VMware AirWatch Directory Services Guide

Integrating your Directory Services

AirWatch v9.3

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Directory Services Overview

AirWatch integrates with your organization's existing directory service – such as Active Directory, Lotus Domino, and Novell e-Directory – to provide directory-based account access. This type of account access lets users authenticate with AirWatch apps and enroll devices using their existing directory service credentials.

Integrating with directory services eliminates the need to create basic user accounts in your organization. Such integration can also help simplify the enrollment process for end users by applying information they already know.

Ongoing LDAP synchronization detects any changes within the system. This synchronization performs necessary updates across all devices for affected users. In cases where administrative approval is required before changes occur, this synchronization obtains such approval.

> You may also migrate Basic Users to LDAP Users, checking against existing directory users. For more information, please see the **Migrating Basic users to Directory (AD) users** KB article: https://support.air-watch.com/solutions/1859.

Integrating AirWatch with your directory service provides many benefits.

- Conduct enrollment for both users and administrators.
- Map directory groups to AirWatch user groups.
- Control AirWatch Console access.
- Apply existing credentials for VMware Content Locker access.
- Assign apps, profiles, and policies by user group.
- Automatically retire end users when they go inactive.

The following sections explain how to integrate your AirWatch environment with your directory service of choice. Also, how to add directory user accounts to AirWatch and how to integrate user groups in AirWatch.

Requirements, Setup, and User Integration

Learn about which Lightweight Directory Access Protocol (LDAP)-based directory services you need, which ports to use, and what organization group to designate as the root. For more information, see Requirements for Directory Services on page 6.

The Directory Services page in system settings enables you to integrate AirWatch with your organization's domain controller. Security Assertion Markup Language (SAML) settings can also be configured on this page. For more information, see Directory Services Setup Overview on page 8.

Provide everyone in your organization with an AirWatch account (required if users intend to use an AirWatch managed device) by integrating your directory users. For more information, see Directory Service User Integration Overview on page 21.

Directory User Group Integrations

If you have user groups in your active directory structure, you can make the same user groups in AirWatch. Enable integrated updates so when you change your active directory user group assignments, those same changes get made in AirWatch. For more information, see Directory User Group Integration Overview on page 27.

Requirements for Directory Services

AirWatch supports integration with Lightweight Directory Access Protocol (LDAP)-based directory services.

- Microsoft Active Directory
- Lotus Domino
- Novell e-Directory

The default port for an unencrypted LDAP communication is 389. Software as a Service (SaaS) environments can use SSL encrypted traffic using port 636.

- Ensure the Directory Sync Service and the Scheduler Service are running on the same server, since they write to and read from the same queues.

You must designate an existing organization group (OG) as the primary root OG from which you manage devices and users.

Directory services (and VMware Enterprise Systems Connector when used) must be enabled in AirWatch at the level of this root OG.

Chapter 2:
Directory Services Setup

Directory Services Setup Overview

Directory services setup requires you to integrate your AirWatch environment with your directory service including attribute mapping for users and user groups.

Use the **Directory Services** page to configure the settings that let you integrate your AirWatch server with your domain controller (the server hosting your directory services).

Security Assertion Markup Language (SAML) settings can also be configured on this page.

After entering server settings, you can filter searches to identify users and groups. You can set options to auto merge and sync between your AirWatch configured groups and directory service groups. You can also map attribute values between AirWatch user attributes and your directory attributes.

> **Note:** For Software as a Service (SaaS) customers, directory services integration requires you to install the VMware Enterprise Systems Connector. For more information, see**VMware Enterprise Systems Connector Guide, available at https://www.vmware.com/support/pubs/workspaceone-pubs.html**.

Set up Directory Services with a Wizard

The AirWatch Console provides a simplified wizard to streamline the directory services setup process. The wizard includes steps to integrate either Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP) or both.

The wizard also automates the provisioning of AirWatch applications to VMware Identity Manager, greatly simplifying the process.

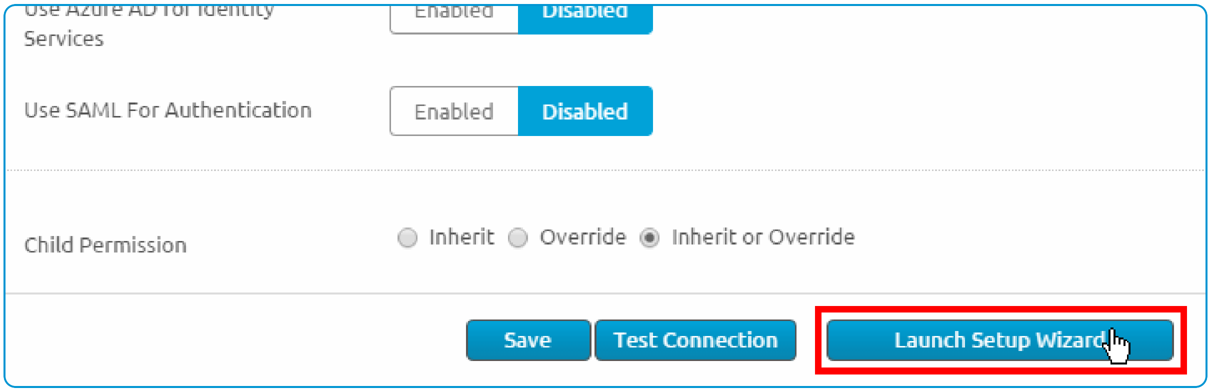
For more information about integrating AirWatch with Identity Manager and deploying Workspace ONE with single sign-on to devices, see the Workspace ONE Quick Start Guide, available at https://docs.vmware.com/en/VMware-Identity-Manager/3.2/ws1_quickconfiguration.pdf.

1. Access the directory services setup wizard from two places.

- The main AirWatch Console Getting Started Wizard.

  Or

- Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services** and select **Launch Setup Wizard**.



Use Azure AD For Identity Services: Enabled [✓ Disabled]

Use SAML For Authentication: Enabled [✓ Disabled]

Child Permission: ○ Inherit ○ Override ● Inherit or Override

2. Upon launching the wizard, select **Configure** to follow the steps. Alternately, you can **Skip wizard and configure manually** to configure settings on your own.

> **Note:** If SAML or LDAP settings are already configured on your directory services server, the AirWatch Console detects it automatically.

Set up Directory Services Manually

If you want to customize your directory service settings, you can skip the wizard and configure your settings manually.

1. Navigate to **Accounts > Administrators > Administrator Settings > Directory Services** and select the **Server** tab.
2. Enter your server information.

