Adding Users and Enrolling Devices

ZENworks® Mobile Management 2.8.x

November 2013

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

Accessing the Dashboard

Accessing the Dashboard

ZENworks Mobile Management dashboard requirements:

- Microsoft Internet Explorer, Firefox, or Safari
- Adobe Flash Player 10.1.0
- Minimum screen resolution: 1024 x 768
- PC running Windows OS

In your Web browser, enter the server address of the *ZENworks Mobile Management* server, followed by ***/dashboard***

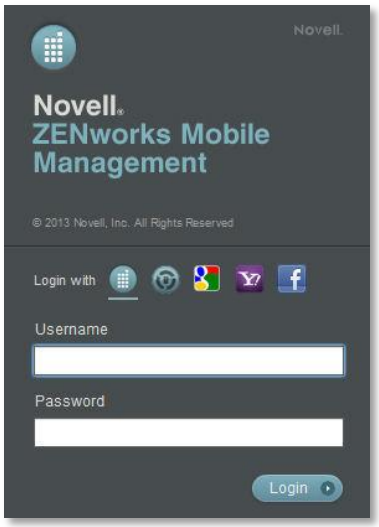
Example: https://my.ZENworks.server/dashboard

Standard Login

Log in to the *ZENworks Mobile Management* dashboard using your administrative login credentials in one of the following formats:

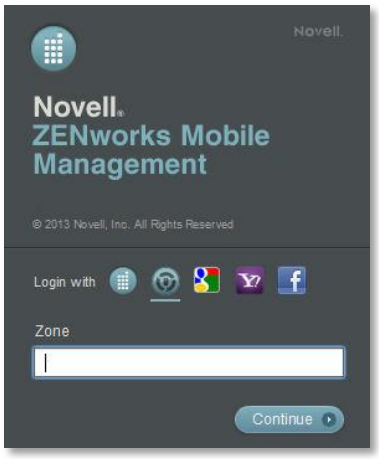
- Locally authenticated logins enter:
  email address and password
- LDAP authenticated logins enter:
  domain\LDAP username and LDAP password

A system administrator can create additional logins to the dashboard with system administrator, organization administrator, or support administrator privileges. See the *System Administration Guide* for details.



OpenID Login

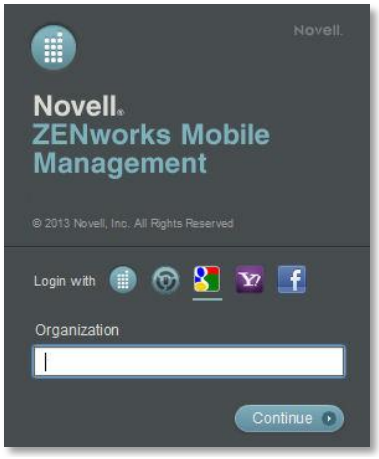
Use your OpenID credentials to log in.



1. At the *ZENworks Mobile Management* login screen, select the icon identifying the OpenID provider you use: *ZENworks, Google, Yahoo!,* or *Facebook*.
2. Enter the **Zone** or **Organization**, an easy to remember name *ZENworks Mobile Management* uses to redirect you to the OpenID provider portal.
3. At the provider site, enter your OpenID credentials.

   Note: If this is the first time you have logged in to *ZENworks Mobile Management* with an OpenID or your OpenID information has changed, you will be prompted for a PIN code before entering the *ZENworks Mobile Management* dashboard.

   Zone Name and new PIN codes are emailed to you from the *ZENworks Mobile Management* server.



Adding Users

Use the *Add New User Wizard* to add users to the *ZENworks Mobile Management* system. The wizard allows you to add users one at a time, import a list of users from a .CSV file, or import users from an LDAP server.

The methods for initially adding and provisioning users are as follows:

- **Manual** - Add individual users manually.

  If an LDAP server is specified when adding the user, that user must be present on the LDAP server. Selecting an LDAP server also allows policy suite, connection schedule, and liability to be assigned according to the settings associated with the LDAP group or folder to which the user belongs.

  Policy suite, connection schedule, and liability can also be assigned according to the settings associated with a local group to which you can assign the user. Local group settings will override LDAP group/folder settings.

  Administrators can also make direct policy suite, connection schedule, and liability assignments to the user, which override settings from all other sources.

- **Batch Import Methods** - User credentials can be imported from an LDAP directory or via a Comma Separated Values (.CSV) file.

  .CSV - All users imported in a single .CSV batch are assigned the same device ownership, plan type, carrier, and expiration.

  If an LDAP server is specified when adding the users, those users must be present on the LDAP server. Selecting an LDAP server also allows policy suite, connection schedule, and liability to be assigned according to the settings associated with the LDAP groups or folders to which users belong.

  Policy suite, connection schedule, and liability can also be assigned according to the settings associated with a local group to which you can assign the group of users. Local group settings will override LDAP group/folder settings.

  Administrators can also make direct policy suite, connection schedule, and liability assignments to the users, which override settings from all other sources.

  LDAP - All users imported in a single LDAP batch are assigned the same device ownership, plan type, carrier, and expiration.

  Policy suite, connection schedule, and liability can be assigned according to the settings associated with the LDAP groups or folders to which users belong.

  Policy suite, connection schedule, and liability can also be assigned according to the settings associated with a local group to which you can assign the group of users. Local group settings will override LDAP group/folder settings.

  Administrators can also make direct policy suite, connection schedule, and liability assignments to the users, which override settings from all other sources.

- **Hands-Off Enrollment** - Configure the organization for hands-off enrollment. To free the administrator from the task of adding users either manually or by batch import, *ZENworks Mobile*

Management can be configured to allow users to self-enroll. When the user enrolls a device an account is created and auto-provisioned on the *ZENworks Mobile Management* server using preset policy suite, connection schedule, and liability settings associated with local groups, LDAP groups or folders or organization default assignments.

User provisioning sources and the order in which they are applied

Users' policy suite, device connection schedule, and liability settings can originate from a variety of sources.

1st **Direct assignment:** An administrator can specify policy suite, device connection schedule, and liability when adding the user(s). Settings assigned this way override settings associated with a local group or LDAP group/folder to which the user belongs or organization defaults. Direct assignments take precedence over all other provisioning sources and will not change as a result of updates to the groups or defaults.

2nd **Local group assignment:** Policy suite, device connection schedule, and liability are obtained from the settings associated with the local group to which users belong. Settings associated with local groups take precedence over settings associated with LDAP groups/folders. Changes made to local group settings will automatically update users.

3rd **LDAP group or folder assignment:** Policy suite, device connection schedule, and liability are obtained from the LDAP group (highest priority group first) to which the user belongs. If the user does not have group membership, the folder (by folder hierarchy) to which the user belongs is the source for the settings. Regular periodic checks with the LDAP server will update user information and assignments if they change.

4th **Organization defaults:** Policy suite, device connection schedule, and liability will default to organization settings when a user is not assigned to a local or LDAP group or when local groups or LDAP groups/folders are not configured with settings.

Welcoming New Users to ZENworks Mobile Management

You can use a Welcome Letter to get information to new users when they are added to the *ZENworks Mobile Management* system. Before you start adding users to *ZENworks Mobile Management*, create Welcome Letters and configure the organization so that they are send automatically. You can also manually issue the email to individual users at any time.

