

System Administration

ZENworks® Mobile Management 2.9.x

May 2014

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Table of Contents

Accessing the Dashboard	4
Organization Administration	6
Updating Organization Information	6
Signing Certificate Upload	8
Google Cloud Messaging (GCM) Toggle	9
APNs Certificate Upload	12
VPP Token Upload	14
iOS Configurator Groups	16
Organization Administrator Roles	17
Predefined Organization Administrator Roles	17
Customized Organization Administrator Roles	18
Organization Administrative Roles: User Privacy Protection	20
Configuring OpenID Providers for Organization Administrators	23
Organization Administrator Logins	25
Creating Organization Administrator Logins	25
Managing Organization Administrator Logins	30
Importing Organization Administrator LDAP Groups	31
Server Logging	33
Synchronization Logs	34
Database Task Scheduler Log	36
Data Usage Log	37
Device Logs	39
Error Chain Log (iOS device specific)	40
Licensing Log	41
Mail Message Log	42
System Administration	43
Managing Multiple Organizations	44
Managing the License	46
Database Task Scheduler	47
Plug-Ins	48
System Administrator Roles	50
Predefined System Administrator Roles	50
Customized System Administrator Roles	52
Configuring an OpenID Provider for System Administrators	53
System Administrator Logins	54
Creating System Administrator Logins	54
Managing System Administrator Logins	59
Importing System Administrator LDAP Groups	60
System Group Emailing	62
System Settings	63
Custom Dashboard and Login Logos	63
Signing Certificate Upload	64
Update Management	65
Administrator Audit Trail	66
Appendix A: Role Permissions	68

Accessing the Dashboard

Requirements

ZENworks Mobile Management dashboard requirements:

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

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

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

Standard Login

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

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

A system administrator can create additional logins to the dashboard with system administrator, organization administrator, or support administrator privileges. See the [System Administrator Logins](#) and [Organization Administrator Logins](#) sections in this guide for details.



OpenID Login

Use your OpenID credentials to log in.

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

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

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



Admin Setup Pin Code

Enter Admin Setup Pin Code

Zone Name

OpenID Identity

OK



Organization Administration

This section of the guide documents topics related to managing a single organization. See [Managing Multiple Organizations](#) for information regarding management of a *ZENworks Mobile Management* server with multiple organizations.

Updating Organization Information

You can update the organization information if administrative contacts or organization defaults change.

Select **System > Organization** and update the following information:

- Organization name and contact information
- Welcome letter enablement – Emails a welcome letter to users when they are added
- EULA enablement - 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](#))
- APNs Certificate *Upload* button (see [description](#))
- APNs Expiration Date
- iOS Configurator Groups button (see [description](#))
- VPP Token *Upload, Remove, Sync Now, and Invite Users* buttons ([description](#))
- VPP Token Organization Name
- VPP Token Expiration Date (*annual*)
- VPP Account E-mail

Organization Settings

Organization Name: * ABC Co

Organization Alias: * ABC Co

Contact Person: * John DOe

Contact Person's E-mail Address: * admin@ex07.notify

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: 99

Note: Limits the number of devices a user can enroll. Select a maximum ranging from 1 to 99.

SMTP Server: EX07

Signing Certificate: [Upload](#)

Use GCM:

Note: GCM must be enabled at the system level before it can be turned on for this organization.

APNs Certificate: [Edit](#) [Test Now](#)

com.apple.mgmt.External.ab4ad141-596f-4353-bfd9-99ea37298f78 (Enabled)

APNs Expiration Date: Oct 11 2014 7:50AM

iOS Configurator Groups: [Export Profile for Configurator](#)

VPP Token: [Edit](#) [Remove](#) [Sync Now](#) [Invite Users](#)

VPP Token Organization Name: Globo Mobile Technologies Inc

VPP Token Expiration Date: Apr 25 2015 1:05PM

Organization and Hands-Off enrollment defaults:

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

Organization Defaults

Policy Enforcement Type: Standard Schedule-Based

Policy Schedule: * General Staff

Policy Suite During Schedule: * Policy A

Policy Suite Outside Schedule: * Policy B

Device Connection Schedule: * Default

LDAP Server: None

Liability: Corporate Individual

Novell Filr: Filr Profile

Hands-Off Enrollment Defaults

Local Groups: [Import 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.

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.



The screenshot shows a dialog box titled "Add Signing Certificate" with a close button (X) in the top right corner. The dialog contains the following elements:

- A label "Certificate File:" followed by a "Browse..." button.
- A label "Password:" followed by an empty text input field.
- An "Upload" button at the bottom center.

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 [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.

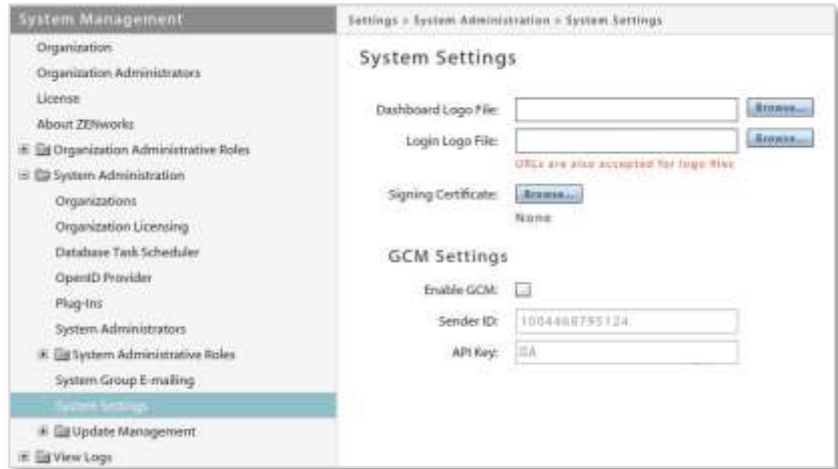
Enter your GCM credentials and enable the GCM service for the system

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.



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.

The screenshot displays the 'Organization Settings' page within a 'System Management' interface. The left sidebar contains navigation options: Organization, Organization Administrators, License, About ZENworks, Organization Administrative Roles, System Administration, and View Logs. The main content area is titled 'Organization Settings' and includes the following fields and controls:

- Organization Name: * ABC Co.
- Organization Alias: * ABC Co.
- Contact Person: * Jeremy Smith
- Contact Person's E-mail Address: * jsmith@company.co
- Contact Person's Secondary E-mail: [Empty field]
- Contact Person's Phone Number: * 3301234567 Ext: [Empty field]
- Contact Person's Secondary Phone: [Empty field] Ext: [Empty field]
- 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: 3 [Spinners]
Note: Limits the number of devices a user can enroll. Select a maximum ranging from 1 to 99.
- SMTP Server: 192.168.2.3
- Signing Certificate: [Upload button]
- Use GCM:
- APNs Certificate: [Edit button] [Test Now button]
com.apple.mgmt.External.af853723-55b9-4018-8360-a62d0df167f7 (Enabled)
- APNs Expiration Date: Oct 11 2014 10:49AM

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.

APNs Certificate Upload

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

The APNs Certificate **Upload** button allows you to apply the APNs certificate that you generated on the Apple Development portal. You need:

- The APNs certificate file (the .pfx format)
- The password you set when exporting the certificate

The APNs certificate settings can be edited if necessary. However, a change to the APNs certificate settings requires iOS device users to reload the APN profile on the device.

To Upload the APNs Certificate:

1. Select **System > Organization**.
2. Click the *Upload* button next to the **APNs Certificate** field.



Apple Push Notifications

Choose an APNs Certificate File:

Certificate Password:

Apple ID:

Use Default URLs:

Server URL:
e.g., https://<ServerAddress>/sync/iOSMDMSync.php.

Check in URL:
e.g., https://<ServerAddress>/sync/iOSMDMSync.php.

3. Click the **Browse** button, then navigate to and select the .pfx file containing the APNs certificate.
4. In the **Certificate Password** field, enter the password you set when exporting the certificate.
5. Enter the **Apple ID** used to generate the certificate, if you want to display it for reference on the *Organization Settings* page. This information can be useful at renewal time.
6. Check the **Use Default URLs** box to populate the *Server URL* and *Check in URL* fields with `http://<ServerAddress>/sync/iOSMDMSync.php`. This is the required format of the URLs. Verify that the `<ServerAddress>` is the external address of the *ZENworks Mobile Management* server.

If you have not accessed the Web site externally, do not use the default check box. Enter the URLs manually, in the format noted above.

7. Click the **Submit** button.

After you have uploaded an APNs certificate, it appears under the APNs Certificate field on the dashboard.



Note: The APNs certificate must be renewed annually. The expiration date is displayed on the *Organization Settings* page. You can also use the *Test Now* button to check the certificate's validity. The test will return the certificate's activation and expiration dates.

8. Click **Save Changes** when you are finished.

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.

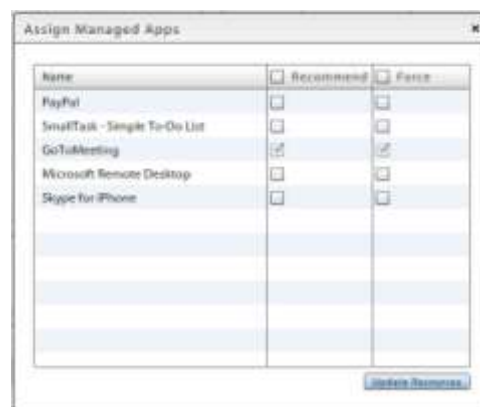
Enroll at: <https://deploy.apple.com> Other helpful sites: <http://www.apple.com/business/vpp/>
<http://www.apple.com/education/it/vpp/>

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 Management > 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.



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




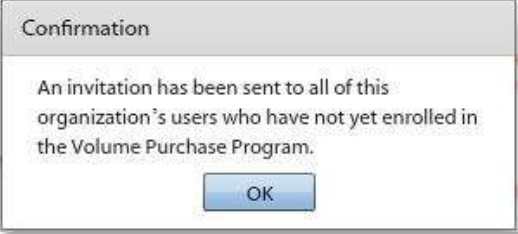


VPP App Licenses can be Reclaimed and Reused. When VPP app assignments are removed from the user device (assuming it is the last iOS 7.0.3+ device associated with the user), they are also removed from the user's iTunes account and the VPP app license is reclaimed for reuse. This is the advantage of the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

<p>Upload/Edit</p>	<p>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.</p> <p>Click Edit to upload a new token or edit/add the E-mail address associated with the VPP account.</p> <p><i>Note:</i> The APNs certificate must be uploaded before managing the VPP token. VPP token will be deleted if APNs certificate is removed.</p>	
<p>Remove</p>	<p>Removes the token from the server. Apps remain intact in the <i>Managed Apps</i> grid and on user devices. License count and automatic discovery of apps, however, no longer function.</p>	
<p>Sync Now</p>	<p>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 <i>Managed Apps</i> grid (iOS section) is accessed.</p>	
<p>Invite Users</p>	<p>Resends the invitation to join VPP to all qualifying users (iOS 7.0.3 or higher) that have not yet enrolled.</p> <p>Once a user accepts the VPP invitation, the application will be pushed out to the device.</p> <p><i>Note:</i> From the <i>User Grid</i>, you can invite an individual user. Select the user, then, on the left panel, click Send VPP Invitation.</p>	 <p>On the <i>User Grid</i>, check the VPP Association Status column to determine the status of the user's association with the program: <i>New</i> (not yet invited), <i>Invited</i> (invitation sent, but not yet accepted), or <i>Associated</i> (user enrolled in the program).</p>

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.