Setting	Description
LDAP	
Directory Type	Select the type of directory service that your organization uses. **Note:** AirWatch supports open source LDAP for directory services. For more information, see the following knowledgebase article: https://support.air-watch.com/resources/115001696028.
DNS SRV	Allow the Domain Name System Service Record to decide which server in its prioritized list of servers can best support LDAP requests. This feature ensures continuity of services in a high availability environment. The default setting is Disabled. With this option disabled, AirWatch uses your existing directory server, the address of which you enter in the Server setting. Supported DNS servers: • active directory integrated Microsoft DNS servers • standalone Microsoft DNS servers
Server	Enter the address of your directory server. This setting is only available when **Enable DNS SRV** is Disabled.
Encryption Type	Select the type of encryption to use for a directory services communication. The options available are **None** (unencrypted), **SSL**, and **Start TLS**.

Setting	Description
Port	Enter the Transmission Control Protocol (TCP) port used to communicate with the domain controller. The default for unencrypted LDAP directory service communication is port 389. Only SaaS environments allow SSL encrypted traffic using port 636. To view a KnowledgeBase article that lists the most up-to-date AirWatch SaaS data center IP ranges, refer to https://support.air-watch.com/articles/115001662168. - When you change the **Encryption Type** setting to **SSL**, the **Port** setting automatically changes to 636. - When you select the **Add Domain** button, the **Port** setting automatically changes to 3268.
Verify SSL Certificate	This setting is only available when the **Encryption Type** is **SSL** or **Start TLS**. Receive SSL errors by selecting the SSL check box.
Protocol Version	Select the version of the Lightweight Directory Access Protocol (LDAP) that is in use. Active Directory uses LDAP versions 2 or 3. If you are unsure of which Protocol Version to use, try the commonly used value of '3'.
Use Service Account Credentials	Use the App pool credentials from the server on which the VMware Enterprise Systems Connector is installed for authenticating with the domain controller. Enabling this option hides the **Bind user name** and **Bind Password** settings.
Bind Authentication Type	Select the type of bind authentication to enable the AirWatch server to communicate with the domain controller. You can select **Anonymous**, **Basic**, **Digest**, **Kerberos**, **NTLM**, or **GSS-NEGOTIATE**. If you are unsure of which Bind Authentication Type to use, try the commonly used GSS-NEGOTIATE. You will know if your selection is not correct when you click **Test Connection**.
Bind user name	Enter the credentials used to authenticate with the domain controller. This account (which the entered user name identifies) allows a read-access permission on your directory server and binds the connection when authenticating users. Clear the bind password from the database by selecting the **Clear Bind Password** check box.
Domain /Server	Enter the default domain and server name for any directory-based user accounts. If only one domain is used for all directory user accounts, fill in the text box with the domain. This entry means that users are authenticated without explicitly stating their domain. **Note:** You can add more domains by selecting the **Add Domain** option. In this case, AirWatch automatically changes the port setting to 3268 for global catalog. You may choose to change the port setting to 3269 for SSL encrypted traffic, or override it completely by entering a separate port.
Is there a trust relationship between all domains?	This setting is available only when you have more than one domain added. Select **Yes** if the binding account has permission to access other domains you have added. This added permission means that the binding account can successfully log in from more domains.

The following options are available after selecting the **Advanced** section drop-down.

Setting	Description
Advanced	
Search Subdomains	Enable subdomain searching to find nested users. Leaving this option disabled can make searches faster and avoids network issues. However, users and groups located in subdomains under the base Domain Name (DN) are not identified.
Connection Timeout	Enter the LDAP connection timeout value (in seconds).
Request Timeout	Enter the LDAP query request timeout value (in seconds).
Search without base DN	Enable this option when using a global catalog and when you do not want to require a base DN to search for users and groups.
Use Recursive OID at Enrollment	Verify user group membership at the time of enrollment. As the system runs this feature at enrollment time, your performance may decrease with some directories.
Use Recursive OID For Group Sync	Verify user group membership at the time of Group synchronization.
Object Identifier Data Type	Select the unique identifier that never changes for a user or group. The options available are **Binary** and **String**. Typically, the Object Identifier is in a **Binary** format.
Sort Control	Option to enable sorting. If this option is disabled, it can make searches faster and you can avoid sync timeouts.

3. The following settings are available after enabling **Use Azure AD for Identity Services** and are only applicable if you are integrating with Azure Active Directory.

   Azure AD integration with AirWatch must be configured at the tenant where Active Directory (such as LDAP) is configured.

Setting	Description
AZURE ACTIVE DIRECTORY	
MDM Enrollment URL	Enter the URL address used to enroll devices.
MDM Terms of Use URL	Enter the URL address of your terms of use agreement. There is a helpful link that displays exactly where in the AirWatch in Azure AD config panel these MDM URLs belong. This link is labeled, "Where in AAD do I paste this info?"
Tenant Identifier	Enter the identification number used to authenticate your Azure AD license. The Azure **Tenant Identifier** is found in your Azure AD Directory Instance URL. For example, if your URL is acme.com/WS/ADExt/Dir/0a12bc34-56d7-93f1-g2h3-i4-jk56lm78n, only the last section (0a12bc34-56d7-93f1-g2h3-i4-jk56lm78n) is your **Tenant Identifier**.

Setting	Description
Tenant Name	Enter the tenant name of your Azure AD instance. There is a helpful link that displays exactly how to obtain the tenant info from your AAD Directory Instance. This link is labeled, "How To Obtain Tenant Info"
Immutable ID Mapping Attribute	The Immutable ID Mapping Attribute points to the sourceAnchor field in Active Directory that is mapped to Azure AD. This enables AirWatch to match the Azure AD immutable ID to the correct local active directory attribute.
Mapping Attribute Data Type	Choose the mapping attribute data type of the field used by AirWatch as the sourceAnchor for Azure AD. The default type is Binary.

4. The following Security Assertion Markup Language (SAML) options are available after enabling **Use SAML for Authentication**. These options are only applicable if you are integrating with a SAML identity provider.

Setting	Description
Enable SAML authentication for	You have the choice of using SAML authentication for **Admins**, **Users**, or **Both**.
Use new SAML Authentication endpoint	A new SAML authentication endpoint has been created for end-user authentication (device enrollment and login to SSP). This authentication replaces the two dedicated enrollment and SSP endpoints with a single endpoint. While you may choose to keep your existing settings, AirWatch suggests updating your SAML settings to take advantage of the new combined endpoint. If you want to use the new endpoint, enable this setting and save the page. Then use the **Export Service Provider Settings** to export the new metadata file and upload it to your IdP. Doing so establishes trust between the new endpoint and your IdP.
SAML 2.0	
Import Identity Provider Settings	Upload a metadata file obtained from the identity provider. This file must be in Extensible Markup Language (XML) format.
Service Provider (AirWatch) ID	Enter the Uniform Resource Identifier (URI) with which AirWatch identifies itself to the identity provider. This string must match the ID that has been established as trusted by the identity provider.
Identity Provider ID	Enter the URI that the identity provider uses to identify itself. AirWatch checks authentication responses to verify that the identity matches the ID provided here.
REQUEST	
Request Binding Type	Select the binding types of the request. The options include **Redirect**, **POST**, and **Artifact**.
Identify Provider Single Sign On URL	Enter the identity provider's Uniform Resource Locator (URL) that AirWatch uses to send requests.

