the directory page whenever you want to sync the directory.

- 10 Click **Save** to create the directory or **Sync Directory** to create the directory and start syncing it.

Results

The connection to the LDAP directory is established. If you clicked **Sync Directory**, users and group names are synced from the LDAP directory to the Workspace ONE Access directory.

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

What to do next

- If you set the Authentication option to Yes, an identity provider named **IDP for *directoryname*** and a Password (cloud deployment) authentication method are automatically created for the directory. You can view these on the **Identity & Access Management > Manage > Identity Providers** and **Connector Authentication Methods** pages. You can also create more authentication methods for the directory from the **Connector Authentication Methods** tab. For more information about creating authentication methods, see [Managing User Authentication Methods in Workspace ONE Access](#).
- Review the default access policy on the **Identity & Access Management > Manage > Policies** page.
- Review the default sync safeguards settings and make changes if required. See [Setting up Directory Sync Safeguards in Workspace ONE Access](#) for information.

Configuring High Availability for Directory Sync in Workspace ONE Access

6

You can configure high availability for directory sync by associating the directory with multiple Directory Sync service instances and then setting up a Sync Services list for the directory. The Directory Sync service instances in the Sync Services list are arranged in failover order. The Workspace ONE Access service uses the first Directory Sync service in the list to sync users and groups for the directory. If the first Directory Sync service is unavailable, it uses the next one in the list, and so on.

Each directory has its own Sync Services list.

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

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

Prerequisites

- You have installed and configured additional Directory Sync service instances. See *Installing Workspace ONE Access Connector* for information.

Procedure

- 1 In the Workspace ONE Access console, navigate to the **Identity & Access Management > Manage > Directories** page.
- 2 Click the directory for which you want to configure high availability.
- 3 Click **Sync Settings**, then click the **Sync Service** tab.
- 4 From the **Select Sync Service** drop-down menu, which displays all the Directory Sync service instances associated with the Workspace ONE Access service, select the Directory Sync service instance to add, then click **+**.

The Directory Sync service instance is added to the **Sync Services** list.

- 5 Add all the Directory Sync service instances that you want to use to the **Sync Services** list.

- 6 In the **Sync Services** list, arrange the entries in failover order by using the up and down arrow keys.

To perform a directory sync, Workspace ONE Access uses the first Directory Sync service instance in the list. If the first instance is unavailable, it tries to use the second one, and so on.

- 7 Click **Save**.

Results

The list of Directory Sync service instances is saved and is applied from the next sync onwards.

You can view which Directory Sync service instances were used for each sync run in the **Sync Log** tab of the directory page.

Managing Directory Settings in Workspace ONE Access

7

After you set up a directory in the Workspace ONE Access service, you can view and modify the directory configuration and sync settings from the **Identity & Access Management > Manage > Directories** page. After you make changes, you can trigger a manual sync or wait for the next scheduled sync run for the changes to take effect.

Examples of settings you can update include setting up sync safeguards, modifying user and group DNs to sync, changing the sync schedule, and changing the failover order of Directory Sync service instances associated with the directory.

You can also monitor the sync status for the directory and troubleshoot problems that occur. Sync logs provide detailed information such as the number of users and groups added during a sync run, the Directory Sync service instance used, and any alerts that were raised.

This chapter includes the following topics:

- [Setting up a Directory Sync Schedule in Workspace ONE Access](#)
- [Syncing a Directory Manually in Workspace ONE Access](#)
- [Viewing Directory Sync Status in Workspace ONE Access](#)
- [Setting up Directory Sync Safeguards in Workspace ONE Access](#)
- [Updating Domains to Sync to Workspace ONE Access Directory](#)
- [Selecting Users and Groups to Sync to Your Workspace ONE Access Directory](#)
- [Specifying Filters for Directory Sync in Workspace ONE Access](#)

Setting up a Directory Sync Schedule in Workspace ONE Access

You can set up a sync schedule so that users and groups are synced automatically from your Active Directory or LDAP directory to the Workspace ONE Access service at regular intervals. When you set up a schedule, changes in the enterprise directory are reflected in your Workspace ONE Access directory without requiring a manual sync.