Select **System > Organization**



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

Organization Administrator Roles

See also [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	<ul style="list-style-type: none">• Can add or remove users and perform all the functions in the right-hand <i>Details</i> panel, except <i>Show Recovery Password</i>• Can email an individual user, but cannot use <i>Group Emailing</i>• Can perform most functions in the left-hand panel of <i>User Profile</i>• Can view the grids in the <i>Audit Data</i> and <i>Search Text Message Log</i> options (<i>User Profile</i>), but cannot view the body or attachments of a text message• Can choose the Visible Columns	<ul style="list-style-type: none">• Restricted from adding or removing users and from all functions in the right <i>Details</i> panel• Restricted from sending an email to an individual user or a group• Restricted from the <i>Location Data</i>, <i>Audit Data</i>, <i>Search Phone Log</i>, <i>Search Text Message Log</i>, and <i>File Archive</i> options in the left panel of <i>User Profile</i>• Read-only access to options in the left panel of <i>User Profile</i>• Can choose the Visible Columns for the <i>Users</i> list

	for the <i>Users</i> list	
Organization	Read-only access	Read-only access
Reporting	Full access (view and export)	Full access (view and export)
System	<ul style="list-style-type: none"> • Read-only access • Restricted from the <i>System Administration</i> option in the left panel 	<ul style="list-style-type: none"> • Read-only access • Restricted from the <i>System Administration</i> 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**



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 [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

Add >>

Remove <<

Restricted:

Support Admin
Restricted Admin
itmanager
jwitmer

Select All Select None Select All Select None

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.



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:
 - o Protect SMS
 - o Protect MMS
 - o Protect Location
 - o Protect Phone Logs
 - o 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.

Restrict Organization Administrative Roles

Not Restricted:		Restricted:
Full Admin FullOrgAdmin_West	Add ->>	Support Admin Restricted Admin itmanager jwitmer
	Remove -<<	
Select All Select None		Select All Select None

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*.
3. Click **Remove** to move a role from *Restricted* to *Not Restricted*.
4. Click **Save Changes** on the option bar at the top of the page.

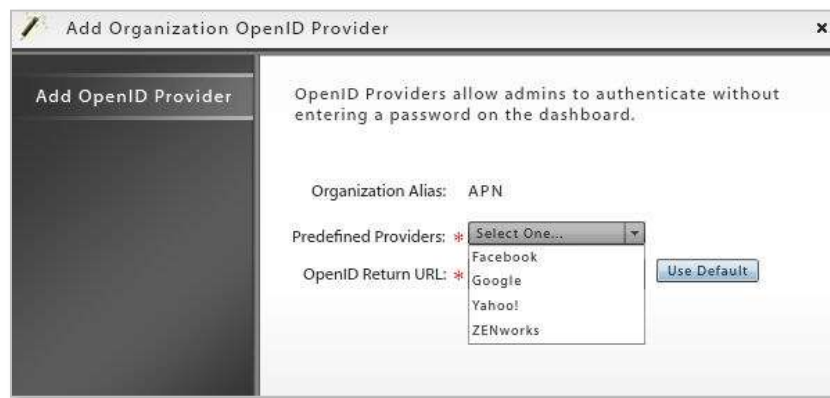
Configuring OpenID Providers for Organization Administrators

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 [OpenID Configuration for System Administrators](#).

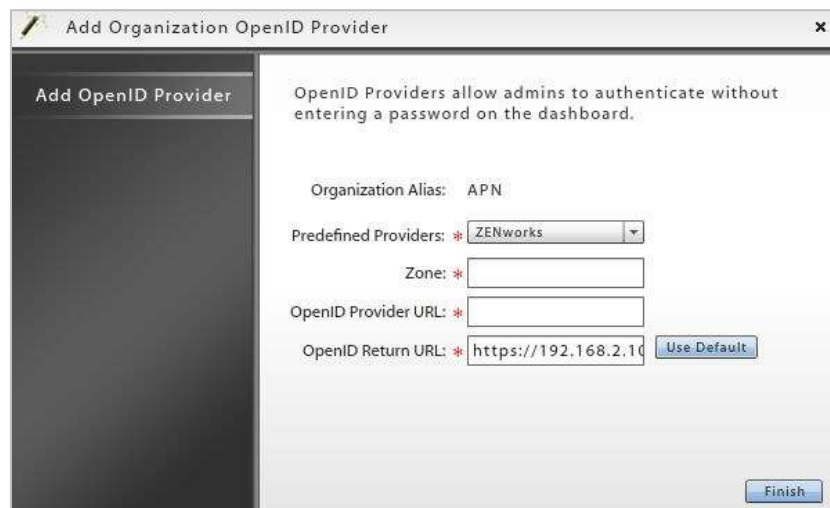
Add an OpenID Provider for Organization Administrators

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*.



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



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.

1. Select **Organization > Administrative Servers > OpenID Providers** and select a provider from the left panel.
2. 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**

The screenshot shows the 'OpenID Provider > Google' configuration page. The main form includes the following fields and controls:

- Organization Alias:** APN
- Enabled:**
- Predefined Providers:** Google (dropdown menu)
- OpenID Return URL:** http://ssl.novell.zmf (text input) with a 'Use Default' button to its right.
- OpenID Pin:** Reset All Pins (button)

Below the main form, there are two text areas:

- OpenID Provider Description:** An empty text input field.
- Notes for OpenID Provider:** A larger empty text area.

3. 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 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.

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**.



The screenshot shows the 'Add Organization Administrator' dialog box. The left sidebar has three tabs: 'Welcome', 'Administrator Details', and 'Account Settings'. The 'Administrator Details' tab is selected. The main area contains the following fields and controls:

- Administrator Login:
- Display Name:
- E-mail Address:
- Password:
- Confirm Password:
- Prompt For Password Change At First Login:

Buttons for 'Back' and 'Next' are located at the bottom right.

7. Enter the [Account Settings](#).



The screenshot shows the 'Add Organization Administrator' dialog box. The left sidebar has three tabs: 'Welcome', 'Administrator Details', and 'Account Settings'. The 'Account Settings' tab is selected. The main area contains the following fields and controls:

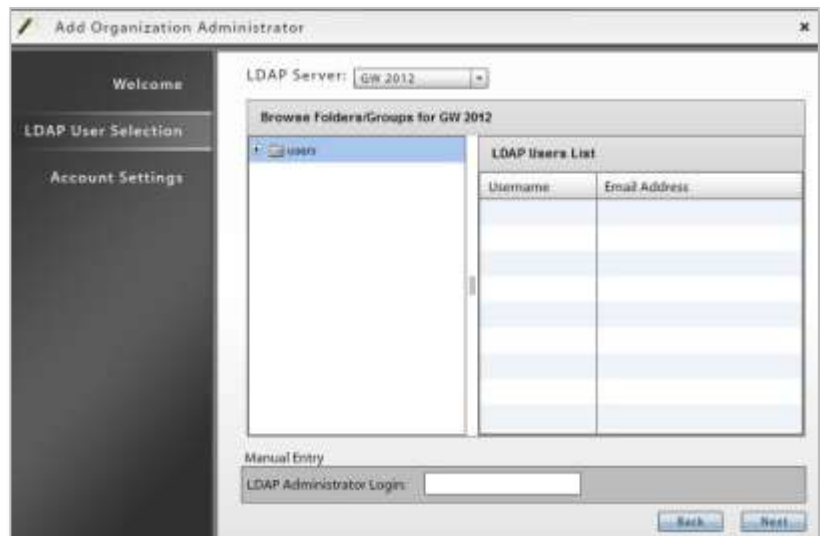
- Role:
- Default View:
- System Timeout (minutes):
- Add to Alert Recipients List:
- Carrier:
- Phone Number:
- Enabled:

Buttons for 'Back' and 'Finish' are located at the bottom right.

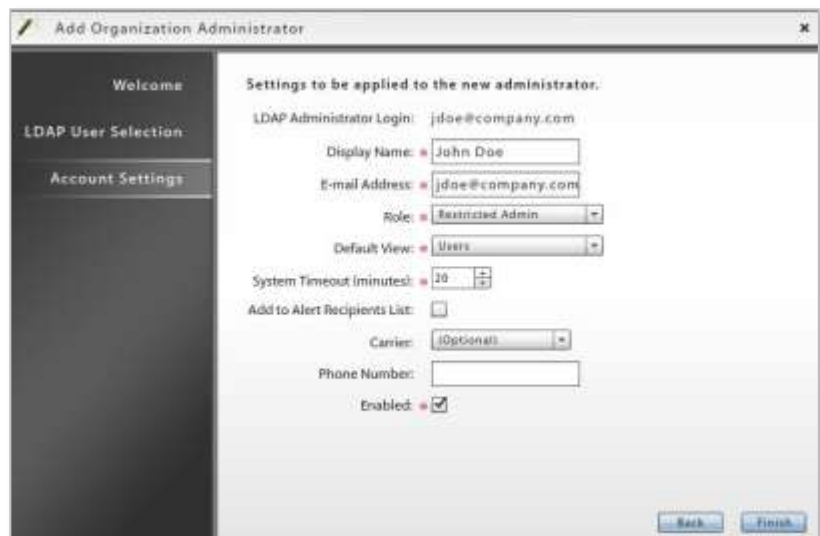
Add an LDAP Authenticated Organization Administrator Login

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**.



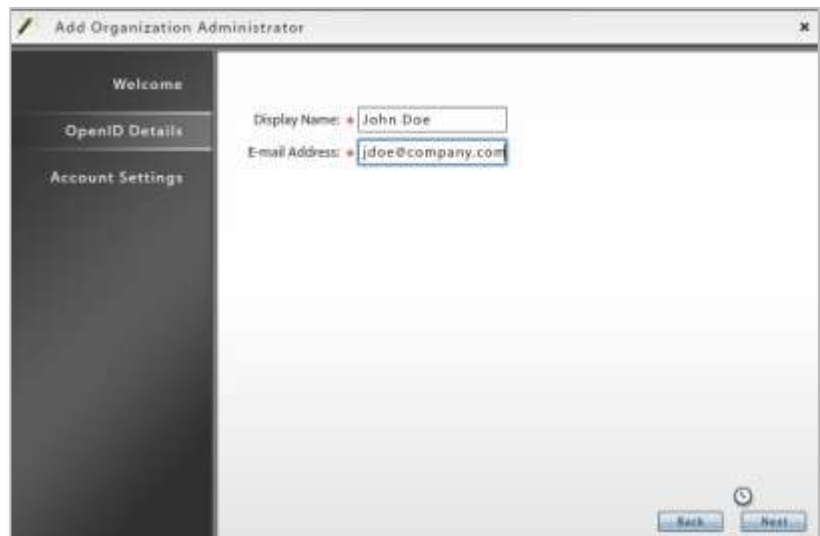
3. Enter a **Display Name** and the **Email Address** for the administrator.
4. Enter the remainder of the [Account Settings](#).



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**.



The screenshot shows the 'Add Organization Administrator' window. On the left is a dark sidebar with three menu items: 'Welcome', 'OpenID Details', and 'Account Settings'. The 'OpenID Details' section is active and contains two text input fields: 'Display Name' with the value 'John Doe' and 'Email Address' with the value 'jdoe@company.com'. At the bottom right of the main content area, there are two buttons: 'Back' and 'Next'.

4. Enter the [Account Settings](#).



The screenshot shows the 'Add Organization Administrator' window with the 'Account Settings' section active. The sidebar on the left is the same as in the previous screenshot. The 'Account Settings' section contains several fields: 'Role' (a dropdown menu set to 'Restricted Admin'), 'Default View' (a dropdown menu set to 'Users'), 'System Timeout (minutes)' (a numeric input field set to '20'), 'Add to Alert Recipients List' (a checkbox that is unchecked), 'Carrier' (a dropdown menu set to 'Optional'), 'Phone Number' (an empty text input field), and 'Enabled' (a checked checkbox). At the bottom right, there are two buttons: 'Back' and 'Finish'.

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**.