Setting	Description
NameID Format	Enter the format in which the identity provider sends a NameID for an authenticated user. This value is not required as AirWatch obtains the user name from the FriendlyName "uid" required attribute.
Authentication Request Security	Select from the dropdown whether or not the Service Provider (AirWatch) signs the authentication requests. You can select **None**, **Sign Authentication Requests (SHA1)**, and **Sign Authentication Requests (SHA256)**. Consider selecting Sign Authentication Requests (SHA256) for a more secure authentication.
RESPONSE	
Response Binding Type	Select the binding types of the response. The options include **Redirect**, **POST**, and **Artifact**.
Sp Assertion URL	Enter the AirWatch URL that the identity provider configures to direct its authentication responses. "Assertions" regarding the authenticated user are included in success responses from the identity provider.
Authentication Response Security	This value specifies whether the IdP signs the response. You can select between **None**, **Validate Response Signatures**, and **Validate Assertions Signatures**. Consider selecting Validate Response Signatures for a more secure authentication.
CERTIFICATE	
Identity Provider Certificate	Upload the identity provider certificate.
Service Provider (AirWatch) Certificate	Upload the service provider certificate.
Export Service Provider Settings button	Exports the metadata file for uploading to your Identity Provider (IdP). This setting establishes trust between the new SAML endpoint (for enrollment and SSP login) and your IdP.

5. Verify that you have established proper connectivity by selecting the **Test Connection** button.

6. Select **Save**.

VMware Identity Manager and Directory Services

After configuring directory integration settings between your AirWatch instance and VMware Identity Manager, your end users must sign in only once using Workspace ONE. Single sign-on enables access to all your organization's available apps without the need to sign in each time.

VMware Identity Manager together with AirWatch enables you to consolidate a list of your organization's suggested Web apps and native mobile apps in unified application catalogs. This functionality does not allow for AirWatch to receive directory changes from Identity Manager.

For more information about integrating AirWatch with Identity Manager and deploying Workspace ONE with single sign-on to devices, see the Workspace ONE Quick Start Guide, available at https://docs.vmware.com/en/VMware-Identity-Manager/3.2/ws1_quickconfiguration.pdf.

Requirements

Before you can integrate directory services with VMware Identity manager, complete the following:

- Set up and configure VMware Enterprise Systems with your AirWatch environment.
- Set up and configure Directory service integration for the selected organization group and not inheriting settings from a parent organization group.
- Accept the End User License Agreement (EULA) found in the VMware Identity Manager console. This EULA displays when you first open the console.

Synchronization Between AirWatch and VMware Identity Manager

Synchronization of directory information between AirWatch and VMware Identity Manager occurs on the same schedule as the AirWatch directory sync. Users are also synced to VMware Identity Manager immediately when added by an administrator manually or from a bulk import.

Also, the integration with VMware Identity Manager supports Just-in-Time provisioning (JIT). Users with directory accounts have their accounts synced to VMware Identity Manager the first time they log in using an enrollment or self-service portal. Manual synchronization is not required to add a single user to VMware Identity Manager immediately.

Integrate VMware Identity Manager with Directory Services

VMware Identity Manager together with AirWatch enable you to consolidate a list of your organization's suggested Web apps and native mobile apps in unified application catalogs. This functionality does not allow for AirWatch to receive directory changes from Identity Manager. Use the following instructions to configure server-related settings.

For more information about integrating AirWatch with Identity Manager and deploying Workspace ONE with single sign-on to devices, see the Workspace ONE Quick Start Guide, available at https://docs.vmware.com/en/VMware-Identity-Manager/3.2/ws1_quickconfiguration.pdf.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager>Configuration**.
2. Enter your server information.

Setting	Description
URL	Bind to AirWatch by entering the URL of your VMware Identity Manager tenant. A valid license for VMware Identity Manager is required.
Admin user name	Enter the administrator user name, which is case-sensitive.
Admin Password	Enter the administrator password, which is case-sensitive.

3. Verify that you have established proper connectivity by selecting the **Test Connection** button.
4. Click **Next** to save your selections and proceed to the next configuration screen.

Setting	Description
Directory	AirWatch imports the directory name based on your existing directory in AirWatch. Enter the same directory name as used by VMware Identity Manager.
Enable Custom Mapping	Enable custom mapping as applicable to map the directory integration in AirWatch to VMware Identity Manager so they are in sync. Most directory service configurations use **Standard** mapping. **Custom** mapping attributes are for customers who have a non-standard directory service database value mapping or an otherwise customized configuration between a directory service and AirWatch.
MAPPING ATTRIBUTES	
ExternalID	Identifies the source of a user, in case multiple users have the same user name.
Password	Directory services user's password.
UserStore	The name of the user store to which a user belongs.
Disabled	Indicates whether the directory account is disabled.
DistinguishedName	Select the distinguished name for the directory services user from the drop-down listing.
Domain	Select the domain name from the drop-down listing.
Email*	Directory service user's email address. The email address mapped according to this attribute must be the same email which was used in the original configuration between directory services and AirWatch. Otherwise this setting, and by extension the user's entire account, syncs incorrectly.
EmployeeID	Select the employee ID from the drop-down listing.
First name*	Directory service user's first name.
Last name*	Directory service user's last name.
Phone	Phone number of the directory service user.
Roles	Default role of the directory service user.
User name*	User name associated with the directory services.
UserPrincipalName	Select the principal user name for the Directory services user from the drop-down listing.

* Required settings for both Standard and Custom attribute mapping.

Note: The mapping attribute settings presented here are default settings. You can add more attributes.

5. Click the **Save** button to save your configuration and refresh the page. You can view all the details in the **Summary** page.

6. Initiate a synchronization of the structures within your directory services and VMware Identity Management by selecting the **Sync Now** button.

Enable and Export AirWatch Certificate Authority

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

Use the following instructions to enable and export the AirWatch Certificate Authority:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager>Configuration**.

   > **Note**: To enable AirWatch Certificate Authority, the organization group type must be Customer. To view or change the group type, navigate to Groups & Settings, Groups > Organization Groups> Organization Group Details.

2. In the Certificate section, click **Enable**.The section displays the issuer root certificate details.
3. Click **Export** and save the file.

Manage the VMware Identity Manager Integration Configuration

After you bind your directory settings between AirWatch and Identity Manager, you can perform some management actions on the settings page.

Navigate to**Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager>Configuration**.

- Edit the VMware Identity Management for Directory Services configuration by selecting the **Edit** button.
- Delete the configuration by selecting the **Delete** button.
- Initiate a synchronization of the structures within your directory services and VMware Identity Management by selecting the **Sync Now** button.

