Configuring Organizations, Device Connection Schedules, and Policy Suites

ZENworks® Mobile Management 3.2.x

October 2015

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

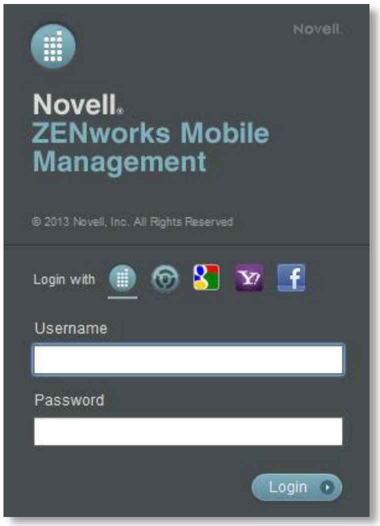
ZENworks Mobile Management dashboard requirements:

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


Novell
Novell. ZENworks Mobile Management
© 2013 Novell, Inc. All Rights Reserved
Login with
Username
Password
Login

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

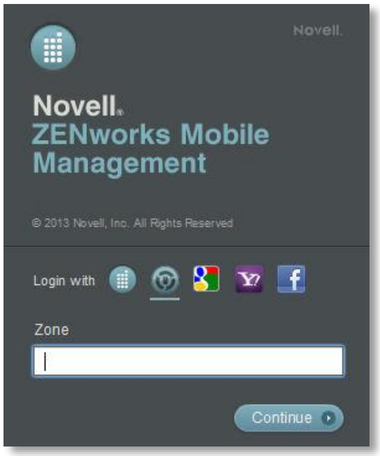
- Locally authenticated logins enter:
  email address and password
- LDAP authenticated logins enter:
  domain\LDAP username and LDAP password

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.

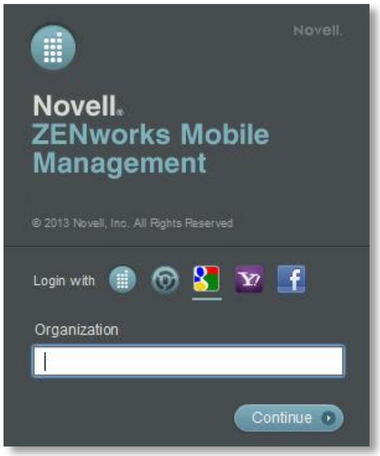
OpenID Login

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*.



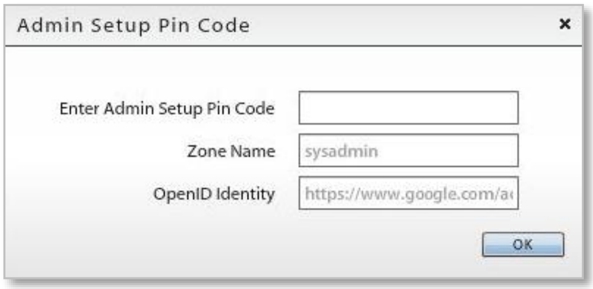
2. Enter the **Zone** or **Organization**, an easy to remember name *ZENworks Mobile Management* uses to redirect you to the OpenID provider portal.



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: sysadmin

OpenID Identity: https://www.google.com/a

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

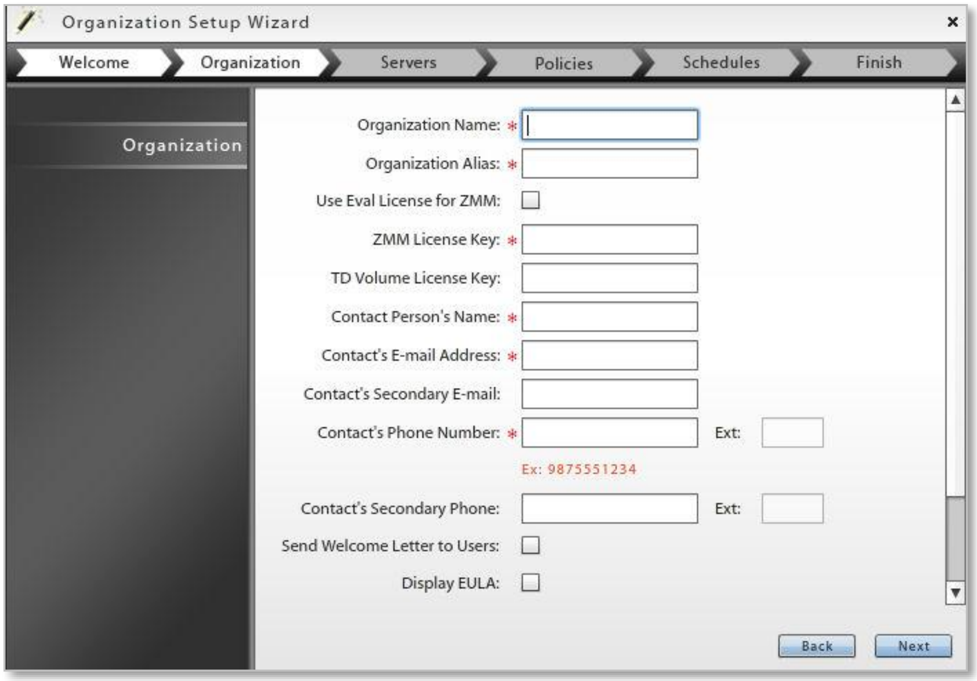
The Organization Setup Wizard displays automatically when you log in to *ZENworks Mobile Management* for the first time. Before you create the first organization, you must enter your Customer Care Center credentials. You only have to enter these credentials when using the wizard for the first time.

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**



- 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

-ActiveSync Server Address

-ActiveSync Server Port

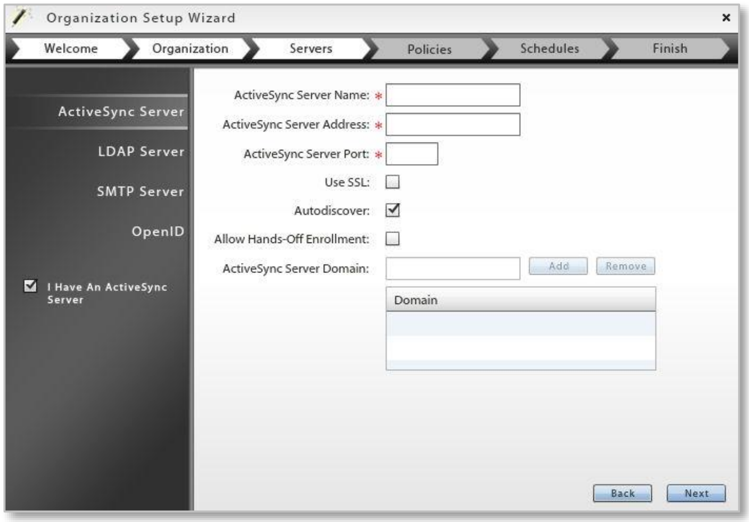
-Use SSL

-Autodiscover

-Proxy ActiveSync Server Traffic by Default (see MDM Proxy)

-Allow Hands-Off Enrollment (see Enabling Hands-Off Enablement)

-ActiveSync Server Domain *(required for hands-off enrollment)*



ActiveSync Server Name: *

ActiveSync Server Address: *

ActiveSync Server Port: *

Use SSL: ☐

Autodiscover: ☑

Allow Hands-Off Enrollment: ☐

ActiveSync Server Domain:

Domain

☑ I Have An ActiveSync Server

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.

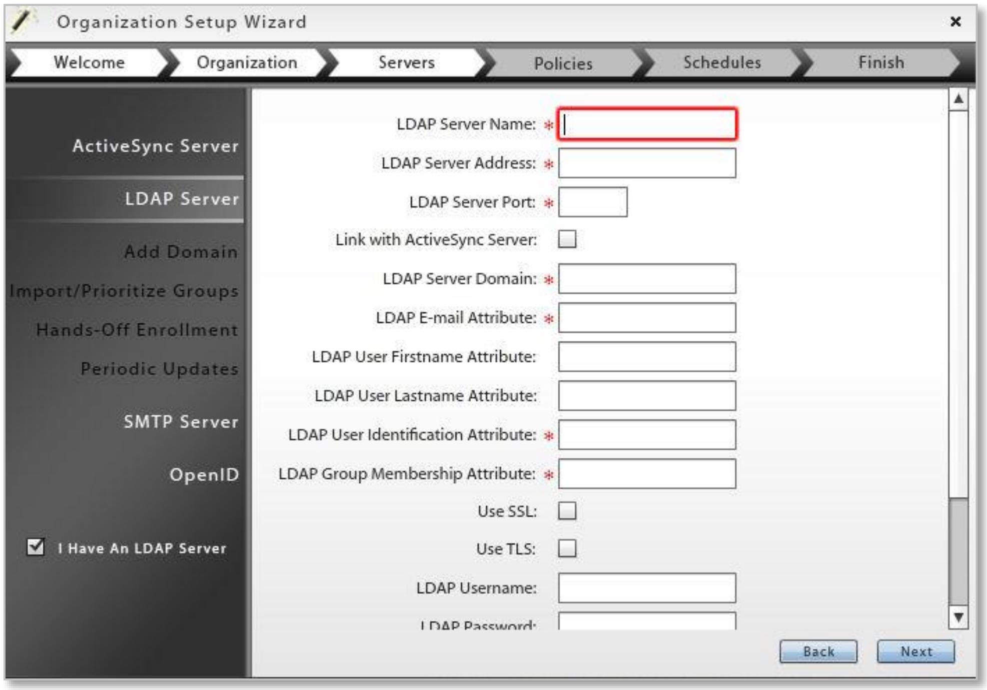
Editing Attributes

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



☑ I Have An LDAP Server

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:

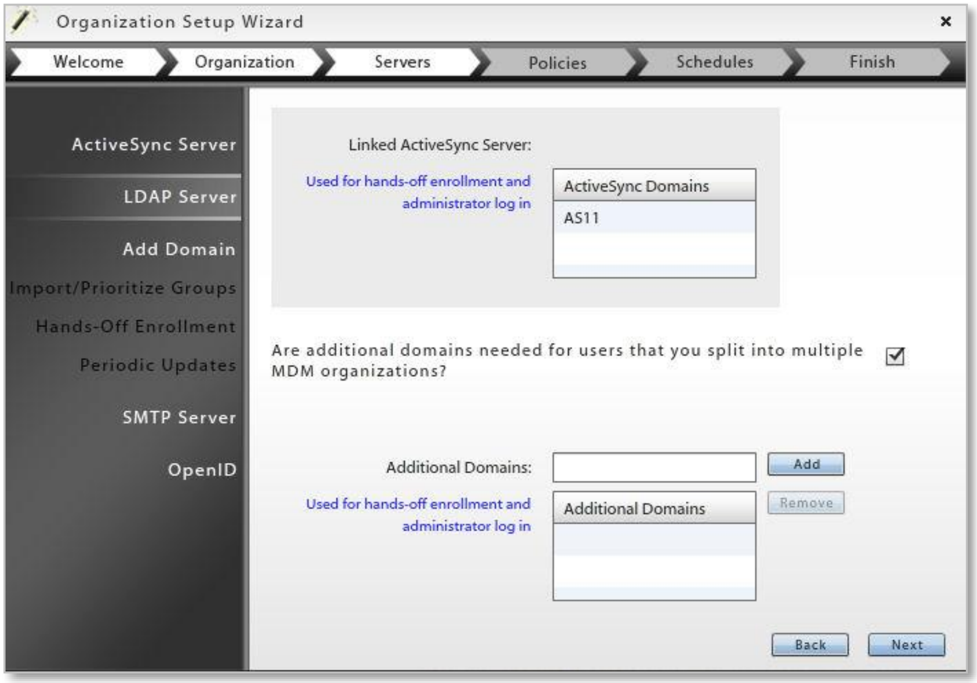
Possible Values for LDAP Server Settings

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.



Linked ActiveSync Server:

Used for hands-off enrollment and administrator log in

ActiveSync Domains
AS11

Are additional domains needed for users that you split into multiple MDM organizations? ☑

Additional Domains:

Used for hands-off enrollment and administrator log in

Additional Domains

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/Device 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.

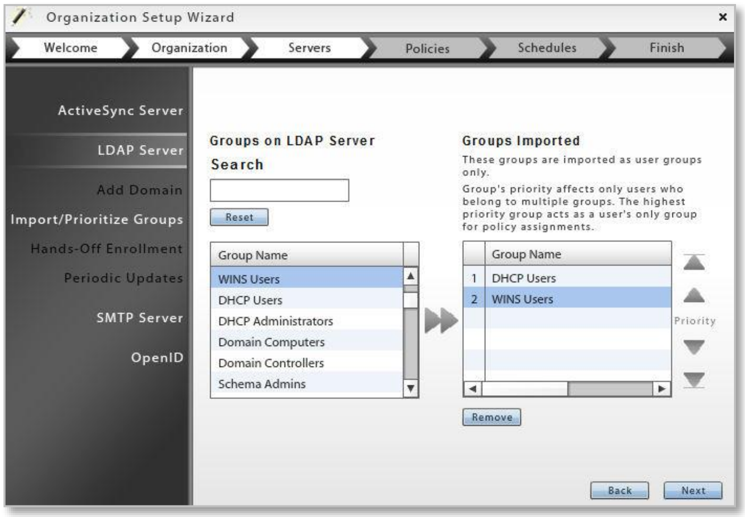
Choosing Groups. Administrators should familiarize themselves with the LDAP server structure and verify that groups they choose for use with the *ZENworks Mobile Management* server contain the following necessary attributes: User Identification Attribute, Group Membership Attribute, Group Object Class, 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.



Groups on LDAP Server

Search

Group Name
WINS Users
DHCP Users
DHCP Administrators
Domain Computers
Domain Controllers
Schema Admins

Groups Imported

These groups are imported as user groups only.

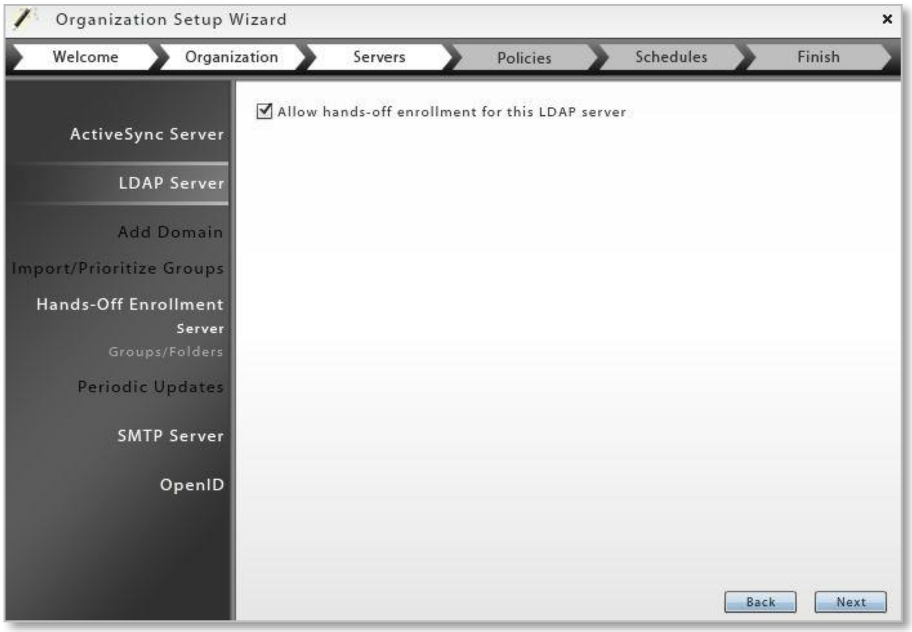
Group's priority affects only users who belong to multiple groups. The highest priority group acts as a user's only group for policy assignments.

	Group Name
1	DHCP Users
2	WINS Users

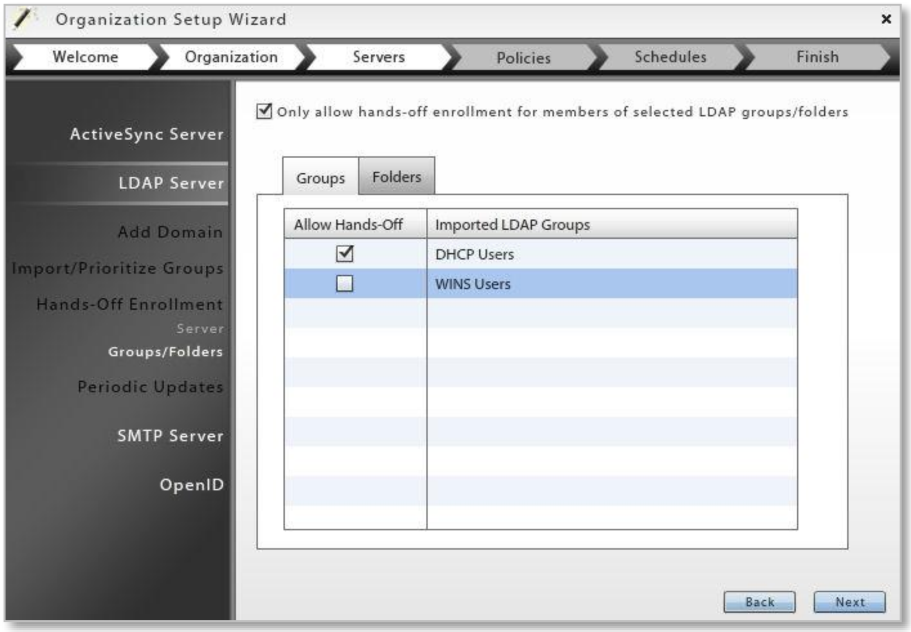
Hands-Off Enrollment

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. (See also Enabling Hands-Off Enrollment.)

- 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.



☑ Allow hands-off enrollment for this LDAP server



☑ Only allow hands-off enrollment for members of selected LDAP groups/folders

Allow Hands-Off	Imported LDAP Groups
☑	DHCP Users
□	WINS Users

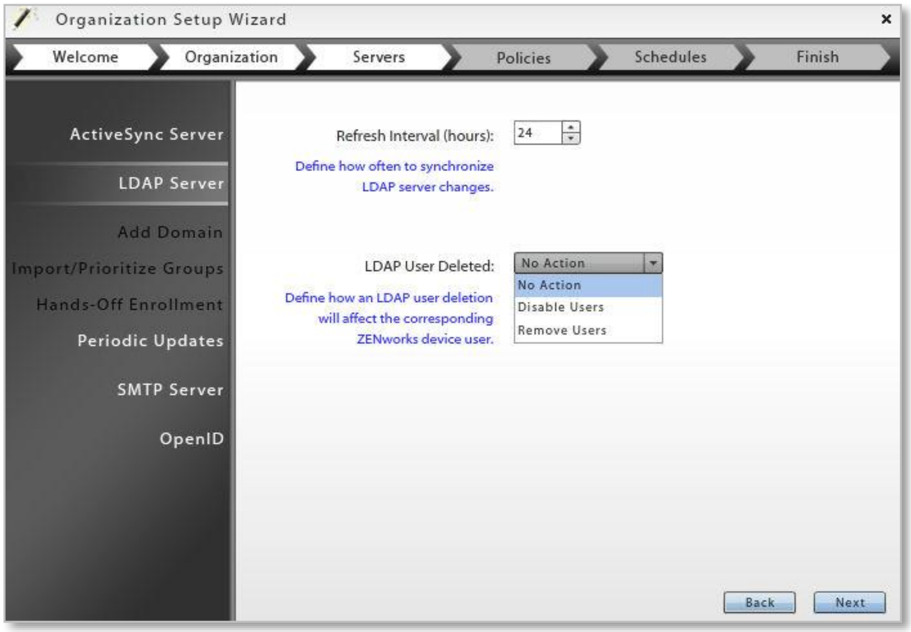
Periodic Updates

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.



Refresh Interval (hours): 24

Define how often to synchronize LDAP server changes.

LDAP User Deleted: No Action

Define how an LDAP user deletion will affect the corresponding ZENworks device user.

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.

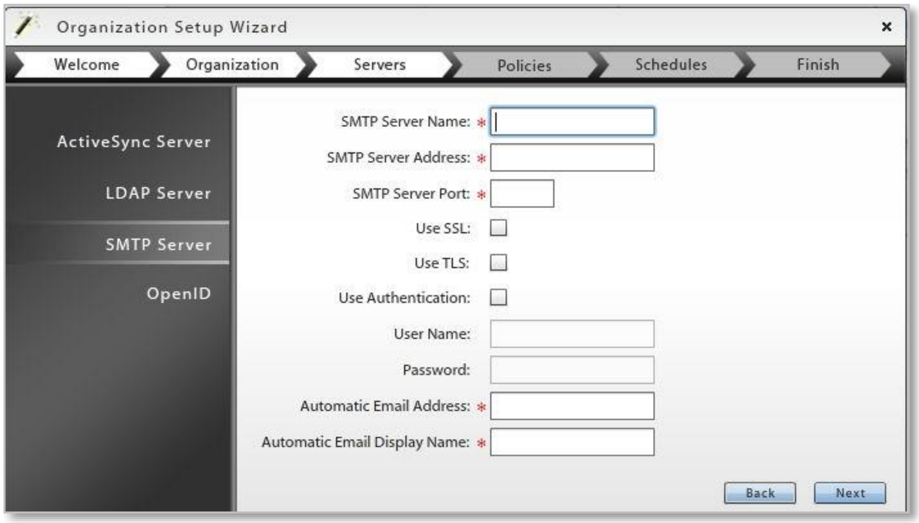
Define the Organization’s Default SMTP Server

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



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.

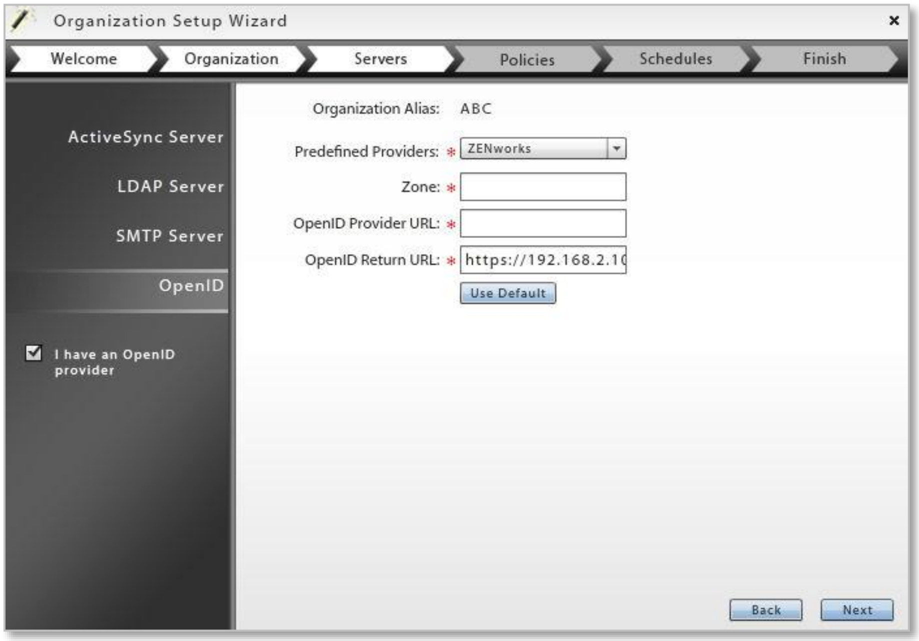
The *Zone* name is emailed to the administrator along with a PIN code they will use the first time they log in with OpenID credentials.

- **OpenID Provider URL** - enter the URL of the ZENworks Primary Server in the following form:

  https://<server:port>/zenworks/?requestHandler=ZENOpenIDHandler

  Replace <server:port> with the hostname (or IP address) and port of the ZENworks Primary Server. The port is required only if the server is using a non-standard port.

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.



☑ I have an OpenID provider

Organization Alias: ABC

Predefined Providers: * ZENworks

Zone: *

OpenID Provider URL: *

OpenID Return URL: * https://192.168.2.1

Create the Organization's Default Policy Suite

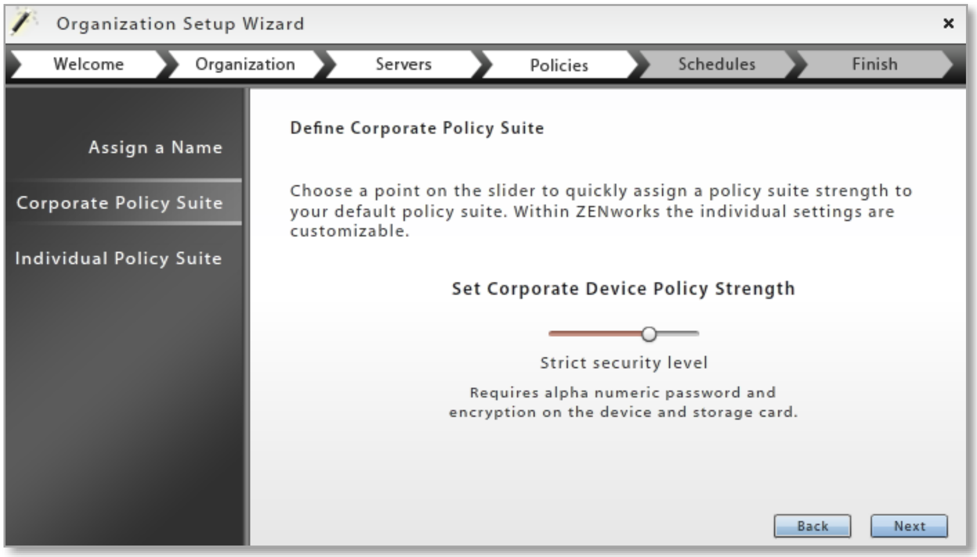
You need to create a default policy suite for the organization. Other policy suites can be created later to accommodate different groups of users. The default policy suite is automatically assigned to users added to the system via hands-off enrollment. For additional information, see Policy Suites.