Settings > Organization Administrators

Organization Administrators

Organization Administrators Administrator Groups

Display Name	Administrator Username	OpenID Identity	Contact E-Mail Address
John Doe	jdoe@company.com		jdoe@company.com

Use OpenID:

User Name: *

Display Name: *

E-mail Address: *

Carrier:

Phone Number:

Add to Alert Recipients List:

Password:

LDAP: *

Role: *

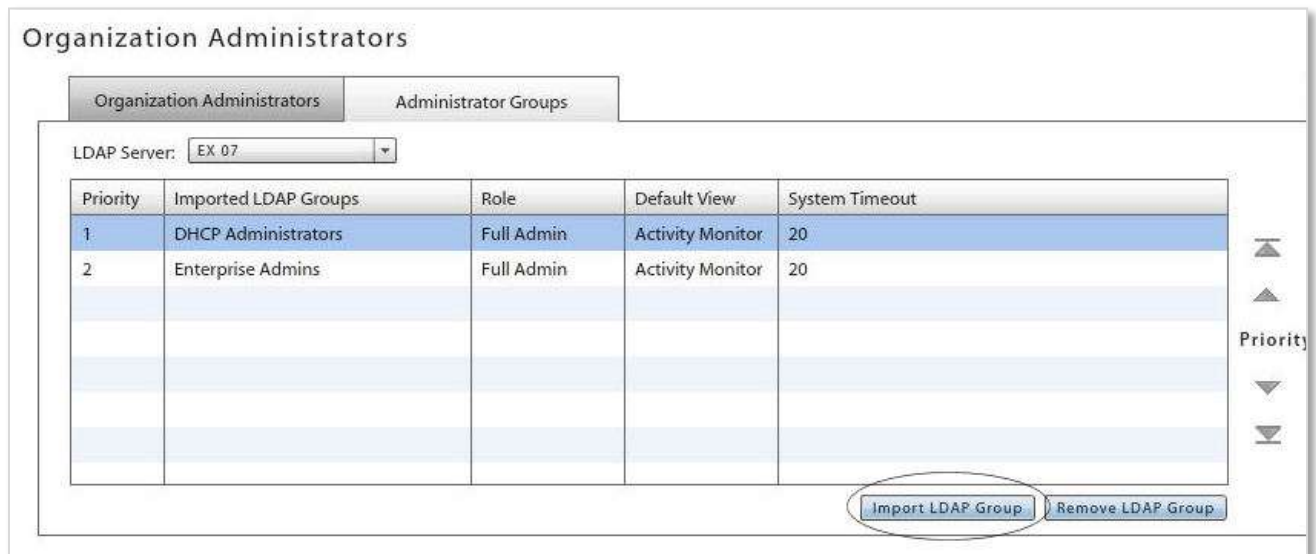
Default View: *

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.



The screenshot shows the 'Organization Administrators' interface with the 'Administrator Groups' tab selected. The 'LDAP Server' dropdown is set to 'EX 07'. A table lists imported LDAP groups with columns for Priority, Imported LDAP Groups, Role, Default View, and System Timeout. The 'Import LDAP Group' button is circled in red.

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**.



The screenshot shows the 'Import/Prioritize Groups' dialog box. It displays 'Groups on LDAP Server' for 'EX 07' and a search field. A list of group names is shown, with 'HelpServicesGroup' selected. The 'Finish' button is highlighted.

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

Organization Administrators | Administrator Groups

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

Priority

Import LDAP Group Remove LDAP Group

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.

Server Logging

System level logs assist administrators with diagnosing problems and in understanding the communications between devices and the server. Both server and device logging options are available.

Viewing Organization and System-Wide Logs

Select the **System** view and expand the **View Logs** option in the left panel. Choose one of the logs.

The following logs can be selected for viewing system-wide information, information from one or more organizations, or information for one or all devices.

- **ActiveSync Log** – Allows you to view events logged during connections between the *ZENworks Mobile Management* server and the ActiveSync server and between the devices' ActiveSync client and the *ZENworks Mobile Management* server.
- **GCM Log** – Allows you to view 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.
- **iOS MDM Sync Log** – Allows you to view successful events logged during connections between the *ZENworks Mobile Management* server and the Apple iOS MDM server and between the *ZENworks Mobile Management* server and the device's iOS MDM functions. Unsuccessful events (errors) are logged in the Error Chain Log. (iOS device specific)
- **ZENworks Sync Log** - Allows you to view events logged during connections between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server.
- **Data Usage Log** – Allows you to track the amount of data being exchanged:
 - Between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server
 - Between the device's ActiveSync client and the *ZENworks Mobile Management* server
 - As iOS MDM traffic between the device and the *ZENworks Mobile Management* servers
 - Between the *ZENworks Mobile Management* and ActiveSync servers.
- **Device Log** – Allows you to view a list of the device logs that have been previously requested. To request a new log, use the user level *Device Log* option associated with a user's profile.
- **Error Chain Log** – Allows you to view detailed messages for errors logged in the *iOS MDM Sync* log. (iOS device specific)

The following log can be selected for viewing information for one or more organizations.

- **Mail Message Log** – Allows you to view records of group emails sent from the dashboard.

The following logs only display system-wide information.

- **Database Task Scheduler Log** – Allows you to view all database task scheduler tasks that executed successfully or that gave an error.
- **Licensing Log** – Allows you to view server license validations that executed successfully or that gave an error.

Synchronization Logs

Synchronization logs give administrators the ability to view events logged during connections between servers and events logged during device connections with servers. There are three logs of this type:

The **ActiveSync Log** logs events that occur during connections between the *ZENworks Mobile Management* server and the ActiveSync server and between the devices' ActiveSync client and the *ZENworks Mobile Management* server.

The **GCM Log** logs successful events that occur during connections between the *ZENworks Mobile Management* server and the Google Cloud Messaging server and between the *ZENworks Mobile Management* server and Android devices using GCM service.

The **iOS MDM Sync Log** logs successful events that occur during connections between the *ZENworks Mobile Management* server and the Apple iOS MDM server and between the *ZENworks Mobile Management* server and the device's iOS MDM functions. Unsuccessful events (errors) are logged in the Error Chain Log. (iOS device specific)

The **ZENworks Sync Log** logs events that occur during connections between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server.

The logs display:

- Organization – Organization name
- DeviceSAKey – A device's internal identifier
- Log code – Code number associated with the logged event
- Description – Description associated with the log code
- Function Name – Displays a returned error; blank when log event is successful
- Details – Description or reason for the error; blank when log event is successful
- Time stamp – Date and time of the log event

Select **ActiveSync Log**, **ZENworks Sync Log**, **GCM Log**, or **iOS MDM Sync Log**.

The **Log Level** defaults to **Normal** and the log populates the grid with system-wide data from the past hour. If you change the log level to **Verbose**, click **Search**.

Narrow or expand the results of the search by:

- Editing the **From/To** filter
- Selecting one or more **Organizations** (hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item)
- Choosing one device by entering its **DeviceSAKey**, all devices, or devices without an SAKey (Null)

Click **Search**. When you edit the date/time filter or the search criteria, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the server log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.

ActiveSync Log

Log Level:

From: :

To: :

DeviceSAKey: ALL NULL

Organization

CAS

EX 2003

Exchange 2007

Organization	DeviceSAKey	Log Code	Description	Fur
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	413	Processing Folder Sync Command	
Exchange 2007	213	428	Processing Sync Command	
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	413	Processing Folder Sync Command	
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	428	Processing Sync Command	
Exchange 2007	213	421	Processing Ping Command	
Exchange 2007	213	428	Processing Sync Command	
Exchange 2007	213	428	Processing Sync Command	
Exchange 2007	213	428	Processing Sync Command	
Exchange 2007	213	413	Processing Folder Sync Command	

Sample Sync Log Grid

Database Task Scheduler Log

The Database Task Scheduler Log enables the administrator to view all database cleanup jobs that executed successfully or that gave an error.

The log displays:

- Database Task Name – Name assigned to the database cleanup task
- Log Code – Code number associated with the logged event
- Description – Description associated with the log code
- Function Name – Displays a returned error; blank when the log event is successful
- Details – Description or reason for the error; blank when the log event is successful
- Time stamp – Date and time a database cleanup job was executed

Select **Database Task Scheduler Log**.

The log populates the grid with system-wide data from the past hour.

Narrow or expand the results of the search by editing the **From/To** filter. Click **Search**. When you edit the date/time filter, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the database task scheduler log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.

Database Task Scheduler Log				
From:	06/05/2012	3	:	04 PM
To:	06/05/2012	4	:	04 PM
				<input type="button" value="Search"/>
Database Task Name	Log Code	Description	Function Name	Details
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha
	801	DatabaseTaskScheduler Error	MainLoop	There are currently no tasks tha

Data Usage Log

The data usage log displays the amount of data being exchanged between the device and servers; and the amount of data associated with the device that is proxied to and from the ActiveSync server. The types of data traffic that are logged include:

- Data between the device's *ZENworks Mobile Management* app and the *ZENworks Mobile Management* server
- Data between the device's ActiveSync client and the *ZENworks Mobile Management* server
- iOS MDM traffic between the device and the *ZENworks Mobile Management* servers (iOS devices only)
- Data between the *ZENworks Mobile Management* and ActiveSync servers

A summary report of data usage statistics is also available in the *Reporting* section.

The log displays:

- Organization – Organization name
- DeviceSAKey – A device's internal identifier
- Traffic Type – ActiveSync, iOS MDM Sync, or *ZENworks*
- Direction – Incoming or Outgoing
- Size (Bytes) – Size of the data transferred
- Time stamp – Date and time of the data transfer

Select **Data Usage Log**.

The log populates the grid with system-wide data from the past hour.

Narrow or expand the results of the search by:

- Editing the **From/To** filter
- Selecting one or more **Organizations** (hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item)
- Choosing one device by entering its **DeviceSAKey**, all devices, or devices without an SAKey (Null)

Click **Search**. When you edit the date/time filter or the search criteria, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the data usage log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.

Data Usage Log

From: 06/05/2012 3 : 08 PM

To: 06/05/2012 4 : 08 PM

DeviceSAKey: ALL NULL

Organization
EX 2003
Exchange 2007
...

Search

Organization	DeviceSAKey ▲	Traffic Type	Direction	Size (Bytes)	Time ▲
Exchange 2007	213	iOS MDM Sync	Incoming	306	06/05/2012 4:0
Exchange 2007	213	iOS MDM Sync	Outgoing	0	06/05/2012 4:0
Exchange 2007	213	iOS MDM Sync	Incoming	1447	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Incoming	13	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Outgoing	153	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Incoming	153	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Outgoing	13	06/05/2012 4:0
Exchange 2007	213	iOS MDM Sync	Outgoing	362	06/05/2012 4:0
Exchange 2007	213	iOS MDM Sync	Outgoing	4143	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Outgoing	0	06/05/2012 4:0
Exchange 2007	213	ZENworks Sync	Outgoing	33	06/05/2012 3:5
Exchange 2007	213	ActiveSync	Incoming	52	06/05/2012 4:0
Exchange 2007	213	ActiveSync	Outgoing	72	06/05/2012 4:0

Device Logs

The Device Logs option at the system level is simply a list of previous requests for device logs. The dashboard grid does not display log records, but gives information on when logs were received. Device logs are available from any device running the *ZENworks Mobile Management* app.