You can set a schedule to sync users and groups weekly, daily, or every hour. Or you can choose to manually sync users and groups. When you set the schedule to Manually, you can use the Sync button on the directory page 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.

If you are using multiple Directory Sync service instances for high availability, see [Chapter 6 Configuring High Availability for Directory Sync in Workspace ONE Access](#) for guidelines on scheduling.

Procedure

- 1 Select the **Identity & Access Management > Manage > Directories** tab.
- 2 Click the directory.
- 3 Click **Sync Settings**.
- 4 In the **Sync Frequency** tab, set the sync frequency, and the day and time of day to run the sync.

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 in Workspace ONE Access](#).

See also [Syncing a Directory Manually in Workspace ONE Access](#) .

Syncing a Directory Manually in Workspace ONE Access

When you want to sync updates from your enterprise directory to your Workspace ONE Access directory immediately, you can start the sync process manually. Directories that do not have a sync schedule set must always be synced manually.

Procedure

- 1 Select the **Identity & Access Management > Manage > Directories** tab.
- 2 Click the directory you want to sync.
- 3 On the left of the page, click **Sync** and select **Sync with Safeguards** or **Sync without Safeguards**.

The **Sync with Safeguards** option enforces the safeguard limits that are set on the **Sync Settings > Safeguards** page and will fail if the changes exceed the limits. **Sync without Safeguards** ignores the safeguards limits.

Results

The sync process starts in the background. If a large number of users and groups are synced, the process can take a while to finish. You can continue using the console in the meantime. To view the sync progress, click the **Refresh** link that replaces the Sync button while sync is in progress.

What to do next

After the sync process is complete, you can view the sync status in the **Sync Log** tab. See [Viewing Directory Sync Status in Workspace ONE Access](#) for more information.

Viewing Directory Sync Status in Workspace ONE Access

You can check the sync status for your Workspace ONE Access directories to see whether sync completed successfully, view alerts, and view the specific changes that were made during sync.

The Directories tab displays sync status for all directories. Detailed sync information for each directory can be found on the **Sync Log** tab on the directory page.

Procedure

- 1 Select the **Identity & Access Management > Manage > Directories** tab.

On this page, you can view information for all the directories that you have set up. For each directory of type Active Directory over LDAP, Active Directory over IWA, or LDAP Directory, you can view the following information:

- The number of synced domains
- The number of synced users and groups
- The time of the last sync
- Any alerts that occurred during the last sync

Click the number in the **Alerts** column to view the alerts. On the Alerts page, use the scrollbars, if they appear, to see the full text of each message.

- 2 To view detailed sync logs for a directory, click the directory name, then select the **Sync Log** tab.

Each time sync is completed, a sync log is generated and displayed on the page. You can view the following information:

- All sync runs
- The time each sync run started
- The Directory Sync service instance that was used to perform sync
- How many users and groups were added or deleted during the sync run

Click the link in the **Sync Details** column to see which users and groups were added or deleted.

- The status of each sync run

A green check mark in the last column indicates that sync completed successfully. A red x indicates that sync failed.

- Any alerts that occurred during the sync

Click the number in the **Alerts** column to view the alerts. On the Alerts page, use the scrollbars, if they appear, to see the full text of each message.

Setting up Directory Sync Safeguards in Workspace ONE Access

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

The sync safeguard thresholds that are set limit the number of changes that can be made to 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. If SMTP is configured in the Workspace ONE Access 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 sync manually with the **Sync > Sync without Safeguards** option on the directory page. When you sync without safeguards, the safeguard values are not enforced for the current 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 activated.

Configure Directory Sync Safeguards in Workspace ONE Access

Configure the sync safeguard threshold settings to limit the number of changes that can be made to users and groups when the Workspace ONE Access directory syncs with your enterprise directory. If any directory safeguard threshold is met, the directory synchronization stops.

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 activated.

Procedure

- 1 In the Workspace ONE Access console, go to the **Identity & Access Management > Manage > Directories** page.
- 2 Click the directory for which to set safeguards, then click **Sync Settings** .
- 3 Click the **Safeguards** tab.
- 4 Set the percentage of changes to trigger the sync to fail.
- 5 Click **Save**.