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.



Define Corporate Policy Suite

Choose a point on the slider to quickly assign a policy suite strength to your default policy suite. Within ZENworks the individual settings are customizable.

Set Corporate Device Policy Strength

Strict security level

Requires alpha numeric 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).

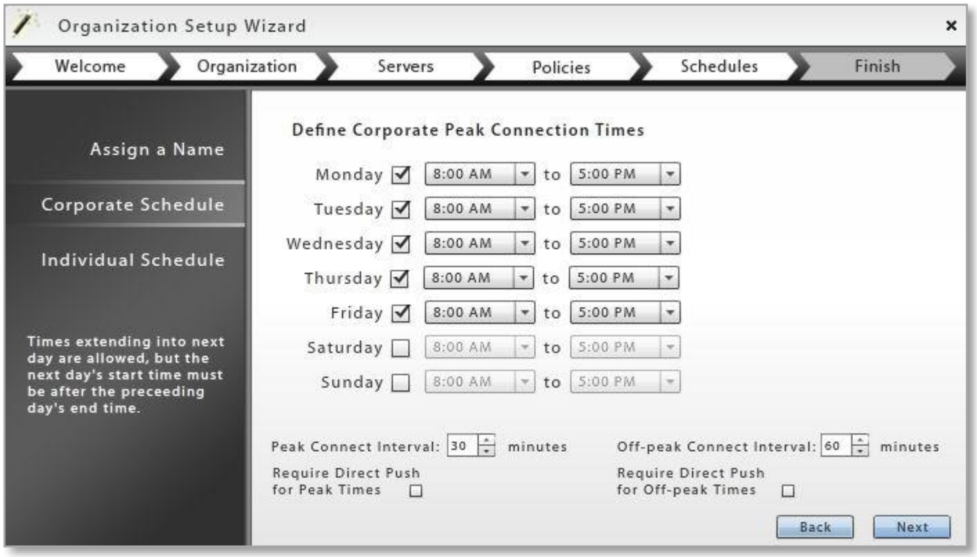
Set an individual device connection schedule (schedule for devices that individuals are responsible for).

Define the following settings:

Corporate	**Individual**
Monday through Sunday peak connect times	Monday through Sunday peak connect times
Peak Connect Interval	Peak Connect Interval
Require Direct Push for Peak Times	Require Direct Push for Peak Times
Off-peak Connect Interval	Off-peak Connect Interval
Require Direct Push for Off-peak Times	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.



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

Define Corporate Peak Connection Times

Monday	☑	8:00 AM	to	5:00 PM
Tuesday	☑	8:00 AM	to	5:00 PM
Wednesday	☑	8:00 AM	to	5:00 PM
Thursday	☑	8:00 AM	to	5:00 PM
Friday	☑	8:00 AM	to	5:00 PM
Saturday	□	8:00 AM	to	5:00 PM
Sunday	□	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 □

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.
- When *ZENworks Mobile Management* is configured so that it does not proxy ActiveSync traffic, users with Android KNOX and iOS devices that retrieve email can be assigned a certificate for authenticating against the ActiveSync Server. See Authentication Certificates.
- Organizations that have recently employed the *ZENworks Mobile Management* system to manage devices can migrate device information from an Exchange ActiveSync server using ActiveSync PowerShell capabilities. See PowerShell Connection.

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 the System to Query an LDAP Server*
- *Adding Users, Enrolling Devices Guide*: *Adding Users via LDAP, Custom Columns*
- In this guide, *Creating Organization 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 *ZENworks Mobile Management* server and the Administrative LDAP server; -Verifies that required LDAP attributes contain values	None – uses the credentials on file
ActiveSync Server	-Connectivity between the *ZENworks Mobile Management* 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 *ZENworks Mobile Management* server and the SMTP server; -Authentication if *Use Authentication* is enabled; -Email delivery	None Optional email delivery test: Provide a test email address, subject, and message body

Configuring an ActiveSync Server to Issue Authentication Certificates

When *ZENworks Mobile Management* is configured so that it does not proxy ActiveSync traffic, users with Android KNOX and iOS devices that retrieve email can be assigned a certificate for authenticating against the ActiveSync Server.

In order to apply a Certificate Template to the ActiveSync server resource, the ActiveSync proxy option must be disabled. From the dashboard navigate to ***System*** > ***Organization Settings*** and remove the mark from the checkbox next to **Proxy ActiveSync Traffic by Default**.

To Authenticate Users for ActiveSync Server Access:

1. From the *ZENworks Mobile Management* administrative dashboard, select ***Organization*** > ***Administrative Servers*** > ***ActiveSync Servers***.
2. Select an existing ActiveSync server from the left panel or add one by clicking *Add ActiveSync Server*.
3. Select a **Certificate Authority** and a **Certificate Template** from the drop-down lists.
4. Click **Save Changes**.

When *ZENworks* configures ActiveSync settings on an Android KNOX or iOS device, the user's certificate is deployed based on the certificate template selection.

ActiveSync Server PowerShell Connection Settings

When an organization chooses not to proxy email mail through the *ZENworks Mobile Management* server, devices will be able to connect directly to the ActiveSync server to access email without the requirement of MDM enrollment. As a means of enforcing enrollment, administrators can configure ActiveSync PowerShell settings and employ its capabilities via the *ZENworks Mobile Management* dashboard to import device and user information from the ActiveSync server. Once devices are imported they can be managed from the dashboard and administrators can monitor who has enrolled with MDM and who has not. The administrator can set a grace period during which devices must enroll in order to access email. Once the grace period ends non-compliant devices will be restricted from accessing email.

The PowerShell integration enables *ZENworks Mobile Management* to:

- Poll the Exchange ActiveSync server at regular intervals for device and user information and import it to the MDM server. Additions and deletions made on the ActiveSync server are synchronized to MDM.
- Monitor who has not yet enrolled with the *ZENworks Mobile Management* server by viewing the Discovered Devices grid.
- Enforce *ZENworks Mobile Management* enrollment of auto-discovered devices accessing email by setting a quarantine date on which unenrolled devices will be blocked from accessing email. Once a device is enrolled the quarantine is lifted and the device can again access email.
- Email users when they are nearing the quarantine date. Each device a user has not yet enrolled will receive an email message.

For information on configuring PowerShell for integration with *ZENworks Mobile Management*, see the PowerShell Configuration guide.

Configuring the System to Query an LDAP Server

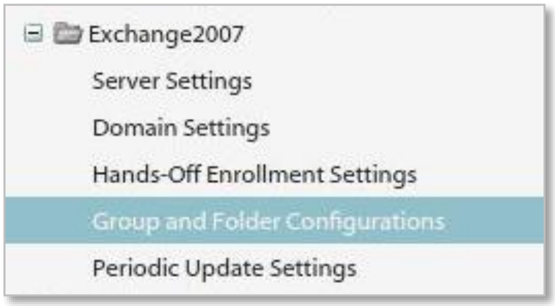
When the LDAP server is fully configured, users associated with an LDAP folder or group can be provisioned automatically when added to *ZENworks Mobile Management* manually, via a batch import, or through hands-off enrollment. This is done by associating each LDAP folder or group with a Policy Suite, 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

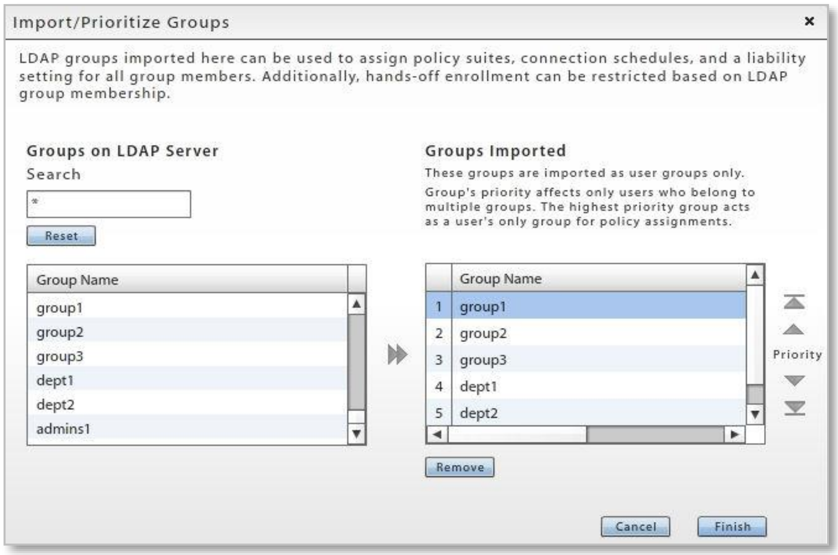
Import LDAP groups into the grid, using the **Import/Prioritize Groups** button.

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.



LDAP groups imported here can be used to assign policy suites, connection schedules, and a liability setting for all group members. Additionally, hands-off enrollment can be restricted based on LDAP group membership.

Groups on LDAP Server

Search: *

Group Name
group1
group2
group3
dept1
dept2
admins1

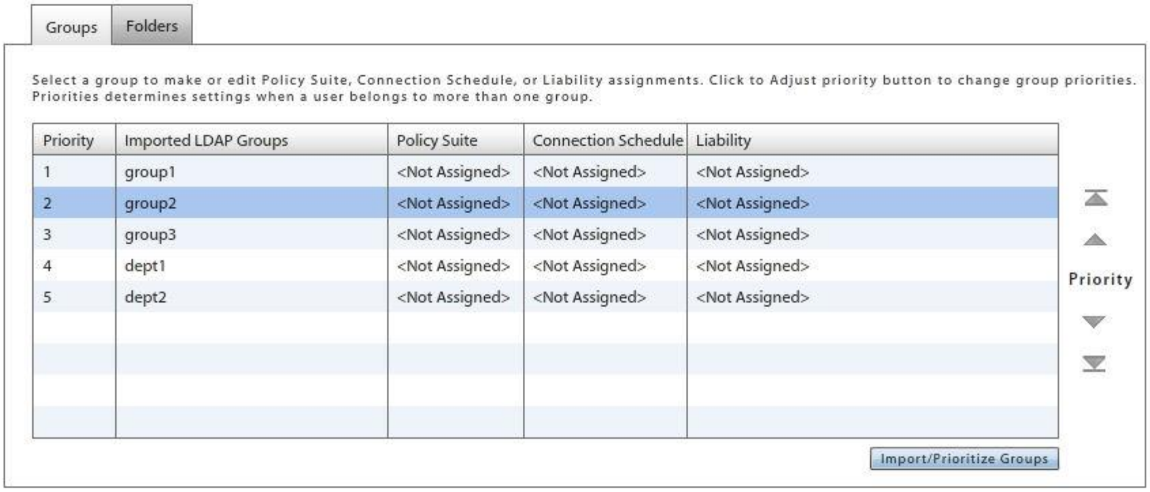
Groups Imported

These groups are imported as user groups only.

Group's priority affects only users who belong to multiple groups. The highest priority group acts as a user's only group for policy assignments.

	Group Name
1	group1
2	group2
3	group3
4	dept1
5	dept2

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.



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.

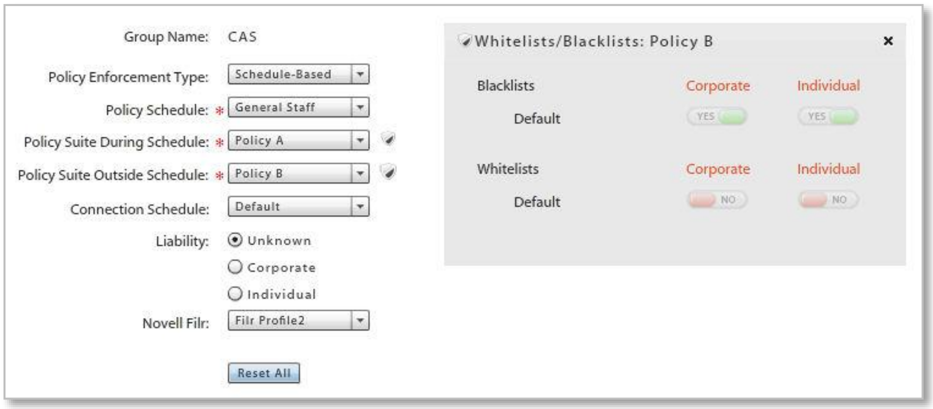
Priority	Imported LDAP Groups	Policy Suite	Connection Schedule	Liability
1	group1	<Not Assigned>	<Not Assigned>	<Not Assigned>
2	group2	<Not Assigned>	<Not Assigned>	<Not Assigned>
3	group3	<Not Assigned>	<Not Assigned>	<Not Assigned>
4	dept1	<Not Assigned>	<Not Assigned>	<Not Assigned>
5	dept2	<Not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

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/Device grid. See the Managing Users and Resources Guide.



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 ○ Corporate ○ Individual

Novell Filr: Filr Profile2

Whitelists/Blacklists: Policy B

Blacklists	Corporate	Individual
Default	YES	YES

Whitelists	Corporate	Individual
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 an Organization

Organization Settings

The *Organization Settings* page has a variety of settings that allow you to determine the features you want to implement for an organization. You can also update the organization information (name, contacts, etc.) or default settings.

To access the *Organization Settings* page select ***System*** > ***Organization***.

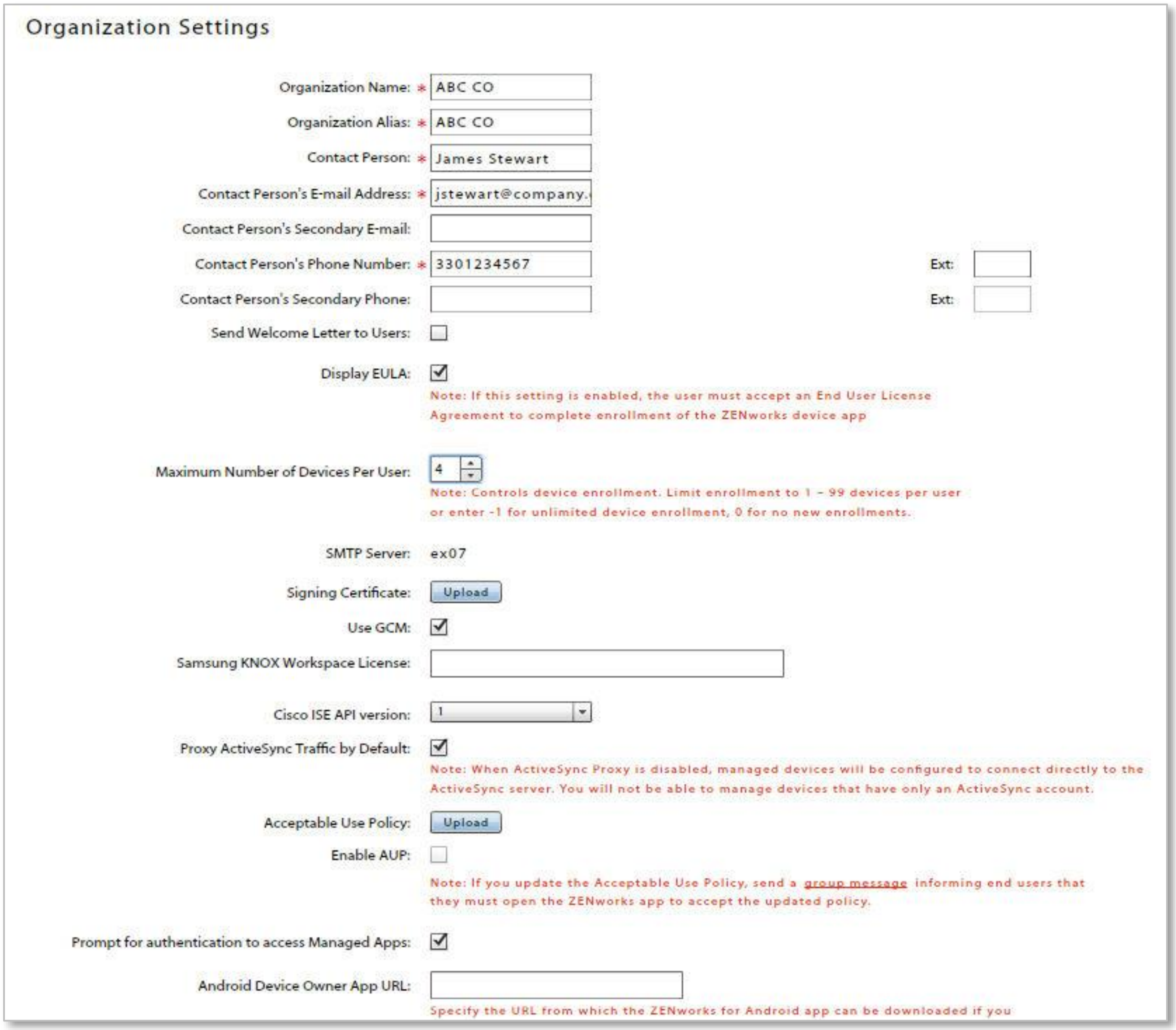
Organization Settings consist of the following:

- General Settings
- iOS Management
- Organization Defaults
- Hands-Off Enrollment Defaults
- Windows Settings

The lists below document the information and settings that can be configured here.

General Settings

- Organization name and contact information
- Welcome letter - Emails a welcome letter to users when they are added
- EULA - when this option is enabled, users must accept an End User License Agreement to complete *ZENworks Mobile Management* app enrollment
- Maximum Number of Devices Per User – limits the number of devices users can enroll
- SMTP server name
- Signing Certificate *Upload* button (see description)
- *Use GCM* checkbox (description)
- Samsung KNOX Workspace License (description)
- Proxy ActiveSync Traffic by Default (description)
- Acceptable Use Policy (description)
- Enable AUP
- Prompt for authentication to access Managed Apps – Prompts for credentials before a user can access Managed Apps on the device
- Android Device Owner URL (description)
- Android Device Owner Checksum



Organization Settings

Organization Name: * ABC CO

Organization Alias: * ABC CO

Contact Person: * James Stewart

Contact Person's E-mail Address: * jstewart@company.

Contact Person's Secondary E-mail:

Contact Person's Phone Number: * 3301234567 Ext:

Contact Person's Secondary Phone: Ext:

Send Welcome Letter to Users: □

Display EULA: ☑

Note: If this setting is enabled, the user must accept an End User License Agreement to complete enrollment of the ZENworks device app

Maximum Number of Devices Per User: 4

Note: Controls device enrollment. Limit enrollment to 1 - 99 devices per user or enter -1 for unlimited device enrollment, 0 for no new enrollments.

SMTP Server: ex07

Signing Certificate: Upload

Use GCM: ☑

Samsung KNOX Workspace License:

Cisco ISE API version: 1

Proxy ActiveSync Traffic by Default: ☑

Note: When ActiveSync Proxy is disabled, managed devices will be configured to connect directly to the ActiveSync server. You will not be able to manage devices that have only an ActiveSync account.

Acceptable Use Policy: Upload

Enable AUP: □

Note: If you update the Acceptable Use Policy, send a group message informing end users that they must open the ZENworks app to accept the updated policy.

Prompt for authentication to access Managed Apps: ☑

Android Device Owner App URL:

Specify the URL from which the ZENworks for Android app can be downloaded if you

Sample Organization Settings page

iOS Management

- APNs Certificate *Upload* button (see description)
- APNs Expiration Date (annual)
- Apple ID
- iOS Configurator Groups button (see description)
- Apple DEP Token *Upload, Edit, Remove*, and *Sync Now* buttons (description)
- Apple DEP Token Expiration Date (*annual*)
- DEP Account E-mail
- NPNS Certificate *Upload* (description)
- Push ZMM to iOS devices (description)
- MDM App Type
- Enterprise App *Upload/Edit* button

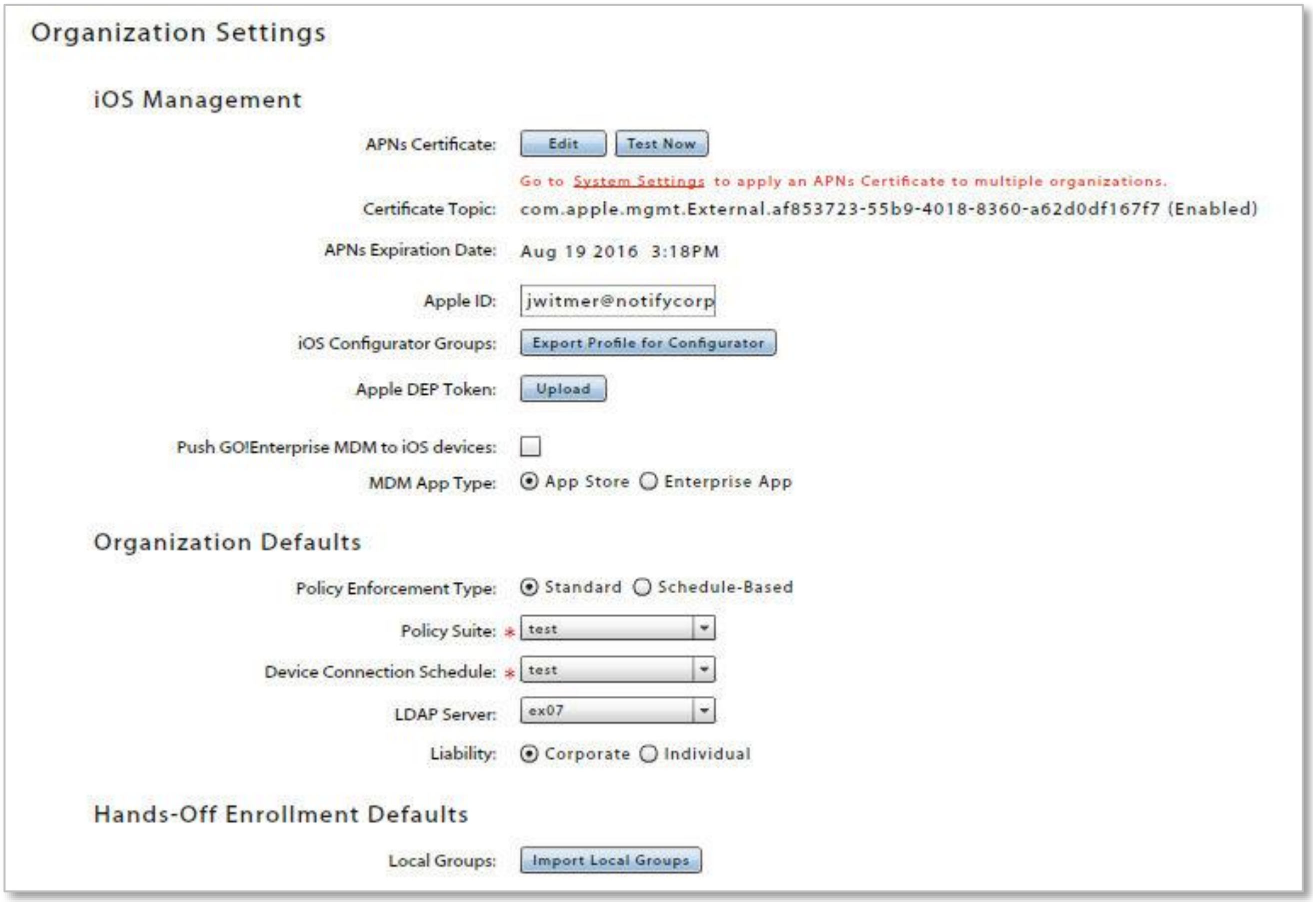
Organization Defaults

- Policy Enforcement Type
- Policy Schedule (description)
- Policy Suite(s)
- Device Connection Schedule
- (Administrative) LDAP Server
- Liability
- Novell Filr (profile)*

Hands-Off Enrollment Defaults

- Local Groups

***** 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.



Organization Settings

iOS Management

APNs Certificate: Edit | Test Now

Go to System Settings to apply an APNs Certificate to multiple organizations.

Certificate Topic: com.apple.mgmt.External.af853723-55b9-4018-8360-a62d0df167f7 (Enabled)

APNs Expiration Date: Aug 19 2016 3:18PM

Apple ID: jwitmer@notifycorp

iOS Configurator Groups: Export Profile for Configurator

Apple DEP Token: Upload

Push GO!Enterprise MDM to iOS devices: □

MDM App Type: ● App Store ○ Enterprise App

Organization Defaults

Policy Enforcement Type: ● Standard ○ Schedule-Based

Policy Suite: * test

Device Connection Schedule: * test

LDAP Server: ex07

Liability: ● Corporate ○ Individual

Hands-Off Enrollment Defaults

Local Groups: Import Local Groups

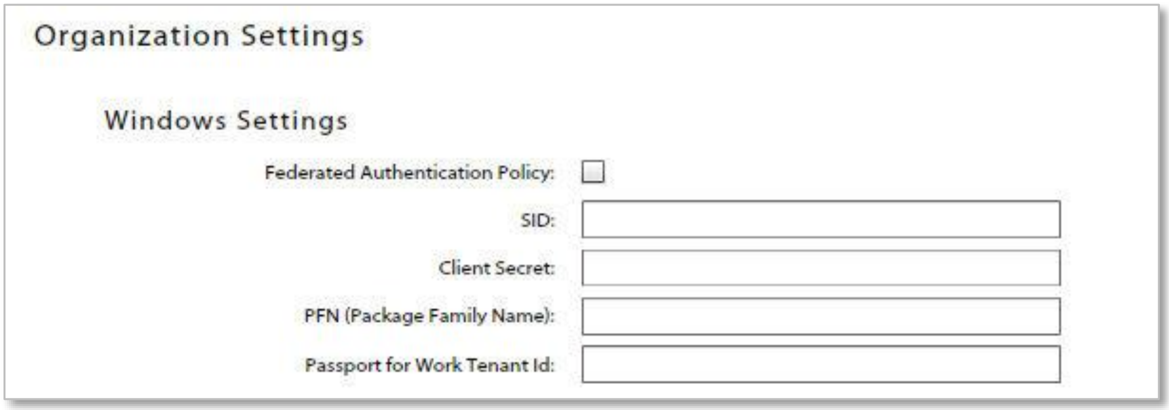
Sample Organization Settings page: iOS Management, Organization Defaults, Hands-Off Enrollment Defaults

Windows Settings

These settings will configure the *ZENworks Mobile Management* server to communication with the Windows Push Notification Services (WNS). WNS provides a mechanism for real-time delivery of policy updates and security commands to Windows 8.1+ devices. Without this configuration, updates are delivered at intervals defined by the connection schedule assigned to the device.