The grid displays:

- Organization – Organization name
- DeviceSAKey – A device's internal identifier
- Time Requested and Requester
- Received – Whether or not log has been received
- Time Received – Date and time a response was received
- Error – Error message if log could not be obtained

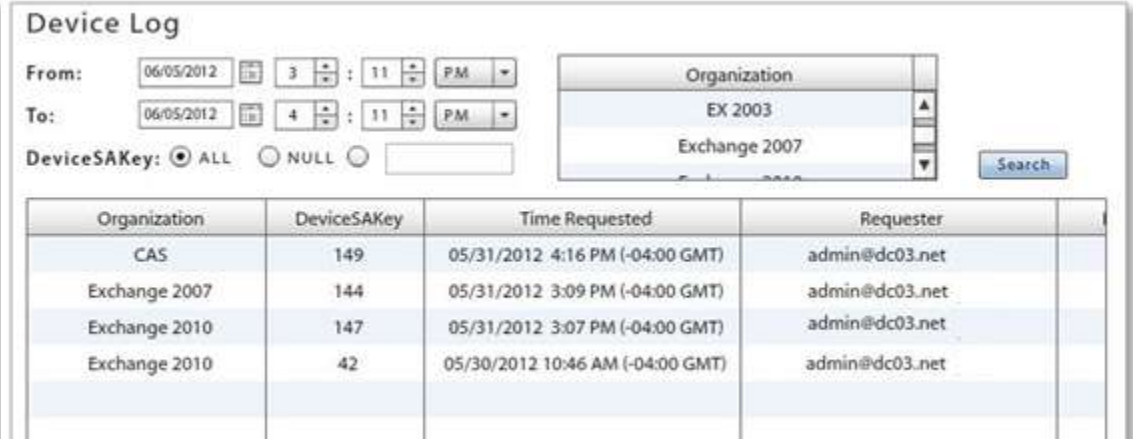
Select **Device Log**.

The log populates the grid with system-wide notifications of log receipts from the past hour.

Narrow or expand the results of the search by:

- Editing the **From/To** filter to filters the time stamp of the logs (not the records in the log)
- Selecting one or more **Organizations** (hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item)
- Choosing one device by entering its **DeviceSAKey**, all devices, or devices without an SAKey (Null)

Click **Search**. When you edit the date/time filter or the search criteria, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.



The screenshot shows the 'Device Log' interface. At the top, there are search filters: 'From' and 'To' date/time pickers, a 'DeviceSAKey' filter with radio buttons for 'ALL', 'NULL', and a text input, and an 'Organization' dropdown menu. A 'Search' button is located to the right of the dropdown. Below the filters is a table with the following data:

Organization	DeviceSAKey	Time Requested	Requester
CAS	149	05/31/2012 4:16 PM (-04:00 GMT)	admin@dc03.net
Exchange 2007	144	05/31/2012 3:09 PM (-04:00 GMT)	admin@dc03.net
Exchange 2010	147	05/31/2012 3:07 PM (-04:00 GMT)	admin@dc03.net
Exchange 2010	42	05/30/2012 10:46 AM (-04:00 GMT)	admin@dc03.net

Device Log Grid

Select a log file and click the **Download Log** button. Save the log file on the desktop or in another designated folder. The file can be viewed in the .txt format.

Error Chain Log (iOS device specific)

The error chain log provides a view of messages detailing errors logged in the *iOS MDM Sync* log.

The log displays:

- Organization – Organization name
- DeviceSAKey – A device's internal identifier
- Error Code – Code number associated with the error
- Error Domain – Contains internal codes used by Apple useful for diagnostics (may change between Apple releases)
- Localized Description – Description of codes
- Time stamp – Date and time the error occurred

Select **Error Chain Usage Log**.

The log populates the grid with system-wide data from the past hour.

Narrow or expand the results of the search by:

- Editing the **From/To** filter
- Selecting one or more **Organizations** (hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item)
- Choosing one device by entering its **DeviceSAKey**, all devices, or devices without an SAKey (Null)

Click **Search**. When you edit the date/time filter or the search criteria, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the error chain log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.

Error Chain Log

From: 06/05/2012 3 : 13 PM
To: 06/05/2012 4 : 13 PM
DeviceSAKey: ALL NULL

Organization
EX 2003
Exchange 2007
Exchange 2007

Organization	DeviceSAKey	Error Code	Error Domain	Localized Description
Exchange 2007	213	4001	MCIInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" could not be installed.
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account already exists.
Exchange 2007	213	4001	MCIInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" could not be installed.
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account already exists.
Exchange 2007	213	4001	MCIInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" could not be installed.
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account already exists.
Exchange 2007	213	4001	MCIInstallationErrorDomain	Profile Failed to Install
Exchange 2007	213	1009	MCProfileErrorDomain	The profile "MDM iOS ActiveSync File" could not be installed.
Exchange 2007	213	21005	MCEASErrorDomain	An identical Exchange account already exists.

Licensing Log

The licensing log is a log of license validations that executed successfully or that gave an error.

The log displays:

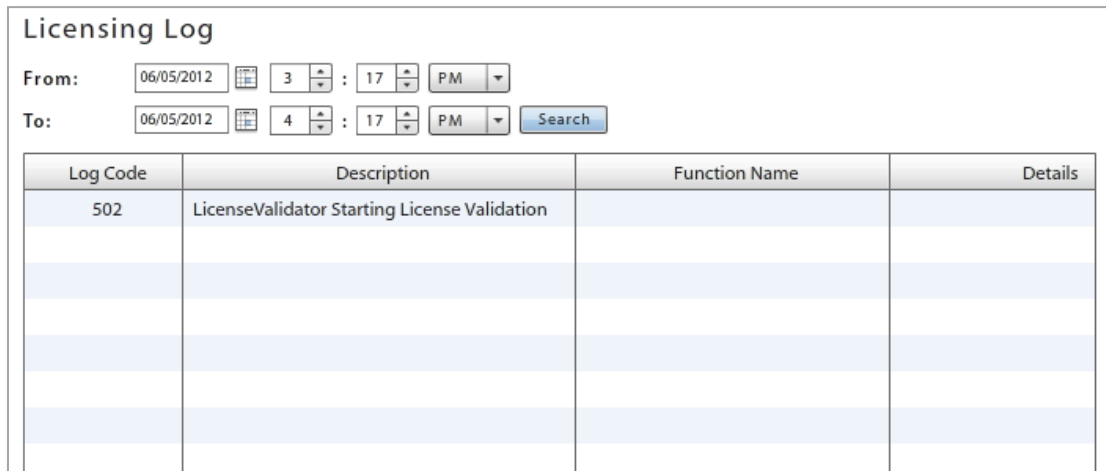
- Log Code – Code number associated with the logged event
- Description – Description associated with the log code
- Function Name – Displays a returned error; blank when log event is successful
- Details – Description or reason for the error; blank when log event is successful
- Time stamp – Date and time the license validation occurred

Select **Licensing Log**.

The log populates the grid with system-wide data from the past hour.

Narrow or expand the results of the search by editing the **From/To** filter. Click **Search**. When you edit the date/time filter, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the licensing log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.



The screenshot shows the 'Licensing Log' interface. At the top, there is a search filter with 'From:' and 'To:' fields. The 'From:' field is set to '06/05/2012' at '3:17 PM'. The 'To:' field is set to '06/05/2012' at '4:17 PM'. A 'Search' button is located to the right of the 'To:' field. Below the filter is a table with four columns: 'Log Code', 'Description', 'Function Name', and 'Details'. The table contains one row of data: Log Code '502', Description 'LicenseValidator Starting License Validation', Function Name (blank), and Details (blank). There are several empty rows below the first one.

Log Code	Description	Function Name	Details
502	LicenseValidator Starting License Validation		

Mail Message Log

The mail message log provides an administrator with a method to view the records of group emails sent from the dashboard.

The log displays:

- Organization – Organization name to which the email was sent
- Administrator – The administrator who sent the email
- SMTP Server – The SMTP server through which the email was sent
- Subject – Email subject
- Message – Body text of the email message
- Recipients Emails – Email addresses of recipients of the email
- Timestamp – Date and time the email was sent
- Ownership – Whether device ownership was specified as criteria for recipients; company/personal/any
- Liability – Whether device liability was specified as criteria for recipients; corporate/individual/any

Select **Mail Message Log**.

The log populates the grid with system-wide data from the past hour.

Narrow or expand the results of the search by:

- Editing the **From/To** filter
- Selecting one or more **Organizations** (hold the SHIFT or CTRL key to select multiple items; hold the CTRL key to unselect an item)

Click **Search**. When you edit the date/time filter or the search criteria, the system maintains the changes as preferred settings for all system level log views until you change the settings or log out of the dashboard.

When the mail message log has populated, it can be sorted by any of the grid columns and data can be exported to a .CSV or .XLS file.

The screenshot shows the 'Mail Message Log' interface. At the top, there are filters for 'From' and 'To' with date and time pickers. Below these is a list of organizations: 'Organization', 'acostello', 'CAS', and 'Exchange 2007'. A 'Search' button is located to the right of the organization list. Below the filters is a table with the following columns: 'Organization', 'Administrator', 'SMTP Server', 'Subject', and 'Message'. The first row of data shows: 'Exchange 2007', 'System Admin Full', 'Exchange 2007', 'Sunday Server Maintenance', and 'The mail server will un'.

Organization	Administrator	SMTP Server	Subject	Message
Exchange 2007	System Admin Full	Exchange 2007	Sunday Server Maintenance	The mail server will un

System Administration

This section of the guide documents topics related to system level management of the *ZENworks Mobile Management* server. The dashboard areas where system tasks are performed require system administrator login credentials. System administrations can include the management of multiple organizations. In addition to all the Organization administration permissions documented in the first part of this guide, a system administrator with full admin status has the following system level permissions:

- View all organizations on the *ZENworks Mobile Management* server
- Add, edit or remove organizations
- Switch organizations without logging out and back in to another organization
- Create administrative roles and administrative logins
- Send group email to one or all organizations, administrators, and users
- Access *System Settings* to upload a signing certificate
- View server and device logs
- Set database cleanup tasks
- Apply a plug-in
- Check for and download *ZENworks Mobile Management* server software updates

System management tasks are performed from the **System** view. This view is only accessible with a system administrator login. The login you create when installing the *ZENworks Mobile Management* server software is a system administrator login.

The screenshot shows the ZENworks Mobile Management System Administration interface. The top navigation bar includes icons for Activity Monitor, Users, Organization, Reporting, and System. The System view is active, showing a breadcrumb trail: Settings > System Administration. The left sidebar lists various system management options, with 'System Administration' selected. The main content area displays a table of Organizations. The table has the following data:

Name	Contact Person	CP Primary Email	CP Primary Phone	CP Primary Phone Ext
Exchange 2007	admin	admin@dc03.net	1	
AC	AC	acostello@gw2012.net	3302251127	

Below the table, there is a field for 'Organization Name' with the value 'Exchange 2007' entered.

Managing Multiple Organizations

Multi-Tenant ZENworks Mobile Management Systems

A single instance of the *ZENworks Mobile Management* server application supports a multi-tenant architecture, which allows an enterprise to manage one or multiple organizations.

Multiple organizations might be used to categorize various divisions of a company. For example: Production/Sales/Management departments can each be an “organization” on the same *ZENworks Mobile Management* server or Seattle/Chicago/Boston divisions can each be a separate “organization.”

Switching Organizations

When you are logged in to the *ZENworks Mobile Management* system with a system administrator login, you initially choose the organization you want to view. You also have access to all other organizations existing on the server through the *System Administration* menu. Switching from one organization to another is accomplished by using the **Switch Organizations** option.