Ignore Safeguard Settings to Complete Syncing to Workspace ONE Access Directory

When you receive notification that your Workspace ONE Access directory sync did not complete because of a safeguard violation, you can override the safeguard setting and complete the sync.

Procedure

- 1 In the Workspace ONE Access console, go to the **Identity & Access Management > Manage > Directories** page.
- 2 Click the directory that did not complete the sync.
- 3 On the left of the page, click **Sync** and select **Sync without Safeguards**.

Results

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

Updating Domains to Sync to Workspace ONE Access Directory

You can view and update the list of domains that sync from your enterprise directory to your Workspace ONE Access directory from the directory's **Sync Settings > Domains** tab. You can only update the list of domains for directories of type Active Directory over Integrated Windows Authentication. Selected domains for directories of type LDAP, or Active Directory over LDAP, cannot be changed.

Tip Choose trusted domains one by one instead of selecting all the domains at once. This ensures that domain save is not a long-running operation that can potentially time out. Choosing domains sequentially ensures that the Directory Sync service spends time trying to resolve a single domain only.

Note For Active Directory over LDAP directories that have the Global Catalog option selected, the Domains tab does not appear.

Procedure

1 In the Workspace ONE Access console, navigate to the **Identity & Access Management > Manage > Directories** page.

2 Click the directory.

3 Click **Sync Settings**, then select the **Domains** tab.

The list of domains that are currently selected for the directory appears.

4 Click the refresh icon next to **Fetch all domains** to see the list of selected and available domains.

When you click the refresh icon, the Directory Sync service connects to the Active Directory server and retrieves the latest list of domains.

5 Select the domains you want to sync to the Workspace ONE Access directory.

Make sure that at least one domain is selected.

6 Click **Save**.

Selecting Users and Groups to Sync to Your Workspace ONE Access Directory

When you configure the connection to your enterprise Active Directory or LDAP directory in the Workspace ONE Access console, you specify the users and groups to sync to Workspace ONE Access. You initially specify users and groups when you create a directory in Workspace ONE Access. Later, you can view and modify the users and groups from the **Users** and **Groups** tabs on the directory's **Sync Settings** page.

Keep the following considerations in mind while adding groups.

- As a best practice, add and sync a small number of groups while creating the directory. After the initial setup, you can add more groups.
- When groups are added and synced, 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.

Note You can override this restriction by selecting the **Sync Group Members to the Directory When Adding Group** option in the **Identity & Access Management > Setup > Preferences** page.

- (Active Directory) When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.
- (LDAP 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.

Keep the following considerations in mind while adding users:

- 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.
- The Bind user that you specified in the Bind Details section is not synced to the Workspace ONE Access service by default. If you want to sync the Bind user, enter the Bind user DN on the users page. After the directory is synced, you can set the role for the Bind user if required.

Procedure

- 1 To navigate to the users and groups pages, choose from the following options.
 - If you are adding users and groups while creating the Workspace ONE Access directory, in the Add Directory wizard proceed to the **Select the groups you want to sync** page.
 - If you are adding or modifying users and groups after creating the Workspace ONE Access directory:
 - a Navigate to the **Identity & Access Management > Manage > Directories** page.
 - b Click the directory you want to update.
 - c Click **Sync Settings**, then select the **Groups** tab.

The page displays the group DNs that you added previously and the number of groups in each group DN that are selected for sync. You can click **Select** to see the list of groups under a group DN.

- 2 Select the groups to sync from your enterprise directory to the Workspace ONE Access directory.

To select groups, specify one or more group DNs and select the groups under them.

- a In the **Specify the top-level group** row, click **+** and specify the top-level group DN. For example, CN=users,DC=example,DC=company,DC=com.

Tip Entering a high-level DN such as the Base DN to search under is not recommended, as search will take a long time. Try to enter a more specific DN to search under.

Important 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.

- b If you want to select all the groups under the group DN you added, select the **Select All** check box.

If groups are added to or deleted from the group DN in the enterprise directory after the Workspace ONE Access directory is created, the changes are reflected in subsequent syncs.

- c If you want to select specific groups under the group DN instead of selecting all of them, click **Select Groups**, make your selections, and click **Save**.