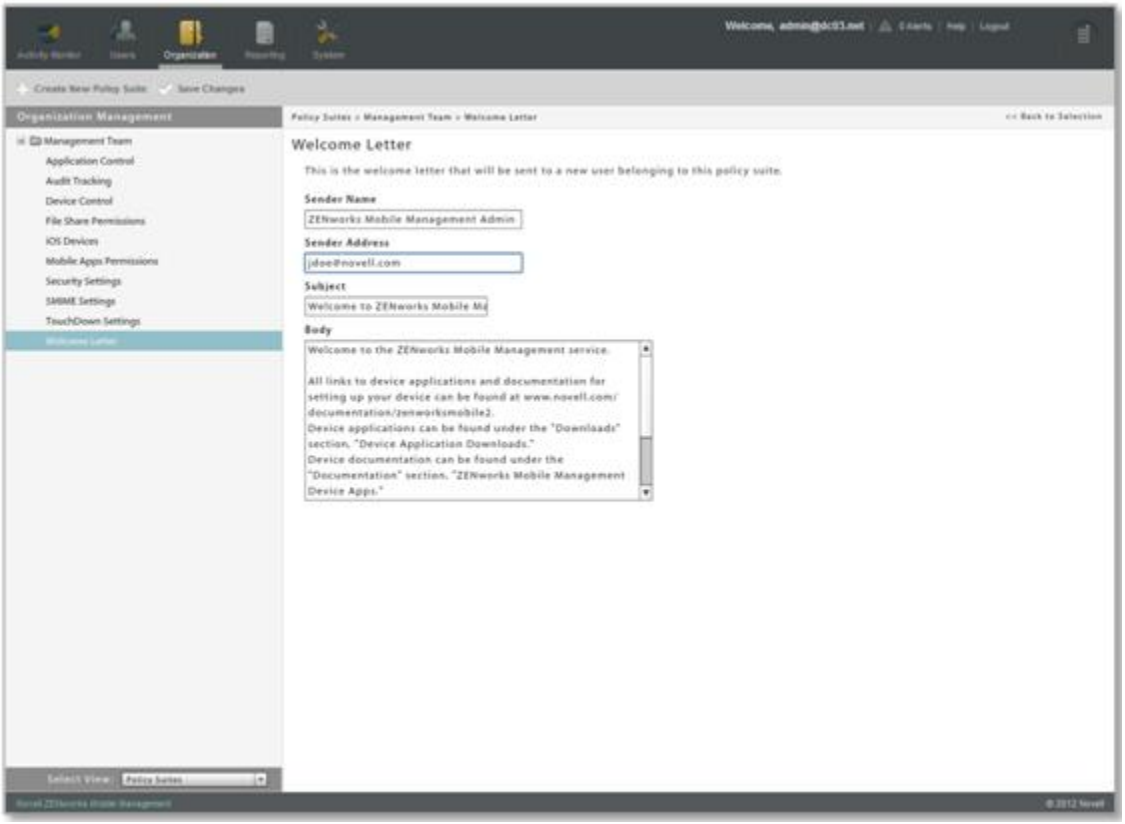
Information you might include in a Welcome Letter:

- Links to resources, such as the device app downloads, user documentation, and the user self-administration portal
- Details of policies that may change device functionality
- New features that make devices more secure

Creating a Welcome Letter

There is a Welcome Letter associated with each policy suite so that users under that policy receive information that pertains specifically to them.

Select ***Organization*** > ***Policy Management*** > ***Policy Suites***. Highlight a policy and select the Welcome Letter option in the left panel to edit the letter.

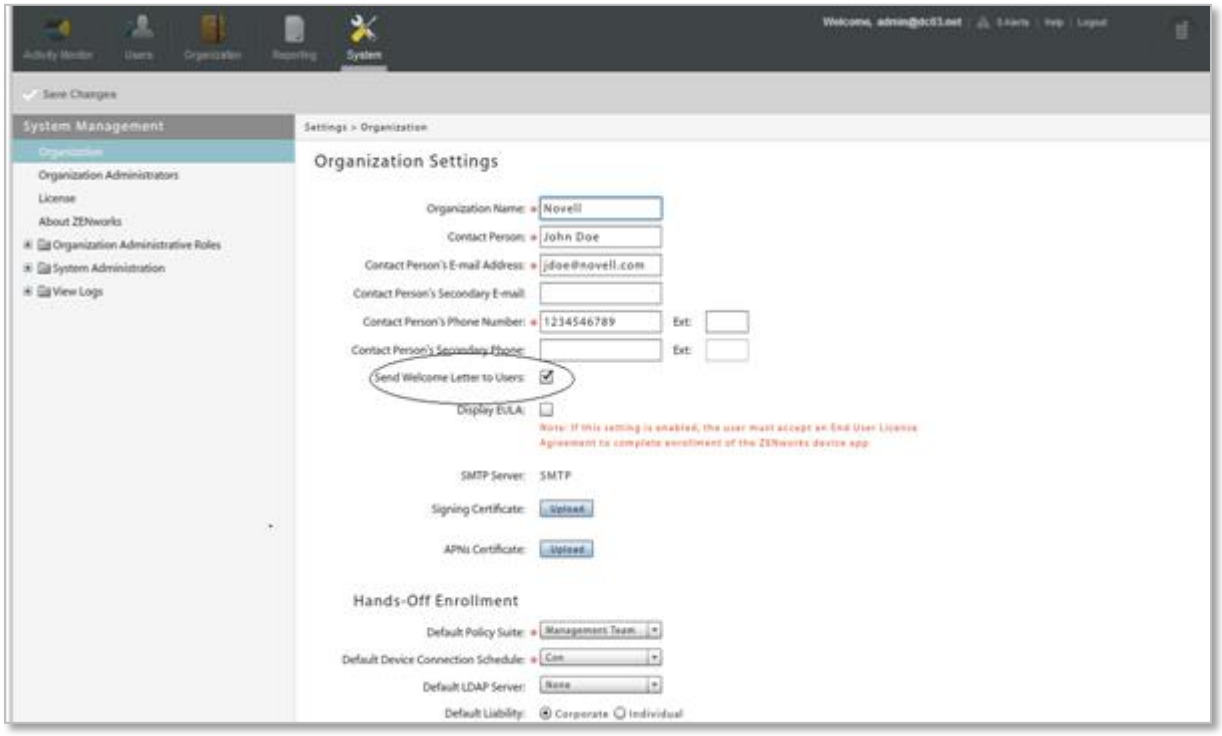


Welcome Letters will not be sent automatically unless the organization is configured to do so. See ***Automating the Welcome Letters*** below.

Automating the Welcome Letters

Configure the organization so that *Welcome Letters* are automatically emailed to every user that is added to the *ZENworks Mobile Management* server.

Select ***System*** > ***Organization*** and select the ***Send Welcome Letter to Users*** option.



Sending the Welcome Letter to Individual Users

You can also issue the Welcome Letter as needed, on a per user basis.

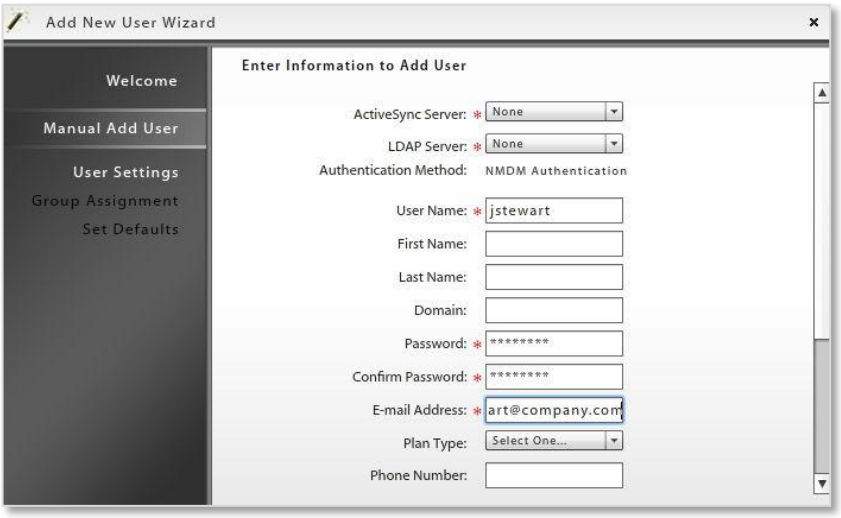
Select ***Users*** and highlight a user. Click the ***Send Welcome Letter*** option in the *User Panel*.

Adding Users Manually

Administrators can manually create individual user accounts in an organization. When a user account is created on the *ZENworks Mobile Management* server, one or more devices can be enrolled.

To Add Users Manually

1. From the *ZENworks Mobile Management* dashboard header, select ***Users***.
2. Click the ***Add User*** option to use the *Add New User Wizard*.
3. Select ***Manual*** from the Add New User Wizard dialog.