Map Directory Services User Information

After entering server settings, you can filter searches to identify users and map values between AirWatch user attributes and your directory attributes.

Use the following instructions to configure user-related settings.

1. Navigate to **Accounts > Administrators > Administrator Settings > Directory Services**.
2. Select the **User** tab. By default, only the **Base DN** information displays.
3. **Base DN** – Select the **Fetch DN** plus sign (+) next to the **Base DN** column. This plus sign displays a list of Base DNs from which you can select to populate this text box. If it does not, revisit the settings you entered on the **Server** tab before continuing.

4. Enter data in the following settings.

Setting	Description
User Object Class	Enter the appropriate Object Class. In most cases, this value is "user."
User Search Filter	Enter the search parameter used to associate user accounts with Active Directory accounts. The suggested format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user. • For AD servers, use "(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))" exactly. • For other LDAP servers, use "CN={EnrollmentUser}" or "UID={EnrollmentUser}"

5. Display more settings by selecting **Show Advanced**.

Setting	Description
Auto Merge	Enable setting to allow user group updates from your directory service to merge with the associated users and groups in AirWatch automatically.
Automatically Set Disabled Users to Inactive	Select Enable to deactivate the associated user in AirWatch when that user is disabled in your LDAP directory service (for example, Novell e-Directory). • **Value For Disabled Status** – Enter a numeric value and select the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user’s status. Select “Flag Bit Match” if the user status is designated by a bitwise flag (which is the default for Active Directory). When “Flag Bit Match” is selected, if any bits from the property match the entered numeric value, then directory service considers the user to be disabled. This setting is only visible when the option **Automatically Set Disabled Users to Inactive** is checked. **Note:** If you select this option, then AirWatch administrators set as inactive in your directory service are not able to log in to the AirWatch Console. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.
Enable Custom Attributes	Enable custom attributes. **Custom Attributes** is a section that appears under the main **Attribute – Mapping Value** table. You must scroll down to the bottom of the page to see the Custom Attributes.
Attributes	Review and edit the **Mapping Values** for the listed **Attributes**, if necessary. These columns show the mapping between AirWatch user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in Active Directory (AD). Update these mapping values to reflect the values used for your own or other directory service types. If you add or remove a custom attribute, you should initiate a manual sync afterward by selecting the **Sync Attributes** button.

Setting	Description
Sync Attributes button	Manually sync the attributes mapped here to the user records in AirWatch. Attributes sync automatically on the time schedule configured for the AirWatch environment.

Map Directory Services Group Information

After entering server settings, you can filter searches to identify user groups. You can also set options to auto merge and sync changes between your AirWatch groups and directory service groups.

Use the following instructions to configure user group-related settings.

1. Navigate to **Accounts > Administrators > Administrator Settings > Directory Services**.
2. Select the **Group** tab. By default, only the **Base DN** information displays.
3. **Base DN** – Select the **Fetch DN** plus sign (+) next to the **Base DN** setting to display a list of Base DNs. Populate this text box by selecting from the list. If a list of Base DNs does not display, revisit the settings you entered on the **Server** tab before continuing.
4. Enter data in the following settings.

Setting	Description
Group Object Class	Enter the appropriate Object Class. In most cases this value should be **group**.
Organizational Unit Object Class	Enter the appropriate Organizational User Object Class.

5. To display more settings, select **Advanced**. Enter data in the following text boxes.

Setting	Description
Group Search Filter	Enter the search parameter used to associate user groups with directory service accounts.
Auto Sync Default	Select this checkbox to automatically add or remove users in AirWatch configured user groups based on their membership in your directory service.
Auto Merge Default	Select this check box to automatically apply sync changes without administrative approval.
Maximum Allowable Changes	Enter the number of maximum allowable group membership changes to be merged into AirWatch. Any number of changes detected upon syncing with the directory service database under this number are automatically merged. If the number of changes exceed this threshold, an administrator must manually approve the changes before they are applied. A single change is defined by a user either leaving or joining a group. A setting of 100 Maximum Allowable Changes means the Console does not need to sync with your directory service as much.

Setting	Description
Conditional Group Sync	Enable this option to sync group attributes only after changes occur in Active Directory. Disable this option to sync group attributes regularly, regardless of changes in Active Directory.
Auto-Update Friendly Name	When enabled, the friendly name is updated with group name changes made in active directory. When disabled, the friendly name can be customized so admins can tell the difference between user groups with identical common names. This can be useful if your implementation includes organizational unit (OU)-based user groups with the same common name.
Attribute	Review and edit the **Mapping Value** for the listed **Attribute**, if necessary. These columns show the mapping between AirWatch user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in AD. Update these mapping values to reflect the values used for your own or other directory service types.

Note: No AD passwords are stored in the AirWatch database except the Bind account password used to link directory services into your AirWatch environment. The Bind account password is stored in an encrypted form in the database and is not accessible from the console.
Unique session keys are used for each sync connection to the Active Directory server.

Note: In some instances, global catalogs are used to manage multiple domains or AD Forests. Delays while searching for or authenticating users may be due to a complex directory structure. You can integrate directly with the global catalog to query multiple forests using one Lightweight Directory Access Protocol (LDAP) endpoint for better results.

To integrate with the global catalog directly, configure the following settings:

- **Encryption Type** = None
- **Port** = 3268
- Verify that your firewall allows for this traffic on port 3268.

Chapter 3:
Directory User Integration

Directory Service User Integration Overview

Every directory user you want to manage through AirWatch Mobile Device Management (MDM) must have a corresponding user account in the AirWatch Console.

You can directly add your existing directory services users to AirWatch using one of the following methods.

- Batch upload a file containing all your directory services users. The act of batch importing automatically creates a user account.
- Create an AirWatch user accounts one at a time by entering the directory user name and selecting **Check User** to auto-populate remaining details.
- Do not import in bulk nor manually create user accounts and instead allow all directory users to self-enroll at enrollment time.

A fourth option, applying AirWatch user groups linked to directory service groups, is explained in the next section. This option can be used with these methods or by itself.

> **Note:** For information about how these methods affect various directory services enrollment options, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Managing Directory Service Users in AirWatch

If you choose to use directory services in AirWatch, note the following.

- Directory users can only be created at the same level as the organization group (OG) where directory services settings are enabled. You can see users at the organization group level where they have a device enrolled. However, users can only be managed at the same level as the directory service settings.
- To delete or edit a user account, you must be at the same level as the directory services settings.
- To add a device to an existing AirWatch user account, you must be at a lower level than the root OG where directory services are enabled.

Adding Directory Users Into AirWatch

You can add directory users into AirWatch one at a time or use a batch import process. Adding individual directory users one at a time is ideal for when you have a few users to add. It is preferable to batch import directory users when you have multiple users to add.