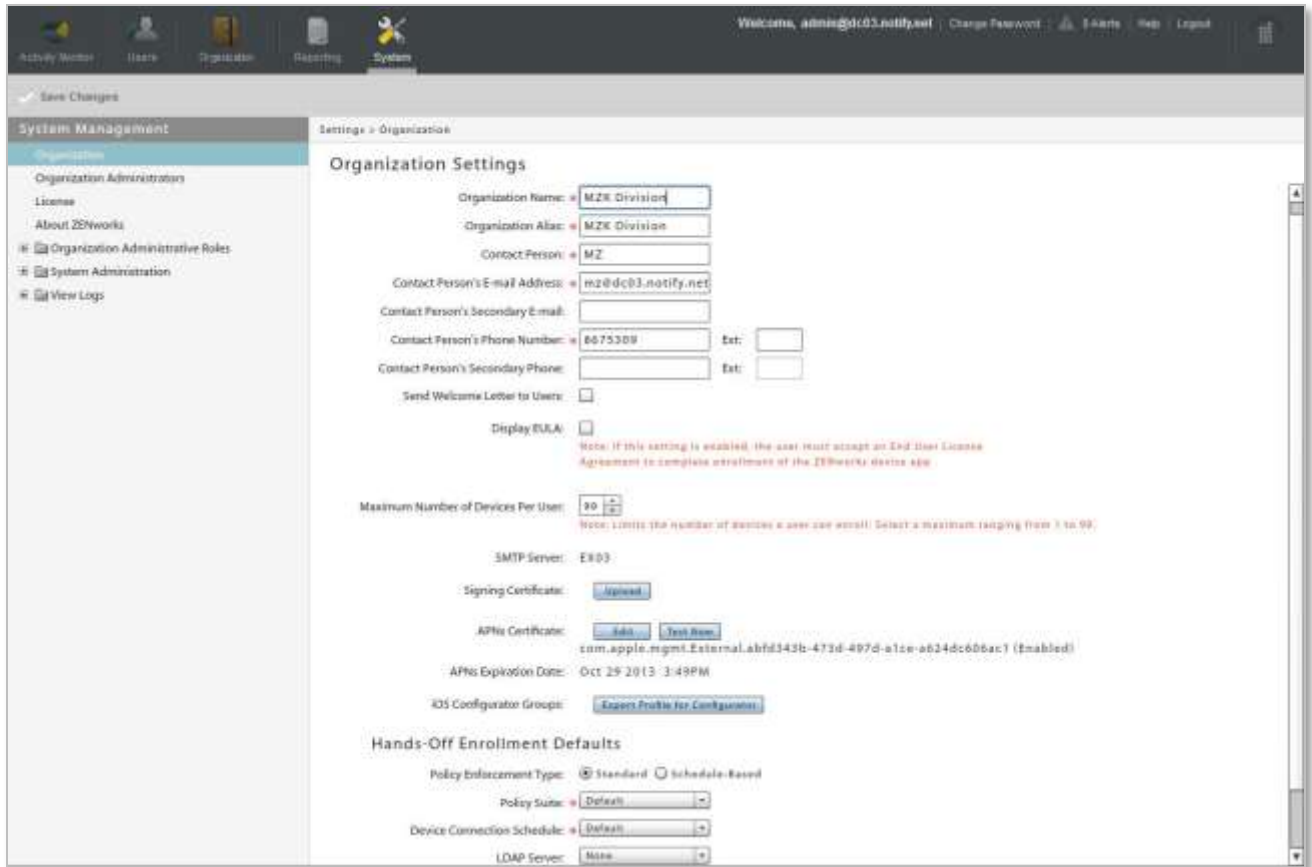
From the *System* view, select **System Administration > Organizations**. Click **Switch Organizations** in the gray option bar.



The Organization List

The organization list gives you access to the configured settings of each organization on the server. Select an organization from the list to view or edit the configured settings for the organization.

- Organization name and contact information
- Welcome letter enablement – emails a welcome letter when users are added
- EULA enablement - 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 below)
- Organization and Hands-Off enrollment configuration
 - Policy Enforcement Type
 - Policy Schedule
 - Policy Suite(s)
 - Device Connection Schedule
 - (Administrative) LDAP Server
 - Liability
 - Local Groups



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.

The SSL certificate being used on the server can also be used as the signing certificate. Export the SSL certificate to a file, selecting the box that ensures that the private key gets exported with the certificate. Then upload it to the *ZENworks Mobile Management* server.

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



Managing the 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**.



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**.

Save Changes

System Management Settings > System Administration > Organization Licensing

Organization Licensing

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

Update License Key:

Database Task Scheduler

For full documentation on the *Database Task Scheduler*, see the [Database Table Maintenance](#) guide.

When devices make a connection to the *ZENworks Mobile Management* Server, information regarding those connections is logged in the database and stored for potential troubleshooting purposes.

The amount of information that is logged depends on several factors, such as the number of users on the *ZENworks Mobile Management* Server, the type of traffic being sent back and forth, the amount of logging taking place, and the frequency of device connection intervals. Over time, this information can build up in the database and grow excessively.

Administrators with full admin login credentials can use the **Database Task Scheduler** to set clean-up jobs to run at regular intervals in order to clear excess data and maintain optimal database performance.

To access the *Database Task Manager*, select **System > System Administration > Database Task Scheduler**.

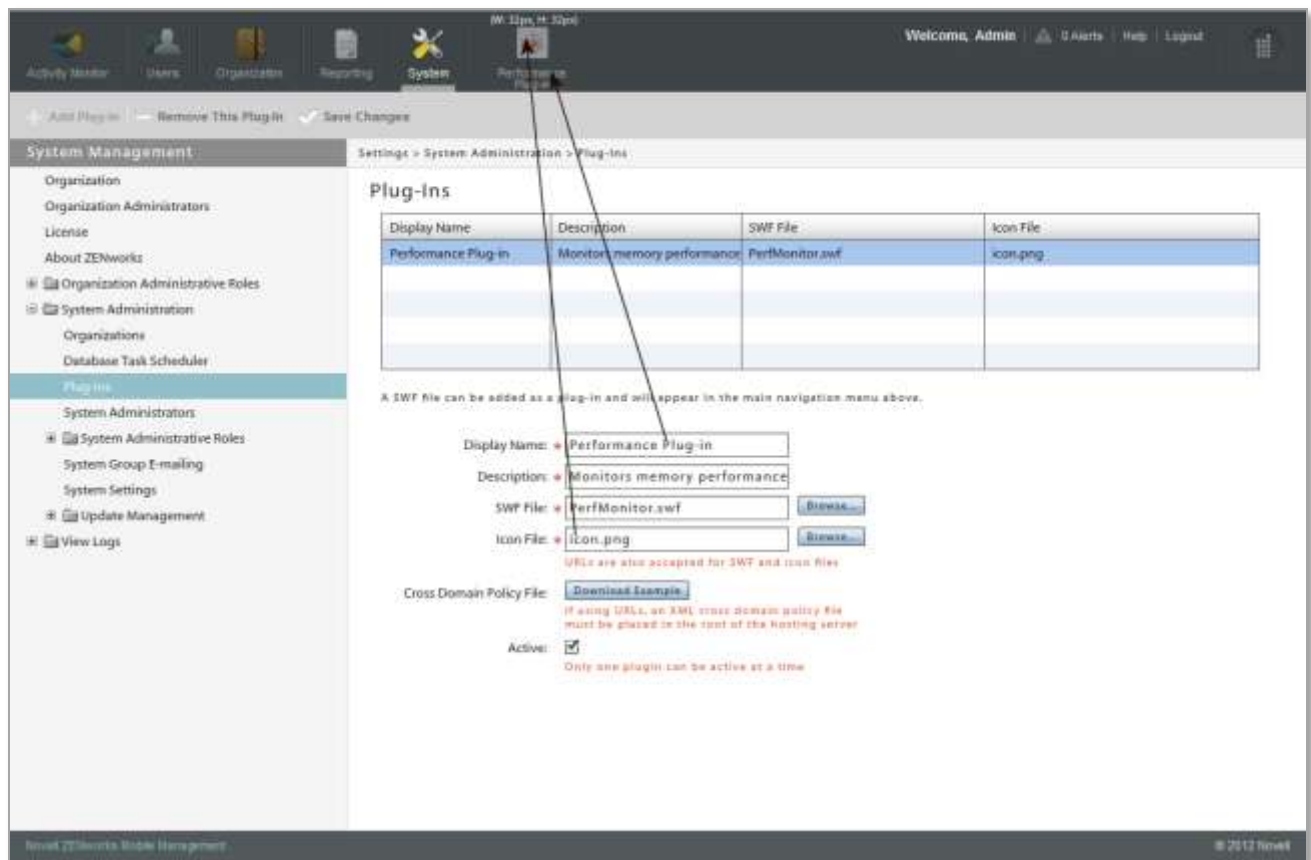
Plug-Ins

The *ZENworks Mobile Management* Plug-Ins feature allows administrators to plug a SWF (Adobe Flash file) into the *ZENworks Mobile Management* dashboard. This lets you add a way to interface with another console to the dashboard.

From the *System* page of dashboard, administrators can define the location of any SWF (Adobe Flash file) they have created.

To further customize the *ZENworks Mobile Management* server pages, administrators can insert custom logos and icons via the [System Settings](#) that appear on the *ZENworks Mobile Management* login page and in *ZENworks Mobile Management* dashboard navigation menu.

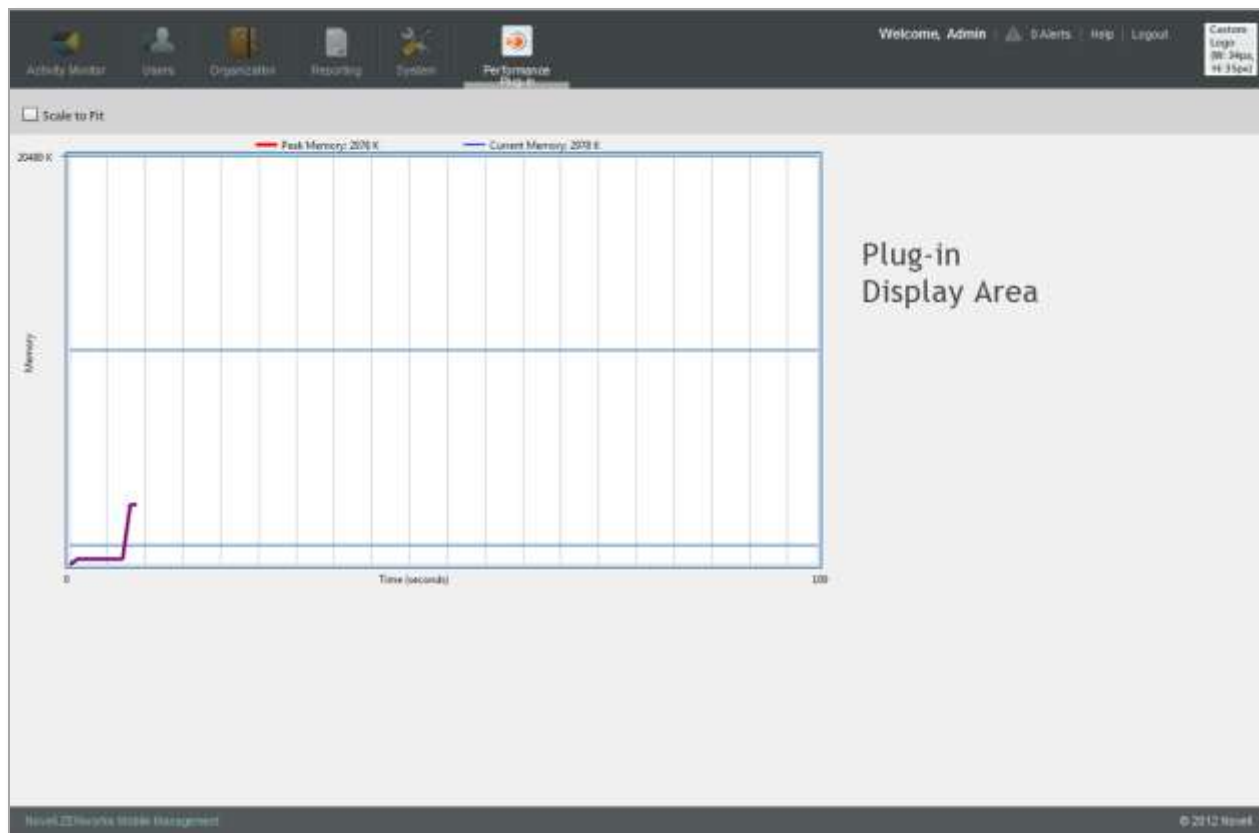
To access *Plug-Ins*, select **System > System Administration > Plug-Ins**. You must be a system administrator with full admin login credentials.