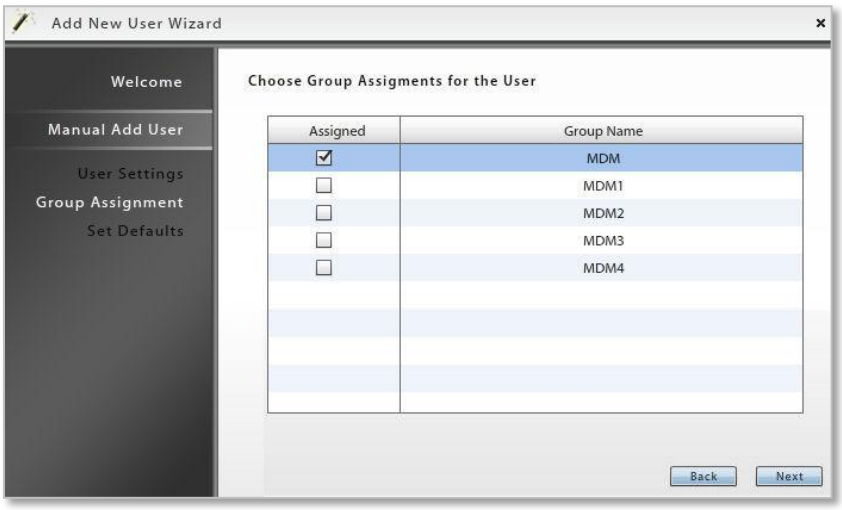
4. Enter the user information (see descriptions below), then click ***Next***. ***** = required field

ActiveSync server *	Select an ActiveSync server for the user or select *None*. If the ActiveSync server is linked to an LDAP server, the LDAP server field will populate as well.
LDAP Server *	Select an LDAP server for the user or select *None*. If an LDAP server is specified when adding the user, that user must be present on the LDAP server. Selecting an LDAP server also allows policy suite, connection schedule, and liability to be assigned according to the settings associated with the LDAP groups or folders to which the user belongs. This server can also be referenced for user updates and custom column information.
Authentication Method	Displays the method used to authenticate the user: ActiveSync, LDAP, or ZMM server authentication
User Name *	For users associated with an ActiveSync server, enter their ActiveSync account user name. For users on systems that do not use the ActiveSync protocol, enter a unique user name for their *ZENworks Mobile Management* user account.
First and Last Name	Enter the user's name.
Domain	If the ActiveSync server to which the user has been assigned requires a domain, enter it here. This also provides one way to configure the user for enrolling multiple devices against a single account. (See, *Enrolling Multiple Devices on a Single Account*.)
Password	***** Required for users on systems that do not use the ActiveSync protocol. Enter a unique password for their *ZENworks Mobile Management* user account.
E-mail Address *	Enter the user's email address.
Plan Type	Choose International, Domestic, or Unknown.
Phone Number	Enter the phone number of the user's mobile device. This can be used for sending an SMS notification to the user regarding their enrollment.
Carrier	Select the user's carrier from the drop-down list. See a list of supported carriers.
Send Enrollment Message	Select the SMS box to send an SMS enrollment message.

Enrollment Message	Enter an SMS enrollment message up to 160 characters. You may want to include links to resources such as the device app downloads, user documentation, and the user self-administration portal.

5. If you are using local groups to categorize users, choose local group assignments for the user.

   Click ***Next***.

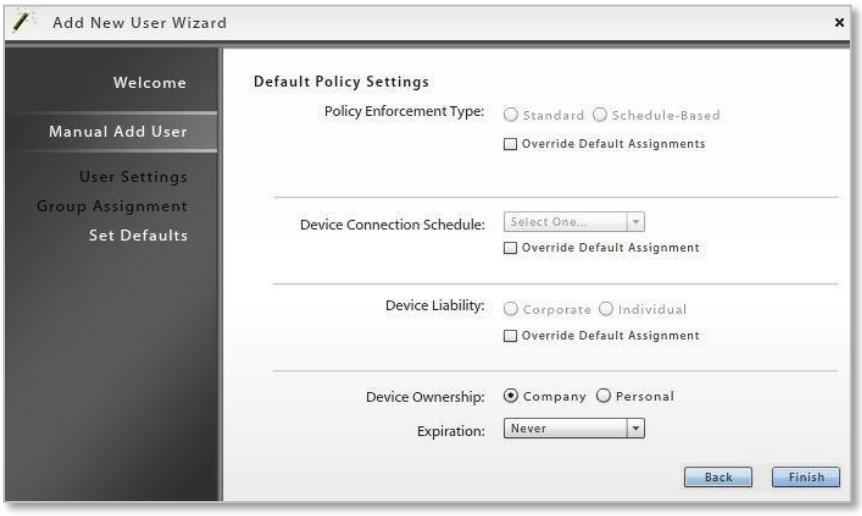


6. Make selections for provisioning the user if necessary, then click ***Finish***.

   If you have categorized the user in a local group or if an LDAP server has been specified and configured for provisioning users, you do not have to make selections for *Policy Schedule/Suite*, *Device Connection Schedule*, or *Liability* unless you want to make direct assignments that override the provisioning settings associated with the local groups or LDAP groups/folders.

   To override provisioning settings associated with local groups or LDAP groups/folders, check the box next to ***Override Default Assignments***. These checkboxes do not appear if you have not specified an LDAP server or local group.

   If not overridden, provisioning settings are obtained from the following sources, in this order: Local group(s), LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization defaults.



Policy Enforcement Type	Select ***Standard*** or ***Schedule-Based***. For schedule-based enforcement, a schedule defines the days and times during which users are working. If this method is chosen, you will also define two policy suites - one to be used during the scheduled hours and one to be used outside the scheduled hours. *Standard* policy enforcement executes the same policy suite at all times.
Policy Schedule (schedule-based)	The schedule that defines the days and times during which users are working.
Policy Suite (standard)	Select a (*Standard*) Policy Suite for the user. (This field is not displayed if you choose *Schedule-Based* enforcement.) If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Policy Suite During Schedule/ **Policy Suite Outside Schedule** (schedule-based)	The policy suite enforced during scheduled hours and the policy suite enforced outside scheduled hours. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Connection Schedule	Select a Device Connection Schedule for the user. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Liability	Liability refers to who owns the data on the device. Liability determines whether the corporate or individual component of the policy suite is assigned to the user. Choose *Corporate* (corporate liable) or *Individual* (individual liable). If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Ownership	Choose *Company* (the user's device is company owned) or *Personal* (the user's device is personally owned).
Expiration	Select a date for the user to be disabled or removed from the system. Choose *Never*, or a date on which to expire the user. Specify the action to take upon expiration: *Disable* or *Remove.* Expirations occur at the beginning of the designated day (12:00 a.m.) **Note:** Setting expirations for users in an organization configured for Hands-off enrollment is counterproductive. Users will be able to re-enroll the device app.

Adding Users via Comma-Separated Values (CSV) Files

An administrator can import a group of users to the *ZENworks Mobile Management* server via a .CSV file. User names, email addresses, and passwords of users are entered into a spreadsheet template.

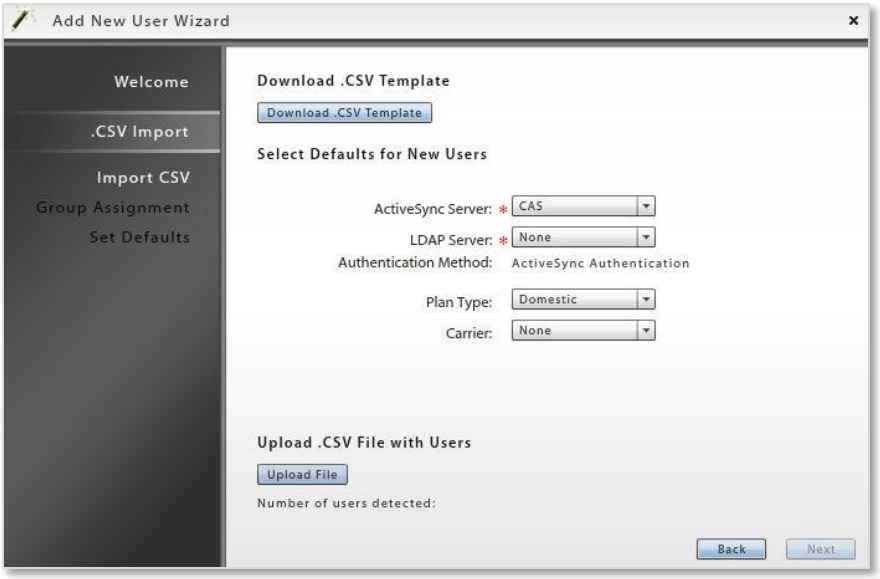
The administrator then makes provisioning assignments for the batch of users. All users imported in a single batch are assigned the same device ownership, plan type, carrier, and expiration.

Policy schedule/suite, device connection schedule, and liability assignments can originate from the settings associated with the LDAP groups/folders or the local groups. Administrators can also make direct assignments to the users, which override settings from all other sources and will not change as a result of updates to the groups or defaults.

The file is then uploaded to the *ZENworks Mobile Management* server where user credentials from the file and the provisioning assignments are merged to create new *ZENworks Mobile Management* user accounts.

