System Administration

ZENworks® Mobile Management 3.2.x

October 2015
Legal Notices

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

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

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

Copyright © 2012-15 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).

Novell Trademarks

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

Third-Party Materials

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

### Accessing the Dashboard  
Accessing the Dashboard

### Administrator Roles and Logins  
Administrator Roles and Logins

- System Administrator Roles  
- Predefined System Administrator Roles  
- Customized System Administrator Roles  
- Configuring an OpenID Provider for System Administrators  
- System Administrator Logins  
- Creating System Administrator Logins  
- Managing System Administrator Logins  
- Importing System Administrator LDAP Groups

### System Administration  
System Administration

- Managing Multiple Organizations  
- The Organization List  
- Managing Organization Licensing  
- Database Task Scheduler  
- Plug-Ins  
- System Group Emailing  
- System Settings  
  - Custom Dashboard and Login Logos  
  - Signing Certificate Upload: Server Level  
  - Enabling GCM Service for the System  
  - APNs Settings  
- Update Management  
- Administrator Audit Trail

### Server Logging  
Server Logging

- Synchronization Logs  
- Database Task Scheduler Log  
- Device Logs  
- Error Chain Log (iOS device specific)  
- Licensing Log  
- Mail Message Log

### Appendix A: Role Permissions  
Appendix A: Role Permissions

### Appendix B: System Maintenance  
Appendix B: System Maintenance
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.
Administrator Roles and Logins

System Administrator Roles

See also Organization Configuration: 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 Organization Configuration: 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

<table>
<thead>
<tr>
<th>Dashboard View</th>
<th>Support System Admin</th>
<th>Restricted System Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Monitor</td>
<td>Read-only access; cannot disable or snooze alerts</td>
<td>Read-only access; cannot disable or snooze alerts</td>
</tr>
</tbody>
</table>

**Activity Monitor**
- Can add or remove users and perform all the functions in the right-hand Details panel, except Show Recovery Password
- Can email an individual user, but cannot use Group Emailing
- Can perform most functions in the left panel of Device Profile
- Can view the grids in the Audit Data and Search Text Message Log options (Device Profile), but cannot view the body or attachments of a text message
- Can choose the Visible Columns for the Users list

**Users**
- Restricted from adding or removing users and from all functions in the right Details panel
- Restricted from sending an email to an individual user or a group
- Restricted from the Location Data, Audit Data, Search Phone Log, Search Text Message Log, and File Archive options in the left-hand panel of Device Profile
- Read-only access to options in the left panel of Device Profile
- Can choose the Visible Columns for the Users list

**Organization**
- Read-only access

**Reporting**
- Full access (view and export)
- Full access (view and export)

**System**
- Read-only access
- Can switch between organizations without logging out of the ZENworks Mobile Management server
- Can view the Update Management page; Can check for and download server software updates. Cannot apply updates, because Support Admins do not have access to the Update Manager
- Can switch between organizations without logging out of the ZENworks Mobile Management server
- Can view the Update Management page; Can check for and download server software updates. Cannot apply updates, because Restricted Admins do not have access to the Update Manager
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.

   ![Create New System Administrative Role Wizard](image)

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 [Organization Configuration: 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 format: `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**

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 Configuration: 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.

7. Enter the Account Settings.
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**.

3. Enter a **Display Name** and the **Email Address** for the administrator.

4. Enter the remainder of the **Account Settings**.

![Add System Administrator](image)
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**.

4. Enter the **Account Settings**.
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

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.
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.

3. Select a group to import and click 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)

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.
Organization Administrator Roles and Logins

Who should have an organization administrator role and login. Organization Administrator Roles and Logins are ideal for those responsible for configuring and maintaining a single organization on a hosted server or on a system with groups of users that have been divided into separate organizations. See full documentation on this topic at: Organization Configuration and Management: Organization Administrator Roles and Logins

Roles

Like System Administrator roles, there are three predefined Organization Administrator roles: Full Admin, Support Admin, and Restricted Admin. The permissions for these roles cannot be altered. In addition, administrators can create customized organization administrator roles to tailor the permissions associated with ZENworks Mobile Management dashboard login credentials. You can set permissions for these roles via the Role Permissions option under the System view: Select Organization Administration Roles > Role Permissions

OpenID Authentication

OpenID is an open standard that allows organization 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.