Sample ZENworks Dashboard with SWF Plugged In

Adding a Plug-In

1. Click **Add Plug-In** in the option bar.
2. Enter a **Display Name** and **Description**. The name you enter appears in the *ZENworks Mobile Management* dashboard navigation menu under the plug-in's icon.
3. In the **SWF File** field, enter a URL for a remote storage location or store the .swf file on the *ZENworks Mobile Management* server and enter the file name.
A file stored locally should be in /Novell/ZENworks/mobile/web/dashboard/plugins/swfs/
 4. In the **Icon File** field, enter a URL for a remote storage location or store the icon file on the *ZENworks Mobile Management* server and enter the file name. This icon appears in the *ZENworks Mobile Management* dashboard navigation menu. Clicking on this icon in the *ZENworks* menu opens the Plug-In display area.
 - A file stored locally should be in /Novell/ZENworks/mobile/web/dashboard/plugins/icons/
 - Acceptable file formats are .png, .jpg, or .gif
 - Image size - W:34px, H:35px
 5. If you are using URLs, place an XML **Cross Domain Policy File** at the root of the hosting server.
So that Adobe Flash does not prevent *ZENworks Mobile Management* from accessing data on the remote locations you have designated, the cross policy file must define exceptions. Click **Download Example** to download a template to assist you in creating an XML file with the appropriate content.
 6. Mark the plug-in as **Active** for it to take effect.



Sample of the plug-in display area

System Administrator Roles

See also [Organization Administrator Roles](#)

Predefined System Administrator Roles

There are six predefined roles built in to the *ZENworks Mobile Management* system. 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: *System Administrative Roles* or *Organization Administration Roles*. Three of the predefined roles are used for organization administrator logins. (See [Predefined Organization Administrator Roles](#).)

The three predefined system administrator roles are:

- **Full System Admin** – There are no limitations with this type of login credential. It gives full administrative permissions in every organization created on the *ZENworks Mobile Management* server. An administrator with this type of login can add organizations and switch organizations without logging off the *ZENworks Mobile Management* server. They can also apply *ZENworks Mobile Management* server updates via the *ZENworks Mobile Management Update Manager* application and configure the *Database Task Scheduler*.
- **Support System Admin** – Gives limited administrative access or read only access in every organization created on the *ZENworks Mobile Management* server. System Administrators can switch organizations without logging out of the *ZENworks Mobile Management* server. Although they cannot apply *ZENworks Mobile Management* server software updates, they can access the Update Management page in the dashboard where they can check for and download *ZENworks Mobile Management* patches in preparation for the application of the update.
- **Restricted System Admin** – Restricted from viewing private data such as Location, MMS/SMS Log, Phone Log, and File Archive. Has Read only permissions for all other views. Restricted administrators can switch organizations without logging out of the *ZENworks Mobile Management* server.

System Administrator credentials give access to all organizations on the *ZENworks Mobile Management* server. System Administrators can switch organizations without logging off the *ZENworks Mobile Management* server. Credentials may be authenticated via an LDAP server and may be assigned *Full Admin*, *Support Admin* (read only), or *Restricted Admin* (limited read only) permissions.

System Administrators also have access to the *Update Management* information on the dashboard. System administrator credentials with *Full Admin* permissions are required to use the *Update Manager* application.

The administrative login created during the process of installing the *ZENworks Mobile Management* server application is a System Administrator Login with the predefined *Full Admin* permissions.

See the table below for details on the various System Administrator roles or view the permissions via the *Role Permissions* option in the *System* view.

Who Should Have System Administrator Logins

A system administrator login is required for anyone who needs access to all organizations on the *ZENworks Mobile Management* server. Some examples are:

- Administrators of a system where users have been grouped into separate organizations.
- Administrators who will apply *ZENworks Mobile Management* server software updates.
- Administrators who will configure database cleanup tasks.

SYSTEM ADMINISTRATOR ROLES		
Dashboard View	Support System Admin	Restricted System Admin
Activity Monitor	Read-only access; cannot disable or snooze alerts	Read-only access; cannot disable or snooze alerts
Users	<ul style="list-style-type: none"> • Can add or remove users and perform all the functions in the right-hand <i>Details</i> panel, except <i>Show Recovery Password</i> • Can email an individual user, but cannot use <i>Group Emailing</i> • Can perform most functions in the left panel of <i>User Profile</i> • Can view the grids in the <i>Audit Data</i> and <i>Search Text Message Log</i> options (<i>User Profile</i>), but cannot view the body or attachments of a text message • Can choose the Visible Columns for the <i>Users</i> list 	<ul style="list-style-type: none"> • Restricted from adding or removing users and from all functions in the right <i>Details</i> panel • Restricted from sending an email to an individual user or a group • Restricted from the <i>Location Data</i>, <i>Audit Data</i>, <i>Search Phone Log</i>, <i>Search Text Message Log</i>, and <i>File Archive</i> options in the left-hand panel of <i>User Profile</i> • Read-only access to options in the left panel of <i>User Profile</i> • Can choose the Visible Columns for the <i>Users</i> list
Organization	Read-only access	Read-only access
Reporting	Full access (view and export)	Full access (view and export)
System	<ul style="list-style-type: none"> • Read-only access • Can switch between organizations without logging out of the <i>ZENworks Mobile Management</i> server • Can view the <i>Update Management</i> page; Can check for and download server software updates. Cannot apply updates, because Support Admins do not have access to the <i>Update Manager</i> 	<ul style="list-style-type: none"> • Read-only access • Can switch between organizations without logging out of the <i>ZENworks Mobile Management</i> server • Can view the <i>Update Management</i> page; Can check for and download server software updates. Cannot apply updates, because Restricted Admins do not have access to the <i>Update Manager</i>

Customized System Administrator Roles

Administrators can create customized system 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 [System 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.

1. Select **System > System Administration > System Administrative Roles > Role Permissions > Add Role**.



2. Choose a method for creating a System Administrative Role:
 - Use the sliders to determine the role's initial settings. The new role copies the settings of the predefined *System Full Admin*, *Support Admin*, or *Restricted Admin*.
 - Copy the settings of an existing role
3. Specify the role permissions to copy.
4. Enter a **Role Name** and **Description**.
5. Click **Finish** to save the new role.
6. Find and select the role in the *System Administrative Roles* grid.
7. Set the permissions associated with dashboard access. See [Appendix A: Role Permissions](#) for a comprehensive list.

Configuring an OpenID Provider for System 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 [OpenID Configuration for Organization Administrators](#).

Manage the OpenID Provider for System Administrators

You can enable or disable the OpenID provider configured for System Administrators. You can also change its settings or reset the OpenID Pin for all users logging in through this OpenID provider.

1. Select **System > System Administration > OpenID Provider**.
2. Configure the following settings:

- **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** – select from a drop-down list of provider types: *Facebook*, *Google*, *Yahoo!*, or *ZENworks*
- **OpenID Provider URL** – (ZENworks provider) enter the URL of the ZENworks Primary Server in the following form: <https://<server>:<port>/zenworks/?requestHandler=ZENOpenIDHandler>
- **OpenID Return URL** – 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.
- **Description and Notes**

The screenshot shows the 'OpenID Provider' configuration page. The breadcrumb trail is 'Settings > System Administration > OpenID Provider'. The page title is 'OpenID Provider'. There are four main sections: 1. 'Enabled' with a checked checkbox. 2. 'Predefined Providers' with a dropdown menu showing 'Google'. 3. 'OpenID Return URL' with a text input field containing 'https://ssl.novell.zm' and a 'Use Default' button. 4. 'OpenID Pin' with a 'Reset All Pins' button. Below these are two large text areas: 'OpenID Provider Description' and 'Notes for OpenID Provider', both currently empty.

3. 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.

4. Enable the OpenID option for each administrator you will allow to log in with OpenID credentials. See also [OpenID Authenticated Administrator Logins](#).

System Administrator Logins

See also, [Organization Administrator Logins](#)

Creating System Administrator Logins

A *System Administrator* with full admin privileges is created during the initial installation of *ZENworks Mobile Management*. It is a local system administrator login in that it authenticates directly against the *ZENworks Mobile Management* server with the unique password you created during the installation.

Additional system administrator logins with assigned roles can be created through the dashboard. For information on roles see [System Administrator Roles](#).

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



Best Practices: Always maintain at least one local system 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.

To create a System Administrator Login, select **System > System Administration > System Administrators > Add System Administrator**.

Choose how the administrator should be authenticated: **Manual** (local), **LDAP**, **OpenID**. The *Add System Administrator* wizard steps you through creating login credentials for system administrators.

- [Add a Manually \(locally\) Authenticated Administrator Login](#)
- [Add an LDAP Authenticated Administrator Login](#)
- [Add an OpenID Authenticated Administrator Login](#)

Enter the administrator details, then choose the account settings.

Add a Manually (locally) Authenticated System Administrator Login

Add a system 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**.



The screenshot shows the 'Add System Administrator' wizard window. The left sidebar has three sections: 'Welcome', 'Administrator Details', and 'Account Settings'. The 'Administrator Details' section is active. The main area contains the following fields and options:

- Administrator Login:
- Display Name:
- E-mail Address:
- Password:
- Confirm Password:
- Prompt For Password Change At First Login:

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

7. Enter the [Account Settings](#).



The screenshot shows the 'Add System Administrator' wizard window. The left sidebar has three sections: 'Welcome', 'Administrator Details', and 'Account Settings'. The 'Account Settings' section is active. The main area contains the following fields and options:

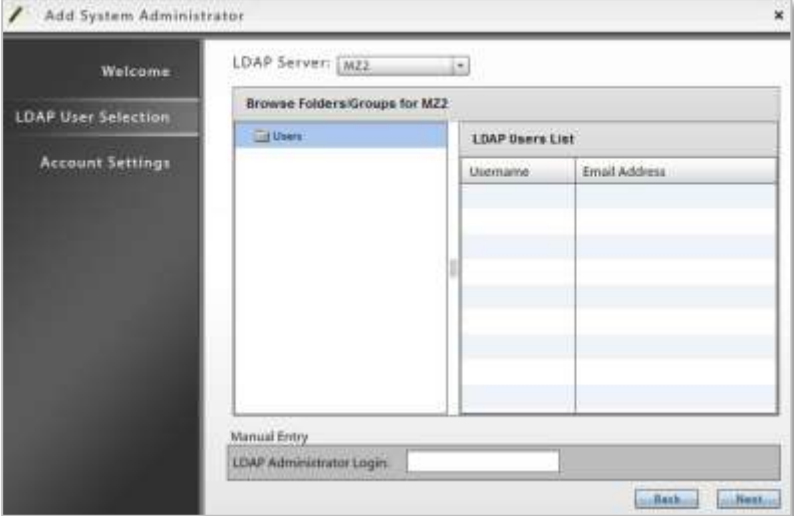
- Role:
- Default View:
- System Timeout (minutes):
- Enabled:

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

Add an LDAP Authenticated System Administrator Login

Add a system 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**.



The screenshot shows the 'Add System Administrator' dialog box. On the left is a sidebar with 'Welcome', 'LDAP User Selection', and 'Account Settings'. The main area has 'LDAP Server: M22' selected. Below is a tree view for 'Browse Folders/Groups for M22' with 'Users' selected. To the right is an 'LDAP Users List' table with columns 'Username' and 'Email Address'. At the bottom, there is a 'Manual Entry' section with an 'LDAP Administrator Login' text box and 'Back' and 'Next' buttons.

3. Enter a **Display Name** and the **Email Address** for the administrator.
4. Enter the remainder of the [Account Settings](#).