Importing Users from .CSV Files

1. From the *ZENworks Mobile Management* dashboard header, select ***Users***.
2. Click the ***Add User*** option to use the *Add New User Wizard*.
3. Select ***.CSV*** from the Add New User Wizard dialog.



4. Download the .CSV spreadsheet template and save it in the desired location. Open the file and enter the information listed below for each user and save the changes to your file.

   Leave the headings in row 1 of the spreadsheet and begin entering user information in row 2.

   - user name
   - first name
   - last name
   - domain
   - email address
   - password

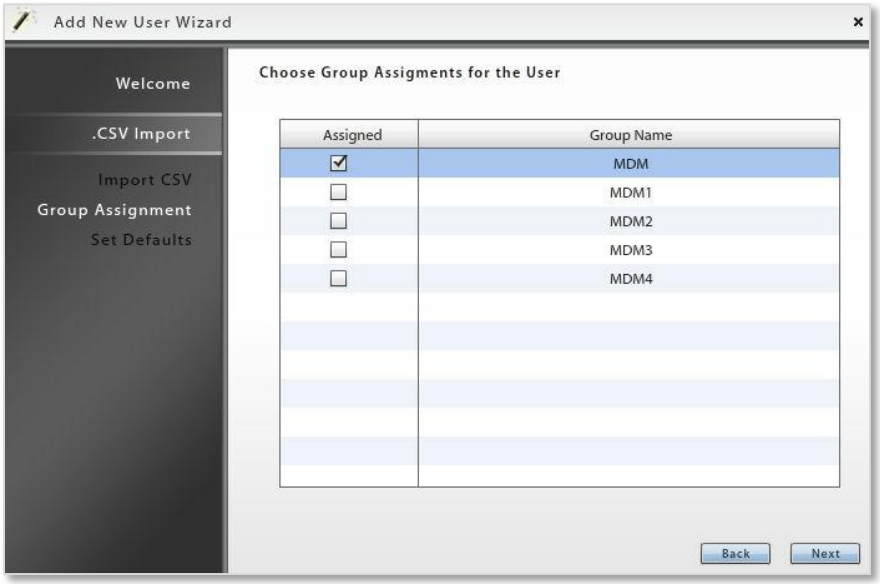
5. In the *Add New User Wizard*, make selections for provisioning the users. ***** = required field

ActiveSync server *	Select an ActiveSync server for the users or select *None*. If the ActiveSync server is linked to an LDAP server, the LDAP server field will populate as well.
LDAP Server *	Select an LDAP server for the users or select *None*. If an LDAP server is specified when adding the users, those users must be present on the LDAP server. Selecting an LDAP server also allows policy suite, connection schedule, and liability to be assigned according to the settings associated with the LDAP groups or folders to which users belong. This server can also be referenced for user updates, and custom column information.
Authentication Method	Displays the method used to authenticate the users: ActiveSync, LDAP, or ZMM server authentication
Plan Type	Choose International, Domestic, or Unknown.
Carrier	Select the users' carrier from the dropdown list. See a list of supported carriers.

6. Upload the .CSV file with the users' credentials by clicking the ***Upload File*** button. When it is finished uploading you will see a number next to the label, ***Number of users detected***. Click ***Next***.
7. If you are using local groups to categorize users, choose local group assignments for the users imported via the .CSV file.

   Policy suite, connection schedule, and liability can be assigned according to the settings associated with the local group(s) to which you assign the group of users. Local group settings will override LDAP group/folder settings.

   Click ***Next***.

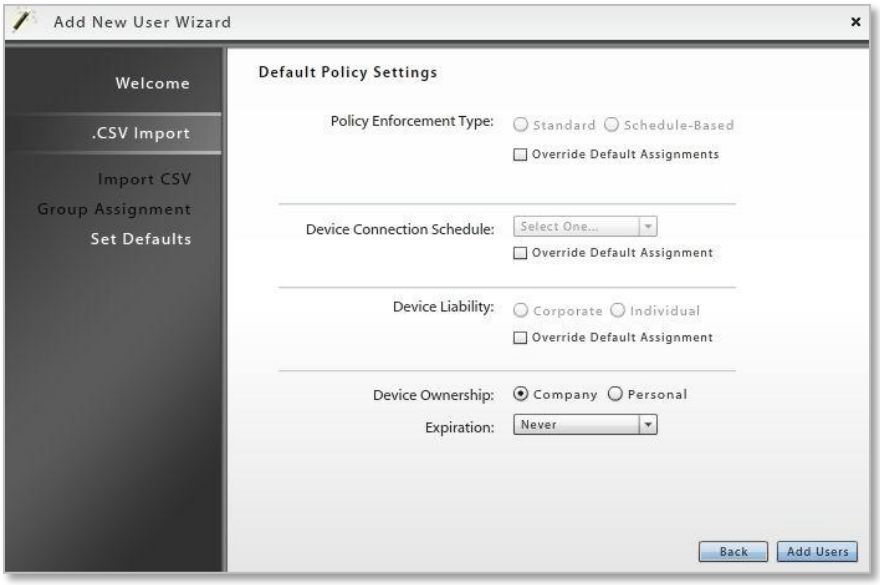


8. Make additional selections for provisioning the users if necessary. Click ***Finish***.

   If you have categorized the users in a local group or if an LDAP server has been specified and configured for provisioning users, you do not have to make selections for *Policy Schedule/Suite*, *Device Connection Schedule*, or *Liability* unless you want to make direct assignments that override the provisioning settings associated with the local groups or LDAP groups/folders.

   To override provisioning settings associated with local groups or LDAP groups/folders, check the box next to ***Override Default Assignments***. These checkboxes do not appear if you have not specified an LDAP server or local group.

   If not overridden, provisioning settings are obtained from the following sources, in this order: Local group(s), LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization defaults.



Policy Enforcement Type	Select ***Standard*** or ***Schedule-Based***. For schedule-based enforcement, a schedule defines the days and times during which users are working. If this method is chosen, you will also define two policy suites - one to be used during the scheduled hours and one to be used outside the scheduled hours. *Standard* policy enforcement executes the same policy suite at all times.
Policy Schedule (schedule-based)	The schedule that defines the days and times during which users are working.
Policy Suite (standard)	Select a (*Standard*) Policy Suite for the user. (This field is not displayed if you choose *Schedule-Based* enforcement.) If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Policy Suite During Schedule/ **Policy Suite Outside Schedule** (schedule-based)	The policy suite enforced during scheduled hours and the policy suite enforced outside scheduled hours. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources,

	in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Connection Schedule	Select the Device Connection Schedule for the user. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Liability	Liability refers to who owns the data on the device. Liability determines whether the corporate or individual component of the policy suite is assigned to the user. Choose *Corporate* (corporate liable) or *Individual* (individual liable). If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Ownership	Choose *Company* (user's device is company owned) or *Personal* (user's device is personally owned).
Expiration	Select a date for the user to be disabled or removed from the system. Choose *Never*, or a date on which to expire the user. Specify the action to take upon expiration: *Disable* or *Remove.* Expirations occur at the beginning of the designated day (12:00 a.m.) **Note:** Setting expirations for users in an organization configured for Hands-off enrollment is counterproductive. Users will be able to re-enroll the device app.

9. Click ***Add Users***. The *Users* grid will begin to populate with new users.

Adding Users via LDAP

When an Administrative LDAP server is defined for an organization, an administrator can retrieve user information from the corporate LDAP directory and use it to add users to *ZENworks Mobile Management*.

All users imported in a single batch are assigned the same domain, device ownership, plan type, carrier, and expiration.