When you click **Select Groups**, all the groups found in the DN are listed. You can narrow the results or search for specific groups by entering a search term in the search box.

- d Select or deselect the **Sync nested group members** option, as needed.

The **Sync nested group members** option is selected by default. When this option is selected, 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 Workspace ONE Access directory, these users will be members of the parent group that you selected for sync.

If the **Sync nested group members** option is not selected, when you specify a group to sync, all the users that belong directly to that group are synced but users that belong to nested groups under it are not synced. Deselecting this option is useful for large directory configurations where traversing a group tree is resource and time intensive. If you deselect this option, ensure that you select all the groups whose users you want to sync.

3 Navigate to the users page.

- If you are adding users and groups from the Add Directory wizard, click **Next** to proceed to the **Select the users you would like to sync** page.
- If you are adding or modifying users and groups from the directory's Sync Settings pages, click **Save** in the **Groups** tab, then select the **Users** tab.

4 Select the users to sync from your enterprise directory to the Workspace ONE Access directory.

- a In the **Specify the user DNs** row, click **+** and enter the user DNs. For example:

```
CN=username , CN=Users , OU=Sales , DC=example , 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.

To check if the user DN is valid and to see the number of users that will be synced, click the **Test** button for that row.

- b Specify filters to include or exclude users from the DNs, if needed.

See [Specifying Filters for Directory Sync in Workspace ONE Access](#) for information.

5 Save your changes.

Specifying Filters for Directory Sync in Workspace ONE Access

When you integrate your Active Directory or LDAP directory with Workspace ONE Access, you specify the user DNs to sync. You can apply filters to the user DNs to include or exclude specific users.

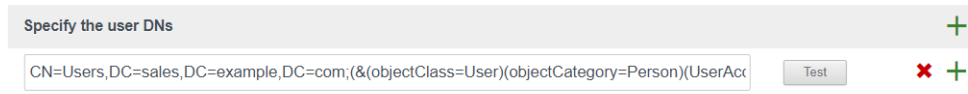
If a DN contains extraneous user objects that do not need to be synced to Workspace ONE Access, you can specify LDAP filters to narrow the query or you can filter out objects after the query is done. The option you use depends on your specific scenario. If a large number of objects in the DN need to be excluded, using an inclusion filter with the DN makes the query and sync process more efficient because Workspace ONE Access does not have to retrieve the extra objects from your Active Directory or LDAP directory. On the other hand, if you need to exclude only a small number of objects, you can use exclusion filters. Exclusion filters are applied after all the user objects are retrieved from your Active Directory or LDAP directory.

Note Inclusion filters are available with Workspace ONE Access Connector 20.10 and later.

Using Inclusion Filters

To specify an inclusion filter, append a semicolon to the user DN that you want to filter, then enter the filter. Use the standard LDAP search filter syntax. For example, if your DN is **CN=Users,DC=sales,DC=example,DC=com** and you want to sync only the users that are enabled, you can use the following query:

```
CN=Users,DC=sales,DC=example,DC=com; (& (objectClass=User)
(objectCategory=Person) (UserAccountControl=512) )
```



To check if the query is valid and to see the number of users that will be synced, click the **Test** button.

If you do not specify a filter, Workspace ONE Access applies the following filter by default.

- For Active Directory: **(& (objectClass=User) (objectCategory=Person))**
- For LDAP directory: The filter that you specified in the **LDAP Configuration** section while creating the LDAP directory in Workspace ONE Access.

Using Exclusion Filters

You can create exclusion filters in the **Add a filter to exclude users** section to exclude users based on the attribute chosen. You can create multiple exclusion filters.

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

Option	Description
Contains	Excludes all users who match the attribute and value set. For example, name contains Jane excludes users named "Jane".
Does not contain	Excludes all users except for those who match the attribute and value set. For example, telephoneNumber does not contain 800 includes only users with a telephone number that includes "800".
Begins with	Exclude all users where the attribute value begins with the specified characters. For example, employeeID begins with ACME0 excludes all users that have an employee ID that includes "ACME0" at the beginning of their ID number.
Ends with	Exclude all users where the attribute value ends with the specified characters. For example, mail ends with example1.com excludes all users that have an email address that ends in "example1.com".

The value is case-insensitive. Do not use the following symbols in the value string.

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

For example, if your DN is **CN=Users,DC=sales,DC=example,DC=com**, and you want to exclude users that are disabled, you can use the following filter:

Specify the user DNs +

CN=Users,DC=sales,DC=example,DC=com Test x +

Add a filter to exclude users +

userAccountControl v contains v 514 x +

Deleting a Workspace ONE Access Directory



When you no longer want to include users and groups in the Workspace ONE Access service that belong to a specific Active Directory or LDAP directory, you can delete the corresponding Workspace ONE Access directory. Deleting a directory also deletes all its users and groups from the Workspace ONE Access service.

Procedure

- 1 In the Workspace ONE Access console, navigate to the **Identity & Access Management > Manage > Directories** page.
- 2 Click the directory you want to delete.
- 3 On the directory page, click **Delete Directory**.

The confirmation dialog displays the number of users and groups that will be deleted. To proceed, click **Delete**.

Results

The directory is deleted from the Workspace ONE Access service and no longer appears on the Directories page. All the users and groups that were part of the directory are deleted. Identity providers and authentication methods associated with the directory are also deleted.

Converting a Directory of Type Other in Workspace ONE Access

9

In Workspace ONE Access, a directory of type Other can be converted to a directory of type Active Directory over LDAP or Active Directory over Integrated Windows Authentication. Use this feature if you are a Workspace ONE customer who has deployed Active Directory synchronization with Workspace ONE Access using AirWatch Cloud Connector (ACC) and want to take advantage of the additional functionality included with the Workspace ONE Access connector.

This one-time migration procedure converts the ACC directory of type Other to a directory of type Active Directory over LDAP or Active Directory over Integrated Windows Authentication, which are associated with the Workspace ONE Access connector. This procedure does not remove the existing directory or any entitlements associated with it.

Converting the Other directory for this use case includes the following tasks.

- 1 Install the Directory Sync service and the User Auth service, which are components of the Workspace ONE Access connector beginning with version 20.01.0.0. See the latest version of *Installing Workspace ONE Access Connector* for information.
- 2 Convert the Other Directory to Active Directory over LDAP or Active Directory over Integrated Windows Authentication.
- 3 Configure additional authentication methods for the directory, if necessary. The Password (cloud deployment) authentication method is available by default when you install and select the User Auth service in addition to the Directory Sync service.
- 4 Edit the default policy and any custom policies to use Password (cloud deployment) instead of Password (AirWatch Connector).
- 5 Stop user and group sync from Workspace ONE UEM to the Workspace ONE Access directory.

Important

- This feature is only applicable to directories that contain users synced from Active Directory. It is not applicable to directories that contain UEM Local Basic Users.
- This feature is not applicable to directories that contain users synced from LDAP directories such as OpenLDAP. It is only applicable to Active Directory over LDAP and Active Directory over Integrated Windows Authentication.

This chapter includes the following topics:

- [Convert Other Directory to Active Directory over LDAP or Active Directory over Integrated Windows Authentication](#)
- [Stop Directory Sync from Workspace ONE UEM to Workspace ONE Access](#)

Convert Other Directory to Active Directory over LDAP or Active Directory over Integrated Windows Authentication

In Workspace ONE Access, you can convert a directory of type Other, which stores users and groups synced from Workspace ONE UEM, to a directory of type Active Directory over LDAP or Active Directory over Integrated Windows Authentication, which are associated with the Workspace ONE Access connector. After you convert the directory, the Directory Sync service of the Workspace ONE Access connector is used instead of ACC to sync users and groups from your enterprise directory to the Workspace ONE Access service.

Prerequisites

- Install the Directory Sync service and the User Auth service, which are components of the Workspace ONE Access connector beginning with version 20.01.0.0. See the latest version of *Installing VMware Workspace ONE Access Connector* for information.

- The following Active Directory information is required:

- If you are converting to Active Directory over LDAP, the Base DN, and Bind user DN and password are required.

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

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

- If you are converting to Active Directory over Integrated Windows Authentication, the user name and password of the Bind user who has permission to query users and groups for the required domains is required.

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

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 Workspace ONE Access console, navigate to **Identity & Access Management > Manage > Directories**.
- 2 Click the directory that you want to convert.
- 3 In the directory page, click the **Convert** button.
- 4 In the Add Directory page, change the name of the directory if required and select the type of directory to which you want to convert the Other directory, **Active Directory over LDAP** or **Active Directory over Integrated Windows Authentication**.
- 5 Enter the Active Directory connection information and continue with the wizard to set up the directory.

The process is the same as creating a new directory. See [Configuring Active Directory Connection to the Workspace ONE Access Service](#) for detailed information.

Follow these guidelines while setting up the directory.

- In the **Directory Sync and Authentication** section, for **Directory Sync Hosts**, select the Directory Sync service that you installed.

All connector instances that have the Directory Sync service installed are listed. You can select multiple instances. Workspace ONE Access uses the first selected instance in the list to sync the directory. If the first instance is unavailable, it uses the next selected instance, and so on. You can reorder the list from the directory's Sync Settings page after creating the directory.

- For **Authentication**, select **Yes**. Also select the User Auth service instances to use for authentication.

- Ensure that you set up the converted directory identically to the Workspace ONE UEM directory so that it has the same directory structure. Select the same domains. When you specify users and groups to sync, make the same selections as the Workspace ONE UEM directory so that the same users and groups are synced to the converted directory.
- Ensure that you set the External ID to the same attribute that it is set to in Workspace ONE UEM.

6 On the last page of the wizard, click **Sync Directory**.

The directory is converted and set up to use the Directory Sync service to sync users and groups. If you set the Authentication option to Yes, an identity provider named **IDP for *directoryname*** and a Password (cloud deployment) authentication method are automatically created for the directory.

7 (Optional) To set up other authentication methods for the directory, navigate to the **Identity & Access Management > Manage > Connector Authentication Methods** page and create authentication methods for the directory.

See [Managing User Authentication Methods in Workspace ONE Access](#) for information.

8 Edit the default_access_policy_set and any custom policies to replace the Password (AirWatch Connector) authentication method with Password (cloud deployment).

- a Navigate to the **Identity & Access Management > Manage > Policies** tab.
- b Click **Edit Default Policy**, then click **Configuration** in the Edit Policy wizard.
- c Edit each policy rule and replace the **Password (AirWatch Connector)** authentication method with **Password (cloud deployment)**.
- d Click the **Policies** tab again and edit custom policies, if any, to replace the **Password (AirWatch Connector)** authentication method with **Password (cloud deployment)**.
- e (Optional) Modify policies to use additional authentication methods, as needed.

Important If you do not change Password (Airwatch Connector) to Password (cloud deployment) or another User Auth service authentication method, users of the converted directory will not be able to log in.

What to do next

Stop directory sync from Workspace ONE UEM to the converted directory.

Stop Directory Sync from Workspace ONE UEM to Workspace ONE Access

After you convert the Other directory to Active Directory over LDAP or Active Directory over Integrated Windows Authentication and associate it with the Workspace ONE Access Directory Sync service, the Directory Sync service is used to sync users and groups from your enterprise

directory to the converted directory. You must stop user and group sync from Workspace ONE UEM to the Workspace ONE Access directory.

Procedure

- 1 In the Workspace ONE UEM console, navigate to your Organization Group.
- 2 Navigate to the **Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager > Configuration** page.
- 3 Click the **Delete** button at the bottom of the page.

Results

The directory conversion is complete. Users and groups are now synced from your enterprise directory to the Workspace ONE Access service by the Directory Sync service. Users can continue to log in and access their applications.

Note The domain name displayed on the login page may be different after the directory is converted if the domain name is different from the domain NETBIOS name. With Workspace ONE UEM sync, the domain NETBIOS name is displayed. With Workspace ONE Access connector sync, the domain name is displayed.

Troubleshooting Workspace ONE Access Directory Integration

10

Use this information to troubleshoot Workspace ONE Access directory integration issues.

Identifying Domain Controller Latency in Windows Connectors

If end users are unable to log in with their Active Directory credentials and get an `Access Denied` error, or if login is very slow, follow these steps to determine whether domain controller network latency is causing the issue. Use the information that is applicable for your Workspace ONE Access connector version.

19.03 Connector

- 1 Check the connector log files `connector-dir-sync` and `connector`, which are available in the `INSTALL_DIR\VMware Identity Manager\Connector\opt\vmware\horizon\workspace\logs` folder.

Frequent "`Triggering forced windows DC discovery`" messages in these files indicate high latency with the listed domain controllers. If this message appears more than three times in an hour, check the network latency for domain controllers. You can set alerts based on connector logs.

- 2 Run the following commands from the connector server:

```
nltest /dsgetdc:domain /try_next_closest_site (gets the closest domain controller cached by the OS)
```

```
nltest /dsgetdc:domain /force (clears the OS cache and tries to determine the closest domain controller again)
```

The connector's Windows OS identifies the nearest domain controller for each domain used by the directory.

- 3 From the connector server, run the `ping` or `psping` command for each domain controller and check if the domain controller responds quickly. Less than 20 ms is a good response time for a `ping` request.
- 4 From the connector server, run the `tracert` command for each domain controller host for a domain and check the number of hops between the connector node and the domain controller host.

- 5 Follow the best practices for domain network latency described in [Best Practices to Avoid Network Latency](#) , if the domain controller is slow to respond.

20.01 and 20.10 Connectors

- 1 On the connector server, check the `krb5.conf` and `domain_krb.json` files, which contain the mapping of the domains to the current domain controllers used for each domain. For the Directory Sync service, the files are located in the `INSTALL_DIR\Workspace ONE Access\Directory Sync Service\conf` folder. For the User Auth service, the files are located in the `INSTALL_DIR\Workspace ONE Access\User Auth Service\conf` folder.

- 2 Run the following commands from the connector server:

```
nltest /dsgetdc:domain /try_next_closest_site (gets the closest domain controller cached by the OS)
```

```
nltest /dsgetdc:domain /force (clears the OS cache and tries to determine the closest domain controller again)
```

The connector's Windows OS identifies the nearest domain controller for each domain used by the directory.

- 3 From the connector server, run the `ping` or `psping` command from the connector server for each domain controller and check if the domain controller responds quickly. Less than 20 ms is a good response time for a `ping` request.
- 4 From the connector server, run the `tracert` command for each domain controller host for a domain and check the number of hops between the connector node and the domain controller host.
- 5 Follow the best practices for domain network latency described in [Best Practices to Avoid Network Latency](#) , if the domain controller is slow to respond.

21.08 Connector

- 1 Check the connector log files. For the Directory Sync service, check the `DirectorySyncService.out` and `eds-service.log` files, which are available in the `INSTALL_DIR\Workspace ONE Access\Directory Sync Service\logs` folder. For the User Auth service, check the `UserAuthService.out` and `eas-service.log` files, which are available in the `INSTALL_DIR\Workspace ONE Access\User Auth Service\logs` folder. Frequent "Triggering forced windows DC discovery" messages in these files indicate high latency with the listed domain controllers. If this message appears more than three times in an hour, check the network latency for domain controllers. You can set alerts based on connector logs.
- 2 On the connector server, check the `krb5.conf` and `domain_krb.json` files, which contain the mapping of the domains to the current domain controllers used for each domain. For the Directory Sync service, the files are located in the `INSTALL_DIR\Workspace ONE Access\Directory Sync Service\conf` folder. For the User Auth service, the files are located in the `INSTALL_DIR\Workspace ONE Access\User Auth Service\conf` folder.

- 3 Run the following commands from the connector server:

```
nlttest /dsgetdc:domain /try_next_closest_site (gets the closest domain controller cached by the OS)
```

```
nlttest /dsgetdc:domain /force (clears the OS cache and tries to determine the closest domain controller again)
```

The connector's Windows OS identifies the nearest domain controller for each domain used by the directory.

- 4 From the connector server, run the `ping` or `psping` command from the connector server for each domain controller and check if the domain controller responds quickly. Less than 20 ms is a good response time for a `ping` request.
- 5 From the connector server, run the `tracert` command for each domain controller host for a domain and check the number of hops between the connector node and the domain controller host.
- 6 Follow the best practices for domain network latency described in [Best Practices to Avoid Network Latency](#) , if the domain controller is slow to respond.