

Configuring Organizations, Device Connection Schedules, and Policy Suites

ZENworks® Mobile Management 2.9.x

May 2014

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 \(http://www.novell.com/info/exports/\)](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.

Copyright © 2012-14 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	4
Configuring the Organization	6
Organization Setup Wizard	6
Enter Organization Information and Set Parameters	7
Define the Organization's Default ActiveSync Server	8
Define the Organization's Default LDAP Server	9
Define the Organization's Default SMTP Server	15
Configure the Organization for OpenID Administrative Login	15
Create the Organization's Default Policy Suite	17
Create the Organization's Default Device Connection Schedule	18
Managing SMTP, ActiveSync, and Administrative LDAP Servers	19
Defining Additional Administrative LDAP or ActiveSync Servers	19
Editing Server Information	20
Configuring an Administrative LDAP Server	21
Configuring the Organization for Hands-Off Enrollment	24
Enabling Hands-Off Enrollment for Users Associated with an ActiveSync Server	27
Enabling Hands-Off Enrollment for Users Associated with an LDAP Server	28
Policy Suites	29
Creating a New Policy	30
Policy Suite Editor	31
Components of the Policy Suite	32
The Welcome Letter	32
Policy Suite Description and Notes	33
Policy Settings by Category	33
Tips on Customizing and Using Policy Suites	38
Device Connection Schedules	40
Create a Device Connection Schedule	40
Editing Device Connection Schedules	42
Tips on Using Device Connection Schedules	43
Policy Schedules	44
Create a Policy Schedule	44
Assign a Policy Schedule	46
Control Resources Users Access Outside Scheduled Hours	47

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
- Desktop computer 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.



Admin Setup Pin Code

Enter Admin Setup Pin Code

Zone Name

OpenID Identity

OK



Configuring the Organization

Organization Setup Wizard

The Organization Setup Wizard is a tool used to create an organization on the *ZENworks Mobile Management* server. The organization might be a company or a distinct group of individuals within a company. A single application of *ZENworks Mobile Management* software can accommodate just one organization or host multiple organizations.

Creating an organization is the first configuration task you must complete after installing the *ZENworks Mobile Management* server software. The wizard automatically appears the first time you log in to the dashboard. You will use the wizard to create any additional organizations as well.

Each organization consists of:

- Its users/devices
- One or more policy suites that enforce functionality settings and security settings for an organization's fleet of mobile devices
- One or more device connection schedules that govern when devices synchronize policy setting updates and send device statistics
- The configuration of the servers with which *ZENworks Mobile Management* interfaces, such as the ActiveSync, LDAP, and SMTP servers

Organization Setup Wizard tasks:

- Enter organization information.
- Define a default ActiveSync Server (if applicable) for the purpose of user authentication and hands-off enrollment.
- Define a default Administrative LDAP Server (optional) for the purpose of leveraging LDAP user information and the LDAP folder and group structure. This information can be used to authenticate users and administrators, control hands-off enrollment, and facilitate user information updates. Administrative LDAP servers can also be used for the purpose of adding users and administrators to the *ZENworks Mobile Management* server via batch imports and importing information into custom column fields.
- Define a default SMTP Server (required) for sending administrative email from the *ZENworks Mobile Management* server.
- Configuring *ZENworks Mobile Management* for administrative **OpenID** login
- Create a default Policy Suite for the organization.
- Create a default Device Connection Schedule for the organization.

The Organization Setup Wizard steps you through each of the above items.

Additional organization configuration steps include creating a welcome letter to be emailed to new users, configuring the Compliance Manager, and adding users.

See the following documentation on:

- [The Welcome Letter](#) (in this guide)
- [Compliance Manager](#)
- [Adding Users and Enrolling Devices](#)

Enter Organization Information and Set Parameters

The Organization Setup Wizard displays automatically when you log in to *ZENworks Mobile Management* for the first time. Before you create the first organization, you must enter your Customer Care Center credentials. You only have to enter these credentials when using the wizard for the first time.

You can also access the wizard via the dashboard.

1. From the *ZENworks Mobile Management* dashboard header, select **System**
2. From the menu panel, select **System Administration > Organizations**.
3. Click the **Add Organization** button.
4. Click **Next** to begin creating a new organization.

Enter the following:

- **Organization Name**
- **Organization Alias** – short name users will enter for OpenID login
- **Use Eval License** or enter a **ZMM License Key**
- **TD Volume License Key** (*TouchDown app*)
- **Contact Name**
- **Contact's primary and secondary email address**
- **Contact's primary and secondary phone number**

The screenshot shows the 'Organization Setup Wizard' window with a progress bar at the top indicating the current step is 'Organization'. The interface includes a sidebar with 'Organization' selected. The main area contains the following fields and options:

- Organization Name: *
- Organization Alias: *
- Use Eval License for ZMM:
- ZMM License Key: *
- TD Volume License Key:
- Contact Person's Name: *
- Contact's E-mail Address: *
- Contact's Secondary E-mail:
- Contact's Phone Number: * Ext:
Ex: 9875551234
- Contact's Secondary Phone: Ext:
- Send Welcome Letter to Users:
- Display EULA:

At the bottom right, there are 'Back' and 'Next' buttons.

- Choose whether you want to send an email **Welcome Letter** to users when they enroll their devices. The letter is associated with the policy suite assigned to the user. Compose or edit the letters via **Organization > Policy Management > Policy Suites**.
- Choose whether to display the **EULA** (*ZENworks Mobile Management* End User License Agreement) when users enroll their *ZENworks Mobile Management* app (recommended).
- Select the **Default Device Liability**. Select **Corporate** when liability for data on device rests with the corporation. Select **Individual** when liability rests with the individual carrying the device. Click **Next**.

Define the Organization's Default ActiveSync Server

ActiveSync Server (optional)

An ActiveSync server is not required, but for systems utilizing the ActiveSync protocol, ZENworks Mobile Management can act as a gateway server. An ActiveSync server allows hands-off enrollment of devices, reducing the amount of manual user configuration. In addition, users are authenticated via their ActiveSync server credentials. ActiveSync Email and PIM traffic are relayed to and from devices by ZENworks Mobile Management.

ActiveSync servers using protocol version 12.0 or greater should be configured to enable *Autodiscover* so that actual server address information can be discovered as users enroll.

Define the following ActiveSync server credentials and settings:

- ActiveSync Server Name -Use SSL
- ActiveSync Server Address -Allow Hands-Off Enrollment
- ActiveSync Server Port -ActiveSync Server Domain (*required for hands-off enrollment*)

The screenshot shows the 'Organization Setup Wizard' window, specifically the 'Servers' step. The 'ActiveSync Server' option is selected in the left-hand navigation pane. The main configuration area includes the following fields and options:

- ActiveSync Server Name: * [Text Input]
- ActiveSync Server Address: * [Text Input]
- ActiveSync Server Port: * [Text Input]
- Use SSL:
- Allow Hands-Off Enrollment:
- ActiveSync Server Domain: [Text Input] [Add] [Remove]

Below the domain field is a table with a header 'Domain' and an empty row. At the bottom right of the wizard are 'Back' and 'Next' buttons.

Defining ActiveSync Server Credentials for Hands-Off Enrollment

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. You must also provide a domain that is configured on this server. Hands-off enrollment requires users to enroll with the domain in one of the following formats: domain\username or user@domain.

If you are planning to link this ActiveSync server with an LDAP server, enabling hands-off enrollment will enable hands-off enrollment for the linked LDAP server as well. In such cases, the LDAP server domain can be used to hands-off enroll in addition to the ActiveSync server domains.

Users are automatically added to the *ZENworks Mobile Management* server when they enroll, as long as their credentials are recognized by the ActiveSync server. *ZENworks Mobile Management* creates the new account by using the ActiveSync user account credentials and the default servers, policy suite, and device connection schedule specified for the organization.

See also [Configuring the Organization for Hands-Off Enrollment](#) and [Managing SMTP, ActiveSync, and Administrative LDAP Servers](#)

Define the Organization's Default LDAP Server

Define a default **Administrative LDAP Server (optional)** for the purpose of leveraging LDAP user information and the LDAP folder and group structure. LDAP server functionality can be used to provision and authenticate users and administrators, update user information, and control who may use hands-off enrollment. In addition, an LDAP server can provide email addresses for the provisioning of users, when linked to an ActiveSync server where users do not have an email address ID (ActiveSync protocols less than v12.0, Data Synchronizer, Exchange 2003). Administrative LDAP servers can also be used to add users to the *ZENworks Mobile Management* server via batch import and import user information into custom column fields.

What you should know about LDAP server configuration

Some LDAP groups innately do not have the necessary attributes needed to be utilized for *ZENworks Mobile Management* LDAP searches and should not be used. An example of this type of LDAP group on an Exchange server is "Domain Users," which does not have a membership attribute.

Likewise, if an attribute value is entered incorrectly in the LDAP Server Settings, functionality will be hindered.

The values entered in the Administrative LDAP Server configuration for the following attributes determine which LDAP groups will facilitate a successful user or administrator enrollment. When groups do not have the necessary attributes, successful enrollment is impossible.