Using the batch import method means uploading a list of directory services users in a CSV (comma-separated values) template file, which has specific columns. To make converting your existing directory service user data easier, consider mapping the text boxes AirWatch requires to existing attributes in your database. You can then use custom queries to create a spreadsheet which you can copy and paste.

- **Pros** – This option creates AirWatch user accounts, which enable you to use enrollment options that require user accounts, such as registration tokens. If you have users not included in Mobile Device Management (MDM), you can omit them from the CSV file. Such omission restricts an enrollment to only known users.
- **Cons** – Back-end configuration is required to automate the creation of a CSV batch file that can be used to upload

users. The alternative is to enter each user manually. Manual entry means that user assignment to organization groups must be thought out beforehand to ensure proper profile, policy, content, and app assignments.

Add Individual Directory Users One at a Time

AirWatch enables you to add directory users in small numbers or if you have a 'one-off' addition to make.

1. Navigate to **Accounts > Users > List View** and select **Add** and then **Add User**. The **Add / Edit User** page displays.
2. In the **General** tab, complete the following settings to add a directory user.

Setting	Description
Security Type	Add an Active Directory user by choosing **Directory** as the Security Type.
Directory Name	This pre-populated setting identifies the Active Directory name.
Domain	Choose the domain name from the drop-down menu.
User name	Enter the user's directory user name and select **Check User**. If the system finds a match, the user's information is automatically populated. The remaining settings in this section are only available after you have successfully located an active directory user with the **Check User** button.
Full Name	Use **Edit Attributes** to allow any option that syncs a blank value from the directory to be edited. Edit Attributes also enables you to populate matching user's information automatically. If a setting syncs an actual value from the directory, then that setting must be edited in the directory itself. The change takes effect on the next directory sync. Complete any blank option returned from the directory in **Full Name** and select **Edit Attributes** to save the addition.
Display Name	Enter the name that displays in the admin console.
Email Address	Enter or edit the user's email address.
Email user name	Enter or edit the user's email user name.
Domain (email)	Select the email domain from the drop-down menu.
Phone Number	Enter the user's phone number including plus sign, country code, and area code. If you intend to use SMS to send notifications, the phone number is required.
Enrollment	
Enrollment Organization Group	Select the organization group into which the user enrolls.

Setting	Description
Allow the user to enroll into additional Organization Groups	Choose whether or not to allow the user to enroll into more than one organization group. If you select **Enabled**, then complete the **Additional Organization Groups**.
User Role	Select the role for the user you are adding from this drop-down menu.
Notification	
Message Type	Choose the type of message you may send to the user, **Email**, **SMS**, or **None**. Selecting SMS requires a valid entry in the **Phone Number** text box.
Message Template	Choose the template for email or SMS messages from this drop-down setting. Optionally, select the **Message Preview** to preview the template and select the **Configure Message Templates** link to create a template.

3. You may optionally select the **Advanced** tab and complete the following settings.

Setting	Description
Advanced Info Section	
Email Password	Enter the email password of the user you are adding.
Confirm Email Password	Confirm the email password of the user you are adding.
Distinguished Name	For directory users recognized by VMware AirWatch, this text box is pre-populated with the distinguished name of the user. Distinguished Name is a string representing the user name and all authorization codes associated with an Active Directory user.
Manager Distinguished Name	Enter the distinguished name of the user's manager. This text box is optional.
Category	Choose the user category for the user being added.
Department	Enter the user's department for your company's administrative purposes.
Employee ID	Enter the user's employee ID for your company's administrative purposes.
Cost Center	Enter the user's cost center for your company's administrative purposes.
Custom Attribute 1–5 (for Directory users only)	Enter your previously configured custom attributes, where applicable. You may define these custom attributes by navigating to **Groups & Settings > All Settings > Devices & Users > Advanced > Custom Attributes**. **Note:** Custom attributes can be configured only at Customer organization groups.

Setting	Description
Certificates Section	
Use S/MIME	Enable or disable the use of Secure/Multipurpose Internet Mail Extensions (S/MIME). If enabled, you must have an S/MIME-enabled profile and you must upload an S/MIME certificate by selecting **Upload**.
Separate Encryption Certificate	Enable or disable the use of a separate encryption certificate. If enabled, you must upload an encryption certificate using **Upload**. Generally, the same S/MIME certificate is used for signing and encryption, unless a different certificate is expressly being used.
Old Encryption Certificate	Enable or disable a legacy version encryption certificate. If enabled, you must **Upload** an encryption certificate.
Staging Section	
Enable Device Staging	Enable or disable the staging of devices. If enabled, you must choose between **Single User Devices** and **Multi User Devices**. If **Single User Devices**, you must select between **Standard**, where users themselves log in and **Advanced**, where a device is enrolled on behalf of another user.

4. Select **Save** to save only the new user or select **Save and Add Device** to save the new user and proceed to the **Add Device** page.

Batch Import Directory Users

If you have many directory users to add to AirWatch, you can save time by initiating a batch import process.

1. Navigate to **Accounts > Users > Batch Status** or **Devices > Lifecycle > Enrollment Status > Add** and select **Batch Import**.
2. Enter the basic information including a **Batch Name** and **Batch Description** in the AirWatch Console.
3. Select the applicable batch type from the **Batch Type** drop-down menu.
4. Select and download the template that best matches the kind of batch import you are making.

   Blacklisted Devices – Import a list of known, non-compliant devices by IMEI, Serial Number, or UDID. Blacklisted devices are not allowed to enroll. If a blacklisted device attempts to enroll, it is automatically blocked.

   Whitelisted Devices – Import pre-approved devices by IMEI, Serial Number, or UDID. Use this import a list of known, trusted devices. The ownership and group ID associated to this device is automatically applied to the device during enrollment.

   User / Device – Choose between a **Simple** and an **Advanced** CSV template. The simple template features only the most often-used options and the Advanced template features the full, unabridged compliment of options.
5. Open the CSV file, which consists of a CSV (comma-separated values) file that is populated with a single row completed with a sample device data. The CSV file features several columns corresponding to the setting that display on the Add / Edit User page. The **GroupID** column corresponds to the **Enrollment Organization Group** setting on the **Add / Edit User** page.

   You can confirm whether or not users are part of the enrollment organization group (OG).

   a. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and check the **Grouping** tab.

   b. If the **Group ID Assignment Mode** is set to **Default**, then your users are part of the enrollment OG.

   c. For a directory-based enrollment, the **Security Type** for each user must be **Directory**.

6. Enter data for your organization's users, including device information (if applicable) and save the file.

7. Return to the Batch Import page and select **Choose File** to locate and upload the CSV file that you had previously downloaded and filled out.

8. Select **Save**.

The user account and device details, if included, are added to the AirWatch Console. From here, you can send your users an enrollment message. This enrollment message prompts them to initiate enrollment or supplies registration tokens for simplified single-click or dual-factor enrollment.