To obtain these credentials, you must have a Windows Store developer account and complete a registration process. Please reference the Microsoft document on Authenticating with WNS.

- Federated Authentication Policy - (optional) Checking this box employs a service to collect user information and authenticate users during enrollment.
  Note: Windows 8.1 tablets can only enroll using Federated Authentication
- SID (Package Security Identifier) - Credential used to authenticate with Windows Push Notification Services (WNS)
- Client Secret - Credential used to authenticate with Windows Push Notification Services (WNS)
- PFN (Package Family Name) - Application identifier
- Passport for Work Tenant Id – Passport for Work policies (see Policy Suites > Windows Devices > Passport for Work) apply only to users associated with an Active Directory. Enter the credential used to identify the Active Directory server here.



Organization Settings

Windows Settings

Federated Authentication Policy: □

SID:

Client Secret:

PFN (Package Family Name):

Passport for Work Tenant Id:

Sample Organization Settings page: Windows Settings

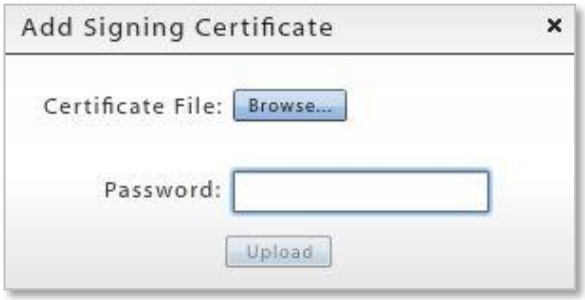
Signing Certificate Upload

The signing certificate is a security measure that authenticates the server and allows iOS devices to recognize it as a trusted source.

The signing certificate *Upload* button allows you to *add a signing certificate for the organization*. This must be a CA signed certificate; because self-signed certificates are currently not supported.

A Signing Certificate designated here for the organization overrides the system-wide Signing Certificate defined in *System Settings*.

1. Select ***System*** > ***System Administration*** > ***Organizations***.
2. Select an organization from the list and click the *Upload* button next to the signing certificate field.



Add Signing Certificate

Certificate File:

Password:

3. Click the ***Browse*** button, then navigate to and select the file containing the certificate.
4. Enter the ***Password*** associated with the file and click ***Upload***.
5. Click ***Save Changes*** on the gray option bar.

Google Cloud Messaging (GCM) Toggle

ZENworks Mobile Management (versions 2.8.2 or higher) can use the Google Cloud Messaging service to let Android devices know that it is time to synchronize. Each device establishes an accredited and encrypted IP connection with the GCM service. Whenever notifications for the device are available, the *ZENworks Mobile Management* server connects with GCM servers. GCM then pings the device telling it to synchronize with *ZENworks Mobile Management*. This method of initiating synchronization is used in place of the *ZENworks Mobile Management* app's device connection schedule, eliminating delayed updates to the device. Using the service offers added functionality in the following ways:

- Security commands such as Full Wipe or Lock Device are applied immediately.
- Changes made to a policy suite or user settings are applied immediately.
- Android corporate resource assignments are applied immediately.
- Fewer resources are used than with direct push, since the connection is not persistent.

There are several things to consider if you elect to use GCM service:

- It requires devices to run Android 2.2 or higher.
- Certain 2.2.x devices will not register with GCM properly. In this case, the *ZENworks Mobile Management* device connection schedule handles the aspects of queuing of messages and delivery to the target Android app running on the device.
- Devices with an Android OS lower than 4.0.4 must have a Gmail account and have the Google Play Store application installed on the device.
- A Google account is not required on devices running Android OS 4.0.4 or higher.

GCM logs can be viewed from the *System* view of the dashboard. They list successful events logged during connections between the *ZENworks Mobile Management* server and the Google Cloud Messaging (GCM) server, and between the *ZENworks Mobile Management* server and Android devices using GCM service (see System Administration Guide: Synchronization Logs).

Obtain your GCM Credentials. Create a Google API project and obtain GCM credentials via the Google APIs Console (see the GCM for Android Setup guide). Only one set of credentials is required per system, regardless of the number of organizations the system hosts. The GCM service can be turned on or left off for each individual organization.

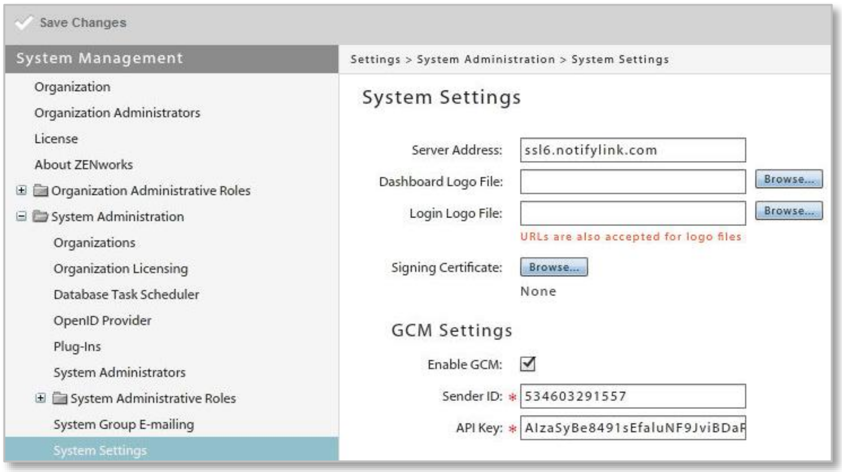
Enter your GCM credentials and enable the GCM service for the system

Once the GCM credentials have been obtained, the GCM service must be enabled for the system on the *ZENworks Mobile Management* server under *System Settings*. GCM credentials (Sender ID and API Key) are also entered here.

Only one set of credentials is required per system, regardless of the number of organizations the system hosts. The GCM service can be turned on or left off for each individual organization.

1. From the *ZENworks Mobile Management* dashboard, select ***System*** > ***System Administration*** > ***System Settings***.

2. Check the box next to **Enable GCM**.
3. Enter the **Sender ID** and the **API Key** that were generated in Steps 1 and 3.
4. Click **Save Changes**.
5. From the *Organization Settings*, turn on the service for each organization that will use GCM.



Server Address: ssl6.notifylink.com

Dashboard Logo File:

Login Logo File:

Signing Certificate: None

Enable GCM: ☑

Sender ID: * 534603291557

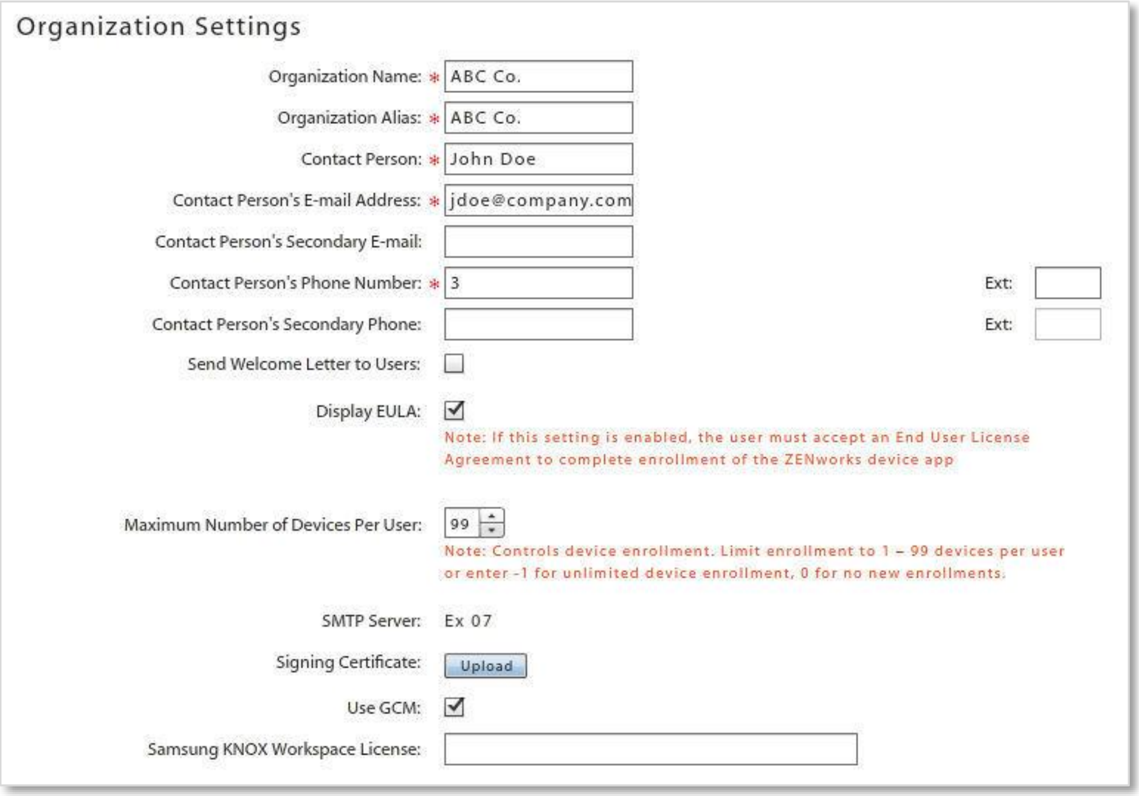
API Key: * AIzaSyBe8491sEfaluNF9JviBDaF

Toggle the service on for each organization that will use GCM

Once the GCM credentials have been entered in the *System Settings*, the GCM service can be turned for individual organizations in *Organization Settings*.

1. From the *ZENworks Mobile Management* dashboard, select ***System*** > ***Organization.***

2. Check the box next to **Use GCM** to turn on the service for the organization.



Organization Settings

Organization Name: *	ABC Co.		
Organization Alias: *	ABC Co.		
Contact Person: *	John Doe		
Contact Person's E-mail Address: *	jdoe@company.com		
Contact Person's Secondary E-mail:			
Contact Person's Phone Number: *	3	Ext:	
Contact Person's Secondary Phone:		Ext:	
Send Welcome Letter to Users:	□		
Display EULA:	☑ Note: If this setting is enabled, the user must accept an End User License Agreement to complete enrollment of the ZENworks device app		
Maximum Number of Devices Per User:	99 Note: Controls device enrollment. Limit enrollment to 1 – 99 devices per user or enter -1 for unlimited device enrollment, 0 for no new enrollments.		
SMTP Server:	Ex 07		
Signing Certificate:	Upload		
Use GCM:	☑		
Samsung KNOX Workspace License:			

3. Click **Save Changes**.

4. To turn on GCM service for other organizations hosted by the system, switch to another organization and mark the **Use GCM** checkbox.

   To switch organizations:
   Select *System* > *System Administration* > *Organizations* and click the **Switch Organizations** button.

Samsung KNOX Workspace License

Enter your organization's license key for Samsung KNOX Workspace. The license key is needed in order to push the Workspace container to KNOX supported Android devices.

To add the KNOX Workspace license:

1. From the dashboard, navigate to **System** > **Organization**.
2. Enter the license code in the **Samsung KNOX Workspace License** field.

Users of KNOX supported devices must be assigned a Policy Suite in which the ***Create KNOX Workspace Container*** rule is enabled. *ZENworks Mobile Management* will push the license to the devices and prompt users to install the KNOX Workspace Container app. This rule is located in the policy suite category ***Samsung KNOX Workspace Policies***.

If a user is assigned a policy that has the Workspace policy enabled, but the license has not been added, the user will not be prompted to install the Workspace app.

To enable the KNOX Workspace Container policy:

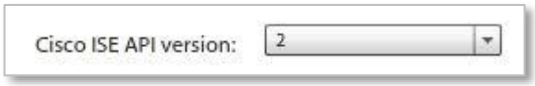
1. From the dashboard, navigate to **Organization** > **Policy Management** > **Policy Suites**.
2. Select a policy suite and choose **Samsung KNOX Workspace Policies**. Enable the **Create KNOX Workspace Container** policy.

Cisco Identity Services Engine (ISE)

Once the Cisco ISE server has been configured for integration with the *ZENworks Mobile Management* server, you must specify the Cisco ISE API version used by the Cisco router. You can do this from the *ZENworks Mobile Management* dashboard. If the Cisco software is upgraded you must update the version specified in the dashboard since Cisco software updates are not backward compatible with API calls used in previous versions.

From the dashboard, navigate to **System** > **Organization**.

Select the ISE API version the Cisco router is using.



Cisco ISE API version: 2

MDM Proxy

The *Organization Settings* page provides an option to disable the *ZENworks Mobile Management* server's function as a proxy for ActiveSync traffic. At installation, the *ZMM* server is configured by default to proxy ActiveSync traffic, including email processed through the ActiveSync server. Disabling this function would primarily be done by an organization wanting to eliminate a possible point of failure for email delivery.

If you disable the MDM proxy:

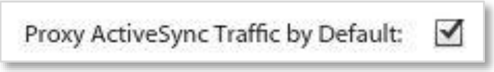
- When the MDM proxy is disabled, managed devices will be configured to connect directly to the ActiveSync server.
- ActiveSync profiles sent to devices carry the ActiveSync server address instead of the *ZENworks* server address.
- Devices connecting directly to the ActiveSync server that have an ActiveSync account, but not the *ZENworks Mobile Management* device application cannot be managed.
- ActiveSync only devices can still connect through the *ZENworks* server if they are enrolled using the *ZENworks* server address. In this case, ActiveSync only devices can be managed as outlined in the *Device Platform Functionality* document.

Alternatives to MDM Proxy:

- Administrators have the option to integrate ActiveSync PowerShell capabilities with *ZENworks Mobile Management*. This will allow you to import device and user information from the ActiveSync server and require enrollment with MDM in order for devices to access email. See ActiveSync Server PowerShell Connection Settings.
- Users with Android KNOX and iOS devices that retrieve email can be assigned a certificate for authenticating against the ActiveSync server. See Configuring an ActiveSync Server to Issue Authentication Certificates.

To disable the MDM proxy:

1. From the dashboard, navigate to ***System*** > ***Organization***.
2. Remove the mark from the checkbox beside ***Proxy ActiveSync Traffic by Default***.



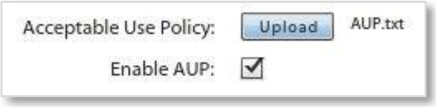
Proxy ActiveSync Traffic by Default: ☑

Acceptable Use Policy

An organization can implement an ***Acceptable Use Policy*** (AUP) that will require end users to agree to follow guidelines for device use and/or for accessing corporate data via the device. When the AUP is enabled, new users must accept the policy in order to complete the enrollment process. Existing users will be prompted to accept the policy as well and will be un-enrolled if they decline.

Changes to the AUP will also prompt existing users to accept an updated policy. If the AUP is declined the device is un-enrolled.

An administrator must upload the policy in an HTML or text file format and then check the ***Enable AUP*** box to implement the policy. The *Acceptable Use Policy* will then be displayed at enrollment and in a prompt on existing user devices.



Acceptable Use Policy: AUP.txt

Enable AUP: ☑

Updating the Policy: If you update the Acceptable Use Policy, send a group message informing end users that they must open the *ZENworks Mobile Management* app to accept the updated policy. Select ***Organization*** > ***Organization Control*** > ***Group Notifications***. Compose either a group notification via APN/GCM push services or a group email.

Provisioning ZENworks Mobile Management as Device Owner for Android 5.0+ Devices

In *Organization Settings*, *Android Device Owner App URL* and *Android Device Owner App Checksum* are both required when administrators need to use Near Field Communication (NFC) provisioning to establish the *ZENworks Mobile Management* application as Device Owner on Android 5.0+ devices.

Android 5.0+ devices must be provisioned with this method in order to use certain Android L functionality.

When *ZENworks Mobile Management* becomes the Device Owner app, certain Android L policies can be applied. A device has to be provisioned with the application using this method only once. Thereafter, users can update the *ZENworks Mobile Management* for Android app through the *ZENworks Mobile Management* portal page or Google Play as new versions are released.

Caution: Provisioning an application as device owner can only be done on the selected Android models that support it. Doing so on devices that do not support it may render a device unusable.

The ***Android Device Owner App URL*** field refers to the URL where the *ZENworks Mobile Management for Android* application can be downloaded.

Android Device Owner App Checksum is what is used to verify that a complete transmission of the application is received when the application is downloaded.
Use the following function to calculate the checksum for the file, MDM_App.apk.

```
cat MDM_App.apk | openssl dgst -binary -sha1 | openssl base64
| tr '+/' '-_' | tr -d '='
```

Important: When the *ZENworks Mobile Management* app is updated, a new checksum must be calculated for the app in order for it to be provisioned on new devices.

To Provision ZENworks Mobile Management as Device Owner:

- ***Android Device Owner App URL*** and ***Android Device Owner App Checksum*** must be entered in the dashboard under *System > Organization > Organization Settings*.
- To provision other Android 5.0+ devices, use an Android 5.0+ device with *ZENworks Mobile Management* v3.8.2 or higher installed.
- Before beginning, verify that the target device has been reset, has the setup screen displayed, and has Wi-Fi connectivity.

1. On the provisioning device, select the **Provision Device Owner** option from the *ZENworks Mobile Management* menu.
2. Hold the provisioning device back-to-back with the target device.
3. A tone indicates that the NFC connection has occurred and the provisioning device now shows a button labeled, **Touch to Beam**. Tap this button.
4. A different tone sounds indicating that the provisioning information has been sent to the target device. The target device will now attempt to download the *ZENworks Mobile Management* app and provision itself.

Once the download and installation are completed, *ZENworks Mobile Management* becomes the Device Owner application and can apply policies requiring device owner or profile owner status. Once a device is provisioned in this way, the *ZENworks Mobile Management* app can be updated, as new versions are released, through the *ZENworks Mobile Management* portal page or Google Play.

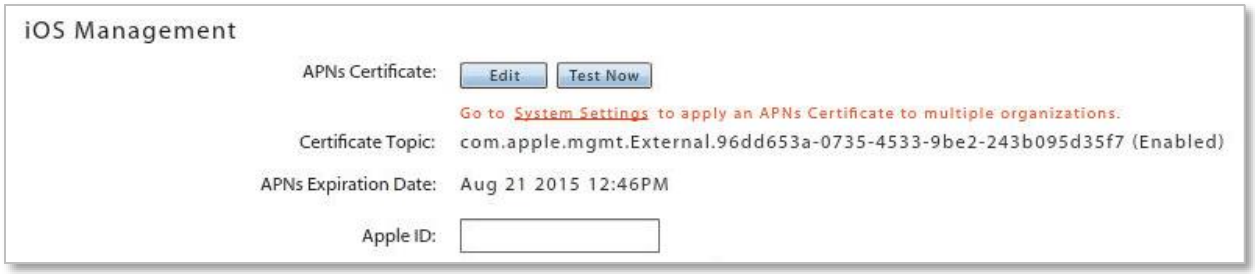
APNs Certificate Set Up

Apple Push Notification Service (APNs) is a highly secure and efficient service for propagating information to the iOS devices in your environment. An APNs certificate applied to the *ZENworks Mobile Management* server provides Apple iOS MDM functionality for iOS devices in your environment. Functionality includes:

- Devices support Selective Wipe, Lock Device, and Clear Passcode
- Full Wipe and Lock Device commands are applied immediately
- You can record and access installed applications on devices
- You can record and access installed configuration profiles on devices
- You have access to additional device statistics
- Configuration profile updates require no user interaction

To access the APNs settings, select ***System*** > ***Organization***

Scroll down to the **iOS Management** information on the **Organization Settings** page to set up or renew a certificate, or to update information associated with the certificate.



iOS Management

APNs Certificate: Edit | Test Now

Go to System Settings to apply an APNs Certificate to multiple organizations.

Certificate Topic: com.apple.mgmt.External.96dd653a-0735-4533-9be2-243b095d35f7 (Enabled)

APNs Expiration Date: Aug 21 2015 12:46PM

Apple ID:

- **APNs Certificate** *Set Up*/Edit button - generate and upload the APNs certificate using the APNs Certificate wizard. At renewal, use the ***Edit*** button. Use the ***Test Now*** button to check the certificate's validity. The test will return the certificate's activation and expiration dates.

  For instructions on using the APNs Certificate wizard, see the Apple Push Notification Guide: Using the APNs Certificate Generation Wizard.

- **APNs Expiration Date** - certificate expiration (annual)
- **Apple ID** - Apple ID associated with the APNs certificate

The APNs certificate settings can be edited if necessary, however, a change to the *Apple ID* associated with the certificate requires iOS device users to reload the APN profile on the device.

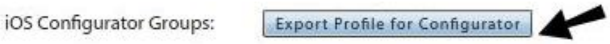
If you have System Administrator privileges, you can apply an existing APNs certificate to multiple organizations on the *ZENworks Mobile Management* server. See also Obtaining an Apple Push Notification Certificate: Applying a Certificate to Multiple Organizations.

iOS Configurator Groups

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. The *ZENworks Mobile Management* app is not installed on the device unless the administrator configures the server to push the app to iOS devices.

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



Any device associated with the Configurator Group will appear on the *ZENworks Mobile Management* User/Device grid with the Configurator Group name. Refer to the Supervised iOS Devices guide for details.

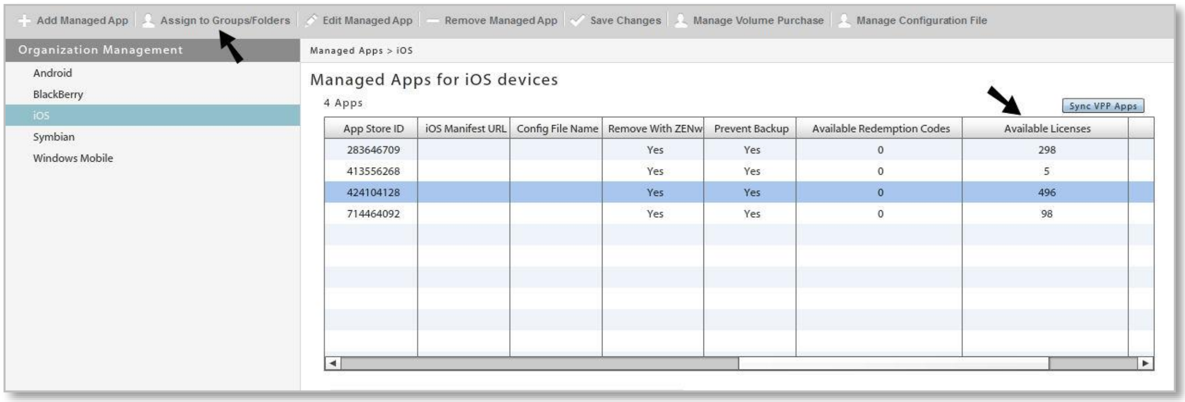
VPP Token Upload

Through Apple’s Volume Purchase Program (VPP), organizations can purchase applications that meet the needs of their users. *ZENworks Mobile Management* provides an efficient way to distribute and manage those applications.

Enroll at: https://deploy.apple.com Other helpful sites: http://www.apple.com/business/vpp/
http://www.apple.com/education/it/vpp/

Once enrolled in the program, Apple will issue your organization a VPP token. When this token is uploaded to the *ZENworks Mobile Management* server, all apps associated with the token populate the *Managed Apps* data grid and users with a qualifying device (running iOS 7.0.3 or higher) receive an invitation to join the Volume Purchase Program. Once the invitation has been accepted, the application(s) are pushed out to the device.

VPP apps can be identified on the *Managed Apps* grid (*Organization* > *Application Management* > *Managed Apps*) by the available licenses listed for each app. The apps can be assigned to an individual user or groups of users via a Policy Suite, LDAP Group/Folder, or Local Group. Use the *Assign to Groups/Folders* button.

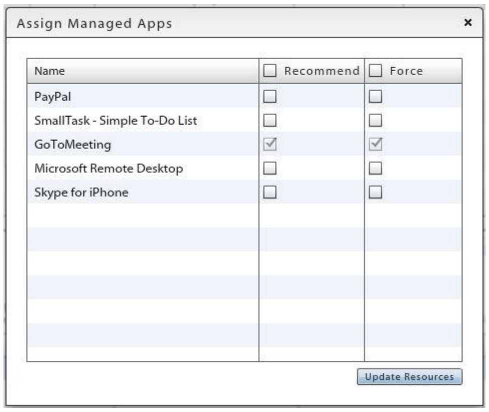


Managed Apps for iOS devices

4 Apps

App Store ID	iOS Manifest URL	Config File Name	Remove With ZENw	Prevent Backup	Available Redemption Codes	Available Licenses
283646709			Yes	Yes	0	298
413556268			Yes	Yes	0	5
424104128			Yes	Yes	0	496
714464092			Yes	Yes	0	98

Assign VPP apps to an individual at the user level. Navigate to *Users* > (select a user) > *Device Profile* > *Corporate Resources* > *Managed App.* Click the *Assign Managed Apps* button.