- User Identification Attribute
- Group Membership Attribute
- Group Object Class
- User Object Class

Any group that appears in LDAP server group lists can be imported, however, administrators should familiarize themselves with the LDAP server structure and verify that groups they choose for use with the *ZENworks Mobile Management* server contain the necessary attributes. They should also verify that they enter attribute values correctly in the Administrative LDAP Server configuration.

When inappropriate groups are chosen or an attribute value is entered incorrectly, hands-off enrollment for users and login/account creation for administrators in such a group will fail when the member search is unsuccessful.

Editing Attributes

Once users or groups have been imported for this LDAP server, the following fields cannot be edited:

Base DN, Group Object Class, and User Object Class

Define the LDAP Server Credentials and Settings

- LDAP Server Name
- LDAP Server Address
- LDAP Server Port
- Link with ActiveSync Server
- LDAP Server Domain
- LDAP E-mail Attribute
- LDAP User Firstname Attribute
- LDAP User Lastname Attribute
- LDAP User Identification Attribute
- LDAP Group Membership Attribute
- Use SSL
- Use TLS
- LDAP Username
- LDAP Password
- LDAP Base DN
- LDAP Group Object Class
- LDAP User Object Class

Possible Values for LDAP Server Settings

LDAP Server Setting	eDirectory	Active Directory	Lotus Notes
LDAP E-mail Attribute	mail	mail	mail
LDAP User First Name Attribute	givenName	givenName	givenName
LDAP User Last Name Attribute	sn	sn	sn
LDAP User Identification Attribute	uid	sAMAccountName	uid
LDAP Group Membership Attribute	member	member	member
LDAP Group Object Class	groupOfNames	group	groupOfNames
LDAP User Object Class	inetOrgPerson	user or organizationalPerson	person

Add Domains

Domain settings determine the server domain credentials with which users hands-off enroll or administrators log in to the dashboard. If the LDAP server is linked to an ActiveSync server, the domain defined for the ActiveSync will be used for hands-off enrollment and administrator login

If you intend to use the same LDAP server for multiple organizations on the *ZENworks Mobile Management* server, you will need to define a unique domain for each organization. This can be done here via the wizard, or at any time using the LDAP server editor.

The screenshot shows the 'Organization Setup Wizard' window, specifically the 'Servers' step. The wizard has a progress bar at the top with steps: Welcome, Organization, Servers (current), Policies, Schedules, and Finish. On the left is a sidebar menu with options: ActiveSync Server, LDAP Server, Add Domain (selected), Import/Prioritize Groups, Hands-Off Enrollment, Periodic Updates, SMTP Server, and OpenID. The main content area is titled 'Servers' and contains the following elements:

- Linked ActiveSync Server:** A section with the text 'Used for hands-off enrollment and administrator log in'. It contains a table with one row: 'ActiveSync Domains' and 'AS11'.
- Are additional domains needed for users that you split into multiple MDM organizations?** A checkbox that is checked.
- Additional Domains:** A section with the text 'Used for hands-off enrollment and administrator log in'. It features an input field, an 'Add' button, a table with one row: 'Additional Domains' and an empty cell, and a 'Remove' button.
- Navigation:** 'Back' and 'Next' buttons at the bottom right.

Import/Prioritize Groups

Groups from the LDAP server are displayed in the left column of this page. Groups that you select to add to the right column will be imported into the *ZENworks Mobile Management* dashboard in the following areas:

- LDAP server editor: *Hands-Off Enrollment Settings*
- LDAP server editor: *Group and Folder Configurations*
- User Grid: *LDAP Folders* view

The groups imported here contain only users. Administrator groups must be imported from the *Organization Administrators* page or *System Administrators* page.

Groups to which users belong are also imported automatically when users are added manually, via a .CSV batch import, or via an LDAP batch import.

Choosing Groups. Administrators should familiarize themselves with the LDAP server structure and verify that groups they choose for use with the *ZENworks Mobile Management* server contain the following necessary attributes: User Identification Attribute, Group Membership Attribute, Group Object Class, and User Object Class. Groups without these attributes should not be used.

Prioritizing Groups. Prioritizing groups need only be done when there are users that belong to multiple groups. The group with the highest priority will determine the user's policy suite, device connection schedule, liability, and corporate resource assignments. . Select a group and use the **Priority** arrows or drag and drop a group to adjust the group's rank.

A user's assignments can be pulled from several sources. The sources are consulted in the following order:

1. Direct assignments applied to the user's record by an administrator (LDAP updates do not affect these assignments.)
2. The group(s) to which the user belongs – the user's highest priority group is consulted first
3. The folder to which the user belongs (by folder hierarchy)
4. Organization defaults

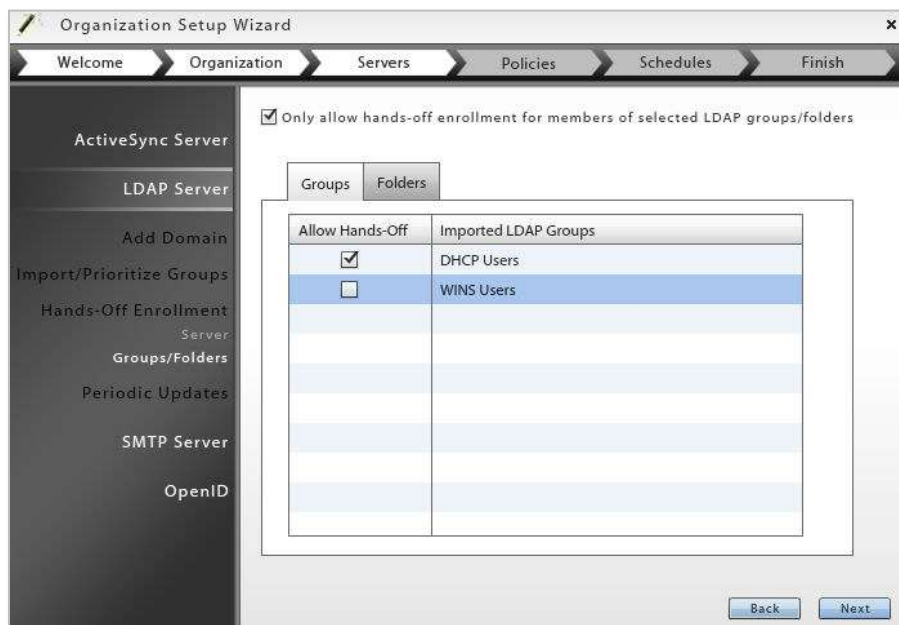
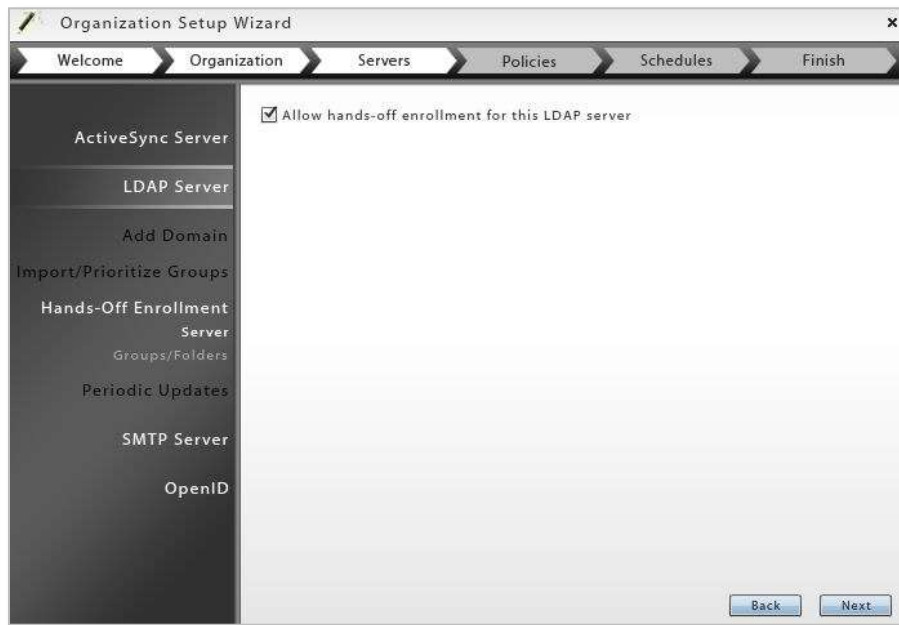
A Prioritization Example. John Doe belongs to the *SalesTeam* group and the *Management* group. The *Management* group has a higher priority, thus any policy suite, device connection schedule, liability, or iOS resource assignments associated with the *Management* group will be assigned to John. If any of these assignments are not defined for the *Management* group, John will get assignments from those defined for the *SalesTeam* group. If an assignment is not defined in either of the groups, it can then be pulled from the LDAP folder to which John belongs, or finally, from the organization defaults. An administrator can also override all these prioritized assignments by manually making direct assignments to John's record.