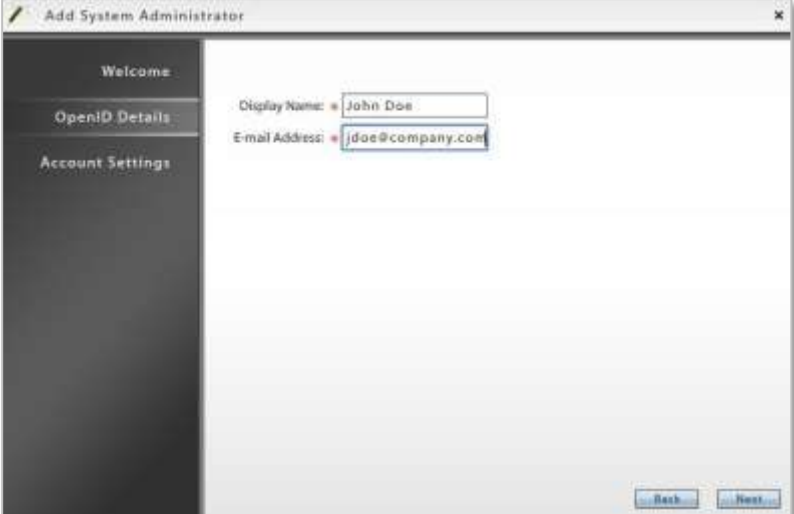


The screenshot shows the 'Add System Administrator' dialog box in the 'Account Settings' step. The sidebar is the same. The main area is titled 'Settings to be applied to the new administrator.' and contains the following fields: 'LDAP Administrator Login: jdoe@company.com', 'Display Name: John Doe', 'E-mail Address: jdoe@company.com', 'Role: Full Admin', 'Default View: System', 'System Timeout (minutes): 20', and 'Enabled: [checked]'. 'Back' and 'Finish' buttons are at the bottom right.

Add an OpenID Authenticated System Administrator Login

Add a system 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**.



The screenshot shows the 'Add System Administrator' dialog box with the 'OpenID Details' tab selected. The 'Display Name' field contains 'John Doe' and the 'Email Address' field contains 'jdoe@company.com'. The 'Account Settings' tab is visible in the sidebar but not selected. 'Back' and 'Next' buttons are at the bottom right.

4. Enter the [Account Settings](#).



The screenshot shows the 'Add System Administrator' dialog box with the 'Account Settings' tab selected. The 'Role' dropdown is set to 'Full Admin', the 'Default View' dropdown is set to 'System', the 'System Timeout (minutes)' spinner is set to 20, and the 'Enabled' checkbox is checked. The 'Back' and 'Finish' buttons are at the bottom right.

System Administrators Account Settings

- **Role** – Assign a permissions level to the login. Choose from:
 - Predefined **Full Admin** – Full administrative permissions
 - Predefined **Support Admin** – Read-only permissions with limited editing capabilities
 - Predefined **Restricted Admin** – Read-only permissions with private data restrictions; cannot view Location Data, Audit Data, MMS/SMS or Phone Logs, and File Archive
 - **Any custom System 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
- **Active Status** – Select the box to *enable* this administrative login
- **Password** – Assign a password if you are creating a login that does not use LDAP authentication.

Managing System Administrator Logins

You must be logged into the *ZENworks Mobile Management* server with system administrator (*Full Admin*) credentials in order to edit or remove a System Administrator.

Best Practices: Always maintain at least one *System Administrator* that authenticates directly against the *ZENworks Mobile Management* server and that does not use LDAP or OpenID authentication.

Managing Individual Administrator Logins

1. Select **System** > **System Administration** > **System Administrators**. Click the **System 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 System Administrator**.

The screenshot displays the 'System Administrators' configuration page in the ZENworks Mobile Management interface. The page is divided into a left-hand navigation pane and a main content area. The navigation pane includes options like 'Add System Administrator', 'Remove System Administrator', and 'Save Changes'. The main content area shows a table of system administrators with columns for Display Name, Administrator User, OpenID Identity, Contact E-Mail, Role, Enabled, and Created. Below the table is a form for editing a selected administrator, with fields for User Name, Display Name, E-mail Address, Password, LDAP, Role, Default View, System Timeout (minutes), Enabled, Created By, and Date Created.

Display Name	Administrator User	OpenID Identity	Contact E-Mail	Role	Enabled	Created
twhitehouse	twhitehouse		twhitehouse@dc03.net	Full Admin	true	01/14/2013 11:49 AM
Robin		https://www.google.com/accounts/o	ngpencer@ex07.net	Full Admin	true	01/14/2013 11:49 AM
John Doe	jdoe@company.com		jdoe@company.com	Full Admin	true	01/14/2013 11:49 AM
cteski	cteski@dc03.net		cteski@dc03.net	Full Admin	true	01/14/2013 11:49 AM
cschuster2	cschuster2		cschuster2@ex07.net	Full Admin	true	01/14/2013 11:49 AM
cschuster2	cschuster2@ex07.net		cschuster2@ex07.net	Full Admin	true	01/14/2013 11:49 AM
admin@dc03.net	admin@dc03.net		admin@ex07.net	Full Admin	true	01/14/2013 11:49 AM

Use OpenID:

User Name:

Display Name:

E-mail Address:

Password:

LDAP:

Role:

Default View:

System Timeout (minutes):

Enabled:

Created By: admin@dc03.net

Date Created: 01/14/2013 11:49 AM [-05:00 GMT]

Importing System Administrator LDAP Groups

Importing system 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 > System Administration > System 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.

System Administrators

System Administrators Administrator Groups

LDAP Server: MZ2

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

Priority

Import LDAP Group Remove LDAP Group

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

Import/Prioritize Groups

Groups on LDAP Server

EX 07

Search

*

Reset

Group Name

HelpServicesGroup

TelnetClients

IS_WPG

WINS Users

DHCP Users

DHCP Administrators

Cancel Finish

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)

The screenshot shows the 'System Administrators' configuration page. At the top, there are tabs for 'System Administrators' and 'Administrator Groups'. Below the tabs, there is a dropdown for 'LDAP Server' set to 'MZ2'. A table lists administrator groups with columns for Priority, Imported LDAP Groups, Role, Default View, and System Timeout. The first row is selected, showing Priority 1, Imported LDAP Groups 'Enterprise Admins', Role 'Full Admin', Default View 'Activity Monitor', and System Timeout '20'. To the right of the table are arrows for adjusting priority. Below the table are buttons for 'Import LDAP Group' and 'Remove LDAP Group'. At the bottom, there are configuration fields for the selected group: Group Name (Enterprise Admins), LDAP Server Name (MZ2), Enforced Role (Full Admin), Added By (admin@dc03.net), and Date Added (01/14/2013 11:55 AM (-05:00 GMT)). There are also fields for Default View (Activity Monitor) and System Timeout (minutes) (20).

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

Group Name: Enterprise Admins
 LDAP Server Name: MZ2
 Enforced Role: Full Admin
 Added By: admin@dc03.net
 Date Added: 01/14/2013 11:55 AM (-05:00 GMT)

Default View: Activity Monitor
 System Timeout (minutes): 20

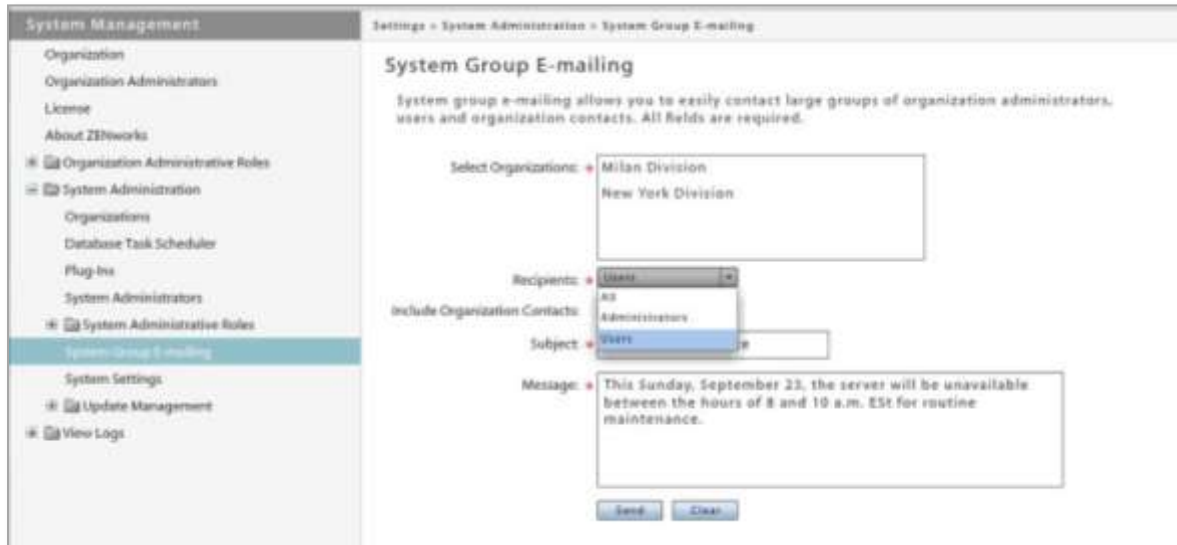
5. If there are administrators that belong to multiple groups, use the arrows to the right of the group grid to prioritize the groups.

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

System Group Emailing

System Group E-mailing gives the administrator the ability to send a system-wide email to one or multiple organizations and can include administrators, users or both. The sender can also elect to copy the organization contacts.

To send a group email, select **System > System Group E-mail**.



System Settings

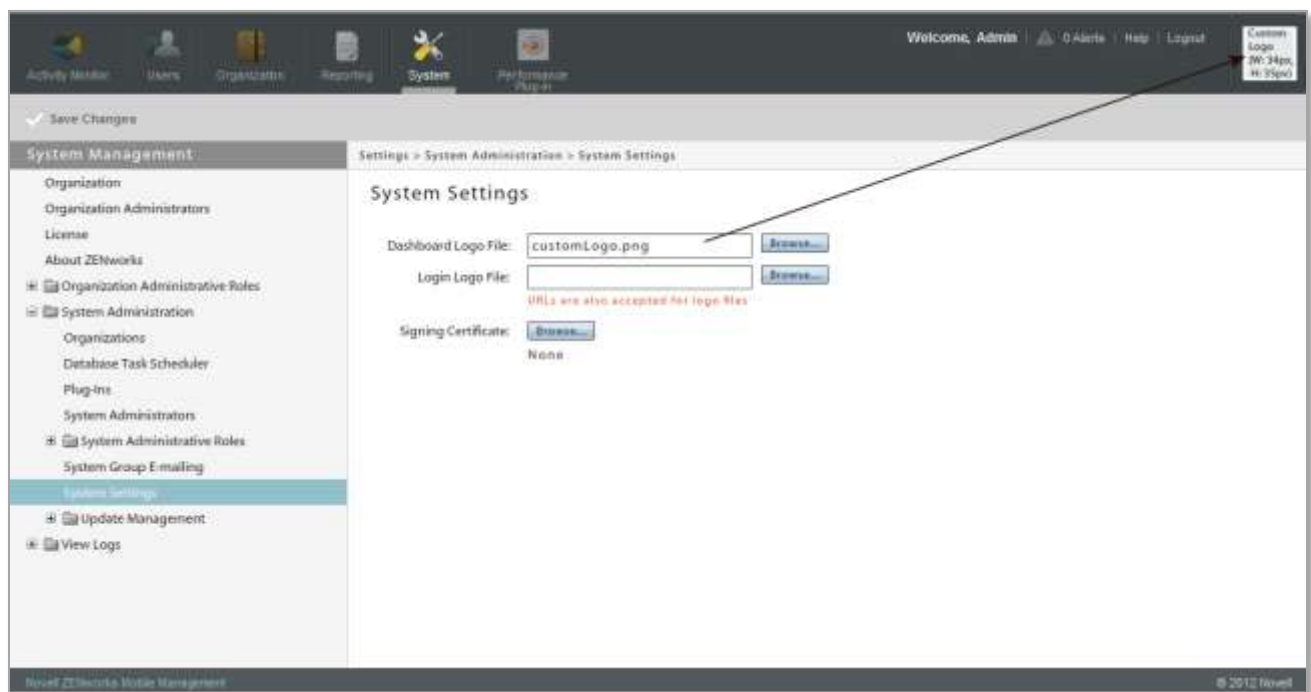
Custom Dashboard and Login Logos

To customize the *ZENworks Mobile Management* server pages, administrators can insert custom logos and icons that appear in *ZENworks Mobile Management's* dashboard navigation menu and on the *ZENworks Mobile Management* login page.