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.

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.
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 Administration can include the management of multiple organizations. In addition to all the Organization administration permissions documented in 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
- 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.
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.

In the right corner of the dashboard header, click Switch Org

The Switch Organizations option can also be accessed from the System view. Select System > Organizations, then 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 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 (description)
- Organization and Hands-Off enrollment defaults
  - Policy Enforcement Type
  - Policy Schedule
  - Policy Suite(s)
  - Device Connection Schedule
  - (Administrative) LDAP Server
  - Liability
  - Local Groups

From the System view, select **System Administration > Organizations.**
Signing Certificate Upload: Organization Level

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**.

See also, [Signing Certificate Upload: Server Level](#).

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 Organization Licensing

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.

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.
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](image)

**Signing Certificate Upload: Server Level**

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. See also, [Signing Certificate Upload: Organization Level](#).

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.
Enabling GCM Service for the System

**ZENworks Mobile Management** can use the Google Cloud Messaging service to let Android devices know that it is time to synchronize. Whenever notifications for the device are available, the **ZENworks Mobile Management** server connects with GCM servers. GCM then pings the Android 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.

**Obtain your GCM Credentials.** You must first 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.

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.

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 via the Google API Console.
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.
APNs Settings

If you have System Administrator privileges, you can apply an existing APNs certificate to multiple organizations on the ZENworks Mobile Management server.

For example, on-premise systems that have categorized various divisions of a company by creating multiple organizations can allow those organizations to share one APNs certificate.

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

A list of organizations appears in the APNs Settings grid. If there is an APNs certificate associated with the organization, the Apple ID, Expiration Date, and Certificate Topic (certificate file) are listed beside it.

<table>
<thead>
<tr>
<th>Organization Name</th>
<th>Apple ID</th>
<th>Expiration Date</th>
<th>Certificate Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS</td>
<td><a href="mailto:cascluster@ev07.notify">cascluster@ev07.notify</a></td>
<td>Aug 21 2015 12:46PM</td>
<td>com.apple.mgmt:External.966idd53a-0735-4533-9be2-243b095d35f7</td>
</tr>
</tbody>
</table>

There are several functions you can perform from this grid.

- **Set Up** an APNs certificate for the first time for one or multiple organizations
  See also, APNS Certificate Generation.
- Renew an APNs certificate for one or multiple organizations (click **Setup**)
  See also, APNS Certificate Generation.
- **Disable/Enable** or **Delete** an APNs certificate for one or multiple organizations
- Copy an existing APNs certificate from one organization to one or multiple organizations (**Copy To**)
  **Caution:** Copying a certificate will overwrite any existing certificate associated with the organization(s) selected.

To select multiple consecutive organizations in the grid, hold the SHIFT key and click on the first and last organization.

To select multiple random organizations in the grid, hold the CTRL key and select organizations.
**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 be 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
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.

- **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.
### Sample Sync Log Grid

<table>
<thead>
<tr>
<th>Organization</th>
<th>DeviceSAKey</th>
<th>Log Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>421</td>
<td>Processing Ping Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>413</td>
<td>Processing Folder Sync Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>428</td>
<td>Processing Sync Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>421</td>
<td>Processing Ping Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>421</td>
<td>Processing Ping Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>428</td>
<td>Processing Sync Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>421</td>
<td>Processing Ping Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>428</td>
<td>Processing Sync Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>428</td>
<td>Processing Sync Command</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>413</td>
<td>Processing Folder Sync Command</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Database Task Name</th>
<th>Log Code</th>
<th>Description</th>
<th>Function Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
<tr>
<td>801</td>
<td>DatabaseTaskScheduler Error</td>
<td>MainLoop</td>
<td>There are currently no tasks that...</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