Hands-Off Enrollment

Configure the LDAP server to allow hands-off enrollment for all LDAP users or for users who are members of selected LDAP groups or folders. If the LDAP server is linked to an ActiveSync server that is configured for hands-off enrollment, hands-off enrollment is enabled for the LDAP server as well.

- Enable the *Allow hands-off enrollment for this LDAP server* option. Click **Next**.
- To limited the ability to hands-off enroll to certain LDAP groups or folders, enable the option, *Only allow hands-off enrollment for members of selected LDAP groups/folders*, then select the groups/folders to which users who may hands-off enroll belong.



Periodic Updates

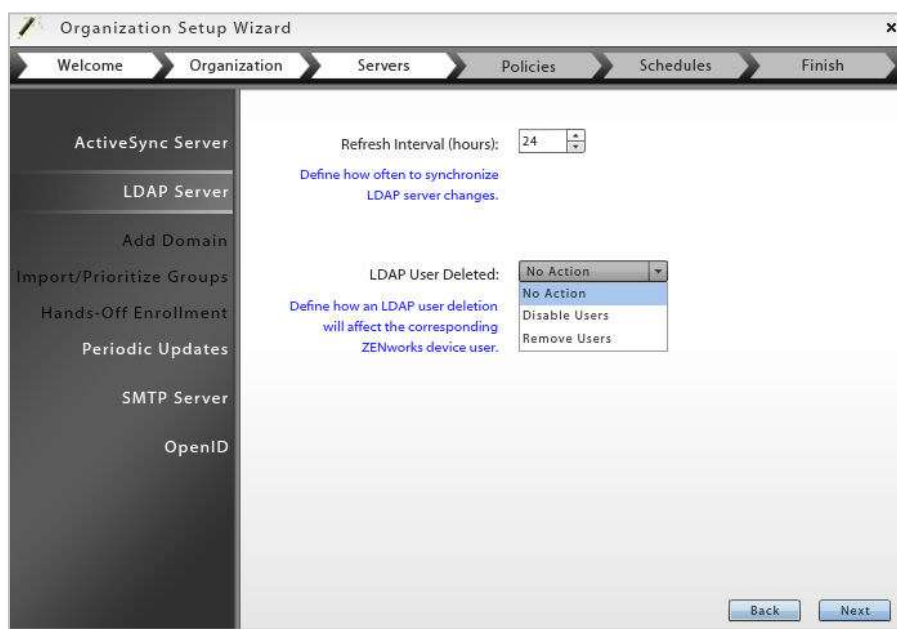
ZENworks Mobile Management regularly accesses the LDAP server to retrieve updates to groups, folders and user information. Users whose folder or group membership changes will be updated with the associated policy suite, connection schedule, and liability assignments of the new group or folder. Similarly, an LDAP authenticated administrator whose group membership has changed will get a role assignment from the new group to which he/she belongs.

Users who have direct policy suite, connection schedule, and liability assignments that override default assignments are not affected by periodic LDAP updates.

- Set the **Refresh Interval** to define how often to synchronize LDAP server changes.
- **LDAP User Deleted** - Define how the *ZENworks Mobile Management* server should handle users that have been deleted on the LDAP server. You can choose to leave the user untouched, disable the user (leave the user on the ZENworks server, but block resources), or remove the user from the ZENworks server.

When no action is taken or the user is disabled, the user retains the settings assigned via the LDAP group/folder.

- Administrators will always be deleted when the group to which they belong is deleted.



Once the LDAP server configuration is completed, this page will display an **Update Now** button which can be used to initiate an update outside the scheduled interval.

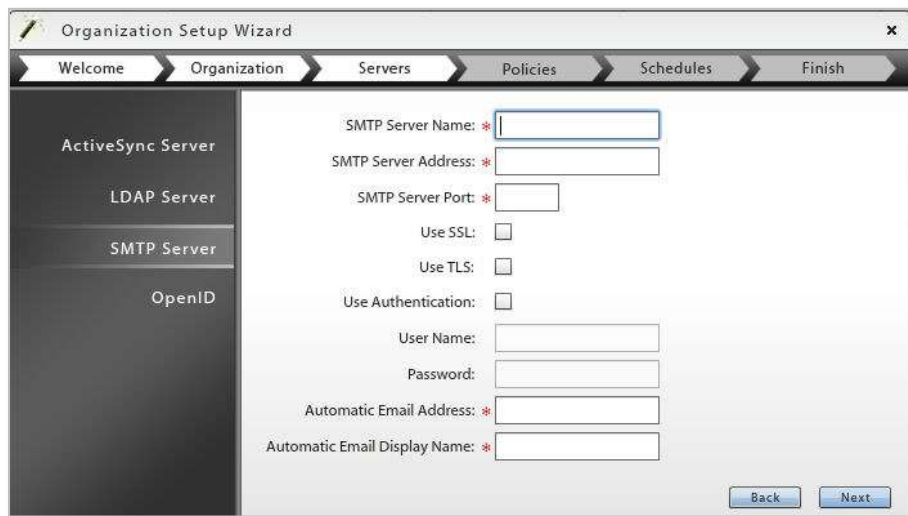
Define the Organization's Default SMTP Server

SMTP Server

ZENworks Mobile Management uses the SMTP server defined here to send administrative email and to send email generated from Group Emailing, Welcome Letters, security command confirmations, etc.

Define the following SMTP server credentials and settings:

- SMTP server name -Use Authentication
- SMTP server address -Username
- SMTP server port -Password
- Use SSL -Automatic Email Address
- Use TLS -Automatic Email Display Name



The screenshot shows the 'Organization Setup Wizard' window. The 'Servers' tab is selected in the top navigation bar. On the left sidebar, 'SMTP Server' is highlighted. The main area contains the following fields and options:

- SMTP Server Name: *
- SMTP Server Address: *
- SMTP Server Port: *
- Use SSL:
- Use TLS:
- Use Authentication:
- User Name:
- Password:
- Automatic Email Address: *
- Automatic Email Display Name: *

At the bottom right, there are 'Back' and 'Next' buttons.

Configure the Organization for OpenID Administrative Login

(optional)

OpenID is an open standard that allows administrators to login and authenticate using an outside source. The organization wizard gives you an opportunity to define the OpenID provider settings for Organization Administrators.

Define the following:

1. Select a **Predefined Provider** – *Facebook, Google, Yahoo!, or ZENworks*
2. If you chose *ZENworks* as the provider, enter the following:
 - **Zone** - enter a friendly name for the Provider URL. Administrators use this at login to access the provider. If there are other organizations on the server or you are defining a provider for both organization and system administrators, this name must be unique.

The *Zone* name is emailed to the administrator along with a PIN code they will use the first time they log in with OpenID credentials.

- **OpenID Provider URL** - enter the URL of the ZENworks Primary Server in the following form: **Error! Hyperlink reference not valid.**
3. At the **OpenID Return URL** field, enter the URL of the server to which the user is returned after successful provider validation. The default is the current *ZENworks Mobile Management* server URL.

The screenshot shows the 'Organization Setup Wizard' window. The 'Organization' step is active, and the 'OpenID' section is selected in the left sidebar. The main area displays the following configuration fields:

- Organization Alias: ABC
- Predefined Providers: * ZENworks (dropdown menu)
- Zone: * (empty text box)
- OpenID Provider URL: * (empty text box)
- OpenID Return URL: * https://192.168.2.10 (text box)

Below the OpenID Return URL field is a 'Use Default' button. At the bottom right of the wizard are 'Back' and 'Next' buttons. In the left sidebar, under the 'OpenID' section, there is a checked checkbox labeled 'I have an OpenID provider'.

Create the Organization's Default Policy Suite

You need to create a default policy suite for the organization. Other policy suites can be created later to accommodate different groups of users. The default policy suite is automatically assigned to users added to the system via hands-off enrollment. For additional information, see [Policy Suites](#).

Define a policy name for the organization's default policy suite.

Set corporate policy strength (policy for devices that the company is responsible for).

Set individual policy strength (policy for devices that individuals are responsible for).

- **Low** - No options are restricted on the device. Passwords can be simple.
- **Moderate** - No options are restricted on the device. Passwords are strong and password expiration is enforced.
- **Strict** - Requires an alphanumeric password and encryption on the device and storage card.
- **High** - Browser and camera are disabled. Requires alphanumeric password and encryption on the device and storage card.



To customize the default policy or create additional policies, use the **Policy Management > Policy Suites** option on the *Organization* page.

Create the Organization's Default Device Connection Schedule

You need to create a default device connection schedule for the organization. Other schedules can be created later to accommodate different groups of users. Device connection schedules dictate peak and off-peak times for devices to synchronize. Times can overlap days to cover different work shift situations and special case employees. The default device connection schedule is automatically assigned to users added to the system via hands-off enrollment. For additional information, see [Device Connection Schedules](#).

Define a schedule name for the organization's default schedule.

Set a corporate device connection schedule (schedule for devices that the company is responsible for).

Set an individual device connection schedule (schedule for devices that individuals are responsible for).