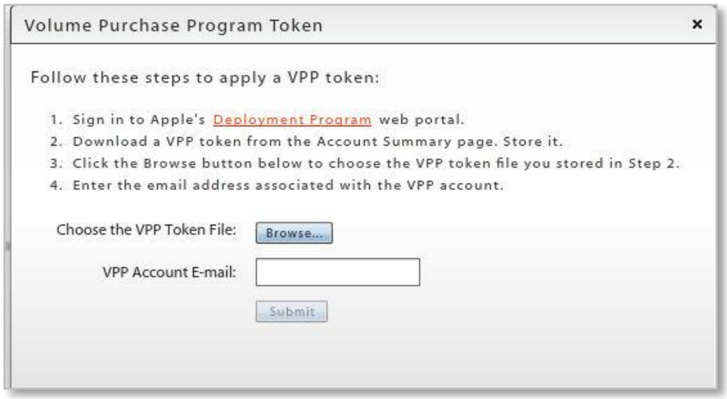
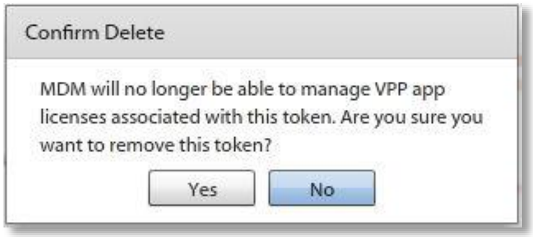
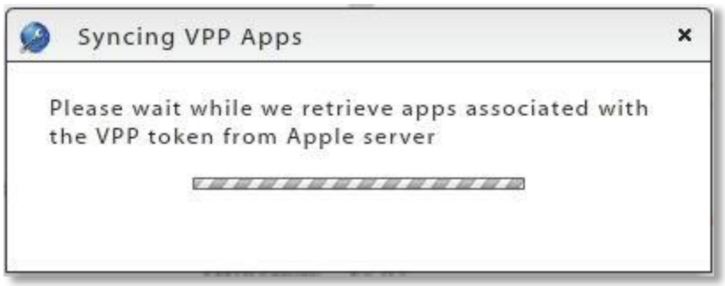
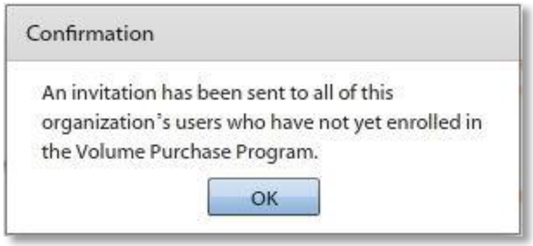
Name	□ Recommend	□ Force
PayPal	□	□
SmallTask - Simple To-Do List	□	□
GoToMeeting	☑	☑
Microsoft Remote Desktop	□	□
Skype for iPhone	□	□

VPP App Licenses can be Reclaimed and Reused. When VPP app assignments are removed from the user device (assuming it is the last iOS 7.0.3+ device associated with the user), they are also removed from the user’s iTunes account and the VPP app license is reclaimed for reuse. This is the advantage of the VPP license model over the VPP redemption code model.

> *Note:* Licenses will not show as reclaimed on the *ZENworks Mobile Management* server until the information has been processed and reported by the Apple server.

VPP licenses are only supported for iOS devices operating on version 7.0.3 or higher. VPP redemption codes can still be used for devices with older iOS versions.

VPP Token Management

Upload/Edit	Click the ***Upload*** button to upload the VPP token issued by Apple. Apps associated with the token are retrieved from the Apple server and qualifying users are invited to join the VPP. Click ***Edit*** to upload a new token or edit/add the E-mail address associated with the VPP account. *Note:* The APNs certificate must be uploaded before managing the VPP token. VPP token will be deleted if APNs certificate is removed.	 Volume Purchase Program Token × Follow these steps to apply a VPP token: 1. Sign in to Apple's Deployment Program web portal. 2. Download a VPP token from the Account Summary page. Store it. 3. Click the Browse button below to choose the VPP token file you stored in Step 2. 4. Enter the email address associated with the VPP account. Choose the VPP Token File: Browse... VPP Account E-mail: Submit
Remove	Removes the token from the server. Apps remain intact in the *Managed Apps* grid and on user devices. License count and automatic discovery of apps, however, no longer function.	 Confirm Delete MDM will no longer be able to manage VPP app licenses associated with this token. Are you sure you want to remove this token? Yes No
Sync Now	Initiates a connection with the Apple server to retrieve the latest information about apps associated with the VPP token. An automatic check is done each time the token is uploaded or edited and each time the *Managed Apps* grid (iOS section) is accessed.	 Syncing VPP Apps × Please wait while we retrieve apps associated with the VPP token from Apple server
Invite Users	Resends the invitation to join VPP to all qualifying users (iOS 7.0.3 or higher) that have not yet enrolled. Once a user accepts the VPP invitation, the application will be pushed out to the device. *Note:* From the *User/Device Grid*, you can invite an individual user. Select the user, then, on the left panel, click ***Send VPP Invitation***.	 Confirmation An invitation has been sent to all of this organization's users who have not yet enrolled in the Volume Purchase Program. OK On the *User/Device Grid*, check the ***VPP Association Status*** column to determine the status of the user's association with the program: *New* (not yet invited), *Invited* (invitation sent, but not yet accepted), or *Associated* (user enrolled in the program).

Apple DEP Token Upload

The Device Enrollment Program (DEP) is part of the Apple Deployment Programs and provides administrators with a streamlined way to deploy multiple organizationally owned iOS devices that are purchased directly from Apple. When a DEP token is uploaded to the *ZENworks Mobile Management* server, information for each device associated with the token populates the User/Device Grid.

Upon device activation, enrollment with the MDM server is automatic and over-the-air configuration of account settings, apps, and IT services is immediate. Each device is associated with an individual user when it is enrolled. Like configurator devices, a DEP device does not install the *ZENworks Mobile Management* app unless the administrator configures the server to push the app to iOS devices.

> ***Note:*** For more information on configuring the system for DEP devices and managing DEP devices, see the Supervised iOS Devices guide.

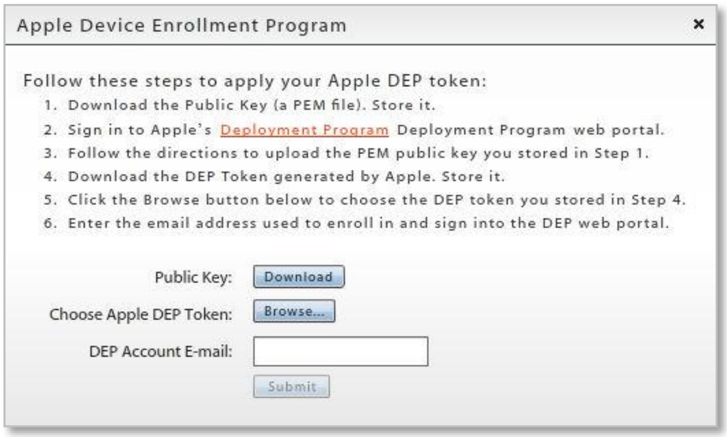
To Upload an Apple DEP Token

You must link the *ZENworks Mobile Management* server to your Apple DEP account. The MDM server will generate a Public Key which you will upload to the Apple web portal. Apple will then issue a token that is associated with the DEP devices your organization has purchased. When this token is uploaded to the *ZENworks Mobile Management* server, information for each device associated with the token populates the User/Device Grid.

DEP devices can be viewed on the *User/Device Grid* by clicking the ***Apple DEP Devices*** button in the upper right corner of the grid.

> *Notes:* The APNs certificate must be uploaded before managing the DEP token. The DEP token will be deleted if the APNs certificate is removed.
>
> You cannot use a single token for multiple organizations. Each organization must have its own token.

1. From the dashboard, navigate to ***System*** > ***Organization***. Click the ***Upload*** button next to the *Apple DEP Token* field. A pop-up appears.



Apple Device Enrollment Program

Follow these steps to apply your Apple DEP token:

1. Download the Public Key (a PEM file). Store it.
2. Sign in to Apple's Deployment Program Deployment Program web portal.
3. Follow the directions to upload the PEM public key you stored in Step 1.
4. Download the DEP Token generated by Apple. Store it.
5. Click the Browse button below to choose the DEP token you stored in Step 4.
6. Enter the email address used to enroll in and sign into the DEP web portal.

2. Click the ***Download*** button next to the *Public Key* field.
3. The MDM server generates the Public Key (a .PEM file labeled *MDM_DEP_Public_Key.PEM* by default). Save the file somewhere on your server.
4. Click the link to Apple's Deployment Program web portal and follow the directions to upload the .PEM file you stored. Apple will issue a DEP token.
5. Download the DEP token and save it somewhere on your server.

6. Click the ***Browse*** button next to the *Choose Apple DEP Token* field to choose the DEP token you stored.
7. Enter the email address you used to enroll in and sign into the DEP web portal (*optional*).
8. Click the ***Submit*** button. Devices associated with the token are retrieved from the Apple server and will populate the User/Device Grid.

The *ZENworks Mobile Management* server generates a default profile for devices associated with the token. The profile is applied to each device as it is activated by a user.

NPNS Certificate

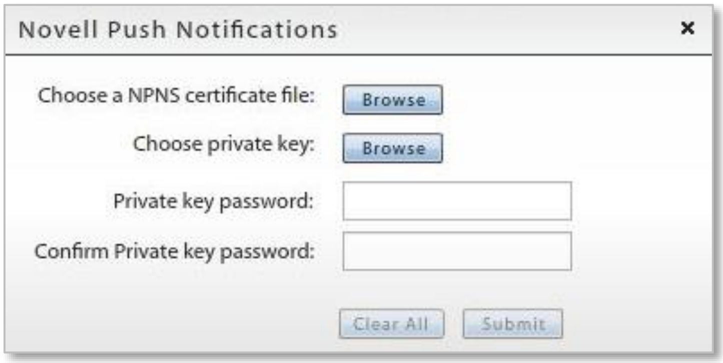
A Novell Push Notification Service (NPNS) certificate is necessary in order to send *Group Notifications* to iOS devices. The certificate enables the *ZENworks Mobile Management* server to connect with and send its notification to the NPNS, which in turn pushes the notification to the target iOS device(s).

The NPNS certificate must be renewed annually. You can set an alert in Compliance Manager as a reminder.

Upload the NPNS Certificate and Private Key

Obtain the NPNS certificate and private key then upload them to the *ZENworks Mobile Management* server. The same process is used for uploading a renewed certificate.

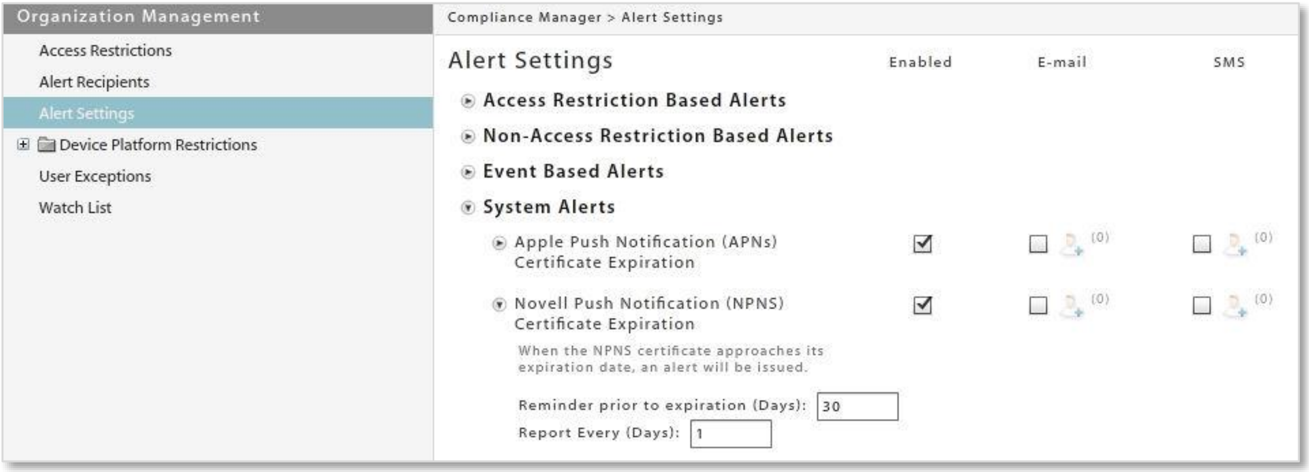
1. From the dashboard, navigate to ***System*** > ***Organization***. Click the ***Upload*** button next to the *NPNS Certificate* field. A pop-up appears.


Novell Push Notifications
×
Choose a NPNS certificate file:
Browse
Choose private key:
Browse
Private key password:
Confirm Private key password:
Clear All
Submit

2. Click the Browse button to select and upload the NPNS certificate file.
3. Click the Browse button to select and upload the private key.
4. Create a password for the private key. There is no need to record the password as it is used for encryption purposes only.

To set the NPNS Certificate Expiration alert:

- From the ***Organization*** page select ***Compliance Manager*** > ***Alert Settings*** > ***System Alerts***.
- Enable the ***Novell Push Notification (NPNS) Certificate Expiration*** alert and configure when you want the reminder to begin and how often to be reminded. The default settings are to issue the reminder 30 days prior to the expiration and repeat it every day.
- You can also choose to have an E-mail and/or SMS alert sent to an administrator.



	Enabled	E-mail	SMS
Apple Push Notification (APNs) Certificate Expiration	☑	□ (0)	□ (0)
Novell Push Notification (NPNS) Certificate Expiration	☑	□ (0)	□ (0)

When the NPNS certificate approaches its expiration date, an alert will be issued.

Reminder prior to expiration (Days): 30

Report Every (Days): 1

Pushing the ZENworks App to iOS Devices

iOS devices do not need to have the *ZENworks Mobile Management* app installed in order to enroll with the *ZENworks* server. From the device, users can navigate to **<yourServerAddress>/mobile/ios**. The server creates a configuration file using the device's authentication token and the server address. It then pushes the MDM profile down to the device.

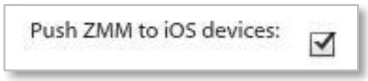
Pushing the *ZENworks Mobile Management* app to the device as a managed app. If desired, an administrator can configure the system to push the *ZENworks* app to devices as well. Installation occurs after the profile loads. The app is treated as a managed app.

When the option to push the app is enabled, the app will be installed on any iOS device that enrolls without the app. This includes:

- Devices enrolled via the *ZENworks Mobile Management* web page at <yourServerAddress>/mobile/ios (App-less enrollment)
- DEP or Configurator devices
- Devices enrolled via the Cisco Identity Services Engine (ISE)

To enable the push option:

1. From the dashboard, navigate to ***System*** > ***Organization***.
2. Mark the checkbox beside, ***Push ZMM to iOS devices***.



Push ZMM to iOS devices: ☑

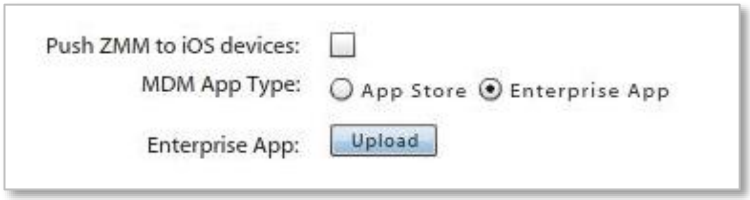
Upload an Enterprise App and Certificate for App Notifications

With *ZENworks Mobile Management* server version 3.8.0 or greater, administrators have the ability, through the *ZENworks* dashboard, to upload the enterprise app or provide a URL from which users can obtain the application. If they upload the app, they can then elect to push the app to iOS devices by marking the checkbox next to **Push ZMM to iOS Devices**.

Administrators can also upload the Apple Push Notification service SSL Certificate necessary to support the Group Notification feature.

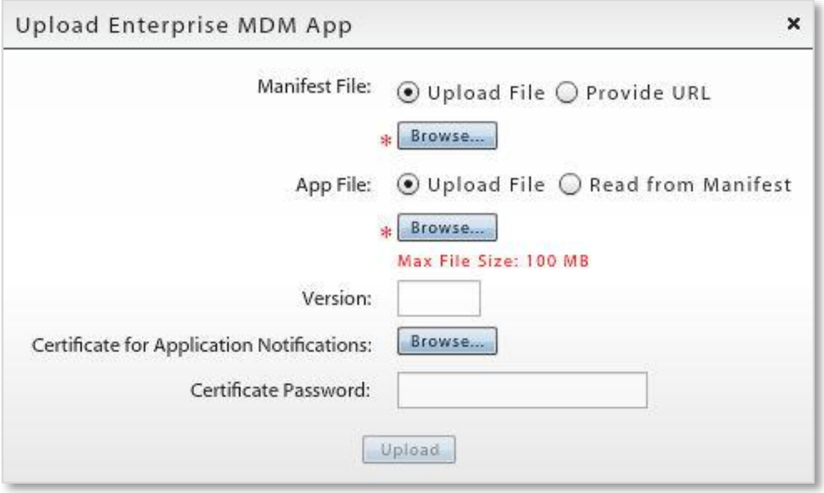
Those using *ZENworks* server versions less than 3.8.0 must use the distribution methods described in the guide mentioned above.

1. From the *ZENworks Mobile Management* dashboard, select **System** > **Organization**.
2. On the *Organization Settings* page scroll down to the *iOS Management* section and select *Enterprise App* from the **MDM App Type** field.



Push ZMM to iOS devices: □
MDM App Type: ○ App Store ● Enterprise App
Enterprise App: Upload

3. Click the **Upload (Edit)** button next to the **Enterprise App** field.
4. From the **Manifest File** field, select **Upload File** and browse to select the file or select **Provide URL** and enter the link from which the app can be downloaded.



Upload Enterprise MDM App ×

Manifest File: ● Upload File ○ Provide URL
* Browse...
App File: ● Upload File ○ Read from Manifest
* Browse...
Max File Size: 100 MB
Version:
Certificate for Application Notifications: Browse...
Certificate Password:
Upload

5. From the **App File**, if you uploaded the manifest file, select **Upload File** and browse to select the app file or select **Read from Manifest** to pull app file information from the manifest.
6. Enter the **Version** number of the enterprise app.
7. (Optional) Browse to select the **Certificate for Application Notifications**, then enter the **Certificate Password**.

You can make updated versions of the app available to users in the same way.

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

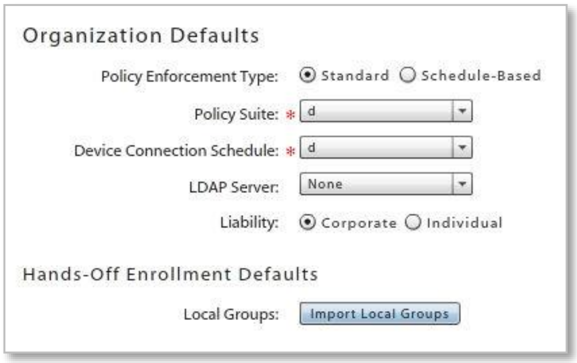
Systems where iOS users are interfacing with a Novell GroupWise DataSync server must use DataSync Update 4 (Mobility 1.2.4) to fully utilize the hands-off enrollment functionality. Users need to enroll using their entire email address in lieu of their username if they are enrolling by the hands-off method. 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

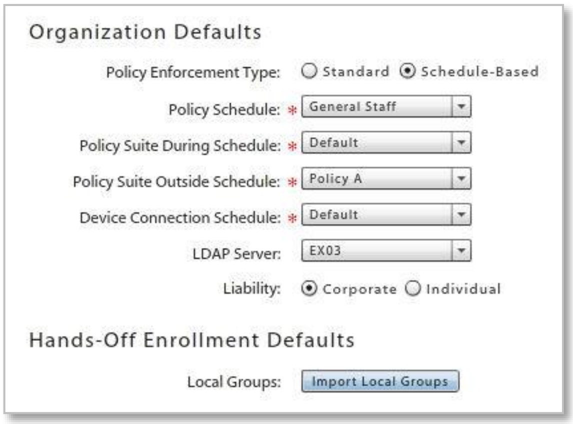
Device Connection Schedule: * d

LDAP Server: None

Liability: ● Corporate ○ Individual

Hands-Off Enrollment Defaults

Local Groups:



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

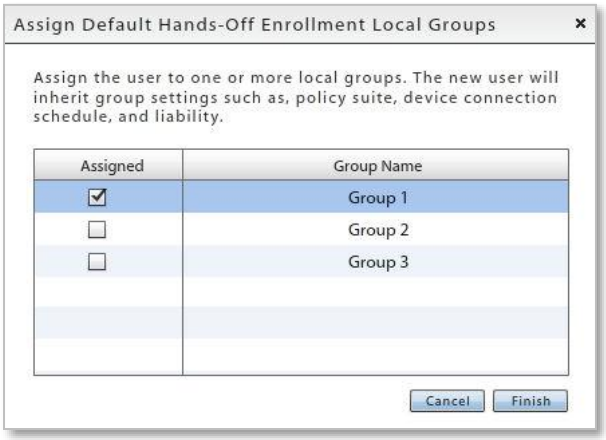
Local Groups:

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.



Assign the user to one or more local groups. The new user will inherit group settings such as, policy suite, device connection schedule, and liability.

Assigned	Group Name
☑	Group 1
□	Group 2
□	Group 3

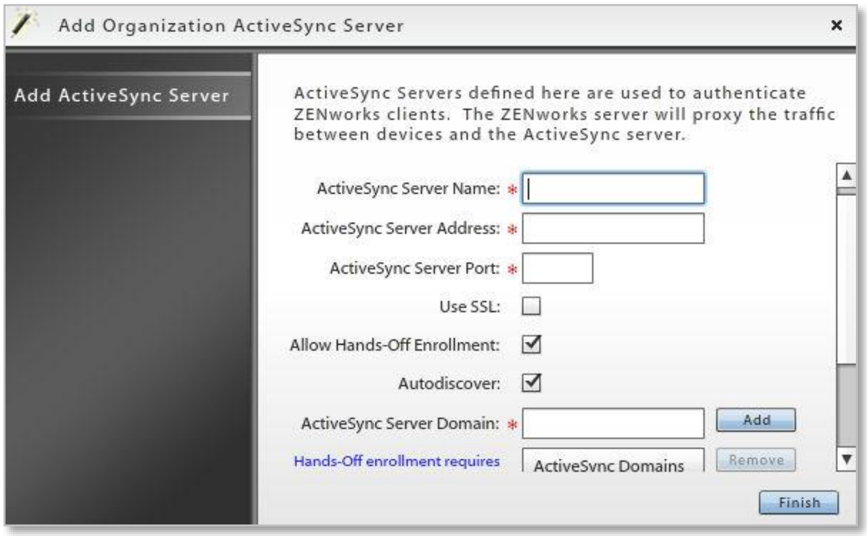
Enabling Hands-Off Enrollment for Users Associated with an ActiveSync Server

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***.



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

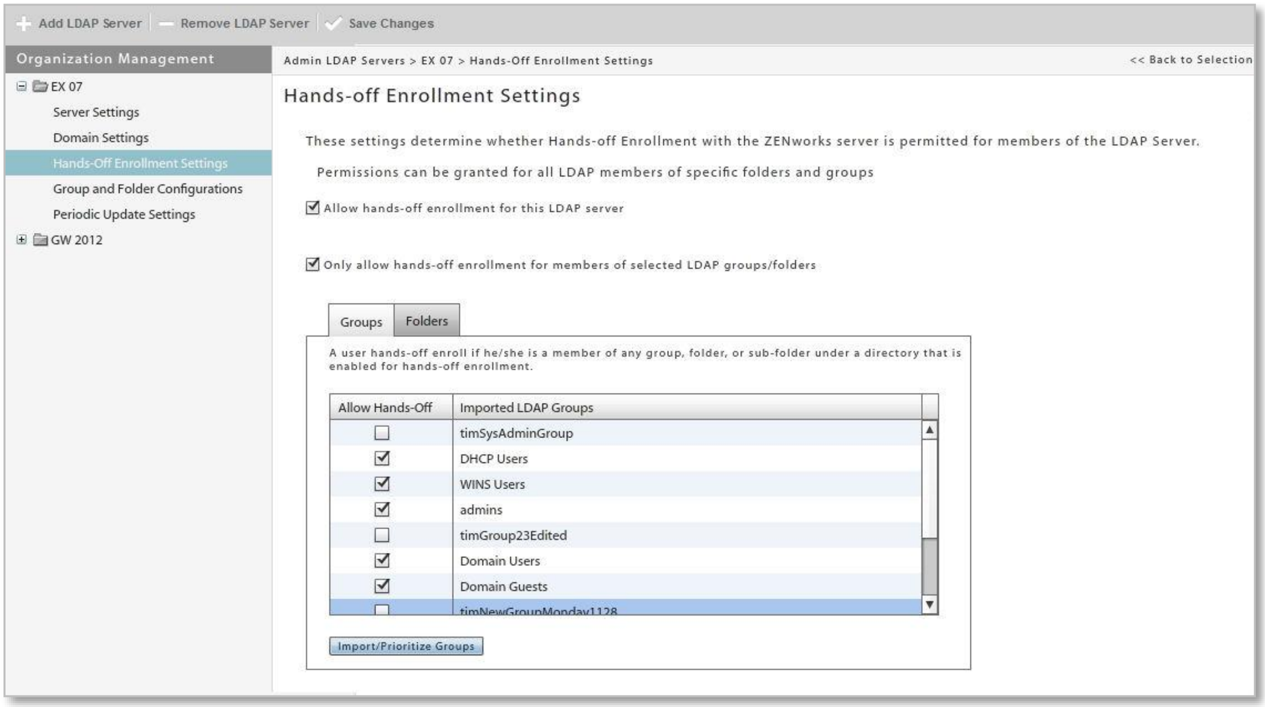
Enabling Hands-Off Enrollment for Users Associated with an LDAP Server

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.



Admin LDAP Servers > EX 07 > Hands-Off Enrollment Settings

Hands-off Enrollment Settings

These settings determine whether Hands-off Enrollment with the ZENworks server is permitted for members of the LDAP Server.