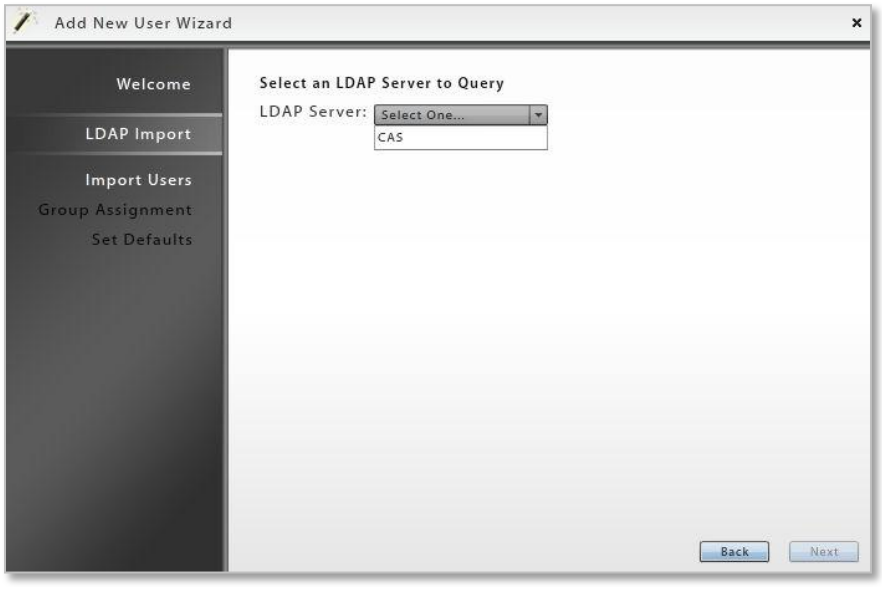
Policy schedule/suite, device connection schedule, and liability assignments can originate from the settings associated with the LDAP groups/folders or the local groups. Administrators can also make direct assignments to the users, which override settings from all other sources and will not change as a result of updates to the groups or defaults.

When assignments originate from settings associated with LDAP groups/folders, regular periodic checks with the LDAP server will update user information and assignments if they change. When assignments originate from settings associated with local groups, changes made to the group settings will automatically update users.

LDAP Configuration Tip: When configuring the Administrative LDAP server, you can limit the number of unnecessary folders/groups pulled from the LDAP server, by entering the LDAP Base DN so that it includes only the required users/groups. This prevents unnecessary users/groups (like computers and computer groups) from being selected.

Importing Users from an LDAP Directory

1. From the *ZENworks Mobile Management* dashboard header, select ***Users***.
2. Click the ***Add User*** option to use the Add New User Wizard.
3. Select ***LDAP*** from the Add New User Wizard dialog.
4. Select an ***LDAP Server*** to query.



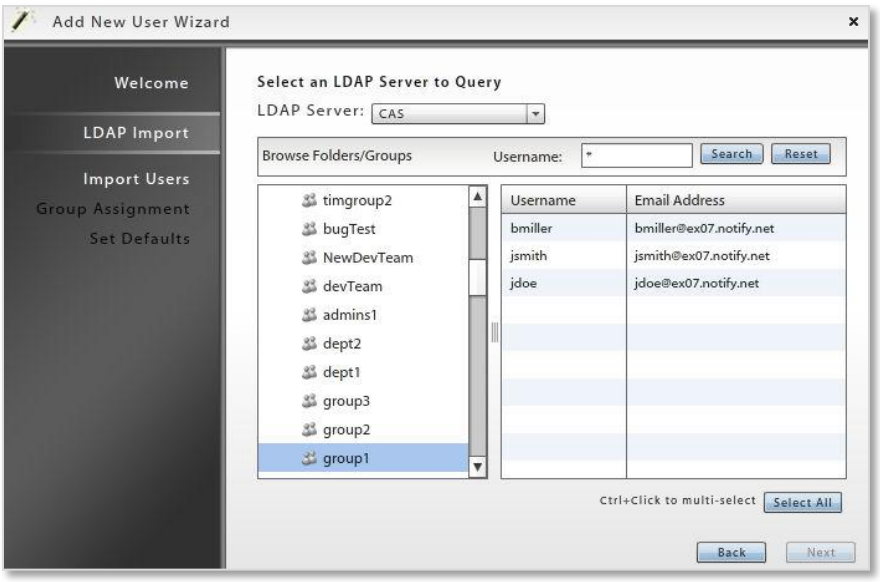
5. Select the users to pull from the LDAP server using the search filter. Browse the LDAP directory in the left panel and select a folder/group. Click ***Search*** to display the members of the folder/group in the right panel.

   Folders and groups are distinguished in the directory list by these symbols.

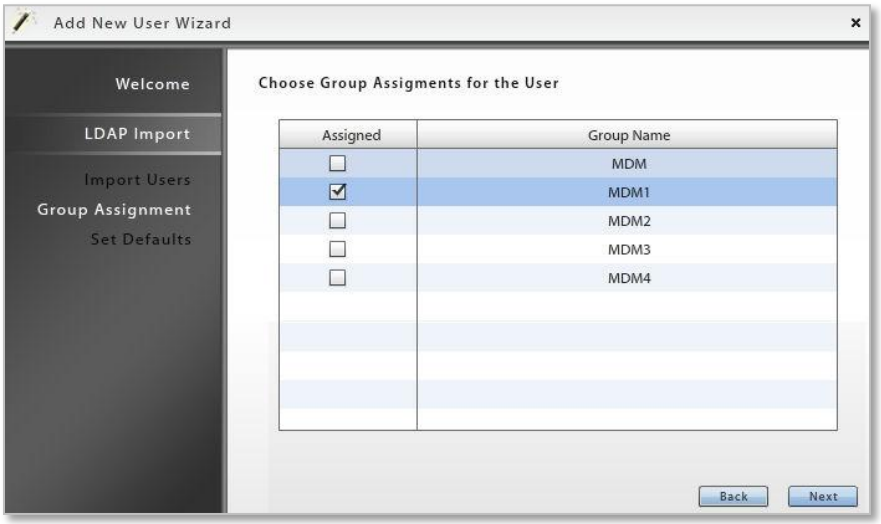
   You can also enter a specific username in the ***Username*** search bar or use a wildcard symbol (*) in the search to filter your search. Examples: ja* returns usernames that begin with “ja”; *son* returns usernames that contain “son.”

6. Select a username from the grid on the right, or hold the Ctrl key down as you click to select multiple usernames, or click ***Select All***. Click ***Next***.



7. If you are using local groups to categorize users, choose local group assignments for the users imported from the LDAP server. Click ***Next***.

   Policy suite, connection schedule, and liability can be assigned according to the settings associated with the local group(s) to which you assign the group of users. Local group settings will override LDAP group/folder settings.

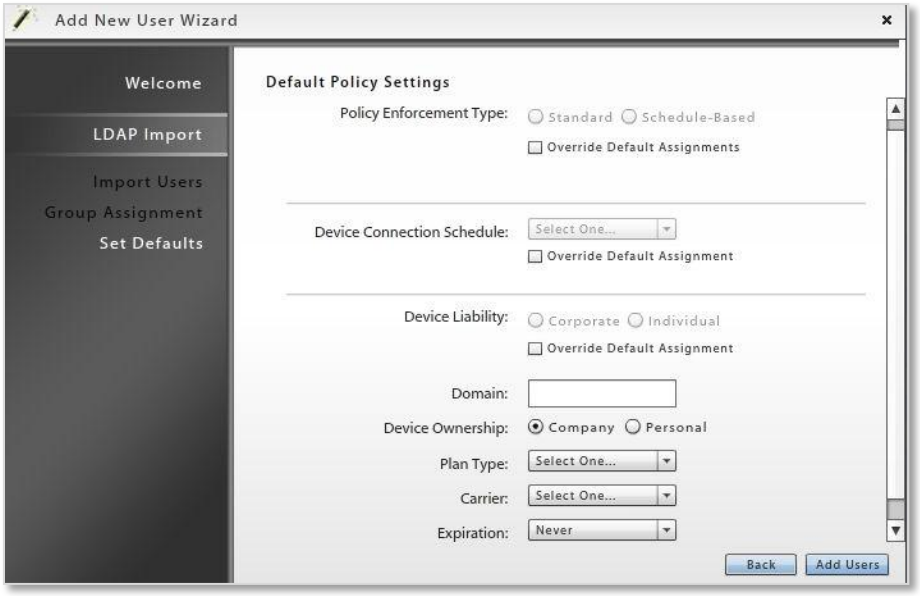


8. Make selections for provisioning the users if necessary.

   If you have categorized the users in a local group or if an LDAP server has been specified and configured for provisioning users, you do not have to make selections for *Policy Schedule/Suite*, *Device Connection Schedule*, or *Liability* unless you want to make direct assignments that override the provisioning settings associated with the local groups or LDAP groups/folders.

   To override provisioning settings associated with local groups or LDAP groups/folders, check the box next to ***Override Default Assignments***. These checkboxes do not appear if you have not specified an LDAP server or local group.

   If not overridden, provisioning settings are obtained from the following sources, in this order: Local group(s), LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization defaults.