Define the following settings:

Corporate

Monday through Sunday peak connect times

Peak Connect Interval

Require Direct Push for Peak Times

Off-peak Connect Interval

Require Direct Push for Off-peak Times

Individual

Monday through Sunday peak connect times

Peak Connect Interval

Require Direct Push for Peak Times

Off-peak Connect Interval

Require Direct Push for Off-peak Times

Regulating the interval at which devices synchronize should be considered carefully to minimize the device battery depletion.

The times you define in the schedule grid designate peak connection times.

Anything that falls outside the peak schedule is off-peak connection time.

Organization Setup Wizard

Welcome Organization Servers Policies Schedules Finish

Assign a Name

Corporate Schedule

Individual Schedule

Times extending into next day are allowed, but the next day's start time must be after the preceding day's end time.

Define Corporate Peak Connection Times

Monday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Tuesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Wednesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Thursday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Friday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Saturday	<input type="checkbox"/>	8:00 AM	to	5:00 PM
Sunday	<input type="checkbox"/>	8:00 AM	to	5:00 PM

Peak Connect Interval: 30 minutes

Off-peak Connect Interval: 60 minutes

Require Direct Push for Peak Times

Require Direct Push for Off-peak Times

Back Next

To edit the default schedule or create additional schedules, use the **Policy Management > Device Connection Schedules** option on the *Organization* page.

Managing SMTP, ActiveSync, and Administrative LDAP Servers

You can define multiple administrative LDAP or ActiveSync servers for an organization, in addition to the servers you defined through the Organization Wizard.

You can also edit information for the administrative LDAP, ActiveSync, or SMTP servers defined through the Organization Wizard.

Administrators will use the LDAP editor to configure LDAP group and folder provisioning assignments

Server Function in the ZENworks Mobile Management Environment

SMTP Server – *ZENworks Mobile Management* uses this server to send administrative email and to send email generated from group emailing, welcome letters, security command confirmations, etc.

ActiveSync Servers – (Optional) With an ActiveSync server defined, *ZENworks Mobile Management* acts as a gateway server relaying email and PIM traffic to and from devices. Users are authenticated via their ActiveSync server credentials. The server can be configured to allow hands-off enrollment. ActiveSync servers using protocol version 12.0 or greater should be configured to enable Autodiscover.

Administrative LDAP Servers defined here are for the purpose of leveraging LDAP user information and the LDAP folder and group structure. LDAP server functionality can be used to authenticate users and administrators, update user information, and control who may use hands-off enrollment.

Administrative LDAP servers can also be used to add users to the ZENworks Mobile Management server via batch import and import user information into custom column fields. In addition, an LDAP server can provide email addresses for the provisioning of users, when linked to an ActiveSync server where users do not have an email address ID (ActiveSync protocols less than 12.0, Data Synchronizer, Exchange 2003).

See the following for further information:

- In this guide, [Configuring an Administrative LDAP Server](#)
- [Adding Users, Enrolling Devices Guide: Adding Users via LDAP, Custom Columns](#)
- [System Administration Guide: Creating Administrator Logins](#)

Note: LDAP servers defined under *iOS Corporate Resources* are for the purpose of configuring LDAP settings to make available to iOS device users. When users synchronize the settings, the device is automatically enabled for accessing corporate directory information.

Defining Additional Administrative LDAP or ActiveSync Servers

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the *drop-down* menu, select **Administrative Servers**, then select **ActiveSync Servers** or **LDAP Servers**.
3. Click the **Add ActiveSync Server** or **Add LDAP Server** option.
4. Enter the server credentials and configure the server, then click **Save Changes**.

LDAP TIP: To limit the number of unnecessary folders/groups pulled from the LDAP server, enter 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.

Editing Server Information

To edit credentials for an existing Administrative LDAP, ActiveSync, or SMTP server:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the *drop-down* menu, select Administrative Servers, then select **ActiveSync Servers** or **LDAP Servers**, or **SMTP Server**.
3. For LDAP or ActiveSync servers, select the server you want to edit from the left panel.
4. Edit the information and click **Save Changes**.

Server Connection Testing

Use the **Test Now** button on the server editing screens to test the connection from *ZENworks Mobile Management* to an Administrative LDAP, ActiveSync, or SMTP server after you have initially added it or if you suspect there is a connection problem.

Server	Tests:	Credentials entered for the test
Administrative LDAP Server	-Connectivity between the <i>ZENworks Mobile Management</i> server and the Administrative LDAP server; -Verifies that required LDAP attributes contain values	None – uses the credentials on file
ActiveSync Server	-Connectivity between the <i>ZENworks Mobile Management</i> server and the ActiveSync server; -Accessibility by an authorized user; -Autodiscover	A set of active user credentials in the format required by the ActiveSync server.
SMTP Server	-Connectivity between the <i>ZENworks Mobile Management</i> server and the SMTP server; -Authentication if <i>Use Authentication</i> is enabled; -Email delivery	None Optional email delivery test: Provide a test email address, subject, and message body

Configuring an Administrative LDAP Server

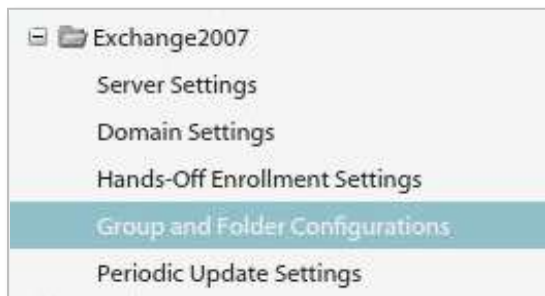
When the LDAP server is fully configured, users associated with an LDAP folder or group can be provisioned automatically when added to *ZENworks Mobile Management* manually, via a batch import, or through hands-off enrollment. This is done by associating each LDAP folder or group with a Policy Suite, Device Connection Schedule, and Liability status. Users are automatically assigned the settings associated with the group or folder to which they belong when they are added.

In addition, changes made to folders and groups will automatically update user information via periodic queries of the LDAP server.

An Administrative LDAP Server might have been added through the *Organization Setup* wizard or through the *Add LDAP Server* wizard. However, adding provisioning assignments to LDAP groups and folders must be done through the LDAP server editor using the *Group and Folder Configuration* option.

To edit an Administrative LDAP server:

1. Select **Organization** from the *ZENworks Mobile Management* dashboard header.
2. From the *drop-down* menu, select **Administrative Servers > LDAP Servers**.
3. Select the server you want to edit from the left panel and expand its menu. You can edit:
 - Server Settings – see [Define the LDAP Server Credentials and Settings](#)
 - Domain Settings – see [Add Domains](#)
 - Hands-Off Enrollment Settings – see [Hands-Off Enrollment](#)
 - Group and Folder Configurations – see below, [Group and Folder Configurations](#)
 - Periodic Updates Settings – see [Periodic Updates](#)



Group and Folder Configurations

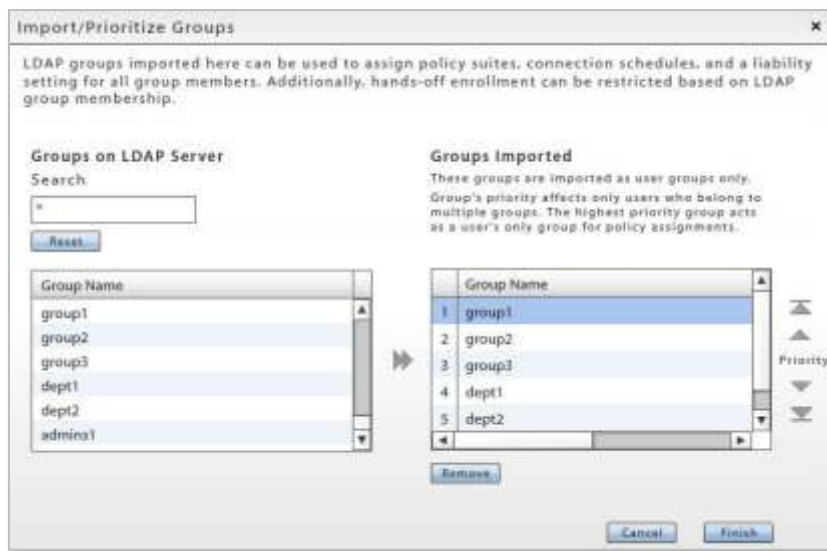
Import LDAP groups into the grid, using the **Import/Prioritize Groups** button.

Any group in the grid:

- can be configured with Policy Suite, Device Connection Schedule, and Liability assignments
- can be prioritized
- is also added to the Hands-Off Enrollment Settings grid

Import Groups. Select a group from the left panel and click the double arrow to designate it as a group to import. You can prioritize the groups here or from the grid. Click **Finish** to return to the grid.

Administrators should familiarize themselves with the LDAP server structure and verify that groups they choose for use with the *ZENworks Mobile Management* server contain the following necessary attributes: User Identification Attribute, Group Membership Attribute, Group Object Class, and User Object Class. Groups without these attributes should not be used.



Prioritize Groups. Prioritizing groups is only necessary when there are users that belong to more than one group. If users only belong to one group, priority does not affect user assignments. See also [Import/Prioritize Groups](#). Select a group and use the **Priority** arrows or drag and drop a group to adjust the group's rank.