Permissions can be granted for all LDAP members of specific folders and groups

☑ Allow hands-off enrollment for this LDAP server

☑ Only allow hands-off enrollment for members of selected LDAP groups/folders

A user hands-off enroll if he/she is a member of any group, folder, or sub-folder under a directory that is enabled for hands-off enrollment.

Allow Hands-Off	Imported LDAP Groups
☐	timSysAdminGroup
☑	DHCP Users
☑	WINS Users
☑	admins
☐	timGroup23Edited
☑	Domain Users
☑	Domain Guests
☐	timNewGroupMonday1128

Configuring the System for SAML Authentication

Security Assertion Markup Language (SAML) is an XML-based standard data format for authenticating and authorizing data between an identity provider and a service provider. SAML provides single sign-on authentication for end-users.

As integrated with *ZENworks Mobile Management*, SAML authentication of end-users will occur:

- Prior to downloading the MDM profile on initial enrollment of iOS devices
- When performing initial enrollment of the *MDM* application for Android
- To grant access to the User Self-Administration Portal
- To grant access to the web-based Managed Applications list

How SAML Works

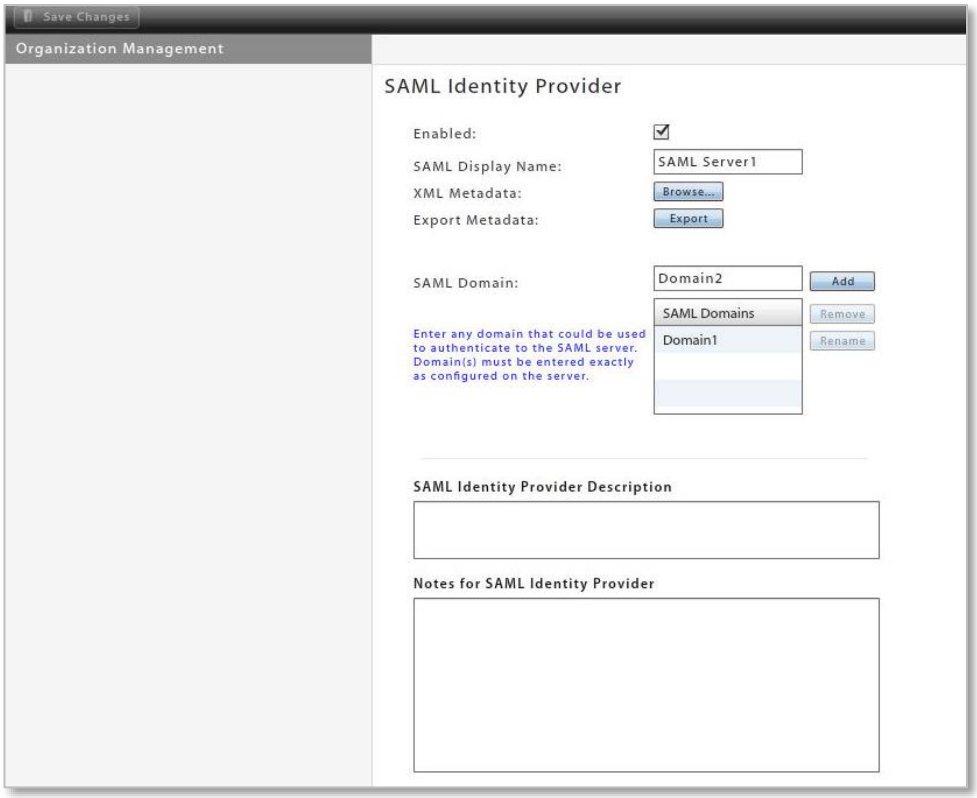
The SAML solution defines three roles: the principal (or end-user), the service provider (your organization), and the identity provider (the SAML server*). The end-user requests service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. Based on that assertion, the service provider determines whether the end-user's request should be granted.

> ***Note:** *ZENworks Mobile Management* has been tested against the following SAML servers: Novell Access Manager (NAM), Oracle Identity Federation (OIF), and SimpleSAMLphp.

To configure the *ZENworks Mobile Management* system for SAML authentication, you must provide an XML file containing the configuration information that identifies your SAML identity provider. You must also export an XML file containing the configuration information that identifies your organization's server.

1. From the dashboard, navigate to ***Organization*** > ***Administrative Servers*** > ***SAML Identity Provider***.
2. Check the ***Enabled*** box.

   Note: SAML Identity Provider information cannot be edited unless this box is checked.
3. Define the following:
   a. ***SAML Display Name*** - Enter a friendly name by which your SAML server will be identified in the dashboard.
   b. ***XML Metadata*** - Browse to locate and enter the XML file containing the configuration information that identifies your SAML identity provider. When you have successfully uploaded the file, the file name is displayed.
   c. ***Export Metadata*** – Export the XML file containing the configuration information that identifies your organization's SAML server.
   d. ***SAML Domain*** – Enter any domain that could be used to authenticate to the SAML server. Domain(s) must be entered exactly as configured on the server.



Enabled: ☑

SAML Display Name: SAML Server1

XML Metadata:

Export Metadata:

SAML Domain: Domain2

Enter any domain that could be used to authenticate to the SAML server. Domain(s) must be entered exactly as configured on the server.

SAML Domains
Domain1

SAML Identity Provider Description

Notes for SAML Identity Provider

4. Enter a ***Description*** and/or ***Notes*** for the SAML Identity Provider (optional).
5. Click ***Save Changes***.

Policy Suite Management

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.

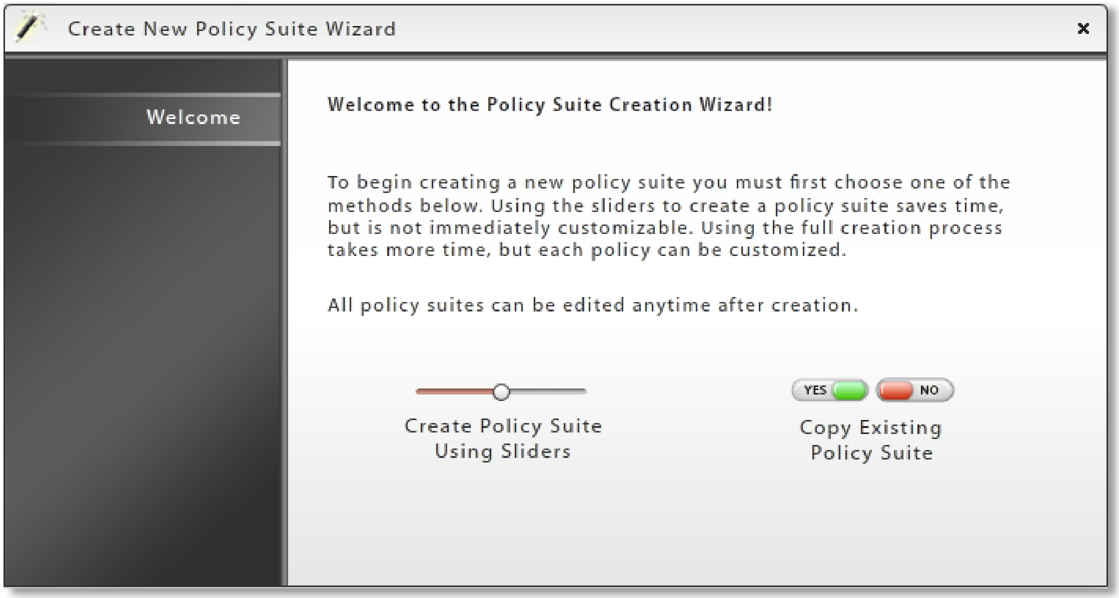
Policy rules are categorized into the following groups:

- Audit Tracking
- Device Control
- File Share Permission
- iOS Devices
- Resource Control
- Samsung KNOX Device Policies
- Samsung KNOX Workspace Policies
- Security Settings
- S/MIME Settings
- TouchDown
- Whitelists/Blacklists Permissions

Policy Suites

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.


Create New Policy Suite Wizard
Welcome

Welcome to the Policy Suite Creation Wizard!

To begin creating a new policy suite you must first choose one of the methods below. Using the sliders to create a policy suite saves time, but is not immediately customizable. Using the full creation process takes more time, but each policy can be customized.

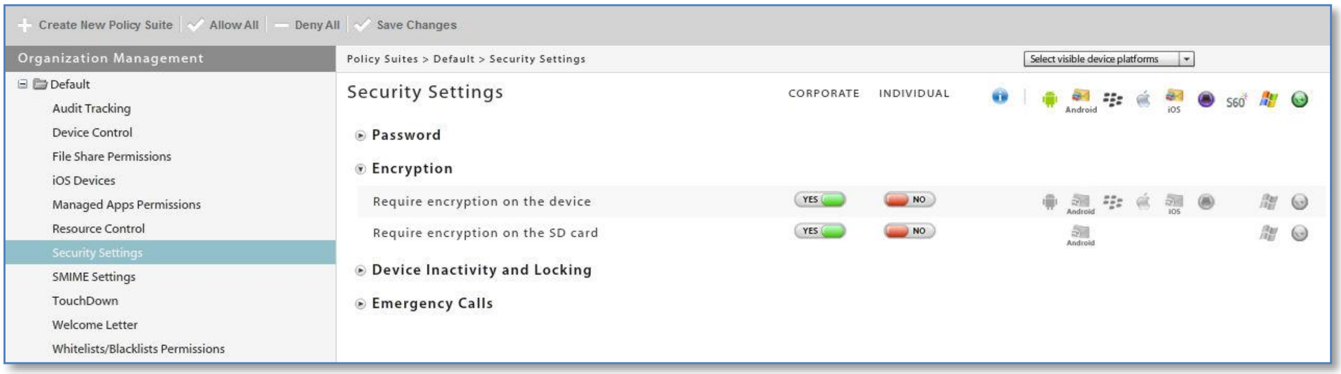
All policy suites can be edited anytime after creation.

Create Policy Suite Using Sliders
YES
NO
Copy Existing Policy Suite

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***.



Require encryption on the device YES NO

Require encryption on the SD card YES NO

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.

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:

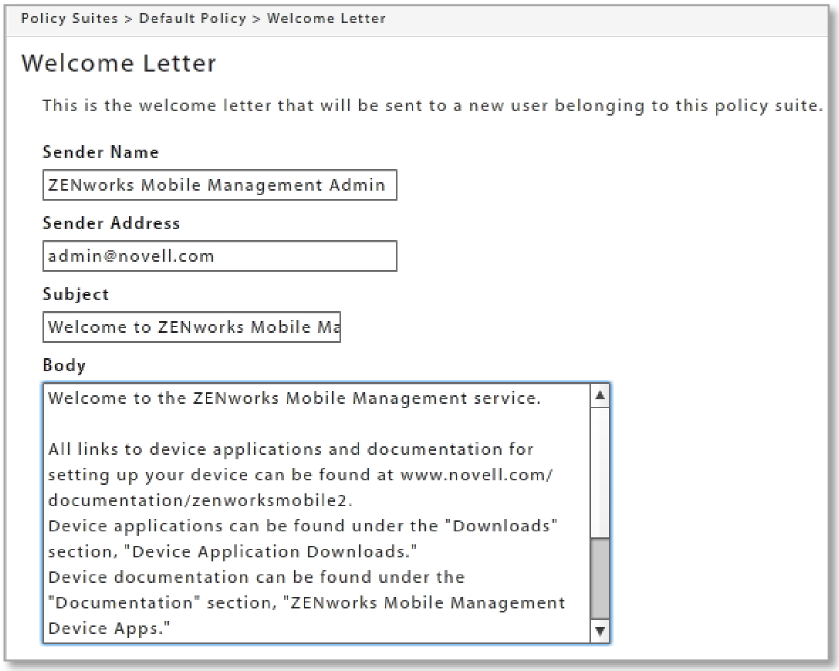
- Links to resources, such as the device app downloads, user documentation, and the user self-administration portal
- Details of policies that may change device functionality
- New features that make devices more secure

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 *Device Panel*.

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



Policy Suites > Default Policy > Welcome Letter

Welcome Letter

This is the welcome letter that will be sent to a new user belonging to this policy suite.

Sender Name

ZENworks Mobile Management Admin

Sender Address

admin@novell.com

Subject

Welcome to ZENworks Mobile Ma

Body

Welcome to the ZENworks Mobile Management service.

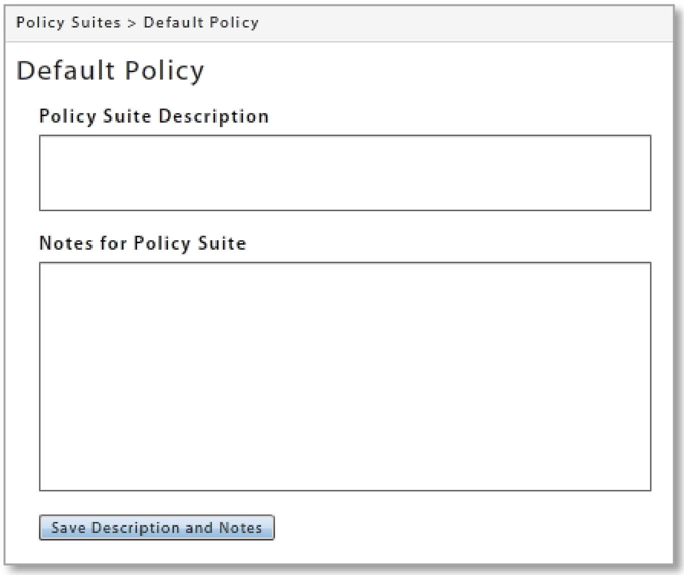
All links to device applications and documentation for setting up your device can be found at www.novell.com/documentation/zenworksmobile2.
Device applications can be found under the "Downloads" section, "Device Application Downloads."
Device documentation can be found under the "Documentation" section, "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

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
- Device Control
- File Share Permissions
- iOS Devices
- Resource Control
- Samsung KNOX Device Policies
- Samsung KNOX Workspace Policies
- Security Settings
- SMIME Settings
- TouchDown
- Whitelists/Blacklists Permissions

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:*** 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**
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)
2	Cell towers only; approximate location, low power, 800 meters distance	Cell towers and GPS; no set accuracy	Cell towers only
3	Cell towers only; Approximate location, low power, 600 meters distance	Cell towers and GPS; 100 meters	Cell towers only
4	GPS; approximate location, low power, 400 meters distance	Cell towers and GPS; 50 meters	GPS; 500 meters to 1 kilometer
5	GPS; fine location, high power, 200 meter distance *Note:* Device constantly checks, even in situations where it is not moving.	Cell towers and GPS; 25 meters	GPS; 100 meters
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.
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)***

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* view of the dashboard.

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.

Samsung KNOX Device Policies

Samsung KNOX Device Policies are applicable for Samsung KNOX devices only.

See a list of Samsung KNOX devices and the certified devices chart for KNOX devices that have been tested and are supported.

KNOX Device policies include policies that allow administrators to create an alternate home screen, restrict access to applications and device features, specify HTTP proxy settings, and enforce password policies. It also allows the administrator to apply the Kiosk Mode which provides a way to specify a single application to which KNOX devices will be locked. See also Managing Users and Resources Guide: Kiosk Mode Apps

Samsung KNOX Workspace Policies

Samsung KNOX Workspace Policies are applicable for Samsung Workspace supported devices only. See a list of Samsung KNOX Workspace Supported devices.

Administrators can install the KNOX Workspace container on supported devices by simply enabling the ***Create KNOX Workspace Container*** option. The container is a virtual Android environment within the mobile device, complete with its own home screen, launcher, apps, and widgets. It keeps corporate information separated from the user's personal space on the device.

Samsung KNOX Workspace employs many of the same KNOX Device password and restrictions policies.

Email. If an email address has been added to the user's *ZENworks Mobile Management* account, the user's email will migrate to the container.

Apps. For KNOX 2.0: Any enterprise app installed after the container has been created is installed within the container. App store apps are installed outside the container. For KNOX 1.0: Only wrapped enterprise apps are installed inside the container.

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.

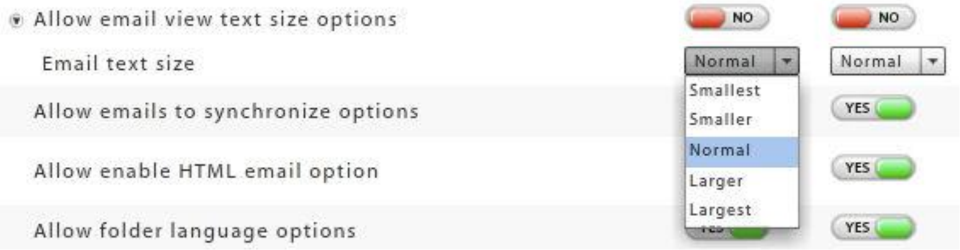
An enabled suppression policy gives the user control of the setting. The policy is enabled when set to YES.

Allow email alerts configuration YES 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:



Allow email view text size options NO NO

Email text size Normal Normal

Allow emails to synchronize options YES

Allow enable HTML email option YES

Allow folder language options YES

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:

Allow email alerts configuration NO NO

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.

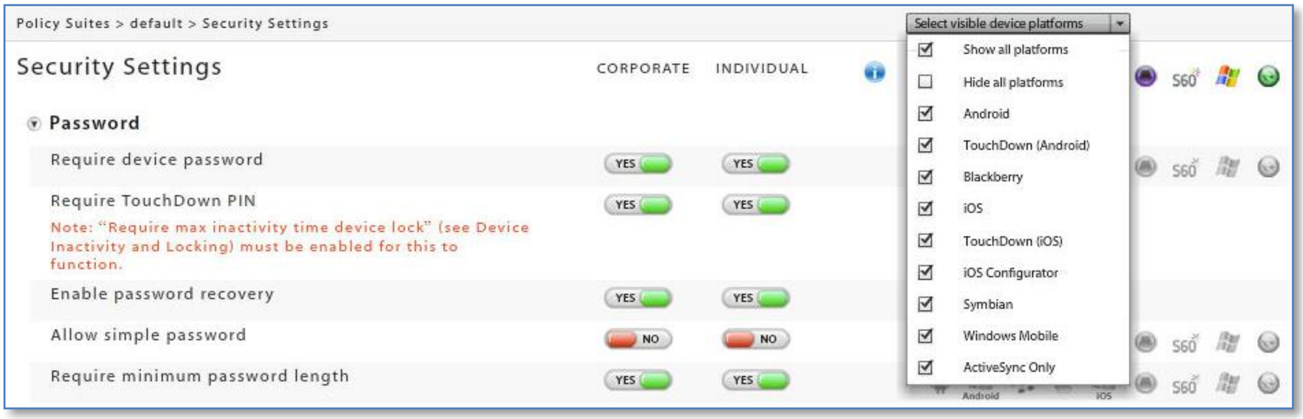
The list of blacklist filter strings must be enabled in *Restricted Apps Permissions* in order for the restrictions to take effect.

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.



Policy Suites > default > Security Settings

Select visible device platforms

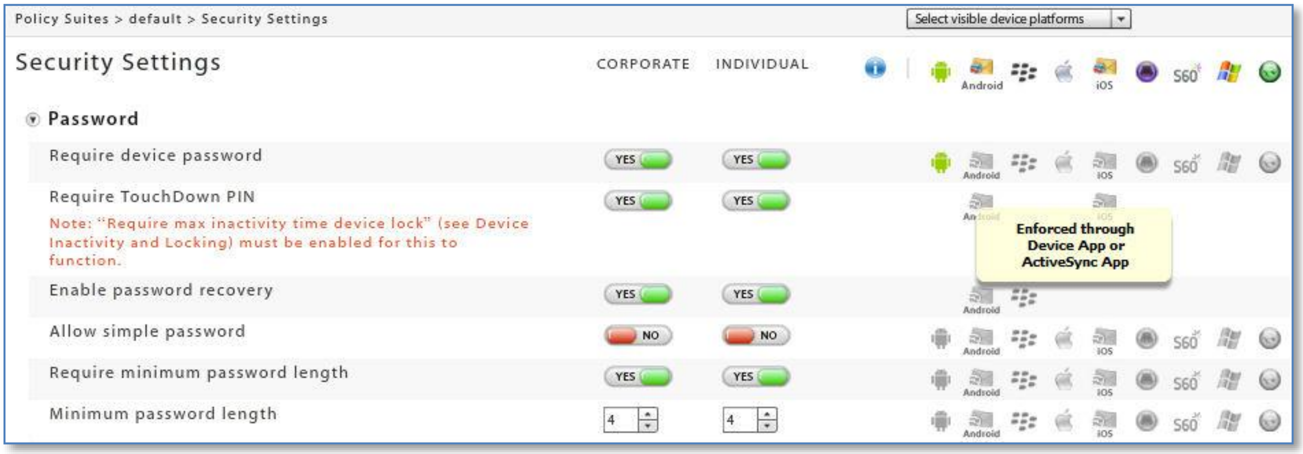
- ☑ Show all platforms
- ☐ Hide all platforms
- ☑ Android
- ☑ TouchDown (Android)
- ☑ Blackberry
- ☑ iOS
- ☑ TouchDown (iOS)
- ☑ iOS Configurator
- ☑ Symbian
- ☑ Windows Mobile
- ☑ ActiveSync Only

Security Settings

Password

	CORPORATE	INDIVIDUAL
Require device password	YES	YES
Require TouchDown PIN Note: "Require max inactivity time device lock" (see Device Inactivity and Locking) must be enabled for this to function.	YES	YES
Enable password recovery	YES	YES
Allow simple password	NO	NO
Require minimum password length	YES	YES

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



Policy Suites > default > Security Settings

Select visible device platforms

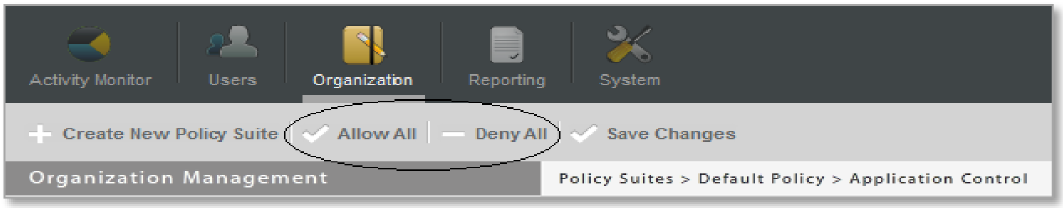
Security Settings

Password

	CORPORATE	INDIVIDUAL
Require device password	YES	YES
Require TouchDown PIN Note: "Require max inactivity time device lock" (see Device Inactivity and Locking) must be enabled for this to function.	YES	YES
Enable password recovery	YES	YES
Allow simple password	NO	NO
Require minimum password length	YES	YES
Minimum password length	4	4

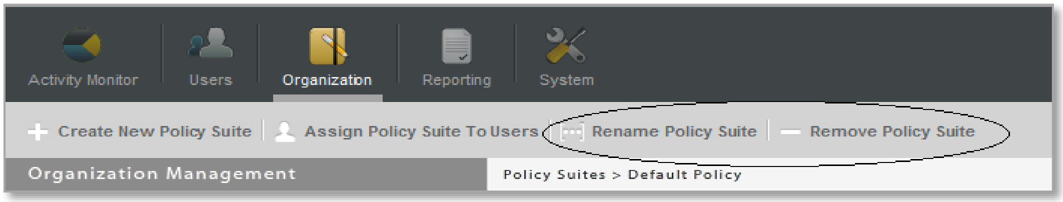
- Click the ⓘ symbol to access the Device Platform Functionality table from the dashboard. This table gives descriptions of each policy and details the functionality across each device platform. The document is also available via the ZENworks Mobile Management documentation portal. [Device Platform Functionality]()

- 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.

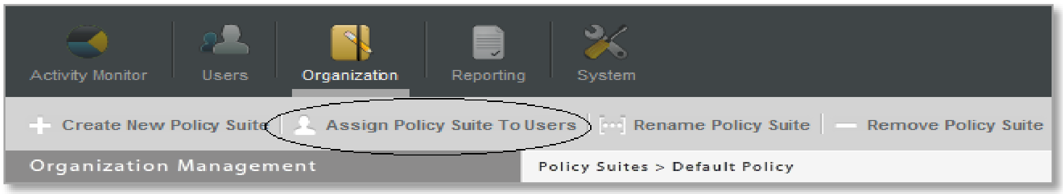


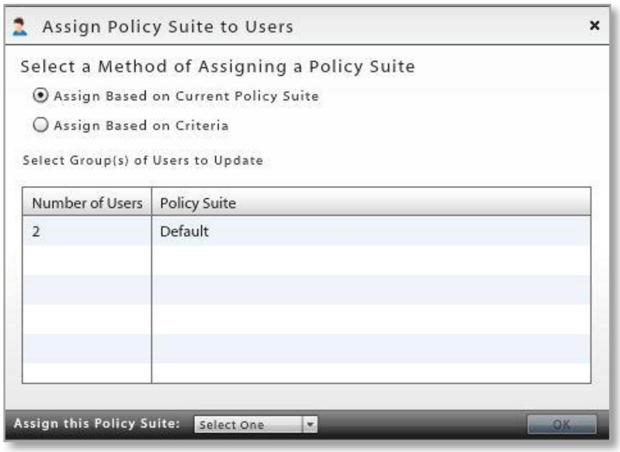
- Some policies determine the options available for other policies. For example, Allow Browser in the Device Control section must be enabled if you plan to enable Allow Safari for iOS devices.

- 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 *Device 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.