Policy Enforcement Type	Select ***Standard*** or ***Schedule-Based***. For schedule-based enforcement, a schedule defines the days and times during which users are working. If this method is chosen, you will also define two policy suites - one to be used during the scheduled hours and one to be used outside the scheduled hours. *Standard* policy enforcement executes the same policy suite at all times.
Policy Schedule (schedule-based)	The schedule that defines the days and times during which users are working.
Policy Suite (standard)	Select a (*Standard*) Policy Suite for the user. (This field is not displayed if you choose *Schedule-Based* enforcement.) If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Policy Suite During Schedule/ **Policy Suite Outside Schedule** (schedule-based)	The policy suite enforced during scheduled hours and the policy suite enforced outside scheduled hours. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy),

	organization default settings.
Device Connection Schedule	Select the Device Connection Schedule for the user. If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Liability	Liability refers to who owns the data on the device. Liability determines whether the corporate or individual component of the policy suite is assigned to the user. Choose *Corporate* (corporate liable) or *Individual* (individual liable). If an LDAP server has been specified, you do not have to make a selection unless you want to make a direct assignment that overrides the default. Defaults are obtained from assignments associated with the following sources, in this order: LDAP group(s) (by priority), LDAP folder (by folder hierarchy), organization default settings.
Device Ownership	Choose *Company* (user's device is company owned) or *Personal* (user's device is personally owned).
Expiration	Select a date for the user to be disabled or removed from the system. Choose *Never*, or a date on which to expire the user. Specify the action to take upon expiration: *Disable* or *Remove.* Expirations occur at the beginning of the designated day (12:00 a.m.) **Note:** Setting expirations for users in an organization configured for Hands-off enrollment is counterproductive. Users will be able to re-enroll the device app.

9. Click ***Add Users*** when you have finished making your selections. The *Users* grid will begin to populate with new users.

Configuring the Organization for Hands-Off Enrollment

Configuring an organization for Hands-Off enrollment enables users to self-enroll. When the user enrolls a device, an account is created and auto-provisioned on the *ZENworks Mobile Management* server using preset organization default assignments or assignments associated with LDAP groups/folders or local groups. This frees the administrator from the task of adding users either manually or by batch import.

Hands-Off enrollment can be configured two ways:

- Enable the *Hands-Off Enrollment* option when defining an ActiveSync server so that users with credentials on the ActiveSync server can self-enroll against the ZENworks Mobile Management server. When the user enrolls a device, an account is created and auto-provisioned using the organization default settings.
- Enable the *Hands-Off Enrollment* option when defining an LDAP server so that users with credentials on the LDAP server can self-enroll against the *ZENworks Mobile Management* server. You can allow hands-off enrollment for all users associated with the LDAP server or you can allow it only for selected LDAP folder/group members. When the user enrolls a device, an account is created and auto-provisioned using assignments associated with LDAP groups/folders to which users belong.

When an ActiveSync server and LDAP server are linked, configuring one server for hands-off enrollment will automatically configure the other server for hands-off enrollment.

Setting expirations for users in an organization configured for hands-off enrollment is counterproductive, since users will always be able to re-enroll the device app.

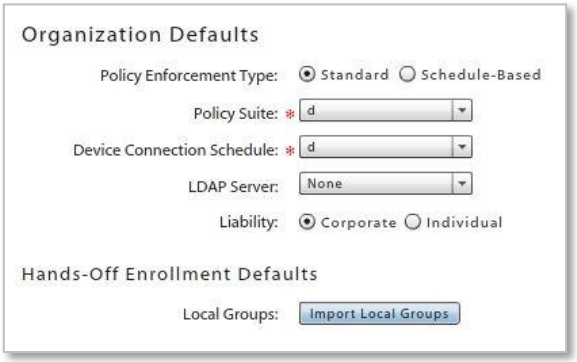
Requirements for Novell GroupWise DataSync and Other ActiveSync 2.5 Mail Servers

Systems where iOS users are interfacing with a Novell GroupWise DataSync server must use DataSync Update 4 (Mobility 1.2.4) to fully utilize the hands-off enrollment functionality. Users need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. Similar processes must be followed to use hands-off enrollment when users interface with Exchange 2003 or any other mail server running ActiveSync 2.5 protocol. A user's username and the string of characters to the left of the @ sign in their email address must be the same.

Organization and Hands-Off Enrollment Defaults

Organization defaults: Policy suite, device connection schedule, and liability will default to organization settings when the enrolling user is not assigned to a local group or LDAP group or when local groups or LDAP groups/folders are not configured with settings.

The organization defaults, as they appear on the *Organization Settings* page, are shown below:



Policy Enforcement Type	Select ***Standard*** or ***Schedule-Based***. For schedule-based enforcement, a schedule defines the days and times during which users are working. If this method is chosen, you will also define two policy suites - one to be used during the scheduled hours and one to be used outside the scheduled hours. *Standard* policy enforcement executes the same policy suite at all times.
Policy Schedule (schedule-based)	The schedule that defines the days and times during which users are working.
Policy Suite (standard)	Select a (*Standard*) Policy Suite for the user. (This field is not displayed if you choose *Schedule-Based* enforcement.)
Policy Suite During Schedule/ **Policy Suite Outside Schedule** (schedule-based)	The policy suite enforced during scheduled hours and the policy suite enforced outside scheduled hours.
Device Connection Schedule	Select the Device Connection Schedule for the user.
LDAP Server	Policy suite, device connection schedule, and liability can be obtained from the LDAP group (highest priority group first) to which the user belongs. If the user does not have group membership, the folder (by folder hierarchy) to which the user belongs is the source for the settings. Regular periodic checks with the LDAP server will update user information and assignments if they change.
Liability	Liability refers to who owns the data on the device. Liability determines whether the corporate or individual component of the policy suite is assigned to the user. Choose *Corporate* (corporate liable) or *Individual* (individual liable).

Hands-Off Enrollment Defaults

Local Groups: If you specify one or more local groups to which users will be added when they enroll, policy suite, device connection schedule, and liability are obtained from the settings associated with the local group(s). Settings associated with local groups take precedence over settings associated with LDAP groups/folders. Changes made to local group settings will automatically update users.

Click the ***Import Local Groups*** button and select the group or group to which enrolling users will be added.

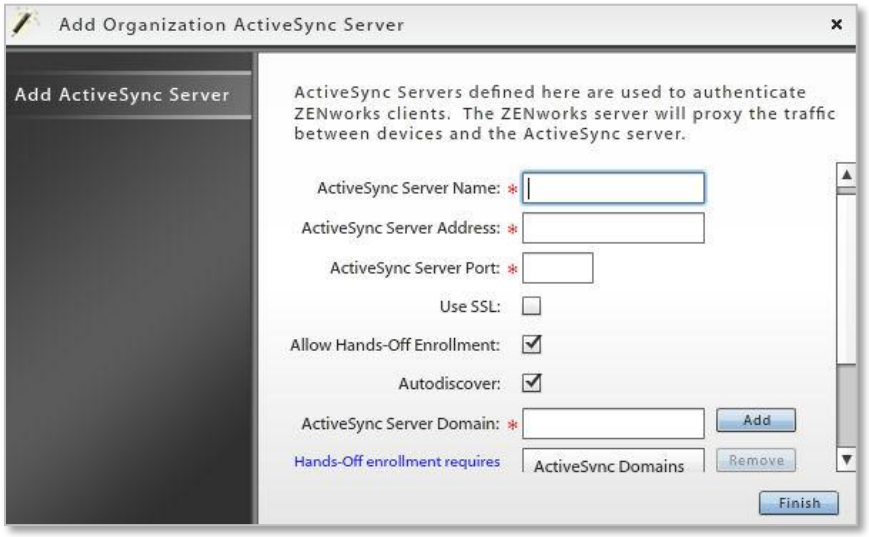
Enabling Hands-Off Enrollment for Users Associated with an ActiveSync Server

Enabling the *Hands-Off Enrollment* option, when defining an ActiveSync server, allows any user with credentials on the ActiveSync server to enroll against the *ZENworks Mobile Management* server. Hands-off enrollment will be set automatically for an ActiveSync server if it is set for a linked LDAP server.

You must also provide a domain that is configured on this server. Hands-off enrollment requires users to enroll with the domain in the **domain**\username or user@**domain** format. If an LDAP server is linked to this ActiveSync server, the LDAP server's domain can also be used for logging in.

Users are automatically added to the *ZENworks Mobile Management* server, as long as their credentials are recognized by the ActiveSync server. *ZENworks Mobile Management* creates the new account using the ActiveSync user account credentials and the user is auto-provisioned using preset organization default assignments or assignments associated with LDAP groups/folders or local groups.