Groups
Folders

Select a group to make or edit Policy Suite, Connection Schedule, or Liability assignments. Click to Adjust priority button to change group priorities. Priorities determines settings when a user belongs to more than one group.

Priority	Imported LDAP Groups	Policy Suite	Connection Schedule	Liability	
1	group1	<Not Assigned>	<Not Assigned>	<Not Assigned>	
2	group2	<Not Assigned>	<Not Assigned>	<Not Assigned>	▲
3	group3	<Not Assigned>	<Not Assigned>	<Not Assigned>	▲
4	dept1	<Not Assigned>	<Not Assigned>	<Not Assigned>	▼
5	dept2	<Not Assigned>	<Not Assigned>	<Not Assigned>	▼
					▼
					▼

Import/Prioritize Groups

Configure the group with setting assignments. Click the *Groups* or *Folders* tab and browse through the list to locate the group or folder you want to configure. Select a group or folder. Select Policy Suite, Connection Schedule, Liability assignments, and a Novell Filr profile* (if applicable). The Blacklist or Whitelist associated with the Policy Suite will display as well. Click *Save Changes*.

* Users of Android devices not using Google Cloud Messaging (GCM) service must synchronize the *ZENworks Mobile Management* application to pull down an assigned Novell Filr profile.

Tip: When you make changes to the assignments, you may want to initiate a synchronization with the LDAP server as well, if the scheduled *Periodic Update* will not occur for several hours. This way you will coordinate the changes you have made on the *ZENworks Mobile Management* server with any changes that may have occurred on the LDAP server. Initiate an update by using the **Update Now** button on the *Periodic Update Settings* page.

These assignments can also be made directly from the user grid. See the [Organization Administration Guide](#).

The screenshot displays the configuration page for a group named 'CAS'. The settings are as follows:

- Group Name: CAS
- Policy Enforcement Type: Schedule-Based
- Policy Schedule: General Staff
- Policy Suite During Schedule: Policy A
- Policy Suite Outside Schedule: Policy B
- Connection Schedule: Default
- Liability: Unknown (selected)
- Novell Filr: Filr Profile1

The 'Whitelists/Blacklists: Policy B' window shows the following settings:

	Corporate	Individual
Blacklists		
Default	Yes	Yes
Whitelists		
Default	No	No

How a user's settings are determined. A user's individual settings are determined by consulting the following sources in this order:

- any direct assignments
- any assignments made to the user's highest priority group (lower priority groups are consulted if there is no associated assignment)
- any assignments made to the user's folder (the folder closest to the user in the folder hierarchy is consulted first)
- organization defaults if none of these have associated assignments

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 or folders. 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 who 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.

If the ActiveSync server is linked to a fully configured LDAP server, however, users who exist on the LDAP server need not enroll using the full email address, as the LDAP server is queried for this information.

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:

Organization Defaults

Policy Enforcement Type: Standard Schedule-Based

Policy Suite: * d

Device Connection Schedule: * d

LDAP Server: None

Liability: Corporate Individual

Hands-Off Enrollment Defaults

Local Groups: [Import Local Groups](#)

Organization Defaults

Policy Enforcement Type: Standard Schedule-Based

Policy Schedule: * General Staff

Policy Suite During Schedule: * Default

Policy Suite Outside Schedule: * Policy A

Device Connection Schedule: * Default

LDAP Server: EX03

Liability: Corporate Individual

Hands-Off Enrollment Defaults

Local Groups: [Import Local Groups](#)

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. <i>Standard</i> 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 (<i>Standard</i>) Policy Suite for the user. (This field is not displayed if you choose <i>Schedule-Based</i> 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 <i>Corporate</i> (corporate liable) or <i>Individual</i> (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 one of the following formats: **domain\username** or **user@domain**. 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 by using the ActiveSync user account credentials and the user is auto-provisioned using preset organization default assignments or assignments associated with local groups or LDAP groups/folders.

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**.

', 'Allow Hands-Off Enrollment: ', 'Autodiscover: ', and 'ActiveSync Server Domain: *' (text input). At the bottom right are 'Add', 'Remove', and 'Finish' buttons. A section labeled 'Hands-Off enrollment requires' contains a text input for 'ActiveSync Domains' and a 'Remove' button."/>

Add Organization ActiveSync Server

Add ActiveSync Server

ActiveSync Servers defined here are used to authenticate ZENworks clients. The ZENworks server will proxy the traffic between devices and the ActiveSync server.

ActiveSync Server Name: *

ActiveSync Server Address: *

ActiveSync Server Port: *

Use SSL:

Allow Hands-Off Enrollment:

Autodiscover:

ActiveSync Server Domain: *

Hands-Off enrollment requires: ActiveSync Domains

Add Remove Finish

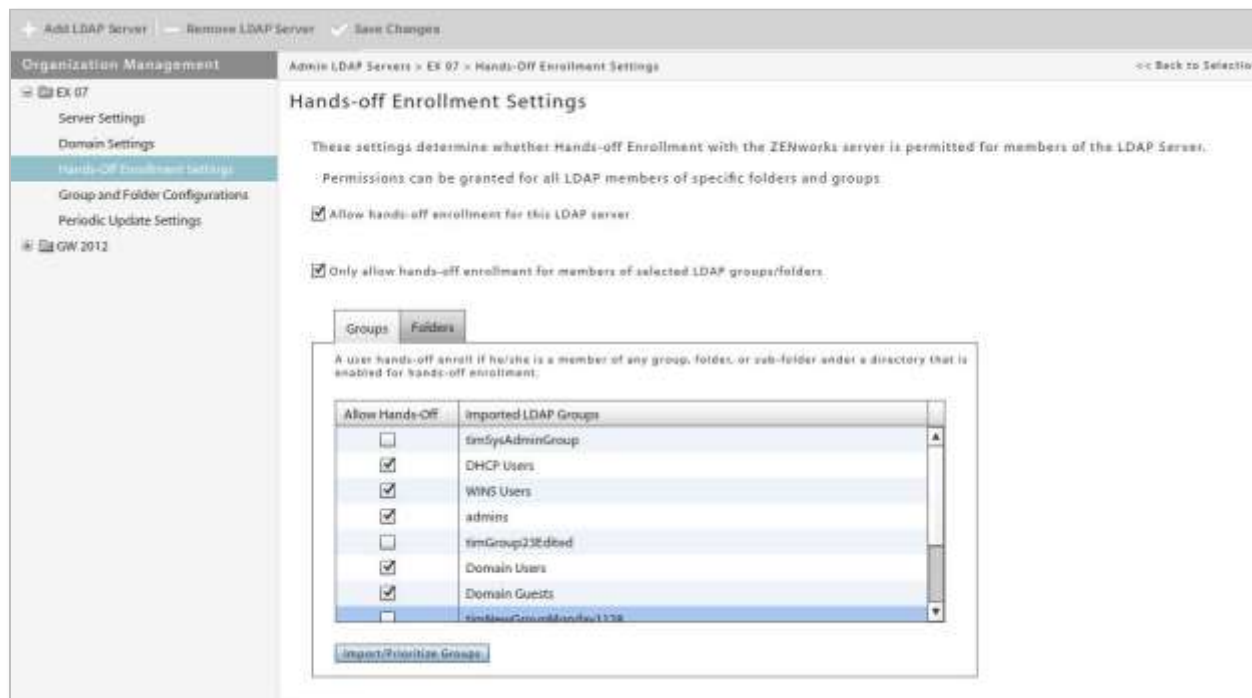
Enabling Hands-Off Enrollment for Users Associated with an LDAP Server

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 local groups or LDAP groups/folders.

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 folders/groups members.



Policy Suites

A policy suite is a set of rules and permissions that enforce an organization's security and usage standards for mobile devices in the enterprise. The policy suite is a key element of the *ZENworks Mobile Management* system. It enables administrators to manage users operating on a variety of device platforms and to enforce policies across those device platforms as consistently as possible.

ZENworks Mobile Management currently supports mail/PIM servers operating with ActiveSync protocol versions 2.5, 12.0, 12.1, 14.0, or 14.1. A handful of the *ZENworks Mobile Management* policies, however, are not supported on systems with less than version 12.0. This information, descriptions of individual policy settings, and functionality of settings across device platforms can be found in the [Device Platform Functionality](#) tables. Information about the policies is also available via the tool tips in the dashboard user interface.

The Policy Wizard guides you through setup of an organization's policy suites, which includes settings for both corporate and individual users/devices. The Wizard allows an administrator to quickly create a new policy suite either by copying an existing policy suite or by choosing from a number of pre-defined policy suite templates which reflect four levels of security strength. The administrator can start with one of these templates and use the Policy Suite Editor to customize the settings associated with any of the policy rules.

Multiple policy suites can be created to accommodate different groups of users. Each user/device can be assigned the policy that best suits their role. See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

ActiveSync Policies. For enterprises utilizing the ActiveSync protocol, *ZENworks Mobile Management* acts as a gateway server. *ZENworks Mobile Management* intercepts policy updates sent from the ActiveSync server and instead enforces ActiveSync policy settings that have been defined in *ZENworks Mobile Management*. When an ActiveSync server is not part of the enterprise, *ZENworks Mobile Management* itself acts as an ActiveSync server and enforces ActiveSync policies.