For more information about these options, refer to "Device Enrollment" in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Directory Service User Self-Enrollment

User Self-Enrollment applies your existing directory service environment to auto discover users based on their email.

There are other considerations.

- **Pros** – Requires the least amount of effort while still supporting the ability to sync changes to user attributes that are made in your directory service. Self-enrollment also creates an AirWatch user account.

- **Cons** – Does not allow you to restrict the enrollment to specific users or user groups. This lack of restriction means that any directory user with a valid email address can enroll a device.

Enable All Directory Users to Self-Enroll

You can enable all your directory users to enroll themselves based on their email addresses. This option requires the least amount of effort while retaining the ability to sync user attributes. However, you are unable to restrict the enrollment to specific users or user groups.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Restrictions** tab.

2. Scroll to the **Enrollment Restrictions** section of this page. Ensure that **Restrict Enrollment To Known Users** and **Restrict Enrollment To Configured Groups** check boxes are both *deselected*.

   When deselected, all directory users and user groups members (as configured in the directory services settings page) are allowed to enroll with a valid email address.

Note: For additional information about enrolling with directory services integration, refer to "Device Enrollment" in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Chapter 4:
Directory User Group Integration

Directory User Group Integration Overview

An alternative to custom user groups without active directory integration is through user group integration that applies your existing active directory structure, providing many benefits.

Once you import existing directory service user groups as AirWatch user groups, you can perform the following.

- **User Management** – Reference your existing directory service groups (such as security groups or distribution lists) and align user management in AirWatch with the existing organizational systems.
- **Profiles and Policies** – Assign profiles, applications, and policies across an AirWatch deployment to groups of users.
- **Integrated Updates** – Automatically update user group assignments based on group membership changes.
- **Management Permissions** – Set management permissions to allow only approved administrators to change policy and profile assignments for certain user groups.
- **Enrollment** – Allow users to enroll with existing credentials and automatically assign an organization group.

Organization Groups vs. User Groups

Organization groups (OG) are still the primary means of performing the following tasks in AirWatch. User groups do not replace organization groups in AirWatch, rather, they are used to represent security groups and business roles.

Organization Groups

- The primary difference between organization groups and user groups is that devices are always tied to an OG.
- You set the administration management permissions in the AirWatch Console through an organization group.
- Profiles, policies, and applications are assigned to organization groups.
  - Even though it is possible to assign these resources to user groups, user groups only act as an extra filter on top of organization groups.
- Tracking assets on AirWatch dashboards. Organization groups are still the primary filter on all console pages for all dashboards and views. OGs define at which business units the devices live, so consider the device groupings you want to view on the AirWatch dashboards.
- Configuring system config settings. System settings are tied to organization groups. If you need different system settings, then you must define different organization groups. Examples of important settings to consider include the following.
  - Enrollment Settings and Restrictions
  - Terms of Use
  - Privacy Policies

Existing MDM assignments are not affected once you import user groups. Facilitate the transition process and ensure that users do not experience any disruption to their current configurations by applying policies to user groups *manually* as needed.

User Groups

- Use user groups to represent security groups or business roles within your organization.
- Users can belong to multiple user groups, but devices still belong to only one organization group.
- AirWatch currently supports the assignment of profiles, policies, and internal apps to user groups.

Transition Options for Best Practices

When defining OGs to represent user groups, one of the following options may help you reconfigure your OG and user group structure to be more streamlined.

- Reconfigure your system to associate profiles, applications, and enrollment restrictions with user groups.
    - Assign each profile, app, and enrollment restriction to the appropriate user groups.
    - Change the organization group assignment to one organization group up.
    - Add a user group assignment.
- You may choose to reconfigure your hierarchy to remove old or unused organization groups.
    - Move up devices one organization group (from child to parent).
    - Delete old organization groups.
- You can choose to leave your structure as-is.
    - At this point, the organization group can be considered the “Primary Security Group” of the device.
    - The user groups are used for assigning profiles and policies.
    - The old, unused organization groups can remain for asset tracking purposes.

Adding Directory Service User Groups to AirWatch

You can add directory service user groups into AirWatch one at a time or use a batch import process. Adding directory user groups one at a time is ideal for when you have a limited number of groups to add. It is preferable to batch import directory user groups when you have multiple groups to add.

Using the batch import method means uploading a list of your existing directory service groups in a .csv (comma-separated values) template file. This method does not immediately create AirWatch user accounts for each of your directory service accounts. However, it ensures AirWatch recognizes them as belonging to a configured group. You can then use this recognition as a means of restricting who can enroll.

User groups in AirWatch can be synced – automatically when configured with a scheduler – with your directory service groups to merge changes or add missing users.

- **Pros** – You have the option of restricting an enrollment to only known groups, which lets you restrict on a user group level who can enroll. This method also keeps your existing directory service group infrastructure and allows you to assign profiles, policies, content, and apps based on these existing group setups.

- **Cons** – Uploading directory service user groups does not automatically create AirWatch user accounts. If you have restricted enrollment for known users, you must add those user accounts into the AirWatch Console manually.

Add Directory User Groups One at a Time

If you have just a few user groups to add to AirWatch, then take the following steps to add a directory service user group.

1. Navigate to **Accounts > User Groups > List View**, select **Add**, then **Add User Group**.
2. Complete the settings in the **Add User Group** screen as applicable, ensuring the user group **Type** is **Directory**.

Setting	Description
Type	Select the type of User Group. • **Directory** – Create a user group that is aligned with your existing active directory structure. • **Custom** – Create a user group outside of your organization's existing Active Directory structure. This user group type grants access to features and content for basic and directory users to customize user groups according to your deployment. Custom user groups can only be added at a customer level organization group.
External Type	Select the external type of group you are adding. • **Group** – Refers to the group object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. • **Organizational Unit** – Refers to the organizational unit object class on which your user group is based. Customize this class by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services > Group**. • **Custom Query** – You can also create a user group containing users you locate by running a custom query. Selecting this external type replaces the Search Text function but displays the Custom Query section.
Search Text	Identify the name of a user group in your directory by entering the search criteria and selecting **Search** to search for it. If a directory group contains your search text, a list of group names displays. This option is unavailable when **External Type** is set to **Custom Query**.
Directory Name	Read-only setting displaying the address of your directory services server.
Domain and **Group Base DN**	This information automatically populates based on the directory services server information you enter on the **Directory Services** page (**Groups & Settings > System > Enterprise Integration > Directory Services**). Select the **Fetch DN** plus sign (+) next to the **Group Base DN** setting, which displays a list of distinguished name elements from which you can select.