Assign Policy Suite to Users ×

Select a Method of Assigning a Policy Suite

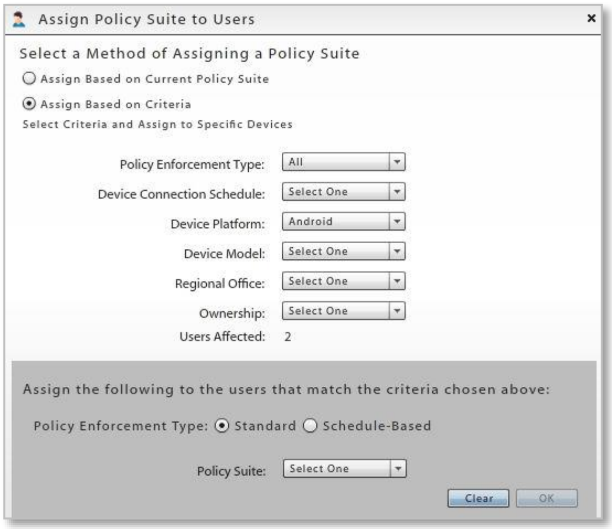
● Assign Based on Current Policy Suite

○ Assign Based on Criteria

Select Group(s) of Users to Update

Number of Users	Policy Suite
2	Default

Assign this Policy Suite: Select One



Assign Policy Suite to Users ×

Select a Method of Assigning a Policy Suite

○ Assign Based on Current Policy Suite

● Assign Based on Criteria

Select Criteria and Assign to Specific Devices

Policy Enforcement Type:	All
Device Connection Schedule:	Select One
Device Platform:	Android
Device Model:	Select One
Regional Office:	Select One
Ownership:	Select One
Users Affected:	2

Assign the following to the users that match the criteria chosen above:

Policy Enforcement Type: ● Standard ○ Schedule-Based

Policy Suite: Select One

Policy Schedules

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

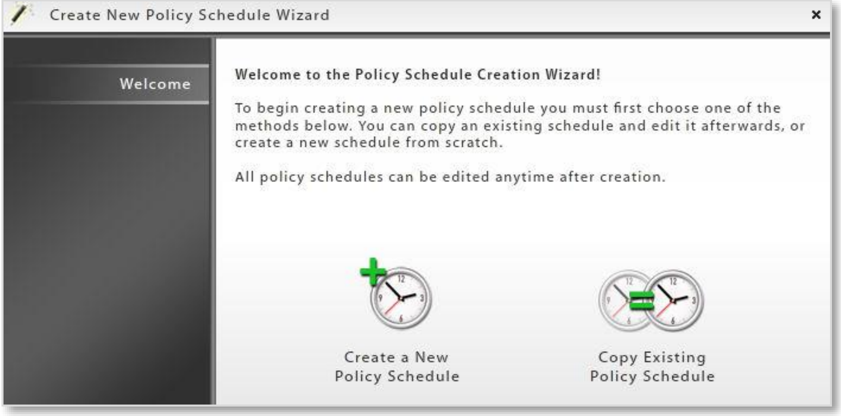
Two Policy Suites can be assigned to an individual user, all users in a LDAP group/folder, or all users in the organization. One Policy Suite governs user devices during scheduled hours, the other governs user devices outside scheduled hours. The schedule determines when each Policy Suite is in effect.

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***.
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.



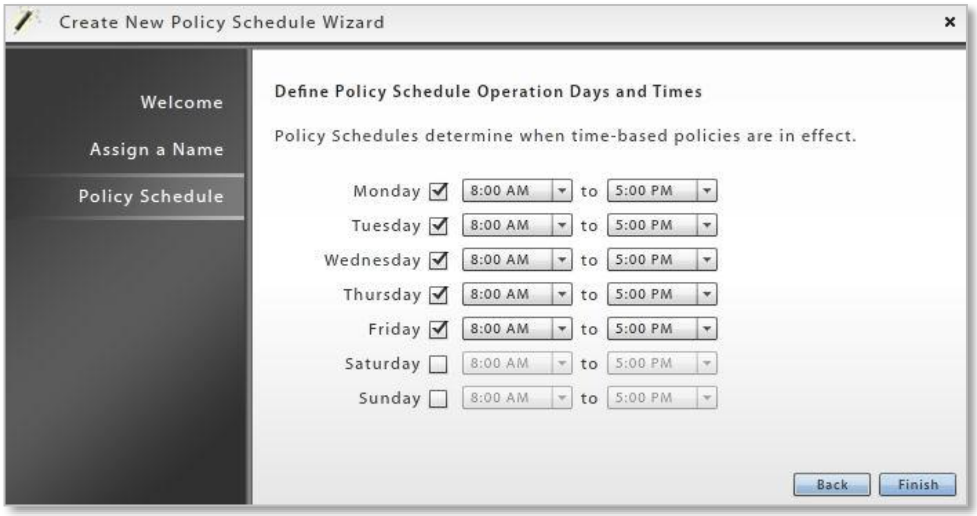
Create New Policy Schedule Wizard

Welcome to the Policy Schedule Creation Wizard!

To begin creating a new policy schedule you must first choose one of the methods below. You can copy an existing schedule and edit it afterwards, or create a new schedule from scratch.

All policy schedules can be edited anytime after creation.

5. Enter a name for the new schedule.
6. Define the hours during which users are working, Monday through Sunday.



Define Policy Schedule Operation Days and Times

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

Monday	☑	8:00 AM	to	5:00 PM
Tuesday	☑	8:00 AM	to	5:00 PM
Wednesday	☑	8:00 AM	to	5:00 PM
Thursday	☑	8:00 AM	to	5:00 PM
Friday	☑	8:00 AM	to	5:00 PM
Saturday	□	8:00 AM	to	5:00 PM
Sunday	□	8:00 AM	to	5:00 PM

Assign a Policy Schedule

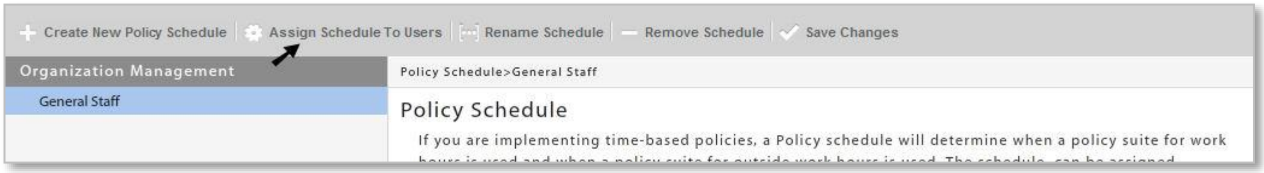
Assign the Policy Schedule to:

- an individual user (*Device 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.

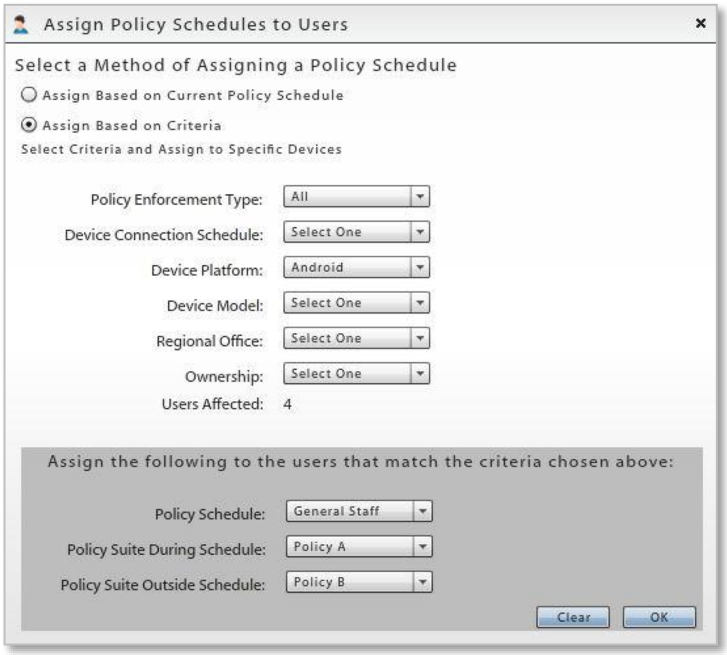
To assign a schedule to all users currently assigned to another Policy Schedule or users that meet selected criteria,

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***.



Policy Schedule

If you are implementing time-based policies, a Policy schedule will determine when a policy suite for work


Assign Policy Schedules to Users

Select a Method of Assigning a Policy Schedule

○ Assign Based on Current Policy Schedule

● Assign Based on Criteria

Select Criteria and Assign to Specific Devices

Policy Enforcement Type: All

Device Connection Schedule: Select One

Device Platform: Android

Device Model: Select One

Regional Office: Select One

Ownership: Select One

Users Affected: 4

Assign the following to the users that match the criteria chosen above:

Policy Schedule: General Staff

Policy Suite During Schedule: Policy A

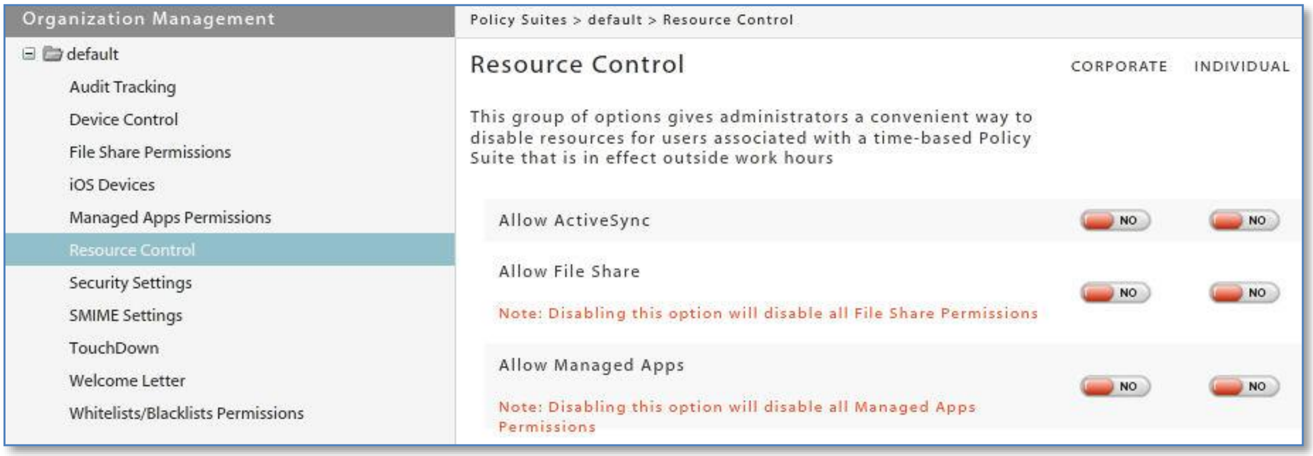
Policy Suite Outside Schedule: Policy B

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.



Resource Control

This group of options gives administrators a convenient way to disable resources for users associated with a time-based Policy Suite that is in effect outside work hours

	CORPORATE	INDIVIDUAL
Allow ActiveSync	NO	NO
Allow File Share Note: Disabling this option will disable all File Share Permissions	NO	NO
Allow Managed Apps Note: Disabling this option will disable all Managed Apps Permissions	NO	NO

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

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 in disabled). Regulating the interval at which devices connect should be considered carefully to minimize the device battery depletion.

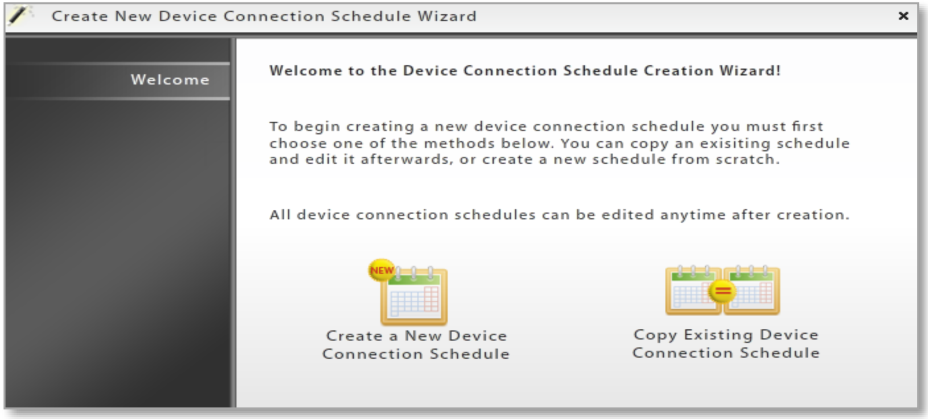
Schedules defined here do not affect ActiveSync synchronization of email/PIM. The device connection schedule controls only the synchronization frequency of *ZENworks Mobile Management* data, such as device statistics, location, and audit tracking data.

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.



Create New Device Connection Schedule Wizard

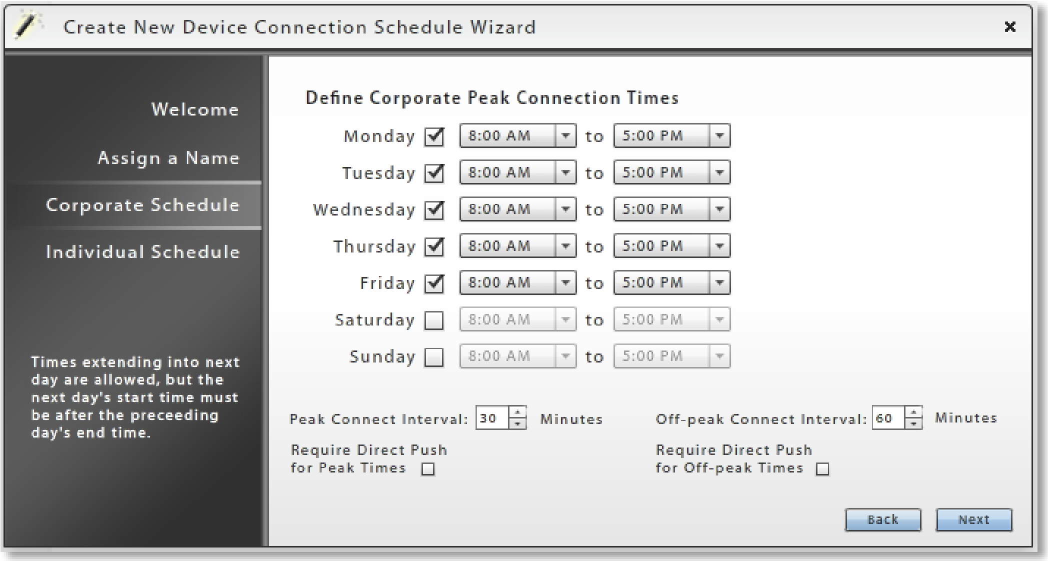
Welcome to the Device Connection Schedule Creation Wizard!

To begin creating a new device connection schedule you must first choose one of the methods below. You can copy an exisiting schedule and edit it afterwards, or create a new schedule from scratch.

All device connection schedules can be edited anytime after creation.

Welcome
NEW
Create a New Device Connection Schedule
Copy Existing Device Connection 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



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

Define Corporate Peak Connection Times

Monday	☑	8:00 AM	to	5:00 PM
Tuesday	☑	8:00 AM	to	5:00 PM
Wednesday	☑	8:00 AM	to	5:00 PM
Thursday	☑	8:00 AM	to	5:00 PM
Friday	☑	8:00 AM	to	5:00 PM
Saturday	□	8:00 AM	to	5:00 PM
Sunday	□	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 □

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.

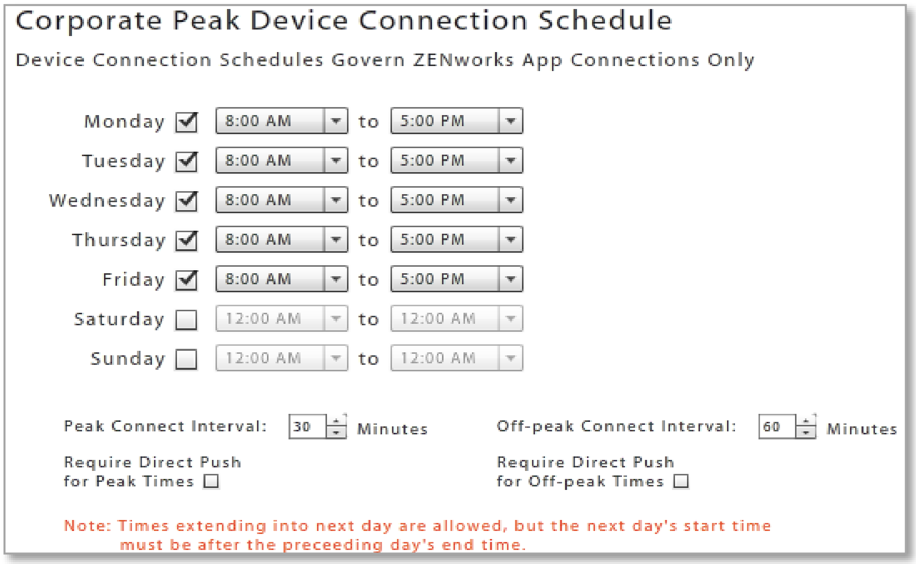
Require Direct Push - The *Require Direct Push* setting determines whether updates from the server, such as security commands, are synchronized immediately or during the next scheduled connection. If this setting is enabled, commands from the server sync to the device as soon as they are issued. Synchronizations 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	☑	8:00 AM	to	5:00 PM
Tuesday	☑	8:00 AM	to	5:00 PM
Wednesday	☑	8:00 AM	to	5:00 PM
Thursday	☑	8:00 AM	to	5:00 PM
Friday	☑	8:00 AM	to	5:00 PM
Saturday	□	12:00 AM	to	12:00 AM
Sunday	□	12:00 AM	to	12:00 AM

Peak Connect Interval: 30 Minutes

Off-peak Connect Interval: 60 Minutes

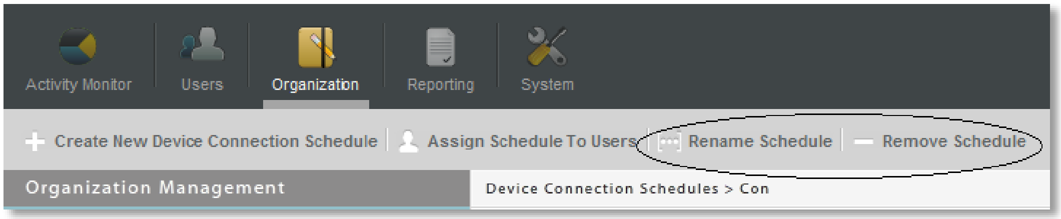
Require Direct Push for Peak Times □

Require Direct Push for Off-peak Times □

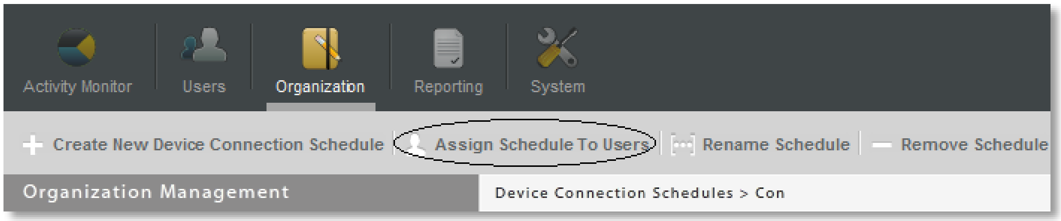
Note: Times extending into next day are allowed, but the next day's start time must be after the preceeding day's end time.

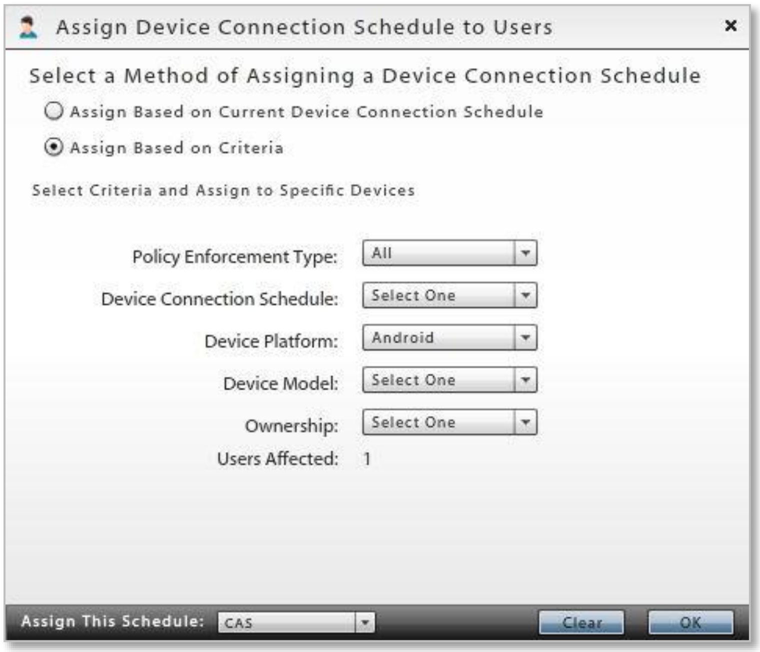
Tips on Using Device Connection Schedules

- Direct Push is not supported for Windows Phones.
- 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 *Device 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.





Assign Device Connection Schedule to Users

Select a Method of Assigning a Device Connection Schedule

○ Assign Based on Current Device Connection Schedule

● Assign Based on Criteria

Select Criteria and Assign to Specific Devices

Policy Enforcement Type: All

Device Connection Schedule: Select One

Device Platform: Android

Device Model: Select One

Ownership: Select One

Users Affected: 1

Assign This Schedule: CAS

Assigning a Device Connection Schedule

The Organization License

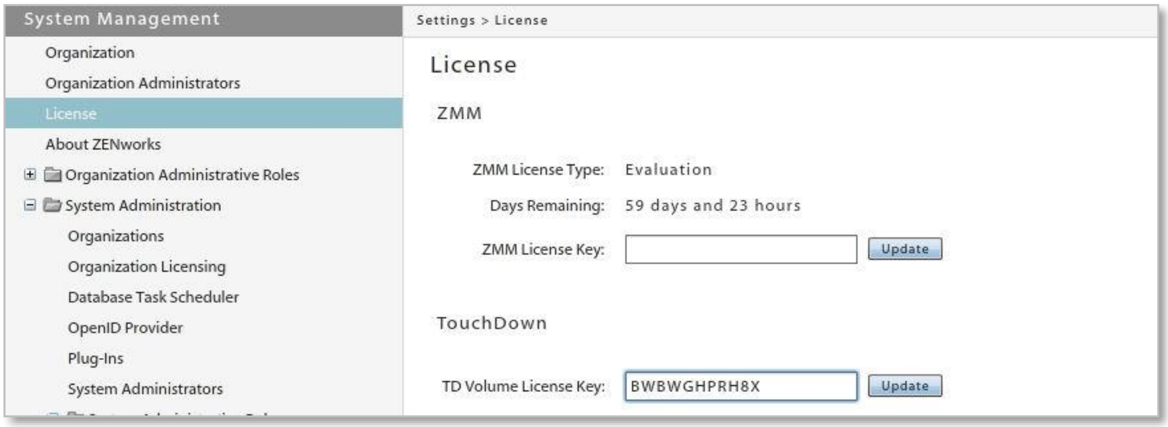
If you are extending a *ZENworks Mobile Management* software evaluation license or moving an organization to a license for a purchased copy of the software, you must enter a new license key for the server.

You can also enter the TouchDown volume license key here, then enable the TouchDown policy to push the license to Android devices using TouchDown. (*Organization* > *Policy Suites* > (policy suite) > *TouchDown* > *Installation* > *Push TD enterprise license to device*)

Updating licenses requires full system admin login credentials.

The Organization License

1. To access the *License* page, select ***System*** > ***License.***
2. The ***License Type*** and number of ***Days Remaining*** on the license display.
3. Enter the license key provided by your Novell Sales Representative in the ***ZMM License Key*** field and click ***Update***.
4. Enter the license key provided by your Novell Sales Representative in the ***TD Volume License Key*** field and click ***Update***.



License

ZMM

ZMM License Type: Evaluation

Days Remaining: 59 days and 23 hours

ZMM License Key:

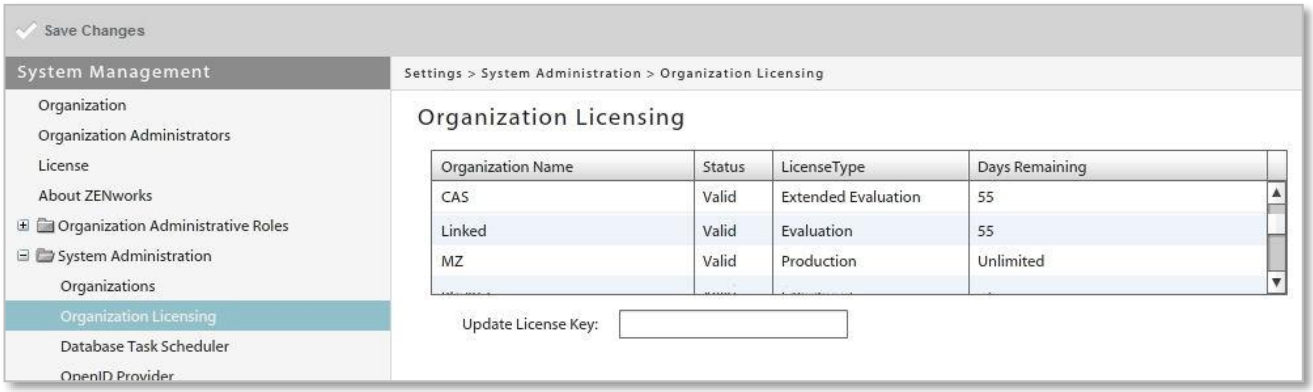
TouchDown

TD Volume License Key: BWBWGHPRH8X

Licenses for Multiple Organizations

If there are multiple organizations on the *ZENworks Mobile Management* server, System Administrators can view a list of organizations and the associated licenses. Any one of the licenses can be updated from this page, as long as the administrator has full system admin login credentials.

1. To access the *Organization Licensing* page, select ***System*** > ***System Administration*** > ***Organization Licensing***.
2. The grid displays each organization on the server, its *Status*, *License Type,* and number of *Days Remaining* on the license.
3. To update a license, select it on the grid and enter the new license key provided by your Novell Sales Representative in the ***Update License Key*** field. Click ***Save Changes***.