Welcome Letter. You can also draft a Welcome Letter that is emailed to users associated with a particular policy suite. In the organization setup, you can enable a setting that issues the letter automatically when the user is added to the system. You can leave this setting disabled and issue the letter manually for each user from the user's profile.

Policy rules are categorized into the following groups:

- Audit Tracking
- Device Control
- File Share Permission
- iOS Devices
- Managed Apps Permissions
- Resource Control
- Security Settings
- S/MIME Settings
- TouchDown
- Whitelists/Blacklists Permissions

Creating a New Policy

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**
2. From the drop-down menu, select **Policy Management > Policy Suites** icon.
3. Click the **Create New Policy** option.
4. Choose a method for creating a policy suite:
 - Create the initial policy suite by using sliders to determine its general policy strength (low, recommended, strict, high security).
 - Create the initial policy suite by copying the settings of an existing policy suite.
5. Use the Policy Suite Editor to customize the new policy.



Policy Suite Editor

To edit an existing policy suite:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the drop-down menu, select **Policy Management > Policy Suites** icon.
3. From the menu panel, select the policy you want to change.
4. Edit the Welcome Letter. Enter information that you want to email to new users when they are added to the *ZENworks Mobile Management* system. This can include a welcome to the system, information about policies, links to resources, etc.
 - To have the letter sent automatically when users are added, enable the setting in *Organization Settings*. From the dashboard, select **System > Organization** and select the **Send Welcome Letter to Users** option.
 - To issue the letter as needed for each user, leave the *Organization Settings* option disabled. Then, select **Users** and highlight a user. Click the **Send Welcome Letter** option in the *User Detail* panel.
5. Select the category you want to edit.
6. Edit the settings and click **Save Changes**.



See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

Descriptions of individual policy settings and functionality of the settings across device platforms can be found in the [Device Platform Comparison](#) tables.

Components of the Policy Suite

The Welcome Letter

For each policy you create, you can compose a new user Welcome letter that can communicate information to users when they are added to the *ZENworks Mobile Management* system. You might include information about:

- 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

Welcome Letters can be configured to email automatically or you can manually email them as needed.

To 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 enable the **Send Welcome Letter to Users** option.

To manually send the letter to an individual user, select **Users** and highlight a user. Click the **Send Welcome Letter** option in the *User Panel*.

To edit the letter, select **Organization > Policy Management > Policy Suites**, highlight a policy, and select the **Welcome Letter** option in the left panel.

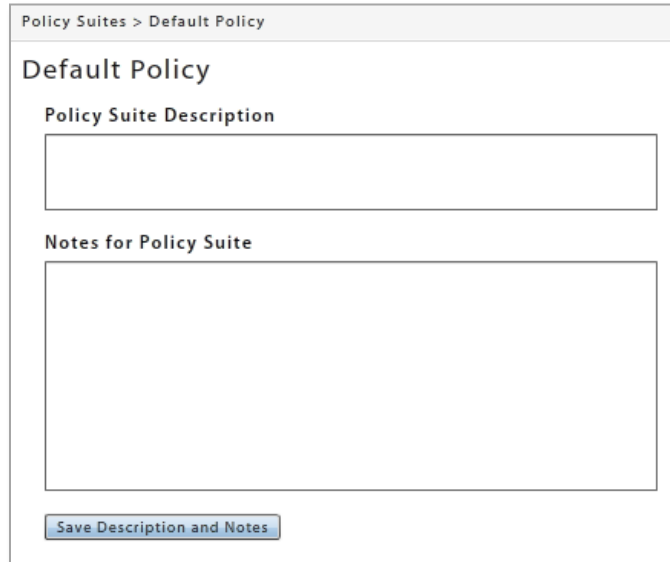
The screenshot shows a web interface for configuring a Welcome Letter. The breadcrumb path is "Policy Suites > Default Policy > Welcome Letter". The page title is "Welcome Letter". Below the title is a descriptive sentence: "This is the welcome letter that will be sent to a new user belonging to this policy suite." The form contains several fields: "Sender Name" with the value "ZENworks Mobile Management Admin", "Sender Address" with "admin@novell.com", and "Subject" with "Welcome to ZENworks Mobile Ma". The "Body" field is a large text area containing the following text: "Welcome to the ZENworks Mobile Management service. All links to device applications and documentation for setting up your device can be found at www.novell.com/documentation/zenworksmobile2. Device applications can be found under the 'Downloads' section, 'Device Application Downloads.' Device documentation can be found under the 'Documentation' section, 'ZENworks Mobile Management Device Apps.'".

See also, [Adding Users and Enrolling Devices](#): *Welcome New Users to ZENworks Mobile Management*.

Policy Suite Description and Notes

Use the **Description** field to provide more details about the purpose of the policy.

Use the **Notes** field for keeping a record of changes made to a policy.



Policy Suites > Default Policy

Default Policy

Policy Suite Description

Notes for Policy Suite

Save Description and Notes

Policy Settings by Category

Descriptions of individual policy settings and functionality of the settings across device platforms can be found in the [Device Platform Comparison](#) tables.

See the [Default Policy Settings](#) document for a comprehensive list of the policy suite rules and their default settings.

Audit Tracking

This option provides rules that enable tracking of information about device usage (Managed and unmanaged apps, phone and text message logs, device file list archive) and location.

Examples: Phone and text message logs, GPS tracking statistics

Location Data and GPS Location Accuracy Recording the location of devices can increase battery consumption. Administrators can adjust GPS location accuracy to offset this.

There are six accuracy levels with 1 being the least accurate and consuming the least battery power and 6 being the most accurate and consuming the most battery power. The function of these levels varies based on the device platform, as described in the table below. The accuracy level can be customized by choosing the positioning method and distance. Distance denotes the distance traveled before the device synchronizes a new location.

Note: [Symbian S60.3](#) devices do not support location accuracy; however, users can choose the positioning technology on the device by selecting *Settings > General > Positioning > Positioning Methods*. Choices are Bluetooth GPS, Assisted GPS, Integrated GPS, or Network Based (Cell

Towers). Windows Mobile devices partially support location accuracy. The positioning method can be set, but distance requirements are not supported.

Android devices differ across models in how often they detect location. *ZENworks Mobile Management* regulates this by updating at least once per device connection interval with a minimum of ten minutes.

Location Accuracy Functionality by Device Platform

Level	Android	BlackBerry (w/ GO!NotifySync)	iOS Devices	Windows Mobile 6
1	Cell towers only; approximate location, low power, 1000 meters distance	Cell towers only; low power, no set accuracy	Cell towers only (Levels 1, 2, 3 are the same)	Cell towers only (Levels 1-4 are the same)
2	Cell towers only; approximate location, low power, 800 meters distance	Cell towers and GPS; no set accuracy	Cell towers only	Cell towers only
3	Cell towers only; Approximate location, low power, 600 meters distance	Cell towers and GPS; 100 meters	Cell towers only	Cell towers only
4	GPS; approximate location, low power, 400 meters distance	Cell towers and GPS; 50 meters	GPS; 500 meters to 1 kilometer	Cell towers only
5	GPS; fine location, high power, 200 meter distance <i>Note:</i> Device constantly checks, even in situations where it is not moving.	Cell towers and GPS; 25 meters	GPS; 100 meters	GPS (Levels 5-6 are the same)
6	GPS; fine location, high power, 1 meter distance	GPS only; 5 meters	GPS; best to 5 meters Device checks location only when it is moving.	GPS
Custom	Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000)	Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000)	Location source: Use GPS or Use Cellular Triangulation . Distance in meters: (1-1000)	Location source: Use GPS or Use Cellular Triangulation . WM devices support the positioning technology chosen, but do not support distance requirements.

Device Control

This option allows you to use different rules to control devices:

- Allow or block the use of device features
- Allow, block, or limit types of email
- Limit the amount of email or calendar items synchronized
- Allow or block the enrollment of multiple devices per user

Examples: Allow Camera. Allow HTML formatted email, Maximum calendar age for synchronization

File Share Permissions

This option provides permissions for whether or not users can access the File Share list. Permissions are granted per folder or subfolder.

iOS Devices

This option provides settings and controls specifically for iOS devices.

These rules govern iOS device features and applications, Safari browser settings, ratings, security, configuration profile, and management controls; and iCloud usage.

This category also includes policies that enable you to record the installed applications and manage mobile apps on iOS devices.

Supervised mode policies for devices enrolled through the Apple Configurator are available as well. A policy suite can be assigned for the Apple Configurator profile and exported from the Organization Settings in the System Management view of the dashboard.

Managed App Permissions

This option provides permissions for whether or not users can access the Managed App list. Permissions are granted per application.

Permissions for Android and iOS managed apps include a **Force Push** option. When it is enabled, Force Push automatically prompts the users to install the app on all devices associated with the policy.