Setting	Description
Custom Object Class	Identifies the object class under which your query runs. The default object class is 'person' but you can supply a custom object class to identify your users with a greater success and accuracy. This option is available only when **Custom Query** is selected as **External Type**.
Group Name	Select a **Group Name** from your **Search Text** results list. Selecting a group name automatically alters the value in the Distinguished Name setting. This option is available only after you have completed a successful search with the **Search Text** setting.
Distinguished Name	This read-only setting displays the full distinguished name of the group you are creating. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Base DN	Identifies the base distinguished name which serves as the starting point of your query. The default base distinguished name is 'AirWatch' and 'sso'. However, if you want to run the query with a different starting point, you can supply a custom base distinguished name. This option is available only when **Custom Query** is selected as **External Type**.
Organization Group Assignment	This optional setting enables you to assign the user group you are creating to a specific organization group. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
User Group Settings	Choose between **Apply default settings** and **Use Custom settings for this user group**. See the **Custom Settings** section for additional setting descriptions. You can configure this option from the permission settings after the group is created. This option is available only when **Group** or **Organizational Unit** is selected as **External Type**.
Custom Query	
Query	This setting displays the currently loaded query that runs when you select the **Test Query** button and when you select the **Continue** button. Changes you make to the **Custom Logic** setting or the **Custom Object Class** setting are reflected here.
Custom Logic	Add your custom query logic here, such as user name or admin name. For example, "cn=jsmith". You can include as much or as little of the distinguished name as you like. The **Test Query** button allows you to see if the syntax of your query is correct before selecting the **Continue** button.
Custom Settings	
Management Permissions	You can allow or disallow all administrators to manage the user group you are creating.
Default Role	Choose a default role for the user group from the drop-down menu.
Default Enrollment Policy	Choose a default enrollment policy from the drop-down menu.

Setting	Description
Auto Sync with Directory	This option enables the directory sync, which detects user membership from the directory server and stores it in a temporary table. Administrators approve changes to the console unless the Auto Merge option is checked. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Auto Merge Changes	Enable this option to apply sync changes automatically from the database without administrative approval.
Maximum Allowable Changes	Use this setting to set a threshold for the number of automatic user group sync changes that are allowed to occur before approval must be given. Changes more than the threshold are in need of admin approval and a notification is sent to this effect. This option is available only when **Auto Merge Changes** is enabled.
Add Group Members Automatically	Enable this setting to add users to the user group automatically. If you want to prevent user groups from automatically syncing during a scheduled sync, this setting must be disabled.
Send Email to User when Adding Missing Users	You can send an email to users while adding missing users. Adding missing users means combining the temporary user group table with the Active Directory table.
Message Template	Choose a message template to be used for the email notification during the addition of missing users to the user group. This option is available only when **Send Email to User when Adding Missing Users** is enabled.

For more information on Distinguished Name, search for Microsoft's TechNet article entitled "Object Naming" at https://technet.microsoft.com.

3. Select **Save**.

Batch Import Directory User Groups

If you have many directory service user groups to add to AirWatch, you can save time by initiating a batch import process.

1. Navigate to **Accounts > User Groups > List View** and select **Add**.
2. Select **Batch Import**.
3. Enter the basic information including **Batch Name** and **Batch Description** in the AirWatch Console.
4. Under **Batch File (.csv)**, select the **Choose File** button to locate and upload the completed CSV file, now ready for importing.

5. Alternately, select the link **Download template for this batch type** and save the comma-separated values (CSV) file and use it to prepare a new importation file.
   - Open the CSV file, which has several columns corresponding to the settings that display on the **Add User Group** page. Columns with an asterisk are required and must be entered with data. Save the file.
   - The last column heading in the CSV file template is labeled "*GroupID/Manage(Edit and Delete)/Manage(Users and Enrollment)/UG assignment/Admin Inheritance.*" This column heading corresponds to the settings and abides by the logic of the **Permissions** tab of the **Edit User Group** page.
6. Select **Import**.

Edit User Group Permissions

Fine-tuning user group permissions allows you to reconsider who inside your organization can edit certain groups. For example, if your organization has a user group for company executives, you may not want lower-level administrators to have management permissions for that user group.

Use the **Permissions** page to control who can manage certain user groups and who can assign profiles, compliance policies, and applications to user groups. Important logic restrictions are highlighted in red.

1. Navigate to **Accounts > User Groups > List View**.
2. Select the **Edit** icon of an existing user group row.
3. Select the **Permissions** tab, then select **Add**.
4. Select the **Organization Group** you want to define permissions for.
5. Select the **Permissions** you want to enable.
   - **Manage Group (Edit/Delete)** – Activate the ability to edit and delete user groups.
   - **Manage Users Within Group and Allow Enrollment** – Manage users within the user group and to allow a device enrollment in the organization group.This setting can only be enabled when Manage Group (Edit/Delete) is also enabled. If Manage Group (Edit/Delete) is disabled, then this setting is also disabled.
   - **Use Group For Assignment** – Use the group to assign security policies and enterprise resources to devices.This setting can only be changed if Manage Group (Edit/Delete) is disabled. If Manage Group (Edit/Delete) is enabled, then this setting becomes locked and uneditable.
6. Select the **Scope** of these permissions, that is, which groups of administrators are allowed to manage or use this user group. Only **one** of the following options may be active.
   - **Administrator Only** – The permissions affect only those administrators at the parent organization group.
   - **All Administrators at or below this Organization Group** – The permissions affect the administrators in the organization group and all administrators in all child organization groups underneath.
7. Select **Save**.

Mapping User Groups for Enrollment and Console Access

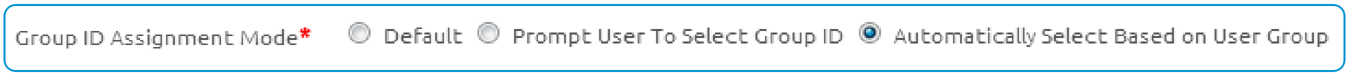
After you add your directory service groups to AirWatch, you can use the resulting AirWatch user groups for enrollment and role-based access.

- In terms of a device enrollment, you can map user groups to existing organization groups and automatically select a Group ID based on a user group.
- In terms of console access, you can restrict the level of AirWatch Console access users have (roles) based on their user group membership.

You can configure settings to select a Group ID automatically based on a user group or allow users to select a Group ID from a list.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Grouping** tab.

2. Choose **Automatically Select Based on User Group** as the **Group ID Assignment Mode**.

   Group ID Assignment Mode* ○ Default ○ Prompt User To Select Group ID ● Automatically Select Based on User Group

   This option works only when your existing directory service is already replete with user group assignments independent from AirWatch.

   Enabling this option ensures that users are automatically assigned to organization groups based on their directory service group assignments. Once selected, the **Group Assignment Settings** section displays all the organization groups (OG) for the environment and their associated directory service user groups.

   When the **Apply mapping on enrollment only** setting is enabled, the user group assignment applies at enrollment time only. After enrollment, devices can be manually moved to another organization group. However, if the **Apply mapping on enrollment only** check box is still enabled, the device does not honor any new user group mapping. The event log captures the identity of the admin requesting this mapping at enrollment time.

