AirWatch User Group Integration

A Guide to Leveraging AD User Groups in AirWatch

© 2012 AirWatch, LLC. All Rights Reserved.

This document, as well as the software described in it, is furnished under license. The information in this manual may only be used in accordance with the terms of the license. This document should not be reproduced, stored or transmitted in any form, except as permitted by the license or by the express permission of AirWatch, LLC.

Other product and company names referenced in this document are trademarks and/or registered trademarks of their respective companies.
Contents

AirWatch User Group Integration ................................................................. 2

Transitioning to User Groups ...................................................................... 3
Prerequisites ................................................................................................. 3
Setting Up User Groups in AirWatch .............................................................. 3
Assigning Profiles, Policies, and Applications to User Groups ...................... 5
Editing User Group Settings and Management Permissions ........................... 6

Optimizing your MDM Strategy with User Groups ..................................... 8
Using Location Groups .................................................................................. 8
User Management Changes for Directory Users .............................................. 8
Helpful Tips ................................................................................................... 9
AirWatch User Group Integration

The latest release of AirWatch introduces **user group integration**. This allows administrators to further streamline MDM management by leveraging existing LDAP/AD user groups in AirWatch. Administrators will be able to more efficiently manage groups of users in AirWatch based on their existing LDAP/AD user group associations.

Once successfully integrated into AirWatch, user groups can act as additional filters (on top of location groups) for determining which devices should receive MDM profiles and policies. Although there are a few steps required to transition to user group integration and management, user groups can further streamline mobile device management for administrators. After transitioning to user groups, the administrator can more easily perform tasks in the following areas:

- **User Management**: Administrators can easily reference their existing LDAP/AD 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 only allow approved administrators to change policy and profile assignments for certain user groups.

- **Enrollment**: Allow users to enroll in AirWatch using the same URL and/or group ID even though their devices may receive different corporate resources.

Relevance of Location Groups

User groups do not replace Location Groups in AirWatch. Location groups are still the primary means of performing the following tasks in AirWatch:

- Setting administration management permissions in the web console

- General asset tracking on the AirWatch dashboards (such as the device, reports, and Email dashboards)

- Configuring system settings

- Assigning profiles, policies and applications: Even though it is possible to assign these resources to user groups, user groups only act as an additional filter on top of location groups. It is still possible to only assign MDM resources to location groups.

It is important to note that the existing MDM assignments **will not be affected** once you import user groups. In order to facilitate the transition process and ensure that your users will not experience any disruption to their current configurations, the administrator must [manually apply policies to user groups](#) as needed.
Transitioning to User Groups

Existing AirWatch customers with an LDAP/AD infrastructure can easily leverage their LDAP/AD groups in AirWatch.

Prerequisites

Before beginning the user group transition process, the following prerequisites must be satisfied:

- The administrator must designate an existing location group as the **primary root location group** from which the administrator will manage devices and users.

- Directory Services (and EIS, when used) must be enabled in AirWatch at the level of this root location group.
  
  - For example, if the root location group is **Internal** and EIS integration is in place, EIS integration should be enabled with the Internal location group selected on the left-hand side of the screen, as shown below:

Setting Up User Groups in AirWatch

To create user groups in AirWatch based on AD/LDAP groups:

- After all **prerequisites** are satisfied, navigate to Users ➔ User Accounts ➔ User Groups

- Click **Add**

- Enter the user group key words in the “Search Text” box and click **Search**.
From the search results, select the desired directory groups and proceed with mapping your existing LDAP/AD group assignments with your new AirWatch user groups.

**Auto Sync and Auto Merge Checkboxes:** When you initially import user groups into AirWatch, they will automatically sync and merge with the existing user group assignments in AirWatch. However, you should check these boxes to ensure that your user group assignments are updated on a regular basis.

- **Auto Sync:** The Auto Sync feature collects changes in LDAP group membership (without taking any action on those changes).
- **Auto Merge:** Auto Merge feature merges any of the changes detected from the Auto Sync process and merges them into AirWatch user groups.
  - To establish the maximum allowable number of group membership changes to be merged into AirWatch, enter a number in the **Maximum Allowable Changes** box when you add a directory group. You can edit this number in the **User Group Settings**.
Assigning Profiles, Policies, and Applications to User Groups

Once you have successfully integrated user groups into AirWatch, they provide additional criteria for assigning profiles, compliance policies and applications.

User Groups appear as an assignment field for the relevant MDM resources. The user group name is followed by the “@” sign and the name of the Location group at which the user group was created. Follow the instructions below to navigate to the appropriate editing page, and then continue to the instructions for assigning the MDM policy to user groups.

- To assign an existing **Profile** to a user group, navigate to the profile editing page (Profiles & Policies →Profiles) and select **Edit Assignment** from the **Actions** menu.
- To assign an existing **Compliance Policy** to a user group, navigate to the compliance editing page (Profiles & Policies →Compliance) and select **Edit** from the **Actions** menu.
- To assign an existing **Application Group** (for internal applications only) to a user group, navigate to the application editing page (Apps →Applications →Application Groups) and select **Edit** from the **Actions** menu.

- In the **Location Group** field, select the appropriate assigned location group.
- Select one or more user groups to receive the resource, and click the appropriate button to **save and publish** the profile, application, or compliance policy.

**Policy Assignment Notes**

If the administrator assigns a profile or policy to both a location group and a user group, AirWatch will use the **user group** as an additional filter for assigning the profile.