Permissions for iOS managed apps are listed by region in the following order: Apps for users in the United States, Apps for users in countries outside the U.S. (in alphabetical order), Apps for users in any region.

Resource Control

The options in the *Resource Control* category have been grouped together to give the administrator a convenient way to disable resources for users associated with a schedule-based Policy Suite that is in effect outside scheduled hours. Administrators can restrict ActiveSync connections, File Share, and Managed Apps. See also Control Resources Users Access.

Security Settings

This option provides rules that enforce compliance with a company's policies for securing mobile devices. Examples: Require Password, Require Encryption, Wipe Device on failed unlock attempts

All Security Settings are dependent on whether you have enabled Require Password.

SMIME Settings

Provides Secure/Multipurpose Internet Mail Extensions settings to add an additional layer of encryption for email messages.

TouchDown

This option provides settings and controls specifically for Android or iOS devices that use the TouchDown application (v7.3.00052 or greater). These rules govern Android and iOS functionality and user access to many TouchDown settings that are configurable on the device. Subcategories include: Installation, General, Signature, Widgets, Phone Book, User Configurable Settings, and Suppressions.

About User Configurable Settings

Users can configure these policies according to preference. Administrators choose the setting for initial device configuration. Changes to these settings do affect existing TouchDown users.

About Suppressions

Suppressions are a specific category of policies that can actually remove the configurable TouchDown setting from the device view. They control whether users have access to settings that configure email, calendar, contacts, tasks, security, synchronization, and device capabilities.

An enabled suppression policy gives the user control of the setting. The policy is enabled when set to YES.



A disabled suppression removes the setting from user devices.

If the disabled suppression has a control setting, the administrator can configure it.

An example of a suppression with a control setting is:



When a disabled suppression does not have a control setting, the setting is locked as it was previously set on the device.

An example of a suppression without a control setting is:



If you plan to disable suppression policies that do not have a control setting, thereby removing it from a device, the setting on the device must be configured accurately before the suppression is imposed.

Here are best practices for deploying devices when suppression policies without control settings are disabled:

- Create two policy suites – one that does not disable suppressions policies and the policy suite you will ultimately assign to the user.
- Initially, assign to the user the policy that does not disable suppression polices.
- Install and register the TouchDown and *ZENworks Mobile Management* apps on devices.

- Configure the TouchDown settings on the device in accordance with your company policies.
- Change the policy assignment for the user from the dashboard (assign the policy with the suppressions disabled) and allow the changes to synchronize.
- Issue the device to the user.

Whitelists/Blacklists Permissions

Permissions for whether or not blacklist or whitelist filters govern what applications can be installed on devices accessing the server.

Blacklists If an application installed on a device matches one of the blacklist filter strings, the user's access to email, shared files, app lists, or other organization resources can be blocked. Restrictions are specified through the Compliance Manager.

The list of blacklist filter strings must be enabled in *Restricted Apps Permissions* in order for the restrictions to take effect.

Whitelists If an application installed on a device does not match one of the whitelist filter strings, the user's access to email, shared files, app lists, or other organization resources can be blocked. Restrictions are specified through the Compliance Manager.

The list of whitelist filter strings must be enabled in *Restricted Apps Permissions* in order for the restrictions to take effect. When whitelist permissions are enabled, blacklist permissions are automatically disabled.


Tips on Customizing and Using Policy Suites

- The Policy Suite configuration pages can display the device platforms that support the policy. Select device platforms to view from the drop-down list.



- The symbols displayed next to a policy represent the device platforms that support the policy. Hover over a symbol to view help text.

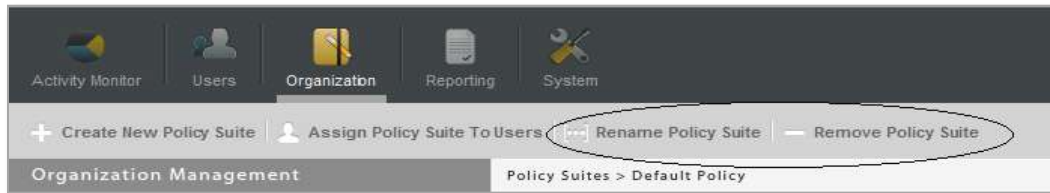


- Click the  symbol to access the Device Platform Functionality table from the dashboard. This table gives descriptions of each policy and details the functionality across each device platform. The document is also available via the ZENworks Mobile Management documentation portal. [Device Platform Functionality](#)
- You can use **Allow All** and **Deny All** buttons in a category to easily allow or deny all settings for corporate and individual devices simultaneously.

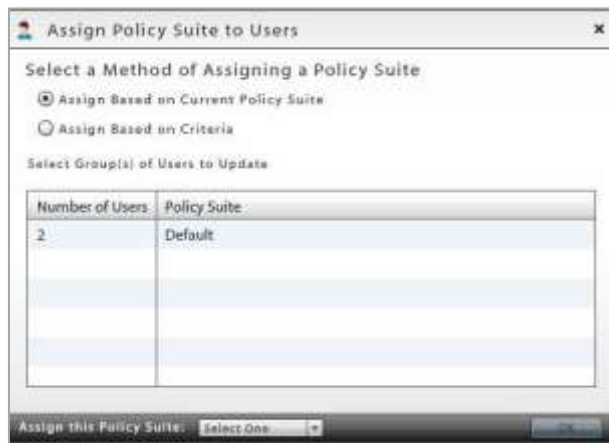


- Some policies determine the options available for other policies. For example, Allow Browser in the Device Control section must be enabled if you plan to enable Allow Safari for iOS devices.

- You must specify a policy suite when you add a user. Users added by import methods all have the same policy suite. Users added to the system via hands-off enrollment are assigned the default policy suite.
- You can change an individual user's policy suite in his or her *User Profile*.
- You can rename or remove a Policy Suite.



- You can select users by criteria and assign or change the group's policy suite by using the **Assign Policy Suite To Users** option. Selection criteria includes policy suite, device connection schedule, device model, ownership, device platform, and custom columns.



Device Connection Schedules

The device connection schedule determines the frequency at which devices connect with the *ZENworks Mobile Management* server. The schedule controls when the devices send statistics and can also control when the server sends updates (if the direct push setting is disabled). Regulating the interval at which devices connect should be considered carefully to minimize the device battery depletion.

Schedules defined here do not affect ActiveSync synchronization of email/PIM. The device connection schedule controls only the synchronization frequency of *ZENworks Mobile Management* data, such as device statistics, location, and audit tracking data.

Creating Device Connection Schedules

- A wizard guides you through setting up of an organization's connection schedules.
- Multiple schedules can exist and individual user, LDAP groups/folders, and organizations can be assigned the appropriate schedule.
- The wizard allows an administrator to quickly create a new device connection schedule or copy an existing schedule. If a schedule is copied, the administrator can edit the settings associated with the new schedule.
- Each schedule can be customized for corporate and individual users.

Create a Device Connection Schedule

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the drop-down menu, select **Policy Management > Device Connection Schedules**.
3. Click the **Create New Device Connection Schedule** option.
4. Choose a method for creating a connection schedule:
 - **Create a New Device Connection Schedule** - Create the initial schedule using system defaults.
 - **Copy Existing Device Connection Schedule** - Create the initial policy suite by copying the settings of an existing schedule.



5. Enter a name for the new schedule.
6. Define the following settings for Corporate and Individual devices:
 - Monday through Sunday Peak Connect Times
 - Peak Connect Interval
 - Require Direct Push for Peak Times
 - Off-peak Connect Interval
 - Require Direct Push for Off-peak Times

Peak Connection Times - The times you define in the schedule grid designate *Peak Connection Times*. Anything that falls outside the peak schedule is off-peak connection time.

Peak and Off-peak Connect Intervals - A schedule's *Peak and Off-peak Connect Intervals* define the frequency at which devices connect with the *ZENworks Mobile Management* server. Peak time are periods during which device usage is consistently higher than average. Conversely, off-peak times are periods during which device usage is consistently lower than average. Consider the following:

- To accommodate the higher traffic, set peak connect intervals at lower values (initiating more frequent connections) than off-peak connect intervals.
- Lower connect intervals increase the efficiency of the *ZENworks Mobile Management* Compliance Manager, since devices report device statistics more frequently allowing the server to detect non-compliance sooner.
- Avoid setting intervals so low that they significantly affect device battery depletion.

Require Direct Push - The *Require Direct Push* setting determines whether updates from the server, such as security commands, are synchronized immediately or during the next scheduled connection. If this setting is enabled, commands from the server sync to the device as soon as they are issued. Synchronizations from the device still occur according to the scheduled connect interval and are not affected by this setting.

When user devices are in Direct Push mode, remote Wipe commands sent from the server sync immediately, regardless of whether or not *Require Direct Push* is enabled.

Editing Device Connection Schedules

To edit an existing device connection schedule:

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the drop-down menu, select **Policy Management > Device Connection Schedules**.
3. From the menu panel, select the schedule you want to change.
4. Select the **Corporate** or **Individual** schedule.
5. Edit the settings and click **Save Changes**.