   For more information about the Event Log, see Reports & Analytics in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

3. Modify the organization group/user group associations and set the rank of precedence for each group by selecting **Edit Group Assignment**. If a user belongs to multiple user groups, the rank determines which user group takes precedence. The user is associated to the OG of the highest-ranked user group to which they belong. Select **Save** when you are finished.

4. Similar to user group mapping to an OG assignment, you can also map roles, or console permissions, based on user groups. Enable the editing of role-based access levels by selecting **Enable Directory Group-Based Mapping** in the **User Role Mapping** section. To edit roles and rank user groups, similar to the method used in step 3, select **Edit Assignment**.

   For each user group, set the rank of precedence and associated role each group has. Just as in step 3, if a user belongs to multiple user groups, the rank determines which user group, and therefore role, takes precedence. The user receives permissions for the highest-ranked user group to which they belong. Select **Save** when you are finished.

   Access the Roles page and define new or edit existing Roles by navigating to **Accounts > Roles**.

5. Select **Save** when you are done mapping user groups to enrollment organization groups and roles.

You can restrict an enrollment to only known users or configured groups. For more information, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Deploying Apps, Policies, and Profiles by User Group

After you import your directory groups into AirWatch you can use them as more criteria when assigning profiles, compliance policies, apps, and content.

Profile, Policy, and Application Assignment Notes

If you assign a profile, policy, or application to both an Organization Group (OG) and a user group, the user group serves as an extra filter. AirWatch uses this extra filter to assign settings or content. Even if you select an OG with many users, AirWatch only assigns to users in the group with a device that is in the assigned OG. The administrator can use both organization groups and user groups to configure more advanced settings.

For example, there may be different OGs set up for countries with different privacy policies. If any of the user groups include users from various countries, ensure *only* the devices that belong to the appropriate OG receive the setting or content. By selecting the appropriate Organization Group together with the user group, you can ensure that only the members in *both* groups receive the setting or content.

User Groups and Smart Groups

When configuring your Mobile Device Management environment, use user groups to define security authentication groups and business roles within your organization. User groups offer a simple one-to-one relationship between your users and the groups to which they belong.

Smart Groups, however, offer a flexible solution to push settings and content. This solution involves targeting selected devices by model, operating system, and device tags in addition to OGs and user groups. Smart Groups can also target individual users across *multiple* organization groups and user groups.

For more information on defining Smart Groups, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Deactivate and Reactivate Users Automatically

You can control how AirWatch reacts when user accounts are removed or disabled in your directory service by using auto sync. Auto sync enables you to set disabled users to inactive.

As users are removed from directory service groups, they are also removed from the associated AirWatch user group and unenrolled from AirWatch.

Conversely, users that have been deactivated and then reactivated in your directory service are reactivated in AirWatch automatically.

Automatically Reactivating AirWatch Users Upon Reactivation in Directory Service

When users deactivated in your directory service are later reactivated, AirWatch automatically reactivates their AirWatch account. This feature is always on and requires no console setting. Also, the event log captures this event which can be referred to for troubleshooting purposes.

For more information about the Event Log, see Reports & Analytics in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Perform Automatic Enterprise Wipe for Users That Do Not Belong to a User Group

You can automatically perform an enterprise wipe when users are removed from user groups. This check occurs at the same frequency as the Sync LDAP Groups scheduler task.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and select the **Restrictions** tab.
2. Select the Restrict Enrollment to the **Configured Groups option**.
3. If you want to enterprise wipe all devices **not** part of any user group automatically, then take the following steps.
   a. Select **All Groups**.
   b. Enable the **Enterprise Wipe devices of users not belonging to the configured groups** option.
4. If you want to enterprise wipe all devices **not** part of only *selected* user groups automatically, then take the following steps.
   a. Choose **Selected Groups** and include the user group names.
   b. Enable the **Enterprise Wipe devices of users not belonging to the configured groups** option.
5. The **Restrict Enrollment To Configured Groups** option means that enrollment is limited in the following ways.
   - Enrollment is limited to users belonging to any user group (All Groups).
   - Enrollment is limited to users belonging to a particular user group (Selected Groups).

   For more information, refer to the Enabling Directory Service-Based Enrollment section of the**VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
6. Select **Save**.

Set Disabled Users to Inactive Automatically

You can enable AirWatch to detect when a user account is disabled in your directory service and automatically set its associated AirWatch user account to inactive.

1. Navigate to **Accounts > Settings > Directory Services**.
2. Select the **User** tab.
3. See advanced configuration options by selecting the **Show Advanced** hyperlink.
4. Select **Automatically Set Disabled Users to Inactive** check box.
   - **Value For Disabled Status** – Enter a numeric value and select the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user’s status. Select “Flag Bit Match” if the user status is designated by a

bitwise flag (which is the default for Active Directory).

  - If any bits from the property match the value you enter, then the directory service considers the user to be disabled. But only when Flag Bit Match is selected.

- If you select this option, then AirWatch administrators set as inactive in your directory service may not log in to the AirWatch Console. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.

Remove Users From User Groups Based on Directory Service Group Membership

You can enable AirWatch to detect when a directory service user account is removed and automatically remove its associated AirWatch user account from the associated group.

1. Navigate to **Accounts > User Groups > Settings > Directory Services**.
2. Select the **Group** tab.
3. See advanced configuration options by selecting the **Show Advanced** hyperlink.
4. Select the **Auto Sync Default** check box.

Synchronization Errors

AirWatch ensures that device management and syncing continues even during rare lapses in connectivity. These steps improve the performance of Directory Services by ensuring that the server maximizes available resources.

Skipping a Tenant After Three Sync Timeouts

If a tenant's directory sync times out three times in a row, AirWatch skips that tenant and proceeds to synchronize the next tenant, as applicable. A sync times out if a device does not respond for 15 minutes. This timing means that the maximum delay is 45 minutes before the next tenant sync attempt.

A console event log is created after the third sync timeout with the following properties.

- **Name of event** – EnterpriseIntegrationLDAPSyncError.
- **Event data** – OG name, error description (Sync failed three times in a row. Sync skipped.).
- **Event severity level** – Error.

Skipping a Tenant After VMware Enterprise Systems Connector Connection Error

Also, if the link to the VMware Enterprise Systems Connector is not working or if the test connection fails, then the sync fails to begin. The next tenant sync commences according to the Lightweight Directory Access Protocol (LDAP) configuration.

The console event log is created after an VMware Enterprise Systems Connector connection error with the following properties.

- **Name of event** – EnterpriseIntegrationACCConnectionFailed.
- **Event data** – Reason and OG name.
- **Event severity level** – Error.

For more information about the Event Log, see Reports & Analytics in the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Troubleshooting Synchronization Errors

Ensure the Directory Sync Service and the Scheduler Service are running on the same server, since they write to and read from the same queues.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.