<table>
<thead>
<tr>
<th>Organization</th>
<th>DeviceSAKey</th>
<th>Error Code</th>
<th>Error Domain</th>
<th>Localized Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>4001</td>
<td>MCEAErrDomain</td>
<td>The profile “MDM iOS ActiveSync File” could not be found</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>1009</td>
<td>MProfileErrorDomain</td>
<td>The profile “MDM iOS ActiveSync File” is not found</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>21005</td>
<td>MCEAErrDomain</td>
<td>An identical Exchange account already exists</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>4001</td>
<td>MInstallationErrorDomain</td>
<td>Profile Failed to install</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>1009</td>
<td>MProfileErrorDomain</td>
<td>The profile “MDM iOS ActiveSync File” is not found</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>21005</td>
<td>MCEAErrDomain</td>
<td>An identical Exchange account already exists</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>4001</td>
<td>MInstallationErrorDomain</td>
<td>Profile Failed to install</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>1009</td>
<td>MProfileErrorDomain</td>
<td>The profile “MDM iOS ActiveSync File” is not found</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>21005</td>
<td>MCEAErrDomain</td>
<td>An identical Exchange account already exists</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>4001</td>
<td>MInstallationErrorDomain</td>
<td>Profile Failed to install</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>1009</td>
<td>MProfileErrorDomain</td>
<td>The profile “MDM iOS ActiveSync File” is not found</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>213</td>
<td>21005</td>
<td>MCEAErrDomain</td>
<td>An identical Exchange account already exists</td>
</tr>
</tbody>
</table>
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.
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.
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 Lock Device, Full Access needs to be enabled for both the Users and Administration categories above it.

<table>
<thead>
<tr>
<th>Parent Category</th>
<th>First Subset Level</th>
<th>Second Subset Level</th>
<th>Third Subset Level</th>
<th>Full Access</th>
<th>Read Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Monitor</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Add User</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Clear Activation Lock</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Clear Passcode</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Disable Device</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Disown Device</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Email Unlock PIN</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Full Wipe</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Lock Device</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Power Off</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Reboot</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Remote Ring</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Reset for Enrollment</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Reset PIN</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Reset to Shared Profile</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Selective Wipe</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Send VPP Invitation</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Send Welcome Letter</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Show Recovery Password</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Suspend Device</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Trigger APN</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Parent Category</td>
<td>First Subset Level</td>
<td>Second Subset Level</td>
<td>Third Subset Level</td>
<td>Full Access</td>
<td>Read Only</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple DEP Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovered Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messaging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send Notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Devices Summary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Access Point Names</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign CalDAV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign CardDAV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Exchange Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign LDAP Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assign Mail Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parent Category</td>
<td>First Subset Level</td>
<td>Second Subset Level</td>
<td>Third Subset Level</td>
<td>Full Access</td>
<td>Read Only</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign Managed Apps</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign Provisioning Profiles</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign SCEP Servers</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign SSO Configurations</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign Subscribed Calendars</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign VPN</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign Web Clips</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Assign Wi-Fi Networks</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Audit Data</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Client Certificates</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Custom Columns</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Configuration</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>File Archive</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iOS MDM Settings</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Last Sync Data</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Local Groups</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Location Data</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Search Phone Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Search Text Message Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User Configuration</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User Information</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>View Logs</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ActiveSync Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration/Feedback Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Device Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Error Chain Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GCM Sync Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iOS MDM Sync Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shared User Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZENworks Sync Log</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Administrative Servers</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Parent Category</td>
<td>First Subset Level</td>
<td>Second Subset Level</td>
<td>Third Subset Level</td>
<td>Full Access</td>
<td>Read Only</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ActiveSync Servers</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Administrative LDAP Servers</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>OpenID Provider</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SAML Identity Providers</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SMTP Server</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Android Corporate Resources</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPs</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi Networks</td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Management</td>
<td></td>
<td>Manage App Categories</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Managed Apps</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Novell Filr</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Whitelist/Blacklists</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Management</td>
<td></td>
<td>Certificate Authorities</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificate Templates</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Certificates</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Manager</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>iOS Corporate Resources</td>
<td></td>
<td>Access Point Names</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CalDAV Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CardDAV Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exchange Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDAP Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mail Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provisioning Profiles</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCEP Servers</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSO Configurations</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subscribed Calendars</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPNS</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web Clips</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wi-Fi Networks</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parent Category</td>
<td>First Subset Level</td>
<td>Second Subset Level</td>
<td>Third Subset Level</td>
<td>Full Access</td>
<td>Read Only</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Organization Control</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Columns</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Plans</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Share</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Notifications</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Groups</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Management</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Connection Schedules</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Schedules</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Suites</td>
<td>● ●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td>● ●</td>
<td></td>
</tr>
</tbody>
</table>
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.