Corporate Peak Device Connection Schedule

Device Connection Schedules Govern ZENworks App Connections Only

Monday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Tuesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Wednesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Thursday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Friday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Saturday	<input type="checkbox"/>	12:00 AM	to	12:00 AM
Sunday	<input type="checkbox"/>	12:00 AM	to	12:00 AM

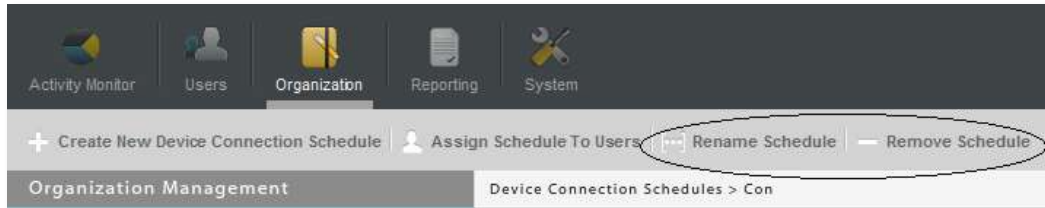
Peak Connect Interval: Minutes Off-peak Connect Interval: Minutes

Require Direct Push for Peak Times Require Direct Push for Off-peak Times

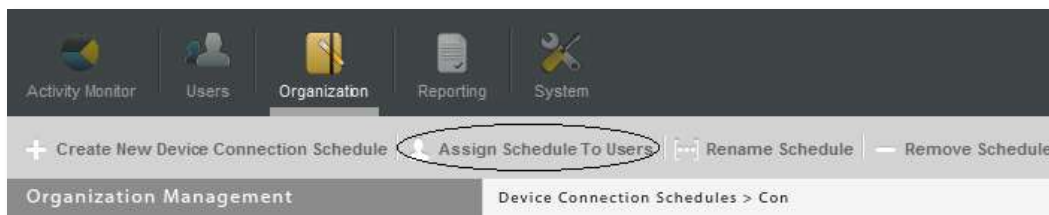
Note: Times extending into next day are allowed, but the next day's start time must be after the preceding day's end time.

Tips on Using Device Connection Schedules

- You must specify a device connection schedule when you add a user. Users added by import methods all have the same device connection schedule. Users added to the system via hands-off enrollment are assigned the default device connection schedule.
- You can rename or remove a device connection schedule.



- You can change an individual user's device connection schedule in his or her *User Profile*.
- You can select users by criteria and assign or change the group's device connection schedule by using the **Assign Schedule To Users** option.

A screenshot of the 'Assign Device Connection Schedule to Users' dialog box. The title bar shows a user icon and the text 'Assign Device Connection Schedule to Users'. The main content area is titled 'Select a Method of Assigning a Device Connection Schedule'. There are two radio buttons: 'Assign Based on Current Device Connection Schedule' (unselected) and 'Assign Based on Criteria' (selected). Below this, there is a section titled 'Select Criteria and Assign to Specific Devices' with several dropdown menus: 'Policy Enforcement Type' (set to 'All'), 'Device Connection Schedule' (set to 'Select One'), 'Device Platform' (set to 'Android'), 'Device Model' (set to 'Select One'), and 'Ownership' (set to 'Select One'). At the bottom, there is a field for 'Users Affected' with the value '1'. At the very bottom of the dialog, there is a field 'Assign This Schedule:' set to 'CAS', and two buttons: 'Clear' and 'OK'.

Assigning a Device Connection Schedule

Policy Schedules

Policy Schedules are used for schedule-based assignment of policies. The schedule defines the days and times during which users are working.

Two Policy Suites can be assigned to an individual user, all users in a LDAP group/folder, or all users in the organization. One Policy Suite governs user devices during scheduled hours, the other governs user devices outside scheduled hours. The schedule determines when each Policy Suite is in effect.

Creating Policy Schedules

- A Wizard guides you through setup of an organization's connection schedule(s).
- The *Wizard* allows an administrator to quickly create a new policy schedule or copy an existing schedule. If a schedule is copied, the administrator can edit the settings associated with the new schedule.
- Multiple schedules can exist and individual users, LDAP groups/folders, and organizations can be assigned the appropriate schedule.

Create a Policy Schedule

1. From the *ZENworks Mobile Management* dashboard header, select **Organization Management**
2. From the drop-down menu, select **Policy Management > Policy Schedules**.
3. Click the **Create New Policy Schedule** option.
4. Choose a method for creating a connection schedule:
 - **Create a New Policy Schedule** - Create the initial schedule using system defaults.
 - **Copy Existing Policy Schedule** - Create the initial policy suite by copying the settings of an existing schedule.



5. Enter a name for the new schedule.

- Define the hours during which users are working, Monday through Sunday.

Create New Policy Schedule Wizard

Welcome

Assign a Name

Policy Schedule

Define Policy Schedule Operation Days and Times

Policy Schedules determine when time-based policies are in effect.

Monday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Tuesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Wednesday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Thursday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Friday	<input checked="" type="checkbox"/>	8:00 AM	to	5:00 PM
Saturday	<input type="checkbox"/>	8:00 AM	to	5:00 PM
Sunday	<input type="checkbox"/>	8:00 AM	to	5:00 PM

Back Finish

Assign a Policy Schedule

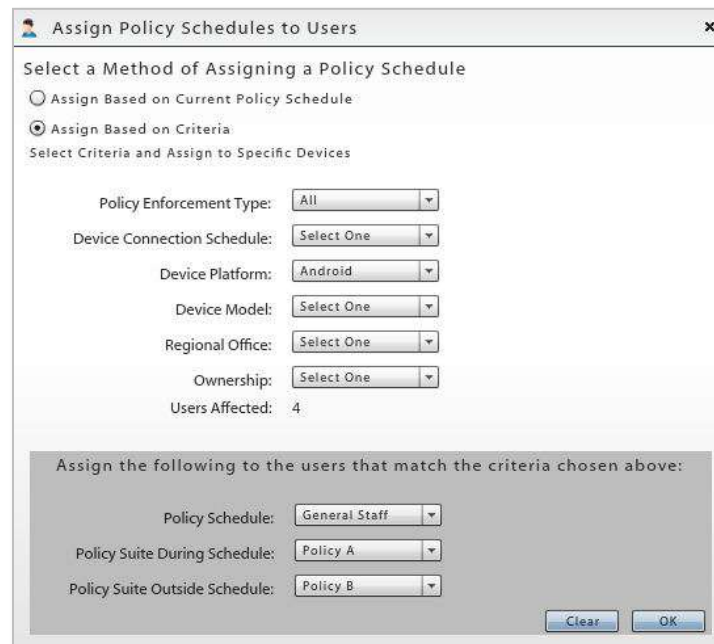
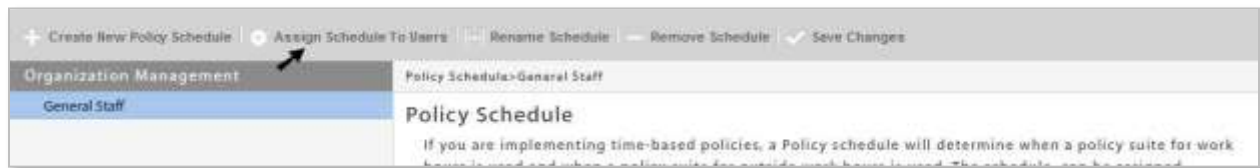
Assign the Policy Schedule to to:

- an individual user (*User Profile*)
- all users in a LDAP group/folder (*Organization > Administrative Servers > LDAP Servers*)
- all users currently assigned to another Policy Schedule or that meet selected criteria (*Organization > Policy Management > Policy Schedules > Assign Schedule to Users*)
- all users in the organization (*System > Organization Settings*)

When you assign a Policy Schedule, you will also select a Policy Suite to be used during scheduled hours and one to be used outside scheduled hours.

To assign a schedule to all users currently assigned to another Policy Schedule or users that meet selected criteria,

1. Click the **Assign Schedule to Users** button on the *Policy Schedule* page.
2. Choose users based on their **Current Policy Schedule** or choose users based on **Criteria** and select the criteria
3. From the drop-down list, select the **Policy Schedule** you want to assign to the users.
4. From the drop-down lists, select the Policy Suite to be used **during scheduled hours** and the Policy Suite to be used **outside scheduled hours**.



Control Resources Users Access Outside Scheduled Hours

Policy Suites that are designated to take affect outside scheduled hours can be configured to restrict users' access to corporate resources. Use the **Resource Control** category in the Policy Suite to restrict resources.

The options in the *Resource Control* category have been grouped together to give the administrator a convenient way to disable resources for users associated with a schedule-based Policy Suite that is in effect outside scheduled hours. Administrators can restrict ActiveSync connections, File Share, and Managed Apps.

1. From the *ZENworks Mobile Management* dashboard header, select **Organization**.
2. From the drop-down menu, select **Policy Management > Policy Suites**.
3. Choose a policy suite and select the **Resource Control** category.



4. Disable the resources you want to restrict and click **Save Changes**.