To insert logos, select **System > System Administration > System Settings**. You must be a system administrator with full admin login credentials.

In the **Dashboard Logo File** field, enter a URL for a remote storage location or store the file on the *ZENworks Mobile Management* server and browse to select the file name. This logo appears in the upper left corner of the *ZENworks Mobile Management* dashboard, next to the navigation menu.

- A file stored locally should be in
Novell/ZENworks/mobile/web/dashboard/images/CustomLogos/
- Acceptable file formats are .png, .jpg, or .gif
- Image size: W:34px, H:35px



Sample Customized Dashboard Logo

In the **Login Logo File** field, enter a URL for a remote storage location or store the file on the *ZENworks Mobile Management* server and enter the file name. This logo appears on the *ZENworks Mobile Management* login page.

- A file stored locally should be in
/Novell/ZENworks/mobile/web/dashboard/images/CustomLogos/
- Acceptable file formats are .png, .jpg, or .gif
- Image size: W:256px, H:129px



Sample ZENworks Mobile Management Login Page with Customized Login Logo

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 in *System Settings* allows you to *add a signing certificate for any organization across the ZENworks Mobile Management system*. This must be a CA signed certificate, because self-signed certificates are currently not supported.

A signing certificate defined for a single organization will override this system-wide signing certificate.

1. Select **System > System Administration > System Settings**
2. Click the **Upload** button next to the signing certificate field.



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

Update Management

The *ZENworks Mobile Management* server product has integrated update management features that facilitate smooth and convenient software updates to the *ZENworks Mobile Management* server. These features consist of the dashboard's *Update Management* page and the **Update Manager** application, which is used on the physical *ZENworks Mobile Management* server(s) to apply updates.

Update Management in the dashboard provides:

- Sections that display current information about available updates and historical information about versions already applied using the Update Manager application
- An option to check for updates
- An option to download the available updates

Updates cannot be applied from the dashboard. A system administrator must use the *ZENworks Mobile Management Update Manager* application to install the updates.

For more information on the *Update Management* page and the *ZENworks Mobile Management Update Manager* application, see the [Update Management Guide](#).

Checking for Updates and Update Notifications

The *ZENworks Mobile Management* server automatically checks for updates once every 24 hours. You can also initiate an on-demand check by using the **Check For Updates** button in the *Update Management* page of the dashboard.

When an update is available, system administrators logging into the *ZENworks Mobile Management* dashboard see a notification for the update in the lower left corner of the dashboard. The notification fades away automatically or the administrator can dismiss it. Clicking the notification navigates to the *Update Management* section of the dashboard where the administrator can view information about the available updates or download the updates.



The Update Management Page

The *Update Management* page is located under the *System* view of the dashboard and is only accessible with a system administrator login. There are two sections of this page, the *Manager* section and the *History* section.

Update Management: Manager

From the *Manager* section, you can view information about the updates that are currently available. The server automatically checks for updates every 24 hours, however, you can initiate an on-demand check for updates from this page. Although updates cannot be applied from this page, you can download updates in preparation for a scheduled maintenance. When you check for updates, you are prompted for Novell login credentials if you have not used them previously to access updates, or if they have changed. You can also reload updates. This removes updates that have been downloaded, but not installed. Available updates are then automatically reloaded. This might be used in a case where an update became corrupted for some reason and could not be installed.

Update Management: History

From the *History* section, you can view statistics about software updates that have already been applied via the *ZENworks Mobile Management Update Manager* application.

Administrator Audit Trail

ZENworks Mobile Management's administrator audit trail provides traceability and accountability for changes, adjustments, and actions performed by *ZENworks Mobile Management* administrators.

Audit trail records can assist administrators in:

- Determining the cause of unexpected behavior or system states
- Identifying compromised administrator accounts
- Identifying malicious administrator activity
- Tracking the source of changes
- Finding trends
- Maintaining general corporate auditing records

Phase One of the Administrator Audit Trail feature audits administrator login/logout activity, updates to Policy Suites, as well as administrator-initiated security and device compliance actions. These logs can be accessed from the database and include sufficient details to restore the historic state of the system.

Phase One functionality does not provide dashboard accessibility. However, Novell Technical Support Staff, can assist *ZENworks Mobile Management* administrators with techniques in using the raw data for troubleshooting and restoration purposes, where applicable.

Phase One of the *Administrator Audit Trail* feature audits the following activities:

- Administrator login/logout activity
- Deletion of an organization
- Updates to policy suites
- Security actions performed from the dashboard
 - Lock Device
 - Selective Wipe
 - Full Wipe
 - Show Recovery Password
 - Wipe Storage Card
 - Disable/Enable Device
- Administrator actions
 - Clear Device Enrollment
 - Clear Passcode
 - Send Welcome Letter
 - Clear ZENworks Authorization Failures
 - Clear ActiveSync Authorization Failures
 - Clear SIM Card Removed or Changed Violation
 - View Device Violation Details

Accessing the Data

Although Phase One does not provide dashboard accessibility, the information listed above is logged and can be viewed in the database or accessed via database queries.

Please contact our Novell Technical Support Staff, for assistance with techniques in using the raw data for troubleshooting and restoration purposes. You can also reference [Accessing Administrator Audit Records](#) in the Knowledge Base, which provides a script to get the audited information and several stored procedures that an administrator can run to view the records.

Future development of ZENworks Mobile Management's Administrator Audit Trail will provide further functionality. The following features are planned for several phases of development:

- In addition to traceability for actions performed by administrators, future functionality will also track actions performed by users via the Desktop and Mobile User Self-Administration Portals.
- Additional log entries for:
 - Creating/removing organizations and users
 - Server configurations and changes
 - Compliance Manager configurations and changes
 - File Share and Managed Apps updates
 - Certificate uploads or removals
 - Update Manager usage
 - Device Connection Schedule updates
 - Custom Columns updates
 - iOS user resource configurations, changes, and assignments
 - Administrator login/logout
- Dashboard access
 - Viewing audit trail log entries in the UI
 - Custom sorting/filtering/searching functionality
 - Audit trail export functionality
 - Viewing detailed record values

Appendix A: Role Permissions

Role permissions associated with dashboard access are listed in a directory tree. There are five parent categories that correspond to the five dashboard views.

The ability to edit a permission in a subset depends on whether or not the categories above the permission are enabled. For example, in order to enable **Clear Device Enrollment**, **Full Access** needs to be enabled for both the **Users** and **Administration** categories above it.

Parent Category	First Subset Level	Second Subset Level	Third Subset Level	Full Access	Read Only
Activity Monitor				•	•
Users				•	•
	Add User			•	
	Administration			•	
		Clear Passcode		•	
		Disable Device		•	
		Full Wipe		•	
		Lock Device		•	
		Reset for Enrollment		•	
		Send Welcome Letter		•	
		Show Recovery Password		•	
		Stop Managing Devices		•	
		Suspend Device		•	
		Trigger APN		•	
		Trigger GCM		•	
		Wipe Storage Card		•	
	Device Compliance			•	•
		Clear ActiveSync Authorization Failures		•	•
		Clear SIM Card Removed or Changed Violation		•	•
		Clear ZENworks Authorization Failures		•	•
		View Device Violation Details		•	•
	Device Reporting			•	•
	E-mail User			•	•

Parent Category	First Subset Level	Second Subset Level	Third Subset Level	Full Access	Read Only
	Location			•	•
	Logging			•	•
	Messaging			•	•
	Remove User			•	
	User Profile			•	•
		All Devices Summary		•	•
		Apps		•	•
		Assign Access Point Names		•	•
		Assign CalDAV		•	•
		Assign CardDAV		•	•
		Assign Exchange Servers		•	•
		Assign LDAP Servers		•	•
		Assign Mail Servers		•	•
		Assign Provisioning Profiles		•	•
		Assign SCEP Servers		•	•
		Assign Subscribed Calendars		•	•
		Assign VPN		•	•
		Assign Web Clips		•	•
		Assign Wi-Fi Networks		•	•
		Audit Data		•	•
		Client Certificates		•	•
		Custom Columns		•	•
		Device Configuration		•	•
		File Archive		•	•
		iOS MDM Settings		•	•
		Last Sync Data		•	•
		Local Groups		•	•
		Location Data		•	•
		Search Phone Log		•	•
		Search Text Message Log		•	•
		Security		•	•
		User Configuration		•	•
		User Information		•	•
		View Logs		•	•

Parent Category	First Subset Level	Second Subset Level	Third Subset Level	Full Access	Read Only
			ActiveSync Log	•	•
			Configuration/Feedback Log	•	•
			Data Usage Log	•	•
			Device Log	•	•
			Error Chain Log	•	•
			GCM Sync Log	•	•
			iOS MDM Sync Log	•	•
			ZENworks Sync Log	•	•
Organization				•	•
	Administrative Servers			•	•
		ActiveSync Servers		•	•
		Administrative LDAP Servers		•	•
		OpenID Provider		•	•
		SMTP Server		•	•
	Android Corporate Resources			•	•
		VPNs		•	•
		Wi-Fi Networks		•	•
	Application Management			•	•
		Managed Apps		•	•
		Novell Filr		•	•
		Whitelist/Blacklists		•	•
	Compliance Manager			•	•
	iOS Corporate Resources			•	•
		Access Point Names		•	•
		CalDAV Servers		•	•
		CardDAV Servers		•	•
		Exchange Servers		•	•
		LDAP Servers		•	•
		Mail Servers		•	•
		Provisioning Profiles		•	•
		SCEP Servers		•	•
		Subscribed Calendars		•	•

Parent Category	First Subset Level	Second Subset Level	Third Subset Level	Full Access	Read Only
		VPN		•	•
		Web Clips		•	•
		Wi-Fi Networks		•	•
	Organization Control			•	•
		Custom Columns		•	•
		File Share		•	•
		Group E-mailing		•	•
		Local Groups		•	•
	Policy Management			•	•
		Device Connection Schedules		•	•
		Policy Schedules		•	•
		Policy Suites		•	•
Reporting					•
System				•	•

Appendix B: System Maintenance

Database cleanup and backup are two key elements in maintaining and ensuring efficient system performance. The best practices outlined below should be incorporated into your organization's system maintenance routine.

Database Cleanup

Verify that the database cleanup tasks have been enabled. When the ZENworks Mobile Management server software is installed, tasks are enabled, by default, with parameters for a system accommodating 1000 devices. Administrators of larger systems should adjust the task parameters according to the recommendations in the Database Maintenance Guide. To verify that the jobs are running, access the Database Task Scheduler from the dashboard and view the task grid. The grid displays which cleanup jobs are enabled, the last time each job was executed, and when each job will run again.

If a database task fails to run, you can check the DatabaseTaskSchedulerLogs database table for errors. See Server Logging in this guide.

Backup

Periodically backing up the database is an essential practice for system maintenance. A daily backup of the database, preferably streamed off-site, is recommended at minimum.

In addition, back up the MDM.ini file on the Web/Http server. This file is found under the ZENworks directory. Default directory: C:\Program Files\Novell\ZENworks\mobile.

Regular backups ensure that data can be recovered if the database becomes compromised. With both a database backup and a backup of the MDM.ini file, a system can be fully restored if necessary.