Organization Licensing

Organization Name	Status	LicenseType	Days Remaining
CAS	Valid	Extended Evaluation	55
Linked	Valid	Evaluation	55
MZ	Valid	Production	Unlimited

Update License Key:

Organization Administrator Roles and Logins

Organization Administrator Roles

See also System Administration Guide: System Administrator Roles

Predefined Organization Administrator Roles

There are three predefined Organization Administrator roles. The permissions for these roles cannot be altered. You can view the set permissions for these roles via the *Role Permissions* option in the *System* view: *Organization Administration Roles.*

The three predefined organization administrator roles are:

- **Full Organization Admin** - Gives full administrative permissions in only one organization on the *ZENworks Mobile Management* server. The *ZENworks Mobile Management System* view on the dashboard is limited to the *Organization*, *Organization Administrators*, *Organization Administrative Roles*, *View Logs*, and *About ZENworks* menu options.
- **Support Organization Admin** – Gives limited administrative access or read only access in only one organization on the *ZENworks Mobile Management* server. Organizational Support Administrators can email individual users, but not groups of users.
- **Restricted Organization Admin** – Restricted from viewing private data such as Location, MMS/SMS Log, Phone Log, and File Archive. Gives Read only permissions for all other views in only one organization on the *ZENworks Mobile Management* server.

Organization administrator credentials give access to one specific organization on the *ZENworks Mobile Management* server. Credentials can be authenticated via an LDAP server and can be assigned *Full Admin*, *Support Admin* (read-only), or *Restricted Admin* (limited read-only) permissions.

Who Should Have an Organization Administrator Login

Organization Administrator Logins are ideal for those responsible for configuring and maintaining a single organization on a system with groups of users that have been divided into separate organizations.

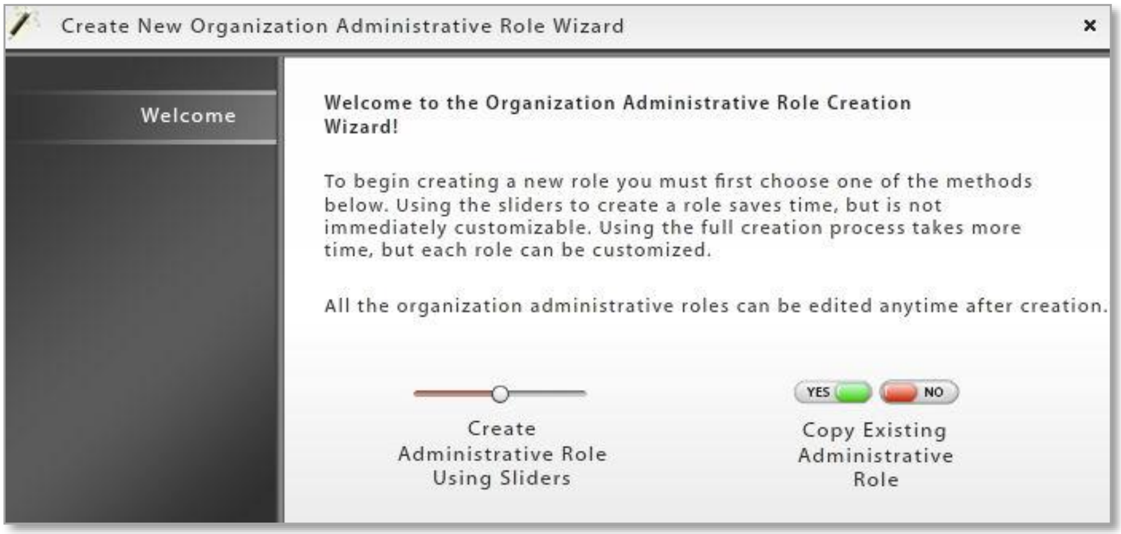
ORGANIZATION ADMINISTRATOR ROLES		
Dashboard View	**Support Organization Admin**	**Restricted Organization Admin**
Activity Monitor	Read-only access; cannot disable or snooze alerts	Read-only access; cannot disable or snooze alerts
Users	• Can add or remove users and perform all the functions in the right-hand *Details* panel, except *Show Recovery Password* • Can email an individual user, but cannot use *Group Emailing* • Can perform most functions in the left-hand panel of *Devcie Profile* • Can view the grids in the *Audit Data* and *Search Text Message Log* options (*Device Profile*), but cannot view the body or attachments of a text message • Can choose the Visible Columns for the *User/Device Grid* list	• Restricted from adding or removing users and from all functions in the right *Details* panel • Restricted from sending an email to an individual user or a group • Restricted from the *Location Data, Audit Data, Search Phone Log, Search Text Message Log*, and *File Archive* options in the left panel of *Device Profile* • Read-only access to options in the left panel of *Device Profile* • Can choose the Visible Columns for the *User/Device Grid* list
Organization	Read-only access	Read-only access
Reporting	Full access (view and export)	Full access (view and export)
System	• Read-only access • Restricted from the *System Administration* option in the left panel	• Read-only access • Restricted from the *System Administration* option in the left panel

Customized Organization Administrator Roles

Administrators can create customized organization administrator roles to tailor the permissions associated with *ZENworks Mobile Management* dashboard login credentials. When a custom role has been created, it appears as a choice in the drop-down list of the *Add Administrator Wizard*'s ***Role*** field. See Organization Administrator Logins.

Administrators who are logged in when changes are made to role permissions must log out and log in again for permission changes to take effect.

Select ***System*** > ***Organization Administrative Roles > Role Permissions*** > ***Add Role***



Create New Organization Administrative Role Wizard

Welcome to the Organization Administrative Role Creation Wizard!

To begin creating a new role you must first choose one of the methods below. Using the sliders to create a role saves time, but is not immediately customizable. Using the full creation process takes more time, but each role can be customized.

All the organization administrative roles can be edited anytime after creation.

Create Administrative Role Using Sliders
YES
NO
Copy Existing Administrative Role

1. Choose a method for creating an Organization Administrative Role:
    - Use the sliders to determine the role's initial settings. The new role copies the settings of the predefined Organization *Full Admin*, *Support Admin,* or *Restricted Admin*.
    - Copy the settings of an existing role
2. Specify the role permissions to copy.
3. Enter a **Role Name** and **Description**.
4. Click **Finish** to save the new role.
5. Find and select the role in the *Organization Administrative Roles* grid.
6. Set the general permissions for the role:
    - **Prevent role from managing administrator accounts, roles and user privacy protections**
        - ○ Locks the role out of modifying administrator accounts, administrator roles, and user privacy protection.
        - ○ Most roles should be locked, except those for administrators requiring full privileges.
        - ○ If set to YES, this permission overrules the *System Section Permissions,* regardless of how they are set.
        - ○ Defaults to YES when creating a role with the sliders. If you are copying an existing role, the setting of the copied role is the default.
    - **Prevent role from viewing protected data as defined in User Privacy Protection**
        - ○ Blocks administrators assigned this role from viewing the protected data of only the users or policy suites designated in User Privacy Protection. (Automatically places the role in the *Restricted* column of the ***Restrict Organization Administrative Roles*** list. See User Privacy Protection.)
        - ○ Defaults to YES when creating a role with the sliders. If you are copying an existing role, the setting of the copied role is the default.
7. Set the permissions associated with dashboard access. See System Administration Guide: Appendix A: Role Permissions for a comprehensive list.

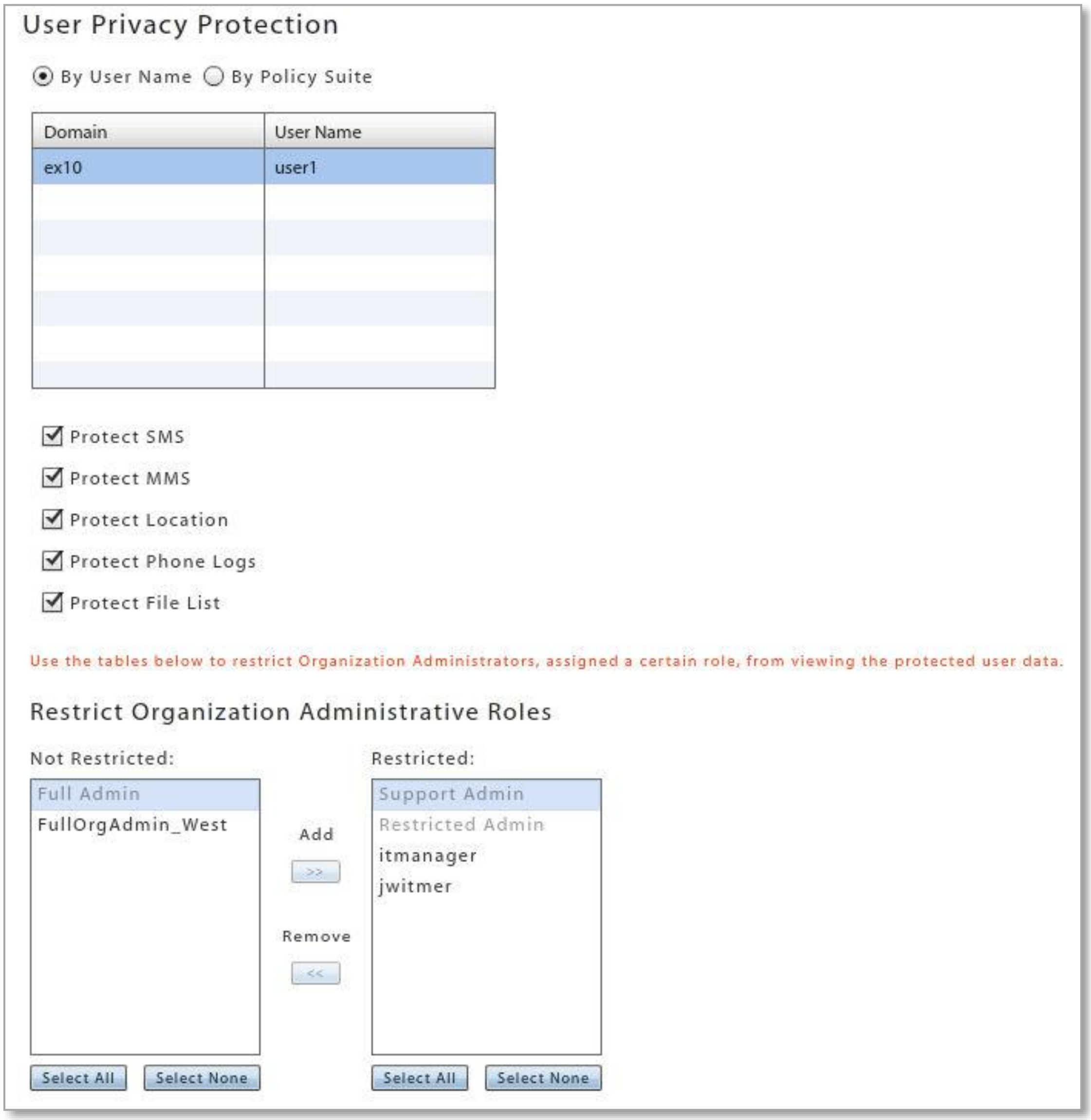
Organization Administrative Roles: User Privacy Protection

Private data includes a user’s SMS/MMS content, location data, phone logs, and file list.

User Privacy Protection provides a way to protect the private data of individual users or users assigned to a particular policy suite without restricting organization administrative roles from viewing the private data of all users.

Example: You assign a role to an administrator with permissions for viewing private data. However, organization administrators in this role must be restricted from viewing the private data of your executive staff. You can add the executive staff users to the *User Privacy Protection* list and designate the administrative role as one that is restricted from viewing the private data of users on this list.

Administrators who are logged in when changes are made to the User Privacy Protection list or the Restrict Organization Administrative Roles list must log out and log in again for permission changes to take effect.



User Privacy Protection

● By User Name ○ By Policy Suite

Domain	User Name
ex10	user1

☑ Protect SMS

☑ Protect MMS

☑ Protect Location

☑ Protect Phone Logs

☑ Protect File List

Use the tables below to restrict Organization Administrators, assigned a certain role, from viewing the protected user data.

Restrict Organization Administrative Roles

Not Restricted:

Full Admin
FullOrgAdmin_West

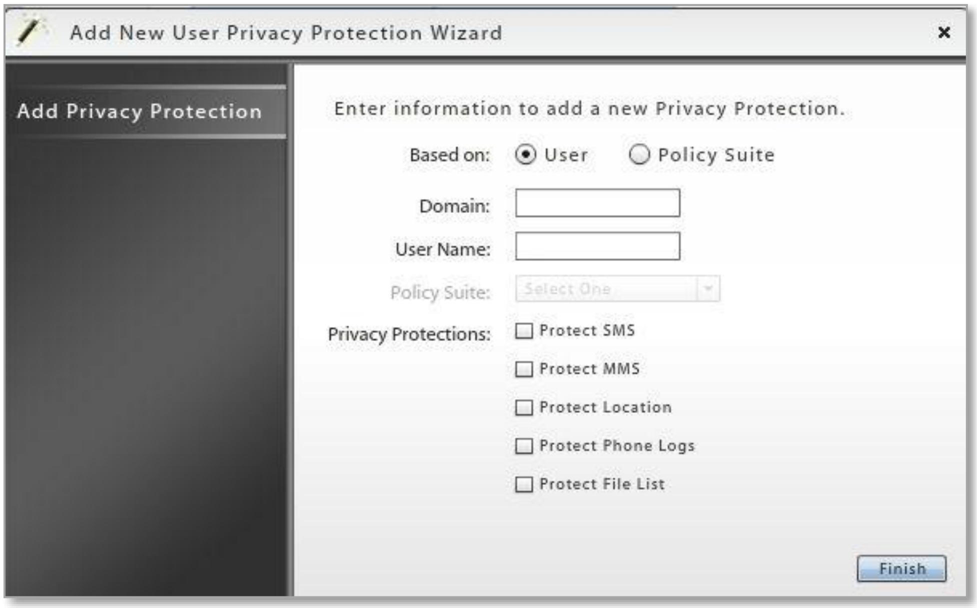
Restricted:

Support Admin
Restricted Admin
itmanager
jwitmer

Select ***System*** > ***Organization Administrative Roles > User Privacy Protection*** > ***Add User Privacy Protection.***

Adding Users to the Privacy Protection List

User Privacy Protection provides a way to protect the private data of individual users or users assigned to a particular policy suite. Administrative roles can be blocked from viewing the private data of users on this list, even if their role permissions allow them to view private data associated with the general user base.



Add New User Privacy Protection Wizard

Enter information to add a new Privacy Protection.

Based on: ● User ○ Policy Suite

Domain:

User Name:

Policy Suite: Select One

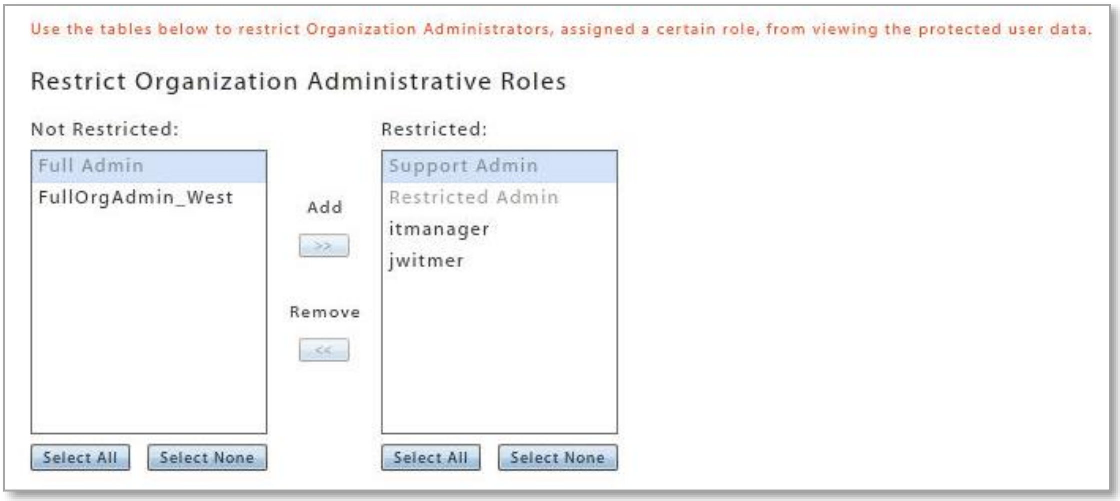
Privacy Protections: □ Protect SMS
□ Protect MMS
□ Protect Location
□ Protect Phone Logs
□ Protect File List

1. Select the **User** or **Policy Suite** option. An individual user or the group of users assigned to a Policy Suite.
2. If you are adding an individual user to the privacy protection list, enter the user's **Domain** and **User Name**.
3. If you are adding users assigned to a policy suite, select a policy suite from the drop-down list.
4. Select the box beside the **Privacy Protections** you wish to enable:
   - Protect SMS
   - Protect MMS
   - Protect Location
   - Protect Phone Logs
   - Protect File List
5. Click **Finish** to save.

Adding Administrator Roles to the Restricted/Not Restricted List

Designate each customized administrative role as one that is **Restricted** or **Not Restricted** from viewing the private data belonging to users on the *User Privacy Protection* list.

All predefined and customized roles are listed in either the *Not Restricted* or *Restricted* list. The predefined roles cannot be moved from one column to another. The predefined *Full Admin* role is always *Not Restricted*. The predefined *Support Admin* and *Restricted Admin* roles are always *Restricted*.



Use the tables below to restrict Organization Administrators, assigned a certain role, from viewing the protected user data.

1. Select an administrative role on either side of the list. (Hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item).
2. Click **Add** to move a role from *Not Restricted* to *Restricted*.
   Click **Remove** to move a role from *Restricted* to *Not Restricted*.
3. Click **Save Changes** on the option bar at the top of the page.

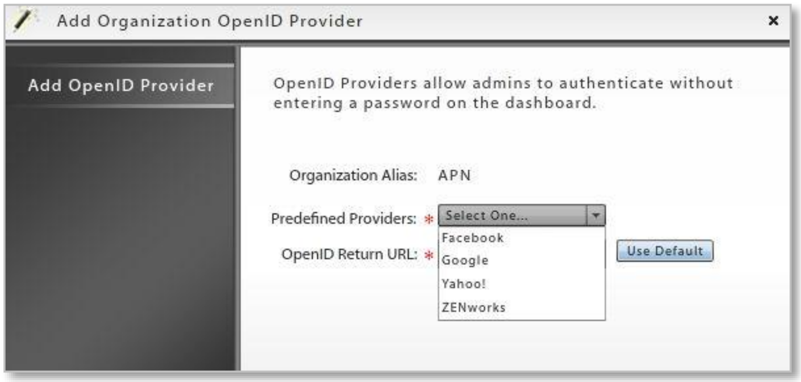
Configuring OpenID Providers for Organization Administrators

OpenID is an open standard that allows administrators to log in and authenticate using an outside source. Configuring the system includes defining the OpenID provider settings and enabling or disabling the OpenID option for each administrator. See also System Administration Guide: OpenID Configuration for System Administrators.

Add an OpenID Provider for Organization Administrators

There can be multiple OpenID providers for Organization Administrators, however, only one of each type can be configured.

1. Select **Organization** > **Administrative Servers** > **OpenID Providers**.
2. Select one of the **Predefined Providers** from the drop-down list. Choose *Facebook, Google, Yahoo!,* or *ZENworks*.



Add Organization OpenID Provider

Add OpenID Provider

OpenID Providers allow admins to authenticate without entering a password on the dashboard.

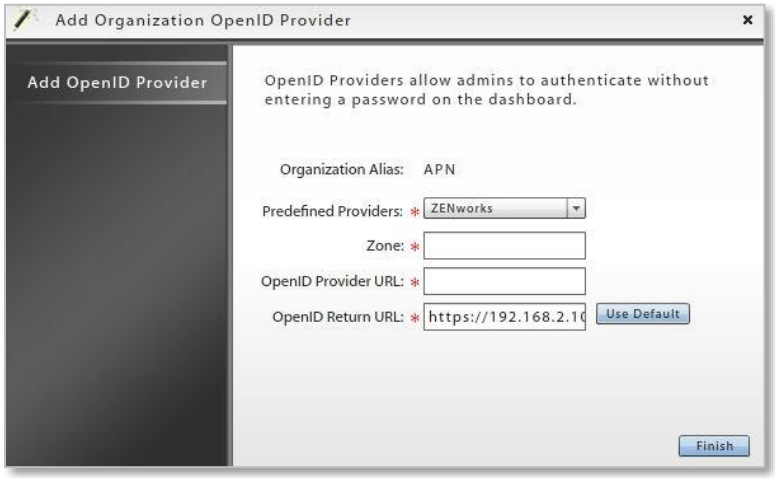
Organization Alias: APN

Predefined Providers: * Select One...

OpenID Return URL: *

3. 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 format: https://<server>:<port>/zenworks/?requestHandler=ZENOpenIDHandler



Add Organization OpenID Provider

Add OpenID Provider

OpenID Providers allow admins to authenticate without entering a password on the dashboard.

Organization Alias: APN

Predefined Providers: * ZENworks

Zone: *

OpenID Provider URL: *

OpenID Return URL: * https://192.168.2.1(

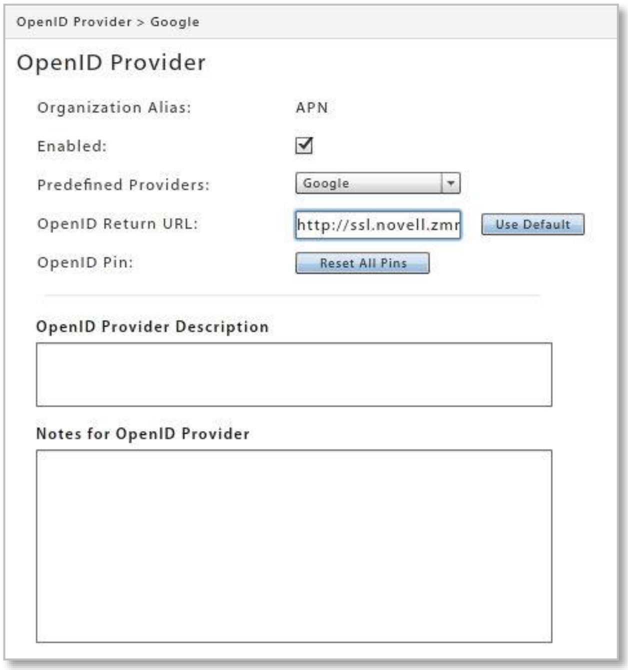
4. At the **OpenID Return URL** field, enter the URL of the server to which the user is returned after successful provider validation. The default is the current *ZENworks Mobile Management* server URL.
5. Enable the OpenID option for each administrator you will allow to log in with OpenID credentials. See also Add an OpenID Authenticated Organization Administrator Login.

Update OpenID Provider Settings

You can enable, disable, or remove an existing OpenID provider. You can also change its settings or reset the OpenID Pin for all users logging in through this OpenID provider.

4. Select **Organization** > **Administrative Servers** > **OpenID Providers** and select a provider from the left panel.
5. You can update any of the following fields:
   - **Enabled** – mark the checkbox to enable the provider; to disable a provider, verify that no administrators are using the provider, then remove the mark from this checkbox.
   - **Predefined Providers** – a drop-down list of the provider types: *Facebook, Google, Yahoo!,* or *ZENworks*
   - **Zone –** (ZENworks provider) the 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* 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** – (ZENworks provider) the URL of the ZENworks Primary Server in the following form: **Error! Hyperlink reference not valid.**
   - **OpenID Return URL -** 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.
   - **Description and Notes**



OpenID Provider > Google

OpenID Provider

Organization Alias: APN

Enabled: ☑

Predefined Providers: Google

OpenID Return URL: http://ssl.novell.zmr

OpenID Pin:

OpenID Provider Description

Notes for OpenID Provider

6. The **OpenID Pin** reset button will reset all administrator pins and issue emails to administrators with the new 4 character pin.

   The first time administrators log in to *ZENworks Mobile Management* with an OpenID they are prompted for a PIN code before entering the *ZENworks Mobile Management* dashboard. If any of the provider settings are updated or you reset pins with this button, new PIN codes are generated and emailed to administrators from the *ZENworks Mobile Management* server.

Organization Administrator Logins

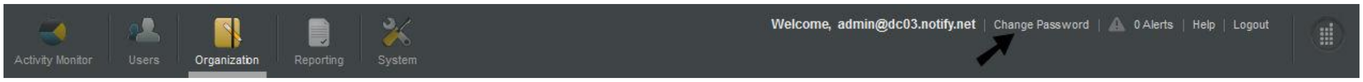
See also, System Administration Guide: System Administrator Logins

Creating Organization Administrator Logins

An organization administrator login gives access to only one organization. It can authenticate against the *ZENworks Mobile Management* server, an LDAP server, or an OpenID provider.

Multiple administrator logins with assigned roles can be created through the dashboard. For information on roles see Organization Administrator Roles.

Login Passwords: Administrators can change their login passwords from an option located in the dashboard header.



Best Practices: Maintain at least one local organization administrator that authenticates directly against the *ZENworks Mobile Management* server and that does not use LDAP or OpenID authentication. This will provide access to the dashboard that is not subject to the availability of external authorities.

ISE Administrator: When *ZENworks Mobile Management* is integrated with Cisco Identity Services Engine (ISE), you must designate an Organization Administrator as the ISE Admin. Once the Organization Administrator account has been created, select the administrator from the grid on the Organization Administrators page and check the box next to the **ISE Admin** field.

To create an Organization Administrator Login, select **System** > **Organization Administrators** > **Add Administrator**.

Choose how the administrator should be authenticated: **Manual (locally)**, **LDAP**, **OpenID**. The Add Organization Administrator Wizard steps you through creating login credentials for organization administrators.