- Even if you select a very large location group, AirWatch will only apply the policy to the users who are a member of the user group and have a device that is in the assigned location group.

- The administrator may wish to use both **location groups and user groups** to configure more advanced settings.
  - For example, there may be different location groups set up for countries with different privacy policies. If any of the user groups include users from various countries, the administrator needs to ensure that only the devices that belong to the appropriate location group receive the policy. By selecting the appropriate location group and the user group, the administrator can ensure that only the members in both the user group and the location group will receive the policy.
Editing User Group Settings and Management Permissions

An additional benefit of user group integration in AirWatch is increased management flexibility enabled by user group settings for automatic updates and editing permissions.

Edit User Group Settings

- User group settings can be configured to automatically detect each time a user leaves or joins a group. The administrator can set a maximum allowable number of automatic changes, and any changes that exceed this threshold will require administrator approval. Navigate to Users→User Accounts→User Groups

  - In order to have management permissions, ensure that you have selected the root location group for your device fleet.

- Select the Actions menu next to the user group and click Edit. The General tab appears by default.

  ![Edit User Group](image)

- Enter the Maximum Allowable Changes in the appropriate field.

  - Any number of changes detected upon syncing with the LDAP/AD database that are under this number will be automatically merged. If the number of changes exceeds this threshold, the administrator must manually approve the changes before they are applied.

  - A single change is defined by a user either leaving or joining a group.
Edit User Group Permissions

User groups allow corporations to re-consider who inside the organization has permission to edit certain groups. For example, if an organization has a user group for company executives, they 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.

- Navigate to Users→User Accounts→User Groups.
  - In order to have management permissions, ensure that you have selected the root location group for your device fleet.
- Select the Actions menu next to the user group you wish to edit.
- Select the Permissions tab and specify the following permissions:
  - Choose the Location Group for which you would like to define permissions.
  - Allow Inheritance — Check whether or not to allow lower location groups to manage/assign policies to the user groups below that level.
  - Permissions — Use these options to determine whether or not the specified location group can assign resources to and manage the selected location group (when allow inheritance is checked, the policies also apply to child location groups).
    - Manage — Checking this box allows administrators at the specified Location Group(s) to manage (edit the user group friendly name, merge, and sync settings) this user group.
    - Assign — Checking this box allows administrators at the specified Location Group(s) to assign compliance policies, profiles and applications to the User Group.
  - Allow Access to User — When Allow Access to User is checked, administrators at the specified location group(s) will have the ability to add or delete users in this user group.
    - Ensure that the Allow Access to User setting is correctly configured before administrators begin adding users to the user group. Administrators that do not have this permission will be able to add devices but will not be able to add users.
Optimizing your MDM Strategy with User Groups

Using Location Groups
Location groups still have a purpose in AirWatch, even for customers that are fully leveraging user groups. Location groups still control the following AirWatch capabilities:

- **Asset Tracking** - Location groups define which business units the devices live at, so be sure to consider the device groupings you wish to view on the AirWatch dashboards. Location Groups are still the primary filter on all console pages for all dashboards and views.

- **System Settings** – System settings are tied to Location groups. You must define different location groups if you need different system settings. Examples of important settings to consider include:
  - Enterprise Integration Servers
  - Enrollment Settings and Restrictions
  - EULAs
  - Privacy Policies

User Management Changes for Directory Users
In addition to the integration of user groups into AirWatch, there are a few changes to user management for Directory security type (previously referred to as “Authentication” security type) users. If you currently use Directory Services in AirWatch, please note the following:

- Directory users can now only be created at the same level as the Location Group where directory services settings are enabled.
  - In order 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 location group where Directory Services are enabled.

- There is now only one location in the AirWatch System Settings for Directory Services (called “Directory Services”). The same directory settings will be used for both enrolling and logging into the console.

- Directory Service settings now allow the administrator to configure custom mapping of user attributes in AirWatch to LDAP user attributes.

User Storage in AirWatch
The addition of user groups also has implications for where directory users are stored in AirWatch. Once you have completed the transition to user groups, AirWatch performs the following actions:

- Directory users are moved to the level where directory service settings are in the console. You will still see them at the Location Group level where they have a device enrolled, but the users can only be managed at the same level as the directory service settings.

- After the upgrade to user groups, AirWatch performs a migration process that pulls the Distinguished Name of existing directory users into AirWatch.
Helpful Tips

User Groups and Location Groups: Functional Differences

- AirWatch recommends that you use User Groups to represent Security Groups or Business Roles within your organization.
- Users can belong to multiple groups, but devices still belong to only one location group.
- AirWatch currently supports the assignment of profiles, policies and internal apps to user groups.

Transition Options for Best Practices

If you have already defined location groups to represent user security groups, one of the following options may help you reconfigure your location group and user group structure to be more streamlined:

- **Reconfigure your system to associate Profiles, Applications and/or Enrollment Restrictions with User Groups:**
  - Assign each profile, app, and enrollment restriction to the appropriate User Groups
  - Change the Location Group assignment to one Location Group up
  - Add user group assignment

- **You may choose to reconfigure your hierarchy to remove old or unused location groups** (keep in mind that location groups still serve several purposes in AirWatch):
  - Move devices one Location Group up
  - Delete old Location Groups

- **You can choose to leave your structure as-is:**
  - At this point, the Location Group can be considered the “Primary Security Group” of the device
  - The User Groups will be used for assigning profiles and policies
  - The old, unused location groups can remain for asset tracking purposes