1. From the *ZENworks Mobile Management* dashboard header, select ***Organization***.
2. From the drop-down menu, select ***Administrative Servers*** > ***ActiveSync Servers***.
3. From the left panel, select an existing ActiveSync server or create a new ActiveSync server by choosing ***Add ActiveSync Server***.
4. Select the box labeled ***Allow Hands-Off Enrollment*** and make sure you have specified at least one ***Domain*** for the server. You can enter multiple domains if necessary for your configuration.
5. Click ***Finish*** or ***Save Changes***.



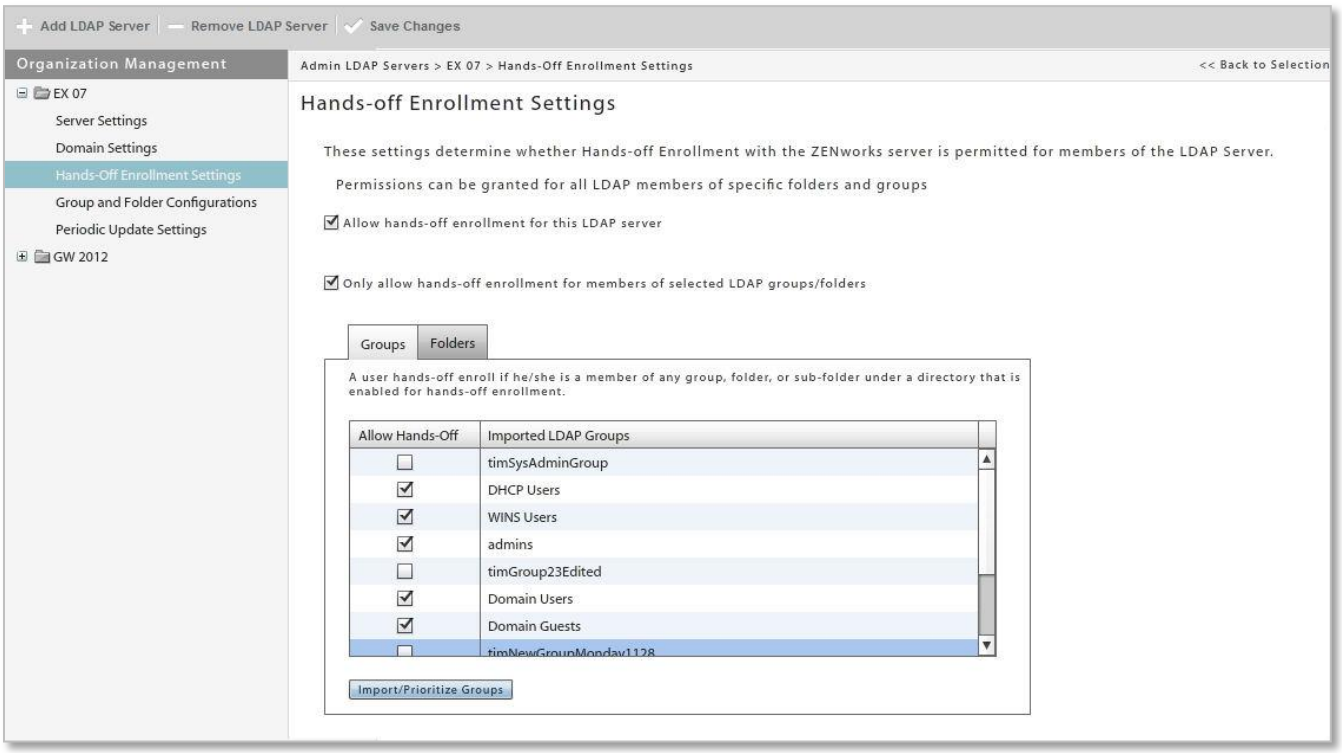
Enabling Hands-Off Enrollment for Users Associated with an LDAP Server

Enabling the *Hands-Off Enrollment* option, when defining an LDAP server, allows users with credentials on the LDAP server to enroll against the *ZENworks Mobile Management* server. Hands-off enrollment will be set automatically for an LDAP server if it is set for a linked ActiveSync server.

Users are automatically added to the *ZENworks Mobile Management* server, as long as their credentials are recognized by the LDAP server or an ActiveSync server associated with the LDAP server. *ZENworks Mobile Management* creates the new account using the user's LDAP account credentials and the user is auto-provisioned using preset organization default assignments or assignments associated with LDAP groups/folders or local groups.

You can allow hands-off enrollment for all users associated with the LDAP server or you can allow it only for selected LDAP folder/group members.

1. From the *ZENworks Mobile Management* dashboard header, select ***Organization***.
2. From the *drop-down* menu, select ***Administrative Servers*** > ***LDAP Servers***.
3. From the left panel, select an existing LDAP server or create a new LDAP server by choosing ***Add LDAP Server***.
4. Select the ***Hands-Off Enrollment Settings*** option. You can allow hands-off enrollment for all users associated with the LDAP server or limit it to selected LDAP folder/group members.



Enrolling Multiple Devices for a Single User

Users can enroll multiple devices with a single *ZENworks Mobile Management* user account. For example, a user might have a smartphone, but also use a companion device, such as a tablet or a second smartphone for foreign travel.

Multiple device enrollment is accomplished by creating an account on the *ZENworks Mobile Management* server and instructing the user to completely enroll one device at a time. Set a limitation for how many devices a user may enroll. Each device enrolled uses a licensed seat on the *ZENworks* server. Set an organization default for the maximum number of devices a user can enroll by selecting ***System*** > ***Organization***. Adjust the *Maximum Number of Devices Per User*. You can override the organization default on an individual user basis by setting a maximum in the user's profile. From the user grid, select a user and click the *User Profile* button. From the left panel select *User Information* and click the *Configuration* tab. Remove the checkmark from the *Auto* box and define the maximum number of devices the user can enroll.

Successful enrollment of multiple devices requires the following:

- Each device must be fully enrolled and complete its first synchronization before another device can be successfully enrolled.
- The user must enroll each device with the same Username, Password, Domain, Server Address, and SSL setting
- The account protocol used on each device associated with the user's account must be the same. For example:
    - **When the first device has the *ZENworks Mobile Management* app and an ActiveSync user account:**
        - Each device must be fully enrolled (have the *ZENworks Mobile Management* app enrolled and the ActiveSync account created and registered) before another device can be added.
        - All subsequently enrolled devices must have the *ZENworks Mobile Management* app and an ActiveSync user account.
    - **When the first device has an ActiveSync account only and does not have the *ZENworks Mobile Management* app:**
        - Each device must have the ActiveSync account created and registered against *ZENworks Mobile Management* before another device can be added.
        - All subsequently added devices must have only an ActiveSync account.

Administration of Multiple Devices

Each device appears as a separate line item in the *Users* grid. Sort the grid by the User Name column to see all devices associated with a single user.

Administrators can select any of a user's devices and view the User Profile associated with the item.

The administrator might change the following for any of a user's multiple devices.	**The administrator should not change the following, unless he/she is changing the information on all of the user's devices:**
Liability	First Name
Ownership	Last Name
Plan Type	Domain
Policy Suite	ActiveSync Server
Device Connection Schedule	Email Address
Carrier	LDAP Server

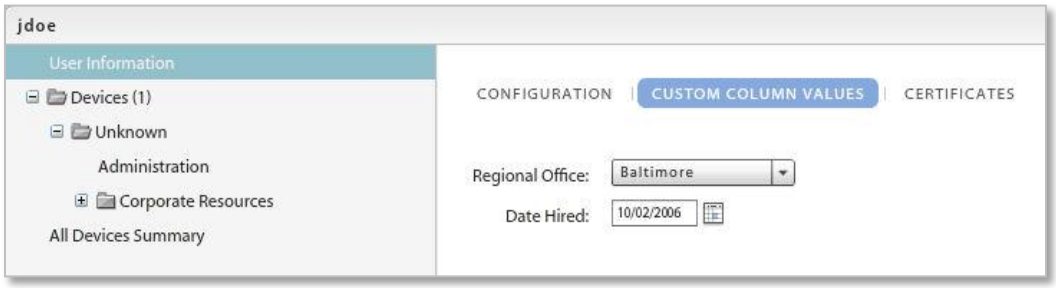
User Self-Administration

Users can view and manage all of their enrolled devices from the desktop or mobile User Self-Administration Portal.

Custom Columns

Administrators can create user information fields that are specific to their organization, but are not part of the *ZENworks Mobile Management* System base installation. These fields can then be viewed in the ***User Profile*** and can be displayed as columns in the user list.