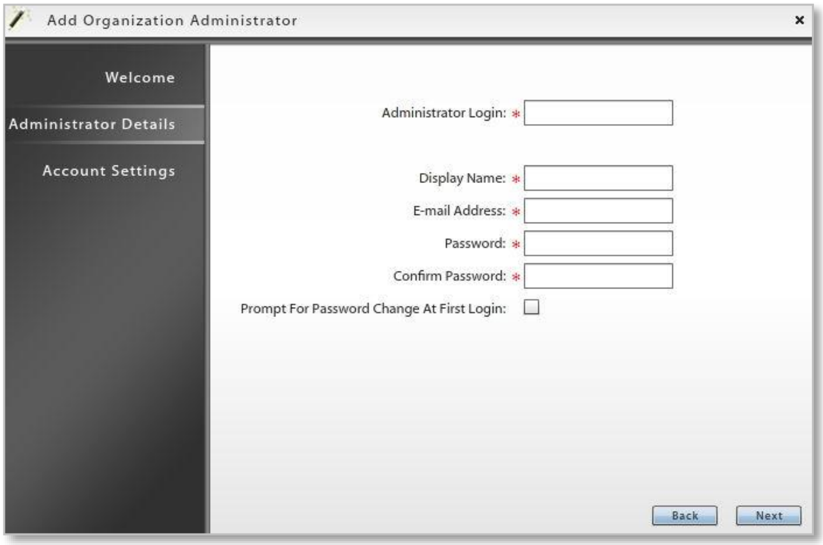
- Add a Manually (locally) Authenticated Administrator Logins
- Add an LDAP Authenticated Administrator Logins
- Add an OpenID Authenticated Administrator Logins

Enter the administrator details, then choose the account settings.

Add a Manually (locally) Authenticated Organization Administrator Login

Add an organization administrator login that authenticates directly against the *ZENworks Mobile Management* server with a unique password.

1. Use the administrator's email address for the **Administrator Login**.
2. Enter a **Display Name**.
3. Enter the administrator's **Email Address**.
4. Create and confirm a **Password** for the administrator login.
5. Mark the checkbox to prompt the administrator for a **Password Change** at his/her first login.
6. Click **Next**.



Add Organization Administrator

Administrator Login: *

Display Name: *

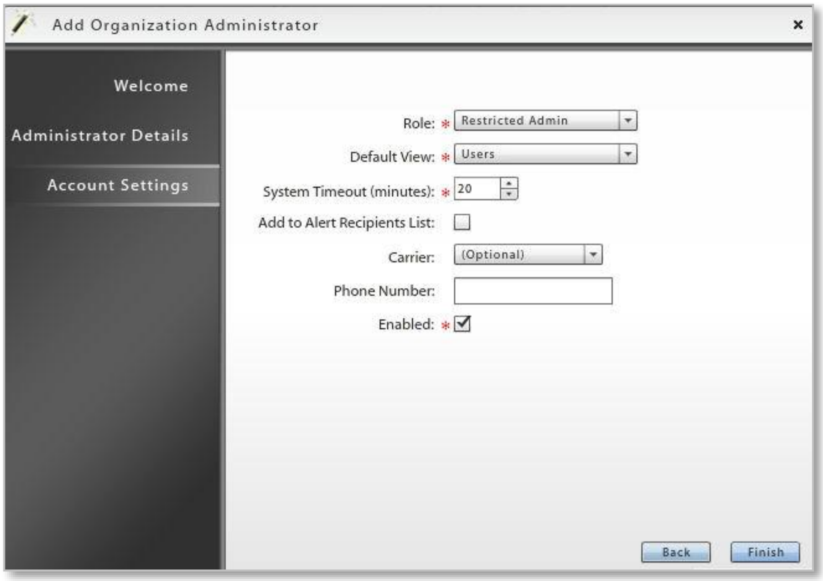
E-mail Address: *

Password: *

Confirm Password: *

Prompt For Password Change At First Login: □

7. Enter the **Account Settings**.



Add Organization Administrator

Role: * Restricted Admin

Default View: * Users

System Timeout (minutes): * 20

Add to Alert Recipients List: □

Carrier: (Optional)

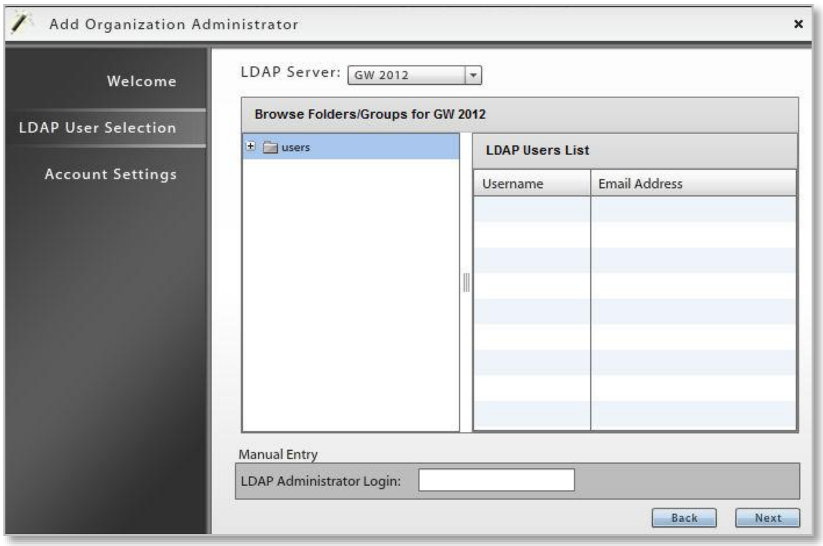
Phone Number:

Enabled: * ☑

Add an LDAP Authenticated Organization Administrator Login

Add an organization administrator login that authenticates using the administrator’s LDAP credentials.

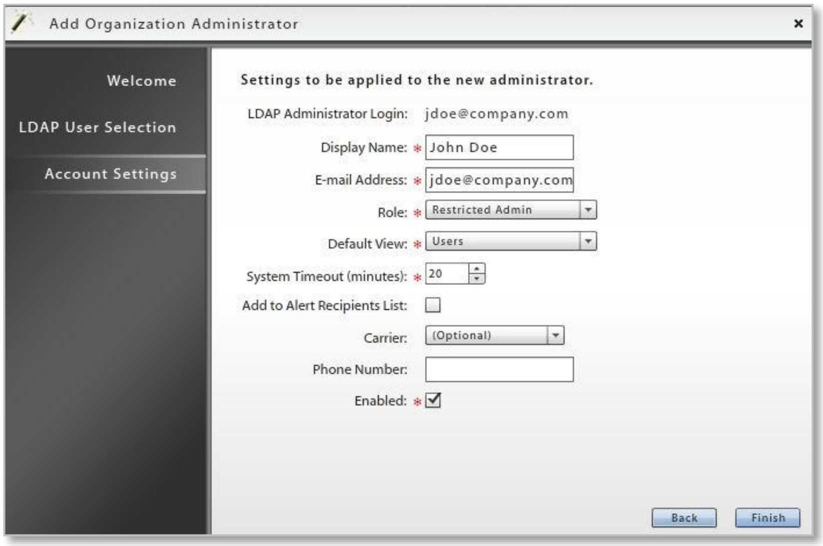
1. Select an LDAP server and browse the LDAP folders/groups to select the administrator, or manually enter the administrator’s LDAP server user name in the **LDAP Administrator Login** field.
2. Click **Next**.



LDAP Server: GW 2012

LDAP Administrator Login:

3. Enter a **Display Name** and the **Email Address** for the administrator.
4. Enter the remainder of the **Account Settings**.



Settings to be applied to the new administrator.

LDAP Administrator Login: jdoe@company.com

Display Name: * John Doe

E-mail Address: * jdoe@company.com

Role: * Restricted Admin

Default View: * Users

System Timeout (minutes): * 20

Add to Alert Recipients List: □

Carrier: (Optional)

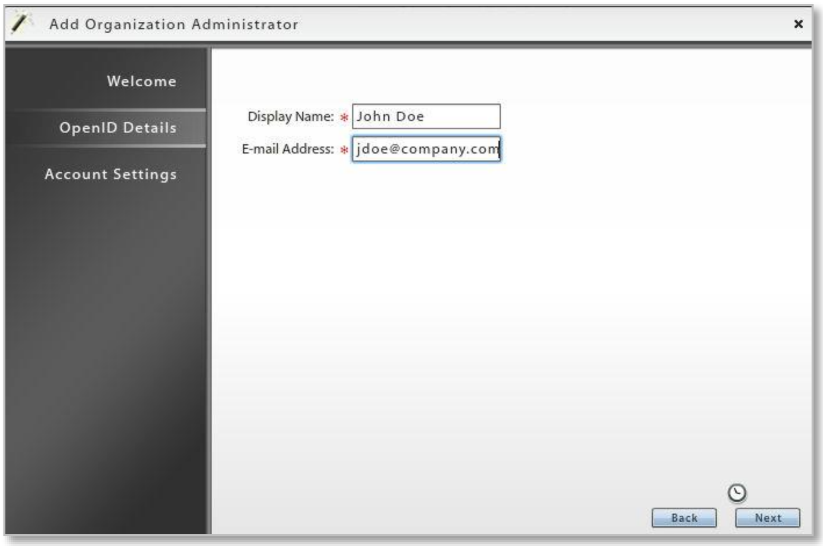
Phone Number:

Enabled: * ☑

Add an OpenID Authenticated Organization Administrator Login

Add an organization administrator login that authenticates using the administrator's OpenID credentials.

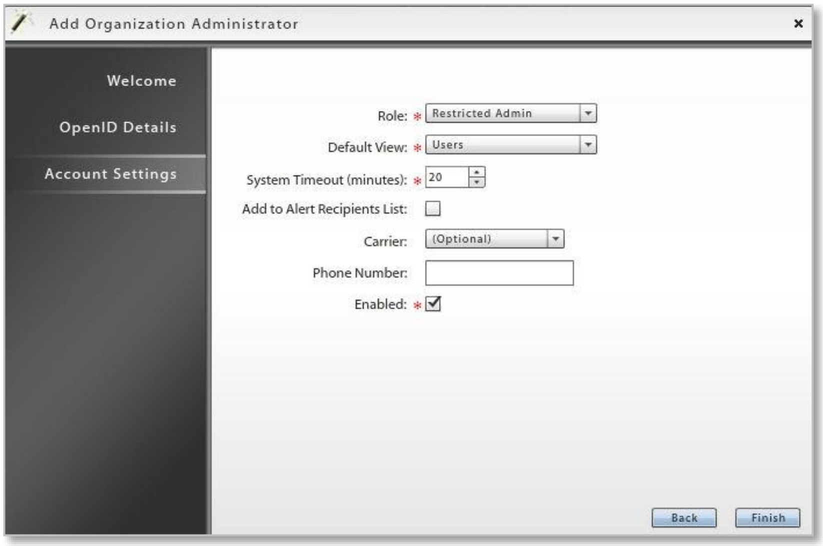
1. Enter the **Display Name** for this login.
2. Enter the administrator's **Email Address**.
3. Click **Next**.



Display Name: * John Doe

E-mail Address: * jdoe@company.com

4. Enter the **Account Settings**.



Role: * Restricted Admin

Default View: * Users

System Timeout (minutes): * 20

Add to Alert Recipients List: □

Carrier: (Optional)

Phone Number:

Enabled: * ☑

Organization Administrator Account Settings

- **Role** – Assign the permissions level to the login. Choose from:
  - Predefined **Full Admin** – Full administrative permissions for a single organization; Restricted from System Administration
  - Predefined **Support Admin** – Read-only permissions with limited editing capabilities for a single organization
  - Predefined **Restricted Admin** – Read-only permissions with private data restrictions for a single organization; cannot view Location Data, Audit Data, MMS/SMS or Phone Logs, and File Archive
  - **Any custom Organization Administrator role created for the system**
- **Default View** – Select the default view at login
- **System Timeout** – Select an inactivity timeout in minutes for this login
- **Add to Alert Recipient List** – Check this box to make this administrator a recipient of Compliance Management email or SMS alerts.
- **Carrier** – Carrier of the administrator's mobile device (optional - needed for receiving SMS notifications for system alerts).
- **Phone Number** – Phone number of the administrator's mobile device (optional - needed for receiving SMS notifications for system alerts).
- **Active Status** – Select the box to **enable** this administrative login

Managing Organization Administrator Logins

You must be logged into the *ZENworks Mobile Management* server with *Full Admin* organization administrator credentials or *Full Admin* system administrator credentials in order to edit or remove an Organization Administrator.

Best Practices: Maintain at least one *Organization Administrator* that does not use OpenID**.** This ensures that you have a way to access the dashboard in the event that an OpenID provider is unavailable.

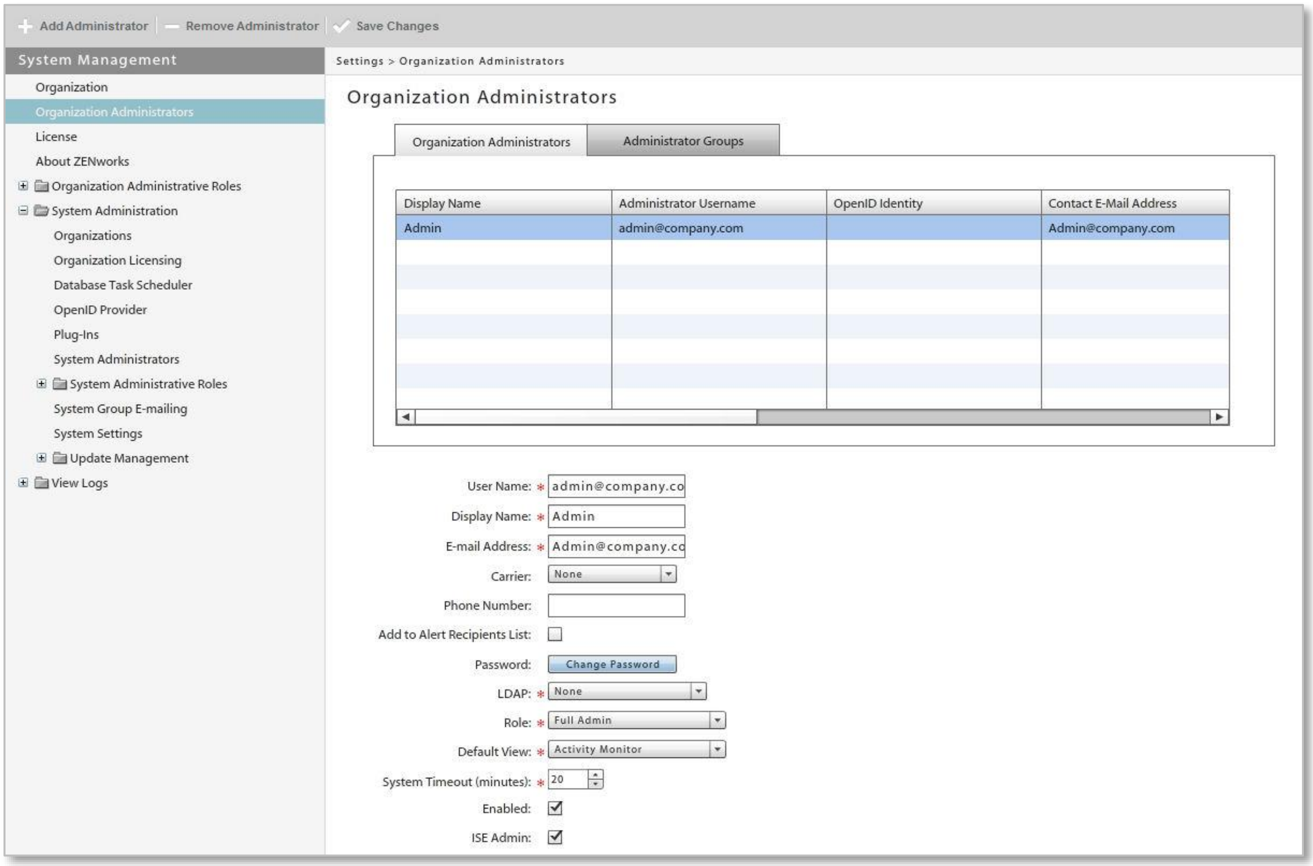
Managing Individual Administrator Logins

1. Select ***System*** > ***Organization Administrators***. Click the ***Organization Administrators*** tab.
2. Select an administrator from the list. Edit the settings and click ***Save Changes***.

   You can also remove the administrator by clicking ***Remove Administrator***.

Designating an Organization Administrator as the ISE Admin

When *ZENworks Mobile Management* is integrated with Cisco Identity Services Engine (ISE), you must designate an Organization Administrator as the ISE Admin. Select the administrator from the grid, then check the box next to the **ISE Admin** field.



Display Name	Administrator Username	OpenID Identity	Contact E-Mail Address
Admin	admin@company.com		Admin@company.com

User Name: * admin@company.co

Display Name: * Admin

E-mail Address: * Admin@company.co

Carrier: None

Phone Number:

Add to Alert Recipients List: □

Password: Change Password

LDAP: * None

Role: * Full Admin

Default View: * Activity Monitor

System Timeout (minutes): * 20

Enabled: ☑

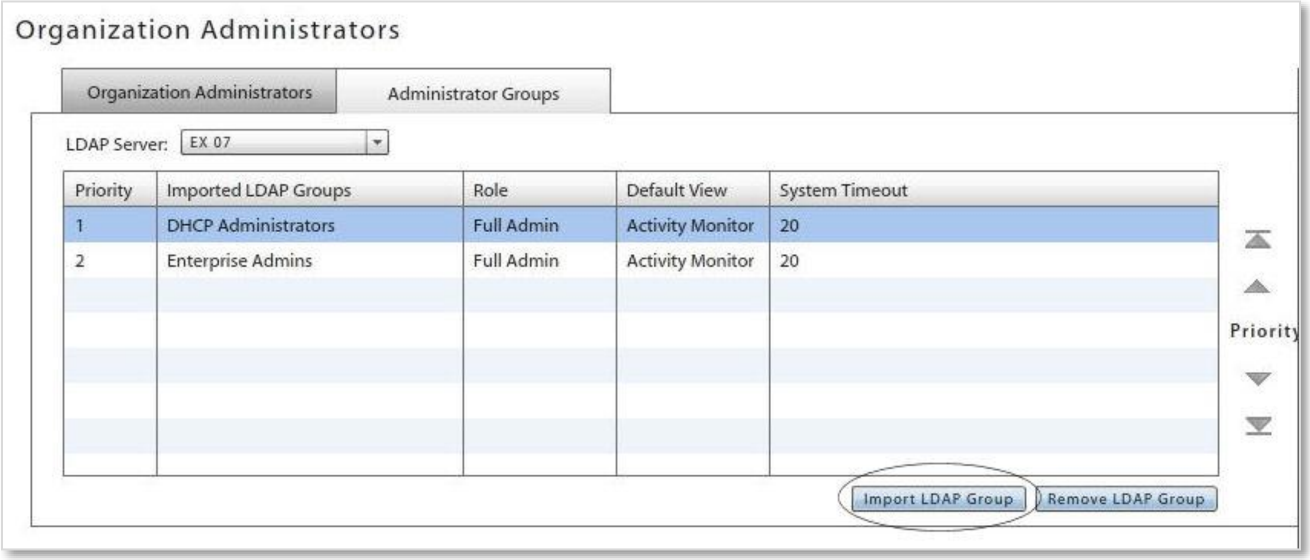
ISE Admin: ☑

Importing Organization Administrator LDAP Groups

Importing administrator LDAP groups into the *ZENworks Mobile Management* server eliminates the need to create administrator logins. Any member of the imported LDAP group can log in to the *ZENworks Mobile Management* dashboard as long as their LDAP credentials are successfully authenticated. At the first successful login, an account on the *ZENworks* server is created for the administrator using the provisioning settings associated with the group.

1. Select ***System*** > ***Organization Administrators***. Click the ***Administrator Groups*** tab.
2. To import an LDAP administrator group, select an LDAP server from the dropdown list. Click the ***Import LDAP Group*** button to select an administrator group to import.

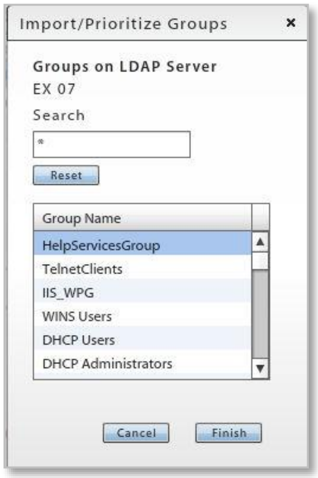
   Administrators should familiarize themselves with the LDAP server structure and verify that groups they choose for use with the *ZENworks Mobile Management* server contain the following necessary attributes: User Identification Attribute, Group Membership Attribute, Group Object Class, and User Object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



LDAP Server: EX 07

Priority	Imported LDAP Groups	Role	Default View	System Timeout
1	DHCP Administrators	Full Admin	Activity Monitor	20
2	Enterprise Admins	Full Admin	Activity Monitor	20

3. Select a group to import and click ***Finish***.

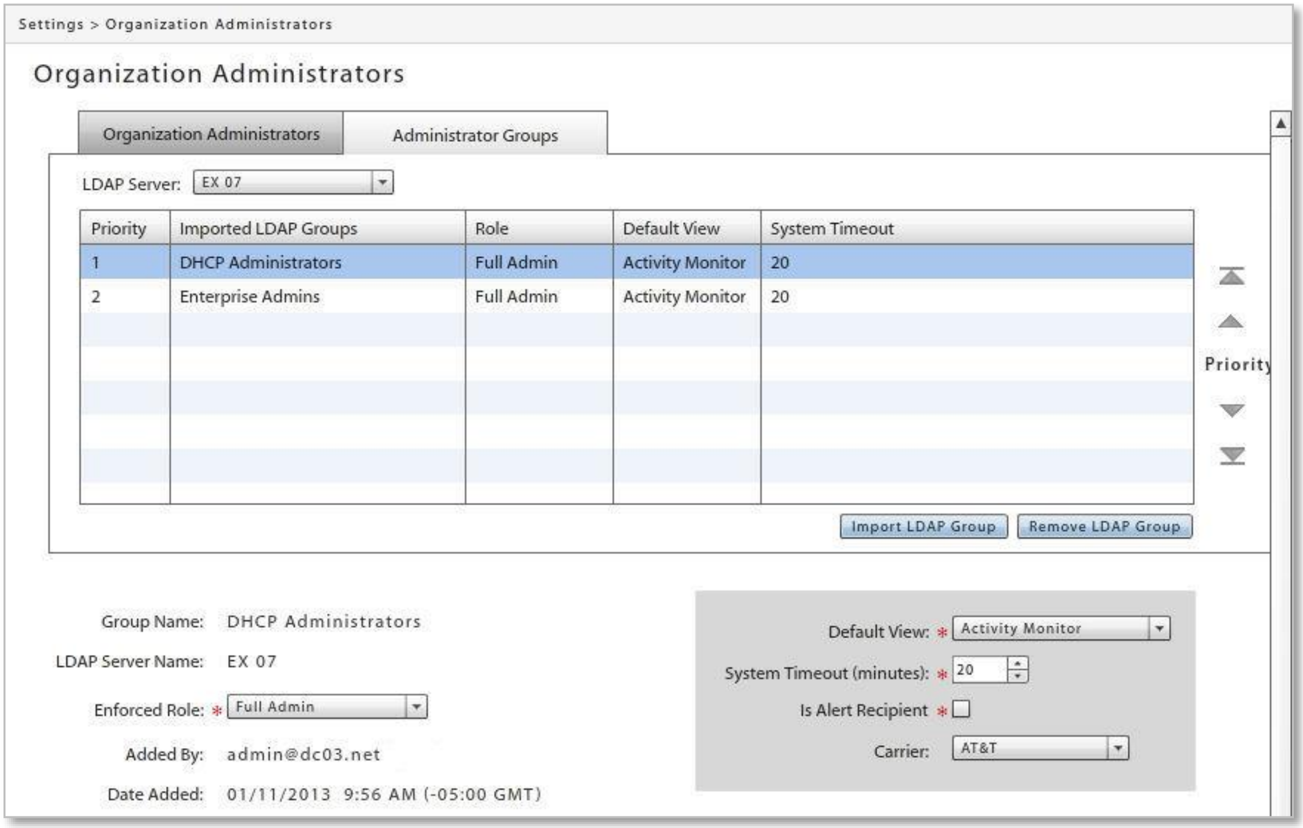


Groups on LDAP Server
EX 07

Search
*

Group Name
HelpServicesGroup
TelnetClients
IIS_WPG
WINS Users
DHCP Users
DHCP Administrators

4. To choose provisioning settings for members of this group, select an *Administrator Group* from the grid and configure these settings for the group.
    - Enforced Role
    - Default View
    - System Timeout
    - Is Alert Recipient (administrators receive *ZENworks Mobile Management* SMS/email alerts)
    - Carrier (required if administrators are an alert recipients)



Settings > Organization Administrators

Organization Administrators

LDAP Server: EX 07

Priority	Imported LDAP Groups	Role	Default View	System Timeout
1	DHCP Administrators	Full Admin	Activity Monitor	20
2	Enterprise Admins	Full Admin	Activity Monitor	20

Group Name: DHCP Administrators

LDAP Server Name: EX 07

Enforced Role: * Full Admin

Added By: admin@dc03.net

Date Added: 01/11/2013 9:56 AM (-05:00 GMT)

Default View: * Activity Monitor

System Timeout (minutes): * 20

Is Alert Recipient * □

Carrier: AT&T

5. If there are administrators that belong to multiple groups, use the arrows to the right of the group grid to prioritize the groups.

    The group with the highest priority will determine an administrator’s provisioning assignments when he or she is added at the first successful login.