There is a limit of ten Custom Columns for each organization. Information for the fields might be one of five types, including an LDAP type field, which will pull information from an Administrative LDAP server defined for the organization. The administrator must manually enter values for other field types. The field types are Text, Drop-down, Numeric, Date, and LDAP.



View of the Custom Columns in the User Profile

Adding Custom Columns

1. From the *ZENworks Mobile Management* dashboard header, select ***Organization***.
2. From the drop-down menu, select ***Organization Control*** > ***Custom Columns***.
3. Click the ***Add Custom Column*** option.
4. Select the ***Custom Column Type*** and the ***Custom Column Name***.
5. The *Type* you select determines the parameters you define for the field.

Type	Parameters
Text	Maximum number of alphanumeric characters.
Drop-down	Enter the choices that appear in a drop-down list.
Numeric	Minimum and maximum numeric values.
Date	None
LDAP	LDAP attribute and LDAP server (at least one must be defined for the organization). *ZENworks Mobile Management* checks the LDAP server daily and automatically applies any updates to custom column LDAP data. An individual user's LDAP data is updated automatically whenever his or her user profile is opened via the dashboard.

6. Click the ***Finish*** button to save.

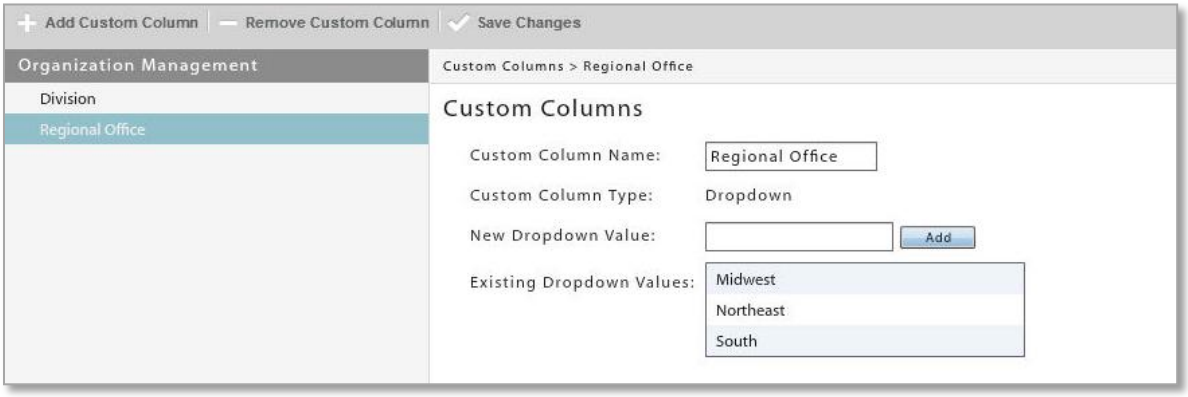
Modifying Custom Columns

Custom Columns can be modified after they are defined, but on a limited basis. For example, you cannot change the *Type* of the column, because this would prevent you from entering correct values in the future.

The administrator can modify custom columns in the following ways:

- Change the custom column name
- Add values to a drop-down type
- Decrease minimum values
- Increase maximum values

1. From the *ZENworks Mobile Management* dashboard header, select ***Organization***.
2. From the drop-down menu, select ***Organization Control*** > ***Custom Columns***.
3. Select the column you want to modify from the left panel and edit the name of the column or other parameters that are editable.
4. Click ***Save Changes***.



User Enrollment

The ZENworks Mobile Management App

Direct users to where they can obtain the *ZENworks Mobile Management* device application. The *ZENworks Mobile Management* app is available for Android, iOS, Windows Mobile 6.1/6.5, and Symbian S60 3rd Edition users.

BlackBerry 4.5-7.1 users can install the *NotifySync for BlackBerry* application, which interfaces with *ZENworks Mobile Management* and provides functionality comparable to the *ZENworks Mobile Management* app. (Requires a *NotifySync* license.)

BlackBerry 10, Windows Phone, and webOS users must enroll by creating an ActiveSync account on the device and specifying the *ZENworks Mobile Management* server in the server address.

ZENworks Mobile Management for iOS: App Store or Enterprise Version

The *ZENworks Mobile Management for iOS* device application is distributed via the Apple App Store. In accordance with Apple privacy regulations, however, App Store applications do not permit background processing to initiate a connection to a server for the purpose of tracking statistics. Thus, the *ZENworks Mobile Management* app obtained from the App Store requires iOS users to initiate synchronization of user/device statistics and location data by opening the application on a daily or more frequent basis.

Because Enterprise (proprietary, in-house) Applications do not fall under the same privacy regulations as App Store applications, organizations can opt to distribute the *ZENworks Mobile Management for iOS* device app as an Enterprise App. Applications distributed in this manner can run on a device in the background without user interaction.

Distributing the application as an Enterprise App requires that your organization maintain an annual Apple iOS Developer Enterprise Program (iDEP) membership. Novell, Inc. will work with organizations who want to pursue this solution. For information, see Distributing ZENworks for iOS as an Enterprise App.

ZENworks Mobile Management for iOS App Store Version Functionality

The functionality of *ZENworks Mobile Management for iOS* obtained through the App Store is outlined below. Recommendations for administrators and users are also included.

- The *ZENworks Mobile Management for iOS* device application cannot run in the background on a user's iOS device, so users should be instructed to open the *ZENworks Mobile Management* app on a daily basis and allow it to complete a synchronization cycle.
  Location and the following device statistics are not updated unless the device application synchronizes:
    - Battery/Charging Status
    - ZENworks App Version

- Downloaded Data (any network)
- Downloaded Data (cellular network)
- Downloaded Data (WiFi)
- GMT Offset
- Jailbroken
- Device UID
- ZENworks App Language
- OS Language
- Timezone
- Uploaded Data (any network)
- Uploaded Data (cellular network)
- Uploaded Data (WiFi)
- Last Device Boot Time (Device Local)

- Because Jailbroken status might not be regularly reported, the Compliance Manager setting that restricts jailbroken devices cannot be reliably enforced. You might want to disable this restriction.
- You might want to disable several Compliance Manager *Device Platform Restrictions* for iOS devices, to alleviate issues caused by infrequent *ZENworks* connections.
  - Restrict if policy out of date
  - Restrict if location not updated
  - Restrict user ZENworks connections

Devices without a ZENworks Mobile Management App

ActiveSync Only Devices

Devices for which a ZENworks device application is not yet available can still enroll with the *ZENworks Mobile Management* server. The devices must have an ActiveSync application. Devices supported for this type of enrollment include BlackBerry 10, webOS, and Windows Phone.

Functionality

Mobile device management functionality for these devices is limited to only the ActiveSync security policies supported by the device platform. Device statistics accessible via the *ZENworks* dashboard display limited information. In addition, there is no audit tracking or location data available for these devices.

Device statistics in the ***Users*** view for these devices are limited to:

- User Name
- Domain
- Active
- Policy Suite
- Device Connection Schedule
- Ownership
- Last ActiveSync Sync
- AS Version
- AS User Agent
- Device Type

Users with Android, iOS, Symbian S60 3rd edition, and Windows Mobile 6 devices should install the *ZENworks* app. Without the *ZENworks* app, these devices are limited to the functionality outlined above. Users with BlackBerry 4.5-7.1 devices should install *NotifySync for BlackBerry*. BlackBerry 4.5-7.1 devices do not have native ActiveSync capabilities and are not supported without the *NotifySync* app.

The ***Device Type*** field might display various descriptions based on the model of the device:

Platform	***Device Platform* column:**
BlackBerry 10	BlackBerry
webOS devices	Palm
Windows Phone devices	WP

Information on policy functionality: Device Platform Functionality

Instructions for other devices: ActiveSync Device Enrollment

iOS Configurator Devices

Apple Configurator is a tool that assists administrators in the deployment and management of iOS devices in business or education settings. It is well suited to environments where devices are often reassigned or where they are shared by multiple users. When integrated with *ZENworks Mobile Management*, the application is useful as a deployment tool since it provisions multiple devices quickly, enrolling them with the *ZENworks Mobile Management* server and staging each device with the appropriate MDM profiles.

Create an iOS Configurator Group profile and export it for use with the Apple Configurator. The *ZENworks Mobile Management* profile, once imported into the Configurator, can be used to quickly configure a fleet of mobile devices.

Select ***System*** > ***Organization***

Any device associated with the Configurator Group will appear on the *ZENworks Mobile Management* user grid with the Configurator Group name. Refer to the Apple Configurator Integration guide for details.